МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра «информационной безопасности»

ОТЧЕТ

по учебной практике

Тема: Безопасность JavaScript

Студентка гр. 1361 _____ Токарева У.В.

Руководитель _____ к.т.н., доц. Племянников А.К.

Санкт-Петербург
2023

ЗАДАНИЕ

НА ПРОИЗВОДСТВЕННУЮ ПРАКТИКУ

Студентка Токарева У.В.

Группа 1361

Тема практики: Безопасность JavaScript

Задание на практику:

1. Пройти основной курс «Безопасность JavaScript» и сдать сертификационный экзамен
2. Пройти дополнительный курс «ИБ офиса. Основы социальной инженерии», написать отзыв о курсе и сдать сертификационный экзамен

Сроки прохождения практики: 30.06.2023 – 13.07.2023

Дата сдачи отчета: 12.07.2023

Дата защиты отчета: 13.07.2023

Студентка _____ Токарева У.В.

Руководитель _____ Племянников А.К.

АННОТАЦИЯ

В рамках учебной практики, для получения навыка безопасной разработки на языке JavaScript, необходимо пройти курс на образовательной платформы “hacktory.ai”. Основные поставленные задачи направлены на приобретение знаний и отработку практических навыков по следующим темам: межсайтовый скриптинг, подделка межсайтовых запросов, уязвимости аутентификации, инъекции в шаблоны, уязвимости фреймворка ReactJS, загрязнение прототипа. Также необходимо пройти курс «Информационная безопасность офиса», в котором основное внимание было уделено социальной инженерии.

SUMMARY

As part of the training practice, in order to gain the skill of safe development in JavaScript, it is necessary to take a course on an educational platform “hacktory.ai ”. The main tasks are aimed at acquiring knowledge and practicing practical skills on the following topics: cross-site scripting, forgery of cross-site requests, authentication vulnerabilities, injection into templates, ReactJS framework vulnerabilities, prototype contamination. It is also necessary to take the course "Information security of the office", in which the main focus was on social engineering.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Цель практики - повышения уровня образованности путем приобретения исовершенствования следующих компетенций:

1) Навык корректировать уязвимости в веб-приложениях, созданных спомощью JavaScript, Html и CSS;

2) Навык тестирования веб-приложений на наличие уязвимостей;

3) Навык эксплуатации наиболее распространённых уязвимостей.

Достижение поставленной цели проходило при выполнении следующихзадач:

1) Ознакомление теории и проверки знаний на практике при выполнении лабораторных работ по теме «Полезная информация и описание инструменто»;

2) Ознакомление теории и проверки знаний на практике при выполнении лабораторных работ по теме «Межсайтовый скриптинг (Cookie)»;

3) Ознакомление теории и проверки знаний на практике при выполнении лабораторных работ по теме «Межсайтовый скриптинг (CSRF, CSP)»;

4) Ознакомление теории и проверки знаний на практике при выполнении лабораторных работ по теме «Подделка межсайтовых запросов(CSRF)»;

5) Ознакомление теории и проверки знаний на практике при выполнении лабораторных работ по теме «Уязвимости аутентификации (Authbypass)»;

6) Ознакомление теории и проверки знаний на практике при выполнении лабораторных работ по теме «Инъекции в шаблоны (SSTI)»;

7) Ознакомление теории и проверки знаний на практике при выполнении лабораторных работ по теме «Уязвимости фреймворка ReactJS»;

8) Ознакомление теории и проверки знаний на практике при выполнении лабораторных работ по теме «Загрязнение прототипа (Prototype Pollution)».

1. ПОЛЕЗНАЯ ИНФОРМАЦИЯ И ОПИСАНИЕ ИНСТРУМЕНТОВ

1.1. Содержательная постановка

Изучить раздел с информацией о среде выполнения лабораторных работ инструменты, необходимые для выполнения работ. Выполнить тест, состоящий из четырех вопросов и выполнить одну лабораторную работу на исследование лабораторного окружения.

1.2. Результаты обучения

Правильно выполненные задания: тест, 1ntr0

1.3. Выводы

В ходе выполнения задачи были приобретены следующие умения:

1) Умение выполнения лабораторных работ в виртуальных машинах;

2) Навык работы с виртуальной машиной;

3) Навык работы с программой BurpSuite.

2. МЕЖСАЙТОВЫЙ СКРИПТИНГ (XSS ИЛИ CROSS-SITE SCRIPTING)

2.1. Содержательная постановка

Межсайтовый скриптинг (Cross-Site Scripting, или XSS) – это атака типа внедрение JavaScript кода, возможная из-за небезопасной обработки пользовательского ввода. В ходе атаки злоумышленник может выполнить вредоносный JavaScript в браузере жертвы. Прочитать теорию и выполнить 4 лабораторных работы. Три лабораторных на атаку и одна работа на защиту. Данная уязвимость позволяет внедрять JavaScript код, который изначально не был предусмотрен функционалом веб-приложения, из-за небезопасной обработки пользовательского ввода.

2.2. Результаты обучения

Правильно выполненные задания: CookieStealer (Атака), CookieStealer (Защита), Chat (Атака), BANG! (Атака).

Все задания были выполнены.

2.3. Выводы

В ходе выполнения задачи были приобретены следующие навыки:

1) Прослушка входящих подключений определенного порта;
2) Внедрение вредоносного кода;
3) Устранение уязвимостей исходного кода;
4) Навык работы с командной строкой;
5) Создание вредоносных ссылок.

3. МЕЖСАЙТОВЫЙ СКРИПТИНГ (CSRF, CSP)

3.1. Содержательная постановка

Прочитать теорию и выполнить 3 лабораторных работы на атаку. С помощью уязвимости необходимо зайти в аккаунт администратора и найти флаг.

3.2. Результаты обучения

Правильно выполненные задания: BANG!BANG! (Атака), BANG!BANG!BANG! (Атака), BANG!BANG!BANG!BANG! (Атака).

Все задания были выполнены.

3.3. Выводы

В ходе выполнения задачи были приобретены следующие навыки:

1) Обход защиты CSRF – токеном;
2) Обход политики защиты контента (CSP);
3) Подмена пароля на страницы другого пользователя.

4. ПОДДЕЛКА МЕЖСАЙТОВЫХ ЗАПРОСОВ (CSRF)

4.1. Содержательная постановка

Cross Site Request Forgery, межсайтовая подделка запросов – это тип атаки на аутентифицированного пользователя, в ходе которой злоумышленник обманным путем заставляет пользователя отправить подделанный запрос веб- приложению. Если жертва заходит на сайт, созданный злоумышленником, от ее лица тайно отправляется запрос на другой сервер, осуществляющий некую вредоносную операцию.

В данном разделе необходимо прочитать теорию и выполнить 2 лабораторные работы, каждая из которых на атаку. Учащемуся нужно проэксплуатировать уязвимость CSRF и с помощью определенных манипуляций получить доступ к аккаунту администратора.

4.2. Результаты обучения

Правильно выполненные задания: Social Like (Атака), ChangeMe (Атака). Все задания были выполнены.

4.3. Выводы

В ходе выполнения задачи были приобретены следующие умения:

1) Внедрение на страницы сайта вредоносного JavaScript кода для генерации и отправки зловредных запросов.

5. УЯЗВИМОСТИ АУТЕНТИФИКАЦИИ (AUTHBYPASS)

5.1. Содержательная постановка

В данном разделе необходимо ознакомиться с теорией и выполнить 2 лабораторных работы, две на атаку.

5.2. Результаты обучения

Правильно выполненные задания: Just Web Task (Атака), Just Web Task 2 (Атака).

Все задания были выполнены.

5.3. Выводы

В ходе выполнения задания были приобретены следующие знания и навыки:

1) Понимание работы JWT токенов;
2) Навык подделки JWT токенов.

6. ИНЪЕКЦИИ В ШАБЛОНЫ (SSTI)

6.1. Содержательная постановка

SSTI (Server-Side Template Injection) – это уязвимость, возникающая в результате небезопасного внедрения пользовательских данных в серверные шаблоны.

В данном разделе необходимо ознакомиться с теорией и выполнить 2 лабораторных работы, две на атаку.

6.2. Результаты обучения

Правильно выполненные задания: Jadeite (Атака). Невыполненные задания: Nephrite (Атака).

6.3. Выводы

В ходе выполнения задания были приобретены следующие навыки:

1) Эксплуатация уязвимости в работе шаблонизатора Jade.

7. УЯЗВИМОСТИ ФРЕЙМВОРКА REACTJS

7.1. Содержательная постановка

В данном разделе необходимо ознакомиться с теорией, методами эксплуатации уязвимости и способами защиты. После чего выполнить 2 лабораторных работы, где каждая задача на атаку.

7.2. Результаты обучения

Правильно выполненные задания:

Атака: Dangerous.

Неправильно выполненые задания: Hosting Panel (Атака) (задача выполнена на половину).

7.3. Выводы

В ходе выполнения задания были приобретены следующие навыки:

1) Понимание работы функции dangerouslySetInnerHTML;

2) Эксплуатация уязвимостей функции dangerouslySetInnerHTML;

3) Эксплуатация уязвимости, связанной с открытой переадресацией (Open redirect);

4) Поиск секретной информации в исходном коде клиентского билда.

8. ЗАГРЯЗНЕНИЕ ПРОТОТИПА (PROTOTYPE POLLUTION)

8.1. Содержательная постановка

Загрязнение прототипа — это инъекционная атака. При эксплуатации злоумышленник может контролировать значения свойств объекта по умолчанию, это позволяет злоумышленнику изменять логику приложения.

В данном разделе необходимо ознакомиться с теорией и выполнить одно задание на атаку.

8.2. Результаты обучения

Невыполненные задания: Joogle (Атака).

8.3. Вывод

В ходе выполнения задания были приобретены следующие навыки:

1) Понимание устройства прототипов в языке программирования JavaScript.

ЗАКЛЮЧЕНИЕ

В ходе летней учебной практики мной были пройдены курсы «Безопасность JavaScript» и «Информационная безопасность офиса». Изучая теорию основного курса и выполняя задания мне удалость узнать, как с помощью уязвимостей, допущенных при создании ресурсов, можно совершать различные атаки JavaScript, а также попробовать применить полученные данные на практике. Более того, я узнала о способах поиска уязвимостей и средствах защиты от атак. Однако, в некоторых темах я не смогла полностью разобраться, так как основной курс оказался для меня достаточно сложным, поэтому курс «Безопасность JavaScript» выполнен мной на 78%.

Курс «Информационная безопасность офиса» являлся дополнительным и показался мне более простым, его процент выполнения составил 100%. В нем я узнала о такой сфере, как социальная инженерия, а также более детально познакомилась с классификацией атак. В число основных результатов поставленных ранее задач входят:

1. Ознакомление с образовательной платформой hacktory.ai и с методами работы в виртуальных машинах;
2. Получение навыков эксплуатации XSS атак для достижения поставленных задач;
3. Изучение исправления уязвимостей;
4. Знакомство с политикой защиты контента (CSP);
5. Обучение воспроизведению CSRF атак;
6. Изучение способов обхода авторизации;
7. Изучение эксплуатации уязвимостей шаблонизатора Jade(Pug);
8. Изучение наиболее распространённые уязвимости фреймворка JavaScript: ReactJS

После прохождения практики я планирую углубиться в изучение языка JS, а также более детально изучить ReactJS и способы работы с ним.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. https://ru.legacy.reactjs.org/docs/dom-elements.html
2. https://excess-xss.com/

ПРИЛОЖЕНИЕ А

СЕРТИФИКАТ О ПРОХОЖДЕНИИ ОСНОВНОГО КУРСА

Сертификат о прохождении основного курса представлен на рисунке 1.

Рисунок 1 – Сертификат о прохождении основного курса

ПРИЛОЖЕНИЕ Б
СЕРТИФИКАТ О ПРОХОЖДЕНИИ ДОПОЛНИТЕЛЬНОГО КУРСА И ОТЗЫВ О КУРСЕ

Сертификат о прохождении дополнительного курса представлен на рисунке 2.

Рисунок 2 - Сертификат о прохождении дополнительного курса.

Отзыв о курсе «Информационная безопасность офиса»

Результат и общее впечатление от курса

Курс «Информационная безопасность офиса» оказался для меня очень интересным. Во-первых, было затронуто много тем, но особенно мне понравился подробный, детальный разбор социальной инженерии, особенно задания, где можно было попробовать себя в роли человека на контрольно-пропускном пункте или задание, где нужно было искать различные предметы в помещении, которые могут быть полезны для социального инженера. На самом деле, очень здорово.

Во-вторых, мне очень понравилось, что все практические задания были, в если можно так сказать, немного игровом формате. Поиск различных

данных, вычисление поддельных сообщений от известных компаний давали возможность почувствовать себя настоящим «хакером» (еще мне кажется важным отметить, что задания второго курса тоже были построены по подобной системе, что мне тоже очень понравилось и оказалось крайне интересным для меня). В целом курс оказался для меня достаточно интересным и не сложным.

Надеюсь, полученные знания помогут мне никогда не попадаться на уловки мошенников и передав полученные знания своим близким, я и их смогу уберечь от различных атак.

Достоинства и недостатки курса

В качестве достоинств данного курса я могу выделить его «понятность» и разнообразность заданий. Также важно отметить большой объем теоретического материала, представленного в данном курсе. Более того, для меня было огромным плюсом иллюстрирование теории на примерах, а также применение ее на практике.

В качестве недостатков могу отметить лишь то, что виртуальная машина периодически сильно зависала, а в тексте с теорией мной была замечена опечатка. Также грустно, что в практических заданиях и тестах нельзя посмотреть, где именно и что оказалось неправильным.

Рекомендации по улучшению курса

Хотелось бы, чтобы была возможность узнать, в чем была допущена та или иная ошибка, мне кажется, это бы сильно помогло во время обучения. Еще было бы здорово добавить видео-уроки, например мне, как и многим людям, гораздо проще воспринимать информацию на слух.