

Структура научной презентации

Простейший шаблон

Карпачев Я. О.

Российский университет дружбы народов, Москва, Россия

Информация

- Карпачев Я. О.
- студент
- Российский университет дружбы народов

Вводная часть

Найти уязвимости с помощью nikto

0. приготовить mysql, apache2
1. найти точку входа на DVWA (айпи адрес + порт или полный URL)
2. запустить проверку на уровне защиты low
3. запустить проверку на уровне защиты imposible

Запускаем две команды одна для mysql, другая для apache2

```
(yokarpachev@vbox)-[~]
$ sudo systemctl start mysql
[sudo] password for yokarpachev:

(yokarpachev@vbox)-[~]
$ sudo systemctl start apache2

(yokarpachev@vbox)-[~]
$ #nikto

(yokarpachev@vbox)-[~]
$ 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
+ Start Time:	2025-04-07 03:41:16 (GMT-7)



Рис. 1: Запуск команд

Запускаем проверку на уровне защиты low, full url path

```
+ Server: Apache/2.4.62 (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 th
e user agent to render the content of the site in a different fashion to th
e MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vuln
erabilities/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: GET, POST, OPTIONS, HEAD .
+ /DVWA///etc/hosts: The server install allows reading of any system file b
y adding an extra '/' to the URL.
+ /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/login.php: Admin login page/section found.
+ /DVWA/.git/index: Git Index file may contain directory listing informatio
n.
+ /DVWA/.git/HEAD: Git HEAD file found. Full repo details may be present.
+ /DVWA/.git/config: Git config file found. Infos about repo details may be
present.
+ /DVWA/.gitignore: .gitignore file found. It is possible to grasp the dire
ctory structure.
+ /DVWA/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/e
tc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wordpress/wp-content/themes/twentyeleven/images/headers/server.php?
filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DVWA/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A
PHP backdoor file manager was found.
+ /DVWA/wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/et
c/hosts: A PHP backdoor file manager was found.
+ /DVWA/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts:
A PHP backdoor file manager was found.
+ /DVWA/wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/e
tc/hosts: A PHP backdoor file manager was found.
+ /DVWA/assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager
was found.
+ /DVWA/login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote
command execution.
+ /DVWA/shell?cat=/etc/hosts: A backdoor was identified.
+ /DVWA/.dockerignore: .dockerignore file found. It may be possible to gras
p the directory structure and learn more about the site.
+ 8074 requests: 0 error(s) and 26 item(s) reported on remote host
+ End Time: 2025-04-07 03:41:36 (GMT-7) (20 seconds)
```

```
+ 1 host(s) tested
```


Запускаем проверку на уровне защиты impossible, ip + port

```
(yokarpache@vbox) ~$ nikto -h 127.0.0.1 -p 80
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 80
+ Start Time: 2025-04-07 03:45:48 (GMT-7)

DWA Security
Security Level

+ Server: Apache/2.4.62 (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.netspar
on/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: 29cf, size: 62f6e9f72a673, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-561
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /assets/mobileise/css/meta.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /login.cgi?cli=aa20aa27ca20/etc/hosts: Some D-Link Router remote command execution.
+ /shellcat/etc/hosts: A backdoor was identified.
+ 8874 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time: 2025-04-07 03:46:04 (GMT-7) (16 seconds)

+ 1 host(s) tested
```

Рис. 3: Запуск команды на уровне защиты impossible

Выводы

Я научился находить уязвимости с помощью утилиты nikto