Сканер XSS

Примеры сканеров XSS

Online Vulnerability Scanner

Acunetix XSS Scanner – платный продукт

Модуль Scanner в Burp Suite версии PRO

Преимещуетсва – находит все уязвимости OWASP Top 10

XSSer – небольшая утилита для поиска и эксплуатации XSS

Может находить ссылки на сайте

Может использовать кастомные векторы

Может использовать дорки (например google) для поиска уязвимостей и т.д.

Можно работать через Proxy

Недостаток – ложные срабатывания

Данный сканер используется для первичной проверки на наличие XSS

XSSStrike

Встроенный модуль Fuzzer для подбора payload, использует фаззинг параметров в своей работе

Встроенный модуль Strike для проведения bruteforce фтфк с использованием payload

Недостаток не все виды WAF обнаруживаются

XSSHanter – для слепой XSS

Подбор начального вектора XSS без использования сканера

Проблема подбора векторов

Может присутствовать защита, которая не позволит выполниться вектору

Векторов для эксплуатации XSS много

XSS не обязательно присутствует в поле ввода, может присутствовать в параметре запроса

В Burp Suite существует ряд плагинов, которые позволяют упростить процесс подбора векторов

Burp Intruder

Нужно выбрать параметр для инъекции

В Intruder нужно выбрать те параметры запроса, в которые будет проводиться инъекция. Делается это на вкладке Positions.

Burp Intruder очень полезен при тестировании системы защиты от XSS, особенно для тестирования правил CSP и WAF (web application firewall)

Основные вектора така XSS

Векторы с кражей Cookie

1. Вначале создается обработчик
2. Далее злоумышленник создает файл, в котором будут храниться перехваченные данные. Для файла обязательно установить права на запись в файл
3. Далее нужно составить вектор таким образом, чтобы он пересылал в переменную «с» куки жертвы. Подойдет такой
4. После этого остается выполнить атаку и ждать результата

Вектор атак XSS с кейлоггером

Чтобы реализовать атаку с использованием кейлоггера, его вначале нужно разработать. Кейлорег буду стостья из серверной части (обработчика данных, на PHP) и клиентской части (перехватчика данных, на JS)

Вектор атаки с фишинговой формой

Подкинуть поддельную форму логина и пароля

Атака CSRF

Межсайтовая подделка запросов