МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Освітньо-професійна програма «Комп'ютерна інженерія

Спеціальність 123 «Комп'ютерна інженерія»

Група: 2БКС-27

КВАЛІФІКАЦІЙНА РОБОТА

БАКАЛАВРА

здобувача освіти денної форми навчання
БКС 27.25.000.00 БКР

Склярова Євгена Ігоровича

м. Одеса
2023 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «Одеський технічний фаховий коледж ОНАХТ»

Освітньо-професійна программа: «Комп'ютерна інженерія»
Спеціальність 123 «Комп'ютерна інженерія»
Група БКС-27

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи бакалавра на тему:

«Аналіз систем захисту веб-сайтувід несанкціонованого доступу»

Проектний матеріал складається з пояснювальної записки на 71 сторінках та мультимедійної презентації на 13 сторінках.

Здобувач освіти _____ (Скляров Є.І.)

Керівник роботи _____ (Харченко Р.Ю.)

Консультанти:

з охорони праці _____ (Чорновол Н.І.)

за дотриманням вимог ЄСКД _____ (Петрашова В.І.)

старший консультант _____ (Кривченко Ю.В.)

До захисту допущений

Завідувач кафедри _____ (Іванова Л.В.)

Завідуючий відділенням _____ (Скорнякова О.В)

Захист «26» 06 2023 р. Протокол ДКК № 3

Оцінка ДКК 4 (добре)

Секретар ДКК _____

АНОТАЦІЯ

Метою даної роботи є аналіз систем захисту веб-сайту від несанкціонованого доступу.

У роботі розглянути причини несанкціонованого доступу, способи несанкціонованого доступу, схеми несанкціонованого доступу до веб-ресурсів із використанням вразливостей програмного забезпечення вебсерверів та веб-сервісів. Описані методи запобіганню порушенню інформаційної безпеки он-лайн ресурсів та вебзастосунків на основі використання як комплексних систем захисту так і спеціалізованих інструментів захисту.

Проведено аналіз систем захисту веб-сайту, до якого увійшли наступні сегменти: аналіз захисту від атак на рівні додатків, аналіз захисту від атак на рівні мережі, аналіз системи легування та ін.

Вивчена процедура реагування на інциденти та проаналізован план реагування на інциденти.

Розглянуто питання з охорони праці та техніки безпеки.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «Одеський технічний фаховий коледж ОНАХТ»

Відділення *Комп'ютерних систем* Кафедра *Комп'ютерної інженерії*

Освітньо-професійна програма *«Комп'ютерна інженерія»*

Спеціальність *123 «Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР Беркань І.В.

"_____" _____ 20 ___ р.

ЗАВДАННЯ

на кваліфікаційну роботу бакалавра

здобувачу освіти *Склярову Євгену Ігоровичу*

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Аналіз систем захисту веб-сайту від несанкціонованого доступу*

затверджена наказом по коледжу від "___" *02* 20 *23* р. №_____

2. Термін здачі студентом кваліфікаційної роботи _____

3. Вихідні дані до роботи *1. Несанкціонований доступ до Веб-сайту; 2. Веб-додаткі; 3. Система захисту веб-сайту; 4. DDoS-атаки; 5. Firewal;l 6. Системи виявлення атак (СВА); 7. HTTP і HTTPS; 8. Web Firewall Application; Результати тестування антивірусів;*

4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити)

1. Несанкціонований доступ до Веб-сайту;

2. Аналіз вразливостей Веб-додатків;

3. Аналіз систем захисту веб-сайту

5. Перелік графічного матеріалу (слайдів мультимедійної презентації) _____

Термін «несанкціонований доступ до інформації»; Способи НСД; Динаміка зниженнякількісті Фаєрвол (Firewall); Найкращі антивіруси для Windows; Перехід від HTTP до HTTPS; Система аутентифікації/авторизації; Хмарне резервне копіювання; Лінійна структура сайту Приклад моніторингу веб-сервісів, на базі Dotcom-Monitor.com; Гратчаста структура сайту Приклад моніторингу веб-додатків на базі Dotcom-Monitor.com; Деревоподібна структура сайту

6. Консультанти по кваліфікаційній роботі, із зазначенням розділів, що стосуються їх

Розділ	Консультант	ПІДПИС	
		Завдання видав	Завдання прийняв
Основний	*Харченко Р.Ю.*		
Охорона праці	*Чорновол Н.І.*		
Нормоконтроль	*Петрашова В.І.*		
Старший консультант	*Кривченко Ю.В..*		

7. Дата видачі завдання 01.05.2023

Керівник роботи *Харченко Р.Ю.* _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	*Аналіз предметної галузі*	5.05.2023	
2.	*Аналіз технічного завдання та пошук літератури*	7.05.2023	
3.	*Огляд безпеки веб-додатків*	9.05.2023	
4.	*Огляд ризиків при несанкціонованому доступі*	11.05.2023	
5.	*Аналіз вразливості сайтів*	13.05.2023	
6.	*Аналіз статистики вразливостей Веб-додатків*	16.05.2023	
7.	*Аналіз вразливостей сайтів*	18.05.2023	
8.	*Огляд сканерів вразливостей*	20.05.2023	
9.	*Перевірка конфігурації сервера*	23.05.2023	
10.	*Визначення складових систем захисту веб-сайту*	25.05.2023	
11.	*Аналіз загальної архітектури сайту*	27.05.2023	
12.	*Аналіз захисту від атак на рівні додатків*	30.05.2023	
13.	*Аналіз захисту від атак на рівні мережі*	3.06.2023	
14.	*Аналіз процедур реагування на інциденти*	5.06.2023	
15.	*Розробка питань з охорони праці*	8.06.2023	
16.	*Оформлення креслень та тексту ПЗ*	10.06.2023	

Здобувач освіти _____
(підпис)

Керівник роботи _____
(підпис

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			БКС 27. 25. 000. 00 БКР	Випускна робота бакалавра	71	
А4			БКС 27. 25 000. 00 БКР ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	БКС 27. 25 000. 00 БКР		
Розробив		Скляров Є.І.			Аналіз систем захисту Web-сайту від несанкціонованого доступу	Літ.	Аркуш 4 / Аркушів
Перевірив		Харченко Р.Ю.				У Д П	
Н. Контр.		Петрашова В.І.				ОТФК ОНТУ, гр. 2БКС-27	
Затверд.		Кривченко Ю.В.					

ЗМІСТ

ВСТУП

Сучасну компанію із сегменту малого бізнесу, не кажучи вже про великі фінансові чи промислові підприємства, складно уявити без веб-додатку. Бажаючи отримати послугу або придбати продукт, ми все частіше вважаємо за краще зробити це онлайн, ознайомившись з асортиментом компанії на її сайті. Завдяки розвитку веб-технологій останніми роками суттєво підвищилися доступність та якість онлайн послуг. Сайт став візитною карткою не тільки для бізнесу, а й для державних структур, істотно впливаючи на репутацію.

Як показують дослідження, у 19% веб-додатків є вразливості, що дозволяють зловмиснику отримати контроль як над самим додатком, так і над ОС сервера. Якщо сервер знаходиться на периметрі мережі організації, зловмисник може проникнути до внутрішньої мережі компанії. У більшості випадків веб-програми вразливі через помилки в коді. Змінами у конфігурації можуть бути усунені лише 17% уразливостей, причому більшість із них мають низький рівень ризику. Для усунення критично небезпечних уразливостей, як правило, потрібно внести виправлення до коду. Кожен другий витік може призвести до розголошення облікових даних, у тому числі для доступу до сторонніх ресурсів. Як приклад можна навести доступні всім користувачам конфігураційні файли з паролями, що зберігаються в них. В середньому на один веб-додаток припадає 33 уразливості, шість з яких мають високий рівень ризику. Число критично небезпечних уразливостей, яке припадає на один веб-додаток, порівняно з 2020 роком, зросло в 2 рази.

Оскільки архітектури веб-додатків стають все більш поширеними і складними, вони можуть стати основним джерелом бізнес-ризиків, якщо власники ресурсів не подбають про високоякісні системи, здатні протистояти хакерським атакам. Така ситуація змушує власників веб-додатків підтримувати свої програми на високому технічному рівні, що неможливо без належної уваги до захисту від кібератак.

1 ТЕХНОЛОГІЧНИЙ РОЗДІЛ

1.1 Несанкціонований доступ до Веб-сайту

1.1.1Безпека веб-додатків

Безпека веб-додатків — це захисні заходи, за яких зловмисник не зможе отримати доступ до конфіденційних даних як ззовні при спробі злому, так і всередині компанії через нелегітимний доступ.Захист веб-додатків є актуальним у будь-яких умовах — у тому числі й усередині периметра компанії.

Загальна стратегія безпеки програмного забезпечення ґрунтується на трьох основних принципах:

- **конфіденційність** - приховування певних ресурсів чи інформації;
- **цілісність** – очікування, що ресурс може бути змінений лише відповідним способом певною групою користувачів; а якщо дані ушкоджуються або неправильно змінюються, повинна бути передбачена процедура відновлення;
- **доступність** - вимоги про те, що ресурси мають бути доступні авторизованому користувачеві, внутрішньому об'єкту або пристрою.

Усі сайти електронної комерції є привабливими цілями для хакерів через особисту та платіжну інформацію, необхідну для завершення продажу. Навіть якщо система безпосередньо не обробляє карткові транзакції, зламаний сайт може спрямувати клієнтів на неправильну сторінку або змінити дані замовлення до того, як вони будуть відправлені платіжному процесору. Злом може мати довгострокові наслідки як для покупців, такі для продавців. Покупці можуть зазнати фінансових втрат, а продавці можуть зіткнутися зі шкодою для своєї репутації, втратою товарів і загрозою судових розглядів..

Інтернет-магазини також є однією з найпривабливіших мішеней для хакерів, оскільки злом може відкрити зловмисникам доступ до особистих даних користувачів та їх платіжної інформації. Незважаючи на розробку нових засобів захисту, кількість атак на веб-додатки зростає з кожним роком.

1.1.2 Несанкціонований доступ (НСД)

Несанкціонований доступ (традиційно використовуване скорочення — НСД) слід розуміти як отримання можливості обробляти дані, що зберігаються на різних носіях та накопичувачах, за допомогою самовільної зміни чи фальсифікації відповідних прав та повноважень. Подібне явище має місце, коли якась інформація призначена лише певному колу осіб, але існуюче обмеження порушується. Термін «несанкціонований доступ до інформації» розкрито на Рисунку 1.1.

Рисунок 1.1 Термін «несанкціонований доступ до інформації»

НСД відбувається через помилки керівного органу або системи комп'ютерної безпеки, а також через підміну підтверджуючих документів і незаконне отримання інформації про інших осіб, які мають право доступу.

Класифікація несанкціонованого доступу

Кіберзлочинці можуть отримати несанкціонований доступ, атакуючи веб-сайти та веб-додатки. Це можливо, якщо веб-сайт заражений шкідливим програмним забезпеченням, зламаний або виявлені вразливості. Крім того, ресурси можуть піддаватися DDoS-атакам. Також зловмисники можуть отримати доступ до інформації, перехопивши дані за допомогою шпигунських

програм або сніферів. Сніфери (sniffers) - це програми, здатні перехоплювати та аналізувати мережевий трафік.

Вразливе програмне забезпечення та подальший його злам – це добре відомі причини несанкціонованого доступу до даних. Інші поширені методи включають використання грубої сили (підбір паролів і злом акаунтів) для вгадування паролів до облікових записів адміністраторів та соціальну інженерію. Серйозні прогалини в безпеці часто виникають через неправильну конфігурацію додатків і програмного забезпечення, несанкціоновану відділом інформаційної безпеки.

Причини несанкціонованого доступу

Причини виникнення несанкціонованого доступу можуть бути такиминаступними.

- Неправильно настроєна система контролю доступу до певних баз даних. Фактичну відповідальність несе адміністратор або інша особа, яка займається відповідним питанням.
- Спостерігаються прогалини у створенні захисту різних засобів авторизації. Це можуть бути паролі, що легко вгадуються, автоматичне збереження даних, що використовуються для авторизації в конкретній системі, збереження логіну та інших відомостей у загальнодоступному місці.
- Використовується застаріле програмне забезпечення, з'являються помилки або конфлікти. Проблема вирішується своєчасним оновленням, встановленням виключно ліцензійних версій програм, виконанням стандартних правил комп'ютерної безпеки, зверненням до профільних фахівців.
- Відбувається зловживання довірою та (або) службовими повноваженнями.
- Застосовуються трояни, клавіатурні шпигуни та інші подібні засоби, схожі на кібершпигунство.
- Прослуховуються та перехоплюються різними способами канали зв'язку. Інші варіанти.

Здійснення несанкціонованого доступу відбувається по-різному, кількість способів зростає у міру розвитку віртуального світу загалом. Впливає і поява нових видів гаджетів. Проте існуючі методи можна умовно звести до двох. Перший – обхід системи доступу, другий – незаконне отримання даних ідентифікованого користувача.

Способи несанкціонованого доступу

Кіберзлочинці можуть отримати особисту інформацію, комерційну таємницю, і нтелектуальну власність (зазвичай особливий інтерес становлять нові технології) та внутрішньофірмові комунікації. Державна таємниця є особливо вразливою до атак. Несанкціонований доступ іноді може повністю або частково паралізувати роботу певних організацій.. Основні способи отримання несанкціонованого доступу до інформації показані на Рисунку 1.2.

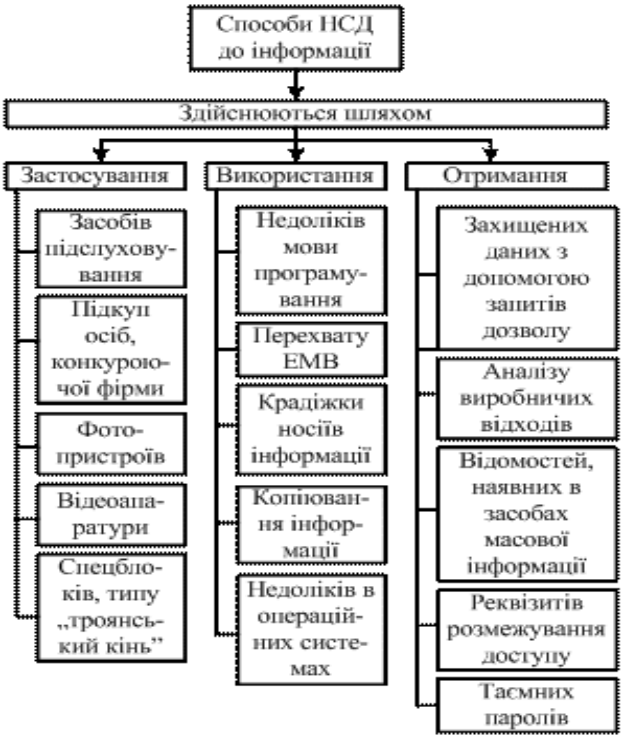


Рисунок 1.2 Способи НСД

- Злам інформаційних ресурсів (корпоративних мереж, веб-сайтів, хмарних сервісів, окремих комп'ютерів та мобільних пристроїв).

- Перехоплення повідомлень. Маються на увазі будь-які надіслані послання, включаючи електронну пошту, месенджери, SMS та інше.
- Збір даних. Може виконуватися законними методами, але переслідувати протиправну мету.
- Шантаж, здирство, дача хабара.
- Викрадення інформації.

Отримання несанкціонованого доступу загрожує не лише витоком даних та (або) ризиком модифікації відомостей, ай ймовірністю впровадження дистанційно керованого програмного забезпечення, що ставить під загрозу систему комп'ютерної безпеки в цілому. З'являється ризик втрати керування. Також важливі дані редагуються, видаляються, зловмисник може заблокувати доступ до них, зняти копії для подальшого протиправного використання.

НСД нерідко спрямований на перехоплення ключових повідомлень, що мають принципове значення для захисту ПК, локальної системи або конкретно взятих документів. В останньому випадку отримання несанкціонованого доступу стає частиною більшої операції, що нерідко має відношення до кіберрозвідки. Зловмисник здатний використовувати ПК як плацдарм для перехоплення даних від інших пристроїв усередині мережі, розсилки спаму, шкідливого коду. Нарешті, НСД дає можливість знищити цінні дані, що зберігаються, і (або) повністю вивести з ладу комп'ютерну систему.

Втрата контролю над керуючими системами, може порушити роботу провайдерів, транспортних організацій, інтернет-магазинів тощо. Деякі об'єкти є стратегічно важливими, тому, важливо розробити грамотно організований захист від атак, які можуть до привести до серйозних наслідків. Для підвищення ефективності протидії загрозам ІБ, що загострилися, необхідна активізація і консолідація сил і технічних засобів суб'єктів критичної інформаційної інфраструктури.

1.1.3 Ризики при несанкціонованому доступі

Несанкціонований доступ до будь–якої системи або даних створює різноманітні ризики і може мати значний вплив на діяльність та безпеку компанії чи організації. Нижче наведено деякі з ризиків, пов'язаних з несанкціонованим доступом:

- Втрата конфіденційної інформації: Несанкціонований доступ може призвести до втрати конфіденційної інформації, такої як особисті дані клієнтів, бізнес-стратегії, плани маркетингу і технічна інформація. Це може призвести до витоку конфіденційної інформації, яка може бути використана зловмисниками для здійснення шахрайства або конкурентного шпигунства.
- Порушення законодавства: Несанкціонований доступ до систем і даних може призвести до порушення законодавства про захист даних і конфіденційність. Це може призвести до покладання відповідальності на компанію або організацію, що може призвести до серйозних фінансових та репутаційних наслідків.
- Втрата даних: Несанкціонований доступ може призвести до втрати або пошкодження даних, що може завдати шкоди роботі компанії або організації. Це може призвести до втрати доступу до важливої інформації, а також до порушення роботи систем компанії або організації.
- Збитки від викрадення: якщо зловмисник отримує доступ до цінних даних, таких як інтелектуальна власність, фінансова інформація або розробки продуктів, то виникнення шкоди може бути дуже значним. Вартість втраченої інформації може бути величезною, якщо зловмисник використовує її для здійснення крадіжок або шахрайства.
- Загрози безпеці: Несанкціонований доступ може створити загрози безпеці для компанії або організації, такі як віруси, шкідливі програми та зловмисний код, які можуть призвести до порушення роботи систем і створення загроз для безпеки даних.

Більшість операційних систем передбачає автоматичний вбудований захист від несанкціонованого доступу (НСД). Але зазначені способи мають істотний недолік: вони швидко застарівають. Відповідно, фахівці рекомендують використовувати пакет програм, що постійно оновлюється, для контролю доступу до окремих документів.

Одними з найнадійніших визнаються апаратні засоби захисту, вони найчастіше використовуються банківськими організаціями під час видачі грошей. Прикладами таких засобів можуть стати електронні замки.

До підвищених запобіжних заходів відносять строгу і посилену автентифікацію. Особливий акцент може бути зроблено на протоколі дій адміністратора та користувачів. Серед технологій, що підтримуються, все більшого поширення останнім часом отримують USB-ключі і всілякі смарт-карти. Надійними визнаються одноразові паролі. Експерти також вважають, що майбутнє – за біометрією. В рамках останньої можуть використовуватися не лише відбитки пальців, а й райдужна оболонка ока, малюнок вен на руках. Максимальний рівень безпеки досягається при багатофакторній автентифікації, коли доступ надається при збігу даних з різних джерел (наприклад, результатів сканування райдужної оболонки ока, пред'явлення смарт-карти та введення пароля). Подібні системи вже успішно реалізовані.

Зведення по ризиках

- Конфіденційні дані часто містять затребувану зловмисниками та інсайдерами інформацію: персональні дані, інформацію про банківські картки, IP-адреси, електронну пошту та багато іншого.
- Надмірний доступ – одна з основних причин витоків даних. Якщо користувачам надається доступ до більшої кількості даних, ніж необхідно для виконання їх робочих обов'язків, це може створити ризик витоку даних. Якщо користувачі мають можливість змінювати, видаляти або передавати даний доступ іншим користувачам, це може також збільшити ризик витоку даних.

- Конфіденційні дані з надлишковим доступом становлять серйозну загрозубезпеки. Тому важливо вживати заходів безпеки для захисту конфіденційної інформації, включаючи обмеження доступу до неї лише потрібним особам, шифрування даних та забезпечення резервного копіювання. Крім того, необхідно проводити регулярну перевірку наявності надлишкового доступу до конфіденційної інформації та забезпечувати відповідний рівень кібербезпеки для попередження можливих кібератак та інших загроз безпеки.
- Перебір паролів (брутфорс) є одним з найпоширеніших методів атак на системи безпеки. Для запобігання таких атак можна використовувати наступні методи:
  - Вимагати складні паролі
  - Блокування доступу
  - Двофакторна аутентифікація
  - Оновлювати паролі
  - Використання криптографічно безпечних алгоритмів

Багато файлів містять критично важливу інформацію про співробітників, клієнтів абопроектах, а також інші відомості, важливі длябізнесу. Ці дані часто регулюються міжнародними, національними або галузевими стандартами.Конфіденційні дані, відкриті для глобальних груп, що представляють для бізнесу значний ризик. Їх слід виявлятита виправляти так, щоб до них мали доступтільки ті користувачі, кому це необхіднодо виконання робочих обов'язків.

1.2 Аналіз вразливостей Веб-додатків

1.2.1 Вразливості сайтів

Для будь-кого, хто керує веб-сайтом, на першому місці має стояти питання безпеки. Критичні загрози та вразливості можуть сильно вдарити як по

репутації, так і по гаманцю.Можна виділити п'ять основних типів уразливостей, з якими може зіткнутися будь-який веб-сайт:

1) IDOR: проста і дуже небезпечна вразливість

IDOR (InsecureDirectObjectReference, небезпечні прямі посилання на об'єкти) – вразливість, яка дозволяє отримати несанкціонований доступ до веб-сторінок чи файлів.

Найпоширеніший випадок IDOR – коли зловмисник перебирає передбачуваний ідентифікатор та отримує доступ до чужих даних.Таким чином, просто перебираючи ID в URL, можна читати та змінювати контактну інформацію всіх зареєстрованих користувачів. Проблема полягає в тому, що при запитах на сайт він не перевіряє належність даних конкретного відвідувача.

До чого може призвести:

- Розголошення конфіденційної інформації. Отримавши доступ до облікових записів користувачів, зловмисники побачать їх особисті дані;
- Обхід аутентифікації: можна отримати доступ одразу до сотень або тисяч облікових записів із цією вразливістю;
- Зміна даних: редагуючи вашу контактну інформацію, зловмисник може використовувати її у своїх цілях. Наприклад, надіслати усі ваші замовлення в інтернет-магазині до себе додому;
- Захоплення облікового запису. У деяких випадках у такий спосіб можна забрати акаунти користувачів, викрасти гроші з їхнього балансу та наробити багато інших неприємностей.

2) XSS: поганий сценарій

XSS - Cross Site Scripting (міжсайтове виконання сценаріїв). Строго кажучи, XSS – не вразливість, а атака. Але умовимося, що під XSS ми розуміємо уразливості, що дозволяють проводити атаку XSS.Коли XSS-атака відбувається, в веб-сторінку вбудовується шкідливий код. І як тільки відвідувач сайту відкриє цю сторінку, почне виконувати якийсь неприємний

сценарій. Найчастіше під шкідливим кодом мається на увазі використання html-тегів або скриптів на JavaScript.

XSS бувають кількох різновидів:

- Збережені (stored). Код, який дозволяє проводити атаку, постійно знаходиться на сервері та виконується автоматично.
- Відбиті (reflected). У цьому випадку шкідливого коду немає на самому сайті, але він міститься в заздалегідь створеному зловмисником веб-посиланні. Обробляючи цей «поганий» шматок коду, сайт може ненавмисно запустити в браузері користувача скрипт, який перехопить дані або виконає інше «корисне навантаження», якщо мається на увазі саме навантаження XSS.
- DOM-based. Варіант відображених, коли шкідливий код не відправляється на сервер, а виконується одразу у браузері.

До чого може призвести:

- Перехоплення сесії користувача (файли cookies);
- Зміна сторінки (наприклад, форми введення логіну/паролю), щоб викрасти конфіденційні дані;
- Впровадження скриптів на сайти з високою відвідуваністю (з метою реклами, накрутки переглядів, DDoS-атак та іншого);
- Використання шкідливих програм на зовнішньо безпечних сайтах.

3) SQL-ін'єкції

SQL-ін'єкція - це атака, спрямована на сайт або веб-додаток, в ході якої користувач може обхідним шляхом отримати інформацію з бази даних за допомогою SQL-запитів. У разі успішної атаки дані користувача інтерпретуються як частина SQL-коду запиту, і таким чином змінюється його логіка. Як і інші атаки, SQL-ін'єкція експлуатує вразливості та недоробки в коді, і потрібно проводити аналіз сайту, щоб знайти «слабкі» місця.

SQL-ін'єкція можлива за відсутності фільтрацій вхідних параметрів - хакери можуть змінювати їх, щоб отримувати потрібні дані. Вразливими

місцями в цьому випадку служать поля введення користувача і URL-адреси, що взаємодіють з базою даних.

До чого може призвести:

- Витік конфіденційних даних (паролей, даних банківських карток та іншого);
- Впровадження шкідливого контенту у вразливі поля;
- Зміна бази даних;
- Доступ до операцій адміністрування.

4) Обхід директорій

Обхід директорій (PathtraversalабоDirectorytraversal) полягає в тому, що хакер отримує доступ до директорій або файлів на сервері за допомогою маніпуляцій змінних, що посилаються на ці файли. Наприклад, для завантаження файлу з сервера вказується його ім'я:

www.site.ru/download?file=file.pdf

За допомогою символу, що означає директорії (../), можна отримати доступ до інших файлів, просто додавши його в рядок:

www.site.ru/download?file=../../../etc/passwd

До чого може призвести:

- Несанкціонований доступ та зміна системних файлів, а також вихідний код сайту або веб-додатки;
- Видалене виконання шкідливого коду;
- Підміна сторінок сайту.

5) Вразливості під час завантаження файлів

На багатьох сайтах користувачі можуть підвантажувати різні файли: наприклад, змінювати свою фотографію профілю або прикріплювати зображення до коментарів. Якщо на сайті доступне завантаження файлів користувачами, потрібно ретельно підійти до питання безпеки.

Найпоширеніша помилка – відсутність перевірки типу файлу. Наприклад, користувач під час завантаження фотографії може замість .jpeg або .png підвантажити php-скрипт і виконати його.

Тип файлу зазвичай перевіряється за заголовком, але така перевірка небезпечна, оскільки заголовок можна підмінити. Перевірки на стороні клієнта також іноді можна обійти. І навіть використання чорного/білого списку розширень може бути неефективним, оскільки іноді шкідливий код вбудовується прямо у файл із «правильним» розширенням.

До чого може призвести:

- Віддалене виконання коду
- SQL-ін'єкції
- Введення шкідливого коду
- Злам веб-додатка

Отже, важливо вживати заходів безпеки під час завантаження файлів, таких як перевірка на віруси та обмеження доступу до завантажуваних файлів.

1.2.2 Статистика вразливостей Веб-додатків

Близько 70% додатків містять критичні вразливості, які дозволяють кіберзлочинцям отримати доступ до конфіденційних даних організацій та користувачів, а також від імені жертви здійснювати у вразливих онлайн-сервісах різні операції.Такі результати аналізу захищеності веб-додатків, що належать організаціям державного та банківського сектора, сфери виробництва, інформаційних технологій, інформаційної безпеки та ін.Було проаналізовано понад 30 веб-додатків під час кіберучень, тестувань на проникнення та проектів щодо аналізу захищеності. Серед обраних для аналізу додатків - інтернет-портали компаній, системи дистанційного банківського обслуговування та ін. Результати дослідження підтверджують, що критичні та легко експлуатовані вразливості містять практично всі веб-додатки, що

аналізуються. Більшість з них пов'язана з відсутністю фільтрації даних, що надходять на стороні веб-сервера, а також з недоліками на рівні бізнес-логіки додатків.

Майже 70% веб-додатків виявилися схильні до IDOR-уразливостей. Експлуатуючи їх, зловмисник може шляхом перебору знайти ідентифікатори, що використовуються в системі, і отримати несанкціонований доступ до даних користувачів. Найчастіше ця вразливість зустрічається у веб-додатках зі складною логічною структурою – наприклад, у системах дистанційного банківського обслуговування. Завдяки IDOR-уразливості кіберзлочинці отримують інформацію про транзакції та стан рахунків користувачів, а також можуть змінити дані їх профілів.

Більше 50% веб-додатків містять недоліки у фільтрації даних, що надходять на сервер, що дає можливість провести атаки типу XSS. Як уже говорилося вище,дані атаки дозволяють кіберзлочинцю впровадити на веб-сторінку шкідливий JavaScript-код, який запуститься в браузері жертви при відкритті сторінки. Цей код, взаємодіючи з веб-сервером шахраїв, може передавати cookie-файли користувача, внаслідок чого кіберзлочинець зможе авторизуватися на інтернет-ресурсах під обліковими даними жертви та діяти від її імені.

Ще 30% уразливостей пов'язані з можливістю впровадження SQL-коду через відсутність чи некоректну фільтрацію вхідних запитів від користувача. Таким чином, шахраї отримують контроль над базою даних організації і в тому числі доступ до конфіденційних даних клієнтів (наприклад, даних паспорта, кредитної картки, інформації про транзакції тощо), а також можливість міняти їх безпосередньо на сервері.

Результати дослідження застосовні передусім до тих організацій, зрілість яких з погляду ІБ недостатньо висока: не збудовані процеси організації системи захисту, необхідні засоби захисту не застосовуються зовсім чи невчасно оновлюються.До таких організацій належать державні організації та

організації, які не працюють в онлайн-сфері. "Якщо ж ми говоримо, наприклад, про представників фінансової сфери, більша частина з них перебуває на високому та середньому рівні зрілості.

Вразливість типу IDOR не випадково входить до топ-10. У наш час заявляти про повну безпеку будь-якого продукту на ринку вкрай ризиковано, в умовах сучасного ринку неможливо "вивести" продукт, який був би повністю "сек'юрним". На сьогоднішній день висока ймовірність подібного роду вразливостей пов'язана з нестачею кадрів.Вразливість типу IDORприсутні у кожному третьому веб-додатку (37%) і, зокрема, у кожній третій системі дистанційного банківського обслуговування (31%), однак він вважає, що частка таких вразливостей знижується. Така динаміка пов'язана в першу чергу з впровадженням процесів безпечної розробки та спільною увагою до проблем захищеності веб-додатків, особливо у фінансовій сфері. Загалом в останні роки в середньому кількість вразливостей, що припадає на один веб-додаток, знизилася в півтора рази. Рисунок 1.3.

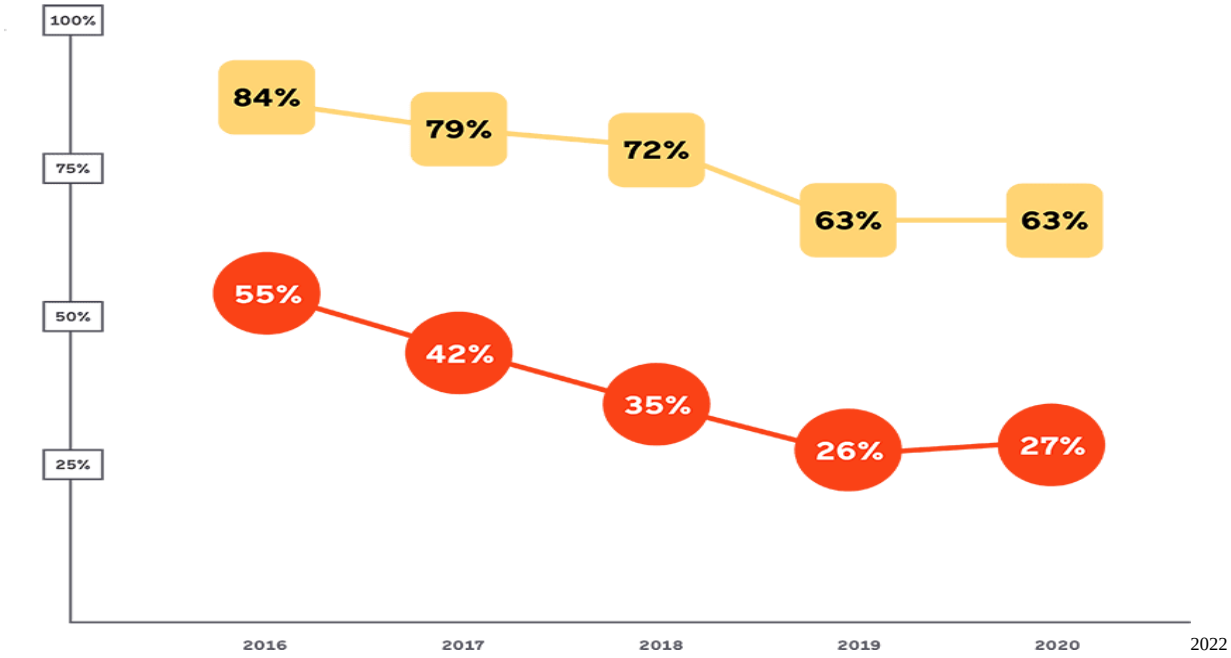


Рисунок 1.3.Динаміка зниженнякількісті вразливостей, що припадає на один веб-додаток

Де, - вразливості середнього ступеня небезпеки

- вразливості високого ступеня небезпеки

Однак рівень уразливості все ще критичний, у кожному другому сайті (50%), а в середньому на один веб-додаток сьогодні припадає чотири вразливості з високим рівнем ризику. Уразливість типу IDOR виникає через те, що посилання на сторінку одного користувача може відрізнятися від посилання на сторінку іншого користувача лише одним ідентифікатором. Якщо контроль доступу реалізований розробниками неефективно або зовсім відсутній, то зловмисник може перебирати значення такого ідентифікатора в засланні та заходити на сторінки інших користувачів, читати на них інформацію, а можливо і змінювати якісь дані. Необхідно в першу чергу суворо розмежовувати привілеї користувачів доступу до сторінок на сайті, а також використовувати ідентифікатори, що складно вгадуються, для параметрів у посиланнях.

Веб-додатки дуже часто потрапляють під атаки кіберзлочинців, оскільки можуть бути для них як джерелом цінних даних про компанію-розробника та користувачів програми, так і зручною вхідною точкою для подальших атак. Проте, розробники поступово починають усвідомлювати значущість забезпечення інформаційної безпеки всіх етапах створення ПЗ. "У сучасних проектах фіксується як підвищення рівня безпеки інструментів розробки, так і збільшення якості та кількості перевірок на вразливості. Однак загальна кількість додатків, що випускаються, настільки велика, що випадків, коли в пріоритет ставиться функціональність, як і раніше дуже багато. Це призводить до того, що програми, доступні кінцевим користувачам, часто містять різні вразливості, у тому числі IDOR.

Захист веб-додатків – це завдання розробника. Не варто повністю покладатися на засоби захисту - зокрема, WebApplicationFirewall не може виявити атаки, спрямовані на вразливість у логіці роботи програми, наприклад IDOR. Необхідно вже на етапі створення програми дотримуватися ключових принципів безпечної розробки: завжди фільтрувати дані, що надходять від користувача, і перевіряти права доступу - на рівні Back-end, а не клієнтського

інтерфейсу. Крім того, необхідно періодично проводити аналіз захищеності програми.

У 20% атак на юридичні особи у 2022 році об'єктами атаки ставали саме веб-ресурси. Імовірність успішної атаки досить велика, якщо організація не дбає про безпеку своїх веб-ресурсів.

Рекомендується використовувати міжмережевий екран рівня програми - webapplicationfirewall - і звичайно ж, регулярно виявляти та усувати вразливості у коді веб-додатків.

Викрадення корпоративних чи особистих даних для подальшого шантажу та інших злочинних дій – одна з найчастіших цілей кібератак. В останні роки значно почастішали випадки атак на медустанови, наприклад, інцидент, що стався 22 березня, коли кібератаці зазнали дані однієї з найбільших мереж лікарень в Європі Assistancepublique - HôpitauxdeParis. Раніше також зазнала атака університетська лікарня міста Брно в Чехії. Внаслідок інциденту адміністрація установи була змушена відключити сервери та призупинити дослідження. Крім очевидної суспільної шкоди через припинення досліджень, зловмисники також можуть викрасти дані пацієнтів і використовувати їх для шантажу або продажу.

Прямі атаки на великі організації здійснюються негаразд часто, оскільки потенційні жертви, зазвичай, мають досить високий рівень зрілості ІБ. Ресурси, витрачені на організацію проникнення, які завжди можуть окупитися. Однак, при відході бізнесу на віддалену роботу став помітним сплеск активності кібершахраїв, які збільшили кількість атак на компанії, їхніх співробітників та контрагентів з використанням методів соціотехнічної інженерії та фішингу. Метою подібних зламів є отримання інформації, яка надалі дозволить реалізувати та розвинути таргетовану атаку на організацію. Один із популярних методів, яким зараз користуються шахраї, - реєстрація фішингових доменів підприємств та реалізація атаки "людина посередині". Зловмисник вклинюється в листування між контрагентами та спілкується зі сторонами

угоди від їхнього імені, таким чином маючи можливість отримати конфіденційну інформацію або безпосередньо вивести кошти з рахунку компанії.

1.2.3 Аналіз вразливостей сайтів

Аналіз вразливостей сайтів є важливим етапом при захисті веб-додатків від можливих атак з боку зловмисників. Для здійснення аналізу вразливостей сайтів можна використовувати різні методики і інструменти, наприклад:

- Сканери вразливостей: це програмні засоби, які автоматично перевіряють веб-додаток на наявність вразливостей, таких як SQL-ін'єкції, XSS-атаки, CSRF-атаки тощо. Найбільш популярними сканерами вразливостей є Acunetix, BurpSuite, Nessus, OpenVAS.
- Ручна перевірка коду: при ручній перевірці програміст аналізує код веб-додатка з точки зору потенційних вразливостей і шукає можливі вразливі місця в коді. Цей підхід потребує значної кваліфікації і досвіду, тому що потрібно розуміти особливості різних типів атак та вміти шукати вразливості в коді.
- Перевірка конфігурації сервера: цей підхід передбачає перевірку налаштувань сервера, який хостить веб-додаток. Наприклад, можна перевірити налаштування файрволу, відкриті порти, наявність вразливих служб тощо.
- Використання спеціальних інструментів: для перевірки вразливостей сайтів можна використовувати різні інструменти, які допомагають зібрати інформацію про сайт та знайти потенційні вразливості. Наприклад, можна використовувати інструменти для сканування портів, виявлення відкритих сервісів та інших слабкість безпеки.

1.2.3.1 Сканери вразливостей

Сканер вразливостей - це інструмент для виявлення можливих слабких місць в програмному забезпеченні, операційних системах, мережах та інших компонентах інфраструктури, які можуть бути використані зловмисниками для злому або крадіжки даних. Аналіз сканера вразливостей включає в себе оцінку знайдених вразливостей та рекомендації щодо їх виправлення.

Основні етапи роботи сканера вразливостей:

- Сканування: сканер вразливостей перевіряє інфраструктуру на наявність вразливостей, використовуючи різні методи, такі як порт-сканування, аналіз коду програм, перевірку на наявність відомих вразливостей та інші.
- Класифікація: вразливості, виявлені сканером, класифікуються за типом та ступенем серйозності.
- Оцінка ризику: визначається ступінь ризику, який вразливості можуть представляти для інфраструктури, від імовірності злому до наслідків від успішного нападу.
- Рекомендації: сканер вразливостей надає рекомендації щодо виправлення виявлених вразливостей, зокрема оновлення програмного забезпечення, встановлення патчів або настройку мережевої безпеки.
- Перевірка: після виправлення вразливостей проводиться повторне сканування для перевірки їх успішного виправлення.

Використання сканера вразливостей є важливим етапом в забезпеченні безпеки інфраструктури, оскільки дозволяє виявити можливі загрози та вжити заходів для їх попередження. Проте варто пам'ятати, що сканер вразливостей не є панацеєю від усіх загроз.

Існує багато різних сканерів вразливостей, які можуть допомогти знайти проблеми з безпекою на вашому веб-сайті або мережі. Ось декілька з найкращих сканерів вразливостей:

1. Nessus є одним з найпопулярніших сканерів вразливостей, який дозволяє знайти вразливості у програмному забезпеченні, мережі та операційній системі. Він має велику базу даних вразливостей та може здійснювати сканування на підставі різних стандартів безпеки, таких як PCI DSS, HIPAA та CIS.

2. OpenVAS є відкритим сканером вразливостей, який має велику базу даних вразливостей та може здійснювати сканування мереж, операційних систем та програмного забезпечення. Він підтримує різні протоколи, такі як SNMP, SSH та SMB.

3. Qualys - це хмарний сервіс сканування вразливостей, який дозволяє виявляти вразливості на веб-сайті та мережі. Він має широкий спектр інструментів для аналізу вразливостей, таких як тест на переповнення буфера, тест на XSS та SQL-ін'єкції.

4. Acunetix - це інструмент сканування вразливостей веб-додатків, який може виявляти різні типи вразливостей, такі як XSS, CSRF та SQL-ін'єкції. Він також має інтеграцію з різними сервісами для управління проектами та системами контролю версій.

5. Burp Suite - це інструмент для тестування вразливостей веб-додатків, який має велику кількість функцій, включаючи перехоплення трафіку.

1.2.3.2 Ручна перевірка коду веб-додатка

Головна мета ручних тестів — заздалегідь переконатися, що заявлений функціонал працездатний, не має помилок і видає очікувані, заплановані результати. Без них не можна бути впевненим, що можна працювати далі. Особливо це актуально для функцій, на реалізацію яких пов'язана подальша технологія. У такому разі метушня зі створенням автотестів на ці фічі стає блокуючим фактором для всієї розробки продукту, зсуваючи терміни та

зриваючи дедлайни. Момент, коли кейси прийде час автоматизувати, все одно рано чи пізно настане — але не варто прагнути наблизити його штучно в гонитві за тотальним винятком ручної праці.

На додаток до цього, на перших етапах розробки програми автоматизація може виявитися досить дорогою. Потрібен спеціаліст, який має специфічну кваліфікацію (і, можливо, не один). Постійна підтримка тестів у актуальному стані потребує витрат ресурсів. А місяці простою, присвячені вдосконаленню автотесту, вдарять за мотивацією команди.

1. Перший крок безпосередньо тестування – смоук-тест: оцінка на те, що додаток або його нова частина взагалі готові до перевірки. Смоук-тест - це перевірка того, чи запускається програма або конкретна функція в принципі.Смоук-тест – швидкий спосіб переконатися, чи можемо ми взагалі розпочати функціональне тестування. Термін прийшов від творців плат і мікросхем, які спочатку повинні були переконатися, чи не згорить нова схема — звідси й назва: задимилася/не задимилася.

2. Наступний етап – проведення регрес-тестів. У ручному або автоматичному режимі проводиться основний заздалегідь запланований масив тестів.Наступний етап – проведення регрес-тестів. У ручному або автоматичному режимі проводиться основний заздалегідь запланований масив тестів.Регресійне тестування добре тим, що воно дозволяє знайти помилки навіть у тих місцях, де раніше все було гаразд. Це відбувається завдяки тому, що регрес – це оцінка функціоналу на стандартний набір кейсів при впровадженні кожного нового модуля та кожної зміни програми. Адже, коли розробники додають новий функціонал, може бути пошкоджена поточна версія або нова фіча може вступати в конфлікт з уже існуючими.

Ручне тестування дає велику перевагу за швидкістю і трудовитратами на перших етапах, а в міру розростання додатка та появи великої кількості регресивних тестів воно переходить у розряд “оперативного тестування”. Воно

буде актуальним і при необхідності терміново перевірити як додаток відреагує на зміну операційної системи або оновлення оточення.

1.2.3.3 Перевірка конфігурації сервера

Один з ключових аспектів забезпечення безпеки та стабільності веб-додатку - це перевірка конфігурації сервера, на якому він хоститься.Конфігурація сервера - це налаштування та параметризація серверного обладнання та програмного забезпечення, які визначають його поведінку та функціональні можливості. Існує багато інструментів для перевірки конфігурації сервера. Деякі з них перераховані нижче:

1. Ping - простий інструмент, що дозволяє перевірити з'єднання з сервером, шляхом надсилання пакетів даних і очікування відповіді.
2. Traceroute - інструмент, який дозволяє відстежувати шлях маршрутизації даних від вашого комп'ютера до сервера.
3. Nmap - потужний сканер мережі, який дозволяє перевірити відкриті порти на сервері та знайти потенційні уразливості.
4. Wireshark - інструмент, який дозволяє перехоплювати і аналізувати мережевий трафік, що проходить через сервер.
5. Netstat - інструмент, який дозволяє перевірити відкриті порти та з'єднання на сервері.
6. Top - інструмент, який дозволяє відстежувати найбільш ресурсомісткі процеси на сервері.
7. Htop - альтернативний інструмент до Top з додатковими можливостями.
8. Apache Bench - інструмент для тестування навантаження на веб-сервері.
9. Siege - інструмент для тестування навантаження на веб-сервері, який дозволяє імітувати багато користувачів.

10. Curl - інструмент для тестування веб-серверів, який дозволяє виконувати HTTP запити та перевіряти відповіді на запити.

1.2.3.4 Використання спеціальних інструментів

Хакери не вільний час для пошуку комп’ютерів з відомими лазівками в системі безпеки, оскільки для зламання такої машини необхідні лише терпіння та фрагмент програмного коду. Для пошуку потенційних жертв за IP -адресою або доменним іменем зазвичай використовується Ping або інша утиліта. Тоді потрібно з’ясувати, яка операційна система та програми працюють на комп’ютері, і запустити відповідну програму. Черв'як, може блукати через Інтернет, стукати всі двері і напасти на всі машини, навіть не намагаючись дізнатися, чи є на них відповідні програми. Судячи з пошкодженням, що "черв'як" SQL Slammer (він же Sapphire) завдав цій стратегії дуже ефективна.

Інструменти оцінки вразливості автоматизують процедуру пошуку та дозволяють адміністраторам мережі визначати рівень безпеки їхніх систем. Політика безпеки, списки управління доступом (ACL), не допоможуть, якщо в мережі є багато прогалин. Але якщо адміністратор знайде прогалини перед сухарі та усунути їх, мережа стане набагато надійнішою.

Більшість інструментів належать до однієї з наступних категорій: продукти серверів, прикладні рівні (база даних або веб -сайти) та контроль пароля та облікові записи.

1. Серверні інструменти оцінки вразливості

Коли говорять про оцінку вразливості, зазвичай означають інструменти, розміщені на комп’ютерах постачальника. Програма на сервері виявляє та ідентифікує операційну систему на певній машині, а потім перевіряє відомі недоліки. Такий інструмент відрізняє систему Windows від машини UNIX та застосовує відповідну процедуру тестування. Більшість продуктів шукають та перевіряють широкі програми та послуги на кожній платформі. Наприклад,

комп'ютерні тестування комп'ютерів UNIX, демони, Sendmail та розділені ресурси SAMBA. Microsoft IIS перевіряється на машинах Windows, відкриваються загальні ресурси NetBIOS та виявляються слабкі паролі.

2. Інструменти прикладного рівня

Більшість прикладних рівнів зосереджені на веб -серверах та базах даних. Зрозуміло, що захистити публічний веб -сервер дуже важко.Засоби оцінки вразливості веб -серверів зазвичай перевіряються IIS, Apache або Iplanet. Інструменти, орієнтовані на IIS, виявляють погано налаштовані анонімні облікові записи користувачів, неправильні дозволи на доступ до каталогів, тестових програм та привілейованих послуг, таких як API Інтернет-сервера (ISAPI). Інструменти Apache та Iplanet шукають фрагменти коду, які можуть потрапити на файли, модельні атаки на каталог CGI-BIN та атакувати з переходом через каталог /etc /passwd. Інструменти для будь-якого веб-сервера обов'язково перевіряють конфіденційну інформацію в прихованих полях, збережених паролях, сценарії поперечних сайтів, неконтрольованому введенні даних та переповненні буферів.

Після того, як сухарі почали використовувати метод операторів SQL і з'явився "черв'як", кілька постачальників випустили інструменти прикладного рівня, спеціально для тестування широких баз даних: SQL Server, Microsoft Exchange Server, Oracle, IBM Lotus Domino, Oracle PL/SQL, Sybase , IBM DB2 та MySQL. Відсутні та стандартні паролі, перевіряється можливість вбудовування та налаштування параметрів безпеки.

3. Програми перевірки пароля та облікові записи

Невелика кількість продуктів атакує систему, вгадуючи паролі. Такий підхід може здатися занадто спрощеним, але часто паролі є найслабшим посиланням у системі мережевої безпеки. Навіть найпотужніший алгоритм шифрування є марним, якщо приватний ключ використовується зі слабким паролем, оскільки обліковий запис адміністратора не може бути заблокований після певної кількості невдалих спроб ввести пароль, і зломщик може провести

цілий день, тихо вибираючи Пароль для доступу до розділеного каталогу. Деякі інструменти сервера складають список неактивних облікових записів, які не видаляються з комп'ютера своєчасно. Поєднуючи програми перевірки паролів та стан облікових записів, ви можете швидко перевірити та зміцнити будь -яку мережу з мінімальним часом та грошима.

Звичайно, багато інструментів для оцінки вразливості вирішують ряд проблем. Рідкісний інструмент сервера, розпізнавання операційної системи, не вивчає додатків, які часто стають мішенню хат. Багато інструментів хостингу Windows перевіряють пароль та стан облікового запису. Але іноді універсальні інструменти не впораються з кожним конкретним завданням. Як правило, спеціалізований аналізатор веб -серверів або сервер баз даних більш ретельно досліджує системні системи, ніж універсальний сканер, хоча є винятки. Незалежно від категорії, до якої належить інструмент, він повинен виконувати три функції: складати мережеву карту та ідентифікувати програми, перевірити вразливі місця та генерувати звіти.

1.3 Аналіз систем захисту веб-сайту

1.3.1 Складові систем захисту веб-сайту

Аналіз систем захисту веб-сайту - це процес визначення потенційних слабких місць і вразливостей веб-сайту, а також встановлення заходів безпеки, які допоможуть уникнути атак та зберегти конфіденційну інформацію.

Основні складові систем захисту веб-сайту:

1) **Фаєрвол** (Firewall) - це програмний або апаратний засіб захисту від зовнішніх атак. Фаєрвол відповідно до Рисунку 1.4 може блокувати підозрілі мережеві з'єднання та трафік.

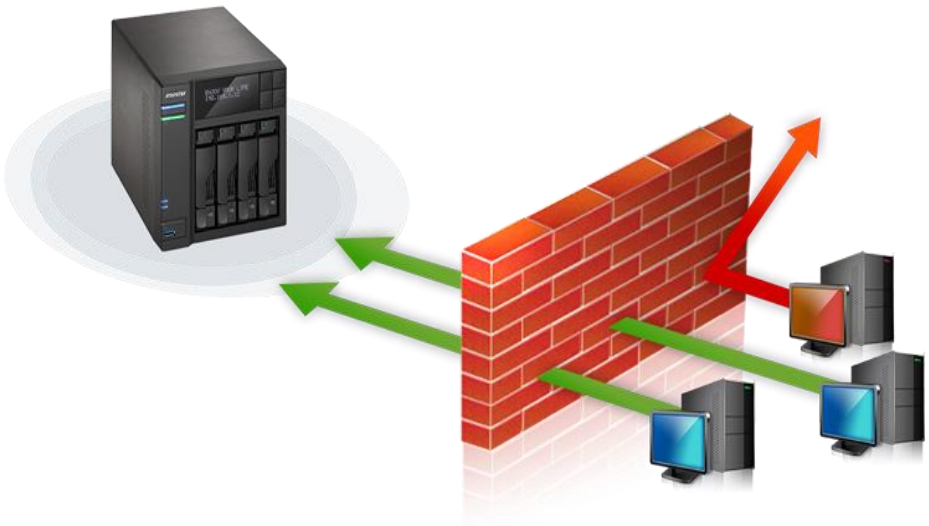


Рисунок 1.4 Фаєрвол (Firewall)

Фаєрвол — це програма, назва якої з англійської трактується, як «протипожежнастіна», вона встановлює перешкоду між комп'ютером і інформацією, що надходить до нього. Існує еквівалент цієї програми – брандмауер. І ця назва вкрай вдало, оскільки вона відображає суть і призначення даного пристрою, тому що завдяки функціональним здібностям ця програма підвищує ступінь захисту комп'ютера.

Це своєрідна стіна з вогню, яка пропускає через себе потік інформації з інтернету, очищаючи його від непотрібного та шкідливого сміття. Отже, комп'ютер, на якому працює фаєрвол, завжди знаходиться під захистом.

Поряд із захистом від шкідливих файлів брандмауер також запобігає надсиланню шкідливих програм на інші комп'ютери або в інтернет. Firewall - це вбудована в операційну систему Windows програма, мета якої перешкоджати проникненню шкідливих файлів, вірусів, троянів, черв'яків, які надходять до неї через інтернет. Фаєрвол був розроблений і адаптований для інших операційних систем, наприклад, для ОС Linux.При інсталяції Windows фаєрвол буде за замовчуванням увімкнено. Однак його також можна вимкнути, якщо він перешкоджає коректній роботі програми або завантажувати файли з інтернету. Firewall може блокувати підключення користувача до програм, яких немає в списку дозволених. Таким чином, кожна невідома програма буде

заблокована фаєрволом автоматично. Є можливість налаштувати роботу брандмауера відповідно до особистих уподобань користувача, наприклад, щоб при блокуванні фаєрволом програми спливало відповідне повідомлення.

Безумовно, фаєрвол – це необхідна та корисна програма для будь-якого комп'ютера. Вона допомагає запобігти незаконному вторгненню в систему і тримати її в безпеці, запобігаючи відправленню шкідливих файлів на інші пристрої. Також, крім вбудованого в систему брандмауера, фахівці рекомендують встановлювати інші антивірусні програми, оскільки фаєрвол не завжди справляється з натиском вірусів.

2) **Антивірус** - програмне забезпечення, яке допомагає виявляти та блокувати шкідливі програми, які можуть пошкодити веб-сайт, Рисунок 1.5.

Рисунок 1.5 Найкращі антивіруси для Windows

Незалежна лабораторія AV-TEST оприлюднила результати чергового етапу тестування антивірусів для домашнього використання на Windows (Рис. 1.6) Найкращим антивірусом визнали вбудований у Windows продукт — Microsoft Defender 4.18.

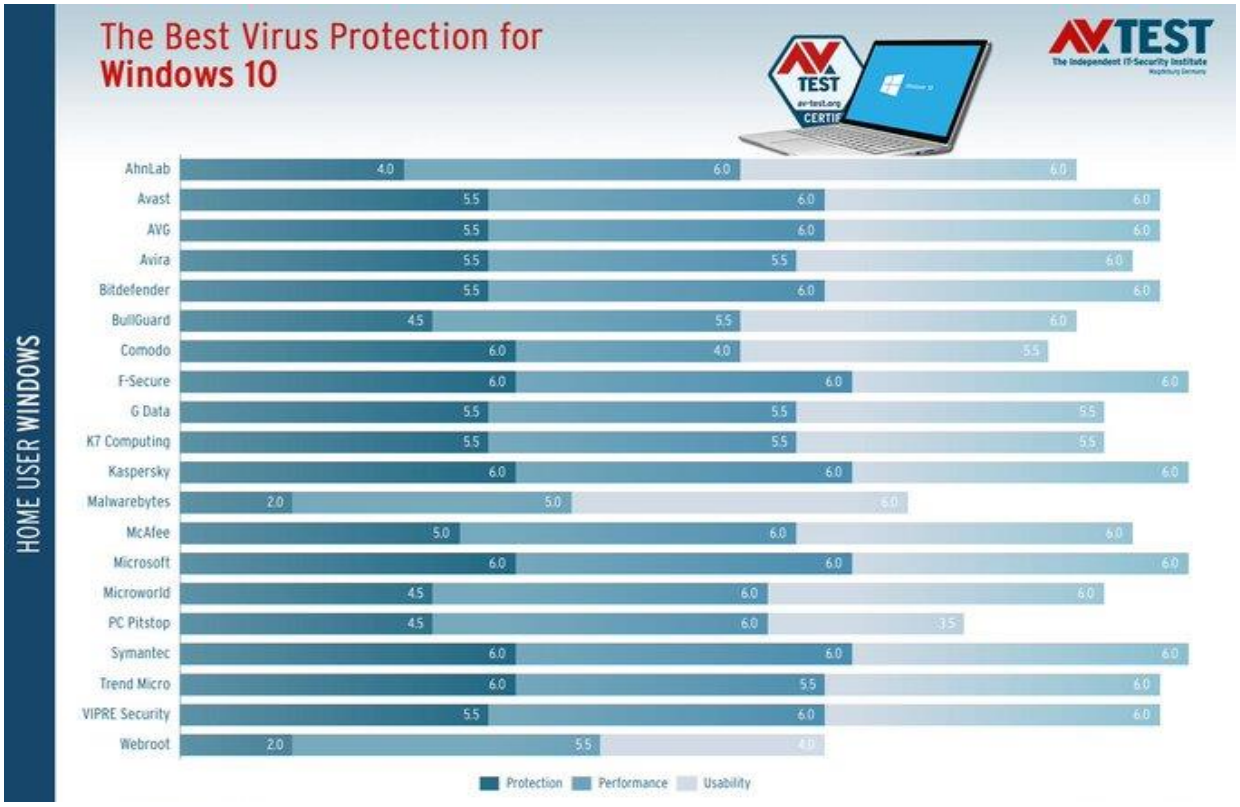


Рисунок 1.6 Результати тестування антивірусів

Microsoft Defender 4.18. набрав максимальні 18 балів за рівень захисту, продуктивність та інтерфейс. Такі ж оцінки отримали F-Secure SAFE, Kaspersky Internet Security та SymantecNorton Security, але ці антивіруси працюють на основі передплати.

Інші популярні продукти, такі як AvastFreeAntivirus, AVG Internet Security, Bitdefender Internet Security, TrendMicro Internet Security, VIPRE Security AdvancedSecurity, набрали 17,5 балів.Найгіршим антивірусом виявився Webroot SecureAnywhere з результатом 11,5 балів. Він отримав 2 бали за захист, 5,5 балів за продуктивність та 4 бали за інтерфейс.

3) **Шифрування** - це процес перетворення конфіденційної інформації в незрозумілий для посторонніх шифрований текст, що знижує ризик її витоку.Протокол HTTPS дозволяє зробити безпечним обмін даними між веб-сайтом та браузером або програмою. Для захисту з'єднання використовується шифрування SSL або TLS.

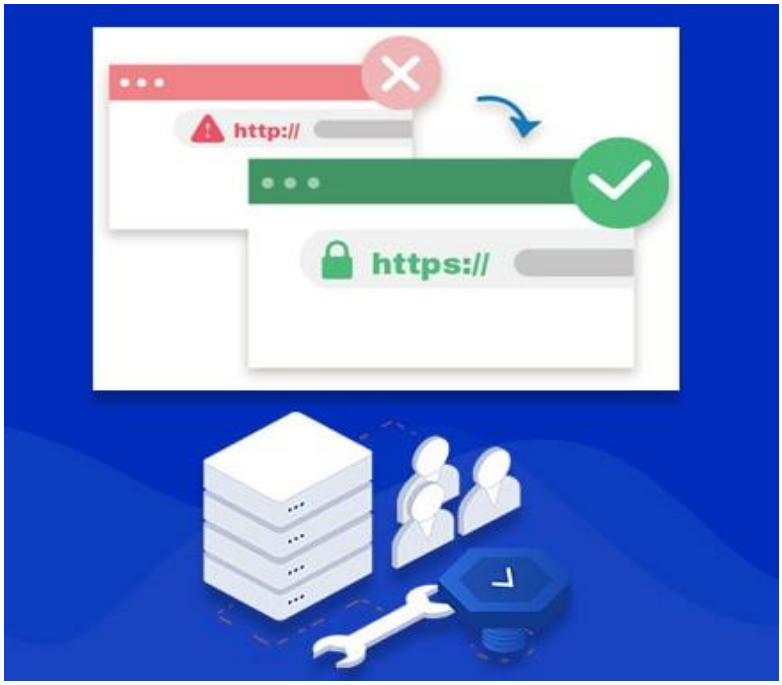


Рисунок 1.7 Перехід від HTTP до HTTPS

HTTP — це протокол, який веб-браузери використовують для передачі файлів із веб-сервера. HTTPS – це захищена версія HTTP (Рис.1.7). HTTPS використовує шифрування SSL, щоб гарантувати, що всі дані, що надсилаються в Інтернеті, зашифровані. HTTP працює без шифрування, що означає, що всі дані через мережу не зашифровані.

Зашифровані веб-сторінки приховують дані, якими ми обмінюємося з ними, щоб ніхто, крім нас, їх не бачив. Важливо використовувати зашифровані сайти, щоб ніхто не міг перехопити наші дані.

4) **Аутентифікація та авторизація** - процеси, які дозволяють перевірити, що користувачі, які звертаються до веб-сайту, є справжніми та мають відповідні права доступу.

Досить важливим завданням при розробці веб-сайтів та додатків є обмеження доступу до деяких розділів сайту, наприклад до панелі адміністратора. Теоретично це досить складний процес, з двома складовими – аутентифікація та авторизація (англ. authentication, authorization) (Рис. 1.8).

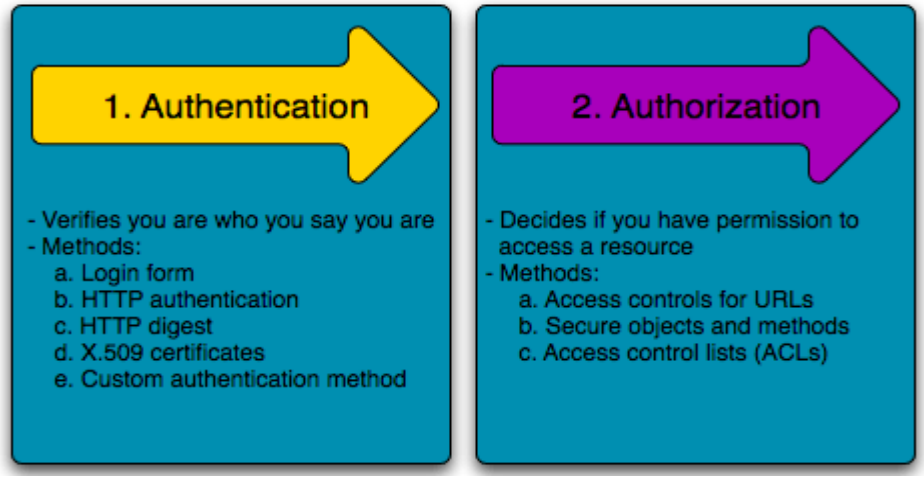


Рисунок 1.8 Система аутентифікації/авторизації

Відразу після введення облікових даних (це може бути пара логін/пароль, одноразовий пароль, ассе, md5-шифр, сертифікат та багато іншого) починається процедура **аутентифікації** (authentication). Вона полягає у перевірці справжності. Наприклад, зіставити ім'я/пароль користувача з обліковим записом базі даних, перевірка контрольної суми файлу тощо.У загальному випадку, для процедури аутентифікації потрібно або щось знати (наприклад, пароль), або мати пристрій аутентифікації (наприклад, ваш смартфон у багатьох сучасних електронних банківських системах), або якісь унікальні біометричні дані - відбитки пальців, рельєф обличчя, голос, райдужна оболонка ока і тощо.

Після цього відбувається **авторизація**. Суть авторизації у наділенні користувача деякими правами. Наприклад, права адміністратора, користувача, анонімa (неавторизованого користувача).

Найчастіше, у php скриптах немає чіткого поділу між першим та другим етапом. У найпростішому випадку це можна зробити однією вибіркою з БД. Але написане тут важливо для розуміння системи захисту у складніших продуктах та фреймворках зокрема.

5) **Резервне копіювання** - це процес створення копій важливої інформації в разі її втрати або пошкодження.

Робота кожного веб-ресурсу, незалежно від його формату (корпоративний сайт, інтернет-магазин, медіа-портал чи інші), базується на складній системі зберігання та обробки. Часто дані є реальною цінністю, на якій будуються мільйони бізнес-проектів. Незважаючи на сучасні технології захисту, навіть найсучасніший веб-ресурс з точки зору безпеки може провалюватися з багатьох причин. Іноді для усунення помилок та пошкоджень потрібні дні або тижні активної роботи програмістів. Поки сайт не працює, бізнес втрачає значну частину прибутку та лояльності клієнтів. Цього можна уникнути за допомогою резервного копіювання.

Backap - це резервна копія всіх даних інтернет -ресурсу, які ви можете використовувати для відновлення сайту до попереднього стану, якщо він пошкоджений або видалений. Backap можна зберігати на комп'ютері, зовнішніх носіях інформації (наприклад, жорсткий диск), сховища сервера або хмар. Резервна копія важлива для будь -якої цінної інформації для вас - від робочих договорів до сімейних фотографій, але сайти особливо це потребують. Збережена копія може знадобитися в таких випадках:

- Проблеми з сервером. Сайт складається з великої кількості файлів, що зберігаються на сервері. Сервери, як і будь-яке обладнання, можуть зазнати невдачі, і працівники, які слідують за своєю роботою, можуть помилитися. Копіювання резерву - це те, що захистить від втрати даних веб-ресурсів.
- Будь-які оновлення сайту. Новий дизайн, функціональність, плагіни можуть призвести до проблем у роботі ресурсу або просто бути невдалим оновленням. "відкат" до попередньої версії за допомогою резервної копії, щоб зробити набагато швидшим і простішим, ніж виправлення помилок.
- Зміна хостингового постачальника. Хостингові постачальники надають послуги для розміщення сайту в мережі. Грубо кажучи, вони продають місце на сервері, де буде зберігатися вся інформація. Копія даних важлива у випадку їх неправильної передачі або, наприклад, для перевірки роботи сайту на новому хостингу.

- Людський фактор. Навіть досвідчені технічні фахівці можуть помилитися. Ви можете випадково плутати кнопки, видалити щось важливе, порушене функціональність за допомогою невдалих оновлення. І сайт без резервної копії не прощає помилок.

- Атаки DOS та DDOS, зараження вірусами. З різних причин зловмисники можуть викреслити частину інформації з бази даних, спровокувати несправність системи за допомогою різних програм (наприклад, методом розбору), впровадити шкідливий код і тим самим порушувати роботу ресурсу. Найшвидший і найефективніший спосіб повернути "викрадену" інформацію або позбутися від вірусів - це "відкати" до "чистого" резервного копіювання.

На основі FTP є найбільш часто використовуваним методом хостинг-провайдерів завдяки можливості автоматизації процесів. Для цього типу резервного копіювання обліковий запис створюється на окремому сервері FTP.

Рисунок 1.9 Хмарне резервне копіювання

Також використовується - хмарне резервне копіювання, коли інформація розміщується на хмарних службах, об'єднана в одну мережу (Рис.1.9), та інші види резервного копіювання, такі якHDD-Backap і CDP-Backap.

6) **Моніторинг** - це процес постійного контролювання веб-сайту для виявлення підозрілого трафіку та активності.

Моніторинг веб-служб – це моніторинг веб-сервісів, таких як протоколи SOAP, GET/POST, TCP та ICMP. (Рис.) 1.10.

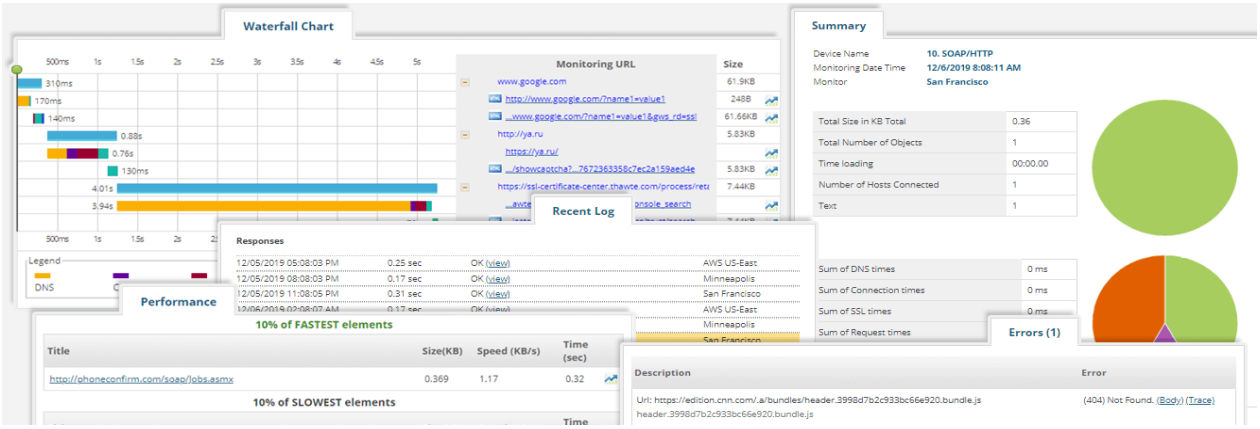


Рисунок 1.10 Приклад моніторингу веб-сервісів, на базі Dotcom-Monitor.com

- Підтримує параметри GET/POST, перевірку вмісту та перевірку сертифікатів SSL;
- Перевірка вмісту відповідей, продуктивності та часу роботи служб SOAP;
- Пінг та перевірка підключення серверів та мережевих пристроїв.

Моніторинг веб-сторінок – це моніторинг швидкості завантаження сторінки на рівні елемента за допомогою кількох браузерів. Відповідно до рисунку 1.11.

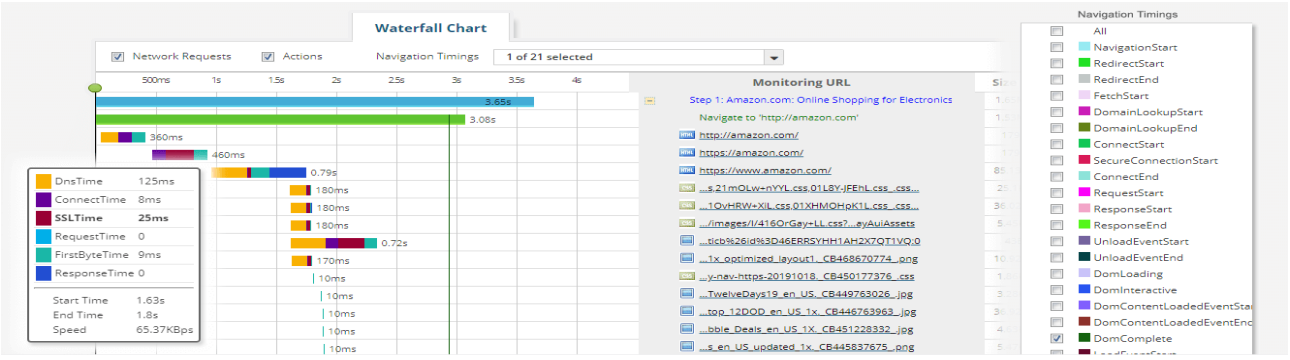


Рисунок 1.11 Приклад моніторингу веб-сторінокна базі Dotcom-Monitor.com

- Визначення найшвидших і найповільніших елементів з часом;
- Перегляд часу завантаження сторінок з усього світу;
- Миттєві оповіщення про проблеми продуктивності.

Моніторинг веб-додатків – це моніторинг багатоступінчастих веб-транзакцій для підвищення продуктивності, функціональності та доступності по всьому світу, відповідно до рисунку1.12.

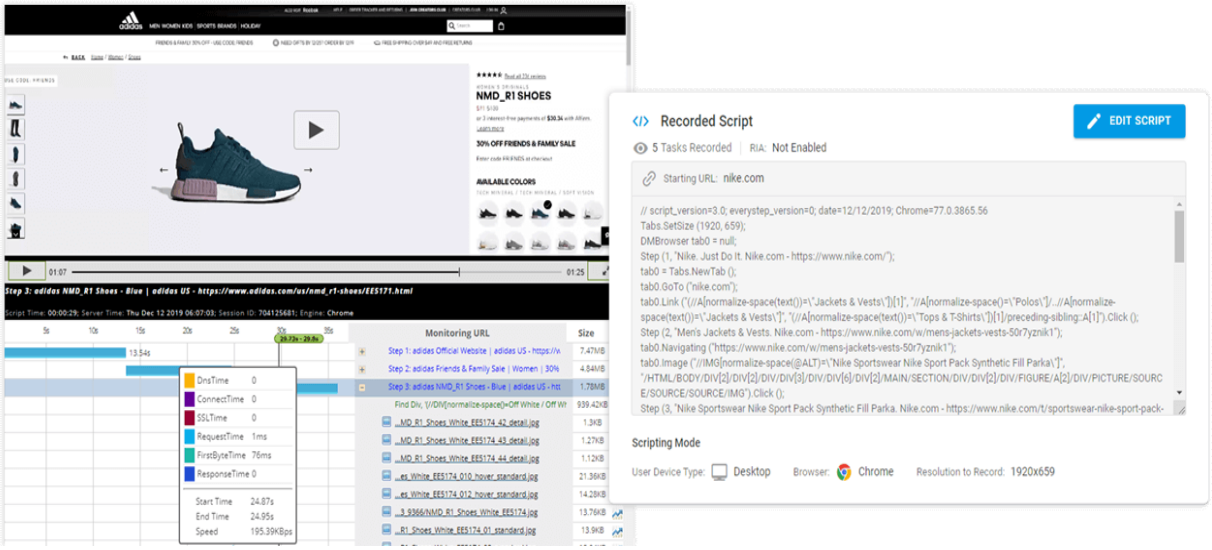


Рисунок 1.12 Приклад моніторингу веб-додатків на базі Dotcom-Monitor.com

- Легко записувати та відтворювати складні веб-переходи;
- Виконує в реальних мобільних/настільних браузерах;
- Відтворення відео помилок з детальною діагностикою.

7) Патчі - це оновлення програмного забезпечення, які містять виправлення виявлених вразливостей.Вони призначені для виправлення помилок, проблем та безпекових уразливостей, які можуть бути виявлені в програмах після їх випуску.Патчі можуть містити не лише виправлення безпекових проблем, але і інші важливі оновлення, такі як нові функції, покращення продуктивності та виправлення помилок, які не впливають на безпеку програмного забезпечення.Оновлення програмного забезпечення за

допомогою патчів є важливим елементом підтримки безпеки та стабільності програмного забезпечення на різних пристроях.

1.3.2 Аналіз систем захисту веб-сайту

Під час аналізу систем захисту веб-сайту рекомендується використовувати комплексний підхід, який включає в себе наступні етапи:

- Аналіз загальної архітектури сайту. Слід оцінити використання протоколів зв'язку, наявність веб-сервера та його налаштувань, наявність систем кешування, реплікації та балансування навантаження.
- Аналіз захисту від атак на рівні додатків. Слід оцінити наявність захисту від SQL-ін'єкцій, XSS-атак, CSRF-атак, використання надійних методів автентифікації та авторизації користувачів, контроль введення даних користувачами.
- Аналіз захисту від атак на рівні мережі. Слід оцінити наявність систем захисту від DDoS-атак, брандмауерів, IPS та IDS.
- Аналіз системи логування та моніторингу. Слід оцінити наявність систем логування, їх налаштування, наявність систем моніторингу захисту та їх ефективність.
- Аналіз процедур реагування на інциденти. Слід оцінити наявність планів реагування на інциденти, процедур повідомлення про інциденти та їх ефективність.

1.3.2.1 Аналіз загальної архітектури сайту

Два вагомих критерії – юзабіліті (зручність користувачів) та ефективне пошукове просування сайту – головні аргументи для розробки та реалізації ефективної структури сайту.

Типи структур сайту

Процес створення будь-якого сайту чи його реконструкції починається із розробки структури. Необхідно сформулювати скільки та яких розділів і підрозділів доцільно зробити, скільки сторінок має бути у кожному з розділів (підрозділів). Особливу увагу доцільно надати повноті охоплення, логіці подачі матеріалу.

Лінійна структура сайту

Це найпростіша структура сайту. Web-сторінки йдуть одна за одною, користувач повинен переглядати їх як презентацію чи слайд-шоу.

Рисунок 1.13 Лінійна структура сайту

У лінійній структурі Рис. 1.13немає поділу контенту (сторінок) на рівні. Всі сторінки на таких сайтах рівноправні, і їх слід побачити кожен відвідувач.Реалізувати такий вид структури дуже легко, так як у більшості випадків вона є набором html-сторінок, з кожної з яких є посилання на наступну-попередню.Дуже важливо, щоб на кожній сторінці сайту були назва та посилання на першу сторінку, бажано також вказувати загальну кількість сторінок та позначати ту, на якій користувач зараз знаходиться. Але навіть при створенні сайту з такою простою структурою веб-майстра припускаються помилок.

Лінійна структура з альтернативними варіантами

Цей вид структури дуже схожий на лінійну, з тією лише відмінністю, що користувачі мають більше варіантів для пошуку інформації, а точніше – вибір між двома гілками. Наприклад, коли на сайті поділяються корпоративні та приватні клієнти. Відповідно до рисунку 1.14.

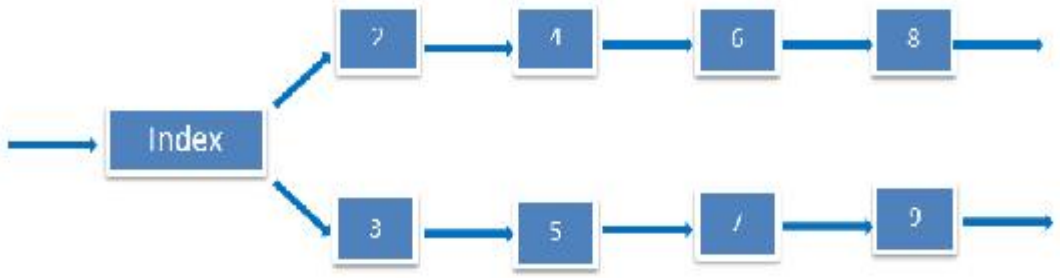


Рисунок 1.14 Лінійна структура сайту з альтернативним варіантом А

Досить часто зустрічається ситуація, коли вже "розділені по гілках" відвідувачі проте зустрічаються на будь-якій сторінці - наприклад, оплата або відгук про роботу. Відповідно до рисунку 1.15

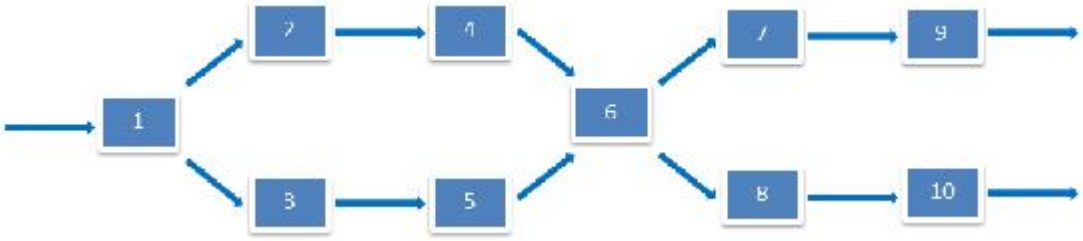


Рисунок 1.15 Лінійна структура сайту з альтернативним варіантом Б

Лінійна структура сайту з відгалуженнями

Ця структура аналогічна дорозі з множинними відгалуженнями від неї. Людина переходить з однієї сторінки на іншу у строгій послідовності як при лінійній структурі Рис. 1.16. Однак відвідувач у разі потреби може завжди перейти на інше відгалуження, а потім повернутися назад.

Основною перевагою лінійної структури з відгалуженнями – це відносно нескладна можливість web-майстрам перейти на неї зі звичайної лінійної структури. При розвитку сайту часто виникає необхідність. Контент сильно розростається і необхідно покращити навігацію.

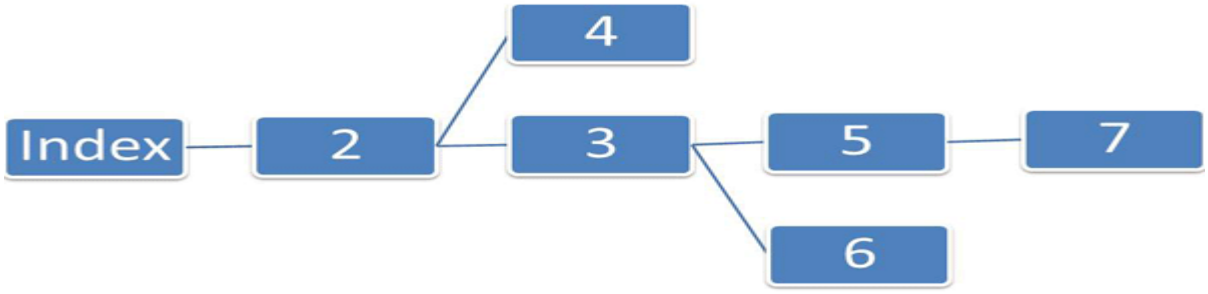


Рисунок 1.16 Лінійна структура сайту з відгалуженнями

Це трохи складніша структура, властива невеликим корпоративним ресурсам, сайтам-візиткам, деяким авторським блогам. Як правило, тут також немає розділів, а є лише окремі статичні сторінки. Але посилання на всі ці сторінки (або більшість з них) розміщені на головній. Завдяки цьому система навігації тут дуже проста та інтуїтивно-зрозуміла, а доступ до всіх сторінок здійснюється лише за 1 або 2 кліки. Характерний приклад сайту з подібною структурою - візитівка якоїсь фірми (з головної проставлені посилання на сторінку з каталогом товарів, прайс-листом, контактними даними, вакансіями тощо).

Гратчаста структура сайту

Одна з найскладніших структур сайту, де всі документи розташовуються у різних гілках відповідно до рисунку 1.17. Однак відвідувач може легко переміщатися цими гілками як горизонтально (зліва направо або між гілками на різних рівнях), так і вертикально (зверху вниз).Цей вид структури характерний переважно для каталогів статей чи посилань.

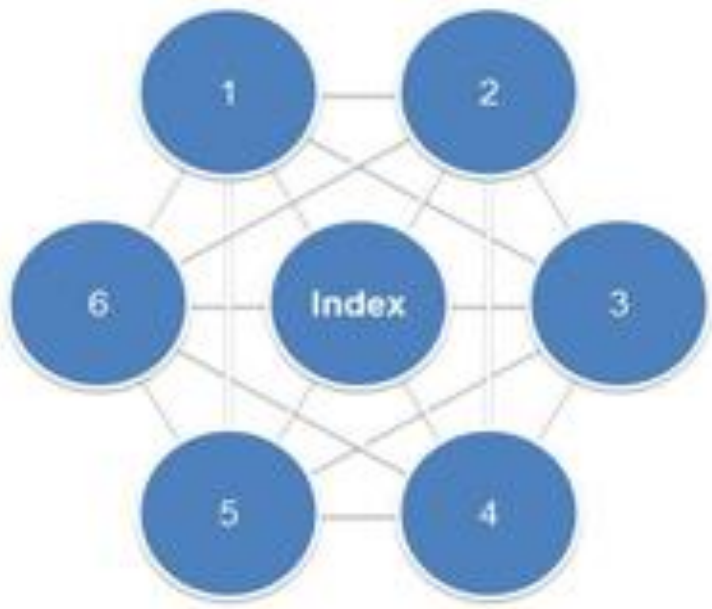


Рисунок 1.17 Гратчаста структура сайту

На перший погляд, вона дуже зручна для користувачів, але для звичайних сайтів її краще не використовувати.

Деревоподібна структура сайту

Деревоподібна структура сайту часто використовується багатьма веб-майстрами як найоптимальніша (Рис.) 1.18.

Ідея застосування такої структури полягає в тому, що людина має вибір і можливість як з головної сторінки сайту, так і будь-якої іншої, перейти в будь-який розділ, підрозділ і на конкретну сторінку (документ).

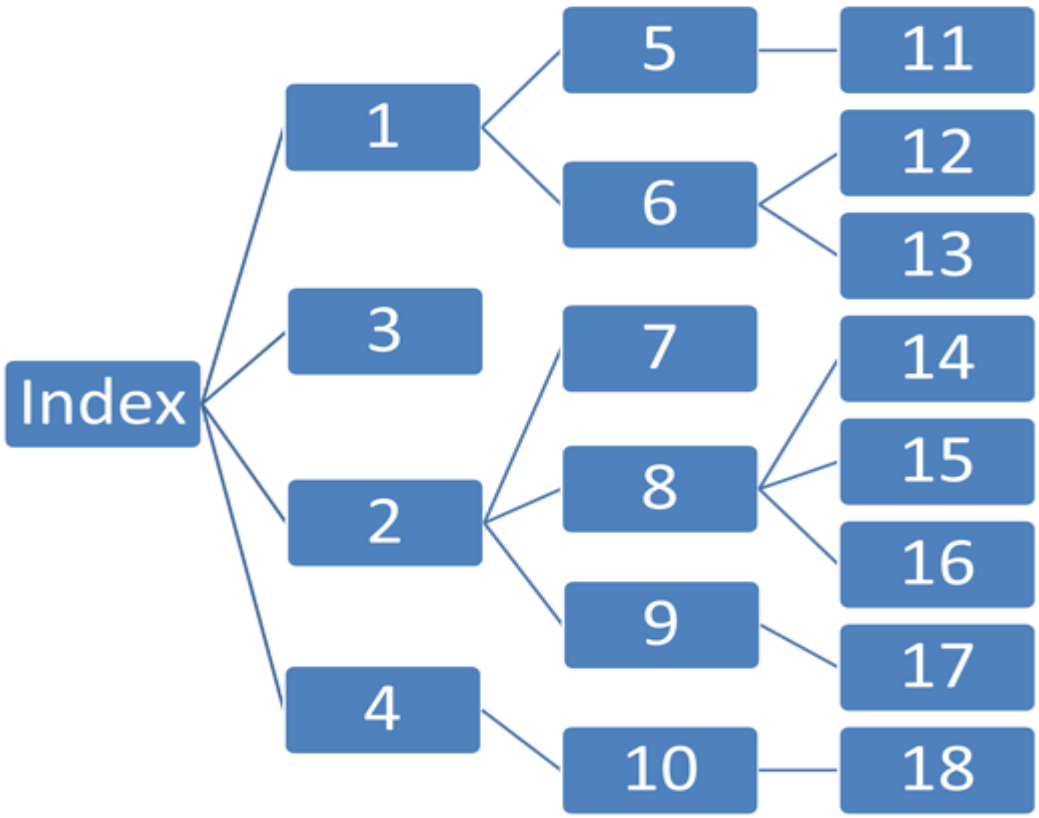


Рисунок 1.18. Деревоподібна структура сайту

Переваги деревоподібної структури сайту

- Головна перевага деревоподібної структури сайту – універсальність. Деревоподібна структура чудово може підійти для будь-якого виду сайту, будь то домашня веб-сторінка, сайт-візитка, корпоративний сайт, портал або каталог.
- Чудова навігація. Ідея застосування такої структури полягає в тому, що людина має вибір і можливість як з головної сторінки сайту, так і будь-якої іншої, перейти в будь-який розділ, підрозділ і на конкретну сторінку (документ).

- Велика гнучкість. Хоча на звичайному HTML таку структуру сайту практично неможливо організувати (та й не потрібно), для її створення пишеться двигун або використовується CMS

Змішана структура сайту

Ця структура характеризується, присутністю двох або більше елементів вище перерахованих структур в одній, проте через складність її реалізації, вона рідко використовується.Рисунок 1.19.

Ця структура вже на порядок складніша за всі розглянуті раніше. У ній всі сторінки також розміщуються у різних гілках. Але користувач має можливість переміщатися по них не тільки вертикально (вгору-вниз), але й горизонтально (тобто між гілками на різних рівнях). Використовується грати в основному тільки в каталогах. При цьому переміщення між гілками на глибинних рівнях здійснюється за допомогою посилань на рубрики в інших розділах.

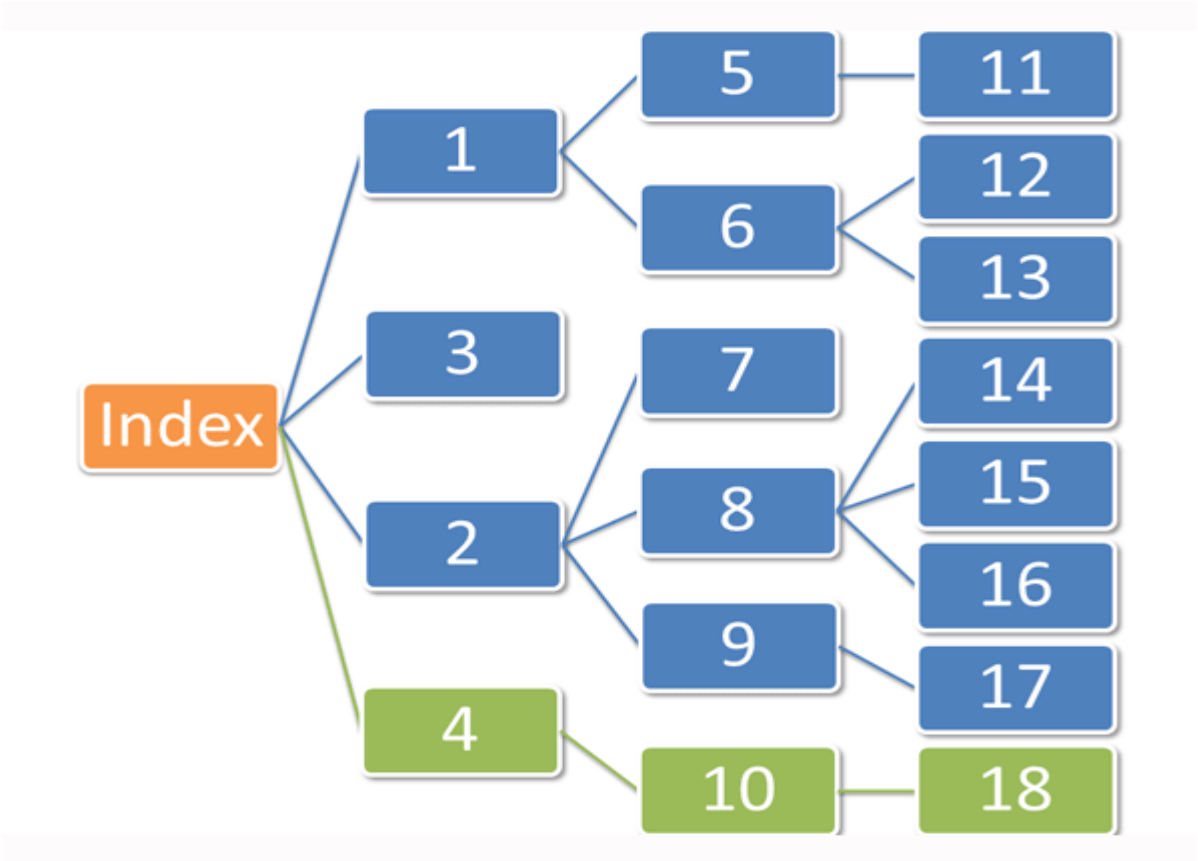


Рисунок 1.19. Змішана структура сайту

Аналіз структури існуючого сайту

Якщо ресурс має великий обсяг, включає складну ієрархію розділів, і грамотна не структурований, то перебування на такому сайті і пошук інформації бувають проблематичними для більшості користувачів, також утрудняється і індексація ресурсу.Для усунення можливих помилок в організації та логіці структури ресурсу, при проведенні внутрішнього та технічного аудитів, виконується також аналіз структури сайту.

Метою проведення аналізу структури сайту є виявлення внутрішніх взаємозв'язків сайту, ефективність їх організації та розробка плану оптимізації структури сайту для подальшої його розкрутки в пошукових системах. Цей аналіз враховує наступні аспекти:

- Логічна структура веб-сайту. Відповідність назви папок та вміст файлів нижчого рівня тематиці папок (розділів) вищого рівня;
- Розміщення однотипних файлів на одній директорії. Наприклад, файли з розширенням .png, .gif, .jpg у папці "img", а файли .pdf у папці "download";
- Відповідність існуючої структури сайту (кластеризованого) семантичного ядру;
- Семантична структура сайту. Мета – використання максимальної кількості ключових слів та словосполучень у тексті сайту за допомогою оптимальної кількості файлів.

Основні етапи проведення аналізу структури сайту

- Аналіз структури сайтів – конкурентів;
- Перевіряє відповідність внутрішніх посилань сайту правильної індексації сайту. Аналіз структури посилання сайту;
- Перевірка наявності непрацюючих посилань;
- Перевірка зручності навігації по сайту як з погляду пошукових систем, так і погляду користувача;
- Перевірка наявності та правильного функціонування картки сайту.

1.3.2.2 Аналіз захисту від атак на рівні додатків

Число компаній, які застосовують веб-технології для підвищення продуктивності роботи і залучення нових клієнтів, зростає з кожним роком. Безсумнівно, інтернет-сервіси несуть з собою безліч переваг, але є й зворотна сторона медалі – з ростом числа додатків збільшується і кількість кіберзагроз. Так, компанія Symantec в своєму звіті Global Internet Security Threat Report (ISTR) вказує, що кіберзлочинці при зломі веб-сайтів зазвичай використовують вразливості веб-додатків, що працюють на сервері, або експлуатують деякі вразливості операційної системи, на якій працюють ці додатки. Наприклад, за допомогою атак типу XSS хакер може перенаправити запити користувачів на шкідливі веб-сторінки, а за допомогою SQL-ін'єкцій – витягувати з баз даних сайту різну конфіденційну інформацію.

ImpervaSecureSphereWebFirewallApplication – один з лідерів в області відображення атак на веб-додатки. Рішення від Imperva забезпечують надійний захист за рахунок одночасного застосування декількох технологій в сфері ІБ: сигнатурний аналіз, перевірка протоколів на аномалії, відстеження сесій, динамічне профілювання.Сімейство Secure-Продуктів Sphere WAF протидіють як Успішно всім з OWASP атакам-TOP10, так і іншим менш відомим, але більш витонченим атакам. Пристрої мають можливості по інспектування зашифрованих даних, що пересилаються по протоколу SSL (HTTPS).

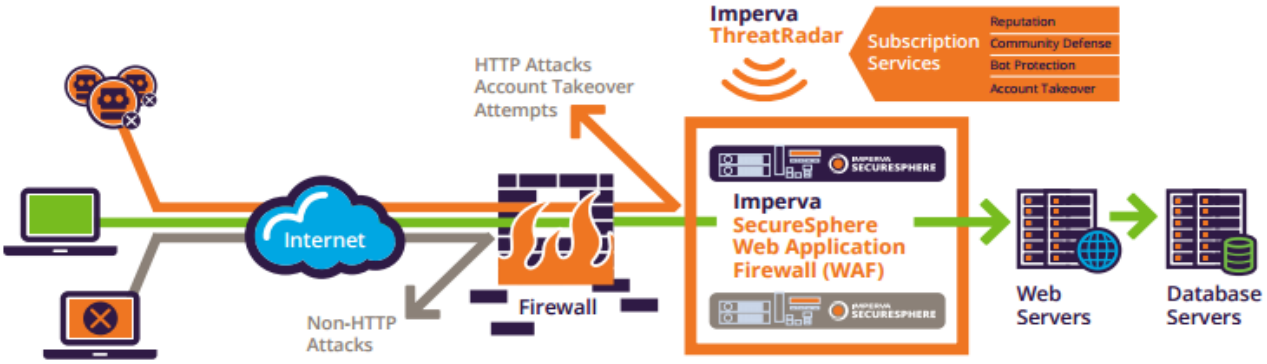


Рисунок 1.20. Захист веб-додатків від Imperva SecureSphere Web Firewall Application

Рішення складається з наступних модулів, (рис.) 1.20:

• SecureSphere Web Firewall Application – захист веб-додатків від кібератак;

• ThreatRadar – репутаційна база даних.

Secure-Sphere WAF здатний глибоко аналізувати логіку роботи легального веб-додатки, виконувати інтелектуальне дослідження спроб проникнення і атак; HTTP-протидіяти атакам, включаючи атаки на переповнення буфера, дії шкідливих програм і зловмисників. Рішення оснащено механізмом захисту від черв'яків і інших шкідливих атак на веб-сервери і додатки, основу якого складають механізми на основі сигнатур популярної системи Snort і власних SQL-сигнатур, що розробляються дослідним центром ADC (Application Defense Center) компанії Imperva. Вбудований міжмережевий екран здійснює надійний захист від неавторизованих призначених для користувача запитів і атак на мережевому рівні.

Попередньо в системі звіти повністю задовольняють вимогам стандартів інформаційної безпеки. Можливе створення призначених для користувача звітів (в тому числі за розкладом) та експорт в різні формати. Додаткові хмарні сервіси дозволяють спростити безпеку і впорається з DDoS-атаками.

Важлива перевага пристроїв SecureSphere WAF: наявність унікального сервісу ThreatRadar, що забезпечує захист від автоматизованих атак. Завдяки швидкому отриманню достовірної інформації про джерела атак, ThreatRadar дозволяє негайно блокувати трафік, що йде від підозрілих джерел, ще до моменту здійснення будь-якого руйнівної дії. Рішення Imperva відрізняються прозорою підтримкою і простим розгортанням.

Важливий організаційний момент при побудові системи захисту веб-додатків – тест на проникнення. Саме він стане оптимальним способом перевірки захищеності інформаційної системи за допомогою імітації

спрямованих атак. Тест на проникнення дає можливість оцінити захищеність інформаційної системи від несанкціонованого впливу, використовуючи різні моделі вторгнень.

1.3.2.3 Аналіз захисту від атак на рівні мережі

Системи виявлення мережевих вторгнень і виявлення ознак кібератак на інформаційні системивже давно застосовують як один із необхідних рубежів оборони інформаційних систем.Сьогодні системи виявлення вторгнень і атак – це зазвичай програмні або апаратно-програмнірішення, (Рис.1.21), які автоматизують процес контролю подій, що відбуваються в інформаційній системіабо мережі, а також самостійно аналізують ці події в пошуках ознак проблем безпеки. Оскількикількість різних типів і способів організації несанкціонованих проникнень у чужі мережі заостанні роки значно збільшилася, системи виявлення атак (СВА) стали необхідним компонентом інфраструктури безпеки більшості організацій.

Незважаючи на існування численнихметодів виявлення аномалій, їхня слабка стійкість, відсутність верифікації, велика кількістьхибних спрацьовувань, вузька спеціалізація та дослідницький характер не дають змоги широкоїх використовувати.

Риунок. 1.21. Програмно-апаратні методи захисту локальних мереж

Міжмережевий екран може працювати на різних рівнях протоколів моделі OSI. На мережевому рівні виконується фільтрація вхідних і вихідних пакетів по IP—адресам (наприклад, не пропускаються пакети з мережі Internet, які направлені на ті сервери, доступ до яких зовні заборонено). На транспортному рівні фільтрація відбувається ще й за номерами портів TCP і прапорців, що містяться в пакетах (наприклад, запити на встановлення з'єднання). На прикладному рівні виконується аналіз прикладних протоколів (FTP, HTTP, SMTP) і контроль за змістом потоків даних (заборона внутрішнім абонентам на отримання будь—яких типів файлів: рекламної інформації або виконуваних програмних модулів).

Віртуальна приватна мережа створюється на базі загальнодоступної мережі Інтернет. І якщо зв'язок через Інтернет має свої недоліки, головним з яких є те, що вона схильна потенційним порушень захисту та конфіденційності, то VPN можуть гарантувати, що направляється через Інтернет трафік так само захищений, як і передача всередині локальної мережі. У теж час віртуальні мережі забезпечують істотну економію витрат у порівнянні з вмістом власної мережі глобального масштабу.

Антивірус – програмний засіб, призначений для боротьби з вірусами. Виходячи з визначення, основними завданнями антивірусу є:

- Перешкоджання проникненню вірусів у комп'ютерну систему
- Виявлення наявності вірусів у комп'ютерній системі
- Усунення вірусів з комп'ютерної системи без нанесення ушкоджень іншим об'єктам системи
- Мінімізація збитку від дій вірусів
- Технології виявлення вірусів

Криптографічний захист (шифрування) інформації – це вид захисту, який реалізується за допомогою перетворень інформації з використанням спеціальних (ключових) даних з метою приховування змісту інформації, підтвердження її справжності, цілісності, авторства тощо. На відміну від

тайнопису, яке приховує сам факт передавання повідомлення, зашифровані повідомлення передаються відкрито, приховується їхній зміст.

Системи **біометричного захисту** використовують унікальні для кожної людини вимірювані фізіологічні характеристики для перевірки особи індивіда. Цей процес називається електронною аутентифікацією. Його суть – визначити, чи справді індивід є тією особою, якою він або вона себе називає. Це відрізняє аутентифікацію від ідентифікації та авторизації. Мета ідентифікації – перевірити, чи відомий індивід системі, наприклад перевіркою пароля, а авторизація полягає в наданні користувачеві доступу до певних ресурсів залежно від його особи.

1.3.2.4 Аналіз системи логування

Роботу додатків потрібно постійно моніторити, щоб запобігати та реагувати на потенційні НП (надзвичайна подія), відловлювати «вузькі місця».Системи логування є обов'язковим інструментом, без якого не обійтися в цьому процесі. Проводячи докладний аналіз даних, що збираються, можна ідентифікувати «вторгнення» в мережу, виявити неправильно налаштоване обладнання і оперативно вжити заходів.

Система логування - це механізм, який використовується для ідентифікації користувачів та контролю доступу до різних ресурсів системи. Основна мета системи логування - забезпечити безпеку та конфіденційність даних, а також контроль за діяльністю користувачів.Системи логування можуть бути реалізовані за допомогою різних технологій, включаючи локальні бази даних, LDAP, ActiveDirectory, OAuth та інші. У деяких системах може бути налаштований рівень логування, що означає, що детальність записів логування може бути налаштована в залежності від потреб користувача.

Системи логування також можуть включати аудиторські функції, які використовуються для відстеження дій користувачів в системі. Ці функції

можуть включати запис дій користувачів, а також збереження цих записів на довготривалому зберіганні для подальшого аналізу в разі необхідності.У загальному, системи логування є важливим елементом безпеки в будь-якій системі, тому їх розробка та використання має бути обов'язковим етапом при розробці будь-якої інформаційної системи.

1.3.2.5 Аналіз процедур реагування на інциденти

Важливим стандартом для перевірки плану реагування на інциденти є публікація NIST під назвою «Посібник з управління інцидентами комп'ютерної безпеки», який детально описує 4 етапи реагування на надзвичайні події: підготовка, виявлення та аналіз, стримування, ліквідація наслідків і відновлення, а також подальша діяльність після інциденту (Рис. 1.22).

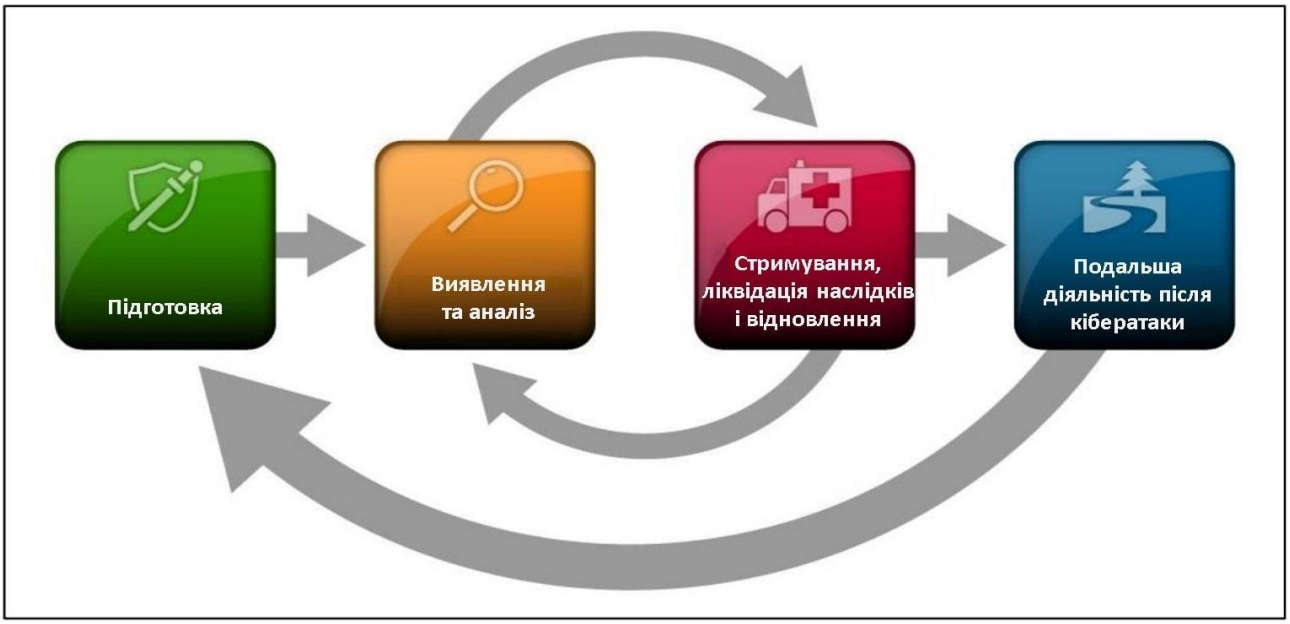


Рисунок 1.22. Етапи реагування на інциденти

Обробка інцидентів безпеки відповідно до цих 4 кроків може допомогти забезпечити успішне повернення до звичайних процесів в роботі веб-ресурсу.

1. Підготовка

Перш ніж станеться будь-який інцидент, важливо встановити належні заходи безпеки для зменшення ризиків інфікування вже відомими загрозами.

Зокрема, це оновлення серверів, операційних систем та додатків до актуальних версій, налаштування посиленого захисту від шкідливих програм. Також корпоративна мережа має бути захищена через брандмауери і VPN. Крім цього, варто не забувати про покращення обізнаності співробітників у галузі інформаційної безпеки для зменшення кількості інцидентів, оскільки саме вони часто піддаються на маніпуляції хакерів.

Важливою частиною налаштування вашої мережі є наявність всіх необхідних інструментів моніторингу та введення журналів для збору та аналізу подій у вашій мережі. Доступні різні варіанти: інструменти віддаленого моніторингу та управління (RMM), інструменти управління інформаційною безпекою та подіями безпеки (SIEM), інструменти організації та автоматизації процесів реагування на інциденти безпеки (SOAR), системи виявлення вторгнень (IDS) і системи запобігання вторгнень (IPS), а також рішення для виявлення та реагування на події безпеки на робочих станціях (EDR).

Все більше організацій, які частіше за всіх зазнають атак (наприклад, банки та урядові установи) використовують інформаційні сервіси, такі як ESET Threat Intelligence. Цей сервіс надає актуальну інформацію про індикатори компрометації, що дозволить швидко реагувати на нові загрози і атаки у разі їх виявлення в реальному середовищі.

Створення команди реагування на інциденти комп'ютерної безпеки

Ще одним важливим кроком є створення та навчання команди реагування на інциденти комп'ютерної безпеки відповідно до вимог вашого підприємства. Компанії малого бізнесу можуть створити тимчасову команду, яка буде складатися з існуючих IT-адміністраторів. Однак організації більших розмірів повинні мати постійну команду, яка буде залучати інших IT-адміністраторів компанії виключно для допомоги в певних атаках, наприклад, адміністратора бази даних, щоб допомогти проаналізувати атаку типу SQL injection.

Альтернативою є залучення команди реагування на інциденти комп’ютерної безпеки на аутсорсингу, хоча це може коштувати дорожче. Якщо ви розглядаєте такий варіант, ви повинні бути готові до більш тривалого часу для реагування. Деяких членів команди реагування на інциденти, можливо, доведеться чекати з інших регіонів, що значно збільшує час для впливу загроз на вашу мережу.

Найголовніше, що у складі будь-якої команди повиннні бути співробітники, які розуміють, як саме будується корпоративна мережа, що є нормальним для неї, а що незвичним.

Керівництво також має відігравати активну роль, зокрема надавати необхідні ресурси та засоби для ефективного виконання роботи команди реагування на інциденти. Це означає забезпечення інструментами та пристроями, які потрібні вашій команді реагування, а також прийняття жорстких управлінських рішень стосовно інциденту.

Уявіть, що команда реагування на інциденти комп’ютерної безпеки виявляє компрометацію сервера електронної комерції, що є важливим елементом введення бізнесу, та потребує його відключення. Керівництво компанії має швидко зрозуміти вплив на бізнес-процеси у разі відключення або ізоляції сервера та повідомити команду реагування на інциденти.

Інші співробітники і відділи компанії також надають важливу підтримку команді реагування. IT-спеціалісти можуть допомогти вимкнути і замінити сервери, відновити дані з резервних копій та очистити систему відповідно до вимог команди. Юристи та відділ зі зв'язків з громадськістю необхідні для управління будь-якими комунікаціями щодо інциденту, наприклад, зі ЗМІ, партнерами, клієнтами та правоохоронними органами.

2. Виявлення та аналіз

На цьому етапі аналітики за допомогою своїх знань та потрібних інструментів мають виявити, що відбувається в мережі та яких заходів потрібно вжити. Завдання аналітика — зіставити події, щоб відтворити їх

послідовність до моменту інфікування, та визначити основну причину, щоб якомога швидше перейти до дій етапу 3.

Однак, як показано на схемі вище, 2 та 3 етапи мають циклічний характер, що означає реагування на інциденти може переключитися назад на другий етап для проведення подальшого аналізу причин. Наприклад, знаходження і аналіз деяких даних на етапі 2 призводить до необхідності вжити конкретних заходів щодо пом'якшення наслідків на етапі 3. Потім на 3 етапі можуть виявитися певні додаткові дані, які потребують аналізу, тобто перехід до етапу 2.

Варто зазначити, що інструмент для виявлення та відслідковування подій на робочих станціях — ESET Enterprise Inspector — дозволяє автоматично визначити підозрілу активність, дослідити та миттєво відреагувати на інцидент безпеки, що допомагає спеціалістам на 2 етапі.

3. Стримування, ліквідація наслідків і відновлення

На 3 етапі команда реагування на інциденти комп’ютерної безпеки повинна прийняти рішення з метою уникнення поширення виявлених загроз, наприклад, відключення сервера, ізоляція робочої станції або припинення використання деяких сервісів. Обрана стратегія стримування має враховувати можливу шкоду у майбутньому, зберігання доказів компрометації та тривалість стримування. Як правило, це означає ізолювати скомпрометовані системи, сегментувати частини мережі або розмістити уражені пристрої в пісочниці.

Перевагою пісочниці є можливість подальшого моніторингу загрози, а також збору додаткових доказів. Однак існує небезпека, що скомпрометований хост може бути додатково пошкоджений, перебуваючи в пісочниці.

Юрист може визначити, що команда реагування має збирати та фіксувати якомога більше доказів. У цьому випадку передача доказів від однієї людини до іншої повинна ретельно реєструватися.

У випадку виявлення шкідливого програмного забезпечення потрібно видалити його зі скомпрометованих систем. Після цього потрібно буде

відключити, закрити чи скинути облікові записи користувачів. Також слід виправити уразливості, відновити системи та файли з чистих резервних копій, змінити паролі, посилити правила брандмауера тощо.

Повне повернення до звичайних бізнес-операцій може зайняти місяці залежно від кібератаки. Для початку слід встановити покращену систему ведення журналів та моніторингу, щоб IT-адміністратори могли запобігти повторенню тієї ж кібератаки. У перспективі потрібно прийняти більш масштабні зміни, які допоможуть зробити корпоративну мережу безпечнішою.

4. Подальша діяльність після кібератаки

Команда реагування на інциденти комп'ютерної безпеки повинна фіксувати та надавати дані щодо зміни подій та їх хронологію. Це допомагає зрозуміти основну причину кібератаки та запобігти повторному чи подібному інциденту безпеки. Крім цього, всі команди мають переглянути ефективність процесів та операцій, які виконуються, виявити недоліки у спілкуванні та співпраці та знайти можливості для покращення поточного плану реагування на подібні інциденти.

Важливим моментом є визначення політики збереження доказів, зібраних під час інциденту безпеки. Тому перед очищенням жорстких дисків зверніться до юридичного відділу. Як правило, більшість організацій зберігають записи про такі випадки протягом двох років відповідно до норм.

2 ОХОРОНА ПРАЦІ

Згідно з ч. 1 ст. 13 Закону України «Про охорону праці» роботодавець зобов'язаний створити на робочому місці в кожному структурному підрозділі умови праці відповідно до нормативно-правових актів, а також забезпечити додержання вимог законодавства щодо прав працівників у галузі охорони праці.

Робота з комп'ютером характеризується значною розумовою напругою і нервово-емоційним навантаженням операторів, високою напруженістю зорової роботи і достатньо великим навантаженням на м'язи рук при роботі з клавіатурою ЕОМ. Велике значення має раціональна конструкція і розташовує елементів робочого місця, що важливе для підтримки оптимальної робочої пози людини-оператора. В процесі роботи з комп'ютером необхідно дотримувати правильний режим праці і відпочинку.

Дотримання норм охорони праці є спільним завданням як роботодавця, так і працівника. У вирішенні питань з охорони праці можна звернутися до законодавства України з охорони праці.

Метою данного розділу дипломного проекту є визначення оптимальних умов праці програміста та обов`язків з охорони праці.

1.Аналіз небезпечних і шкідливих факторів, що впливають на програміста при розробці даного програмного комплексу

На робочому місці розробника програмного забезпечення: підвищений рівень отримуваного електромагнітного випромінювання, статична електрика, високий рівень шуму, несприятливі умови мікроклімату, підвищена напруга на зір та мозок тощо.

Під час робочого процесу програміст піддається впливу великої кількості шкідливих та небезпечних факторів, а саме: шуми, вібрації, інфрачервоне випромінювання, електромагнітне випромінювання, електричний струм, емоційне та нервове навантаження, сидяче положення тіла протягом

дового часу. Тому дуже важливо забезпечити правильний нормований графік та організувати робочий процес так, щоб мінімізувати вплив усіх перелічених раніше небезпечних та шкідливих факторів.

2 Гігієнічні вимоги до виробничого середовища.

Вимоги, що пред'являються до умов праці на виробництві, визначаються необхідністю забезпечення таких умов праці на робочому місці, при яких виключено несприятливий вплив на працездатність і здоров'я працюючих і можуть бути забезпечені оптимальні границі поділу і кооперації праці, а в кінцевому підсумку підвищення ефективності та якості праці.

2.1 Вимоги до приміщення

Обємно-планувальні рішення будівель та приміщень для роботи з ВДТ мають відповідати вимогам ДСанПІН 3.3.2.007-98. Розміщення робочих місць з ВДТ ЕОМ і ПЕОМ у підвальних приміщеннях, на цокольних поверхах заборонено. Площа на одне робоче місце становить не менше 6,0 $м^2$, а об’єм – не менше ніж 20,0 $м^3$. У приміщеннях слід щоденно робити вологе прибирання. Вони повинні бути оснащені аптечками першої медичної допомоги. При приміщеннях мають бути обладнанні побутові приміщення для відпочинку.

Для стін і робочих поверхонь використовують мало насичені (основні) кольори, для невеликих помешкань або ділянок, що рідко потрапляють у поле зору працюючих, а також для створення контрастності – кольори середньої насиченості (допоміжні), для маленьких по площі поверхонь – насичені (акценти) – як функціональне фарбування. Стелі у всіх приміщеннях повинні бути білими. Поверхні устаткування в приміщеннях повинні бути матовими або напівматовими для виключення випадку відблисків світла в очі працюючого, а стіни бути пофарбованими фарбами пастельних тонів.

2.2 Освітлення

Відповідність характеристик систем освітлення нормативним вимогам гарантує не тільки збереження здоров'я, а й високі продуктивність і якість

праці. На підприємствах використовується природне і штучне освітлення. Перше призначено для роботи в денний час, а друге - у вечірній, коли природного освітлення недостатньо. Приміщення для роботи з ВДТ повинні мати природне та штучне освітлення, відповідно до ДБН В.2.5-28:2018 « Природне і штучне освітлення».

Для штучного освітлення у приміщенні використовуються люмінесцентні лампи типу ЛБ, які в порівнянні з лампами розжарювання мають ряд істотних переваг: за спектральним складом світла вони близькі до природного світла, мають підвищену світлову віддачу (у 2-5 разів вищу, ніж у ламп розжарювання); мають триваліший термін служби – до 10 тис годин.. Допускається застосування ламп розжарювання у світильниках місцевого освітлення.

2.3 Шум

Рівні шуму та вібрації на робочих місцях осіб, що працюють з ПК, визначаються відповідно до ДСанПіН 3.3.2.007-98.

Для забезпечення дотримання допустимих рівнів шуму на робочих місцях застосовуються засоби звукопоглинання, вибір яких обґрунтовується спеціальними інженерно-акустичними розрахунками (п. 3.3.3 ДСанПіН 3.3.2.007-98).

2.4 Мікроклімат

У виробничих приміщеннях на робочих місцях мають забезпечуватись оптимальні значення параметрів мікроклімату: температури, відносної вологості й рухливості повітря – ДСН 3.3.6.042-99 «і норми мікроклімату виробничих приміщень».

Параметри мікроклімату	значення параметрі	
	Взимку	влітку
Температура, C^0	22-24	23-25
Відносна вологість, %	40-60	40-60
Швидкість руху повітря, м/с	0,1	0,1-0,2

Нормалізація параметрів мікроклімату у виробничих приміщеннях здійснюється за допомогою систем опалення. Ці системи поділяються на водяні парові та повітряні. Кількість теплоти, що генерується системою опалення, має відповідати втрат теплоти в приміщенні (через будівельні конструкції, на нагрів повітря в приміщенні, технологічні тепловтрати, нагрів надходять матеріалів і напівфабрикатів). Основними засобами захисту від теплових випромінювань є екранування та теплоізоляція, а також пристрій місцевих припливних систем вентиляції. При природній вентиляції (за допомогою вікон) повітря надходить у приміщення і видаляється з нього внаслідок різниці температур і тиску.. Механічна вентиляція забезпечується вентиляторами, що забирають повітря зовні і направляє його до будь-якого робочого місця. або устаткування, а також видаляють забруднене повітря

2.4 Вимоги до організації робочого місця працівника

До самостійної роботи на комп'ютерах допускаються особи, які пройшли медичний огляд, навчання по професії, вступний інструктаж з охорони праці та первинний інструктаж з охорони праці на робочому місці. В подальшому вони проходять повторні інструктажі з охорони праці на робочому місці один раз на півріччя, періодичні медичні огляди один раз на два роки

Робочі місця повинні бути розташовані так, щоб у поле зору працюючого не попадали поверхні, що мають властивість віддзеркалювання, вікна освітлювальні прилади. Відеотермінали повинні встановлюватися під кутом 90-100 градусів від вікон, так, щоб світло падало з боку. Робочі місця з ВДТ доцільно розміщати в глибині приміщення. Розташування відео термінала, при якому працюючий звернений обличчям або спиною до вікон, неприпустимо при будь-якому способі реалізації загального висвітлення, як прямим, так і відбитим світлом.

Робочий стіл повинен регулюватися по висоті в границях 680-800 мм, а ширина – забезпечувати можливість виконання операцій в зоні досяжності моторного поля Рекомендовані розміри столу: висота 725 мм, ширина 600-1400 мм, глибина 800-1000 мм. Робочий стілець повинен бути оснащений підйомно-поворотним пристроєм для регулювання висоти сидіння і спинки, а також кута її нахилу. Регулювання кожного параметра повинне вироблятися легко, бути незалежним і надійно фіксуватися.

Розташування екрана ВДТ має забезпечувати зручність зорового спостереження у вертикальній площині під кутом $+30^0$ до нормальної лінії погляду працюючого.

Клавіатуру слід розташовувати на поверхні столу на відстані 100…300 мм від краю, звернутого до працюючого.

3 Пожежна безпека

Під пожежною безпекою розуміють систему державних і суспільних заходів, спрямованих на охорону від вогню людей і власності. Пожежна безпека приміщень, що мають електричні мережі, регламентується ГОСТ 12.1.033-81, ГОСТ 12.1.004-85. Робота оператора ЕОМ повинна вестися в приміщенні, що відповідає категорії Д пожежної безпеки (негорючі речовини й матеріали в холодному стані).

 Куріння у не відведених для цього місцях	 Порушення правил користування електроприладами	 Необережне поводження з вогнем

Всі приміщення повинні бути забезпечені первинними засобами пожежогасіння: пожежним водопостачанням (пожежні крани ПК), пожежні щити з набором пожежного інструменту, вуглекислотними або порошковими вогнегасниками. У випадку виникнення пожежі необхідно відключити електроживлення, викликати по телефону 101 пожежну команду, евакуювати людей із приміщення відповідно до плану евакуації і приступити до ліквідації пожежі.

ВИСНОВКИ

У кваліфікачійній роботі був проведен аналіз систем захисту веб-сайту від несанкціонованого доступу та виявлено, що існує безліч інструментів та методів захисту, які можуть бути використані для запобігання несанкціонованому доступу до веб-сайту. Було проаналізовано тести на проникнення та дана оцінка захищеністі різноманітних інформаційних системи від несанкціонованого впливу.

Аналіз систем захисту веб-сайту від несанкціонованого доступу дозволяє визначити ефективність технічних та організаційних заходів для забезпечення безпеки веб-ресурсу. З метою запобігання несанкціонованому доступу до веб-сайту важливо використовувати не лише технічні засоби, а й забезпечувати належний рівень організації роботи з персоналом та користувачами.

Перш за все, для захисту веб-сайту необхідно мати надійну систему аутентифікації та авторизації, що дозволяє перевіряти ідентичність користувачів та відповідно надавати або обмежувати їх доступ до різних ресурсів сайту. Також можна використовувати різноманітні криптографічні протоколи, такі як SSL / TLS, щоб захистити передачу конфіденційної інформації між користувачами та сервером.

Для захисту веб-сайту від атак відмови в обслуговуванні (DDoS) можна використовувати різні техніки, такі як кешування статичного вмісту, розподілене сховище файлів, географічну реплікацію та інші. Також можна встановити фільтри, які дозволяють блокувати трафік від підозрілих IP-адрес та захистити веб-сайт від SQL-ін'єкцій та інших відомих типів вразливостей.

Для захисту веб-сайту від зловмисників можна використовувати відстеження відвідувачів, системи виявлення вторгнень, системи моніторингу безпеки та інші інструменти. Також важливо регулярно виконувати аудит безпеки, щоб виявляти та усувати вразливості та слабкі місця в системі захисту.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 17799:2005. Informationtechnology. Security techniques. Code ofpracticeforinformationsecuritymanagement.
2. ISO/IEC 27001:2005. Informationtechnology. Security techniques. Informationsecuritymanagementsystems. Requirements.
3. ISO/IEC TR 27035:2011. Informationtechnology − Security techniques − Informationsecurityincidentmanagement.
4. ISO/IEC 20000:2011. Informationtechnology. Servicemanagement. Part 2: Code ofpractice.
5. DefiningIncidentManagementProcessesforCSIRTs: A WorkinProgress // CMU/SEI-2004-TR-015: ESC-TR-2004-015 ChrisAlberts, AudreyDorofee, GeorgiaKillcreceOctober 2004 NetworkedSystemsSurvivabilityProgram.
6. Замула О.А. Аналіз міжнародних стандартів в галузі оцінювання ри- зиків інформаційної безпеки / О.А. Замула, В.І. Черниш // Системи обробки інформації: зб. наук. пр. – Х.: ХУПС, 2011. – Вип. 2 (92). – С.53-56.
7. Гавриленко О.В. Відповідність національної нормативної бази у сфері технічного захисту інформації міжнародним стандартам: зіставлення документів, шляхи гармонізації. Матеріали XVII Міжнародної науково-практичної конференції «Безпека інформації у інформаційно-телекомунікаційних системах», м.Київ, 2015.
8. НД ТЗІ 2.5-004-99 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”. [Електрон. ресурс]: –Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40386&cat_id=38835.
9. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 5 липня 1994 року № 80/94-ВР, Відомості Верховної Ради України (ВВР), 1994, № 31. – с.286

10. СОУ Н НБУ 65.1 СУІБ 1.0:2010. Настанова. Методи захисту в банківській діяльності. Система управління інформаційною безпекою. [Електрон. ресурс]: – Режим доступу: http://www.uk.xlibx.com/4yuridicheskie/1354389-1-sou-nbu-651-suib-10-2010-standart-organizacii-ukraini-nastanova-metodi-zahistu-bankivskiy-diyalnosti-siste.php.

11. НД ТЗІ 3.7-003-05 “Порядок проведення робіт із створення комплек- сної системи захисту інформації в інформаційно-телекомунікаційній системі”. [Електрон. ресурс]: – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=46074&cat_id=38835.

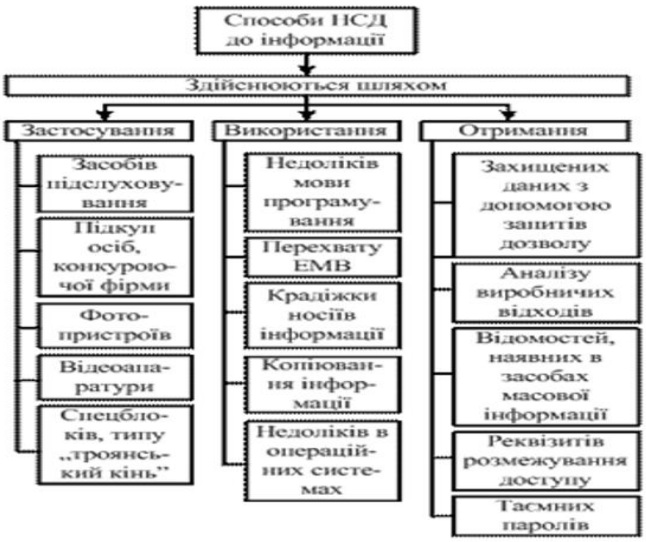
12. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.

13. СкембрейцДж. Безопасность Web-приложений — готовыерешения / Дж. Скембрейц, М. Шема. — М.: Издательскийдом «Вильямс», 2003. — 384 с.

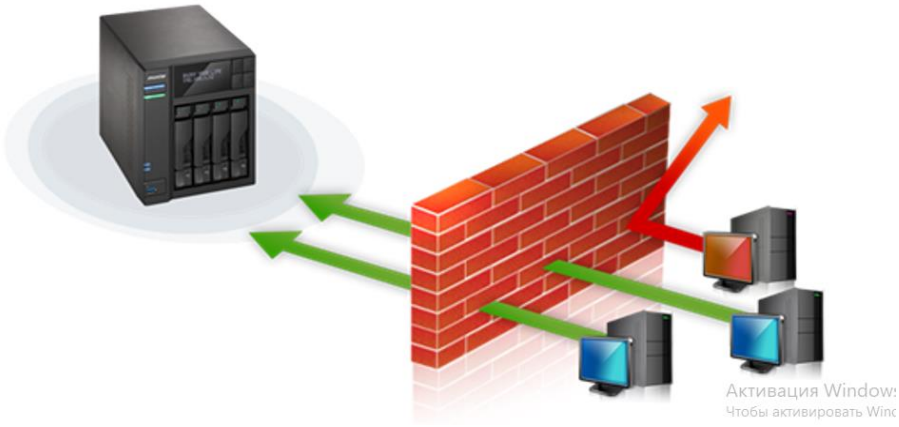
ДОДАТОК Б

Слайди мультимедійної презентації

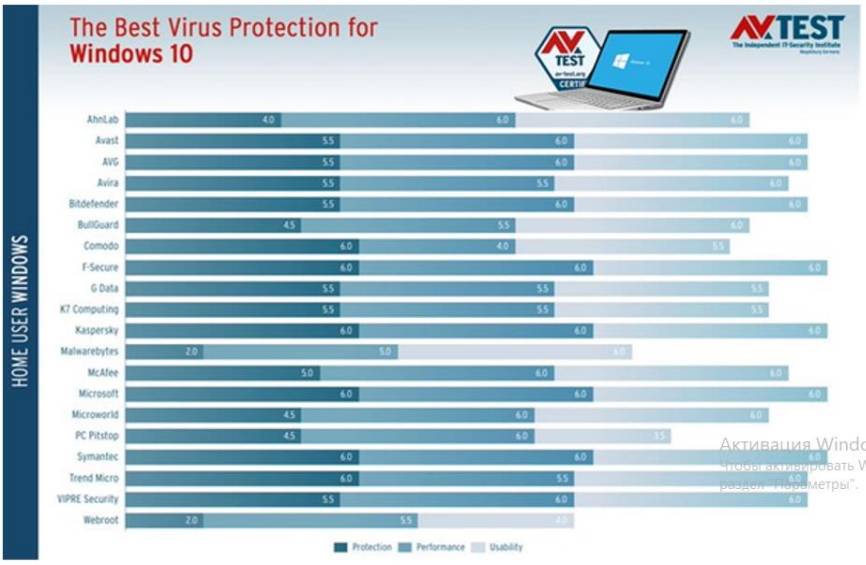
Способи НСД



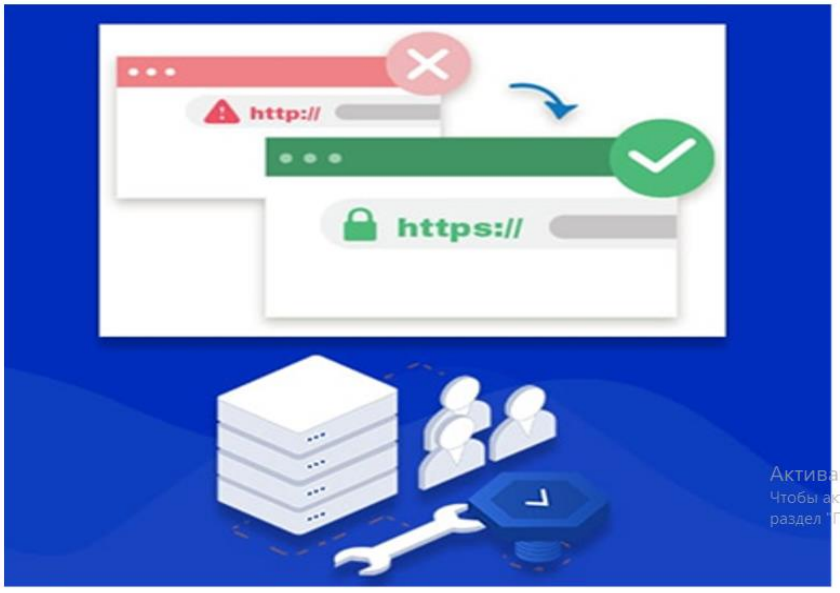
Аналіз застосування Firewall



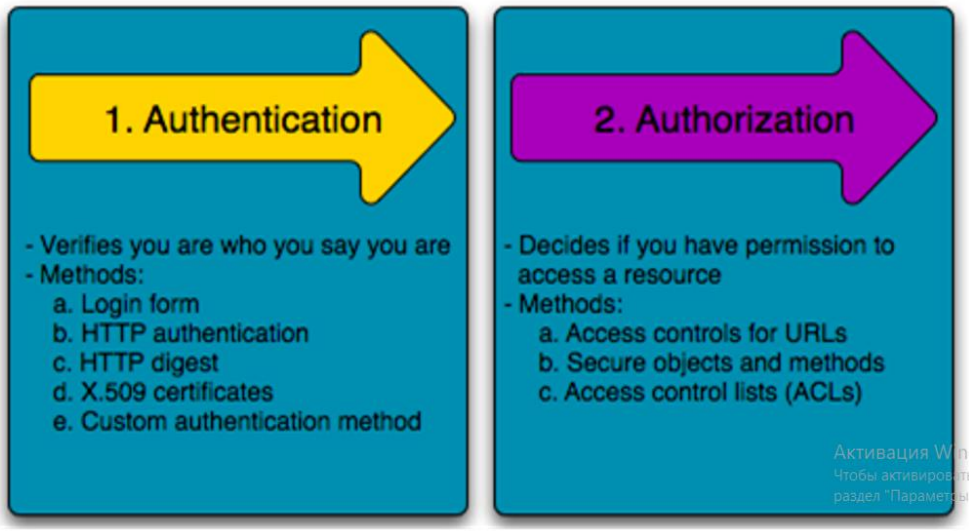
Результати тестування антивірусів



Перехід від HTTP до HTTPS

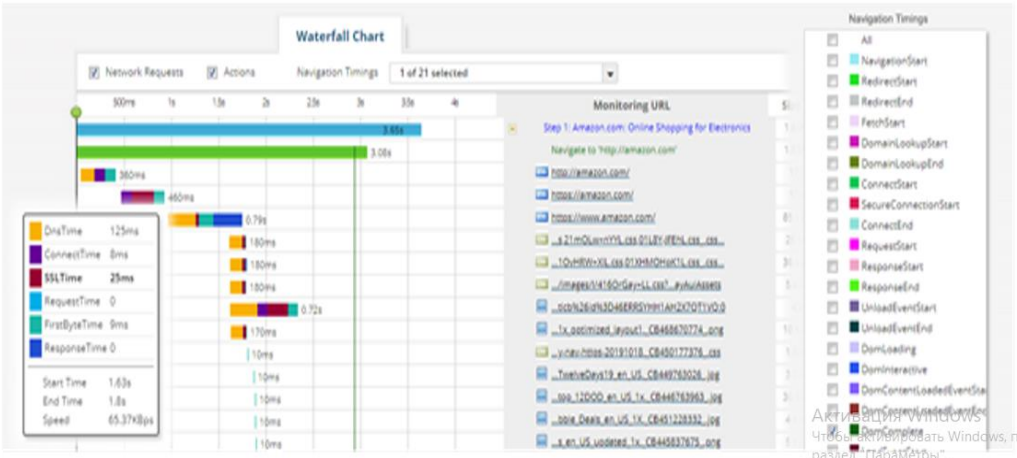


Система аутентифікації/авторизації

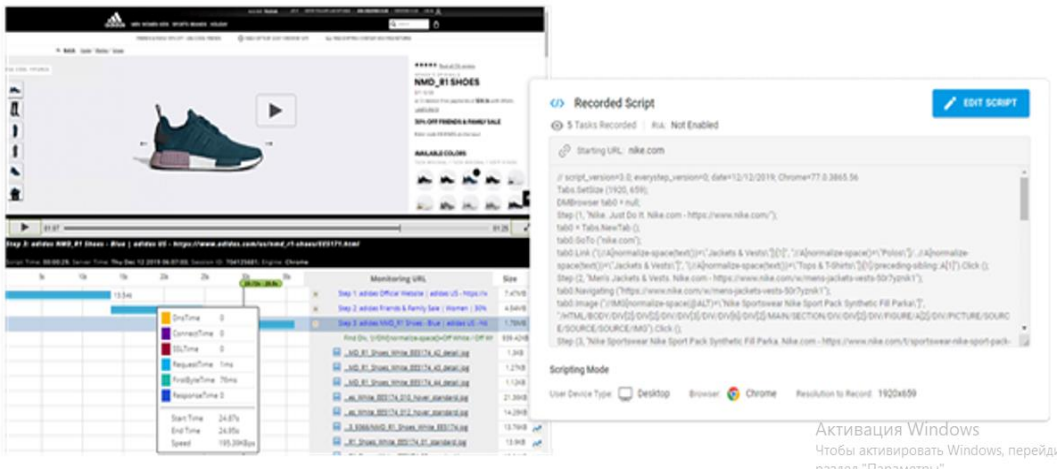


Хмарне резервне копіювання

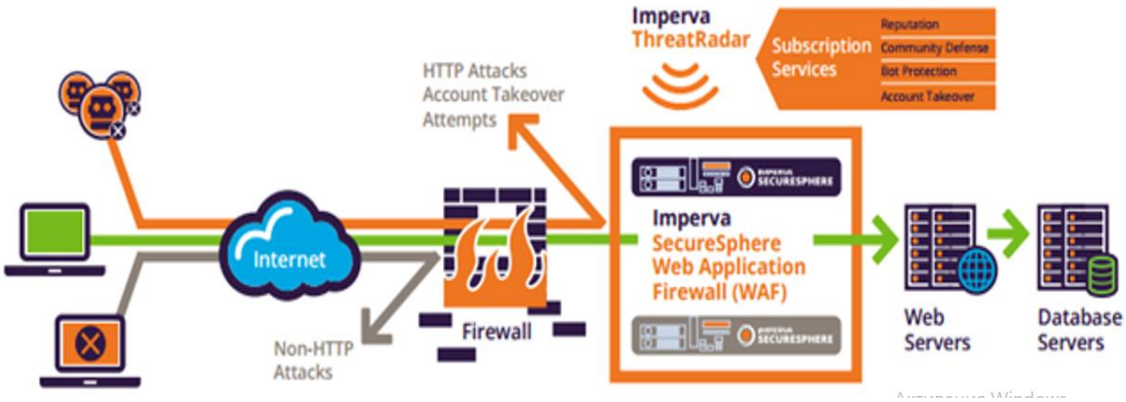
Приклад моніторингу веб-сторінок



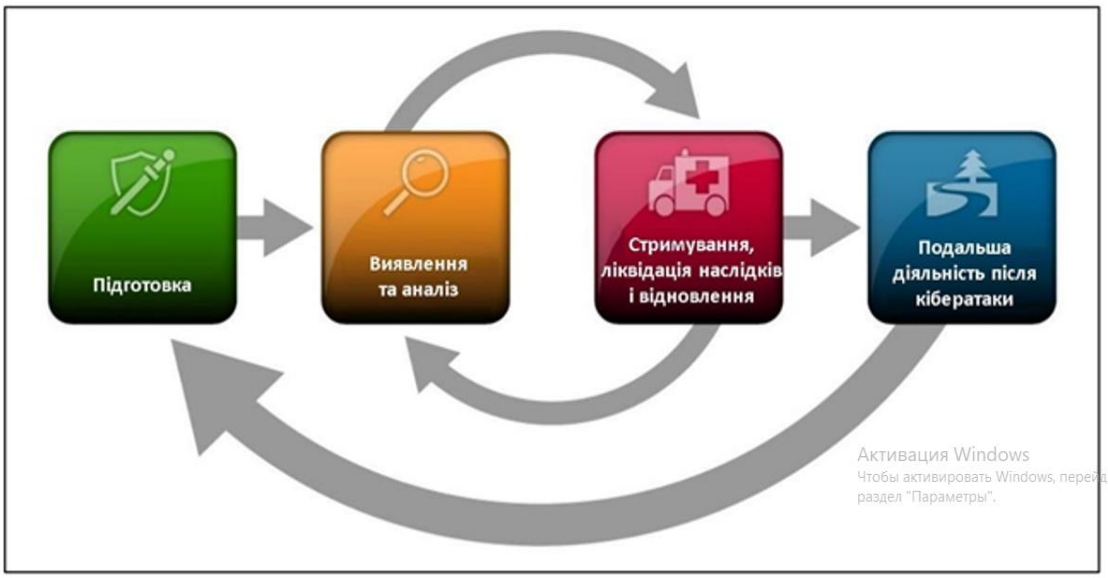
Приклад моніторингу веб-додатків



Захист веб-додатків від Imperva Secure Sphere Web Firewall Application



Етапи реагування на інциденти



ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на випускну роботу бакалавра здобувача освіти

відділення комп'ютерних систем

Склярова Євгена Ігоровича

(прізвище, ім`я та по батькові)

Спеціальність **123 «Комп'ютерна інженерія»**

Освітня програма **Обслуговування комп'ютерних систем та мереж**

Керівник дипломного проекту (роботи) **Шевцов Юрій Сергійович**

(прізвище, ім`я та по батькові)

Тема дипломного проекту (роботи)

Аналіз систем захисту веб-сайту від несанкціонованого доступу

Обсяг розрахунково-пояснювальної записки 71 сторінок

Обсяг графічної (презентаційної) частини 13 аркушів (слайдів)

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ (РОБОТИ)

а) заключення про ступінь відповідності виконаного дипломного проекту (роботи) завданню

Дипломний проект повністю відповідає завданню до дипломного проектування. Графічна частина складається з окремих слайдів, оформлених у вигляді презентації, передбачених технічним завданням. Якість виконання пояснювальної записки та слайдів добра.

б) характеристика виконання кожного розділу дипломного проекту (роботи)

Пояснювальна записка дипломного проекту виконана якісно, у повному обсязі. В дипломному проекті здобувачем проаналізовано системи захисту веб-сайту від несанкціонованого доступу. Розглянуті технічні та програмні методи захисту. В дипломному проекті в останніх розділах проаналізовано економічні показники та питання охорони праці.

в) оцінка якості виконання пояснювальної записки та графічної частини дипломного проекту (роботи) _____

Презентаційні матеріали виконані якісно, демонстративно та відповідають вмісту теоретичного матеріалу

г) перелік позитивних якостей дипломного проекту (роботи)_____

Здобувачем проаналізовані системи захисту веб-сайту від несанкціонованого доступу, що є дуже актуальною тематикою в наш час.

д) основні недоліки дипломного проекту (роботи) _____

Серед недоліків роботи варто вказати, відсутність посилань на перелік використаних джерел та наявність орфографічних помилок в тексті пояснювальної записки

Оцінка розрахункової частини _____ *4 (добре)*

Оцінка графічної частини _____ *5 (відмінно)*

Загальна оцінка _____ *4 (добре)*

Прізвище, ім'я, по батькові рецензента _____ *Василіу Євген Вікторович*

Місце роботи і посада рецензента _____ *Державний університет інтелектуальних технологій і зв'язку, д.т.н., проф. кафедри КБ та ТЗІ, декан факультету інформаційних технологій та кібербезпеки*

Підпис: _____

«16» 06 2023 р.

ПІДПИС ПОСВІДЧУЮ
НАЧАЛЬНИК ВІДДІЛУ КАДРІВ ДУІТЗ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ * ВІДДІЛ КАДРІВ * 43997335 *

ВСП «Одеський технічний фаховий коледж ОНТУ»

ВІДГУК

керівника про випускну роботу бакалавра

Склярова Євгена Ігоровича

(прізвище, ім`я та по батькові)

Спеціальність 123 "Комп'ютерна інженерія"

Тема випускної роботи Аналіз систем захисту веб-сайту від несанкціонованого доступу

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ (РОБОТИ)

а) Обсяг і якість виконання роботи (графічного матеріалу і розрахунково-пояснювальної записки) Випускна робота виконана відповідно технічному завданню. Пояснювальна записка до випускної роботи містить 71 сторінку. У пояснювальній записці зроблено аналіз систем захисту веб-сайту від несанкціонованого доступу, які розділяються на технічні та програмні. Графічна частина складається з 13 слайдів, оформлених у вигляді презентації, передбачених технічним завданням. Якість виконання пояснювальної записки та слайдів добра, розробку виконано у повному обсязі.

б) Самостійність роботи

Протягом виконання випускної бакалаврської роботи Скляров Є. І. поступово та послідовно виконував всі етапи, проявив ініціативу у створенні загальної концепції та реалізації випускної роботи. Всі роботи він виконував самостійно, з оглядом на рекомендації керівника.

в) Теоретична підготовка здобувача освіти

Скляров Є. І. під час роботи над випускною бакалаврською роботою вивчив достатню кількість літературних джерел за даною тематикою.

Вважаю, що теоретична підготовка здобувача освіти добра і він готовий до захисту роботи.

г) Вміння розв`язувати виробничі і конструкторські питання на базі останніх досліджень науки і техніки, передових методів виробництва

Під час виконання роботи Скляров Є. І. мав змогу самостійно приймати окремі рішення з виконання програмної частини роботи та показав вміння організовано працювати над поставленою задачею, користуючись сучасними комп'ютерними програмними засобами.

Оцінка розрахункової частини Добре

Оцінка графічної частини Відмінно

Загальна оцінка Відмінно

Прізвище, ім`я, по батькові Харченко Роман Юрійович к.т.н.

Місце роботи і посада керівника роботи

доцент каф. "Морського радіозв'язку" НУ «Одеська Морська академія»

Підпис

«12» 06 2023 р.

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Скляров Євген Ігорович,
здобувач освіти гр. 4ФКГ-06, та

Харченко Роман Юрійович,
керівник дипломного проекту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до випускної кваліфікаційної роботи бакалавра на тему:

«Аналіз систем захисту веб-сайту від несанкціонованого доступу»
(автор роботи – Скляров Є. І., керівник роботи – Харченко Р.Ю.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2023 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи, і даємо згоду на обробку персональних даних.

Виконавець _____ / Скляров Є. І /

Керівник _____ / Харченко Р.Ю./

« 12 » _____06_____ 2023 р.

ВСП «Одеський технічний фаховий коледж ОНТУ»

ВІДГУК

керівника про випускну роботу бакалавра

Склярова Євгена Ігоровича

(прізвище, ім`я та по батькові)

Спеціальність 123 "Комп'ютерна інженерія"

Тема випускної роботи Аналіз систем захисту веб-сайту від несанкціонованого доступу

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ (РОБОТИ)

а) Обсяг і якість виконання роботи (графічного матеріалу і розрахунково-пояснювальної записки) Випускна робота виконана відповідно технічному завданню. Пояснювальна записка до випускної роботи містить 71 сторінку. У пояснювальній записці зроблено аналіз систем захисту веб-сайту від несанкціонованого доступу, які розділяються на технічні та програмні. Графічна частина складається з 13 слайдів, оформлених у вигляді презентації, передбачених технічним завданням. Якість виконання пояснювальної записки та слайдів добра, розробку виконано у повному обсязі.

б) Самостійність роботи

Протягом виконання випускної бакалаврської роботи Скляров Є. І. поступово та послідовно виконував всі етапи, проявив ініціативу у створенні загальної концепції та реалізації випускної роботи. Всі роботи він виконував самостійно, з оглядом на рекомендації керівника.