

Индивидуальный проект.

Этап 4. Использование nikto

Стариков Данила Андреевич

19 апреля 2024

Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия

Цели и задачи

- Познакомиться с утилитой `nikto` для поиска уязвимостей веб-серверов
- Проверить ее работу на ранее установленном сервере DVWA

Результаты

```
(dastarikov@dastarikov)-[~]  
$ sudo service mysql start  
  
(dastarikov@dastarikov)-[~]  
$ sudo service apache2 start  
  
(dastarikov@dastarikov)-[~]  
$ firefox 127.0.0.1 &  
[1] 36195
```

Рис. 1: Запуск веб-сервера DVWA.

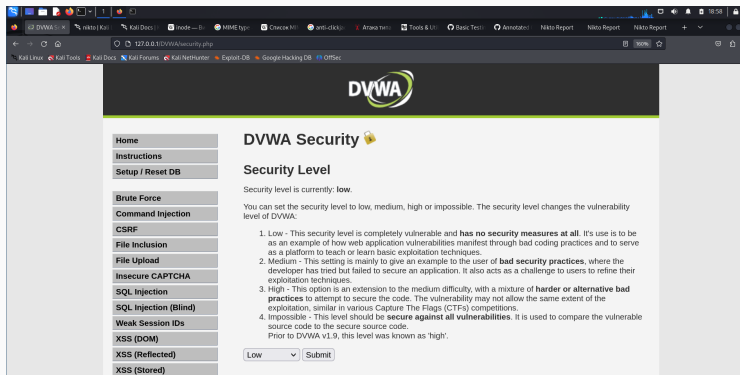


Рис. 2: Проверка работы сервера.

```
datahax@datahax:~$ man nikto
NIKTO(1)
NAME
    nikto - Scan web server for known vulnerabilities
SYNOPSIS
    nikto [options ...]
DESCRIPTION
    Multiple hosts
    Examine a web server to find potential problems and security vulnerabilities, including:
    • Server and software misconfigurations
    • Default files and programs
    • Insecure files and programs
    • Outdated servers and programs
    Nikto is built on libWhisker (by RFP) and can run on any platform which has a Perl environment. It supports SSL, proxies, host authentication, IDS evasion and more. It can be updated automatically from the command-line, and supports the optional submission of updated version data back to the maintainers.
```

Рис. 3: Man-page nikto.

```
(dastarikov@dastarikov)-[~]
$ nikto -Display 1234EP -o report.html -Format htm -Tuning 123bde -host 127.0.0.1
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 80
+ Start Time: 2024-04-19 18:21:15 (GMT3)

+ Server: Apache/2.4.58 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 29cd, size: 612b112e93ec6, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ ../ - 200/OK Response could be Appending '../' to a directory may reveal PHP source code.
+ /?mod=node&id=some_thing&op=view - 200/OK Response could be Sage 1.0b3 may reveal system paths with invalid module names.
+ /?mod=some_thing&op=browse - 200/OK Response could be Sage 1.0b3 reveals system paths with invalid module names.
- STATUS: Completed 1000 requests (~29% complete, 12 seconds left): currently in plugin 'Nikto Tests'
- STATUS: Running average: Not enough data.
+ ../ - 200/OK Response could be Appending '../' to a directory allows indexing
+ / - 200/OK Response could be Appears to be a default Apache Tomcat install.
```

Рис. 4: Консольный вывод программы во время работы.

127.0.0.1 / 127.0.0.1 port: 80	
Target IP	127.0.0.1
Target hostname	127.0.0.1
Target Port	80
HTTP Server	Apache/2.4.58 (Debian)
Site Link (Name)	http://127.0.0.1:80/
Site Link (IP)	http://127.0.0.1:80/
URI	/
HTTP Method	GET
Description	/: The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://127.0.0.1:80/ http://127.0.0.1:80/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
URI	/
HTTP Method	GET
Description	/: 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.
Test Links	http://127.0.0.1:80/ http://127.0.0.1:80/
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
URI	/
HTTP Method	GET
Description	/: Server may leak inodes via ETags, header found with file /, inode: 29cd, size: 612b112e93ec6, mtime: gzip.
Test Links	http://127.0.0.1:80/ http://127.0.0.1:80/
References	CVE-2003-1418
URI	/
HTTP Method	OPTIONS
Description	OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
Test Links	http://127.0.0.1:80/ http://127.0.0.1:80/
References	

Рис. 5: Пример найденной уязвимости веб-сервера.

Host Summary	
Start Time	2024-04-19 18:37:42
End Time	2024-04-19 18:38:01
Elapsed Time	19 seconds
Statistics	4300 requests, 0 errors, 5 findings

Scan Summary	
Software Details	DirBt 2.3.0
CLI Options	-Display 123456 -o report0.html -format htm -tuning 123bde -host 127.0.0.1
Hosts Tested	1
Start Time	Fri Apr 19 18:37:41 2024
End Time	Fri Apr 19 18:38:01 2024
Elapsed Time	20 seconds

© 2008 Chris Sufo

Рис. 6: Итоговый отчет по тестированию веб-сервера.

Host Summary

Start Time	2024-04-19 18:35:45
End Time	2024-04-19 18:36:17
Elapsed Time	32 seconds
Statistics	8074 requests, 0 errors, 15 findings

Scan Summary

Software Details	Nikto 2.5.0
CLI Options	-Display 1234EP -o report.html -Format htm -host 127.0.0.1
Hosts Tested	1
Start Time	Fri Apr 19 18:35:44 2024
End Time	Fri Apr 19 18:36:17 2024
Elapsed Time	33 seconds

Рис. 7: Итоговый отчет по тестированию веб-сервера с большим числом тестов.

ИТОГ



- В результате работы познакомились с утилитой **nikto** и проверили уязвимости веб-сервера DVWA с разными параметрами теста.