

# Основы информационной безопасности

Индивидуальный проект № 4. Использование nikto

---

Смирнов-Мальцев Е. Д.

5 октября 2024

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Смирнов-Мальцев Егор Дмитриевич
- студент группы НКНбд-01-21
- Российский университет дружбы народов

## Цель работы

---

Научиться определять уязвимости сайтов с помощью 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.

## Выполнение лабораторной работы

---



# Экран помощи nikto

```
(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
```

# Создание отчета в nikto

```
root@kali:~# nikto -h http://localhost/DVWA/ -o report.html -format htm
- Nikto v2.1.5.4

-----
+ Target IP:      127.0.0.1
+ Target Hostname: localhost
+ Target Port:    80
+ Start Time:     2024-10-05 18:35:21 (GMT+3)
-----

+ Server: Apache/2.4.42 (Debian)
+ /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.netasparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page /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/tests/: Directory indexing found.
+ /DVWA/tests/: This might be interesting.
+ /DVWA/database/: Directory indexing found.
+ /DVWA/database/: Database directory found.
+ /DVWA/docs/: Directory indexing found.
+ /DVWA/.git/index: Git index file may contain directory listing information.
+ /DVWA/.git/HEAD: Git HEAD file found. Full repo details may be present.
+ /DVWA/.git/config: Git config file found. Info about repo details may be present.
+ /DVWA/.gitignore: .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.
+ 3500 requests: 0 error(s) and 15 time(s) reported on remote host
+ End time:      2024-10-05 18:35:50 (GMT+3) (29 seconds)
-----

+ 1 host(s) tested
```

Restore Session	
Nikto Report	
file:///home/egorsmimovmja/colreport.html	
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OJSec	
<b>Host Summary</b>	
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
<b>Scan Summary</b>	
Software Details	Nikto 2.5.0
CLI Options	-h http://localhost/DVWA/ -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	
<b>localhost / 127.0.0.1 port 80</b>	
Target IP	127.0.0.1
Target hostname	localhost
Target Port	80
HTTP Server	Apache/2.4.62 (Debian)
Site Link (Name)	<a href="http://localhost:80/DVWA/">http://localhost:80/DVWA/</a>
Site Link (IP)	<a href="http://127.0.0.1:80/DVWA/">http://127.0.0.1:80/DVWA/</a>
URI	/DVWA/
HTTP Method	GET
Description	/DVWA/: The anti-clickjacking X-Frame-Options header is not present.
Test Links	<a href="http://localhost:80/DVWA/">http://localhost:80/DVWA/</a> <a href="http://127.0.0.1:80/DVWA/">http://127.0.0.1:80/DVWA/</a>
References	<a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options</a>
URI	/DVWA/
HTTP Method	GET
Description	/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.
Test Links	<a href="http://localhost:80/DVWA/">http://localhost:80/DVWA/</a> <a href="http://127.0.0.1:80/DVWA/">http://127.0.0.1:80/DVWA/</a>
References	<a href="https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/">https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/</a>

## Выводы

---

Мы смогли с помощью nikto определить уязвимости DVWA.