Introduction

This report will be mainly delivering the writeup that is created based on “Web Exploitation” category. This writeup will include the source of challenge, selected challenge, step by step solution that comes with explanation, justification, analysis as well as proper screenshots to support the statements. Other than that, the tools and scripts that are being used throughout the flag capturing will be explained in detailed.

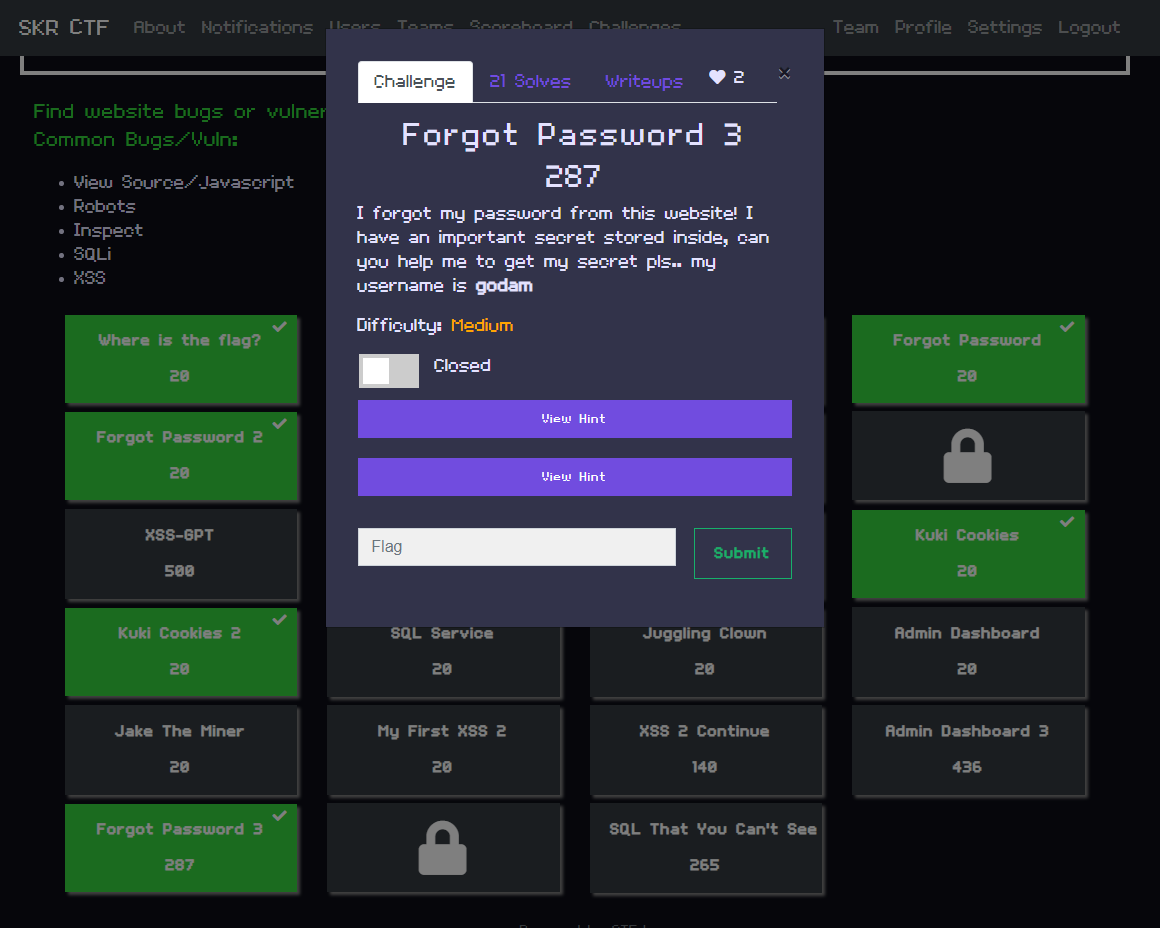
Source of Challenge

A screenshot of a computer

Description automatically generated

Later work

Selected Challenge



As the selected category for this report writing is Web Exploitation, the author opts for the “Forgot Password 3” challenge from SKRCTF. The difficulty of this challenge is Medium and only 21 challengers manage to solve this question. However, necessary tools and scripts will be wisely utilized throughout the flag finding process and they will be mentioned below along with appropriate step by step solutions.

Step by Step Solution with Screenshots

Analysis

Description

A screenshot of a computer screen

Description automatically generated with medium confidence

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

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

Second Hint

A screenshot of a computer

Description automatically generated

Regarding this hint, it stated that the author will need to examine the redirecting request during the login process, so BurpSuite, a web exploitation tool, will be considered as an essential tool to use during the exploitation process, with the justification explained later.

Source tab analysis

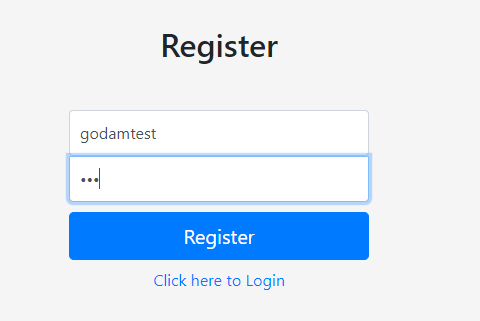
A screenshot of a login box

Description automatically generated with medium confidence

A screenshot of a computer program

Description automatically generated with medium confidence

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 the source tab where elements, sources, network, and application data reside. Hence, the author will click the link provided below the form, which will redirect the author to a registration page from which the author can attempt to find vulnerabilities.



A picture containing text, screenshot

Description automatically generated

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 when the form is submitted.

A screenshot of a computer program

Description automatically generated with medium confidence

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

BurpSuite analysis

A screenshot of a computer

Description automatically generated

As the hint stated that it is necessary for the author to look at the request redirection of the page. So, BurpSuite will be used for the upcoming analysis because one of the features 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).

After registering, say u check all page d only profile page source got store md5 which is one vulnerability, then try to intercept login and say new acc id start with 6 so we just need to bruteforce from 1-5 then say 5 is godam then get the md5 from the home page then enter in url then bomb got the flag

Exploitation with burpsuite

Justification

Conclusion