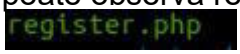
schematics

Din descrierea chall ne dam seama ca este un fel de magazin deci de aici ne dam seama ca poate contine un database pe undeva deci poate putem sa ne folosim de o vulerabilitate de tip sqli.Un **SQL injection (SQLi)** este o vulnerabilitate de securitate care permite unui atacator să introducă sau să manipuleze comenzi SQL într-o aplicație, pentru a obține acces neautorizat la baza de date sau pentru a modifica datele stocate acolo. Această vulnerabilitate apare de obicei atunci când aplicațiile web nu filtrează corect datele introduse de utilizatori și permit inserarea de comenzi SQL malițioase în interogările care sunt executate pe baza de date. De exemplu, într-un formular de logare, un atacator ar putea introduce un input precum:

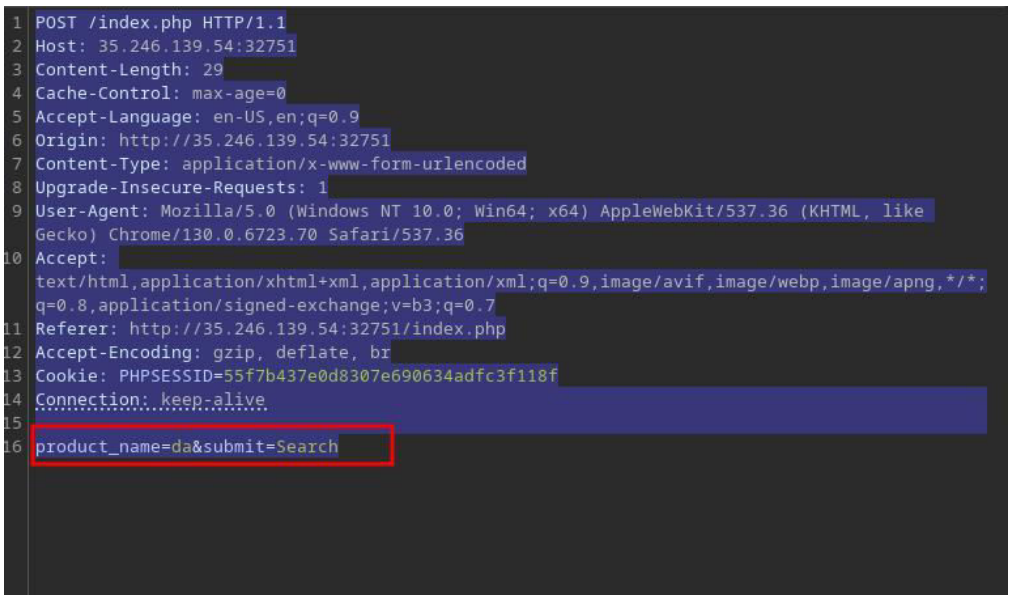
' OR '1'='1

Cand acessam url vedem ca ne cere sa ne logam pe site doar ca nestiind ce users exista acolo este cam greu sa incercam sa facem un sqli.Asa ca m-am gandit sa flosesc dirbuster pentru endpointuri unde se poate observa register.php:



La inceput credeam ca era vorba sa acessam contul la admin doar ca nu aveam nicio informatie ca ar fi fost acolo flagul sau cum sa reusesc asta.Revenind la index.php dupa ce ne logam putem vedea ca avem un search bar unde gasim produsele prezente din magazin:

Aici mi-am dat seama ca puteam incerca sa gasim manual u payload care sa dea dump la tot database-ul sau un tool automatic ca sqlmap.



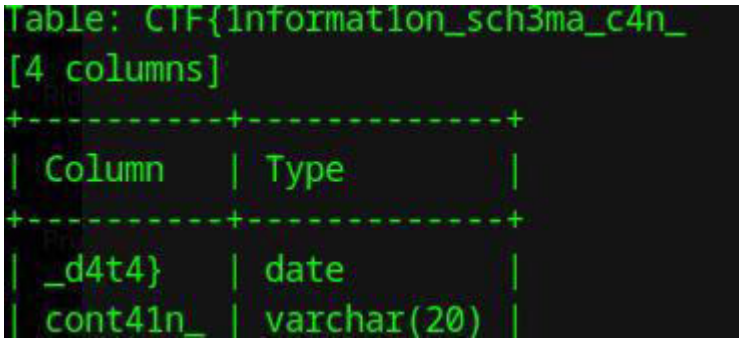
Asa cum se vede din burpsuite avem 2 parametri injectabili “product_name” si “submit”.Singurul lucru ramas este sa folosim toolul sqlmap pentru a obtine tot informatiile din database. Folosim:

sqlmap –cookie="PHPSESSID=cookie" --url http://35.246.139.54:32751/index.php --forms -- columns

`--forms`: Analizează formularele de pe pagina indicată pentru a căuta posibile puncte de intrare pentru SQL injection.

`--columns`: Încearcă să extragă și să afișeze numele coloanelor din tabelele bazei de date de pe serverul țintă.

Dupa putin timp obtinem rezultate cu jumtate din flag iar restul aflandu-se in acelasi tabel:



Flag:

CTF{1nformat1on_sch3ma…._d4t4}

Trolled by masquerade8077