

Основы информационной безопасности. Индивидуальный проект

Этап № 4. Использование nikto

Нзита Диатезилуа Катенди

27 сентября 2024 г.

Российский университет дружбы народов, Москва, Россия

Информация

- Нзита Диатезилуа Катенди
- студент
- Российский университет дружбы народов
- 1032215220@pfur.ru
- <https://github.com/NzitaKatendi>

Вводная часть

Целью данной работы является Nikto сканирования уязвимостей веб-приложения.

Задачи:

- Проанализировать уязвимости веб-приложения DVWA с помощью сканера Nikto.

Инструмент: DVWA, Nikto

Выполнение лабораторной работы

```
(dknzita@dknzita)-[~]
```

```
$ perl -v
```

```
This is perl 5, version 38, subversion 2 (v5.38.2) built for x86_64-linux-gnu-thread-multi  
(with 44 registered patches, see perl -V for more detail)
```

```
Copyright 1987-2023, Larry Wall
```

```
Perl may be copied only under the terms of either the Artistic  
License or the  
GNU General Public License, which may be found in the Perl 5 s  
ource kit.
```

```
Complete documentation for Perl, including FAQ lists, should b  
e found on  
this system using "man perl" or "perldoc perl". If you have a  
ccess to the  
Internet, point your browser at https://www.perl.org/, the Per  
l Home Page.
```

```
(dknzita@dknzita)-[~]
```

```
$ 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
```

Сканирование и анализ

```
(dknzita@dknzita)-[~]
$ nikto -h http://localhost/DVWA/ -o report.html -Format html
- Nikto v2.5.0

+ Target IP:      127.0.0.1
+ Target Hostname: localhost
+ Target Port:    80
+ Start Time:     2024-10-02 07:42:22 (GMT-4)

+ 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 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/
+ 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/login.php: Admin login page/section 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. Infos 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.
+ 7850 requests: 0 error(s) and 16 item(s) reported on remote host
+ End Time:      2024-10-02 07:42:35 (GMT-4) (13 seconds)

+ 1 host(s) tested
```

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/DVWA/
Site Link (IP)	http://127.0.0.1:80/DVWA/
URI	/DVWA/
HTTP Method	GET
Description	/DVWA/: The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://localhost:80/DVWA/ http://127.0.0.1:80/DVWA/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
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	http://localhost:80/DVWA/ http://127.0.0.1:80/DVWA/
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
URI	/DVWA/
HTTP Method	OPTIONS
Description	OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
Test Links	http://localhost:80/DVWA/ http://127.0.0.1:80/DVWA/
References	
URI	/DVWA/config/
HTTP Method	GET
Description	/DVWA/config/: Directory indexing found.
Test Links	http://localhost:80/DVWA/config/ http://127.0.0.1:80/DVWA/config/
References	
URI	/DVWA/config/
HTTP Method	GET

The image shows a terminal window with the output of a Nikto scan. The scan was performed on 127.0.0.1 port 80. The output lists various findings, including missing headers, directory listings, and several PHP backdoor file managers. To the right of the terminal, a table summarizes the findings, categorized by URI, HTTP Method, Description, Test Links, and References.

```
(dknzita@dknzita)-[~]
$ 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: 2024-10-02 07:46:24 (GMT-4)

+ 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.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: 29cf, size: 6229b4608334d, mtime: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ ///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 config 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/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.
+ /shell?cat=/etc/hosts: A backdoor was identified.
+ 8074 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time: 2024-10-02 07:46:37 (GMT-4) (13 seconds)

+ 1 host(s) tested

*****
Portions of the server's headers (Apache/2.4.62) are not in
```

URI	HTTP Method	Description	Test Links	References
/	GET	CVNWA: The anti-clickjacking X-Frame-Options header is not present.	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
/	GET	CVNWA: 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.	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
/server-status	GET	CVNWA: This reveals Apache information. Comment out appropriate line in the Apache config file or restrict access to allowed sources.	https://osvdb.org/view/vuln/561	https://osvdb.org/view/vuln/561
/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts	GET	CVNWA: A PHP backdoor file manager was found.	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
/wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts	GET	CVNWA: A PHP backdoor file manager was found.	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts	GET	CVNWA: A PHP backdoor file manager was found.	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
/wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts	GET	CVNWA: A PHP backdoor file manager was found.	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts	GET	CVNWA: A PHP backdoor file manager was found.	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
/wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts	GET	CVNWA: A PHP backdoor file manager was found.	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
/assets/mobirise/css/meta.php?filesrc=	GET	CVNWA: A PHP backdoor file manager was found.	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
/login.cgi?cli=aa%20aa%27cat%20/etc/hosts	GET	CVNWA: Some D-Link router remote command execution.	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
/shell?cat=/etc/hosts	GET	CVNWA: A backdoor was identified.	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

Рис. 4: Проверка уязвимостей с указанием порта

Заключение

В результате выполнения работы был использован сканер Nikto для сканирования уязвимостей веб-приложения.

1. DVWA [Электронный ресурс]. GitHub, Inc, 2024. URL: <https://github.com/digininja/DVWA>.
2. Обзор сканера Nikto для поиска уязвимостей в веб-серверах [Электронный ресурс]. 2006–2024, Habr, 2023. URL: <https://habr.com/ru/companies/first/articles/731696/>.