Introduction

The RCE is when an attacker places the intended or injects the malicious code into the target machine to exploit the system's vulnerability. The RCE attack was reported as CVE-2022-29464 [1] [2], and another was reported as a POC for exploiting SAP GateWay vulnerability [3].

However, I tried to follow the provided GitHub Repos of the write-up, and the owner explained the RCE process for exploiting the vulnerabilities. So, those can not be demonstrated because we lack detailed information, and it is illegal to exploit corporate infrastructures without permission.

Remote Code Execution is one of the processes in the Cyber Kill Chain [4], which is used to gain access to target systems via horizontal or vertical privilege escalation. If we consider the complete picture of penetration testing, we only require the REC part for students as the submissions. This will be challenging for them if they don't have robust penetration skills.

Suggestion

There is a simple RCE LAB via uploading a web shell using the PortSwigger platform, which is an online web application security training platform.

RCE LAB Requirement:

https://portswigger.net/web-security/file-upload/lab-file-upload-remote-code-execution-via-web-shell-upload

LAB Prerequisites:

1. **Create a new account on the PortSwigger platform**

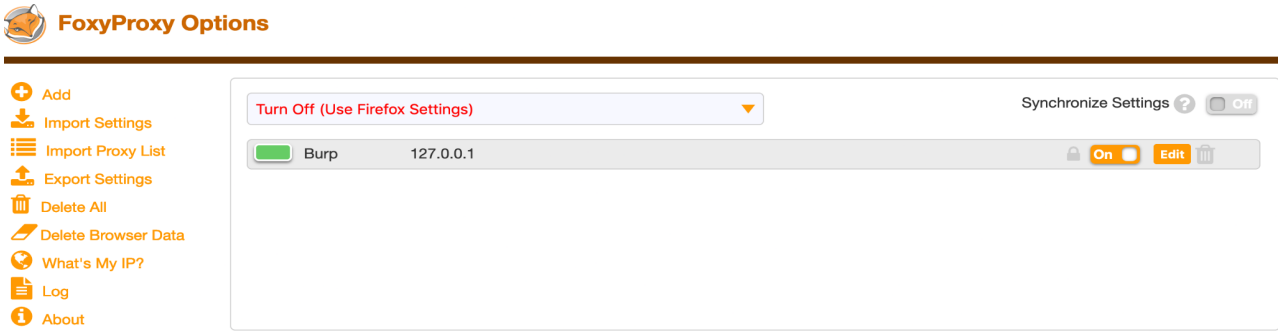
   The registration link is **https://portswigger.net/users/register**

2. **BurpSuite Community Installation**

   https://portswigger.net/burp/communitydownload

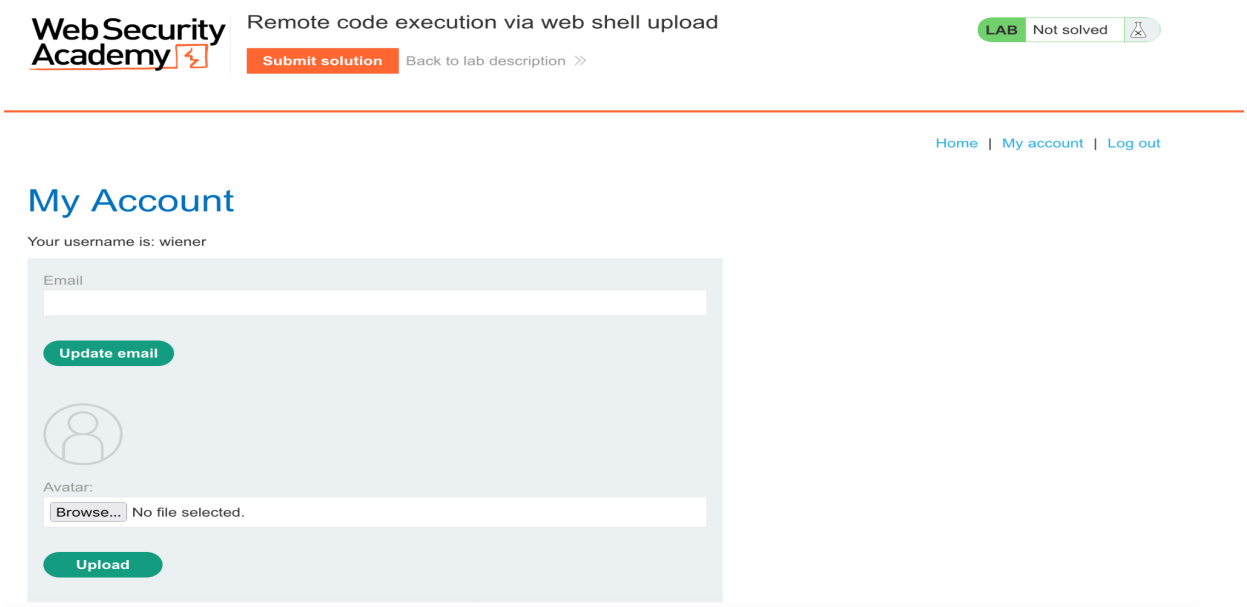
3. **Set up a FoxyProxy in Firefox or Chrome Browser**

   https://cybergeeks.cloud/2021/07/usando-burp-suite-e-foxyproxy-no-firefox/



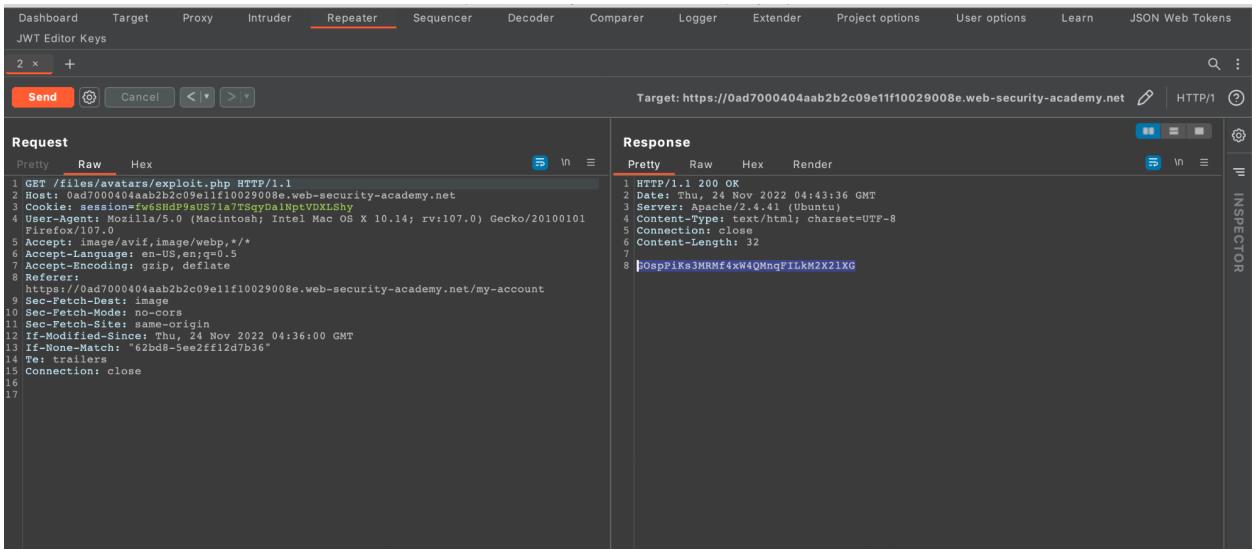
Exploitation:

The objective of this is to get the user secrets with uploading php script or other scripts like javascript, python script.

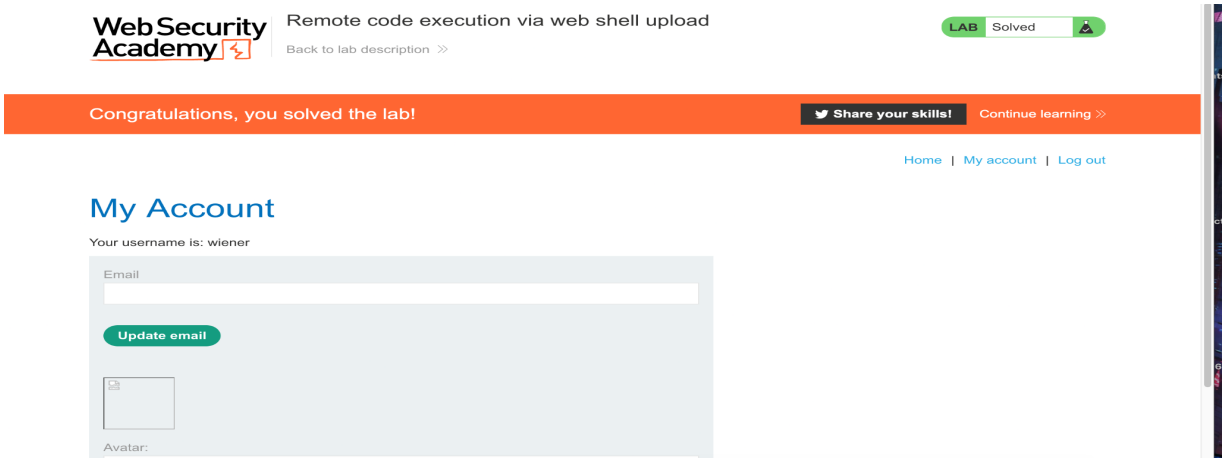


Using BurpSuite Repeater for fordwarding the request before injecting the arbitrary code into server to get the credentials.

Exploit the user credentials via code execution, and send the Http.request to the server.



Submit the credentials, then the lab completion will be look like this



Question-Answer and Hands-on LAB:

Given payloadbox:

https://github.com/payloadbox/command-injection-payload-list

1. What is the Remote Code Execution Attack?
2. How to achieve RCE in this LAB with given PHP script?
3. Show the LAB Solved Result
4. What system the server is used (Easy)?

   Answer will be shown after using <?php echo exec("uname -a"); ?>

5. What is the current user (Easy)?

   Answer will be shown after using <?php echo exec("whoami"); ?>

6. What are file permission and file owner for secret file (Midium)?

   Answer will be shown after using <?php echo exec("ls -l /home/carlos"); ?>

Advanced RCE Questions

Writeup:

https://medium.com/r3d-buck3t/rce-with-server-side-template-injection-b9c5959ad31e

7. According to the given RCE writeup, what is the server-side template engine and what is the server-side template injection?
8. Which essential payload for confirming SSTI in the case?

Practice Room is in here: https://tryhackme.com/room/learnssti

And here: https://app.hackthebox.com/machines/278

Reference

1. "WSO2 documentation," *Security Advisory WSO2-2021-1738 - WSO2 Platform Security - WSO2 Documentation*. [Online]. Available: https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1738. [Accessed: 17-Nov-2022].

2. wso2, “Carbon-kernel/fileuploadservlet.java at 4.4.x · WSO2/carbon-kernel,” *GitHub*. [Online]. Available: https://github.com/wso2/carbon-kernel/blob/4.4.x/core/org.wso2.carbon.ui/src/main/java/org/wso2/carbon/ui/transports/FileUploadServlet.java. [Accessed: 18-Nov-2022].

3. Chipik, “Chipik/SAP_GW_RCE_EXPLOIT: SAP gateway RCE exploits,” *GitHub*. [Online]. Available: https://github.com/chipik/SAP_GW_RCE_exploit. [Accessed: 18-Nov-2022].

4. “Cyber kill chain®,” *Lockheed Martin*, 29-Jun-2022. [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. [Accessed: 21-Nov-2022].