# Step by Step Solution with Screenshots

## Question Analysis

### Description

A screenshot of a computer screen

Description automatically generated with medium confidence

Figure 3 CTF Question

The username is godam, as stated in the description. This information will be used as an additional hint to solve this challenge later on.

### First Hint

A screenshot of a computer

Description automatically generated

Figure 4 CTF Hint 1

As for this hint, it stated that the password is encrypted with MD5 hash.

### Second Hint

A screenshot of a computer

Description automatically generated

Figure 5 CTF Hint 2

Regarding this hint, it stated that the author will need to examine the redirecting request during the login process.

## Developer tools analysis

A screenshot of a login box

Description automatically generated with medium confidence

Figure 6 Login Page

A screenshot of a computer program

Description automatically generated with medium confidence

Figure 7 Source Code for login page

In the beginning of the challenge, this login page will be the first interface which the user will be interacting with. However, there is not much information given on this page despite looking through developer tools.

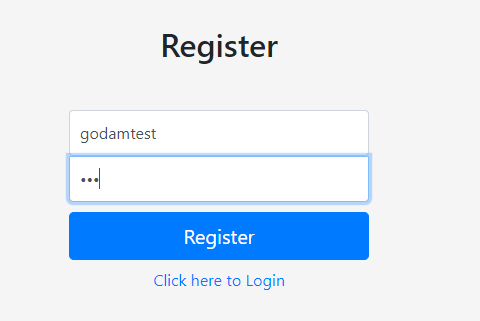


Figure 8 Registration Page

A picture containing text, screenshot

Description automatically generated

Figure 9 Source Code for registration page

On the registration page, the source tab is similar to the login page where the information given indicates the password that is entered by the author will be encrypted with MD5 hash on form submit.

A screenshot of a computer program

Description automatically generated with medium confidence

Figure 10 Profile Page with source code

After logging into the system with the recent created account, the author noticed that the system stores the md5 hashed password in the profile page’s source code for authentication purpose. However, storing sensitive information on client side makes it a potential vulnerability.

## BurpSuite analysis

As hint 2 stated that it is necessary to look at the request redirection when login. So, BurpSuite, a web exploitation tool will be used for the upcoming analysis because one of the tools provided by BurpSuite, Burp Proxy, is to intercept HTTP requests and allow users to view or modify them before sending them to the target server (PortSwigger, 2023).

A screenshot of a computer

Description automatically generated

Figure 11 BurpSuite

The first request which the author will be intercepting is the login page’s form submit request. To start the interception process, the author will turn on the intercept mode on BurpSuite and intercept the request after submitting the login form.

A screenshot of a computer

Description automatically generated with medium confidence

Figure 12 Intercepted Login Request

This is the intercepted request where the author can view and modify. The intercepted request shows the username and password that has been used to login.

A screenshot of a computer

Description automatically generated with medium confidence

Figure 13 Redirected Request

A screenshot of a computer

Description automatically generated

Figure 14 Send to Intruder

Then, the next redirecting request will include a session id for login purpose. This will be a vulnerability as the author is able to modify the session id in order to impersonate someone else. Although the session id for this newly created account justified that the possible id range for the targeted account is from 1 to 6. However, to relate to real life scenarios, the author may need to test thousands of ids in order to hijack the session. So, the author will have to use another BurpSuite tool, Intruder to brute force the session id. In order to do so, the author will need to send the request to intruder.

## Attack with BurpSuite Intruder

A screenshot of a computer

Description automatically generated

Figure 15 BurpSuite Intruder

A screenshot of a computer

Description automatically generated with medium confidence

Figure 16 Pitchfork

Select PitchFork as the attack type because PitchFork mode allows multiple payloads, all the three session ids and account id are highlighted with the § symbol to indicate that they are the payloads position (Portswigger, 2023).

A screenshot of a computer

Description automatically generated

Figure 17 Set Payloads

Then, set the payload type to number for all payloads with sequential number from 1 to 7.

A screenshot of a computer

Description automatically generated

Figure 18 Set Redirections

Then, tick the On-site only option under Redirections section so BurpSuite will return all the redirected requests and responses.

A screenshot of a computer

Description automatically generated

Figure 19 Set Grep

As the first page after the author logged in display the username, so the author did an assumption that the server response might include the username “godam” in the HTML code so the author added a grep function where BurpSuite will highlight the result that has the word “godam”.

A screenshot of a computer

Description automatically generated with medium confidence

Figure 20 Start Attack

Start the attack.

A screenshot of a computer

Description automatically generated with medium confidence

Figure 21 Attack Result

This is the attack result. As the author has added a grep function, BurpSuite will return a block of code under godam column for any matching value. Based the figure above, the author will know that the request that uses session id of 5 will login to godam’s account.

A screenshot of a computer

Description automatically generated with medium confidence

Figure 23 Modify request

So, go back to BurpProxy where the author can modify the session id to 5.

A screenshot of a computer screen

Description automatically generated with medium confidence

Figure 24 logged in as godam

After forwarding the request, the author has been successfully logged into godam’s account.

A screenshot of a computer

Description automatically generated

Figure 25 find md5 hashed password

As mentioned above, the first vulnerability of this system is that the md5 hashed password is stored in the source code of the profile page, so the author is able to get godam’s hashed password which is 8d1beddb87179b224441ce3a7a66c6a9.

A screenshot of a computer

Description automatically generated

Figure 26 modify url

A screenshot of a computer

Description automatically generated

Figure 27 found flag

Next, go to the index.php where the flag is stored. Enter the hashed password as the argument for the password parameter in the URL, the author will then get the flag.

# Justification

As shown in the step-by-step solution, the author did 2 main analyses to find the vulnerabilities of the system in order to find the flag. First of all, developer tools analysis. Developer tool is a tool that is available in most web browsers like Chrome, Firefox and more that provides the feature to inspect the source code, local session, and much more (Nobledesktop, n.d.).

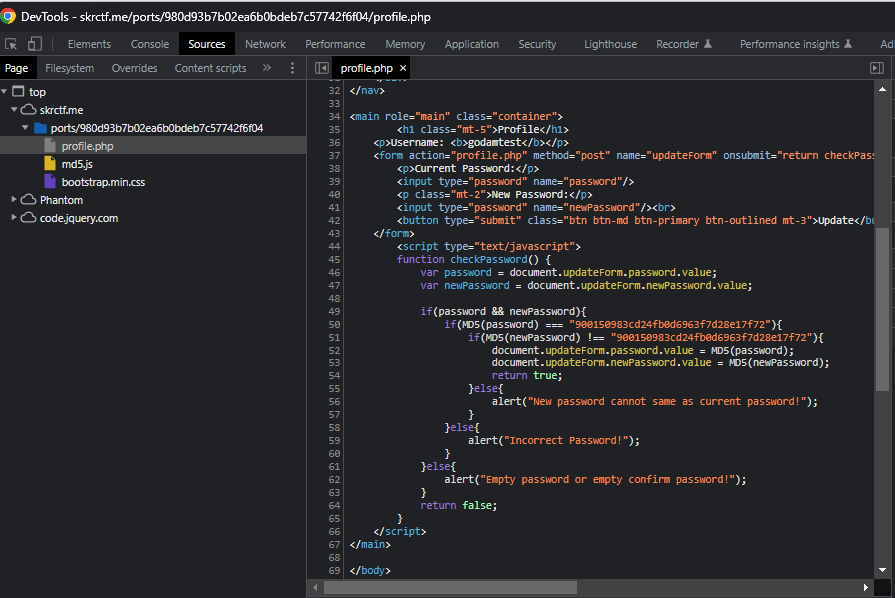


Figure 28 Source Tab

However, in the flag capturing process, the only useful vulnerability that has been mentioned previously is located in the source code which the author can find it via the code. The author can inspect the HTML, CSS, and JavaScript under the source tab, which can provide the author an insight into the system (Howard University CyberSecurity Center, n.d.).

Secondly, HTTP request inspection using BurpSuite. As mentioned above, BurpSuite is a set of web penetration tools whereas the author has used two provided tools which includes BurpSuite Proxy and BurpSuite Intruder to perform analysis and attack to the web application respectively. Firstly, the author has used BurpSuite Proxy as its feature is to intercept the requests and responses of the web application to view and modify the content (GeeksForGeek, n.d.), this is where the author can analyse the possible vulnerabilities in the request or response. Secondly, BurpSuite Intruder is a tool to perform bruteforce or dictionary attack in input field, HTTP request and more (Kucukkarakurt, 2022). Hence, the author has used BurpSuite Intruder to hijack godam’s session.