

Использование nikto

Этап 4

Абу Сувейлим М. М.

10 января 2003

Российский университет дружбы народов, Москва, Россия

Информация

- Абу Сувейлим Мухаммед Мунифович
- Студент
- Российский университет дружбы народов
- 1032215135@pfur.ru
- <https://mukhammed-abu-suveilim.github.io/>

Вводная часть

- Выполнить простейшие команды инструмента nikto.
- Отсканировать сайт университета <esystem.rudn.ru> на безопасности веб-сервера.

1. Парасрам Шива Х.Т. Замм Алекс. Kali Linux. Тестирование на проникновение и безопасность. СПб, 2020. 448 с.
2. OTUS. Проверяем на уязвимости любой сайт с помощью Nikto. 2020.

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.

Выполнение лабораторной работы

Во-первых, установим инструмент nikto, если он уже не установлен на виртуальной машине, командой (рис. 1):

```
—(snabu@snabu) ~$  
—$ sudo apt install nikto  
[sudo] password for snabu:  
nikto is already the newest version (1:2.5.0~git20230314.00ff645-0kali1).  
nikto set to manually installed.  
The following packages were automatically installed and are no longer required:  
  glibd-caplet libdisplay-info1 libgnomekb08 libndctl6 libpostproc57 libproxy1-plugin-webkit librs0.3 libx265-199 openjdk-17-jre-headless python3-pendulum rwho  
  libavfilter9 libgssapi12-104 libjsncp025 libplacebo310 libproxy1-plugin-gsettings libravie libsofiaiencid1 libsox-lv16 python3-diskcache python3-pytdata samba-nd-provision  
  libdaxctl1 libgnomekbd-common libjxl0.7 libmmt libproxy1-plugin-networkmanager libx2-10 libz1f-udev openjdk-17-jre python3-mistune2 rwho samba-dfs-modules  
Use 'sudo apt autoremove' to remove them.  
Summary:  
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 670  
—(snabu@snabu) ~$  
—$ nikto  
- Nikto v2.5.0
```

Figure 1: Установка nikto

Можно увидеть, что у нас версия nikto - v2.5.0

Далее, выполняем простую задачу/команду:

```
nikto -h esystem.rudn.ru -ssl
```

nikto - это сам инструмент для сканирования веб-серверов на наличие уязвимостей.

`-h esystem.rudn.ru` — указывает цель сканирования, в данном случае - `esystem.rudn.ru`. - параметр `-h` используется для задания хоста, который будет проверяться. Вместо доменного имени можно было бы указать IP-адрес веб-сервера.

`-ssl` - этот флаг указывает Nikto на то, что сканируемый веб-сервер использует SSL/TLS для шифрования соединения (т.е. работает через HTTPS на порту 443 по умолчанию). Это важно для корректного установления безопасного соединения между сканером и сервером.

Анализ результатов

После выполнения предыдущей команды, мы получили следующую информацию (рис. 2):

```
root@kali:~# nikto -h esystem.rudn.ru -ssl
- Nikto v2.5.0

-----
+ Target IP:      185.178.246.57
+ Target Hostname: esystem.rudn.ru
+ Target Port:    443
-----

+ SSL Info:      Subject: /C=ru, o=rudn.ru
                  Ciphers: TLS_AES_128_GCM_SHA256
                  Issuer: /C=RU/O=GlobalSign/ou=sa/OU=GlobalSign/GC R3 DV TLS CA 2020
+ Start Time:    2024-10-05 16:13:50 (GMT+3)
-----

+ Server: ddos-guard
+ / Cookie _ddg8 created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ / Cookie _ddg9 created without the httpsonly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ / Cookie _ddg9 created without the httpsonly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ / Cookie _ddg9 created without the httpsonly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ / 19 address found in the _ddg9 cookie. The IP is 92.129.26.48
+ / Cookie _ddg10 created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ / Cookie _ddg10 created without the httpsonly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ / Cookie _ddg1 created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ / Cookie _ddg1 created without the httpsonly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ / Cookie MoodleSession created without the httpsonly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ / Retrieved access-control-allow-origin header: *
+ / Uncommon header 'content-style-type' found, with contents: text/css.
+ / Uncommon header 'content-script-type' found, with contents: text/javascript.
+ / The site uses TLS and the Strict-Transport-Security header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ / The x-content-type-options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.setsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ / /AAJmnb.js: Uncommon header 'dng-cache-status' found, with contents: MISS.

+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (10) reached for host, giving up. Last error: opening stream: can't connect: Connect failed: ; Connection timed out at /var/lib/nikto/plugins/WQ.pm line 5254.
+ Connection timed out
+ Scan terminated: 28 error(s) and 15 item(s) reported on remote host
+ End Time:      2024-10-05 16:25:28 (GMT+3) (698 seconds)
-----

+ 1 host(s) tested

root@kali:~#
```

Figure 2: Команда nikto -h esystem.rudn.ru -ssl

IP-адрес цели: 185.178.208.57

Имя хоста: esystem.rudn.ru

Порт: 443 (порт по умолчанию для HTTPS)

Сертификат сайта выдан для домена *.rudn.ru.

Используемый шифр для TLS: TLS_AES_128_GCM_SHA256.

Сертификат выдан центром сертификации GlobalSign.

Найденные проблемы и предупреждения

Пять cookies файлов (__ddg8_, __ddg9_, __ddg10_, __ddg1_, MoodleSession) были созданы без флагов безопасности:

- Без флага Secure - эти cookies не защищены при передаче через незащищенные соединения (HTTP). Флаг Secure гарантирует, что cookie передаются только через зашифрованные соединения (HTTPS).
- Без флага HttpOnly - это значит, что данные cookies могут быть доступны через JavaScript на стороне клиента, что увеличивает риск XSS-атак (межсайтовый скриптинг).

В cookie файле __ddg9_ обнаружен IP-адрес 57.129.24.68, что является потенциальной утечкой информации.

Отсутствует заголовок Strict-Transport-Security (HSTS), который предотвращает атаки с понижением уровня безопасности, обеспечивая принудительное использование HTTPS.

Отсутствует заголовок X-Content-Type-Options, который предотвращает автоматическое определение браузером типа контента, что может привести к уязвимостям, связанным с MIME-типа (Multipurpose Internet Mail Extensions).

Заголовок `access-control-allow-origin` настроен на разрешение запросов от любых источников (*), что может быть небезопасно.

Обнаружены нестандартные заголовки: `content-style-type` (указан как `text/css`) и `content-script-type` (указан как `text/javascript`).

В ответе от сервера содержится заголовок `ddg-cache-status: MISS`, что означает, что запрашиваемый ресурс не был найден в кеше (это относится к DDoS-защите сайта).

Выводы

В результате выполнения работы мы повысили свои навыки использования инструмента nikto