|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ | | | | | | | | | | | | | | | | | | | | |
| Федеральное государственное автономное образовательное  учреждение высшего образования | | | | | | | | | | | | | | | | | | | | |
| **Дальневосточный федеральный университет** | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| **ШКОЛА ЕСТЕСТВЕННЫХ НАУК** | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| **Кафедра информационной безопасности** | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| **О Т Ч Е Т** | | | | | | | | | | | | | | | | | | | | |
| о прохождении учебной практики (учебно-лабораторного практикума) | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | |  |  | Выполнил студент  гр. С8117-10.05.01ммзи | | | | | | | | |
|  |  |  | | | | | | Смирнова А. А. | | |
|  | | | | | | | | | |  |  | (подпись) | | | | | |  | | |
|  | | | | | | | | | | | | | | | | | | | | |
| Отчет защищен с оценкой | | | | | | | | | |  |  | Руководитель практики | | | | | | |  | |
|  | | | | | | | | | |  |  | Старший преподаватель кафедры информационной безопасности ШЕН | | | | | | | | |
|  | | | |  | С.С. Зотов | | | | |  |  |  | | | | |  | С.С. Зотов | | |
| (подпись) | | | |  | (И.О. Фамилия) | | | | |  |  | (подпись) | | | | |  | (И.О. Фамилия) | | |
| « | 26 | » | июня | | | | | | 2021 г. |  |  |  | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| Регистрационный № | | | | | | | |  | |  |  | Практика пройдена в срок | | | | | | | | |
| « | 26 | » | июня | | | | | | 2021 г. |  |  | с | « | 22 | » | февраля | | | | 2021 г. |
|  | | | | | | | | | |  |  | по | « | 26 | » | июня | | | | 2021 г. |
|  | | | | | |  | Е.В. Третьяк | | |  |  | на предприятии | | | | | | | | |
| (подпись) | | | | | |  | (И.О. Фамилия) | | |  |  |
|  | | | | | | | | | |  |  | Кафедра информационной | | | | | | | | |
|  | | | | | | | | | |  |  | безопасности ШЕН ДВФУ | | | | | | | | |
|  | | | | | | | | | |  |  |  | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| г. Владивосток | | | | | | | | | | | | | | | | | | | | |
| 2021 | | | | | | | | | | | | | | | | | | | | |

**Содержание**

Задание на практику 3

Введение 4

1 Описание веб-приложений 5

2 Реализация A1, А2, А3, A6, A7 (клиентская часть) 9

Заключение 16

Список использованных источников 17

**Задание на практику**

- Проведение исследования в области защиты от взлома веб-приложений.

- Написание отчета по практике о проделанной работе.

**Введение**

Учебная практика (учебно-лабораторный практикум) проходил на кафедре информационной безопасности ШЕН ДВФУ в период с 22 февраля 2021 года по 26 июня 2021 года.

Целью прохождения практики является приобретение практических и теоретических навыков по специальности, а также навыков оформления проведенного исследования в отчетной форме.

Задачи практики:

1. Исследовать нормативную базу по информационной и компьютерной безопасности в области уязвимостей веб-приложений.
2. Реализовать 9 веб-приложений c уязвимостям из OWASP Top 10.
3. На основе полученных знаний написать отчет по практике о проделанной работе.

# **1 Описание веб-приложений**

**1.1 A1. Injections**

По этой уязвимости реализовывалось два веб-приложения: первое веб-приложение содержит NOSQL уязвимость, второе – SQL уязвимость.

В обоих случаях реализовывалась форма отправки данных на клиенте с именем пользователя и паролем и соответствующая логика, допускающая соответствующую инъекцию, на сервере.

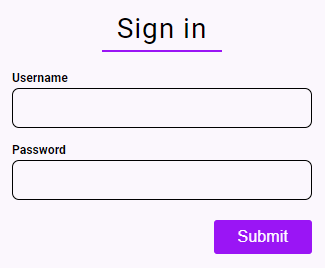


Рисунок 1 – Форма отправки данных

При успешном проведении атаки пользователю высвечивается флаг.

**1.2 A2. Broken auth**

Данный случай показывает, как плохие требования к паролю могут привести к соответствующим последствиям. Клиент состоит из двух частей: из формы отправки данных (форма входа) и формы регистрации.

В форме регистрации есть требование к паролю, которое подразумевает, что пароль должен состоять только из 6 цифр, не больше и не меньше.

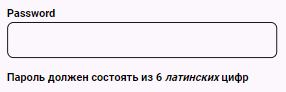


Рисунок 2

Данный случай легко решается перебором всех возможных комбинаций пароля.

**1.3 A3. Cross Site Scripting (XSS)**

Этот случай нацелен на проведение XSS-атаки [1]. На клиенте расположена форма отзывов к продукту, где поле комментария уязвимо к XSS-атаке. Пользователь отправляет данные с JavaScript(JS)-кодом, на сервере этот код никак не обрабатывается, и всё сохраняется в базу данных. Если любой пользователь зайдёт на страничку с этими отзывами, он получит отзыв с JS кодом, который запустится на его клиенте.

**1.4 A4. Insecure dor**

Клиент веб приложение состоит из трёх частей: форма входа, отображение данных пользователя и страница 404.

Случай заключается в том, что пользователь по URL может просмотреть данные всех людей, которые пользуются данным приложением, если же такого пользователя не существует, то показывается страница 404.

**1.5 A5. Miscofiguration**

Пользователю необходимо суметь авторизироваться в системе, проанализировав какая серьёзная уязвимость скрывается на сервере.

Клиент состоит из двух частей: поле поиска файлов и формы авторизации.

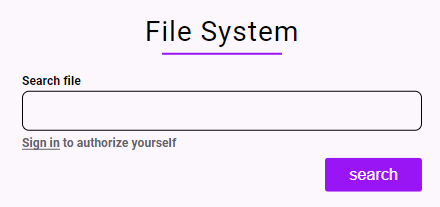


Рисунок 3 – Поисковая система файлов

**1.6 A6. Sensetive data exposure**

Целиком и полностью весь случай состоит из двух клиентов и сервера. Случай подразумевает клиент пользователя, которому необходимо войти в систему и клиент жертвы.

Клиент жертвы работает следующим образом: каждые 5 секунд делается POST запрос на авторизацию с валидными данными, уязвимость заключается в том, что данные передаются по HyperText Transfer Protocol (HTTP).

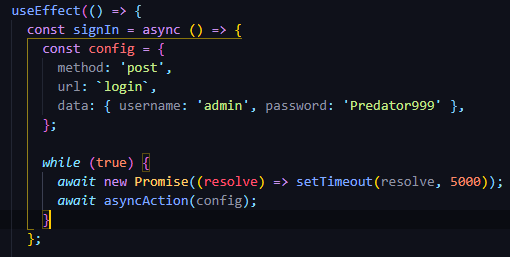


Рисунок 4 – Код автоматической авторизации

Пользователю необходимо прослушать траффик внутри сети Wi-Fi и авторизироваться, узнав данные жертвы.

**1.7 A7. Access controls**

Веб приложение показывает список пользователей, зарегистрированных в системе веб приложения с дезактивированной кнопкой удаления пользователя. Пользователю необходимо сделать запрос на удаление пользователя из списка. Уязвимость заключается в том, что на сервере не проверяются права пользователя, удаляющего пользователя из базы данных.

**1.8 A8. Cross-Site Request Forgery (CSRF)**

Данное приложение направленно на проведение CSRF-атаки [2].

**2 Реализация A1, А2, А3, А4, A6, A7 (клиентская часть)**

Моей задачей было реализовать клиентскую часть веб-приложений A1(NOSQL), А2, А3, A6, A7

**2.1 A1**

В данной уязвимости пользователь заходит на страницу авторизации, где находится форма с вводом логина и пароля. Инъекция находится в поле для ввода пароля.

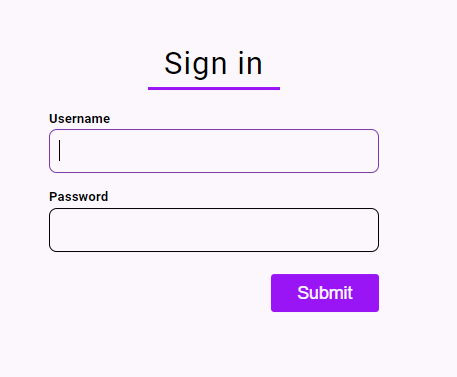


Рисунок 5– Форма входа

В случае успешно проведенной атаки пользователю высвечивается флаг, иначе появляется уведомление о неверно введённом пароле

**2.2 A2**

На главной странице пользователь увидит форму входа и кнопку регистрации.

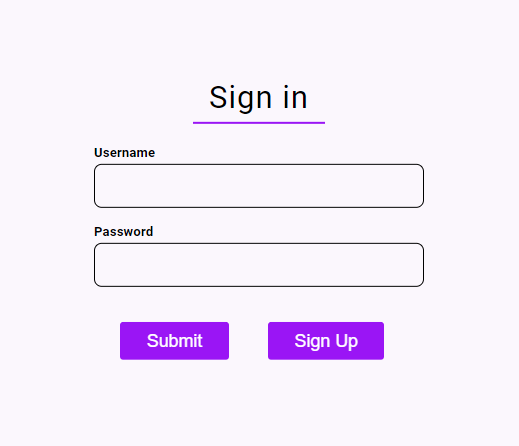


Рисунок 6– Форма входа

При переходе на страницу регистрации пользователь найдет требование к паролю, которое поможет ему в переборе паролей.

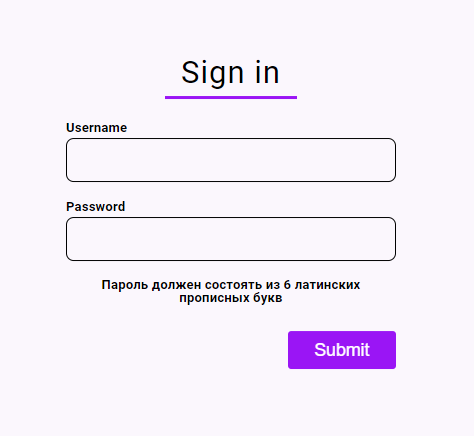


Рисунок 7– Форма регистрации

**2.3 A3**

На главной странице расположена форма отзывов к продукту, где поле комментария уязвимо к XSS-атаке. Пользователь, зайдя на страничку с этими отзывами, получит отзыв с JS кодом, который запустится на его клиенте.

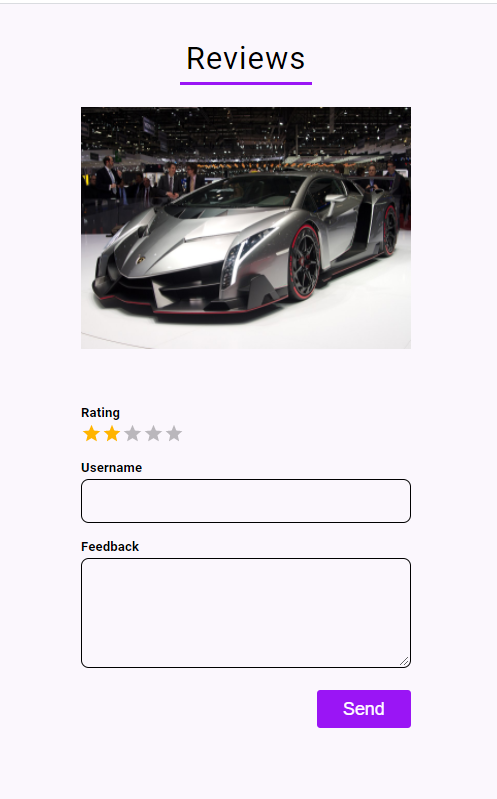


Рисунок 8– Форма отзыва

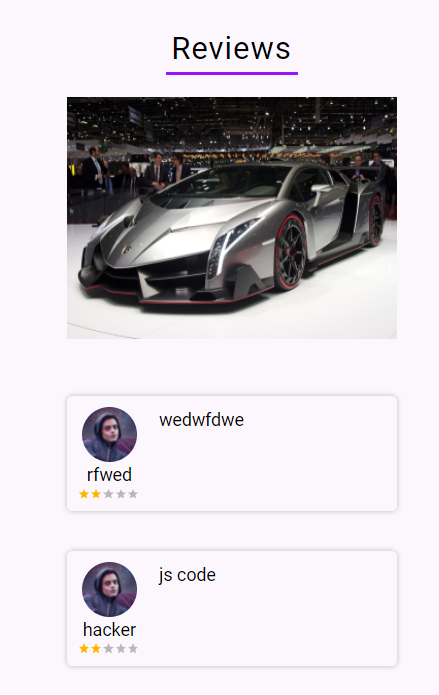


Рисунок 8– Отзывы пользователей, с введённым js кодом

**2.4 A4**

На главной странице увидит форму входа.

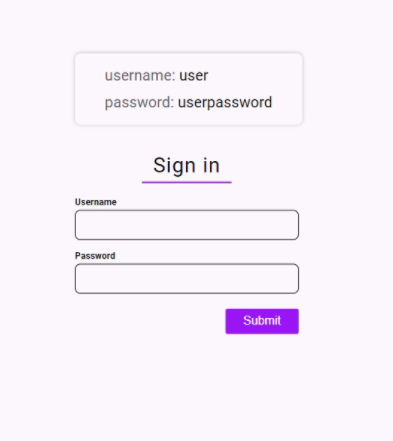


Рисунок 9– форма входа с данными для входа

При вводе URL страницы пользователя отобразятся данные этого пользователя.

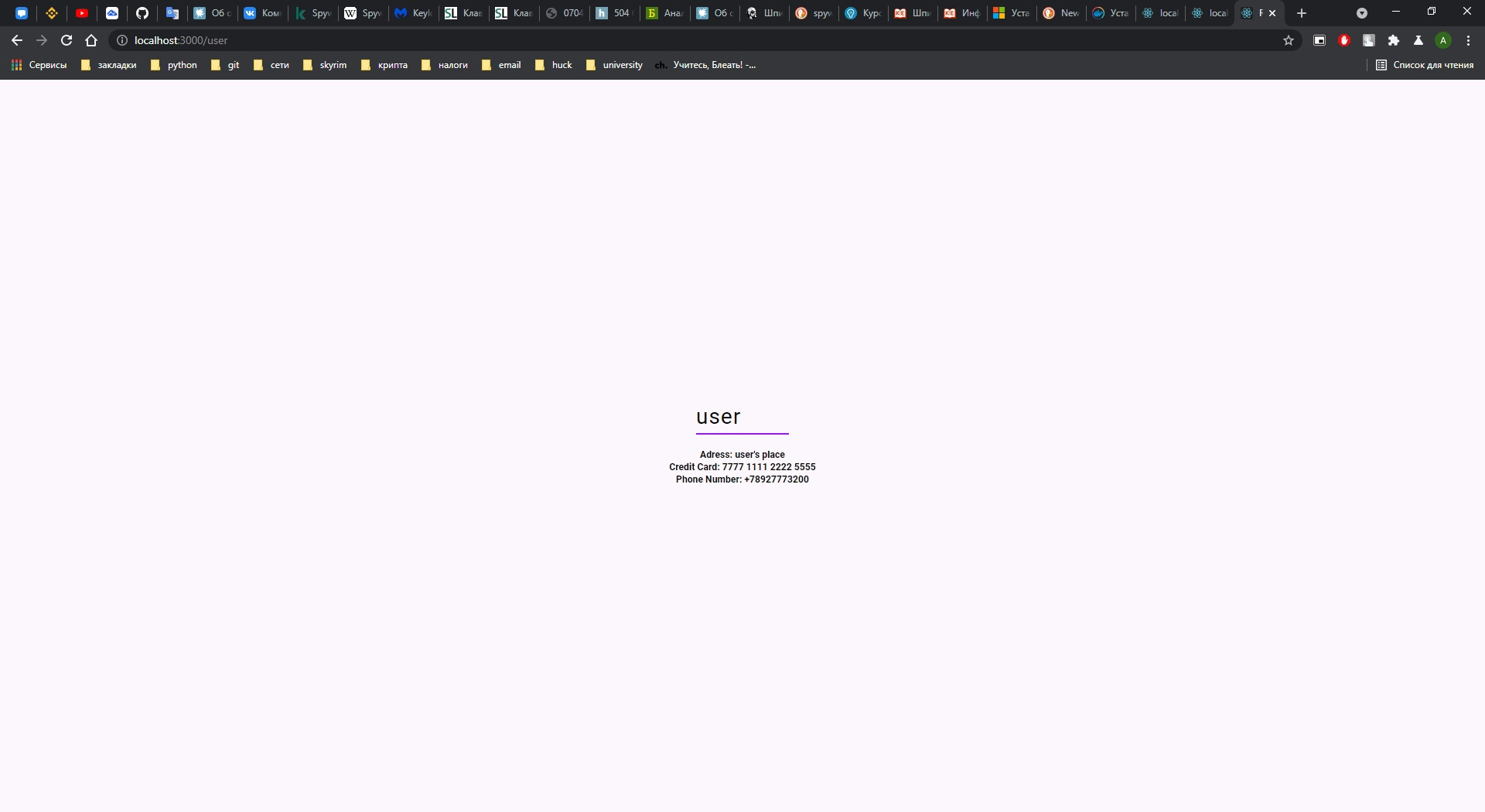


Рисунок 10– Страница с данными пользователя

В случае, если такого пользователя не существует, отобразится страница 404.

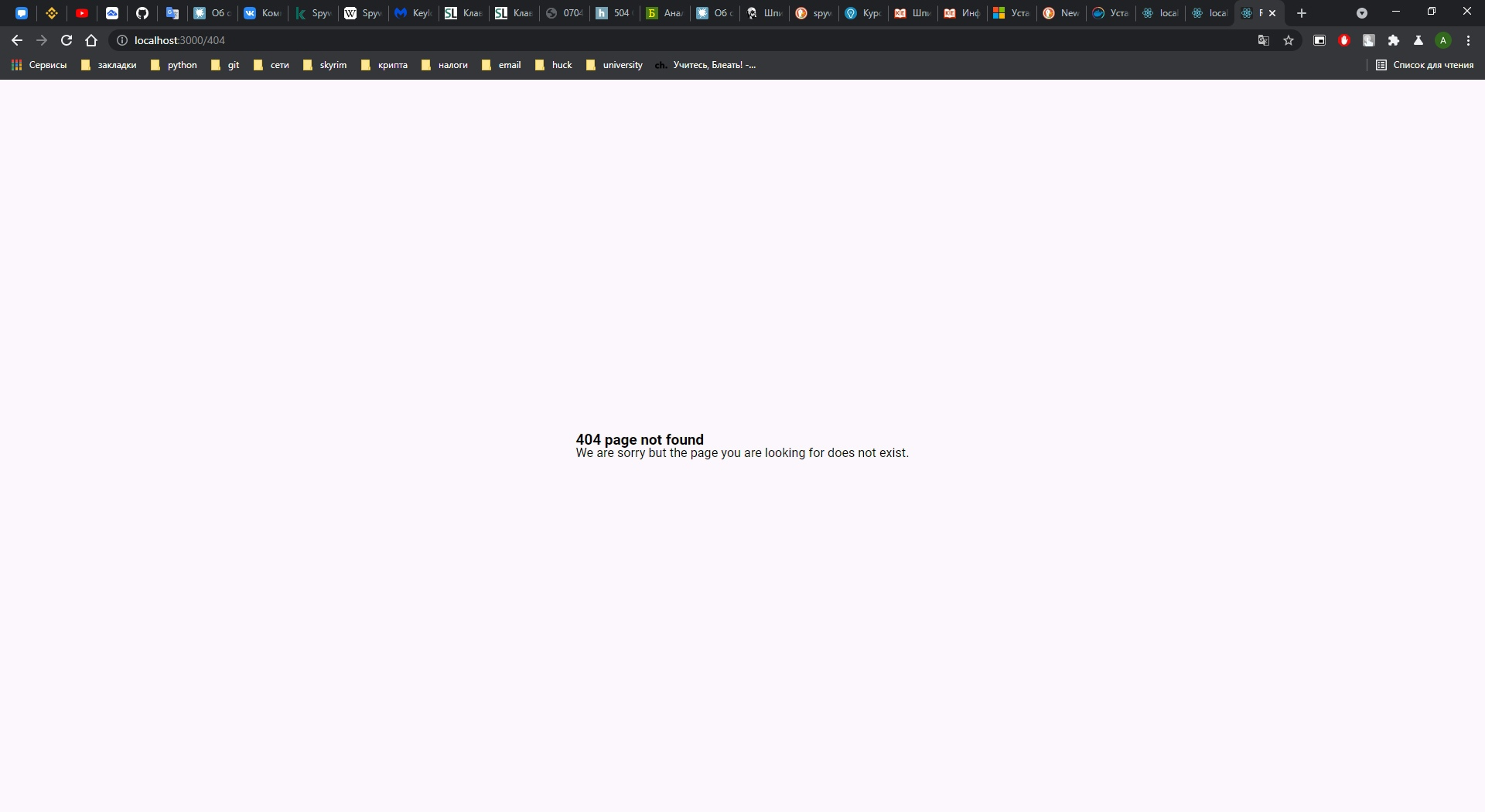


Рисунок 11– Страница 404

**2.4 A6**

На обоих клиентах находится форма входа

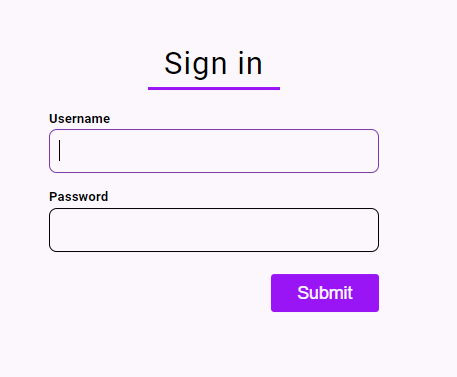


Рисунок 12– Форма входа

Каждые 5 секунд делается POST запрос с клиента жертвы на авторизацию с валидными данными.

Пользователь слушает траффик внутри сети Wi-Fi и, узнав данные жертвы, авторизируется.

**A7**

У нас есть список пользователей с деактивированной кнопкой удаления.

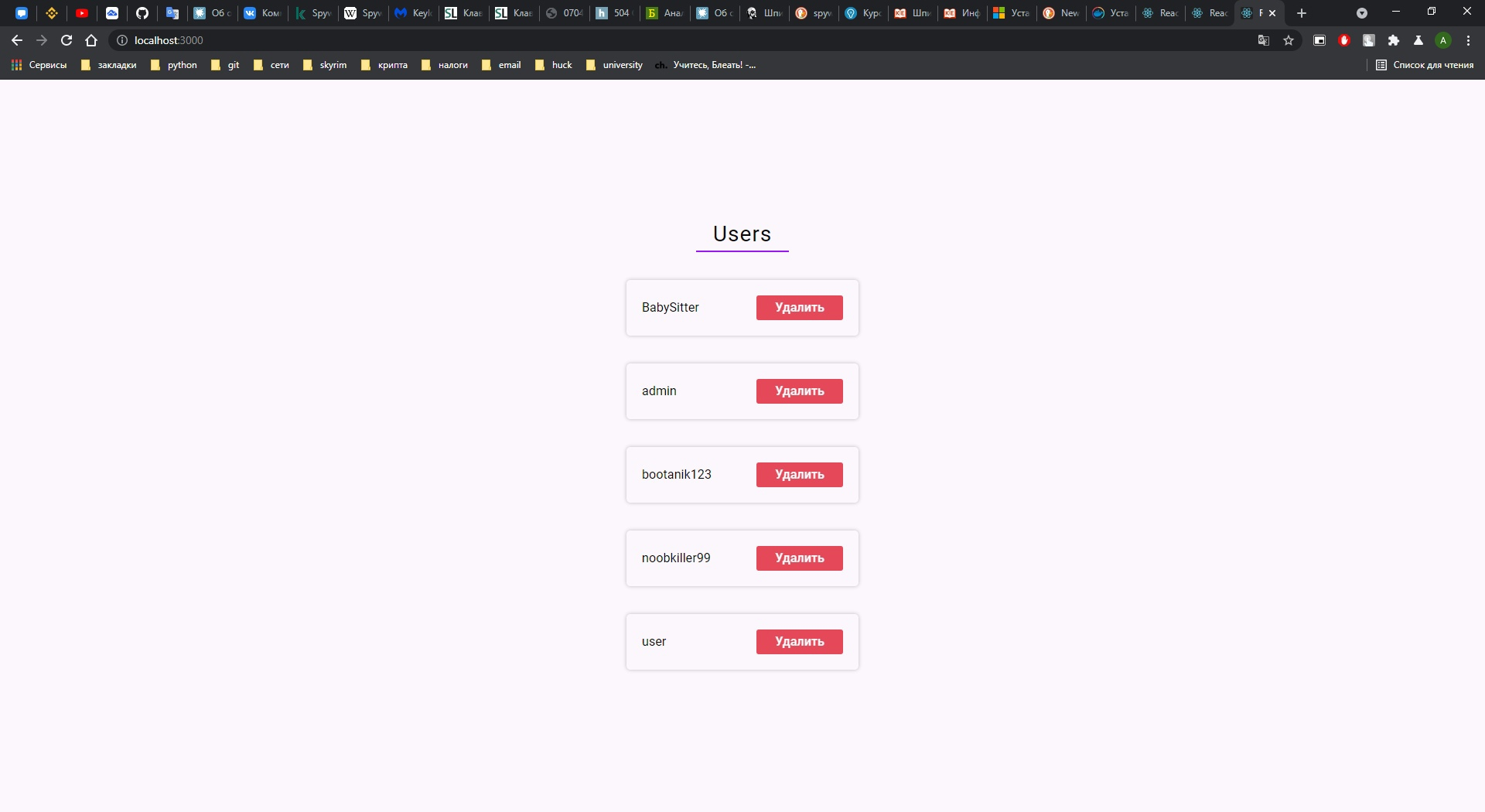


Рисунок 13– Страница со списком пользователей

Пользователю необходимо сделать запрос на удаление пользователя из списка.

**2.4 Технологии**

В качестве технологий при создании A1(API), A5, A5 использовались следующие технологии и языки программирования:

На стороне клиента использовался такой язык программирования как JavaScript, а также следующие технологии:

* react;
* axios;
* formik;
* node-sass;

**Заключение**

Для достижения данной цели, в процессе прохождения учебной практики (учебно-лабораторного практикума) исследовал нормативную базу по информационной и компьютерной безопасности в области уязвимостей веб-приложений, реализовал веб-приложения со следующими уязвимостями: A1, A2, A3, А4, А6, А7.

Также были изучены требования к написанию отчета по практике. В результате прохождения практики был составлен отчет по практике, соответствующий предъявленным требованиям.

В ходе прохождения практики все задачи были выполнены, а цель достигнута.

**Список используемых источников**

1. XSS-атака [Электронный ресурс]. – Режим доступа: https://owasp.org/www-community/attacks/xss/
2. CSRF-атака [Электронный ресурс]. – Режим доступа: <https://owasp.org/www-community/attacks/csrf>