Piscine Pro

Cybersecurity 2x1

Summary: In this Module you will learn about Deserialization with RCE.

Version: 1.00

Contents

Chapter I

A word about this Piscine Pro

Welcome!

You are about to embark on the module of this professional training in cybersecurity. Our aim is to introduce you to the world of cybersecurity and engage in a peer-learning experience, following the educational model of 42.

Instead of providing a course with a single solution for each problem, which may become outdated in a few years, we have opted for a peer-learning approach. Your task is to explore elements that could be beneficial for your challenges, identify the ones of actual interest through testing and manipulation. Collaborate with others, exchange perspectives, generate new ideas collectively, and, ultimately, conduct your own experiments.

Peer-evaluation plays a crucial role in discovering alternative approaches and uncovering special cases that might not have crossed your mind, potentially impacting your program. Just as different clients prioritize different aspects, each reviewer will bring a unique perspective. Additionally, this process might lead to new connections and collaborations in the future.

By the end of this program, your journey will differ from that of other participants. You'll have tackled distinct projects, chosen specific challenges over others, and that's perfectly normal. It's an experience that blends both collective and personal growth, with everyone benefiting from their unique encounters during this period.

Best of luck to all!

Chapter II

Introduction

What this Module will show you:

- Discovery in IT security from a developer's point of view.
- Discovery the best-known vulnerabilities.
- Discover how to detect this vulnerability and the possible risks of not protecting an application from it.

Chapter III

General instructions

Unless explicitely specified, the following rules will apply every day of this Professional training.

- This subject is the one and only trustable source. Don't trust any rumor.
- This subject can be updated up to one hour before the turn-in deadline.
- The assignments in a subject must be done in the given order. Later assignments won't be rated unless all the previous ones are perfectly executed.
- Be careful about the access rights of your files and folders.
- Your assignments will be evaluated by your peers.
- You must not leave in your turn-in your workspace any file other than the ones explicitly requested By the assignments.
- You have a question? Ask your left neighbor. Otherwise, try your luck with your right neighbor.
- Every technical answer you might need is available in the `man` or on the Internet.
- By Thor, by Odin! Use your brain!!!

Chapter IV

Exercise 01

	Exercise 01
Ex01: Mandatory Part	
Turn-in directory : *ex*01/	
Files to turn in : `Readme.md, Payloads.md, Fix.md, and any other necessary files`	
Allowed functions : `None`	

To accomplish this project, you must first download the tar file available on your project page. Then, extract the contents of this file wherever you prefer.

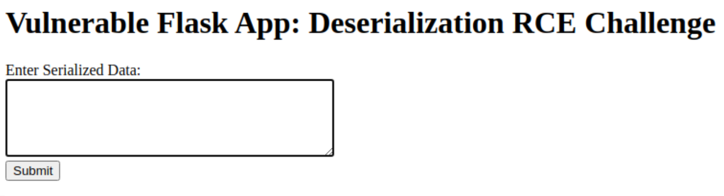
```
> ./start.sh
./start.sh
Cleaning Docker...
[..]
Waiting for the server to start...
[...]
You can connect on this website:
http://....
```

`It is important to access this directory via your terminal to proceed.`

Once the command has executed, you can access the application through the browser of your choice using the address provided in the terminal.

`If you encounter any issues during this step, it's important to contact a technical representative from the professional training program.`

Your project is now underway! Bellow is the page you should see:

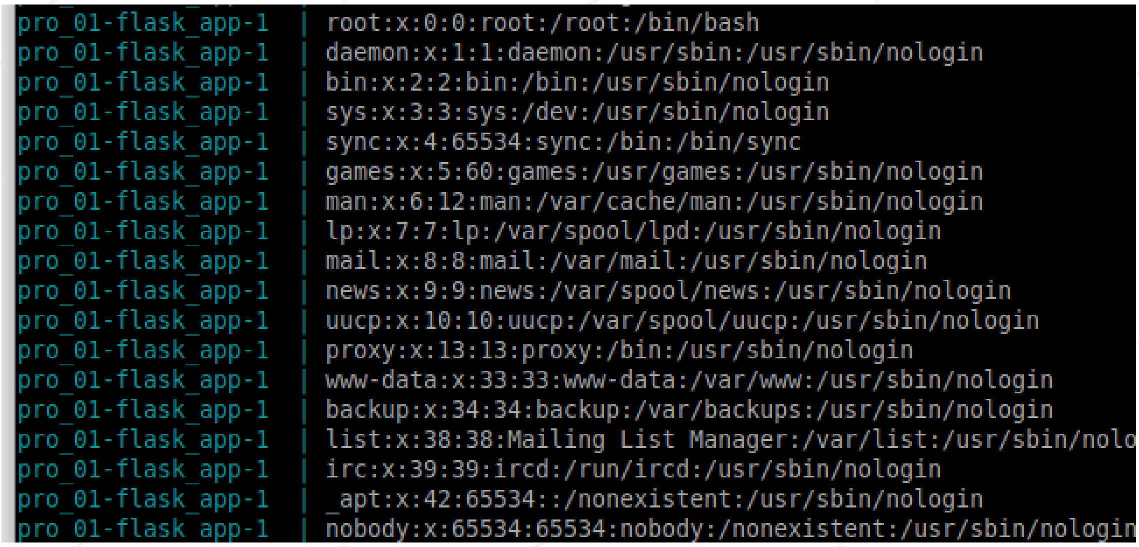


Vulnerable Flask App: Deserialization RCE Challenge

- You must now find a way to exploit this website!

- Your objective is to display the contents of /etc/passwd file.

Here is the excepted output:



```
pro_01-flask_app-1  | root:x:0:0:root:/root:/bin/bash
pro_01-flask_app-1  | daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
pro_01-flask_app-1  | bin:x:2:2:bin:/bin:/usr/sbin/nologin
pro_01-flask_app-1  | sys:x:3:3:sys:/dev:/usr/sbin/nologin
pro_01-flask_app-1  | sync:x:4:65534:sync:/bin:/bin/sync
pro_01-flask_app-1  | games:x:5:60:games:/usr/games:/usr/sbin/nologin
pro_01-flask_app-1  | man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
pro_01-flask_app-1  | lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
pro_01-flask_app-1  | mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
pro_01-flask_app-1  | news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
pro_01-flask_app-1  | uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
pro_01-flask_app-1  | proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
pro_01-flask_app-1  | www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
pro_01-flask_app-1  | backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
pro_01-flask_app-1  | list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nolo
pro_01-flask_app-1  | irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
pro_01-flask_app-1  | _apt:x:42:65534::/nonexistent:/usr/sbin/nologin
pro_01-flask_app-1  | nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

To do so, you must learn on what OWASP is.

- When you are certain about the type of vulnerability, you should document the vulnerability type and provide an explanation of it in a Readme.md file.

- Document the various payloads you were able to use in a Payloads.md file.

- Identify at least 2 different scenarios in which these vulnerabilities could be exploited.

- The final step is relatively simple: find a way to protect a web application from this type of vulnerability. Once you have determined the protective measures, document them in the Fix.md file.

- Don't hesitate to include sources if necessary.

Chapter V

Bonus part

If you find yourself with some available time, you might consider exploring this optional bonus task. While it is not mandatory, please avoid dedicating excessive time to it.

You are now required to create a script in the programming language of your choice that utilizes various different payloads with the purpose of showcasing the vulnerability. The objective is for the application to run in a state where this script can automatically demonstrate the presence of the vulnerability.

Make sure to restart the application as needed to verify the proper functioning of your program.

Automated scripts for exploiting the website.

It's important to ensure that your chosen program is operating correctly and can reliably demonstrate the vulnerability whenever the application is functioning.

The bonus part will only be assessed if the mandatory part is PERFECT. Perfect means the mandatory part has been integrally done and works without malfunctioning. If you have not passed ALL the mandatory requirements, your bonus part will not be evaluated at all.

Chapter VI

Submission and peer-evaluation

- Create a `professional_training` folder at the root of your home, and move around in it.
- Create a new `module02` folder and navigate to it.
- From now on, all exercises should be in the correct folder rendering. Exercise 00 in the `ex00` folder, Exercise 01 in the `ex01` folder, etc ... you get the logic.

Please note, during your defense anything that is not present in the folder for the day will not be checked.