**LAPORAN PRAKTIKUM IV**

**MELAKUKAN SERANGAN WEB SERVER XVWA**

****

**DISUSUN OLEH :**

Nama : Diki Candra

Nim : 2022903430010

Kelas : TRKJ 2B

Jurusan : Teknologi Informasi dan Komputer

Program Studi : Teknologi Rekayasa Komputer Jaringan

Dosen Pembimbing : Atthariq, S.ST, MT

**JURUSAN TEKNOLOGI INFORMASI DAN KOMPUTER**

**PRODI TEKNOLOGI REKAYASA KOMPUTER DAN JARINGAN**

**POLITEKNIK NEGERI LHOKSEUMAWE**

**TAHUN 2023/2024**

**LEMBARAN PENGESAHAN**

Laporan Yang Berjudul : Melakukan Serangan Web Server XVWA

Disusun Oleh : Diki Candra

Nim : 2022903430010

Jurusan : Teknologi Informasi & Komputer

Program Studi : Teknologi Rekayasa Komputer Jaringan

Mata Kuliah : Databases Aplication

Tanggal Praktikum : 26 Oktober 2023

Tabel Penilaian : :

Mengetahui,

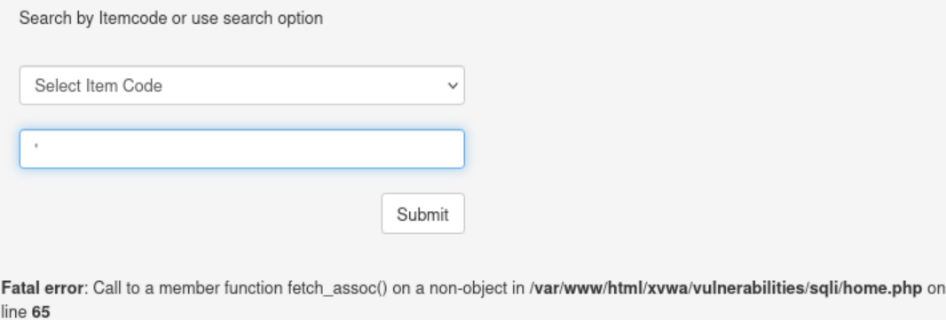
Dosen Pembimbing, Penyusun,

Atthariq, S.ST, MT Diki Candra

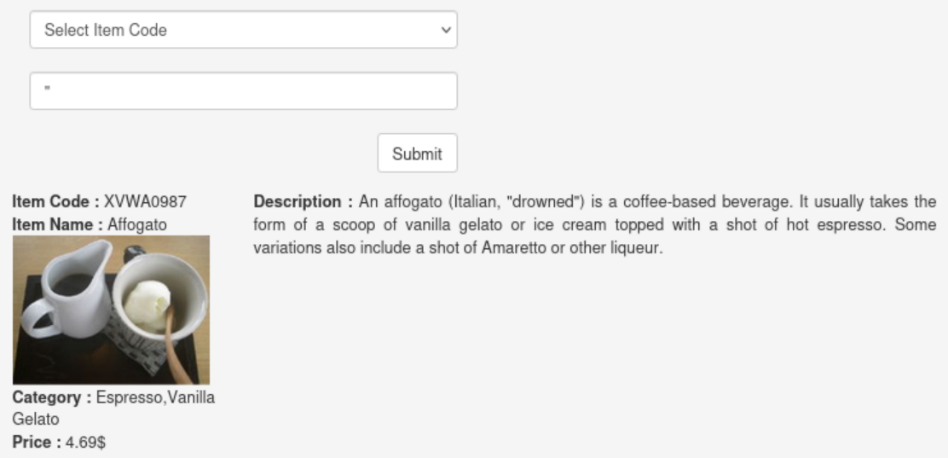
NIP 197807242001121001 NIM 2022903430010

PRAKTIKUM MENGUJI WEB SERVER XVWA

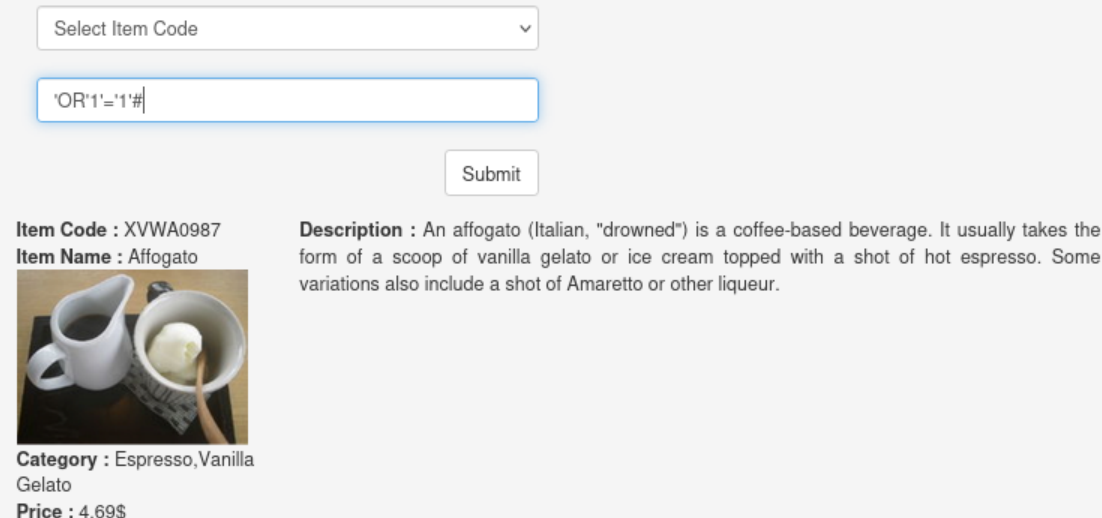
1. Ketik ‘ pada kolom pencarian, tanda petik tunggal (') adalah salah satu karakter yang digunakan dalam serangan SQL Injection untuk menguji apakah suatu aplikasi web rentan terhadap injeksi SQL atau tidak.



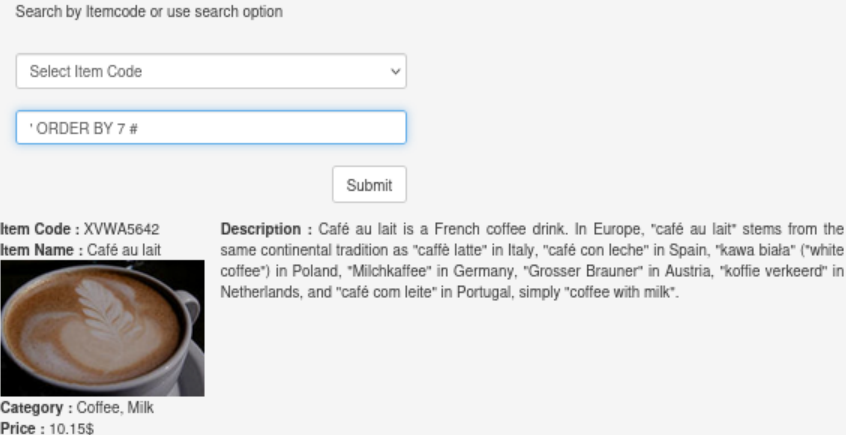
1. Ketik (“) pada kolom pencarian, tanda kutip ganda ("), seperti tanda kutip tunggal ('), dapat digunakan dalam konteks uji keamanan dan uji penetrasi untuk mengidentifikasi kerentanan yang berkaitan dengan kelemahan input (Input Vulnerabilities) dalam aplikasi web.



1. Ketik ('OR '1'='1' #) pada kolom pencarian, Teks **'OR '1'='1' #** adalah payload yang digunakan untuk uji SQL Injection dalam aplikasi web. Ini mencoba memanipulasi pernyataan SQL dengan memasukkan kondisi yang selalu benar (1=1) dan mengakhiri komentar SQL. Tujuannya adalah untuk mengidentifikasi kerentanan SQL Injection dalam aplikasi web.



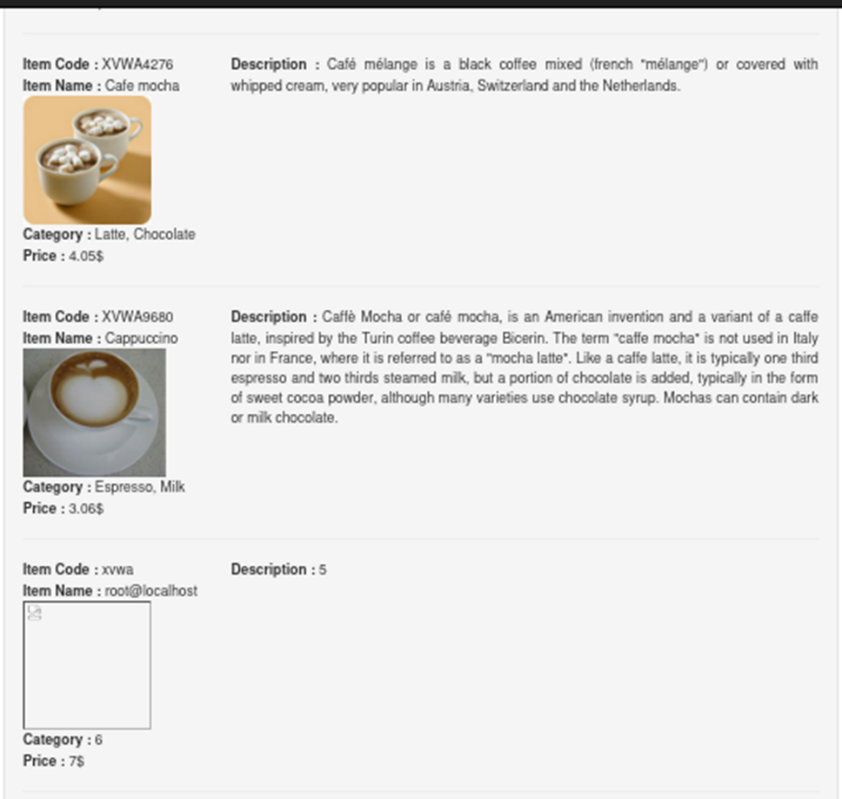
1. Ketik (‘ ORDER BY 7 #) pada kolom pencarian, digunakan untuk mencari tahu berapa banyak kolom yang dapat diurutkan dalam pernyataan SQL, mengidentifikasi kerentanan SQL Injection.



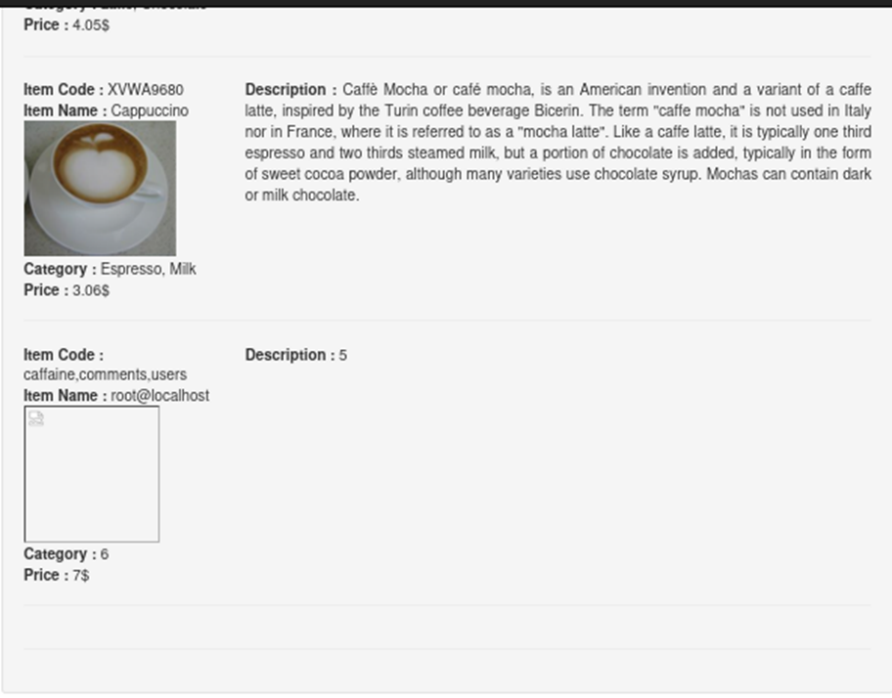
1. Ketik (‘ UNION SELECT 1,2,3,4,5,6,7 #) pada kolom pencarian, dengan perintah ini, anda mencoba menggabungkan hasil dari beberapa kolom dalam database dan melihat apakah Anda dapat mengambil data dari tabel tertentu.



1. Ketik (' UNION SELECT 1,database(),3,user(),5,6,7 #) pada kolom pencarian, dengan perintah ini, Anda mencoba untuk mendapatkan informasi tentang database yang digunakan (dalam kasus ini, database apa yang sedang digunakan) dan informasi pengguna saat ini yang terhubung ke database.



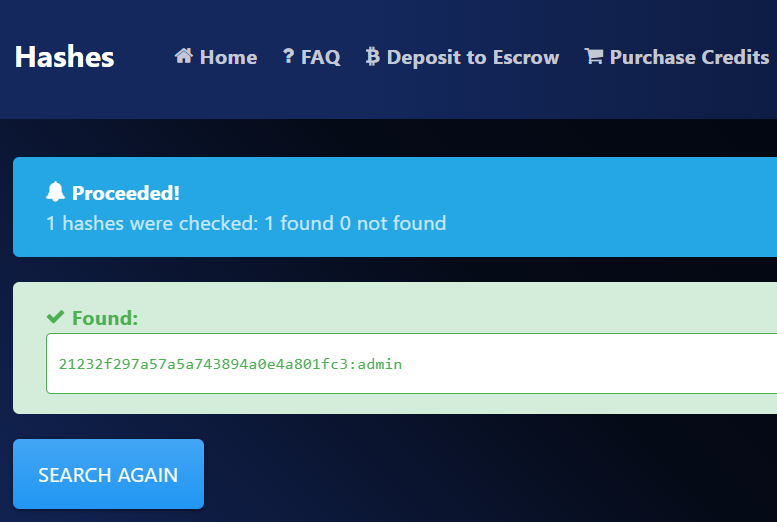
1. Ketik (‘ UNION SELECT 1,group\_concat(table\_name),3,user(),5,6,7 from information\_schema.tables where table\_schema = database() # ) pada kolom pencarian, dengan perintah ini, Anda mencoba untuk mengekstraksi daftar nama tabel dalam database saat ini yang sedang digunakan oleh aplikasi web.



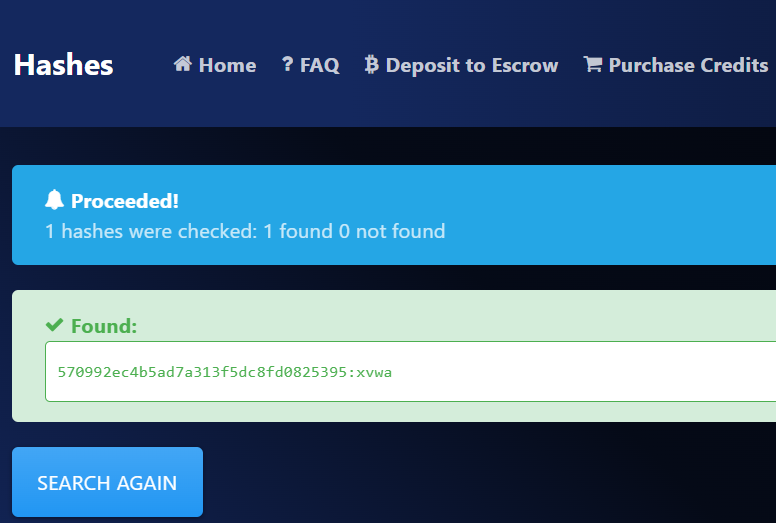
1. Ketik (‘ UNION SELECT 1,group\_concat(username,0x3a,password),3,user(),5,6,7 from users #) pada kolom pencarian, digunakan untuk mengekstraksi informasi dari tabel "users" dalam database yang terkait dengan aplikasi web tersebut. Dalam hal ini, Anda mencoba untuk mengambil data dari kolom "username" dan "password" dari tabel "users". Perintah tersebut akan menggabungkan (union) hasilnya dalam satu baris dan memisahkan antara username dan password dengan tanda ":" (0x3a dalam notasi heksadesimal).



1. Lalu salin kode admin dan ketikan pada web [https://hashes.com/en/decrypt/hash seperti ini, 21232f297a57a5a743894a0e4a801fc3](https://hashes.com/en/decrypt/hash%20seperti%20ini,%2021232f297a57a5a743894a0e4a801fc3). Kode "21232f297a57a5a743894a0e4a801fc3" adalah hasil dari hash suatu nilai atau kata sandi. Hash adalah nilai yang dihasilkan dari sebuah fungsi hash yang mengambil input (dalam hal ini kata sandi) dan menghasilkan string numerik yang panjang dan unik yang merepresentasikan input tersebut. Hash ini sering digunakan dalam pengamanan dan penyimpanan kata sandi.



1. Selanjtnya salin kode XVWA (570992ec4b5ad7a313f5dc8fd0825395), Kode "570992ec4b5ad7a313f5dc8fd0825395" adalah sebuah hash. Hash ini mungkin dihasilkan dari suatu data atau pesan tertentu menggunakan algoritma hash seperti MD5 atau SHA-256.



**Kesimpulan**

Praktikum diatas berkaitan dengan serangan SQL Injection dan teknik yang sering digunakan dalam uji penetrasi dan pengujian keamanan. Ini menunjukkan pentingnya perlindungan terhadap serangan semacam ini dan perlu memahami cara melindungi sistem dan aplikasi dari kerentanan ini.