

Лабораторная работа – уязвимости аутентификации

В данной лабораторной работе вам предлагается попробовать свои силы в решении задач, схожих с реальными случаями проведения тестирования на проникновение.

Ваша задача – обнаружение и эксплуатация уязвимостей аутентификации.

Вам необходимо сделать **любое количество** из предложенных заданий для получения балла.

ВНИМАНИЕ: максимальный балл за эту работу — **12** (если вы выполните заданий больше, чем требуется, максимальная оценка все равно будет 12). Вы можете выбрать любые из предложенных заданий для получения максимальной оценки. Максимальный балл за каждое задание приведен рядом с заданием.

Часть 1 – Необходимые инструменты

Обязательные требования:

- Для выполнения **всех** заданий вам потребуется инструмент Burp Suite Community Edition — это интегрированная платформа для тестирования безопасности веб-приложений. Скачать Burp Suite Community Edition можно по ссылке:

<https://portswigger.net/burp/communitydownload>

Для загрузки потребуется ввести вашу почту.

- Для выполнения Заданий вам потребуется зарегистрироваться на сайте PortSwigger.

Часть 2 - Требования к сдаче заданий и к оформлению отчета

Обязательные требования:

- В решении требуется описать способ атаки или обхода защитных механизмов и приложить доказательства выполнения (скриншоты/логи).
- Все шаги выполнения атаки должны быть подтверждены соответствующими скриншотами и текстовыми комментариями к ним.
- На **каждом** скриншоте должна быть информация о выполнившем работу студенте в формате **Фамилия_Имя_Группа** (Пример: Иванов_Иван_БИБ221).
- На **каждом** скриншоте должна быть видна панель задач с **датой и временем** выполнения данного скриншота.
- Из отчета должна быть понятна последовательность ваших рассуждений при проведении атак.
- Используйте шаблон отчета, который прикреплен к заданию.

Часть 3 – Ссылки на задания

- Задание 1 – PortSwigger — перечисление (определение) имён пользователей и подбор пароля методом грубой силы (brute-force). (уровень - Apprentice) (2,5 балла)
В приложении есть аккаунт с предсказуемым логином и паролем.
Задача студента: найти валидный username, перебрать пароль и получить доступ к странице аккаунта.

<https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-different-responses>

- Задание 2 – PortSwigge. Перечисление (определение) имён пользователей по времени отклика сервера (уровень – Practitioner, средняя сложность) (3,5 балла)

Лабораторная работа демонстрирует уязвимость, при которой злоумышленник может определить корректные учётные имена по различиям во времени отклика сервера. Задача студента: определить существующий username с помощью анализа времени ответа сервера, затем перебором (brute-force) подобрать пароль выбранного пользователя и получить доступ к его странице аккаунта.

<https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-response-timing>

- Задание 3 – PortSwigge. Обход защиты от brute-force по ip (уровень - Practitioner, средняя сложность) (3,5 балла)

Лабораторная работа демонстрирует уязвимость, обусловленную логическим дефектом в механизме защиты от перебора паролей по IP.

Задача студента: подобрать (brute-force) пароль жертвы, выполнить вход под её учётной записью и получить доступ к странице аккаунта.

<https://portswigger.net/web-security/authentication/password-based/lab-broken-bruteforce-protection-ip-block>

- Задание 4 – PortSwigge. Уязвимость в логике функции «сброс пароля» (уровень - Apprentice) (2,5 балла)

Демонстрация уязвимости в реализации механизма сброса пароля. Из-за логического дефекта злоумышленник может изменить пароль другого пользователя без надлежащей проверки прав или токенов.

Задача студента: Восстановить (сбросить) пароль пользователя Carlos, затем выполнить вход под его учётной записью и получить доступ к странице «Мой аккаунт».

<https://portswigger.net/web-security/authentication/other-mechanisms/lab-password-reset-broken-logic>

- Задание 5 – PortSwigge. Подбор куки «остаться в системе» (уровень – Practitioner, средняя сложность) (3,5 балла)

Лабораторная работа демонстрирует уязвимость механизма «оставаться в системе»: cookie, обеспечивающая сохранение авторизации после закрытия браузера, подвержена подбору методом грубой силы.

Задача студента: подобрать (brute-force) cookie пользователя Carlos и получить доступ к его странице «Мой аккаунт».

<https://portswigger.net/web-security/authentication/other-mechanisms/lab-brute-forcing-a-stay-logged-in-cookie>

- Задание 5 – PortSwigger. Простой обход двухфакторной аутентификации (уровень - Apprentice) (2,5 балла)

Лабораторная работа демонстрирует уязвимость в механизме двухфакторной аутентификации: при наличии корректного логина и пароля обход 2FA возможен без доступа к коду подтверждения.

Задача студента — использовать обнаруженный вектор обхода, получить доступ к учётной записи Carlos и открыть страницу «Мой аккаунт».

<https://portswigger.net/web-security/authentication/multi-factor/lab-2fa-simple-bypass>

- Задание 6 — PortSwigger. Двухфакторная аутентификация с логической уязвимостью (уровень – Practitioner, средняя сложность) (3,5 балла)

Лабораторная работа демонстрирует логическую уязвимость в реализации двухфакторной аутентификации, позволяющую обойти её при определённой последовательности действий.

Задача студента: требуется получить доступ к странице «Мой аккаунт» пользователя carlos. Доступны учётные данные wiener:peter; также предоставлен доступ к почтовому серверу для получения кода 2FA.

<https://portswigger.net/web-security/authentication/multi-factor/lab-2fa-broken-logic>

- Задание 7 - PortSwigger (уровень – Practitioner, средняя сложность) (3,5 балла)

Лабораторная работа демонстрирует уязвимость в механизме смены пароля, из-за которой возможен подбор пароля жертвы посредством последовательных попыток через форму восстановления/смены пароля.

Задача студента: используя предоставленный список кандидатов на пароль, перебором определить пароль пользователя carlos и получить доступ к его странице «Мой аккаунт». В решении следует зафиксировать последовательность действий и доказательства успешного доступа (логи/скриншоты)

<https://portswigger.net/web-security/authentication/other-mechanisms/lab-password-brute-force-via-password-change>

Часть 4 – Чеклист для самопроверки содержания отчета:

Обязательно для всех заданий:

- Для оформления отчета, просьба использовать шаблон оформления, прикрепленный к заданию
- Наличие скриншотов, соответствующих шагам выполнения задания, с информацией о студенте и временными отметками.

Техническое содержание:

- Ясное и краткое описание уязвимости: что именно нарушено (например, возможность перечисления пользователей, обход 2FA, подбор stay-logged-in cookie, логический дефект защиты от bruteforce и т. д.)
- Указаны исходные данные: адрес лаборатории, учётные данные (если даны), используемые wordlists, версии инструментов.
- Подробное воспроизводимое пошаговое описание эксплуатации (шаги должны быть достаточно конкретны, чтобы третье лицо могло воспроизвести результат):
 - какие HTTP-запросы выполнялись (метод, путь, ключевые заголовки и тело);
 - какие параметры варьировались и с какими значениями;
 - какие инструменты/скрипты и с какими опциями применялись.

Доказательства и воспроизводимость

- Снимки экрана/логи для ключевых шагов:
 - исходная страница входа / форма;
 - примеры запросов/ответов (включая заголовки и тело ответа);
 - отличия ответов/таймингов (для задач с перечислением по разнице в ответах);
 - успешный вход / доступ к странице «My account»;
 - Наличие скриншота с отметкой Lab Solved с главной страницы каждого задания (ссылки на задания в данной методичке – это ссылки на главные страницы заданий).

Анализ уязвимости и риск

Попробуйте оценить потенциальный риск данной уязвимости.

- Классификация нарушенного механизма: указать, что нарушено — **автентификация** (Authentication), контроль доступа или обе модели; при необходимости — вертикальный/горизонтальный контроль (если релевантно).
- Оценка потенциального ущерба: какие данные/действия доступны злоумышленнику при успешной эксплуатации (чтение личных данных, изменение настроек, транзакции и т.п.).
- Оценка вероятности эксплуатации (низкая/средняя/высокая) и обоснование (наличие публичных wordlists, простота автоматизации, необходимость доступа к почте и т.д.).