

Основы информационной безопасности

Индивидуальный проект № 4. Использование nikto

Смирнов-Мальцев Егор Дмитриевич

Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение лабораторной работы	6
4	Выводы	8
	Список литературы	9

Список иллюстраций

3.1	Экран помощи nikto	6
3.2	Создание отчета в nikto	6
3.3	Отчет nikto	7

1 Цель работы

Научиться определять уязвимости сайтов с помощью nikto.

2 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.

Более подробно про Unix см. в [1–4].

3 Выполнение лабораторной работы

Просмотрел флаги для команды nikto (рис. fig. 3.1).

```
(egorsmirnovmaljce@kali)~$ nikto
- Nikto v2.5.0
-----
+ ERROR: No host (-host) specified

Options:
  -ask+           Whether to ask about submitting updates
                  yes   Ask about each (default)
                  no    Don't ask, don't send
                  auto  Don't ask, just send
  -check6+       Check if IPv6 is working (connects to ipv6.google.com or value set in nikto.conf)
  -cgidirs+      Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
  -config+       Use this config file
  -Display+      Turn on/off display outputs:
                  1     Show redirects
                  2     Show cookies received
                  3     Show all 200/OK responses
                  4     Show URLs which require authentication
                  D     Debug output
                  E     Display all HTTP errors
                  P     Print progress to STDOUT
                  S     Scrub output of IPs and hostnames
                  V     Verbose output
```

Рис. 3.1: Экран помощи nikto

Создал с помощью nikto отчет о DVWA (рис. fig. 3.2).

```
(egorsmirnovmaljce@kali)~$ nikto -u http://localhost/DVWA/ -r report.html -snopt hta
- Nikto v2.5.0
-----
+ Target IP: 127.0.0.1
+ Target hostname: localhost
+ Target port: 80
+ Start time: 2024-10-05 18:35:11 (GMT3)
-----
+ Server: Apache/2.4.42 (Ubuntu)
+ /DVWA/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /DVWA/: 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/
+ /DVWA/: /DVWA/ redirects to: login.php
+ No CGI Directories found (use "-C all" to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ /DVWA/config/: Directory indexing found.
+ /DVWA/config/: Configuration information may be available remotely.
+ /DVWA/inputs/: Directory indexing found.
+ /DVWA/inputs/: This might be interesting.
+ /DVWA/database/: Directory indexing found.
+ /DVWA/database/: Database directory found.
+ /DVWA/output/: Directory indexing found.
+ /DVWA/output/: Directory indexing found.
+ /DVWA/output/index: Git index file may contain directory listing information.
+ /DVWA/output/index: Git index file found. Full repo details may be present.
+ /DVWA/output/config: Git config file found. Info about repo details may be present.
+ /DVWA/output/config: Gitignore file found. It is possible to grasp the directory structure.
+ /DVWA/dockerignore: dockerignore file found. It may be possible to grasp the directory structure and learn more about the site.
+ 828 requests: 4 error(s) and 15 item(s) reported on remote host
+ End time: 2024-10-05 18:35:50 (GMT3) (39 seconds)
-----
+ 1 host(s) tested
```

Рис. 3.2: Создание отчета в nikto

Просмотрел отчет (рис. fig. 3.3).

Host Summary	
Start Time	1970-01-01 03:00:00
End Time	1970-01-01 03:00:00
Elapsed Time	0 seconds
Statistics	4 requests, errors, findings
Scan Summary	
Software Details	Nikto 2.5.3
CLI Options	-h http://localhost/OVWAV -o report.html -format htm
Hosts Tested	0
Start Time	Sat Oct 5 18:32:26 2024
End Time	Sat Oct 5 18:32:27 2024
Elapsed Time	1 seconds
© 2008 Chris Sulo	
localhost / 127.0.0.1 port 80	
Target IP	127.0.0.1
Target hostname	localhost
Target Port	80
HTTP Server	Apache/2.4.62 (Debian)
Site Link (Name)	http://localhost:80/OVWAV
Site Link (IP)	http://127.0.0.1:80/OVWAV
URI	/OVWAV/
HTTP Method	GET
Description	/OVWAV/: The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://localhost:80/OVWAV/ http://127.0.0.1:80/OVWAV/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
URI	/OVWAV/
HTTP Method	GET
Description	/OVWAV/: 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://localhost:80/OVWAV/ http://127.0.0.1:80/OVWAV/
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerability/testing-content-type-header/

Рис. 3.3: Отчет nikto

4 Выводы

Мы смогли с помощью nikto определить уязвимости DVWA.

Список литературы

1. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.
2. Robbins A. Bash Pocket Reference. O'Reilly Media, 2016. 156 с.
3. Zarrelli G. Mastering Bash. Packt Publishing, 2017. 502 с.
4. Newham C. Learning the bash Shell: Unix Shell Programming. O'Reilly Media, 2005. 354 с.