CALIFORNIA STATE UNIVERSITY
SAN BERNARDINO

Cole Ramos <005658194@coyote.csusb.edu>

Week 8 Alternative Lab

1 message

Google Forms <forms-receipts-noreply@google.com>
To: 005658194@coyote.csusb.edu

Mon, May 21, 2018 at 11:35 PM

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 *

005658194@coyote.csusb.edu

Please put your First and Last Name.

Cole Ramos

Please put your ID number.

005658194

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

OWASP ZAP

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

localhost, 127.0.0.1 Port 8080

What type of website platform is SME using?

WordPress

What does he do to get around the IP checks?

Tor

What is the first attack type he tries?

IDOR

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

He hacking into police site show their vulnerability, and to show the injusticed of police and corruption

Who is Yuri Jardine? Why is he important?

Juri Jardine was victim of brutal beating at a night and false accusations by police for being the protagonist. Political statement being made, that there is no justice in Barcelona.

Who is Ester Quintana? Why is she important?

Ester Quintana was a protester who was returning home, when a police office rubber bullet was shoot at her face, causing her to lose her left eye. The police claim innocence, and we can see that no action taken against offices. No justice until 4 years later.

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

2

What is the first sql injection statement from MySQL Map?

--dbms=mysql --technique=U

How many databases are there?

6

What is the root document to upload files?

Root file /var/www/wp-content/uploads/2016/05

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?

Standard php file upload vulnerability

How many tables does the "campus" database have?

25

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

select*from campus.alumnos where tipo_usuario = 3

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

1094

What kind of file is file.php?

PDF file

Where does he upload this file?

Criminologia is where the file is upload

What kind of file are the databases saved in?

He save files in the databases are back.tar.gz

What does the touch command do in linux?

can change timestamps, directories and creates new empty files.

Why is it important that the site admins reuse passwords?

He mentioned that admin user use the same password for is twitter account, which opens the admin user to more frequent attacks.

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

Use IP from same city or at least same country, and copy their agent so they don't get emails about a "new device" signing into their accounts.

Create your own Google Form