STANLEY ONYEDIKA EPUNA

STUDENT ID: 45731365

CTF REPORT 2

16TH MAY 2020

ABSTRACT

Capture the Flag (CTF) competitions allow students to learn cybersecurity skills in a fun and engaging way. It is an effective platform to increase students' interest in cybersecurity and prepare them for defending against real cyber attackers. A typical CTF competition requires at least some basic technical security knowledge and months of diligent preparation. The primary goal is to teach students with little or no technical knowledge about the different cybersecurity challenges that a cybersecurity professional must address and the problem-solving skills needed for a cybersecurity career, all without direct use of technology

1. Introduction

This report contains some technical writeups of the CTF2 task. It's a well written technical detail to reproduce the captured flags.

This CTF 2 commenced on the 5th of May 2020, 10:00 AM with its finish time set at 12:00 PM. We were provided with 6 tasks to complete. We had to input the flag results on the mobi.science.mq.edu.au server to correlate our result.

To be able to connect and start working on the tasks, the VPN hosted by MQ needed to be fully working so we could access the CTF website (10.46.225.208).

This challenge we did was a Web CTF which comprises of 6 tasks with flags in them.

This report was completed by Stanley-TEAM 16 on the 16th of May 2020. This exercise focused on using a web browser and some tools to get your flags. These flags can be gotten under a Windows environment, but it is best used on a Linux environment which has suitable web penetrating tools that could help get the flags.

Connection methods:

1. The entry point to the network is using a Macquarie University VPN
2. The server where the flags would be submitted: https://moby.science.mq.edu.au
3. The server where we would find our Task and Flags: https://10.46.225.208

The method needed for Burp Suite to work:

1. Burp suite needs to be installed in your kali Linux environment.
2. Configure burp suite for your web browser (Firefox) using Foxy Proxy.

Team Members

i. Stanley Onyedika Epuna
ii. Divya Kaur
iii. Abhishek Sobti
iv. Sadiq Abuwala Mohammad
v. Ayush Wadhwa

Flags:

Flag1 (INDICIES):

Overview

This flag reference manipulating the website address and altering figures using burp suite:

Method used:

Firstly, since this is Web exploitation, its best we check the page source for some clues, so in the source file, we may use burp suite to alter the incoming packets.

The web exploiting tool Burp suite was used to alter the incoming packet of the website (http://10.46.225.208/index.html) to manipulate it and forward it back to the web browser.

Once the burp suite is opened in the kali Linux environment, you will need to create a temporary project then stick with the default and start burp. Get back to the web browser and activate the foxy proxy to transfer the incoming packet of the website to Burp Suite.

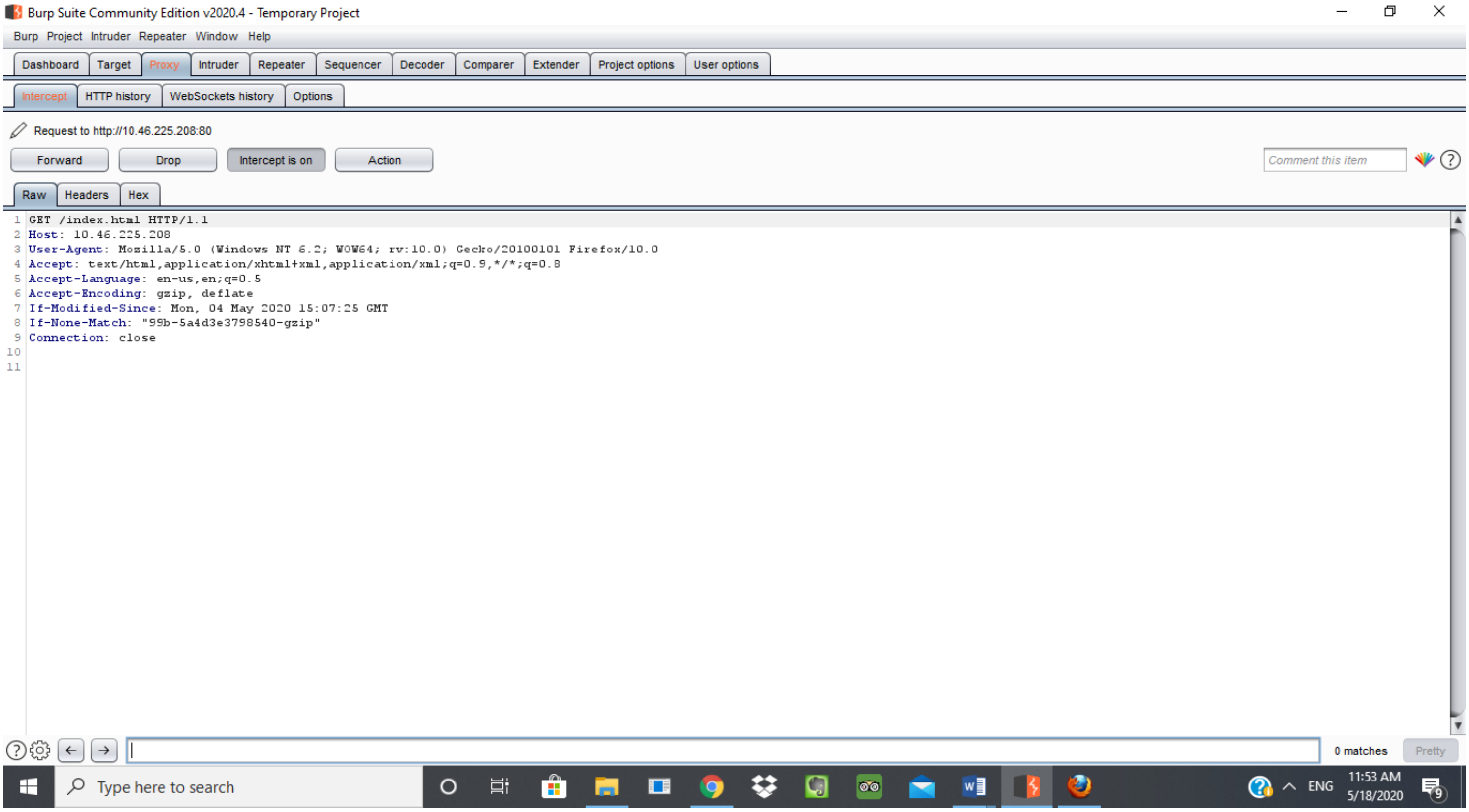
Now in the burp suite, the incoming packets have arrived. If you check the intercept in the proxy header you would see a parameter “If-None-match” with its values "99b-5a4d3e3798540-gzip". Removing the figures in the value and forwarding the packets back to the web browser reveals the Flag.

Flag reflection:

This Flag focuses on the importance of understanding how to use burp suite to alter the information gotten from the incoming packets from the website.

This Flag was solved by Sadiq Abuwala Mohammed.

I was not able to get this flag irrespective of me using the burp suite and also with the suitable practice of Natas over the wire exercises. I wasn’t able to figure out that removing the values in the parameter “If-Not-Match would get the flag. Instead what I tried doing was to copy those values thinking it was the password and inputting on the Moby scoreboard. Thanks to the swift intervention of my teammate who guided us on how it is done.


Burp Suite Community Edition v2020.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Comment this item
Raw Headers Hex
0 matches
Pretty
Type here to search
ENG
11:53 AM
5/18/2020

Request to http://10.46.225.208:80

```
GET /index.html HTTP/1.1
Host: 10.46.225.208
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:10.0) Gecko/20100101 Firefox/10.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
If-Modified-Since: Mon, 04 May 2020 15:07:25 GMT
If-None-Match: "99b-5a4d3e3798540-gzip"
Connection: close


```

FLAG 2 (BUSTED):

Overview:

In this task, to access the flag we need help from a user.

To solve this task, we need to deploy a web penetrating tool called Nmap Automator to get the directories of files located in the webserver.

Run Nmap Automator in terminal: ./nmapAutomator.sh 10.46.225.208 Vulns (to scan for vulnerabilities on the website).

After the scan I found out that flag3 and flag6 had vulnerabilities in them, also I found out there was a file called robots.txt. I decided to open the folder using: https://10.46.225.208/robots.txt

Then I saw a text which says user agent = * and disallowed: /json/. In this case, I need to access the JSON folder and change the user agent to *.

I accessed the website: https://10.46.225.208/json and turned on Foxy Proxy so I could get the incoming packet to Burp suite. In Burp suite I changed the user agent as it was mention in the robots.txt directory and forwarded it back to the web browser but I was not still able to access the JSON directory. I tried my best to access that folder by using other techniques like Nmap full scan but no avail.

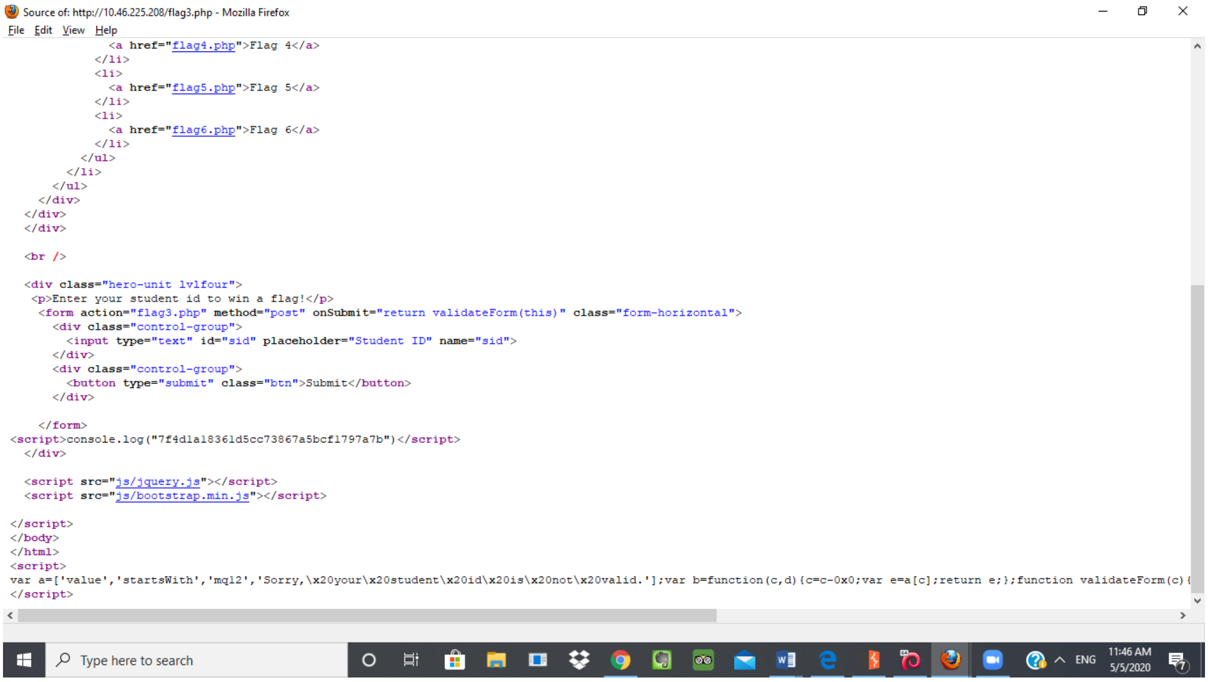
FLAG 3 (CONSOLATION PRIZE):

Overview

In this task, it is expected that you input your Student ID to get the flag.

Method Used:

It is needed to go to the Page source (ctrl +U) to get a hint on how to solve the flag. In the page source, it stated you need to enter your student ID and password to be able to get the flag, Once the details have been inputted and the login is Ok. View the page source again and the password is visible on the “console.log” script.



```
              <a href="flag4.php">Flag 4</a>
            </li>
            <li>
              <a href="flag5.php">Flag 5</a>
            </li>
            <li>
              <a href="flag6.php">Flag 6</a>
            </li>
          </ul>
        </li>
      </ul>
    </div>
  </div>
  </div>

  <br />

  <div class="hero-unit lvlfour">
   <p>Enter your student id to win a flag!</p>
    <form action="flag3.php" method="post" onSubmit="return validateForm(this)" class="form-horizontal">
      <div class="control-group">
        <input type="text" id="sid" placeholder="Student ID" name="sid">
      </div>
      <div class="control-group">
        <button type="submit" class="btn">Submit</button>
      </div>

    </form>
<script>console.log("7f4d1a18361d5cc73867a5bcf1797a7b")</script>
  </div>

  <script src="js/jquery.js"></script>
  <script src="js/bootstrap.min.js"></script>

</script>
</body>
</html>
<script>
var a=['value','startsWith','mql2','Sorry,\x20your\x20student\x20id\x20is\x20not\x20valid.'];var b=function(c,d){c=c-0x0;var e=a[c];return e;};function validateForm(c){
</script>
```

The flag: 7f4dlal836ld5cc73867a5bcfl797a7b

<u>Flag reflection</u>:

This Flag was gotten by team member: Divya Kaur

I tried putting in my student one-id username and password and the login was failed. So, it was confusing not to get the task. All thanks to Divya who was swift on getting the flag.

FLAG 4 (SECRET AGENT):

Overview:

To be able to solve this task you need to change the web browser to “mosaic 3 and above”.

Firstly, turn on Foxy Proxy on your Web browser and reload the page so the incoming packet would be directed to burp suite. Click on the burp suite and you could see the incoming packet. Locate where the user agent parameter is and change it to “mosaic 3 and above” and then forward back the packet to the web browser.

Then a new page was displayed in the web browser with Login and password details. For the login details, I searched google on how to get the username and password. When I put the details username: god2 and password:12345 I got a text: }1e3f82955284124205089decab {4galf- but I did not successfully get the password.

Reflection

We could not get this flag, but Stanley and Mohammed tried their best to get up to this point in the flag. This flag reminds me of a task in Natas where burp suite was used to alter the user-agent parameter to be able to get the password for the required level.

FLAG 6 (DO YOU LIKE SEQUELS):

Open the page source to figure out any hint of this specific task. We had to figure out the username and the password to have a successful login to the site. We as a group figured out to get the username and password which are ‘or’x’=’x and ‘or’x’=’x, when inputted I got the login success but was not able to crack and get the flag.

Reflection

On the course of the CTF, I realized it is a different type of challenge compared to the 1st CTF task which had to do with remote connection exploitation. It was told we aren’t to be concerned with the number of flags we get but we should understand steps are taken to get the flags or even if the flags aren’t gotten we should attempt the task, in that case, it will broaden our reasoning. Moreover, people only care about the flags but not the steps were taken to get the flags which are not a way to learn and practice. With this advice given to our teammates, it changed our thinking and perception on how to solve the task ahead.

During the CTF we were asked to solve 6 flags which we were only able to solve only two of them. Flag 2 and Flag 6 caught our attention because we saw examples on how to solve that particular task using the weekly NATAS exercises but was not successful with it. Honestly, I was not so satisfied with my performance in the group task but I was happy with the approach of my team members used in getting the flags.

Conclusion

This capture the flag task provides valuable experience in Web exploitation with different approaches being used to solve the problems. I was capable of doing some task which seems difficult at first, but thanks to the weekly practice I do on NATAS which helped build some skills and techniques in approaching the task. I may need to develop myself more in more exercise on a web penetration test to be able to challenge myself in the next CTF challenge coming up.

In this CTF there were not any ethical implications since it was hosted by Macquarie University. If it was carried out in a real situation there could be some legal breach and repercussion. I am glad I could be able to practice this CTF challenge which could help me build up myself in the task ahead.