

Индивидуальный проект

4 Этап

Прокопьева М. Е.

Российский университет дружбы народов, Москва, Россия

Информация

- Прокопьева Марина Евгеньвна
- студент
- Российский университет дружбы народов

Вводная часть

Цель работы

Научиться тестированию веб-приложений с помощью сканера nikto

Задание

Использование nikto.

Теоретическое введение

nikto — базовый сканер безопасности веб-сервера. Он сканирует и обнаруживает уязвимости в веб-приложениях, обычно вызванные неправильной конфигурацией на самом сервере, файлами, установленными по умолчанию, и небезопасными файлами, а также устаревшими серверными приложениями. Поскольку nikto построен исключительно на LibWhisker2, он сразу после установки поддерживает кросс-платформенное развертывание, SSL (криптографический протокол, который подразумевает более безопасную связь), методы аутентификации хоста (NTLM/Basic), прокси и несколько методов уклонения от идентификаторов. Он также поддерживает перечисление поддоменов, проверку безопасности приложений (XSS, SQL-инъекции и т. д.) и способен с помощью атаки паролей на основе словаря угадывать учетные данные авторизации.

Для запуска сканера nikto введите в командную строку терминала команду: #
nikto

По умолчанию, как ранее было показано в других приложениях, при обычном запуске команды отображаются различные доступные параметры. Для сканирования цели введите `nikto -h -p` , где — домен или IP-адрес целевого сайта, а — порт, на котором запущен сервис

Сканер nikto позволяет идентифицировать уязвимости веб-приложений, такие как раскрытие информации, инъекция (XSS/Script/HTML), удаленный поиск файлов (на уровне сервера), выполнение команд и идентификация программного обеспечения. В дополнение к показанному ранее основному сканированию nikto позволяет испытателю на проникновение настроить сканирование конкретной цели. Рассмотрим параметры, которые следует использовать при сканировании.

Указав переключатель командной строки -T с отдельными номерами тестов, можно
Используя при тестировании параметр -t, вы можете установить значение тайм-аута для каждого ответа.

Параметр -D V управляет выводом на экран.

Параметры -o и -F отвечают за выбор формата отчета сканирования.

Существуют и другие параметры, такие как -mutate (угадывать поддомены, файлы, каталоги и имена пользователей), -evasion (обходить фильтр идентификаторов) и -Single (для одиночного тестового режима), которые можно использовать для углубленной оценки цели (**parasram?**).

Выполнение лабораторной работы

Выполнение лабораторной работы

Чтобы работать с nikto, необходимо подготовить веб-приложение, которое будем сканировать. Это будет DVWA. Для этого запустила apache2

```
zsh: corrupt history file /home/meprokojjeva/.zsh_history
[meprokojjeva@meprokojjeva]~$ sudo systemctl start mysql
[sudo] пароль для meprokojjeva:
[meprokojjeva@meprokojjeva]~$ sudo systemctl start ap
Failed to start ap.service: Unit ap.service not found.
[meprokojjeva@meprokojjeva]~$ sudo systemctl start apache2
```

Ввожу в адресной строке браузера адрес DVWA, перехожу в режим выбора уровня безопасности, ставлю минимальный (необязательно, nikto при обычном сканировании для режима impossible и low выдаст одинаковые потенциальные уязвимости, что логично, ведь они остаются, но изменяется сложность, с которой их можно использовать)

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Authorisation Bypass

DVWA Security

Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.

Low

Submit

Security level set to low

Запускаю nikto Проверить веб-приложение можно, введя его полный URL и не вводя порт, попробовала просканировать

```
(meprokojjeva@meprokojjeva)~  
$ nikto  
  
(meprokojjeva@meprokojjeva)~  
$ nikto -h http://127.0.0.1/DVWA/  
- Nikto v2.5.0
```

```
+ Target IP: 127.0.0.1  
+ Target Hostname: 127.0.0.1  
+ Target Port: 80  
+ Target URI: http://127.0.0.1/DVWA/ (CMT2)
```


Выводы

Научилась использовать сканер nikto для тестирования веб-приложений