

**System and Network Programming**

**IE2012**

**Assignment**

|  |  |
| --- | --- |
| IT Number | Name |
| IT21385414 | Gallage E.D.S |

Acknowledgment

I would like to convey our gratitude to a number of individuals who provided unwavering support and significantly aided in the accomplishment of our project. Special thanks to Mr. Lakmal Rupasinghe, our respective system and network programming, for the clear instructions and helpful guidance. Finally, I want to express my gratitude to the faculty of computers and the Sri Lanka Institute of Information Technology for providing us with the tools and resources we required.

Table of Content

1. Introduction.
2. Steps to complete the tasks.
3. Introduction

In this project I used ubuntu server 18.04 version as the base. And kali Linux virtual machine to connect with the server. The entire project was built around a SQL Injection attack and capture the flag. To do that, I run a website locally using Apache2 and hide three flags in the server to perform a SQL Injection attack.

In the server we have two users, as root and user. Two flags were in on both interfaces. Third flag was on source code of the website. And it was encrypted using Caesar Cipher with a key. Attacker needs to find all flags to complete the task.

We just supply the second user's username and password at this early stage. The attacker can then get remote access to the server by using the "ssh" command. The attacker must next gain access to the website database and discover the root user's password using a locally hosted website on port 80. That component is what SQL Injection requires.

The attacker will now have root-level access to the server and must locate 3 secret flags to finish the mission.

**Tryhackme Room Link**: <https://tryhackme.com/jr/theboysmv/>

1. Steps to Complete the room

* We must first deploy the computer and the attack box offered by tryhackme (ubuntu server I uploaded). Simply select the Start Machine option in Task 1 (Introduction section) to deploy the machine.
* We've now launched both the attack box and the server. After the server has been successfully deployed, an IP address will be provided in the active machine information. We need that IP address to connect to the server using the attack box.
* Before connecting to the server, we'll use the **"ping"** command to see if the server responds.
* Now we can observe the server respond to our "ping" command. That means the server is working.
* Next, we need to look at the server's open ports. We'll do a "nmap" scan for that.
* As a result, • Port 80 - ssh • Port 22 - http are both open.
* There is a website running on this server if port 80/http is open. And port 22/ssh open indicates that we can connect to the server by establishing a ssh communication channel.
* The following step is to connect to the server. We'll need at least one of the user's credentials for this
* We can now use that to execute the **"ssh"** command.
* **ssh [Username]@[IPAddress]**
* If this command is executed properly, it will first request that the connection be verified, followed by the user's password.
* So, to start, we must respond "yes" to the connection request.
* The user password must then be provided to connect to the server.
* To fulfill the second assignment, we must first find the user flag. To do this, we can use "ls" to list files.
* We can now see that there is a file. To view the file, we can use the "cat" command.
* We can now see that there is a file. To view the file, we can use the "cat" command.
* This, as you can see, is not the flag file. A hint is offered in the second challenge. It instructs you to inspect hidden files to find the flag. We can use the "ls -al" command to see hidden files.
* Now we can see there is a hidden file with the same name **(user.txt).**
* To view hidden file, we can do a **“cat [filename]”.**
* Now we can complete the second task.
* In the next task (website), they state that there is a website hosted on port 80 that is hosted locally. Because the site is hosted on port 80, we can quickly launch it by entering the IP address into the browser's search bar.
* After running the site, we can observe in the login screen that the website is vulnerable to SQL injection attacks. We can now move forward by delivering answers.
* We can answer the first task using the vulnerability we discovered.
* The next four answers are about discovering a flag hidden on the website. In that task, we can find a hint for that. They are instructing you to examine the source code.
* We can now inspect the source code of each page by right-clicking on it and selecting the source code option.
* A crucial detail is mentioned in a remark in the Index.html file. And we can see in that comment that they used a popular shift cipher to encrypt it.
* So, we know that the most used shift cipher is the Caesar cipher. Because Caesar cipher has only 26 potential keys, we may easily perform a brute force attack to acquire the plain text.
* We may now open our browser and look for Caesar cipher online decoder.
* We can decode the flag and obtain the key using this website.
* We now have everything we need to provide replies and finish the task 3.
* The fourth task (Root Access) is based on a SQL Injection attack on the website database via the login page.
* After a successful SQL Injection attack on the database, we can obtain the root's username and password.
* With it, we can finish task 4 and go on.
* In the final challenge (Root Flag), we must locate the flag buried in the root. To do this, we can use the "ls" program to list all files.
* We can now inspect the file using the "cat" command.
* As you can see, it includes the flag. We can finish the room by making it the flag.

1. Reference Materials

<https://infosecwriteups.com/how-to-make-our-own-ctf-challenge-with-ease-6b15f76865b5>

<https://www.digitalocean.com/community/tutorials/how-to-install-linux-apache-mysql-php-lamp-stack-ubuntu-18-04>

<https://vitux.com/how-to-work-with-tables-select-update-delete-create-table-alter-table-drop-table-in-mysql/#:~:text=Step%20%23%205%3A%20Create%20a%20Table,you%20want%20for%20your%20table>.

<https://cryptii.com/pipes/caesar-cipher>

<https://crackstation.net/>