

# 10. CSRF

Disusun oleh :

Chaerul Umam, M.Kom (chaerul@dsn.dinus.ac.id)

Hafidh Akbar Sya'bani (akbar@dinustek.com)

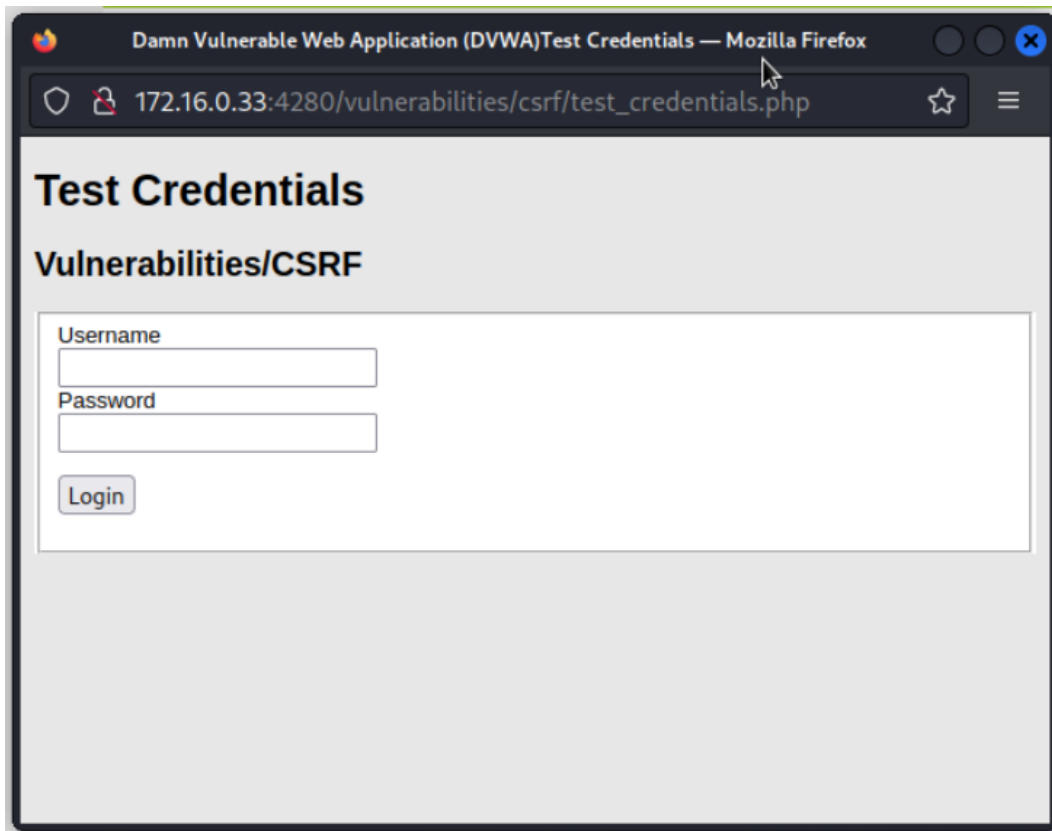


## CSRF (Cross Site Request Forgery)

Pada tampilan awal DVWA klik bagian CSRF

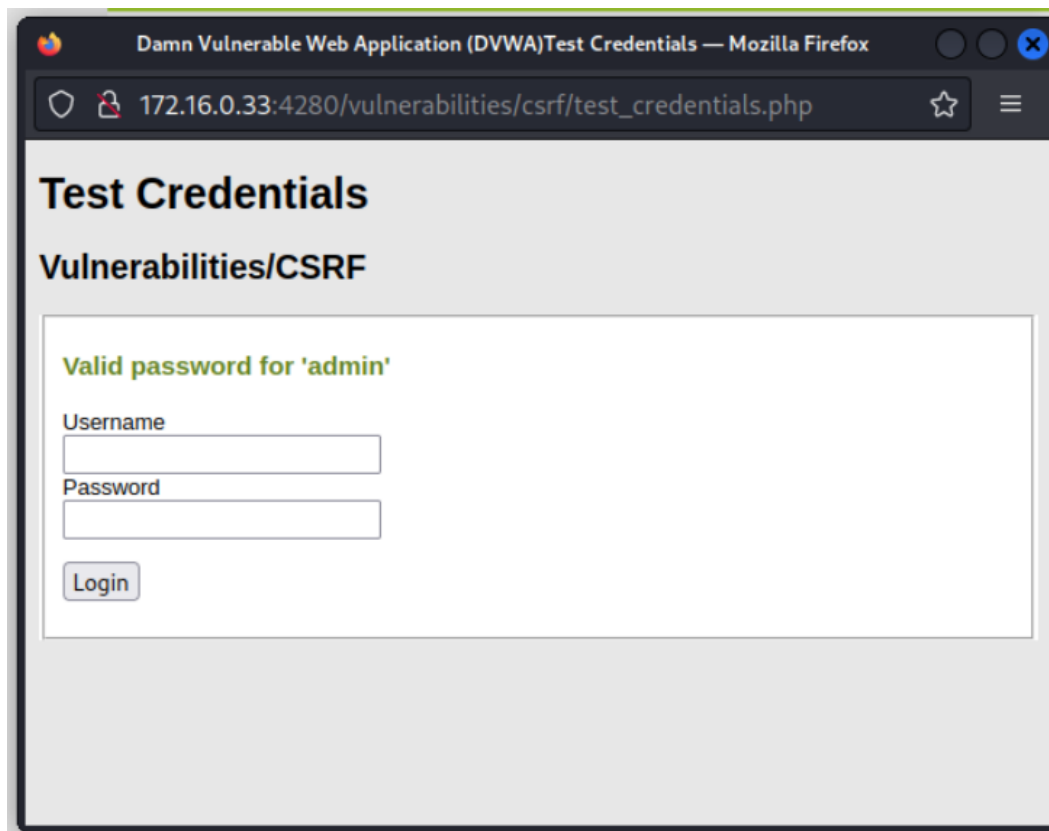
The screenshot shows the DVWA web application interface. At the top, there's a dark header with the DVWA logo. Below it, a sidebar on the left contains a list of vulnerability categories: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, **CSRF** (highlighted in green), File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), and CSP Bypass. The main content area is titled "Vulnerability: Cross Site Request Forgery (CSRF)". Inside this area, there's a box titled "Change your admin password:" containing a "Test Credentials" button, input fields for "New password:" and "Confirm new password:", and a "Change" button. Below this box, there's a note: "Note: Browsers are starting to default to setting the [SameSite cookie](#) flag to Lax, and in doing so are killing off some types of CSRF attacks. When they have completed their mission, this lab will not work as originally expected." At the bottom, there's an "Announcements:" section with a bulleted list: [Chromium](#), [Edge](#), and [Firefox](#).

Klik pada Test Credential, akan terbuka window baru menampilkan halaman login



Gunakan username dan password default

- Username: admin
- Password: password



Dapat diketahui username dan password saat ini adalah admin dan password. Tutup window login page dan kembali ke CSRF

Terdapat field untuk mengganti password akun sebelumnya pada halaman CSRF, disini password dari akun tersebut dapat diubah. Isikan kata apa saja untuk mengganti password lama dengan yang baru lalu klik Change.

## Vulnerability: Cross Site Request Forgery (CSRF)

**Change your admin password:**

Test Credentials

New password:  
newpassword

Confirm new password:  
newpassword

Change

Akan muncul teks bahwa password telah terganti

## Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

New password:

Confirm new password:

Password Changed.

Perhatikan pada URL yang baru setelah password diganti

```
http://172.16.0.33:4280/vulnerabilities/csrf/?password_new=newpassword&password_conf=newpassword&Change=Change#
```

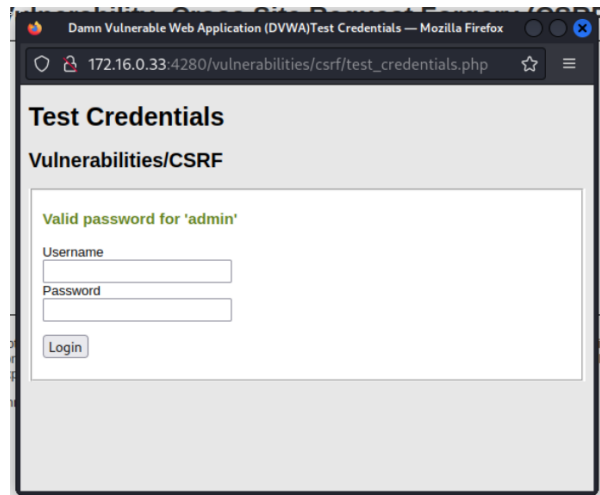
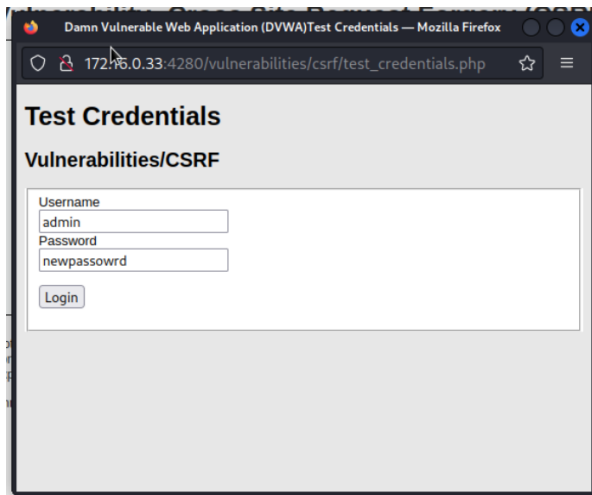
CSRF/XSRF bekerja dengan menipu sebuah website hingga seolah olah korban melakukan request kepada website.

Dapat dilihat bahwa password baru yang diketikkan akan masuk ke URL, terdapat 2 parameter yaitu:

- password\_new = newpassword
- password\_conf = newpassword

Pada web ini untuk mengganti password dapat dilakukan hanya dengan mengganti nilai pada 2 parameter diatas. Ini berarti hanya dengan mengakses URL tadi di browser korban yang masih memiliki cookie yang belum expired, password dari akun korban bisa diganti.

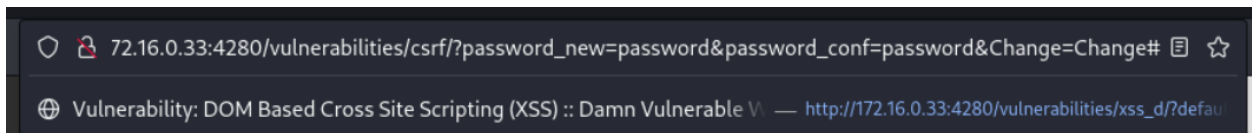
Coba login dengan password yang baru



Coba untuk kembalikan password seperti semula hanya dengan menggunakan URL saja, pertama ganti password menjadi password semula pada URL

```
http://172.16.0.33:4280/vulnerabilities/csrf/?password_new=password&password_conf=password&Change=Change#
```

Buka URL tersebut di browser



Password berhasil diganti

**Change your admin password:**

New password:

Confirm new password:

**Password Changed.**

Coba login menggunakan password yang baru saja diganti

Damn Vulnerable Web Application (DVWA) Test Credentials — Mozilla Firefox

172.16.0.33:4280/vulnerabilities/csrf/test\_credentials.php

**Test Credentials**

Vulnerabilities/CSRF

Username  
admin

Password  
password

Damn Vulnerable Web Application (DVWA) Test Credentials — Mozilla Firefox

172.16.0.33:4280/vulnerabilities/csrf/test\_credentials.php

**Test Credentials**

Vulnerabilities/CSRF

**Valid password for 'admin'**

Username

Password

Dengan metode ini pelaku CSRF mengisi password yang diinginkan dan mengirimkannya ke korban, saat korban membuka URL tersebut, website akan menyetujui cookie yang tersimpan di browser dan melakukan penggantian password pada akun korban. Selanjutnya pelaku dapat melakukan login ke akun korban dengan password yang telah diganti.

