# Securitatea Datelor

**Laboratorul nr.8: Cross Site Request Forgery**

**(CSRF)**

1CUPRINS:

1. Definiție ........................................................................................................................................... 3
2. Scenariu ........................................................................................................................................... 3
3. Impactul atacului CSRF .................................................................................................................... 3
4. Demonstrație atac CSRF .................................................................................................................. 4

## 1.DEFINIȚIE

Cunoscut și sub numele de cross site request forgery sau CSRF, poate fi folosit pentru a pacăli un utilizator autentificat să facă anumite modificări neintenționate pe site. Profită de încrederea pe care o oferă site-ul tău utilizatorilor deja autentificați.

## **2.** SCENARIU

* Boby navighează pe mysite.com, si este autentificat ca și utilizator legitim.
* Mysite.com are un buton, care atunci când este apăsat, vă trimite automat un ecard la toate contactele lui Boby salvate, automat cu un link.
* În timp ce Boby navighează, are o întrebare despre anumite funcții, și merge pe forumul favorit cu informații despre mysite.com – mysiteforums.com
* El deschide un articol interesant al unui alt utilizator. Acesta conține o etichetă cu imagine care arata in felul urmator: <img src=’http://www.mysite.com/send-ecards’/>
* Browserul lui Boby încearcă să încarce imaginea, și trimite datele de autentificare ale lui Bob împreună cu solicitarea pentru mysite.com/send-e-cards.
* Mysite.com primește cererea de la Bob pentru trimiterea e-card-ului, și o trimite.
* Atacul a fost realizat cu succes, chiar dacă Bob nu a apăsat niciodată butonul send.

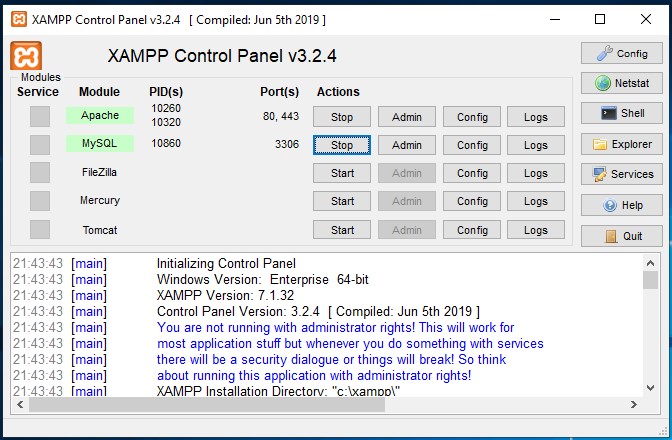
Acest tip de atac a fost utilizat cu succes în raspandirea virusilor, atat prin intermediul MySpace, cât si Facebook. Atacurile de aceasta natură, faciliteaza autopropagarea, deoarece atacă site-uri unde utilizatorii își stochează informații personale.

## 3.IMPACTUL ATACULUI CSRF

CSRF poate fi folosit pentru orice tip de atac, de la păcălirea unui utilizator pentru schimbarea parolei și până la retragerea de fonduri, dacă site-ul permite tranzacții cu cardul.

## 4.DEMONSTRAȚIE ATAC CSRF

* Pasul 1.Pornim modulele Apache și MySQL din XAMPP (necesare aplicației DVWA).



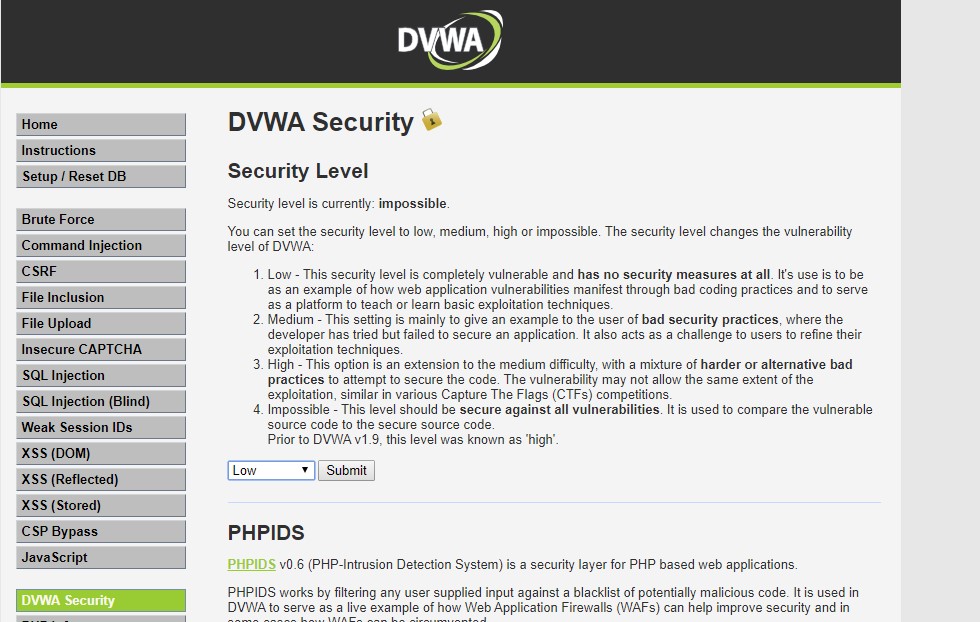
* Pasul 2. Accesăm aplicația dvwa cu browserul Mozilla Firefox <http://localhost/dvwa/login.php>



Ne autentificăm cu următoarele credențiale:

Username: admin Passsword: password

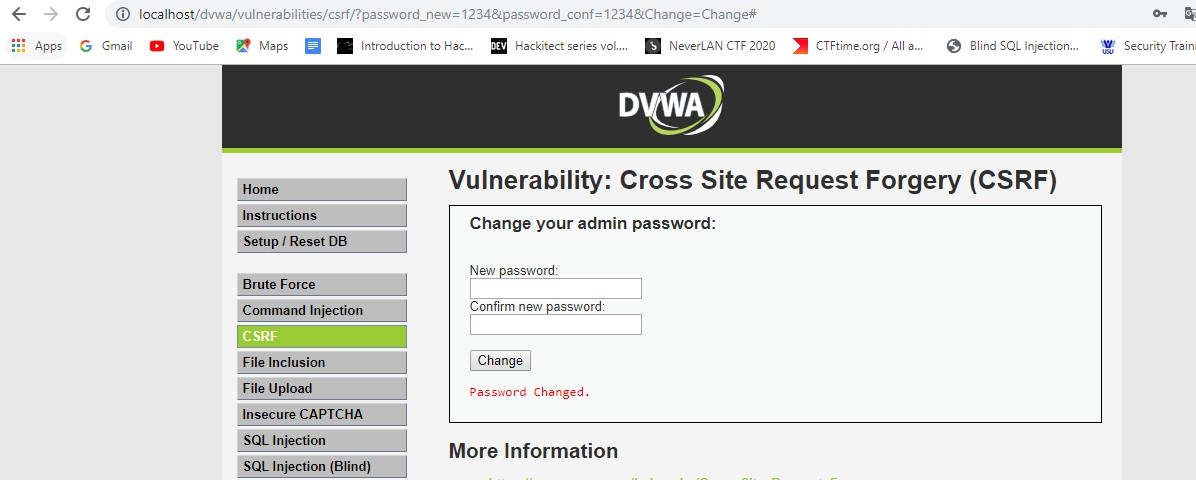
Pasul 3. Din tab-ul din partea stângă accesăm categoria DVWA Security – setăm nivelul de securitate Low și apăsăm butonul Submit



* Pasul 4. Selectăm din tab-ul din partea stăngă categoria CSRF



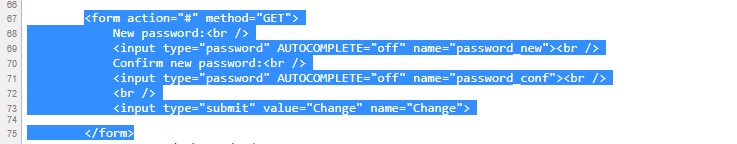
Pasul 5. Introducem o nouă parolă (ex:1234) și apăsăm butonul Change.



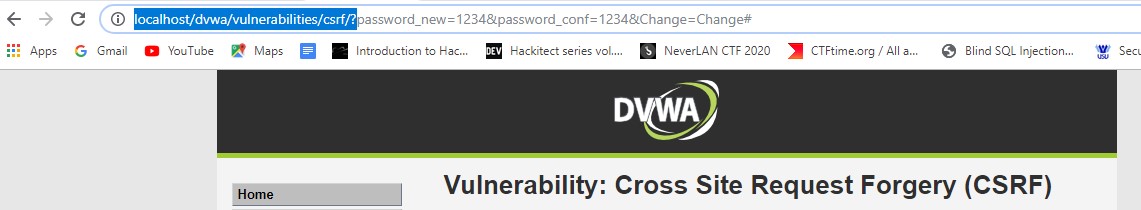
* Pasul 6. Apăsăm combinația de taste Ctrl+U (View page source)



Pasul 7. Copiem următoarea porțiune de cod

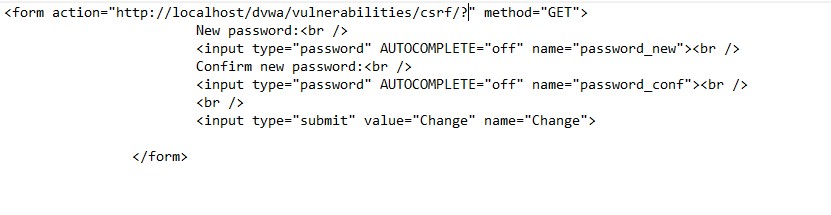


* Pasul 8. În codul copiat facem următoarea modificare:
  + Din url copiem următorul fragment

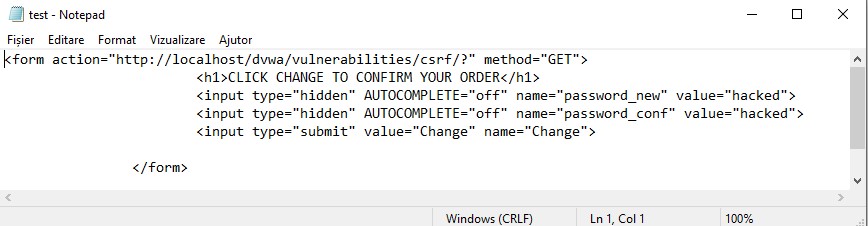


<http://localhost/dvwa/vulnerabilities/csrf/?>

* + Îl introducem în cod astfel (pe prima linie în loc de #)

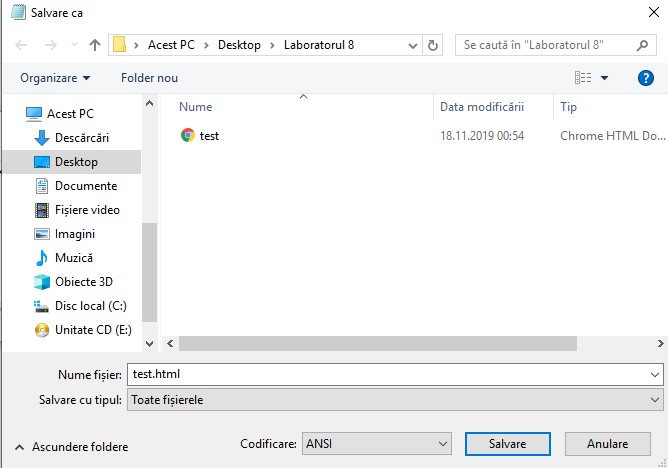


* + Moficăm codul ca în imagine

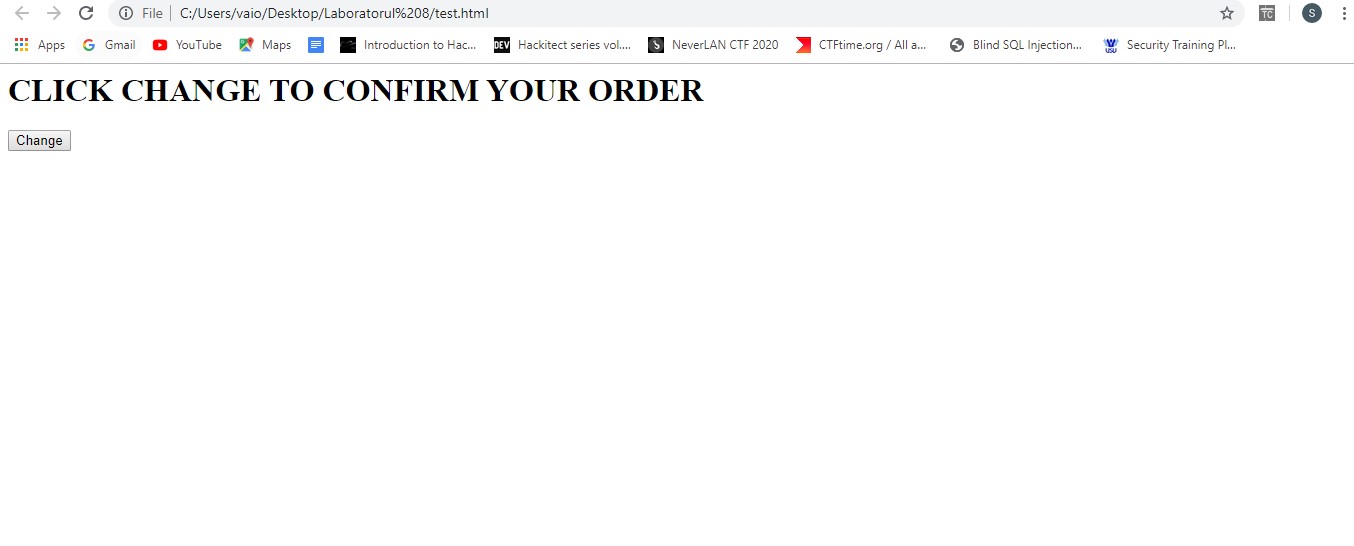


|  |  |  |
| --- | --- | --- |
| Valoarea pentru noua parolă a fost setată ca | hacked | , aceasta se va seta după apăsarea |
| butonului Change | | |

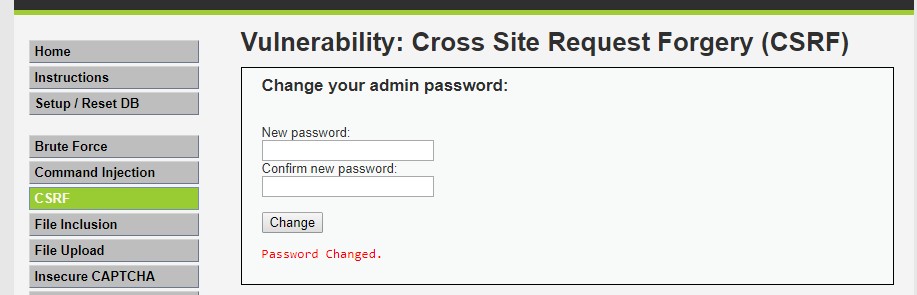
* + Îl salvăm cu extensia .html



* Pasul 9. Deschidem fișierul salvat



* Pasul 10. Apăsăm butonul Change și apare mesajul că parola a fosst schimbată cu succes



* Pasul 11. Ne autentificăm cu noua parolă hacked

