10. CSRF

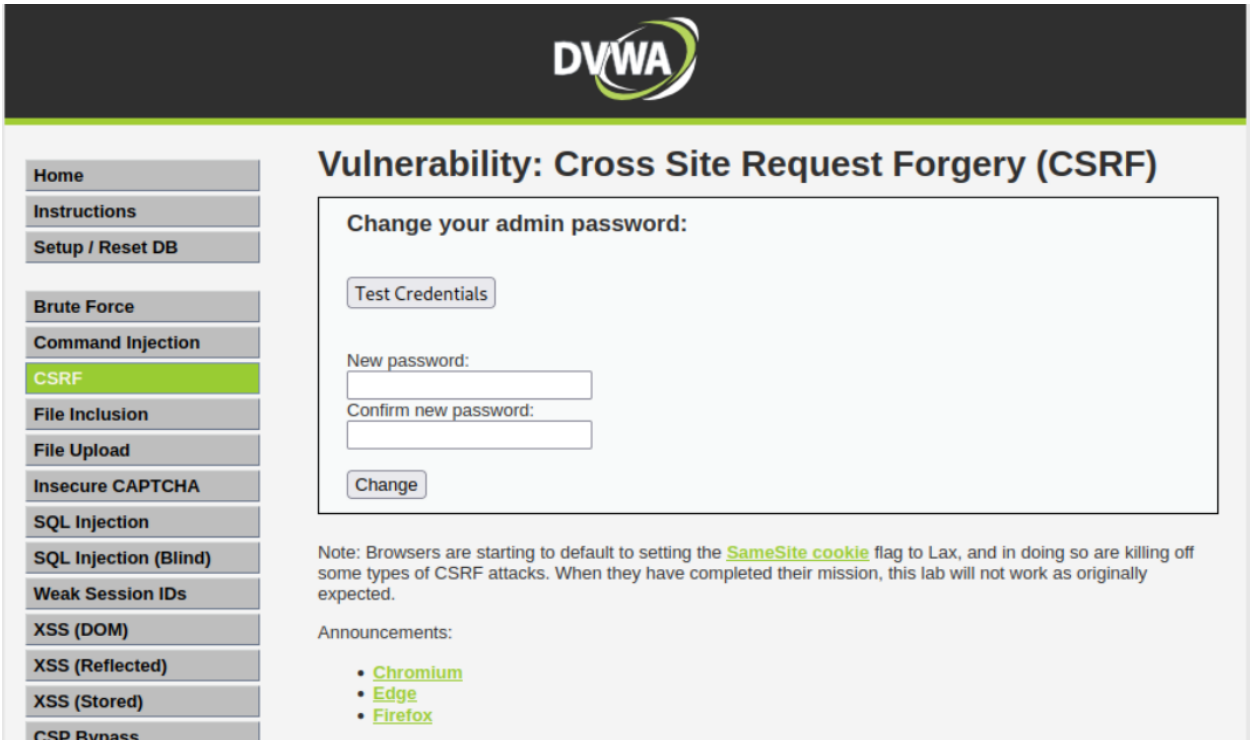
Disusun oleh :

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

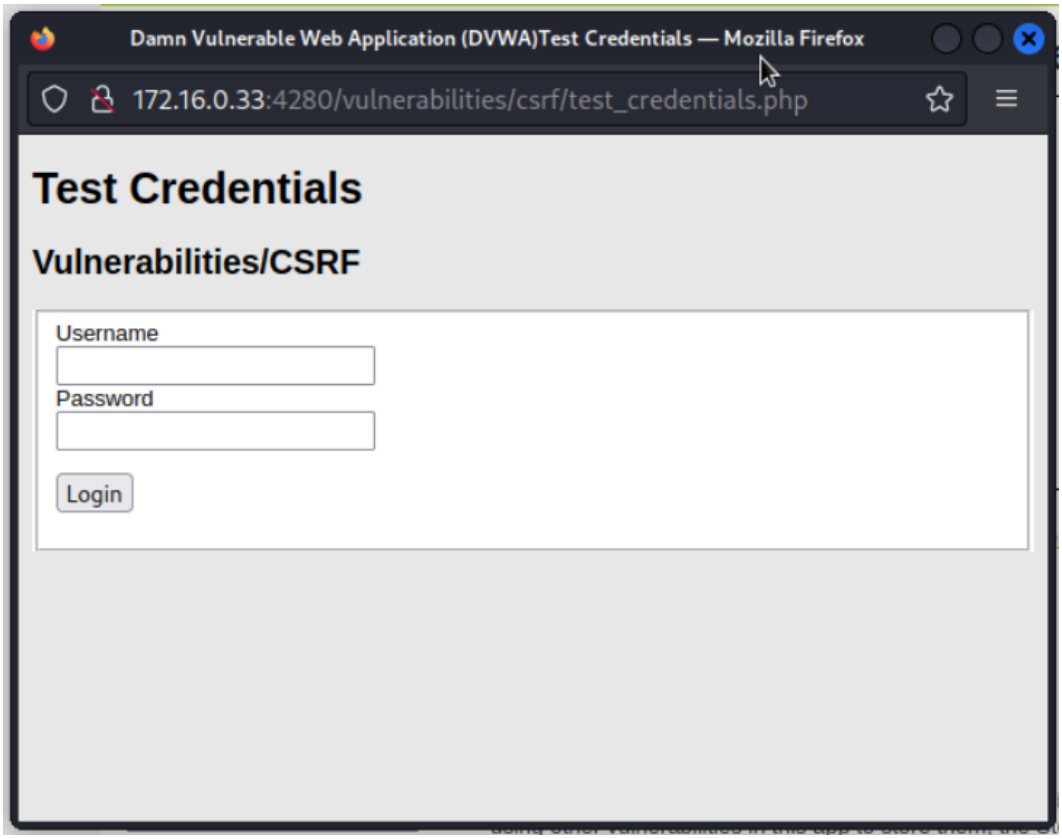
Hafiidh Akbar Sya'bani (akbar@dinustek.com)

☠️ CSRF (Cross Site Request Forgery)

Pada tampilan awal DVWA klik bagian CSRF

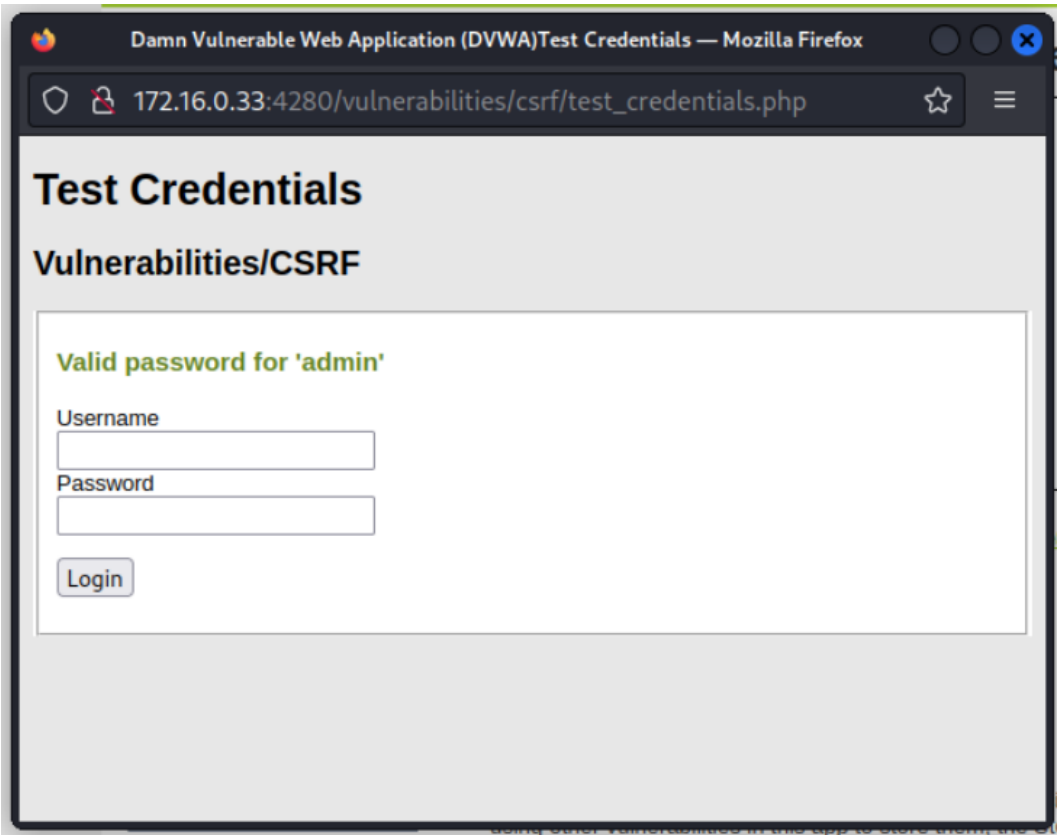


Klik pada Test Credential, akan terbuka window baru menampilkan halaman login



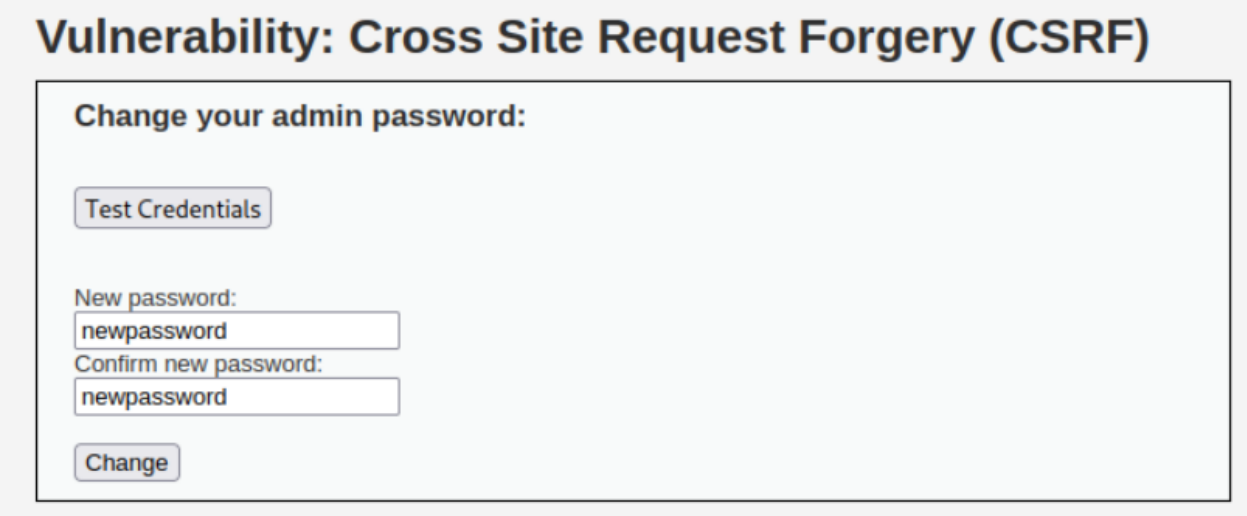
Gunakan username dan password default

- Username: admin
- Password: password

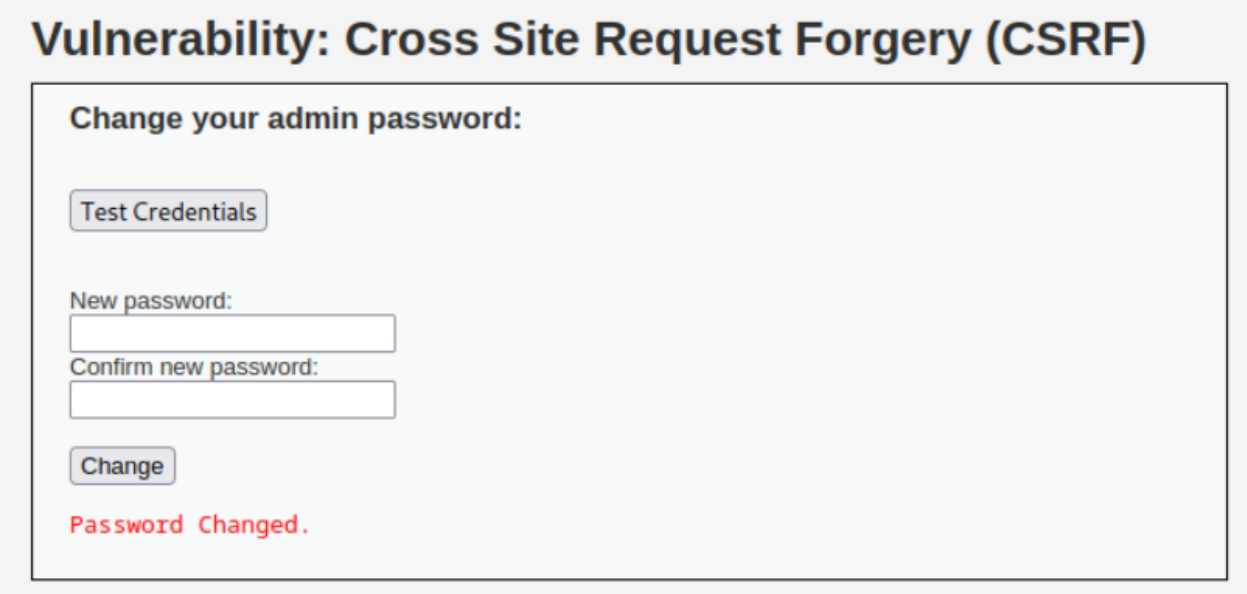


Dapat diketahui username dan password saat ini adalah admin dan password. Tutup window login page dan kembali ke CSRF

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.



Akan muncul teks bahwa password telah terganti



Perhatikan pada URL yang baru setelah password diganti

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

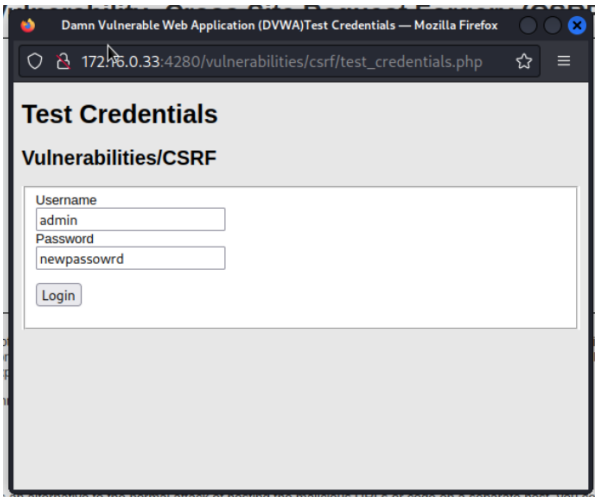
CSRF/XSRF bekerja dengan menipu sebuah website hingga seolah olah korban melakukan request kepada website.

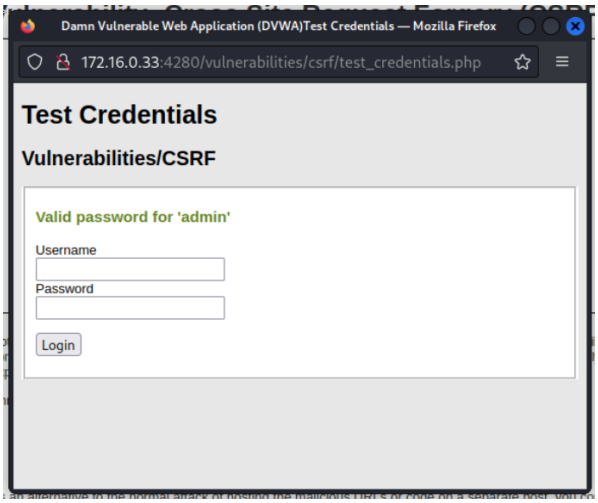
Dapat dilihat bahwa password baru yang diketikkan akan masuk ke URL, terdapat 2 parameter yaitu:

- 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

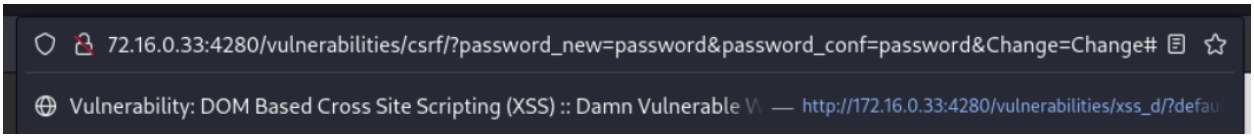




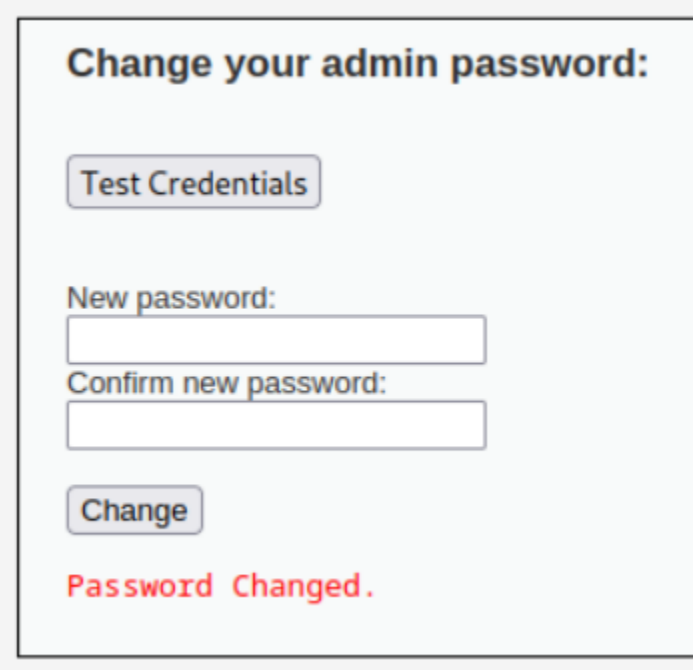
Coba untuk kembalikan password seperti semula hanya dengan menggunakan URL saja, pertama ganti password menjadi password semula pada URL

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

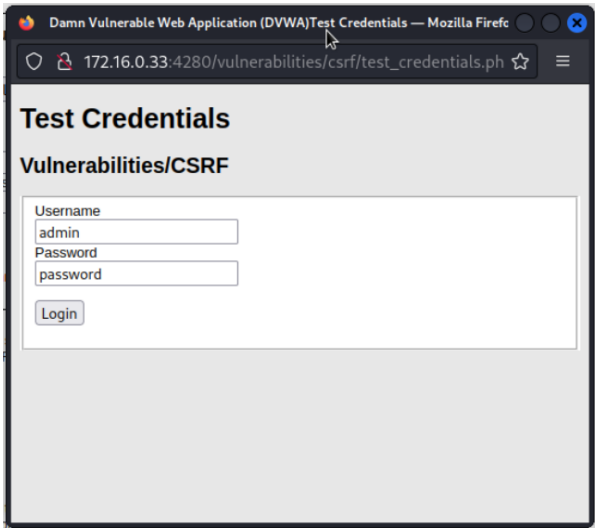
Buka URL tersebut di browser

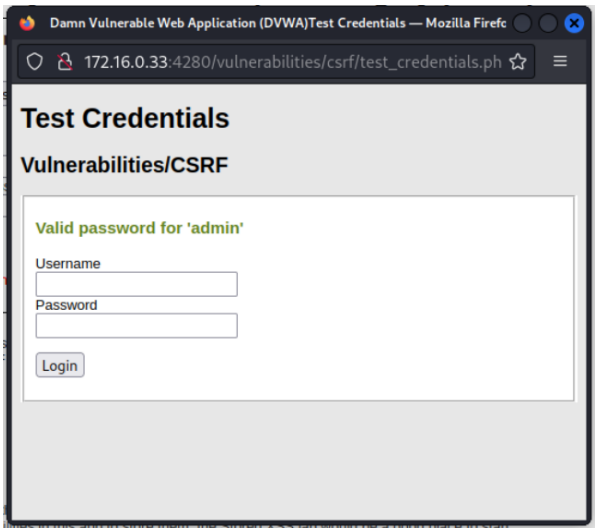


Password berhasil diganti



Coba login menggunakan password yang baru saja diganti





Dengan metode ini pelaku CSRF mengisikan 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.