**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 : 09 November 2023

Tabel Penilaian : :

Mengetahui,

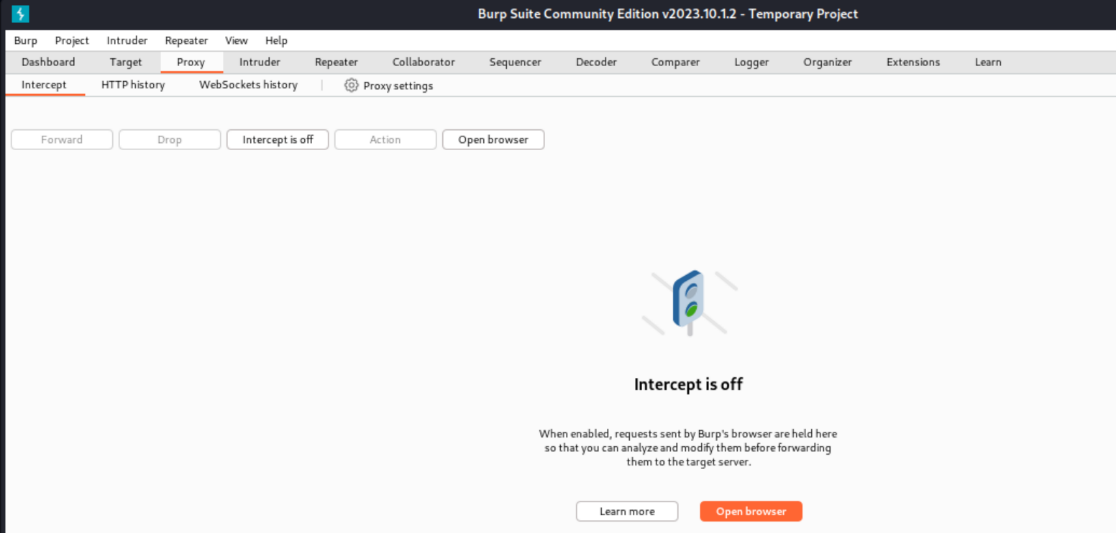
Dosen Pembimbing, Penyusun,

Atthariq, S.ST, MT Diki Candra

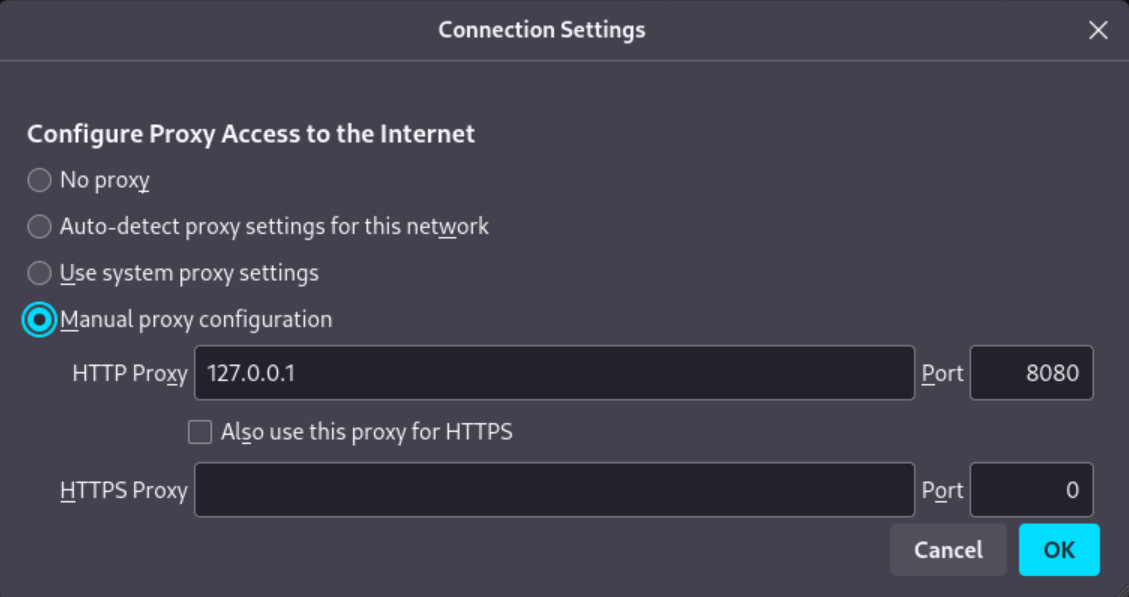
NIP 197807242001121001 NIM 2022903430010

PRAKTIKUM MENGUJI WEB SERVER XVWA

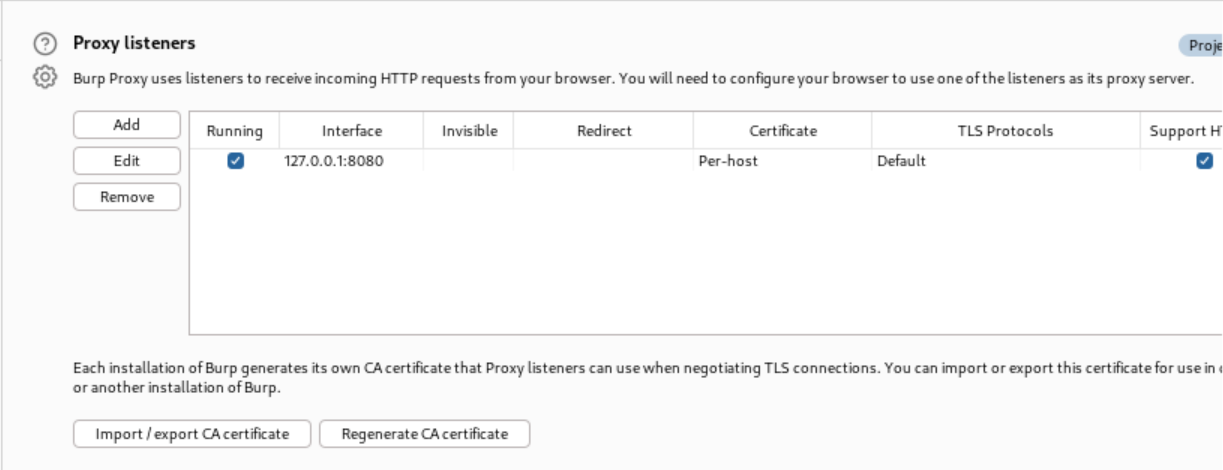
1. Buka **Burpsuite** dengan perintah $ burpsuite



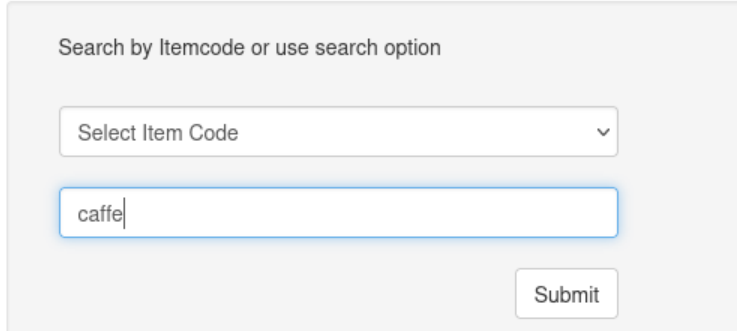
1. Ubah proxy pada browser dengan IP local 127.0.0.1 dan port 8080



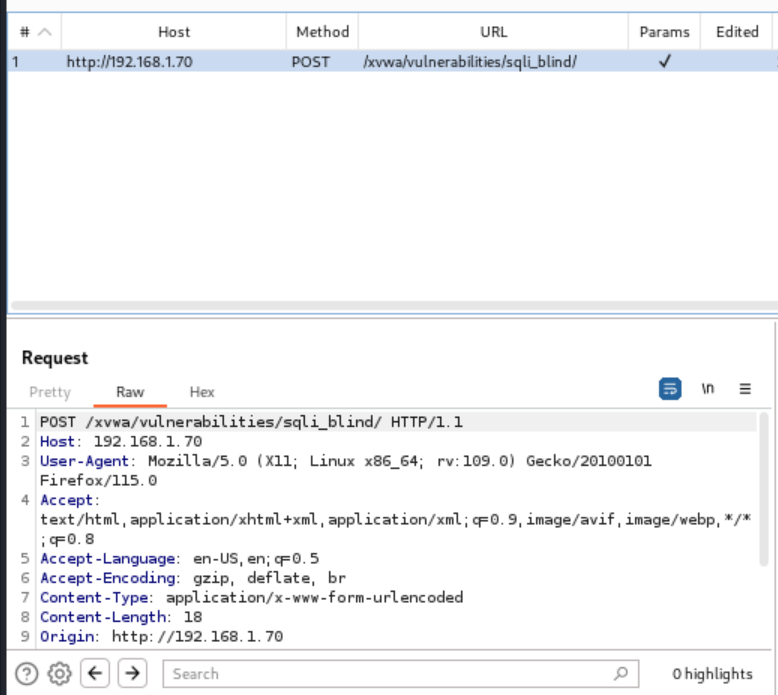
1. Cek proxy pada Burpsuite pastikan sudah Running



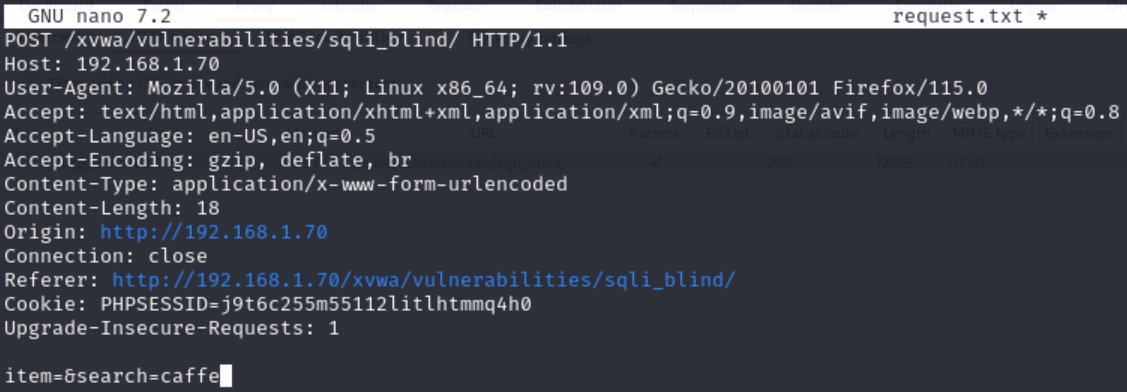
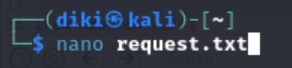
1. Ketik caffe pada XVWA di menu SQL injection(blind)



1. Kembali lagi ke burpsuite buka menu proxy dan lihat HTTP history, selanjutnya copy text yang ada pada tampilan request.



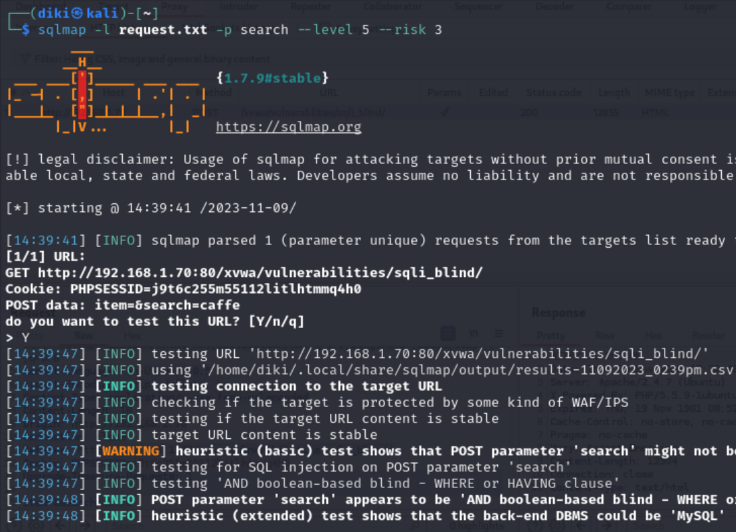
1. Lalu, pastekan dalam bentuk file txt dengan perintah $ nano request.txt



1. Berikutnya lakukan perintah $ sqlmap -l request.txt -p search –level 5 – 3

Penjelasannya:

* **sqlmap**: Ini adalah perintah utama untuk menjalankan SQLMap.
* **-l request.txt**: Parameter ini digunakan untuk menentukan lokasi (file **request.txt**) yang berisi permintaan HTTP yang akan dianalisis oleh SQLMap. Permintaan ini adalah permintaan HTTP yang dapat berpotensi terkena serangan SQL Injection.
* **-p search**: Parameter ini digunakan untuk menentukan parameter yang dapat dimanipulasi untuk menguji serangan SQL Injection. Parameter **search** di sini adalah nama parameter yang menjadi target.
* **--level 5**: Ini adalah parameter yang mengatur tingkat kedalaman analisis SQL Injection. Dalam hal ini, tingkat 5 digunakan, yang berarti SQLMap akan mencoba berbagai jenis serangan SQL Injection dengan tingkat yang tinggi.
* **-- 3**: Ini adalah parameter yang digunakan untuk menentukan metode HTTP yang akan digunakan. **--3** mengindikasikan penggunaan metode HTTP GET.



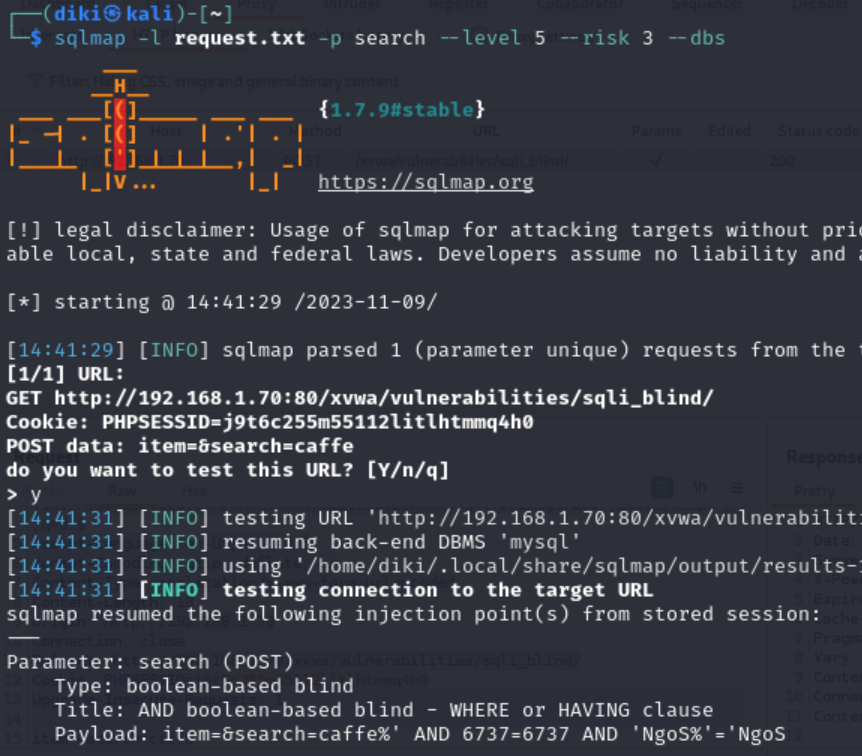
1. Lakukan perintah $ sqlmap -l request.txt -p search –level 5 – 3 –dbs

Penjelasannya:

* **--dbs**: Parameter ini digunakan untuk menginstruksikan SQLMap untuk mencoba mengekstrak informasi tentang database yang digunakan oleh situs web target.

Pada perintah ini hampir sama dengan sebelumnya bedanya pada ujung querynya saja yang di tambah **--dbs**

Jadi, perintah ini digunakan untuk menjalankan SQLMap pada permintaan HTTP yang ada dalam file **request.txt** untuk mencari kerentanan SQL Injection pada parameter **search**. Perintah juga mengatur tingkat analisis yang tinggi (level 5) dan menggunakan metode HTTP GET. Selain itu, dengan menambahkan **--dbs**, SQLMap akan mencoba mengekstrak informasi tentang database yang digunakan oleh situs web target.



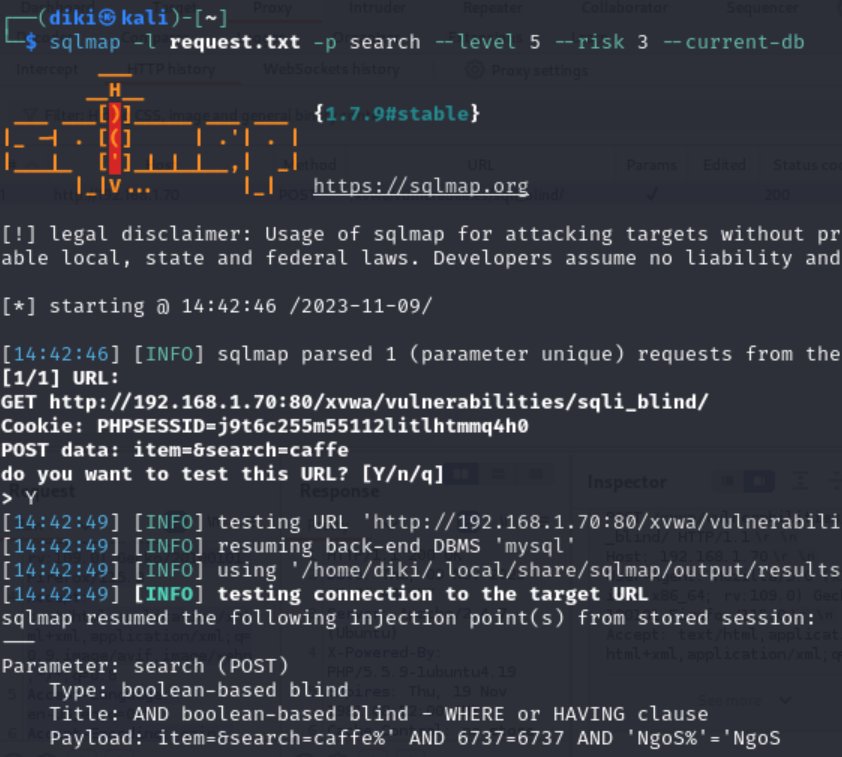
1. Selanjutnya, Lakukan perintah $ sqlmap -l request.txt -p search –level 5 – 3 –current-db

Penjelasannya :

* **--current-db**: Parameter ini digunakan untuk mengekstrak nama database yang sedang digunakan oleh aplikasi atau situs web target saat ini.

Pada perintah ini hampir sama dengan sebelumnya bedanya pada ujung querynya saja yang di tambah **–current-db**

Jadi, perintah ini digunakan untuk menjalankan SQLMap pada permintaan HTTP yang ada dalam file **request.txt** untuk mencari kerentanan SQL Injection pada parameter **search**. Perintah juga mengatur tingkat analisis yang tinggi (level 5) dan menggunakan metode HTTP GET. Dengan menambahkan **--current-db**, SQLMap akan mencoba mengekstrak nama database yang sedang digunakan oleh situs web atau aplikasi yang sedang diuji.



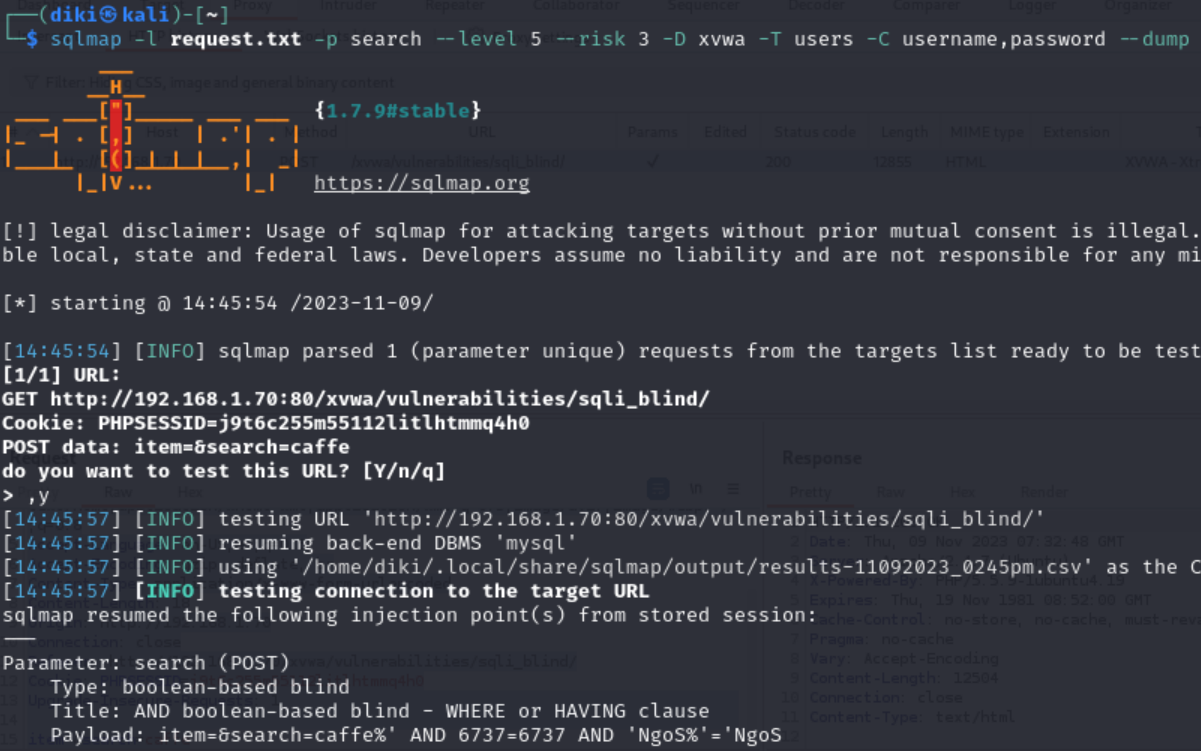
1. Berikutnya, Lakukan perintah $ sqlmap -l request.txt -p search –level 5 – 3 -D xvwa -C username,password --dump

Penjelasannya:

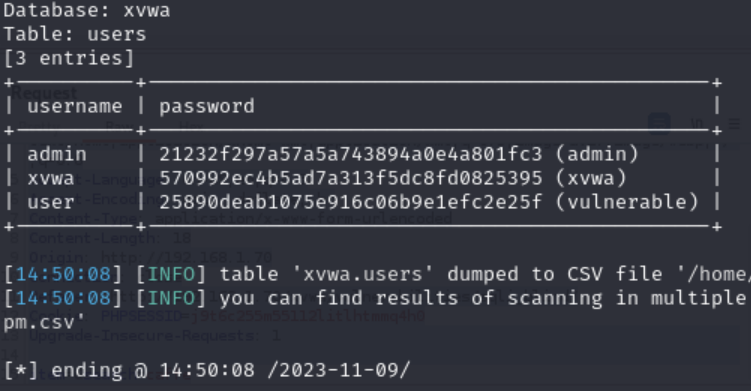
* **-D xvwa**: Parameter ini digunakan untuk menentukan nama database yang akan diakses atau diserang. Dalam hal ini, nama database yang disebut adalah **xvwa**.
* **-C username,password**: Parameter ini digunakan untuk menentukan nama kolom atau bidang dalam tabel database yang akan diambil datanya. Dalam perintah ini, Anda mencoba mengekstrak data dari kolom **username** dan **password**.
* **--dump**: Ini adalah parameter yang menginstruksikan SQLMap untuk mengambil dan menampilkan data dari kolom yang Anda tentukan sebelumnya. Dalam hal ini, Anda mencoba mengekstrak data dari kolom **username** dan **password** dan menampilkannya.

Pada perintah ini hampir sama dengan sebelumnya bedanya pada ujung querynya saja yang di tambah -**D xvwa -C username,password --dump**

Dengan perintah ini, Anda mencoba mengekstrak data login (username dan password) dari tabel yang ada dalam database **xvwa** yang mungkin terkena kerentanan SQL Injection.



Lanjutannya



**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.