MODUL PRAKTIKUM

KEAMANAN INFORMASI

DISAMPAIKAN PADA
SEMESTER GENAP
TAHUN AKADEMIK 2023/2024

DEPARTEMEN TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA
MALANG

TIM PENYUSUN

1. ADHITYA BHAWIYUGA, S.KOM, M.SC.
2. ARI KUSYANTI, S.T., M.SC.
3. DANY PRIMANITA KARTIKASARI, S.T., M.KOM.
4. FARIZ ANDRI BAKHTIAR, S.T., M.KOM.
5. M. ALI FAUZI, S.KOM., M.KOM., PH.D.

BAB 2

KERENTANAN DAN ANCAMAN

BAGIAN 1 (SQL Injection)

2.1.1 DASAR TEORI

SQL Injection adalah kerentanan web yang mengizinkan penyerang untuk mengusik query SQL yang dibuat oleh aplikasi menuju database. Secara umum, kerentanan ini memungkinkan penyerang untuk melihat data yang tidak dapat mereka lihat dan mungkin dimiliki oleh pengguna lain dan/atau bisa diakses oleh aplikasi tersebut. Pada banyak kasus yang terjadi, penjahat dapat memodifikasi hingga menghapus data, menyebabkan kerusakan permanen.

2.2.1 TUJUAN PERCOBAAN

1. Mahasiswa mampu memahami konsep SQL Injection
2. Mahasiswa mampu mempraktikkan SQL Injection

2.3.1 ALAT DAN BAHAN

Dalam rangka melaksanakan langkah-langkah praktikum yang terdapat pada bab ini, peserta praktikum perlu menyiapkan beberapa perangkat berikut:

- Perangkat komputer Desktop/Laptop dengan kapasitas RAM minimum 8 GB
- Perangkat lunak virtualisasi (Oracle VM VirtualBox/VMWare Workstation)
- Koneksi internet
- Beberapa tools yang dibutuhkan dalam praktikum

2.4.1 PROSEDUR PERCOBAAN

Instalasi Persiapan Lingkungan Praktikum

Berikut merupakan langkah-langkah yang perlu dilakukan dalam mempersiapkan kebutuhan praktikum :

1. Buka terminal pada sistem operasi Linux.
2. Pada terminal, lakukan instalasi git:
   `sudo apt install git`
3. Lakukan instalasi docker-compose dengan perintah:
   `sudo apt install docker-compose`
4. Kemudian lakukan cloning github repository untuk lab percobaan bagian 1:
   `git clone` https://github.com/adhiyaksactf/sqli-part1.git

5. Lakukan cloning github repository untuk lab percobaan bagian 2:
   `git clone https://github.com/adhiyaksactf/sqli-part2.git`
6. Masuk ke dalam direktori sqli-part1 dengan perintah:
   `cd sqli-part1`
7. Melakukan build docker untuk sqli-part1 dengan perintah:
   `sudo docker-compose up -d`
8. Jalankan perintah berikut untuk mengecek apakah service sudah berjalan:
   `sudo docker ps`
9. Apabila berhasil maka service akan berjalan pada port 81, sehingga dapat mengakses pada browser dengan alamat localhost:81
10. Kembali pada terminal Anda lakukan perintah untuk masuk ke direktori sqli-part2:
    `cd ../sqli-part2`
11. Melakukan build docker untuk sqli-part2 dengan perintah:
    `sudo docker-compose up -d`
12. Jalankan perintah berikut untuk mengecek apakah service sudah berjalan:
    `sudo docker ps`
13. Apabila berhasil maka service akan berjalan pada port 82, sehingga dapat mengakses pada browser dengan alamat localhost:82

SQL Injection Basic

Berikut ini langkah-langkah yang perlu dilakukan dalam menyelesaikan lab praktikum:

1. Masuk pada bagian lab pertama (localhost:81).
2. Lakukan percobaan serangan SQL Injection untuk mem-bypass halaman login milik admin dengan menggunakan query berikut:
   `' OR 1=1#`

Berikan Screenshot

3. Apabila Anda berhasil, Jelaskan bagaimana query yang Anda gunakan dapat mem-bypass laman tersebut, tanpa perlu mengetahui username dan password milik admin.

Berikan Screenshot dan Penjelasan

SQL Injection Union Based

Berikut ini langkah-langkah yang perlu dilakukan dalam menyelesaikan lab praktikum:

1. Masuk pada bagian lab kedua (localhost:82).
2. Setelah berhasil masuk ke dalam web, pelajarilah bagaimana web tersebut bekerja, dan temukan letak celah dari website tersebut. (Celah atau titik injeksi berada di parameter url article)
3. Apabila Anda berhasil menemukan letak celah atau titik injeksi dari website tersebut, berikanlah tanda ' (single-quote) pada parameter tersebut. Jelaskan bagaimana dapat menyebabkan website tersebut menampilkan error.

Berikan Screenshot dan Penjelasan

4. Lakukan serangan berikutnya untuk mengetahui berapa jumlah kolom yang dimiliki database pada website tersebut dengan menggunakan query:
   `1 ORDER BY 4#`
5. Lalu coba kurangi nilai ORDER BY menjadi 3, lalu apa yang terjadi pada laman web tersebut?

Berikan Screenshot dan Penjelasan

6. Selanjutnya kita bisa mencari column yang dapat kita injeksi. dengan menggunakan query statement berikut:
   `1 UNION SELECT 'test',NULL,NULL`

Berikan Screenshot dan Penjelasan

7. Kita bisa menampilkan informasi terkait database, dengan mengganti 'test' menjadi @@hostname untuk menampilkan nama host dari DB, database() untuk nama database, @@version untuk menampilkan versi dari DB.

Berikan Screenshot
Hostname : Database : Versi :

8. Berikutnya tampilkan table yang dimiliki database dengan menggunakan query berikut:
   `1 UNION SELECT table_name,NULL,NULL FROM information_schema.tables WHERE table_schema=database()#`

Berikan Screenshot dan Penjelasan

9. Dari table yang telah Anda ekstraksi, tampilkan column dari table yang memiliki kemungkinan memuat username dan password dari admin. Dengan menggunakan query berikut, dan ganti nama_table menjadi nama tabel yang Anda temukan.

   `1 UNION SELECT column_name,NULL,NULL FROM information_schema.columns WHERE table_name='nama_table'#`

Berikan Screenshot dan Penjelasan

10. Setelah Anda mengetahui nama kolom dari sebuah table, tampilkan value dari kolom tersebut. Dengan menggunakan query berikut, dan ganti kolom1 dan kolom2 sesuai dengan column yang telah Anda temukan:

    `1 UNION SELECT kolom1,NULL,kolom2 FROM nama_table#`

Berikan Screenshot dan Penjelasan

11. Setelah Anda berhasil menemukan kredensial dari admin lakukan login pada laman flag, untuk mendapatkan flagnya.

Berikan Screenshot
Flag :

BAGIAN 2 (Cross-site Scripting)

2.1.2 DASAR TEORI

Cross-site scripting (XSS) merupakan serangan berjenis code injection yang memungkinkan penjahat untuk mengeksekusi kode jahat javascript di browser pengguna.

Penyerang tidak menarget korban secara langsung. melainkan ia akan mengeksploitasinya pada website yang dikunjungi korban sehingga website tersebut akan mengirimkan kode jahat javascript tersebut ke pengguna. Browser pengguna akan melihat kode tersebut sebagai bagian sah dari website dan website tersebut pada akhirnya menjadi kaki tangan penyerang

Sama seperti injection vulnerability lainnya, satu satunya cara agar dapat melakukan serangan adalah dengan menginjeksi kode jahat tersebut pada halaman web yang dimuat oleh korban pada suatu website. Hal ini dapat terjadi jika website tersebut langsung memasukkan input user ke halamannya karena penyerang dapat memasukkan string yang akan dianggap sebagai kode oleh browser korban.

Sebagai contoh, dibawah ini merupakan script server-side yang digunakan untuk menampilkan komen terakhir pada suatu website:

```
print "<html>"
print "Latest comment:"
print database.latestComment
print "</html>"
```

Script tersebut mengasumsikan komen hanya berisi teks. Namun, karena input user dimasukkan langsung, penyerang dapat memasukan komen seperti “<script> … </script>”. User manapun yang mengunjungi tautan tersebut akan menerima response dari script yang dimasukkan seperti berikut:

```
 <html>
Latest comment:
<script>...</script>
</html>
```

Dari sini, browser akan memuat halaman tersebut, mengeksekusi tags <script> dan attacker akan sukses dengan serangannya. Jika kita lihat sekilas, kemampuan mengeksekusi javascript pada browser korban mungkin tidak terlihat begitu berbahaya. Lagipula, javascript

berjalan di lingkungan yang sangat terbatas yang memiliki akses begitu minim ke file user dan sistem operasi.

Faktanya, kita bisa membuka javascript console pada browser dan mengeksekusi kode javascript apapun tanpa harus takut merusak komputer saat ini juga. Namun, potensi javascript sebagai kode jahat menjadi lebih jelas ketika kita memperhitungkan hal hal berikut:

- Javascript memiliki akses ke informasi sensitif pengguna seperti cookies dan session.
- Javascript dapat mengirim HTTP requests dengan konten semaunya dan destinasi yang juga semaunya dengan menggunakan XMLHttpRequest atau mekanisme lain.
- Javascript dapat membuat modifikasi semaunya ke HTML dari halaman web dengan menggunakan metode manipulasi DOM.

  Fakta ini akan sangat berbahaya dan memberikan kebocoran data jika dikombinasikan.

2.2.2 TUJUAN PERCOBAAN

1. Mahasiswa mampu memahami konsep Cross Site Scripting
2. Mahasiswa mampu mempraktikkan Cross Site Scripting

2.3.2 ALAT DAN BAHAN

Dalam rangka melaksanakan langkah-langkah praktikum yang terdapat pada bab ini, peserta praktikum perlu menyiapkan beberapa perangkat berikut:

- Perangkat komputer Desktop/Laptop dengan kapasitas RAM minimum 8 GB
- Perangkat lunak virtualisasi (Oracle VM VirtualBox/VMWare Workstation)
- Koneksi internet
- Beberapa tools yang dibutuhkan dalam praktikum

2.4.2 PROSEDUR PERCOBAAN

Instalasi Persiapan Lingkungan Praktikum

Berikut merupakan langkah-langkah yang perlu dilakukan dalam mempersiapkan kebutuhan praktikum :

1. Buka terminal pada sistem operasi Linux.
2. Kemudian lakukan cloning github repository untuk lab praktikum XSS:
   `git clone https://github.com/noverdy/ki-xss.git`
3. Masuk ke dalam direktori ki-xss dengan perintah:
   `cd ki-xss`
4. Melakukan build docker untuk sqli-part1 dengan perintah:
   `sudo docker-compose up -d`
5. Jalankan perintah berikut untuk mengecek apakah service sudah berjalan:

```
sudo docker ps
```

6. Apabila berhasil maka service akan berjalan pada port 1337, sehingga dapat mengakses pada browser dengan alamat localhost:1337

Stored XSS (Cross-site Scripting)

Berikut ini langkah-langkah yang perlu dilakukan dalam menyelesaikan lab praktikum:

1. Pertama lakukan pengujian HTML Injection pada bagian form Create Notes, berikan teks dengan ukuran h2 bertuliskan NIM Anda.

Berikan *Screenshot*

2. Berikutnya, Masukkan komentar dengan potongan kode berikut:

   <script>alert(“NIM ANDA”)</script>

   Mengapa hal tersebut dapat terjadi?

Berikan *Screenshot* dan Penjelasan

3. Berikutnya, kita akan menampilkan session cookie milik kita dengan kode berikut:
   <script>alert(document.cookie)</script>

   Jelaskan mengapa kita dapat menampilkan session cookie milik kita dengan kode di atas.

Berikan *Screenshot* dan Penjelasan

2.5. KESIMPULAN

Pada bagian ini, tulislah kesimpulan apa saja yang didapat dari hasil melaksanakan kegiatan-kegiatan pada bab ini.
