Лабораторная работа – IDOR

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 уязвимости типа IDOR категории Broken Access Control.

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

ВНИМАНИЕ: максимальный балл за эту работу — 10 (если вы выполните заданий больше, чем требуется, максимальная оценка все равно будет 10). 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:

- 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 — IDOR (по названию) (уровень - Apprentice) (2,5 балла)
  https://portswigger.net/web-security/access-control/lab-insecure-direct-object-references
- Задание 2 – PortSwigger. Модификация user id через параметр запроса (уровень - Apprentice) (2,5 балла)
  https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter-with-unpredictable-user-ids

- Задание 3 – PortSwigger. Простой пример file path traversal (уровень - Apprentice) (2,5 балла)
  https://portswigger.net/web-security/file-path-traversal/lab-simple
- Задание 4 – PortSwigger. File path traversal с обходом простой защиты (уровень – Practitioner, средняя сложность) (3 балла)
  https://portswigger.net/web-security/file-path-traversal/lab-sequences-stripped-non-recursively
- Задание 5 – PortSwigger. Обход защиты при помощи null byte (уровень – Practitioner, средняя сложность) (3 балла)
  https://portswigger.net/web-security/file-path-traversal/lab-validate-file-extension-null-byte-bypass
- Задание 5 – PortSwigger. Повышение привилегий (уровень - Apprentice) (2,5 балла)
  https://portswigger.net/web-security/access-control/lab-user-role-can-be-modified-in-user-profile
- Задание 6 — PortSwigger. Утечка данных через управление id (уровень – Apprentice, средняя сложность) (2,5 балла)
  https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter-with-data-leakage-in-redirect
- Задание 7 - PortSwigger (уровень – Practitioner, средняя сложность) (3 балла)
  https://portswigger.net/web-security/access-control/lab-url-based-access-control-can-be-circumvented

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.
- К каждому выполненному заданию необходимо указать, механизм какого типа контроля доступа (вертикальный или горизонтальный) был нарушен. Указать так же, путем эксплуатирования какого типа IDOR (Directory Traversal, Body Manipulation, URL Tampering, Cookie ID Manipulation) была выполнена атака.

Пример: «Как можно видеть из Рисунка 3, мы успешно зашли на страничку под пользователем admin, тем самым повысив свои привилегии, нарушив механизм вертикального контроля доступа путем эксплуатации IDOR типа URL-Tampering».

- Наличие скриншота с отметкой Lab Solved с главной страницы каждого задания (ссылки на задания в данной методичке – это ссылки на главные страницы заданий).