**Resurse laborator XSS**

**Setup:**

1. Se formeaza echipe de cate 2 studenti (ATTACKER / VICTIM)
2. VICTIM urmeaza toti pasii laboratorului anterior, logandu-se insa la final cu user=admin, pass=passadmin
3. ATTACKER porneste din command prompt NC.exe cu urmatoarea comanda: nc -nlvp 81
4. ATTACKER acceseaza pagina de login de pe sistemul VICTIM: http://VICTIM\_IP/login.php si se logheaza cu user=raul, pass=passraul
5. ATTACKER posteaza mesajul XSS (vezi mai jos), inlocuind inainte ATTACKER\_IP cu IP-ul propriu al masinii atacatorului.
6. ATTACKER se delogheaza din aplicatie (trebuie sa se reintoarca la pagina de login).
7. VICTIM re-acceseaza login.php, fiind logat (refresh, F5, etc)
8. ATTACKER urmareste ce se intampla in Command Prompt, asteptand sa apara un request de la VICTIM, care include cookie-ul victimei (ar trebui sa arate precum in [aceasta imagine](https://www.cs.ubbcluj.ro/~alungana/ss/lab11/nc.png)).
9. ATTACKER instaleaza si porneste BURP Proxy si isi seteaza la browser urmatorul proxy: 127.0.0.1, port 8080
10. ATTACKER da refresh (F5) la pagina de login (accesul va fi intrerupt in proxy)
11. ATTACKER analizeaza in BURP Proxy HTTP request-ul (trebuie sa arate ca in [aceasta imagina](https://www.cs.ubbcluj.ro/~alungana/ss/lab11/xss.png)). Va adauga in headere urmatoarea linie, inlocuind cu session ID-ul al victimei (colectat cu NC), dupa care apasa 'Forward'.

Cookie: PHPSESSID=xxxxxxxxxxxxxxxxxxxxxxxxxx

Daca exista deja headerul Cookie in request, doar se inlocuieste valoarea PHPSESSID cu cea a victimei.

1. In acest moment, ATTACKER ar trebui sa fie logat cu userul cu care era logat VICTIM
2. VICTIM va incerca sa fixeze problema in login.php (va dori de asemenea sa elimine din baza de date mesajul malitios)
3. ATTACKER va incerca din nou sa repete atacul, postand un nou mesaj

Daca rulati acest exercitiu intr-o masina virtuala, puteti efectua intregul exercitiu fara ajutorul altor colegi. Masina virtuala poate fi VICTIM, iar masina reala poate fi ATTACKER. Puteti obtine IP-ul fiecareia ruland ipconfig in fiecare dintre ele.

**Resurse:**

* [nc.exe](https://www.cs.ubbcluj.ro/~alungana/ss/lab11/nc.zip)
* [Mesaj XSS](https://www.cs.ubbcluj.ro/~alungana/ss/lab11/xss.txt) (inlocuiti ATTACKER\_IP cu ip-ul propriu!)
* [BURP Proxy](https://portswigger.net/burp/download.html)