

Основы информационной безопасности

Индивидуальный проект. Этап № 4. Использование Nikto

Подлесный Иван Сергеевич.

07.09.2024

Российский Университет дружбы народов

Информация

- Подлесный Иван Сергеевич
- студент группы НКНбд-01-21
- Российский университет дружбы народов

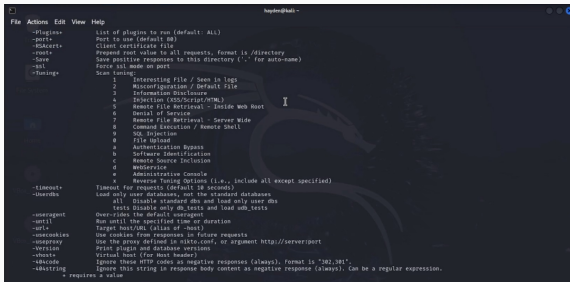
Вводная часть

Цель работы

Целью данной работы является сканирование уязвимостей с помощью приложения Nikto

Ход работы

Проверим, что nikto установлен



```

File Actions Edit View Help
~Plugins~
~port~      List of plugins to run (default: All)
~MSAccept~  Port to use (Default 80)
~root~      Client certificate file
~root~      Prepend root value to all requests, format is /directory
~save~      Save positive responses to this directory ('.' for auto-save)
~ssl~       Force ssl mode on port
~Tuning~    Scan tuning:
            1 Interesting File / Seen in logs
            2 Misconfiguration / Default file
            3 Information Disclosure
            4 Injection (XSS/Script/HTML)
            5 Remote File Retrieval - Inside Web Root
            6 Denial of Service
            7 Remote File Retrieval - Server Wide
            8 Command Execution / Remote Shell
            9 SQL Injection
            0 File Upload
            a Authentication Bypass
            b Software Identification
            c Remote Source Inclusion
            d Webservice
            e Administrative Console
            A Reverse Tuning Options (i.e., include all except specified)
~timeout~   Timeout for requests (Default 20 seconds)
~Userdb~    Load only user databases, not the standard databases
            all Disable standard dbm and load only user dbm
            tests Disable only db tests and load web tests
~useragent~ Over-rides the default useragent
~until~     Run until the specified time or duration
~url~       Target host/URL (alias of -host)
~usercookies Use cookies from responses in future requests
~useproxy~  Use the proxy defined in nikto.conf, or argument http://server:port
~version~   Print plugin and database versions
~host~     Virtual host (for Host header)
~404code~   Ignore these HTTP codes as negative responses (always). Format is "302,301".
~404string~ Ignore this string in response body content as negative response (always). Can be a regular expression.
            * requires a value
```

Figure 1: Проверка установки ПО

Затем проверим сайт DVWA, указав опции для сохранения отчета в формате html

```
File Actions Edit View Help
kaylen@kali: ~
--(huyden@kali):~$
$ nikto -u http://localhost/DVWA/ -o report.html -format html
Nikto v2.5.0

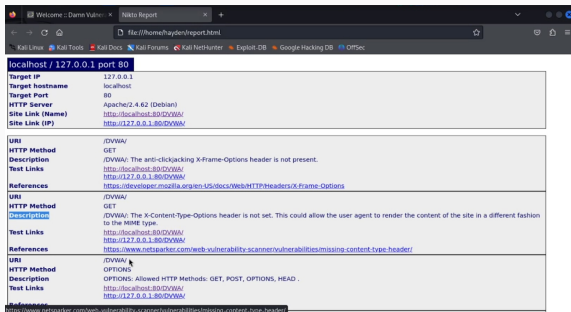
+-----+
+ Target IP:      127.0.0.1
+ Target Hostname: localhost
+ Target Port:    80
+ Start Time:     2024-10-04 22:43:53 (GMT)
+-----+

+ 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-headers/
+ 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/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. 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.
+ 7450 requests, 0 errors(s) and 36 item(s) reported on remote host
+ End Time:      2024-10-04 22:44:19 (GMT) (26 seconds)
+-----+

+ 1 host(s) tested

*****
Portions of the server's headers (Apache/2.4.62) are not in
the Nikto 2.5.0 database or are newer than the known string. Would you like
to submit this information (won server specific data) to CIRT.net
for a Nikto update (or you may email to submit@cirt.net) (y/n)?
```

Figure 2: Форма для ввода пароля



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/
<hr/>	
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
<hr/>	
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.netparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
<hr/>	
URI	/DVWA/
HTTP Method	OPTIONS
Description	OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
Test Links	http://localhost:80/DVWA/ http://127.0.0.1:80/DVWA/
References	https://www.netparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

Figure 3: Отчет об уязвимостях в формате html

Посмотр информацию об уязвимостях по порту 80

[illegible]

Figure 4: Данные о запросе на вход

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