Домашнее задание

Дисциплина: Программирование на Python
Тема: Взаимодействие в WWW: взаимодействие с сервисами

Форма проверки: самопроверка
Имя преподавателя: Дарья Погудина
Время выполнения: 180 минут

Цель задания:
Научиться использовать инструмент Scapy для анализа сетевого трафика и эксплуатации уязвимостей cross-site scripting (XSS) на учебном сайте Google Gruyere.

Инструменты для выполнения ДЗ:
Scapy, Google Gruyere, браузерные инструменты разработчика для анализа веб-страниц

Правила приёма работы:

1. Выполните все пункты задания.
2. Разместите готовый код в репозитории на GitHub.
3. В личном кабинете, в поле ответа к домашней работе, вставьте ссылку на GitHub с выполненным заданием. Отправьте работу на проверку.
4. Важно: убедитесь, что по ссылке есть доступ.

Критерии оценки:

Задание считается выполненным:

- прикреплён файл с выполненным заданием.

Задание считается невыполненным:

- файл с заданием не прикреплён или пуст.

Дедлайн: 7 дней после соответствующего вебинара.

Прежде чем выполнять задание:

1. Посмотрите запись видеолекции и вебинара по теме «Взаимодействие Python с WWW».
2. Установите Scapy для работы в Python. Для этого можно использовать команду **pip install scapy**.

Задание

Этап 1. Изучение Scapy

- Изучите основы работы с Scapy по документации.
- Настройте Scapy для перехвата HTTP-трафика, используйте скрипт scapy для отправки HTTP-запросов.

Этап 2. Анализ трафика

- Ознакомьтесь с инструментом Google Gruyere и запустите его.
- Запустите Scapy и начните собирать трафик, взаимодействуя с сайтом Google Gruyere.
- Проанализируйте полученные данные, обращая внимание на запросы и ответы HTTP.

Этап 3. Эксплуатация XSS

- Осуществите рекон-анализ сайта Google Gruyere для поиска потенциальных точек входа XSS.
- Попытайтесь эксплуатировать уязвимости XSS, используя обнаруженные точки.

  Примеры XSS-атак:

  <script>alert('XSS')</script>

  <img src="nonexistent.jpg" onerror="alert('XSS')">

- Запишите все свои шаги эксплуатации уязвимостей и полученные результаты, сделайте скриншоты.

Этап 4. Анализ результатов

- Используя Scapy, проанализируйте, как XSS-атака отображается в сетевом трафике (проанализируйте ответ на HTTP-запрос).
- Опишите, какие изменения в трафике произошли во время XSS-атаки.

Этап 5. Отчёт

Подготовьте отчёт: опишите процесс эксплуатации XSS, анализ трафика, выводы и рекомендации по устранению найденных уязвимостей.

Чек-лист самопроверки

Критерии выполнения задания
Настроен Scapy для перехвата HTTP-трафика
Запущен Scapy и выполнен сбор трафика во время взаимодействия с сайтом Google Gruyere
Проанализированы полученные запросы и ответы HTTP
Проведён рекон-анализ сайта Google Gruyere для поиска потенциальных точек входа XSS
Проведена эксплуатация уязвимости XSS
Найдены следы XSS-атаки в сетевом трафике
Описаны изменения в трафике, которые произошли во время XSS-атаки
Подготовлен отчёт: • описаны действия, выполненные при эксплуатации уязвимости XSS и представлены скриншоты результатов; • описан анализ трафика; • представлены скриншоты следов XSS-атаки в сетевом трафике; • представлены выводы и рекомендации по устранению найденных уязвимостей
В личном кабинете прикреплён файл с отчётом
Название файла содержит фамилию и имя студента, номер домашнего задания