LAPORAN PRAKTIKUM XV
SQL INJECTION

DISUSUN OLEH **:**

Nama	: Diki Candra
Nim	: 2022903430010
Kelas	: TRKJ 2B
Jurusan	: Teknologi Informasi dan Komputer
Program Studi	: Teknologi Rekayasa Komputer Jaringan
Dosen Pengajar	: Aswandi, S.Kom, M.Kom.

JURUSAN TEKNOLOGI INFORMASI DAN KOMUNIKASI

PRODI TEKNOLOGI REKAYASA KOMPUTER DAN JARINGAN

POLITEKNIK NEGERI LHOKSEUMAWE

TAHUN 2022/2023

LEMBARAN PENGESAHAN

Laporan Yang Berjudul : Sql Injection

Disusun Oleh : Diki Candra

NIM : 2022903430010

Jurusan : Teknologi Informasi & Komputer

Program Studi : Teknologi Rekayasa Komputer Jaringan

Mata Kuliah : Ethical Hacking

Tabel Penilaian

Mengetahui,

Dosen Pembimbing,

Penyusun,

Aswandi, S.Kom, M.Kom
NIP. 197209242010121001

Diki Candra
NIM. 2022903430010

I. Capaian Praktikum/Kompetensi

1. Pahami SQL Injection:

Pelajari cara SQL injection bekerja dan mengapa serangan ini dapat menjadi ancaman serius.

Pahami teknik-teknik umum yang digunakan oleh penyerang untuk menyusupkan kode SQL berbahaya.

2. Pelajari Cara Melindungi dari SQL Injection:

Pahami praktik terbaik untuk mencegah SQL injection, seperti penggunaan parameterized queries atau prepared statements.

Pelajari tentang mekanisme otentikasi dan otorisasi yang kuat.

3. Pelajari Uji Penetrasi yang Etis:

Jika Anda berminat dalam keamanan informasi, pelajari prinsip-prinsip uji penetrasi yang etis.

Pahami proses mendapatkan izin sebelum melakukan uji penetrasi.

Pelajari Keamanan Aplikasi

Pelajari keamanan aplikasi secara umum, termasuk praktik keamanan frontend dan backend.

Pahami konsep keamanan seperti enkripsi, hashing, dan manajemen sesi.

II. Keselamatan Kerja

Praktikum *sql injection* diharapkan mengikuti aturan keselamatan kerja, sebagai berikut:

1. Pelatihan dan Kesadaran:
2. Praktik Pengembangan Aman:
3. Pengujian Keamanan:
4. Pemantauan dan Pembaruan:
5. Manajemen Akses dan Otorisasi:
6. Enkripsi Data:
7. Pemulihan dan Rencana Keamanan:

III. Teori

SQL Injection adalah sebuah kerentanan keamanan web yang memungkinkan penyerang dapat menggangu kueri yang telah dibuat oleh aplikasi ke databasenya. Biasanya serangan ini dugnakan untuk mengambil isi database pada aplikasi. Dalam beberapa kasus penyerang dapat memodifikasi atau menghapus data ini, menyebabkan perubahan terus-menerus pada konten atau perilaku aplikasi.

Dalam beberapa situasi penyerang dapat meningkatkan serangan SQL Injection untuk mengkompromikan server yang mendasarinya atau infrastruktur back-end lainnya, atau melakukan serangan penolakan layanan.

IV. Alat dan Bahan

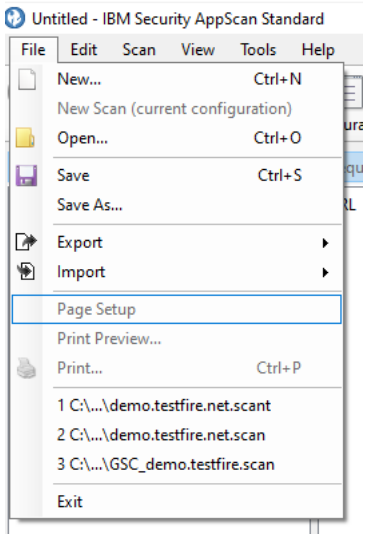
Berikut ini merupakan alat dan bahan yang digunakan pada pelaksanaan praktikum perancangan *malware threats*, adalah sebagai berikut:

I. VMWare

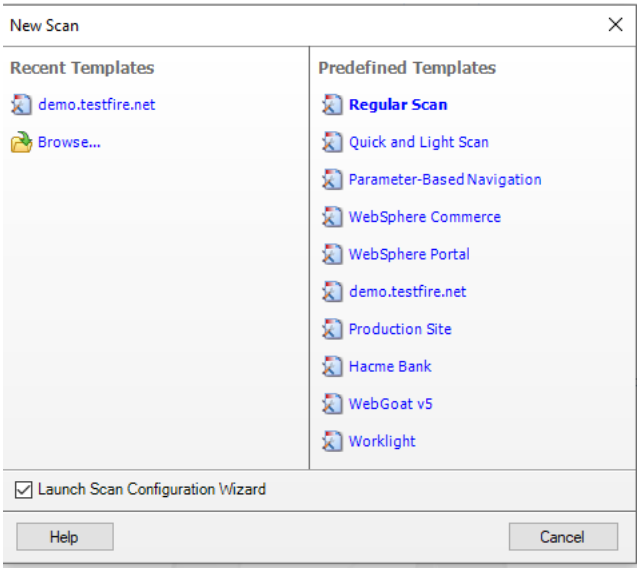
II. Windows

V. Langkah percobaan

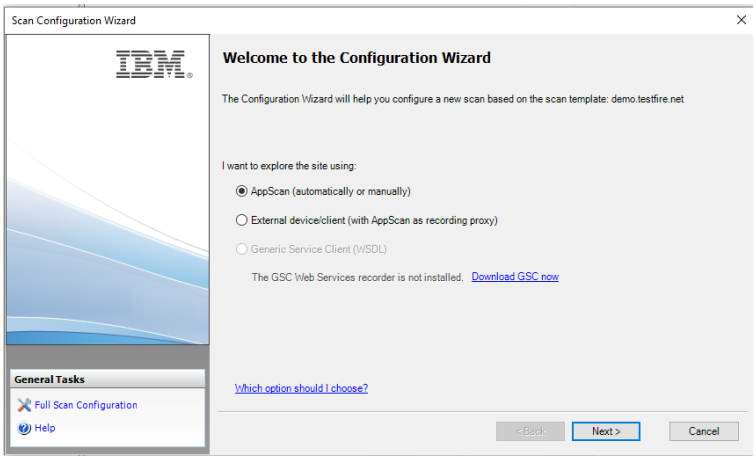
1. Unduh dan pasangkan aplikasi IBM Security Appsca Standard.
2. Bukalah aplikasi tersebut.
3. Pilih “File” lalu “New”.



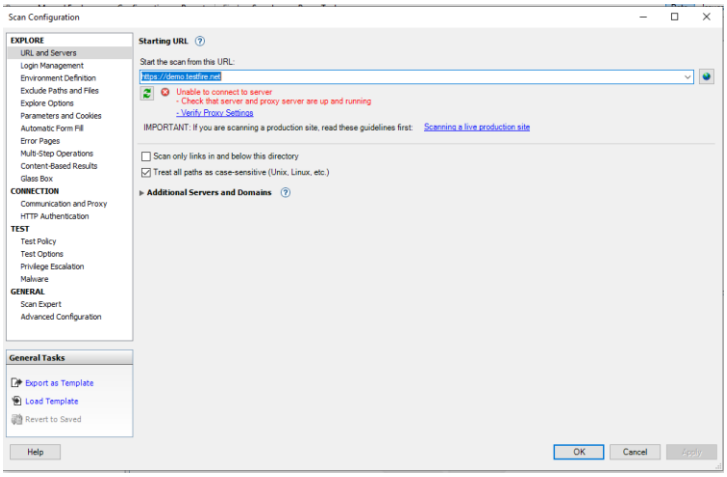
4. Pilih Pindai template, Pemindaian reguler akan memulai pemindaian baru. Dalam kasus kami, kami menggunakan template demo.testfire.net yang telah ditentukan sebelumnya

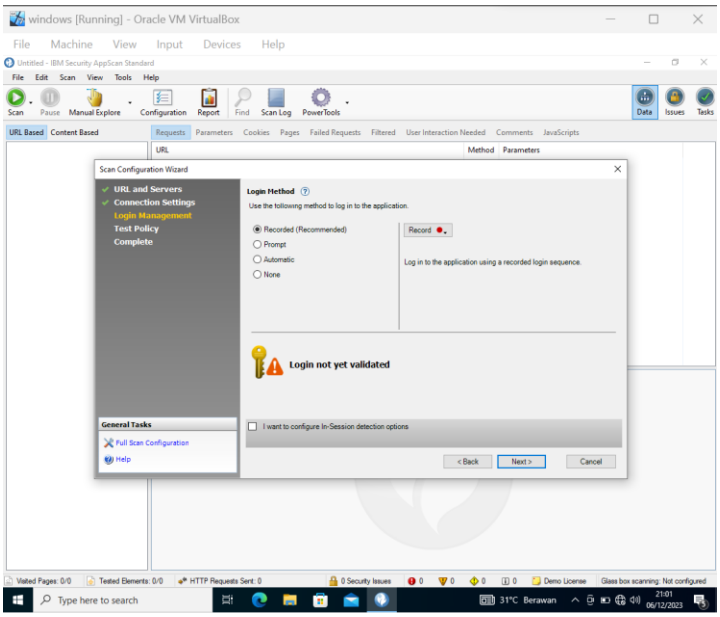


5. Klik Berikutnya
6. Jika Anda ingin mengedit konfigurasi, Klik Konfigurasi stan penuh

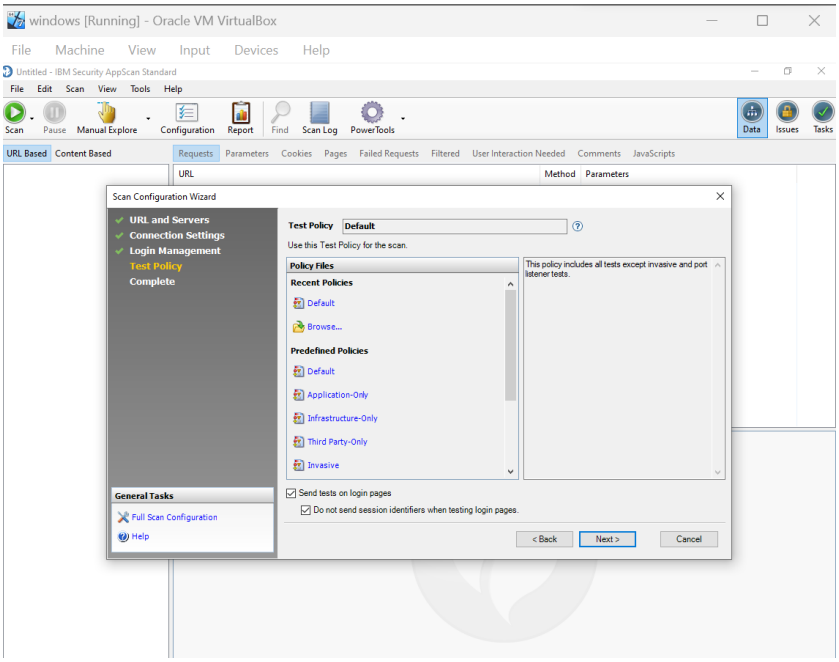


7. Klik Next
8. Pilih method yg ingin kita login





9. Pilih Policy file lalu
10. Tekan Next



Kesimpulan :

untuk melindungi sistem dan data dari serangan SQL injection, penting untuk menerapkan praktik keamanan aplikasi yang baik, memahami risiko yang terlibat, dan terus memperbarui kebijakan dan sistem keamanan sesuai dengan perkembangan teknologi dan ancaman keamanan yang muncul. Tetap berpegang pada prinsip-prinsip etika dan kepatuhan hukum alam semua tindakan keamanan informasi.