CALIFORNIA STATE UNIVERSITY SAN BERNARDINO

Eduardo Torres <004717712@coyote.csusb.edu>

Week 8 Alternative Lab

1 message

Google Forms <forms-receipts-noreply@google.com> Mon, May 21, 2018 at 11:38 PM
To: 004717712@coyote.csusb.edu

Thanks for filling out Week 8 Alternative Lab

Here's what we got from you:

Week 8 Alternative Lab

Please watch this video (https://vimeo.com/167411059) to answer the questions below. ****Note: I did not pick out the music. It was included by the hacker. Feel free to turn it down.

Email address *

004717712@coyote.csusb.edu

Please put your First and Last Name.

Eduardo Torres

Please put your ID number.

004717712

What type of web-application security scanner is he using?

He is using OWASP ZAP. OWASP ZAP helps with detecting or finding vulnerabilities in a web app

What is his proxy? Make sure to include the port number.

His proxy is "localhost" (127.0.0.1) with port 8080

What type of website platform is SME using?

SME is using WordPress as its website platform

What does he do to get around the IP checks?

He uses tor which allows him to bypass the IP filter

What is the first attack type he tries?

He attempts an IDOR attack by manipulating an id tag

He makes an interesting statement about the activities of the police. What do you think his motivation is?

My initial thought about his possible motivation is that he is trying to hack into the police website to see if it could be done.

Who is Yuri Jardine? Why is he important?

Yuri Jardine was assaulted by some Mossos police agent while attempting to defend a woman.

Who is Ester Quintana? Why is she important?

Ester Quintana, who participated in a protest, was also assaulted by Mossos agents, who wounded her by shooting a rubber pellet into her left eye, causing her to lose her eye.

How many tries does it take until he starts getting something in SQLMap?

It took him two tries for him to receive results on SQLMap.

What is the first sql injection statement from MySQL Map?

It is a UNION query with the payload: "id=-8990 UNION ALL SELECT NULL..." followed by 10 columns

How many databases are there?

6 databases were retrieved

What is the root document to upload files?

The root document to upload files is "/var/www/wp-content/uploads/"

Within the php file for the website...there is a task called TODO. What is written next to that task?

Fix command injection

What type of vulnerability does he find in the php file?

He discovered that it is possible to upload a PHP file

How many tables does the "campus" database have?

The "campus" database has 25 tables.

What SQL injection statement does he use to look for the user that has the possibility escalate his privileges?

He used, "SELECT * from campus.alumnos where tipo_usuario = 3"

What is the first password he finds for the administrator Antonio?

He found Antonio's password to be "1094"

What kind of file is file.php?

File.php is an executable script

Where does he upload this file?

He uploads the file in the "Criminologia" course, within the "Temari" section

What kind of file are the databases saved in?

backup.tar.gz, or zip file.

What does the touch command do in linux?

It is a command used to update the access date or change the date of a file

Why is it important that the site admins reuse passwords?

He mentions that admins reuse passwords, meaning that there is a good chance that you can attempt the same password on other sites and make a successful log in to those other sites.

What is his advice when using a victims password to login in other places?

He mentions that it would be wise to use an IP from the same city or country. He also explains that copying the victims "user agent" prevents them from receiving a "new device" notification.
