Unit 1: Scanning For Web Vulnerabilities Tools and HTTP Utilities

1

Unit Structure

1.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Identify different kinds of web vulnerabilities using various tools.
- Usage of HTTP utilities.

1.2 INTRODUCTION

This block is focus to tools that aid in the analysis anddefence of the software that runs on systems and drives web applications. It explains how to use command-line and proxy tools to find vulnerabilities in web applications. Also delves into the techniques for successful, optimal password cracking.

1.3 SCANNING FOR WEB VULNERABILITIES TOOLS

Web vulnerabilities scanners are the software programs that scan web sites; generally it looks for web vulnerabilities like XSS (cross site scripting), SQL injection, file-directory listing and insecure web server configuration. This kind of software is also referred as Dynamic Application Security Testing Tools.

1.3.1 NIKTO

Nikto is a tool to find the insecure and various files, settings and programs on the web server.

When hackers or penetration testers are looking to attack a target they usually first want to compile a list of target surfaces after that they'll use a tool like Nikto to scan for vulnerabilities and discover the weakest link allowing him to spend a minimal amount of time and effort actually attacking the target.

It is examine the web server to identify potential problems, including:

- Poor server configuration settings
- Default files
- Unsafe files

Nikto is built on Perl programming Open Source platform. It includes SSL, host login authentication, proxy and many more. Nikto can be updated through command-line. Nikto is very easy to run in Windows or any Unix based operating system. In Kali

Linux it is pre-installed. You shouldn’t need to install it separately. To run nikto use –h option with targeted host name or IP address in terminal to start the vulnerability scanning. The following example describes the usage of nikto tool:

```
root@kali:~# nikto -h axxxxxxxxxr.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          6x.1xx.2xx.98
+ Target Hostname:    axxxxxxxxxr.com
+ Target Port:        80
+ Start Time:         2019-04-11 10:58:06 (GMT5.5)
---------------------------------------------------------------------------
+ Server: LiteSpeed
+ Cookie PHPSESSID created without the httponly flag
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the
user agent to protect against some forms of XSS
+ 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
+ Uncommon header 'link' found, with contents:
<https://1199.pk/index.php?rest_route=/>; rel="https://api.w.org/"
+ /webmail/blank.html: IlohaMail 0.8.10 contains an XSS vulnerability.
Previous versions contain other non-descript vulnerabilities.
+ /securecontrolpanel/: Web Server Control Panel
+ /webmail/: Web based mail package installed.
+ OSVDB-3233: /mailman/listinfo: Mailman was found on the server.
+ OSVDB-2117: /cpanel/: Web-based control panel
+ OSVDB-3268: /includes/: Directory indexing found.
+ OSVDB-3092: /includes/: This might be interesting...
+ OSVDB-3092: /old/: This might be interesting...
+ OSVDB-3092: /img-sys/: Default image directory should not allow directory
listing.
+ OSVDB-3093: /webmail/lib/emailreader_execute_on_each_page.inc.php: This
might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ /controlpanel/: Admin login page/section found.
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening
stream: can't connect (connect error): Network is unreachable
+ Scan terminated:  20 error(s) and 18 item(s) reported on remote host
+ End Time:           2019-04-11 12:01:54 (GMT5.5) (3828 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Table-1 lists the additional options to run the Nikto tool.

➢ Nikto command-line options

Following is a table

Nikto Option	Description
-config+	Use this config file

-Display+	Turn on/off display outputs
-dbcheck	Check database and other key files for syntax errors
-Format+	Save file (-o) format
-Help	Extended help information
-host+	Target host
-id+	Host authentication to use, format is id:pass or id:pass:realm
-list-plugins	List all available plugins
-output+	Write output to this file
-nossl	Disables using SSL
-no404	Disables 404 checks
-Plugins+	List of plugins to run (default: ALL)
-port+	Port to use (default 80)
-root+	Prepend root value to all requests, format is /directory
-ssl	Force ssl mode on port
-Tuning+	Scan tuning
-timeout+	Timeout for requests (default 10 seconds)
-update	Update databases and plugins from CIRT.net
-Version	Print plugin and database versions
-vhost+	Virtual host (for Host header)
	+ requires a value

Table-1 Nikto command-line options

1.3.2 W3AF

W3AF is the acronym of Web Application Attack and Audit Framework. This framework is to find the web application vulnerabilities like SQL injection, XSS and many more.

W3AF is built on Open Source community for Web Application Exploitation Framework. It also provides information about web app vulnerability and supports to pen-testing. W3AF is available for almost all operating system like Linux, MAC OS, and Windows etc. It is developed in python programming language and support for both CUI as well as GUI environment.

Before executing W3AF users should to know the basics and workflow. This will helps to user for getting better idea in the process of identifying web app vulnerabilities.

In W3AF there are main three plugin types which are as follows:

- Crawl
- Audit
- Attack

Crawl plugin

This plugin will finding only URLs in which the injection points occurs. Input for this plugin is the URL and it will provide one or more injection points.

Audit plugin

It takes the input as injection point found by crawl and identifies the web app vulnerability like SQL injection.

Attack plugin

This is to exploit the vulnerabilities found by audit. They generally return a dump of table on remote server if it is SQL injection vulnerability.

There are other plugins available in W3AF like: Infrastructure, Grep, Output, Mangle, Bruteforce, and Evasion.

How to Run W3AF

As described earlier, W3AF have CUI as well as GUI environment. For the command line execute:

```
$ ./w3f_console
w3af>>>
```

From this point you will be able to execute the various commands of W3AF.

```
w3af>>> help
|----------------------------------------------------------------  |
| start          | Start the scan.                                  |
| plugins        | Enable and configure plugins.                    |
| exploit        | Exploit the vulnerability.                       |
| profiles       | List and use scan profiles.                      |
| cleanup        | Cleanup before starting a new scan.              |
|----------------------------------------------------------------  |
| help           | Display help. Issuing: help [command] , prints |
|                | more specific help about "command"               |
| version        | Show w3af version information.                   |
| keys           | Display key shortcuts.                           |
|----------------------------------------------------------------  |
| http-settings  | Configure the HTTP settings of the framework.  |
| misc-settings  | Configure w3af misc settings.                    |
| target         | Configure the target URL. |
|----------------------------------------------------------------  |
| back           | Go to the previous menu.                         |
| exit           | Exit w3af.                                       |
|----------------------------------------------------------------  |
| kb             | Browse the vulnerabilities stored in the         |
|                | Knowledge Base                                   |
|----------------------------------------------------------------  |
w3af>>>
w3af>>> help target
Configure the target URL.
w3af>>>
```

To get into configuration menu, just enter its name and press enter, you can see how prompt will change according to your context menu.

```
w3af>>> http-settings
w3af/config:http-settings>>>
```

Every configuration menus have following commands:

- Help
- View
- Set
- Back

Usage of these commands in http-settings menu as following:

```
w3af/config:http-settings>>> help
|-----------------------------------------------------------------|
| view     | List the available options and their values.         |
| set      | Set a parameter value.                               |
| save     | Save the configured settings.                        |
|-----------------------------------------------------------------|
| back     | Go to the previous menu.                              |
| exit     | Exit w3af.                                            |
|--------------------------------------------------------------|
w3af/config:http-settings>>> view
|--------------------------------------------------------------|
| Setting        | Value    | Description                       |
|--------------------------------------------------------------|
| url_parameter  |     | Append the given URL parameter to
                 everyaccessed URL. |

...
|--------------------------------------------------------------|
| basic_auth_user | | Set the basic authentication username for HTTP
requests |
| basic_auth_passwd | | Set the basic authentication password for
HTTPrequests |
| basic_auth_domain | | Set the basic authentication domain for HTTP
requests |
|--------------------------------------------------------------|
w3af/config:http-settings>>> set timeout 5
w3af/config:http-settings>>> save
w3af/config:http-settings>>>back
w3af>>>
```

As shown in above example, the view command will display all the configurable arguments, with their possible values and description. The set command will change the value of argument. The save command will perform the commit operation over the changes in argument’s value. Lastly back command will exit from current menu context.

Plugins can be configured using following commands:

```
w3af>>> plugins
w3af/plugins>>> help
|--------------------------------------------------------------|
| list           |List available plugins.                      |
|--------------------------------------------------------------|
| back           |Go to the previous menu.                     |
| exit           |Exit w3af.                                   |
|--------------------------------------------------------------|
| output         |View, configure and enable output plugins    |
| audit          |View, configure and enable audit plugins     |
| crawl          |View, configure and enable crawl plugins     |
| bruteforce     |View, configure and enable bruteforce plugins |
| grep           |View, configure and enable grep plugins      |
| evasion        |View, configure and enable evasion plugins   |
| infrastructure |View, configure and enable infrastructure    |
|                |plugins                                      |
| auth           |View, configure and enable auth plugins      |
| mangle         |View, configure and enable mangle plugins    |
|--------------------------------------------------------------|
w3af/plugins>>>
```

You can list all the plugins by providing plugin name as following command:

```
w3af>>> plugins
w3af/plugins>>> list audit
|----------------------------------------------------------------|
| Plugin name   | Status    | Conf     | Description              |
|----------------------------------------------------------------|
| blind_sqli    |          | Yes      | Identify blind SQL       |
|               |          |          | injection vulnerabilities|
...
w3af/plugins>>>
```

To turn on the XSS and SQLI plugins, we have to apply the following command:

```
w3af/plugins>>> audit xss, sqli
w3af/plugins>>> audit
|----------------------------------------------------------------|
| Plugin name   | Status    |Conf | Description                   |
|----------------------------------------------------------------|
| sqli          | Enabled  |     | Find SQL injection bugs.      |
...
| xss           | Enabled  | Yes | Identify cross site scripting |
|               |          |     | vulnerabilities.              |
...
w3af/plugins>>>
```

To start the scan, we should apply the following command:

```
w3af>>> target
w3af/config:target>>> set target http://localhost/
w3af/config:target>>> back
w3af>>> start
```

1.4HTTP UTILITIES

The following tools are used to perform connections over HTTP or HTTPS. Basically they are not supposed to find any vulnerability, but its functionality can be extends the supports towards the vulnerability scanner.

1.4.1 CURL

Transferring data from one place to another is one the main task done using computers connected to a network. There are so many GUI tools out there to send and receive data, but when you are working on a console, only equipped with command line functionality, using CURL is inevitable.

A less known fact is that CURL can work with a wide range of protocols and can solve most of your scripting tasks with ease.

CURL: CURL is an easy to use command line tool to send and receive files, and it supports almost all major protocols(DICT, FILE, FTP, FTPS, HTTP, HTTPS, LDAP, POP3, SMTP and many more) in use.

Features of CURL:

- Can be used inside your shell scripts with ease
- Supports features like pause and resume of downloads
- It has around 120 command line options for various tasks
- It runs on all major operating systems
- Supports cookies, forms and SSL
- Both CURL command line tool and libcurl library are open source, so they can be used in any of your programs
- It supports configuration files
- Multiple upload with a single command
- Progress bar, rate limiting, and download time details
- Ipv6 support

Table-2 lists the additional options of the CURL utility.

➢ CURL command-line options

Following is a table

Usage: curl [options...] <url>

CURL Option	**Description**
-b, --cookie <data>	Send cookies from string/file
-d, --data <data>	HTTP POST data

-G, --get	Put the post data in the URL and use GET
-I, --head	Show document info only
-H, --header <header/@file>	Pass custom header(s) to server
-0, --http1.0	Use HTTP 1.0
--http1.1	Use HTTP 1.1
--http2	Use HTTP 2
-i, --include	Include protocol response headers in the output
-4, --ipv4	Resolve names to IPv4 addresses
-6, --ipv6	Resolve names to IPv6 addresses
-l, --list-only	List only mode
-o, --output <file>	Write to file instead of stdout
-x, --proxy [protocol://]host[:port]	Use this proxy
-U, --proxy-user <user:password>	Proxy user and password
-B, --use-ascii	Use ASCII/text transfer
-u, --user <user:password>	Server user and password
-A, --user-agent <name>	Send User-Agent <name> to server
-v, --verbose	Make the operation more talkative
-V, --version	Show version number and quit

Table-2CURL command-line options

1.4.2 OpenSSL

OpenSSL is free security protocol and putting into use library given by Free Software community. OpenSSL libraries are used by a lot of businesses/projects in their systems and products. OpenSSL libraries and sets of computer instructions can be used with openssl command. It is the most common library for establishing the encrypted connection.

The S represents in HTTPS connection that uses Secure Socket Layer for transport data. Encrypted connections in web are often uses the HTTPS connection but it provides limited security. The Secure Socket Layer and Transport Layer Security protocol offer security from reading a plaintext data points between sender and receiver.

How to use OpenSSL

To check the version of OpenSSL following command will be used:

```
root@kali:~# openssl version
OpenSSL 1.1.0h 27 Mar 2018
root@kali:~#
```

To see the list of available common cipher standards

```
root@kali:~# openssl list -cipher-commands

aes-128-cbc       aes-128-ecb       aes-192-cbc       aes-192-ecb
aes-256-cbc       aes-256-ecb       base64            bf
bf-cbc            bf-cfb            bf-ecb            bf-ofb
camellia-128-cbc  camellia-128-ecb  camellia-192-cbc  camellia-192-
ecb
camellia-256-cbc  camellia-256-ecb  cast              cast-cbc
cast5-cbc         cast5-cfb         cast5-ecb         cast5-ofb
des               des-cbc           des-cfb           des-ecb
des-ede           des-ede-cbc       des-ede-cfb       des-ede-ofb
des-ede3          des-ede3-cbc      des-ede3-cfb      des-ede3-ofb
des-ofb           des3              desx              rc2
rc2-40-cbc        rc2-64-cbc        rc2-cbc           rc2-cfb
rc2-ecb           rc2-ofb           rc4               rc4-40
seed              seed-cbc          seed-cfb          seed-ecb
seed-ofb
root@kali:~#
```

We can use a listed above symmetric encryption cipher commands in OpenSSL.

Let’s see how it works in terminal.

First of all create one plaintext file using nano command and provide a name like *msg*.

```
root@kali:~# openssl enc -aes-256-cbc -base64 -in msg -out enc
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:
root@kali:~# cat enc
U2FsdGVkX1/u76rxzLD9wtLgM2J3Ps8K7/FjMroOszzEQ/bMyQgUvu+Lxsn0F3fT
root@kali:~#
```

Above listed command is used for encryption of plaintext file named *msg* which is mentioned with *–in msg* parameter. *enc* specify the encryption using *–aes-256-cbc* cipher command with *–base64* parameter. Finally the encrypted file is transformed using *–out enc* parameter.

It will ask for the encryption password while cipher the plaintext file. It asks for retyping the password for verifying process.

Now, for decryption of file we have to use some commands like as shown below:

```
root@kali:~#openssl enc -aes-256-cbc -d -base64 -in enc -out dec
enter aes-256-cbc decryption password:
root@kali:~# cat dec
hi this is demo of OpenSSL
root@kali:~#
```

As illustrate in above *–d* parameter is used for decryption with *–base64* parameter and decrypted file will transform into plaintext file named with *dec* using *–out* parameter in the example.

1.4.3 STunnel

It is a program to provide encryption between client and remote server. It runs on cross platform operating system. You could also encrypt any type of network communication so for instance you could encrypt unencrypted messages with Stunnel.So they're encrypted send it across the network and send it to another Stunnel program running in server mode and it will accept that secure communication and then forward it on to the service that wants it.

If you want to bypass a firewall or intrusion prevention system so you wanted to hide essentially your malware or your bad programs or your information by encrypting it. Using Stunnel you can bypass any types of detection scheme by the administration on that network would not be able to see what you are doing cause of sending encrypted traffic across the network.

There are two ways to pass encrypted message to the server over the network through Stunnel, one is to any secure service like https, pop3, imap4 and another way is to any non-secure service like http. To pass the encrypted message to any non-secure service you could use another Stunnel program situated at server side.

Any secure communications over the network rely on certificates. Firstly you required a proper PEM file which includes encryption key for communications. Stunnel has a default file named as stunnel.pem.

What is Tunneling

It means that program (daemon) runs on the client as well as server machine. For example, the Windows 2000 PC is the client and server is any *NIX machine. So, Stunnel will then execute as client on Windows and the server mod on UNIX machine.

e.g.

```
Windows:
stunnel –d 5800 –r unix_ip_address:5800 –c

UNIX:
stunnel –d 5800 –r 5801
```

As above illustrated in above example –d indicate Stunnel program execute in daemon mode on port 5800; -r indicate that remote host machine; -c indicate that client mode.

The following is the short version of configuration file avail by default. This example of file will demonstrate the use TLS client mode service like pop3, imap, smtp.

```
; Sample stunnel configuration file for Unix by Michal Trojnara
1998-2019
; Some options used here may be inadequate for your particular
configuration
; This sample file does *not* represent stunnel.conf defaults
; Please consult the manual for detailed description of available
options

; ******************************************************************
; * Global options                         ;
******************************************************************
; It is recommended to drop root privileges if stunnel is started by
root
;setuid = nobody
;setgid = nogroup

; PID file is created inside the chroot jail (if enabled)
;pid = /usr/local/var/run/stunnel.pid
;
;
[gmail-pop3]
client = yes
accept = 127.0.0.1:110
connect = pop.gmail.com:995
verifyChain = yes
CApath = /etc/ssl/certs
checkHost = pop.gmail.com
OCSPaia = yes

[gmail-imap]
client = yes
accept = 127.0.0.1:143
connect = imap.gmail.com:993
verifyChain = yes
```

```
CApath = /etc/ssl/certs
checkHost = imap.gmail.com
OCSPaia = yes

[gmail-smtp]
client = yes
accept = 127.0.0.1:25
connect = smtp.gmail.com:465
verifyChain = yes
CApath = /etc/ssl/certs
checkHost = smtp.gmail.com
OCSPaia = yes
```

Check your Progress 1:

1. What is Nikto in Cyber Security?
2. W3AF stands for __________
3. What is the use of curl command?
4. Define OpenSSL
5. How STunnel works?

1.5LET US SUM UP

This block covers the various Web Application Tools for Pentesting as well as to find the web vulnerabilities. Using this student can learn the basic concepts of Nikto, W3AF, OpenSSL, etc.

1.6CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check your Progress 1:

1. The Nikto web server scanner is a security tool that will test a web site for thousands of possible security issues. Including dangerous files, mis-configured services, vulnerable scripts and other issues. It is open source and structured with plugins that extend the capabilities.

2. W3AF stands for Web Application Attack and Audit Framework.
3. The curl command transfers data to or from a network server, using one of the supported protocols (HTTP, HTTPS, FTP, FTPS, SCP, SFTP, TFTP, DICT, TELNET, LDAP or FILE). It is designed to work without user interaction, so it is ideal for use in a shell script.
4. OpenSSL is a software library for applications that secure communications over computer networks against eavesdropping or need to identify the party at the other end. It is widely used by Internet servers, including the majority of HTTPS websites.
5. STunnel works by listening on another port and then redirecting that traffic through to the unsecured port.

1.7 FURTHER READING

For more focus on cyber security domain use CEH (Certified Ethical Hacking) books. Also you can refer “Anti-Hacker Toolkit By Mike Shema”

1.8ASSIGNMENTS

- How to useW3AF?

1.9ACTIVITIES

- Perform Curl command on various protocol.