МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеська національна академія харчових технологій
Університет Інформатики і прикладних знань, м.Лодзь, Польща
Національний технічний університет України «Київський політехнічний інститут»
Навчально-науковий інститут комп'ютерних систем і технологій «Індустрія 4.0» ім. П.М. Платонова

XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції

Одеса

22-23 квітня 2021 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 22-23 квітня 2021 р**.** - Одеса, Видавництво ОНАХТ, 2021 р. – 229 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані за тематичними напрямками конференції.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Котлик С.В.

2. Кузніченко С.Д., Бучинська І.В. (2019) Вибір операторів агрегування для багатокритеріальної оцінки придатності територій. Кібербезпека: освіта, наука, техніка, 2019. – Том 2 № 6. – С.46–56.
3. Yager R (1988) "On ordered weighted averaging aggregation operators in multicriteria decision making", IEEE Transactions on System, Man, and Cybernetics 18:183–190.
4. Кузніченко С.Д., Бучинська І.В., Коваленко Л.Б. (2019) Використання OWA-оператора Ягера з нечіткими квантифікаторами в ГІС-орієнтованих багатокритеріальних моделях прийняття рішень. Матеріали 8-ї Міжнародної науково-технічної конференції "Інформаційні системи та технології", КоблевеХарків, 9–14 вересня 2019 р. с 113–116.

КЛАСИФІКАЦІЯ ЗАГРОЗ ВЕБ-ЗАСТОСУНКІВ

ЛАВРЄНОВ В.А., ст. 551 гр.
СІРЕНКО О.І., науковий керівник, ст. викл. кафедра КІ
Одеська національна академія харчових технологій

Безпека веб-застосунків, є одним з найбільш важливих питань інформаційної безпеки. Велика частина веб-сайтів і веб-застосунків в Інтернеті, мають різного роду уразливості, а також схильні до постійних атак.

Мета даної роботи, розібрати основні вразливості веб-застосунків і класифікувати їх за певними ознаками. Розглянемо основні загрози веб-застосунків. Загрози інформаційної безпеки веб-додатки поділяються на три основні типи:

1. Загрози конфіденційності (несанкціонований доступ до даних).
2. Загрози цілісності (несанкціоноване спотворення або знищення даних).
3. Загрози доступності (обмеження або блокування доступу до даних).

Головним джерелом усіх загроз інформаційній безпеці веб-застосунків, є зовнішні порушники – люди, які мають несанкціонований доступ до веб-застосунку. Зовнішній порушник, може виявляти максимально можливу кількість векторів атаки для складання та реалізації потенційно успішних сценаріїв злому, або ж масово атакувати, зазвичай використовує кілька поверхневих вразливостей.

Загрози безпеці, найчастіше пов'язані з наступними п'ятьма параметрами:

1. Вразливості веб-застосунків або їх компонентів.
2. Використання механізмів перевірки ідентифікації.
3. Клієнт-сайд атаки, атаки на користувачів.
4. Витік або розголошення критичної інформації.
5. Логічні атаки.

Вразливості веб-застосунків, працюють за рахунок виконання коду на віддаленому сервері. На сервер надходять дані у вигляді оброблених користувачем запитів, подібні дані використовуються при складанні команд, що застосовуються для генерації динамічного контенту. При відсутності певних вимог безпеки при розробці веб-застосунків, зовнішній порушник може отримати доступ до модифікації виконуваних команд, прикладом можна вважати SQL-ін'єкції.

Атаки, спрямовані на використовувані веб-застосунком методи перевірки ідентифікатора користувача, або спрямовані на методи, які використовуються веб-сервером для визначення вчинення дій дозволу користувача. Один з найбільш частих і простих видів атак, прикладами можуть бути методи перебору паролів або обходи авторизації.

Клієнт-сайд, передбачає, що при відвідуванні веб-ресурсу, між користувачем і сервером встановлюються довірчі відносини, тим самим не чекаючи атак з боку сайту. Цим користується зовнішній порушник, використовуючи властиві для цього методи проведення атак на клієнтів, наприклад, такі як міжсайтовий скриптинг.

Розголошення інформації, як правило, зустрічається в двох формах. Перший – розголошення про компоненти і структуру веб-застосунку, а другий – витік інформації з веб-застосунку, з причин, не надійного захисту.

Логічні атаки спрямовані на експлуатацію функцій додатка або логіки його функціонування. Логіка додатка є очікуваний процес функціонування програми при виконанні певних дій, наприклад, відновлення пароля, реєстрація облікового запису або транзакції в інтернет-магазинах. Застосунок може вимагати від користувача коректного виконання декількох послідовних дій для виконання певного завдання. Зовнішній порушник обходить або використовує ці механізми в своїх цілях. До таких атак можна віднести DoS та DDoS.

Існує два основних види атак на веб-застосунки – це цільові атаки і нецільові атаки.

Цільові атаки – це будь-які напади зовнішніх порушників на конкретний сайт або їх групу, об'єднану однією ознакою. Такі операції протиставляються масовим атакам за допомогою вірусів або інших шкідливих програм, де жертва обирається за принципом доступності. Мета у таких атак, зазвичай, є отримання конфіденційної інформації для матеріальної вигоди.

Нецільові атаки здійснюються на випадкові сайти. Основним завданням нецільової атаки, є отримання несанкціонованого доступу до веб-застосунків, атакуючи відразу велику вибірку ресурсів, відібраних за якимось критерієм, наприклад, веб-застосунки працюють на певній системі управління контентом. При позитивному результаті, зовнішній порушник, створює акаунт адміністратора всередині веб-застосунку для впровадження на ресурс шкідливих сценаріїв, або для крадіжки бази даних.

Поширення атак на веб-застосунки пов'язані з двома головними факторами: відсутність безпеки, або ж, знижена безпека веб-застосунку і низький поріг входу для зовнішніх порушників.

Як правило, більшість веб-застосунків не використовують спеціальні засоби моніторингу та виявлення загроз, а також захисту від загроз. Також причиною може служити безвідповідальність адміністратора і команди розробників, які допускають до фінальної версії, код з помилками.

У даній роботі були зібрані і класифіковані, за кількома ознаками, основні загрози і види атак веб-застосунків, а також були вказані основні причини поширення атак на веб-застосунки. Для позбавлення від можливості зіткнення з даними проблемами, необхідно дотримуватися базових заходів безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Уязвимости и угрозы веб-приложений в 2019 году [Електронний ресурс] // Positive Technologies. – Режим доступу: https://www.ptsecurity.com/ru-ru/
2. Уязвимости сайтов [Електронний ресурс] // ANTI-MALWARE. – Режим доступу: https://www.anti-malware.ru/
3. Классификация угроз безопасности Web-приложений [Електронний ресурс] // InfoSecurity. – Режим доступу: http://www.infosecurity.ru/
4. Как защитить сайт: виды угроз безопасности и способы их избежать [Електронний ресурс] // RedKrab. – Режим доступу: https://webevolution.ru/

UDC: 004.056.5:336.74

PROOF OF ZERO-KNOWLEDGE IN THE TASKS OF ANONYMIZATION OF FINANCIAL TRANSACTIONS

PROKOPOV E. K.(*prokopov.emmanuil@stud.onu.edu.ua*)
Odessa I.I. Mechnikov National University

XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Одеса

22-23 квітня 2021 р.

Збірник включає доповіді учасників конференції. Тези доповідей публікуються у вигляді, в якому вони були подані авторами.

Відповідальність за зміст і форму подачі матеріалу несуть автори статей.

Редакційна колегія: Котлик С.В., Корнієнко Ю.К.

Комп'ютерний набір і верстка: Соколова О.П.

Відповідальний за випуск: Котлик С.В.