Ministry of Education and Science of Ukraine

ODESSA NATIONAL ACADEMY OF FOOD TECHNOLOGIES

International Competition of
Student Scientific Works

BLACK SEA SCIENCE 2018

PROCEEDINGS

April, 4, 2018

ODESSA, ONAFT 2018

Ministry of Education and Science of Ukraine

Odessa National Academy of Food Technologies

International Competition of Student Scientific Works

BLACK SEA SCIENCE 2018

Proceedings

April 4, 2018

Odessa, ONAFT 2018

Міністерство освіти і науки України

Одеська національна академія харчових технологій

Міжнародний конкурс студентських наукових робіт

BLACK SEA SCIENCE 2018

Матеріали

4 квітня 2018 року

Одеса, ОНАХТ 2018

UDC 001(262.5):378.4.091.27(08)
BBC 421D221
B64

Black Sea Science 2018: Proceedings of the International Competition of Student Scientific Works, April 4, 2018, Odessa / Odessa National Academy of Food Technologies; B. Yegorov, M. Mardar (editors-in-chief.) [*et al.*]. – Odessa: ONAFT, 2018. – 827 p.

Proceedings of International Competition of Student Scientific Works «Black Sea Science 2018» contain the works of winners of the competition.

The author of the work is responsible for the accuracy of the information.

ISBN 978-966-289-181-2 Odessa National Academy of Food Technologies

УДК 001(262.5):378.4.091.27(08)
ББК 421D221
В64

Black Sea Science 2018: Матеріали Міжнародного конкурсу студентських наукових робіт, 4 квітня 2018 р., Одеса / Одеська національна академія харчових технологій; Б. В. Єгоров, М. Р. Мардар (відп. ред.) [та ін.]. – Одеса: ОНАХТ, 2018. – 827 с.

Збірник включає матеріали робіт переможців Міжнародного конкурсу студентських наукових робіт «Black Sea Science 2018**».**

За достовірність інформації відповідає автор публікації.

ISBN 978-966-289-181-2 Одеська національна академія харчових технологій

Organizing committee:

Prof. Bogdan Yegorov, D.Sc., Rector of Odessa National Academy of Food Technologies, Head of the Committee

Prof. Maryna Mardar, D.Sc., Vice-Rector for Scientific and Pedagogical Work and International Relations of Odessa National Academy of Food Technologies, Deputy Head of the Committee

Prof. Stefan Dragoev, D.Sc., Vice-Rector on Research and Business Partnerships of University of Food Technologies (Bulgaria)

Prof. Baurzhan Nurakhmetov, D.Sc., First Vice-Rector of Almaty Technological University (Kazakhstan)

Prof. Andrzei Kowalski, Dr. habil., Director of Institute of Agricultural and Food Economics (Poland)

Dr. Olivera Djuragic, Ph.D., Director of Scientific Institute of Food Technology of University of Novi Sad (Serbia)

Prof. Mircea Bernic, Dr. habil., Vice-Rector on Research and Doctorate of Technical University of Moldova (Moldova)

Prof. Jacek Wrobel, Dr. habil., Rector of West Pomeranian University of Technology (Poland)

Prof. Michael Zinigrad, D.Sc., Rector of Ariel University (Israel)

Dr. Mei Lehe, PhD, Vice-President of Ningbo Institute of Technology, Zhejiang University (China)

Prof. Plamen Kangalov, Ph.D., Vice-Rector on Education of "Angel Kanchev" University of Ruse (Bulgaria)

Dr. Alexander Sychev, Ph.D., Assoc. Professor of Sukhoi State Technical University of Gomel (Belarus)

Dr. Hanna Lilishentseva, Ph.D., Assoc. Professor, Head of the Department of Merchandise of Foodstuff of Belarus State Economic University (Belarus)

Prof. Heinz Leuenberger, Ph.D., University of Applied Sciences and Arts Northwestern Switzerland (Switzerland)

Організаційний комітет:

Єгоров Богдан Вікторович – д.т.н., професор, ректор – Одеська національна академія харчових технологій – голова оргкомітету

Мардар Марина Ромиківна – д.т.н., професор, проректор з науково–педагогічної роботи та міжнародних зв'язків – Одеська національна академія харчових технологій – заступник голови оргкомітету

Драгоєв Стефан Георгієв– д.т.н., професор, проректор з наукової роботи і бізнес партнерства – Університет харчових технологій (Болгарія)

Нурахметов Бауржан Кумаргалієвич – д.т.н., професор, перший проректор – Алматинський технологічний університет (Казахстан)

Ковальські Анджей – доктор-хабілітат, професор, директор інституту економіки сільськогосподарської та харчової промисловості – Інститут сільськогосподарської та продовольчої економіки (Польща)

Дюрагіц Олівера – доктор, директор інституту харчових технологій – Університет в м. Нові Сад (Сербія)

Бернік Мірча – доктор-хабілітат, професор, проректор з наукової роботи та докторантури – Технічний університет Молдови (Молдова)

Вробель Яцек– доктор-хабілітат, професор, ректор – Західнопоморський технологічний університет (Польща)

Зініград Михаїл – доктор наук, професор, ректор – Аріельський університет (Ізраїль)

Лехе Мей – доктор, віце-президент – Технологічний інститут Нінбо Чжэцзянського університету (Китай)

Кангалов Пламен – професор, доктор, проректор з навчальної роботи – Русенський університет «Ангел Канчев» (Болгарія)

Сичев Олександр Васильович – к.т.н, доцент, проректор з навчальної роботи – Гомельський державний технічний університет ім. П. Й. Сухого (Білорусь)

Лілішенцева Анна Миколаївна – к.т.н, доцент, зав. кафедрою товарознавства продовольчих товарів – Білоруський державний економічний університет (Білорусь)

Леунбергер Хайнц – доктор, професор – Університет прикладних наук і мистецтв Північно-західної Швейцарії (Швейцарія)

SOFTWARE TRAINER FOR DEMONSTRATING VULNERABILITIES OF WEB APPLICATIONS

Author – Babiychuk V.
Supervisor – Smyrnova K.
Odessa National Academy of Food Technologies

In the work the problems of training of specialists in information security in the educational process of higher educational institutions are considered.

Since the theoretical foundations are not enough to conduct a high-quality audit of the information security of web systems, and practical fixing causes a number of difficulties due to the specific actions required, solutions are proposed in the form of a computer simulator that demonstrates the various vulnerabilities of real web systems.

The proposed system allows you to learn to "see" the network through the eyes of an attacker and personally conduct various types of attacks to better understand the vulnerabilities of the Web applications being examined.

ПРОГРАММНЫЙ ТРЕНАЖЕР ДЛЯ ДЕМОНСТРАЦИИ УЯЗВИМОСТЕЙ ВЕБ-ПРИЛОЖЕНИЙ

Автор – Бабийчук В.Д.
Руководитель – Смирнова Е.В.
Одесская национальная академия пищевых технологий

Введение

Большинство современных решений разрабатываются как веб-приложения. Веб-технологии используются практически во всех отраслях – банковские системы, торговые площадки, интернет-магазины, блоги и простые страницы-визитки какой-либо компании. Веб-приложения имеют ряд неоспоримых преимуществ – возможность удаленной работы, быстрая разработка, независимость от клиентской платформы. Для управления такими приложениями

достаточно наличие веб-браузера, который доступен даже на мобильном телефоне.

Однако, территориальная доступность веб-приложений несет в себе и существенный минус. В веб приложениях приходится уделять дополнительное внимание безопасности предоставляемого решения. Безопасность веб-приложений находится в первой десятке угроз информационной безопасности уже свыше 10 лет. Несмотря на это, специализированных средств защиты веб-приложений достаточно мало и они больше рассчитаны на корпоративное использование, так как имеют достаточно высокую цену. Поэтому обеспечение защиты, по большей части, возлагается на разработчика приложения. Разработчик, без соответствующего опыта в сфере информационной безопасности, предусмотреть все возможные проблемы не в состоянии. И, зачастую, даже крупные корпоративные ресурсы, государственные ресурсы имеют массу возможных уязвимостей – XSS (Cross-Site Scripting, межсайтовое выполнение сценариев), SQL Injection (внедрение операторов SQL), CSRF (Cross-Site Request Forgery, подделка межсайтовых запросов), отсутствие защиты от подбора учетных данных (Brute Force) и другие.

Разработчикам необходимо научиться “видеть” сеть глазами злоумышленника – понимать суть возможных атак, видеть проблемные места и иметь понимание того, как закрывать такие бреши. Разнообразные существующие руководства по веб-безопасности дают лишь теоретическое представление атак на веб-приложения. Но без практического закрепления эти знания невозможно будет применить на реальном проекте.

В работе рассматривается разработка программного тренажера для демонстрации веб-уязвимостей, который поможет более качественному обучению будущих разработчиков и специалистов по информационной безопасности.

1 Аналитический обзор

Сегодня информация – это главный актив любой компании. Эффективный контроль, защита от несанкционированного доступа, хищения и любого другого не предусмотренного регламентом использования этих активов становится одной из первостепенных задач не только для отдельно взятых компаний, но и для мирового сообщества в целом.

Широкое использование информационных технологий приводит ко множеству вопросов, связанных с обеспечением информационной безопасности.

Практика последних лет показывает, что подготовка специалистов по информационной безопасности становится не только актуальной, но и необходимой для существования различного рода предприятий, особенно критически важных.

Очень часто считают, что обеспечить информационную защиту предприятия может практически любой человек, связанный с миром информационных технологий, способный установить и настроить необходимые программные и аппаратные средства. Однако большая часть проблем в данной области не решается путем применения программно-аппаратных средств.

Если говорить об обучении будущих специалистов по информационной безопасности, то помимо получения качественной теоретической базы, необходимо применять полученные знания практически – для конфигурации систем безопасности, проектирования новых систем, а также для проведения тестирования на проникновение.

Если инженер думает о том, как сделать рабочую конструкцию, специалист по информационной безопасности думает за счёт чего она ломается. То есть специалист должен думать, как злоумышленник. Если этих навыков нет, он не сможет заметить большинство проблем в безопасности систем.

Идея тренажеров для наглядного изучения приемов взлома веб-приложений не нова. Разработчики OWASP (Open Web Application Security Project – открытый проект обеспечения безопасности веб-приложений) предоставляют несколько продуктов для детального изучения наиболее популярных веб-уязвимостей. Рассмотрим детальнее эти продукты, чтобы дать обоснование разрабатываемому продукту.

1.1 Проект DVWA

DVWA(DamnVulnerable Web Application) – веб-приложение, основанное на PHP/MySQL и имеющее большое количество уязвимостей. Главной целью проекта является улучшение понимания написания безопасного кода веб-разработчиками, а также дать возможность студентам и преподавателям больше узнать о безопасности веб-приложений в контролируемой среде.

Рисунок 1.1 – Интерфейс приложения DVWA

Проект платформ независимый. Однако, для его запуска необходимо наличие веб-сервера, содержащего связку Apache+PHP+MySQL.

DVWA предоставляет пользователю ряд упражнений, распределенных по категориям. На странице каждого упражнения имеются подсказки, а также возможность посмотреть исходный код для большего понимания работы приложения в случаях неудачных попыток взлома. Для упражнений можно выбрать уровень сложности либо включить имеющийся веб-файерволл и систему обнаружения вторжений, которые значительно усложняют процесс взлома.

1.2 Проект WebGoat

Это официальная сборка от сообщества OWASP, включающая операционную систему на базе Linux и установленный веб-сервер со всеми имеющимися уязвимостями, необходимыми для понимания наиболее популярных векторов атак на веб-приложения.

Реализована база для проведения около 30 различных видов атак. Проект OWASP WebGoat – это кроссплатформенный инструмент, его можно запустить в любой операционной системе, в которой будут работать Apache Tomcat и Java SDK.

Задания, как правило, привязаны к какой-либо реальной проблеме. Например, в одном из заданий предлагается провести SQL-инъекцию с целью украсть список поддельных кредитных номеров. Также некоторые задания сопровождаются учебной составляющей, показывающей пользователю полезные подсказки и уязвимый код.

При достаточно большом количестве аналогичных систем, все они обладают рядом недостатков:

- нацелены на демонстрацию, а не на тренинги;
- нет возможности их расширять, демонстрируя не определенный вектор атаки, а связку векторов:
- не везде доступны теоретические сведения о методике проведения атаки;
- абсолютно все системы не имеют языковой локализации (только английский язык), что не всегда удобно применять в учебном процессе.

Рис. 1.2. Интерфейс проекта WebGoat

2 Объект, предмет и задачи исследования

Объект исследования -обучение и подготовка специалистов по информационной безопасности в рамках высшего учебного заведения.

Предметом исследования являются интерактивные компьютерные тренажеры как компоненты электронного учебника для усвоения практического материала учебного курса.

Задачи работы:

- провести анализ методики подготовки специалистов по информационной безопасности в ведущих технических высших учебных заведениях мира;
- выявить особенности обучения в рамках аудиторной работы со студентами;

- разработать и обосновать методику подготовки студентов по направлению Информационная безопасность.

3 Результаты работы

Разрабатываемый тренажер имитирует структуру настоящих компаний. Главной целью продукта является обучение молодых специалистов основам информационной безопасности и закрепление навыков анализа веб-систем на возможные угрозы информационной безопасности. Приложение способствует обучению студентов способам защиты информации посредством показа им типичных ошибок разработчиков. Такой подход будет полезен не только в рамках изучения основ тестирования на проникновение, но и будет способствовать совершенствованию навыков проектирования и реализации веб-систем среди разработчиков.

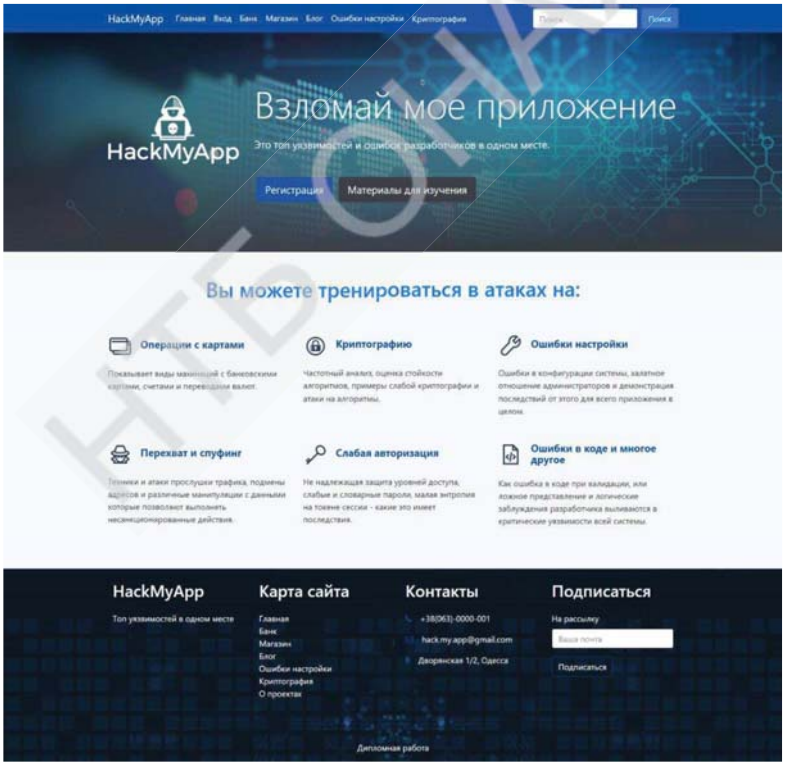

Рис. 3.1. Главное окно тренажера

Основная идея внедрения системы в учебный процесс состоит в следующем. Разработанное приложение запускается локально на каждом персональном компьютере класса вычислительного центра. Целью студента является проведение определенного вида атаки, наградой за которое является “флаг” (секретный код). Флаги генерируются при старте системы на сервере. Флаг обменивается на баллы за выполнение работы. Финальная оценка за практические занятия напрямую зависит от количества собранных флагов. Подобная практика положительно зарекомендовала себя во всем мире под названием CTF (Capture the Flag – захват флага).

Рассмотрим основные разделы рассматриваемого тренажера.

На вкладке «Главная» находится основная информация о данном WEB-приложении с возможностью регистрации. Регистрация необходима для возможности получения флагов за выполненные задачи.

Как видно по главной странице, обучающимся предложены различные вектора атак, которые они смогут опробовать в системе. Для демонстрации взяты наиболее популярные векторы атак на веб-системы согласно рейтингу OWASP TOP10 (Open Web Application Security Project, открытый проект обеспечения безопасности веб-приложений) за 2017 год:

- A1 Внедрение кода;
- A2 Некорректная аутентификация и управление сессией;
- A3 Межсайтовый скриптинг;
- A4 Нарушение контроля доступа;
- A5 Небезопасная конфигурация;
- A6 Утечка чувствительных данных;
- A7 Недостаточная защита от атак (NEW);
- A8 Подделка межсайтовых запросов
- A9 Использование компонентов с известными уязвимостями;
- A10 Недостаточное журналирование и мониторинг.

Для любого вектора атаки предоставляется теоретический материал о методике проведения этого вектора, а также о способах защиты от подобных атак.

Главной особенностью проекта является предоставление структуры реальных систем, в которые заранее “заложены” присущие им уязвимости. В качестве таких систем выступают: банк, интернет-магазин, блог. Помимо этого, можно потренироваться на ошибках настройки сервера и на взломе криптографических алгоритмов.

На вкладке «Банк» находится обучающая часть с примером WEB-банка, которая показывает основные уязвимости банковских систем, таких как: уязвимости конвертации валют, открытость базы данных системы банкинга и т.д.

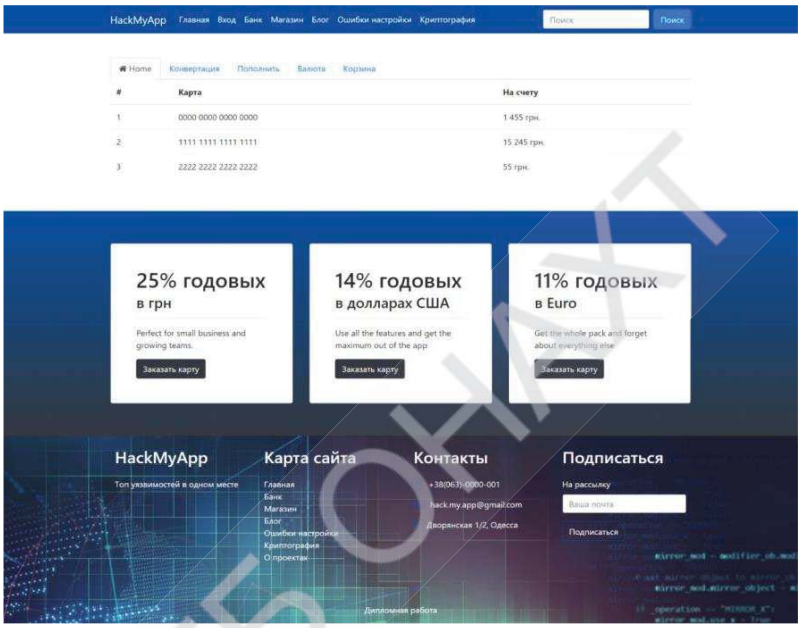

Рис. 3.2. Работа с уязвимостями интернет-банкинга

На вкладке «Магазин» расположен тренажер для интернета магазина, с возможностью регистрации пользователей и покупки различных товаров. Основная задумка данной части тренажера – показать, как злоумышленник может завладеть данными рядового пользователя, его счетами, личными данными и балансом в интернет-магазинах и на торговых площадках.

Вкладка «Блог» показывает типичную страницу блога и демонстрирует основные уязвимости автоматизированных систем наполнения контентом, которые чаще всего используются для создания и ведения блогов. Так же, как и в «Магазине» основная угроза приходится на личные данные и счета пользователей.

Рис. 3.3. Работа с типичными уязвимостями интернет-магазина

Рис. 3.4. Страница блога

Все системы являются фиктивными и с заранее подготовленными уязвимостями. Пример отработки вектора атак приводится ниже на примере внедрения sql-инъекции и результата, который можно получить (рисунок 3.5) и на примере уязвимости конвертации валют (рисунок 3.6).

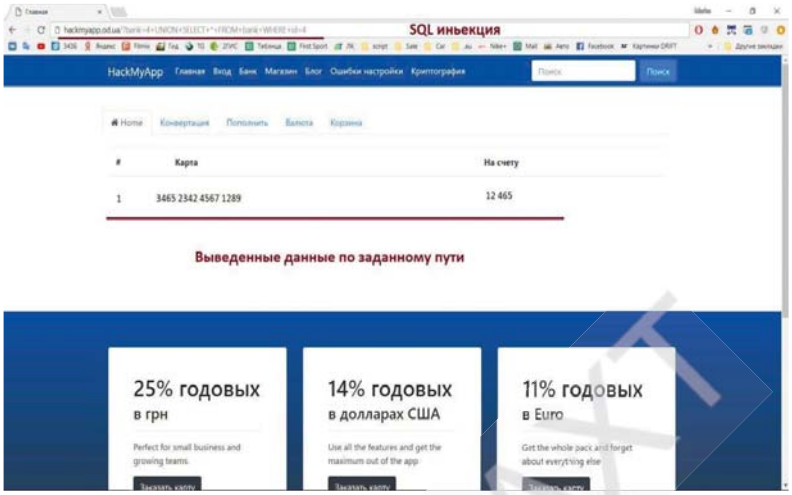

Рис. 3.5. Внедрение sql-инъекции

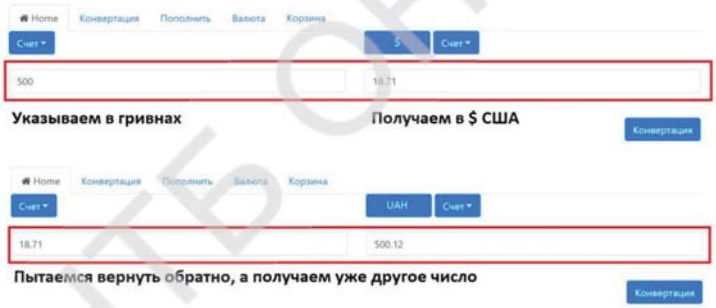

Рис. 3.6. Демонстрация уязвимости конвертации валют

Выводы

Разрабатываемый программный продукт направлен на повышение уровня квалификации разработчиков на раннем этапе их обучения, а также на подготовку специалистов по информационной безопасности и пентестеров (тестирование на проникновение). Внедрение тренажера в учебный процесс высших учебных заведений позволит выпускать специалистов, способных повысить безопасность программных продуктов, выпускаемых IT компаниями.

Тренажер рассчитан на студентов, имеющих начальные познания в проектировании баз данных, в построении компьютерных сетей, а также с пониманием основ веб-разработки.

В ходе проектирования данного продукта были решены следующие задачи:

- Демонстрация возможных технологий защиты от внедрения кода;
- Примеры неправильной проработки аутентификации и управления сессией;
- Результаты нарушения контроля доступа;
- Вывод результатов утечки данных;
- Следствия недостаточной проработки защиты.

Список литературы

1. Karim N. S. A., Saba T., Albuolayan A. Analysis of software security model in scenario of Software Development Life Cycle (SDLC) // Journal of Engineering Technology (ISSN: 0747-9964). – 2017. – Т. 6. – №. 2. – С. 304-316.

2. Vega E. A. A., Orozco A. L. S., Villalba L. J. G. Benchmarking of Pentesting Tools // World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering. – 2017. – Т. 11. – №. 5. – С. 590-593.

3. Andreatos A. S. Designing educational scenarios to teach network security // Global Engineering Education Conference (EDUCON), 2017 IEEE. – IEEE, 2017. – С. 1606-1610.

Наукове видання

Міжнародний конкурс студентських наукових робіт

BLACK SEA SCIENCE 2018

Матеріали

Верстка – Н.М. Ковальчук

Формат 60х84/16. Гарнітура Times New Roman.
Умовно-друк. арк. 48,07. Тираж 300. Замовлення № 0518-105.

Видавництво і друкарня – Видавничий дім «Гельветика»
73034, м. Херсон, вул. Паровозна, 46-а, офіс 105
Телефон +38 (0552) 39 95 80
E-mail: mailbox@helvetica.com.ua
Свідоцтво суб'єкта видавничої справи
ДК № 4392 від 20.08.2012 р.