Don Bosco Institute of Technology, Kurla (W), Mumbai – 400070
Department of Information Technology
Secure Application Development Lab

Roll no.: 52 **Date**: 22/ 09 / 2024

Name: Afzal Siddiquie

Experiment No. 5

Aim: Demonstrate CSRF vulnerability using DVWA.

Objectives: The objective of this experiment is to

- Understand and Identify CSRF vulnerabilities in applications.

Outcomes: After study of this experiment, the student will be able to

- Identify CSRF vulnerabilities in application.

Prerequisite: Knowledge of Vulnerabilities and HTTP protocol and commands.

Requirements: PC and Internet

Brief Theory:

Cross-site request forgery (CSRF)

Cross-site request forgery (also known as CSRF) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform. It allows an attacker to partly circumvent the same origin policy, which is designed to prevent different websites from interfering with each other.

What is the impact of a CSRF attack?

In a successful CSRF attack, the attacker causes the victim user to carry out an action unintentionally. For example, this might be to change the email address on their account, to change their password, or to make a funds transfer. Depending on the nature of the action, the attacker might be able to gain full control over the user's account. If the compromised user has a privileged role within the application, then the attacker might be able to take full control of all the application's data and functionality.

How does CSRF work?

For a CSRF attack to be possible, three key conditions must be in place:

- **A relevant action.** There is an action within the application that the attacker has a reason to induce. This might be a privileged action (such as modifying permissions for other users) or any action on user-specific data (such as changing the user's own password).
- **Cookie-based session handling.** Performing the action involves issuing one or more HTTP requests, and the application relies solely on session cookies to identify the user who has made the requests. There is no other mechanism in place for tracking sessions or validating user requests.
- **No unpredictable request parameters.** The requests that perform the action do not contain any parameters whose values the attacker cannot determine or guess. For example, when causing a user to change their password, the function is not vulnerable if an attacker needs to know the value of the existing password.

Laboratory Exercise

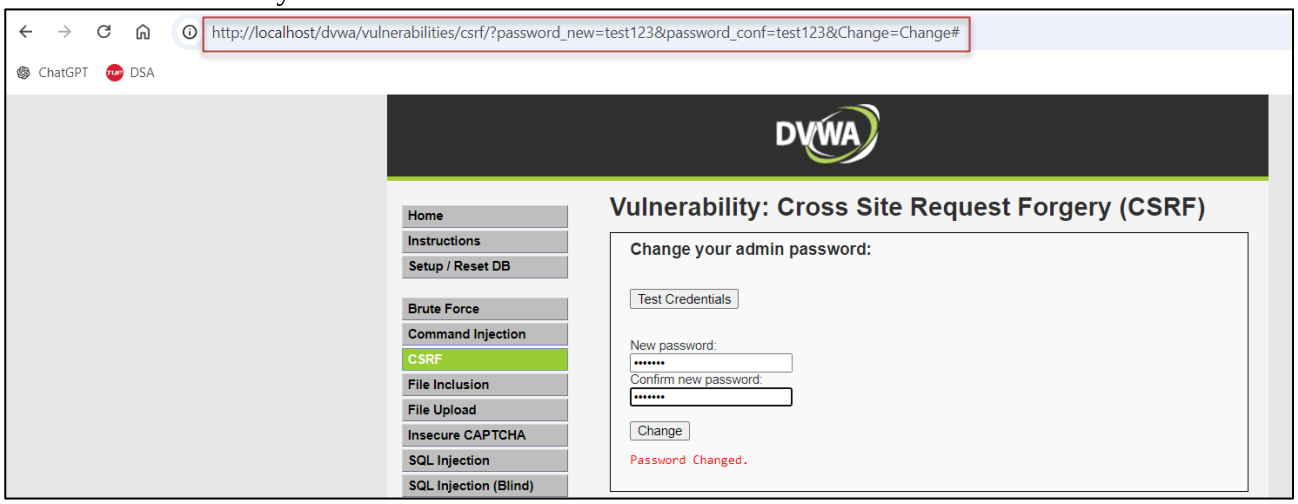
1. Follow step by step process for available in the following URL:

https://docs.google.com/document/d/10DVGOmEWyXGnEPYjAhcoglnxQL5U3sM-/edit?usp=sharing&ouid=105710360085268780210&rtpof=true&sd=true

2. Add the screenshot of your output.

Copy the form tag code into the notepad

Change your password and click “Change” and then
Select the URL from your browser



http://localhost/dvwa/vulnerabilities/csrf/?password_new=test123&password_conf=test123&Change=Change#

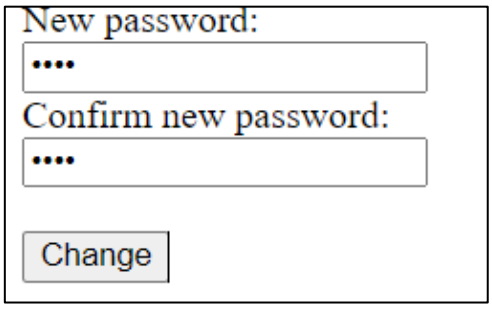
Add the above URL to form action after changing the password

```
<body>
    <form action="http://localhost/dvwa/vulnerabilities/csrf/?password_new=test123&password_conf=test123&Change=Change#" method="GET">
        New password:<br />
        <input type="password" AUTOCOMPLETE="off" name="password_new"><br />
        Confirm new password:<br />
        <input type="password" AUTOCOMPLETE="off" name="password_conf"><br />
        <br />
        <input type="submit" value="Change" name="Change">

    </form>
</body>
```

Now run the file, This file acts as our malicious link which is used for CSRF.

Now , suppose the user wants to change password to “test123” and clicks on the change button, the actual password value is “test123” and not “test”. But the account is updated with “test” on the target system, since our malicious script is running, the password values are changed to what the attacker wants. In our DVWA page, it will show a “Password changed” message.



Now try logout and login again with a changed password “test123”. Login will fail. Now try with password test. It will login. This is how CSRF attack take place.

Conclusion: Understood what is CSRF attack and how is it carried out.

Mention your References:

01. http://localhost/dvwa/vulnerabilities/csrf/
02. https://docs.google.com/document/d/10DVGOmEWyXGnEPYjAhcoglnxQL5U3sM-/edit