Laporan Cyber Security

SQL Injection Menggunakan Cyberfox dengan Ekstensi Hackbar pada Website Vulnweb

Muhammad Mardiansyah

PUSAT PELATIHAN KERJA DAERAH JAKARTA UTARA

Penetration Testing Website vulnweb

1. Ringkasan Eksekutif

Melakukan pengujian keamanan dasar untuk menemukan potensi kerentanan pada aplikasi web uji coba testphp.vulnweb.com dengan metode manual menggunakan ekstensi Hackbar pada Cyberfox.

2. Lingkup Pengujian (Scope)

- **Browser**: Cyberfox
- **Ekstensi**: Hackbar (untuk manipulasi parameter HTTP dan testing manual SQLi/XSS)
- **Target Legal**: http://testphp.vulnweb.com (website uji coba dari Acunetix, legal untuk dites)

3. Metodologi Pengujian

Pengujian dilakukan berdasarkan kerangka kerja OWASP Testing Guide dengan tahapan:
- Active Reconnaissance = Memberikan payload pada inputan untuk melihat celah.
- Vulnerability Assessment = Mencari celah pada sistem.
- Exploitation = Melakukan exploitasi dengan sqlmap.
- Reporting = Membuat laporan penetration testing.

4. Temuan dan Rekomendasi

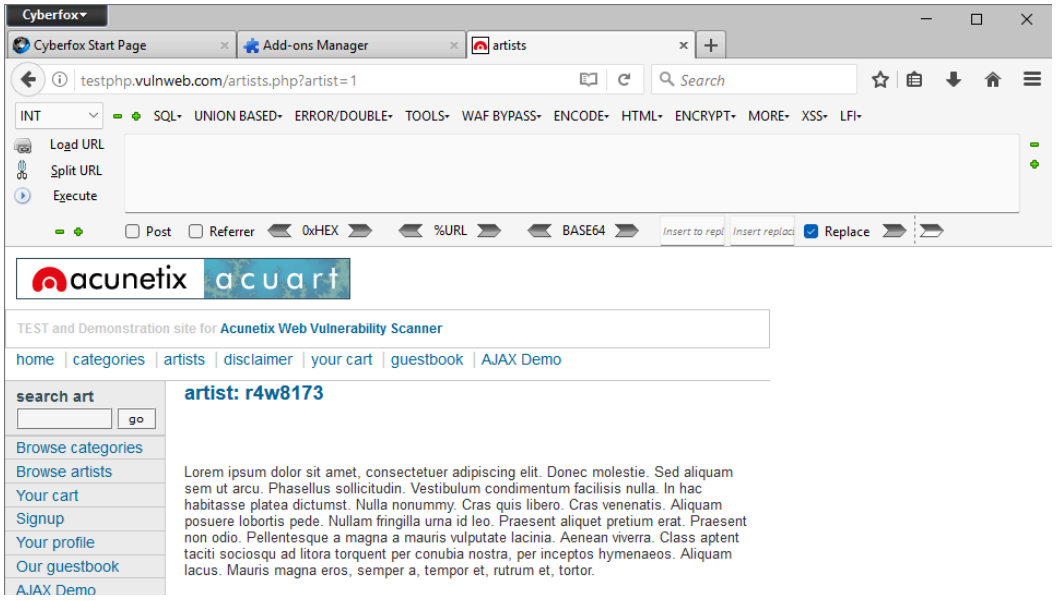
No	Nama Kerentanan	Risiko	Deskripsi Singkat	Rekomendasi
1	SQL Injection	Tinggi	Parameter input tidak divalidasi dengan baik.	Gunakan parameterized queries dan validasi input. atau gunakan prepared parameter $statement

5. Detail Temuan (Contoh)

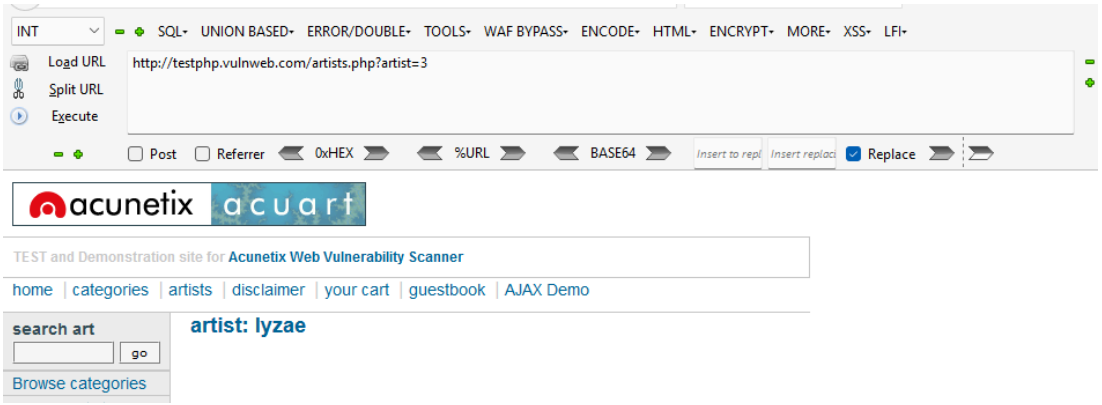
- Nama Kerentanan: SQL Injection
- URL Terdampak: http://testphp.vulnweb.com/artists.php?artist=1
- Metode Uji: Menyisipkan nilai 1 pada kolom submit dan mendapatkan nilai id=1
- Risiko: Akses data tidak sah dan potensi manipulasi database.

6. Lampiran

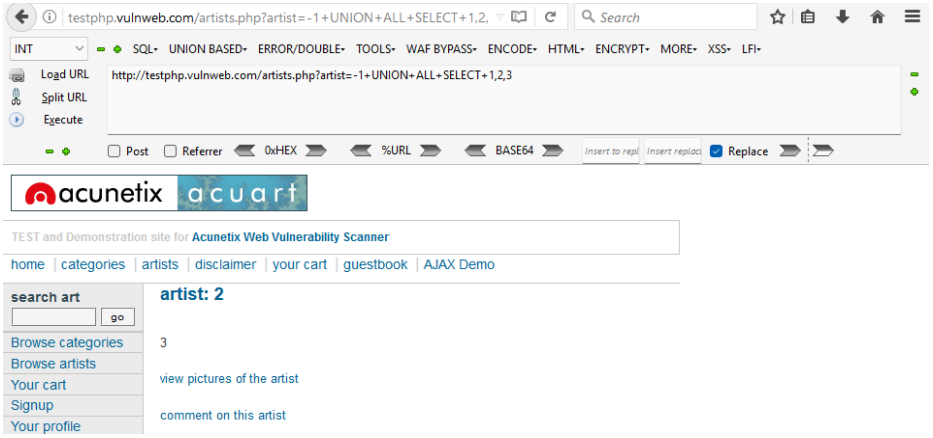
Pada gambar dibawah merupakan website testphp.vulnweb.com dan search engine cyberfox dengan extensi hackbar yang digunakan untuk sql injection. Gambar dibawah adalah melakukan pengecekan apakah ada parameter yang dapat kita eksploitasi, dan ternyata terdapat parameter yang dapat dieksploitasi seperti artist=1.



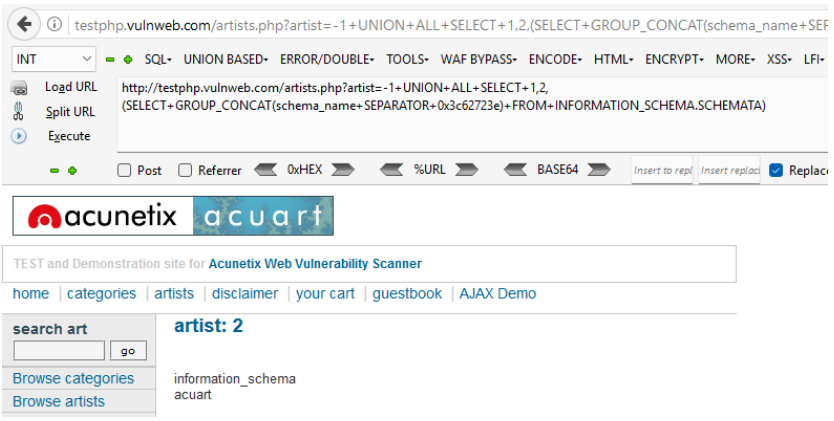
Mengganti nilai artist = 1 menjadi artis = 3, pengecekan ini berfungsi untuk melihat target dan posisi kita pada web dan menjadikan indikasi awal bahwa website bisa kita injeksi.



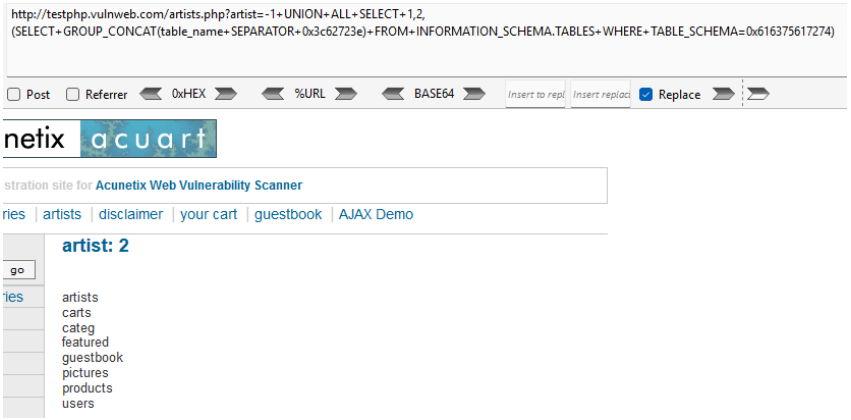
Melakukan fungsi union select untuk menentukan posisi kita pada sebuah website.



Payload SQL injection `(SELECT GROUP_CONCAT(schema_name SEPARATOR 0x3c62723e) FROM INFORMATION_SCHEMA.SCHEMATA)` digunakan oleh penyerang untuk mencuri informasi nama-nama database (schema) yang ada di server MySQL. Payload ini mengeksploitasi fungsi `GROUP_CONCAT` untuk menggabungkan semua nama database menjadi satu baris teks



Payload sql injection table name digunakan untuk mengeksploitasi data tabel pada database yang telah kita lakukan sebelumnya. digunakan untuk melihat/mencuri data tabel pada database.



7. Kesimpulan

Setelah melakukan penetration testing terhadap website **http://testphp.vulnweb.com** menggunakan **search engine Cyberfox** dan ekstensi **Hackbar**, berikut adalah kesimpulan yang dapat diambil:

1. Efektivitas Cyberfox + Hackbar

- Cyberfox berfungsi baik sebagai browser alternatif yang ringan dan mendukung ekstensi seperti Hackbar.
- Hackbar sangat membantu untuk eksploitasi manual terhadap parameter URL (GET) dan form (POST).
- Kombinasi ini cocok untuk latihan pengujian manual pada website uji coba, terutama untuk SQL Injection dan XSS.

2. Kerentanan yang Berhasil Ditemukan

- SQL Injection berhasil dideteksi pada parameter artist di URL /artists.php.

3. Keunggulan Metode Manual Ini

- Dapat menguji parameter secara real-time dan melihat respon langsung dari server.
- Memberikan pemahaman mendalam tentang cara kerja input user yang tidak di validasi.
- Membantu pemula dalam belajar dasar-dasar serangan web secara legal.