CSOC 1030: Assignment #5

August 02, 2023

**Prepared By**: *Ashish Kishor Hedau*

Table of Contents

[Exposure of ‘Swagger File’ due to client-side implementation and weak password recovery mechanism for ‘Forgotten Password’ 2](#_Toc137283759)

[Description 2](#_Toc137283760)

[Impact 2](#_Toc137283761)

[Recommendations 2](#_Toc137283762)

[Steps to Reproduce 3](#_Toc137283763)

# Exposure of ‘Swagger File’ due to client-side implementation and weak password recovery mechanism for ‘Forgotten Password’

## Description

The assessed web application “<http://10.5.30.50>” is a simple login page with Username and Password field, and a recover option with Username and a 4-digit recovery pin. The web application is designed in a way in which an ‘attacker’ can’t get access without a valid username. The recovery option is meant to be an alternative access method for legitimate users who have forgotten their passwords. It is essential to keep the recovery pin secure and not share it with anyone, as it could be used to reset the password and gain unauthorized access if in the hands of an attacker.

## Impact

A malicious actor could get hold of client-side ‘swagger’ file which in the context of API (Application Programming Interfaces) describes the API’s structure, endpoints, request/response formats, authentication requirements, and other important information. In this scenario, the attacker could get hold of valid usernames by browsing through directories mentioned in the ‘swagger file’. Consequently, they could brute force the PIN field in the ‘recovery option’ to get unauthorized access and hence compromising the web application.

**Note: CWE-200** Exposure of Sensitive Information to an Unauthorized Actor (<https://cwe.mitre.org/data/definitions/200.html>)

**CWE-640** Weak password recovery mechanism for Forgotten Password (<https://cwe.mitre.org/data/definitions/640.html>)

## Recommendations

Ensure the ‘swagger file’ is not accessible to the public. It should be accessible only to authenticated and authorized users. Restrict access to the file using proper server-side authentication and authorization mechanisms. Implement OTP on the recovery option as the current 4-digit PIN implementation can be brute forced using proxy.

## Steps to Reproduce

The assessed application ( <http://10.5.30.50> ) was found to have a login type functionality that requires a user to submit an email and a password to login. The main login page also has a redirect link to a forgotten password page when a user clicks the “Click here” link.

![A screenshot of a login screen

Description automatically generated]()

The image below shows the page when a user clicks the ‘Click here’ link on the main login page gets redirected on this. Here, a user can recover his/her password by simply entering the username and a permanent 4-digit PIN.

![A screenshot of a computer

Description automatically generated]()

We started the enumeration by brute forcing the directories by using dirsearch. The command used here was ‘**dirsearch -u** [**http://10.5.30.50/api**](http://10.5.30.50/api)’. As the brute force was complete, we found the ‘swagger file’.

.

![A screenshot of a computer

Description automatically generated]()

The below image shows the excerpts from the downloaded ‘swagger file’. It contained some critical paths to the list of all usernames (**/debug/users**) and disabled usernames (**/debug/users/disabled**).

![A screenshot of a computer program

Description automatically generated]()

Here, it displays the disabled usernames from the path we found earlier.

![A screenshot of a computer

Description automatically generated]()

Here, the image shows the usernames we got by opening the directory (**/api/debug/users**). [mike@marines.mil](mailto:mike@marines.mil) is highlighted as his account is still enabled, the other been Linda Johnson (linda@fbi.gov).

![A screenshot of a computer

Description automatically generated]()

We used Burpsuite as the proxy to find the 4-digit PIN to recover the password. The highlighted target is shown below in the red box.

![A screenshot of a computer

Description automatically generated]()

The payload list is added starting from (0000-9999) which is already available in Burpsuite.

![A screenshot of a computer

Description automatically generated]()

As highlighted below in red, we were successfully able to find a ‘200’ response for the PIN **0159.**

![A screenshot of a computer

Description automatically generated]()

We went back to the recover password page with [mike@marines.mil](mailto:mike@marines.mil) as the username and 0159 as the 4-digit Recovery Pin. As from the image below we got **geLngc@ygnYk** as the new password.

![A screenshot of a computer

Description automatically generated]()

Here we used the new Password we generated with the recovery PIN option.

![A screenshot of a login box

Description automatically generated]()

As seen in the image below, we were successfully able to login to the environment with the credentials.

![A screenshot of a computer

Description automatically generated]()