Rakamin

Secure Coding

Cross-Site Scripting
(XSS) & SQL Injection

Rakamin

XSS & SQL Injection – Ancaman Tak Terlihat

Badan Siber dan Sandi Negara (BSSN) menerima **332** aduan siber sepanjang **2021**. Untuk jenis serangan yang paling banyak dilaporkan ialah serangan *SQL Injection* sebanyak **79** aduan.

"Mengapa XSS & SQL Injection Masih Menjadi Musuh Utama Developer?"

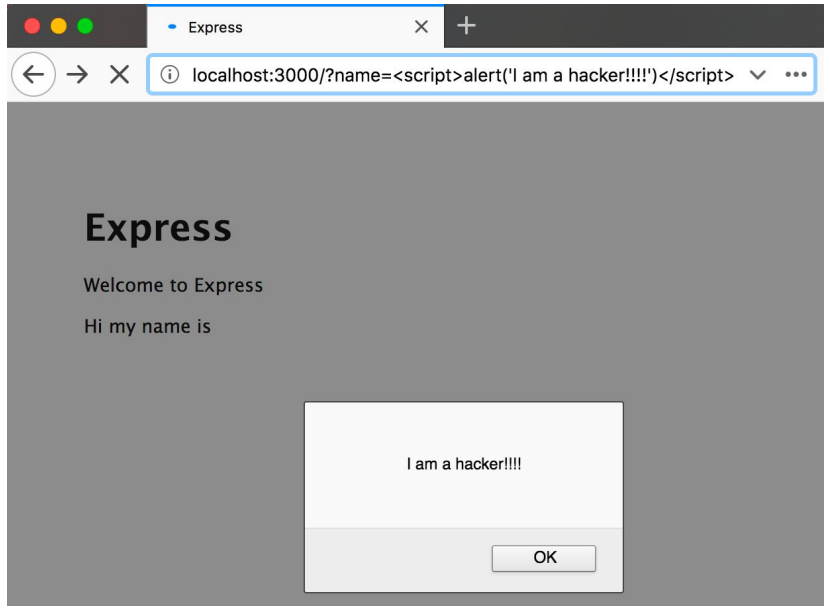
1. **XSS** membahayakan **end-user/pengguna akhir**:
   - Contoh: Akun e-wallet diretas karena klik popup jahat di situs e-commerce.
2. **SQL Injection** menghancurkan **bisnis**:
   - Contoh: Database 500 ribu pelanggan startup healthtech bocor karena kueri tidak aman.

sumber

Rakamin

1. Cross-Site Scripting (XSS)

Serangan di mana penyerang menyisipkan skrip jahat (biasanya JavaScript) ke halaman web, yang dieksekusi oleh korban saat mengaksesnya.



Contoh Kasus di Indonesia:

- Penyerang menyisipkan `<script>alert("Akun Anda diretas!")</script>` di kolom komentar e-commerce.
- Pengguna yang membuka halaman tersebut melihat pop-up atau diarahkan ke situs phishing.

Jenis XSS:

1. **Reflected XSS**: Skrip jahat tercermin dari input pengguna (misal: melalui URL atau form pencarian).
   - Contoh: `https://tokopedia.com/search?query=<script>malware()</script>`
2. **Stored XSS**: Skrip disimpan di server (misal: di database komentar).
3. **DOM-based XSS**: Manipulasi DOM browser tanpa melibatkan server.

Rakamin

1. Cross-Site Scripting (XSS)

Dampak:

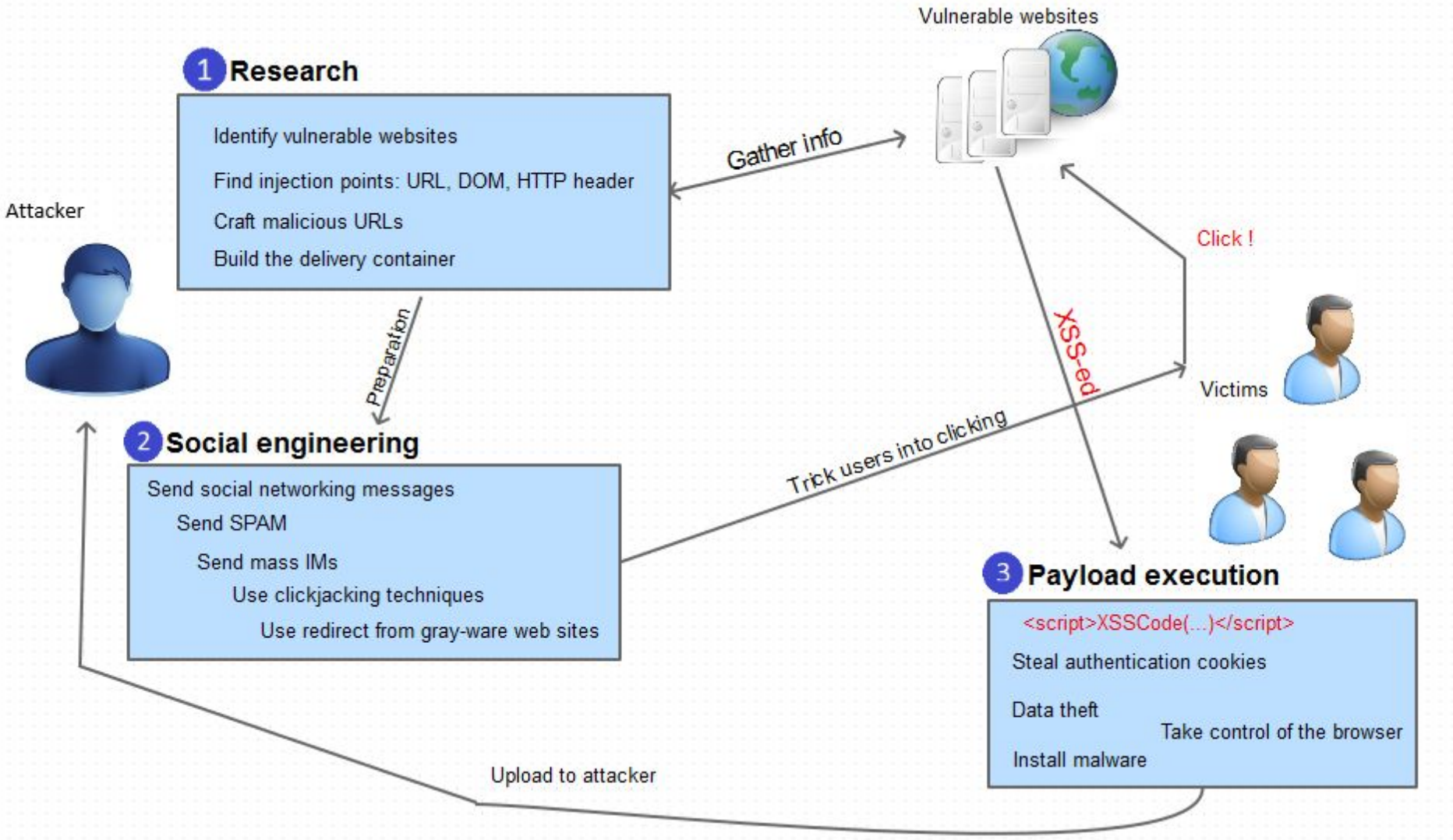
- Pencurian cookie/sesi login (misal: akun e-wallet atau bank digital).
- Defacement halaman web.
- Redirect ke situs palsu (phishing).

Mitigasi:

- **Sanitasi Input**: Filter karakter khusus seperti `<`, `>`, `&` dengan library seperti `DOMPurify`.
- **Content Security Policy (CSP)**: Blok eksekusi skrip dari sumber tidak tepercaya.
- **Escaping Output**: Gunakan `htmlspecialchars()` (PHP) atau template engine (React, Vue).

sumber

1. Cross-Site Scripting (XSS)



2. SQL Injection

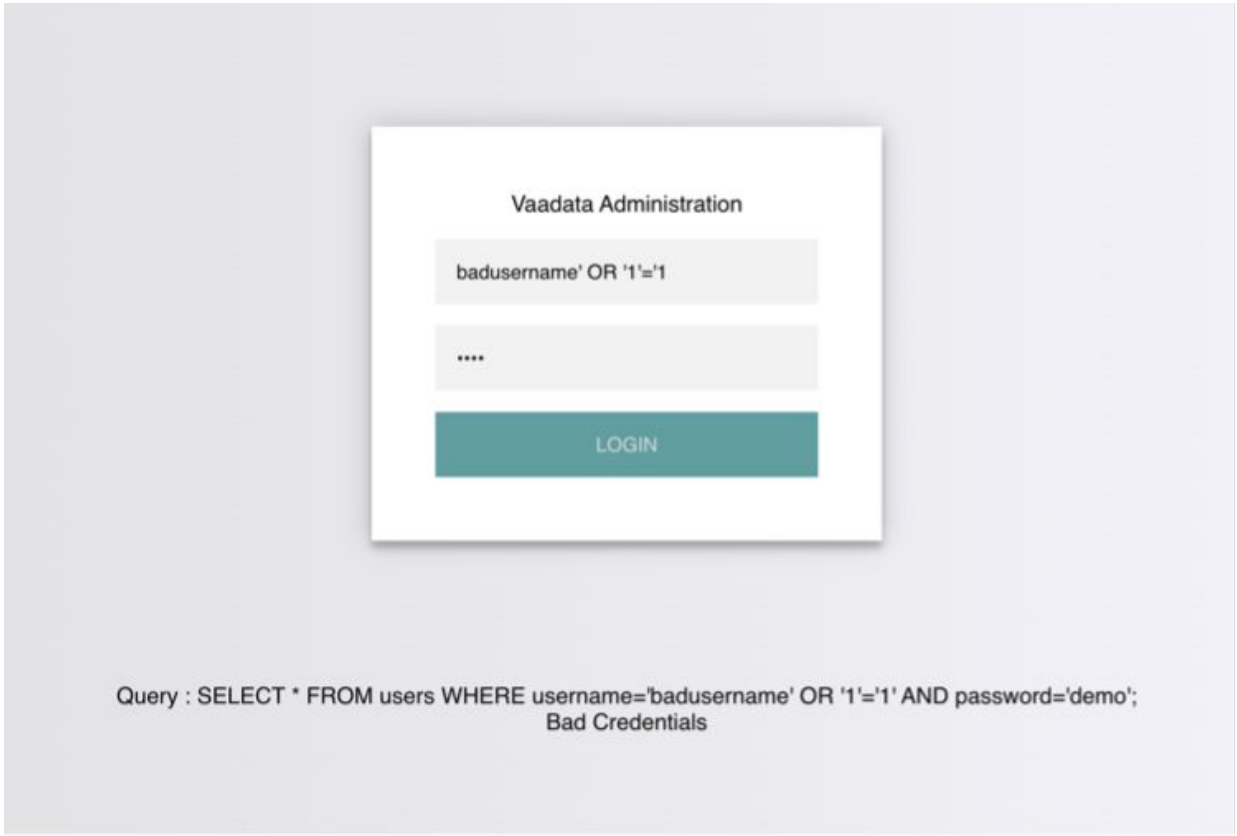
Serangan di mana penyerang menyuntikkan kueri SQL jahat melalui input pengguna untuk memanipulasi database.

Contoh Kasus di Indonesia:

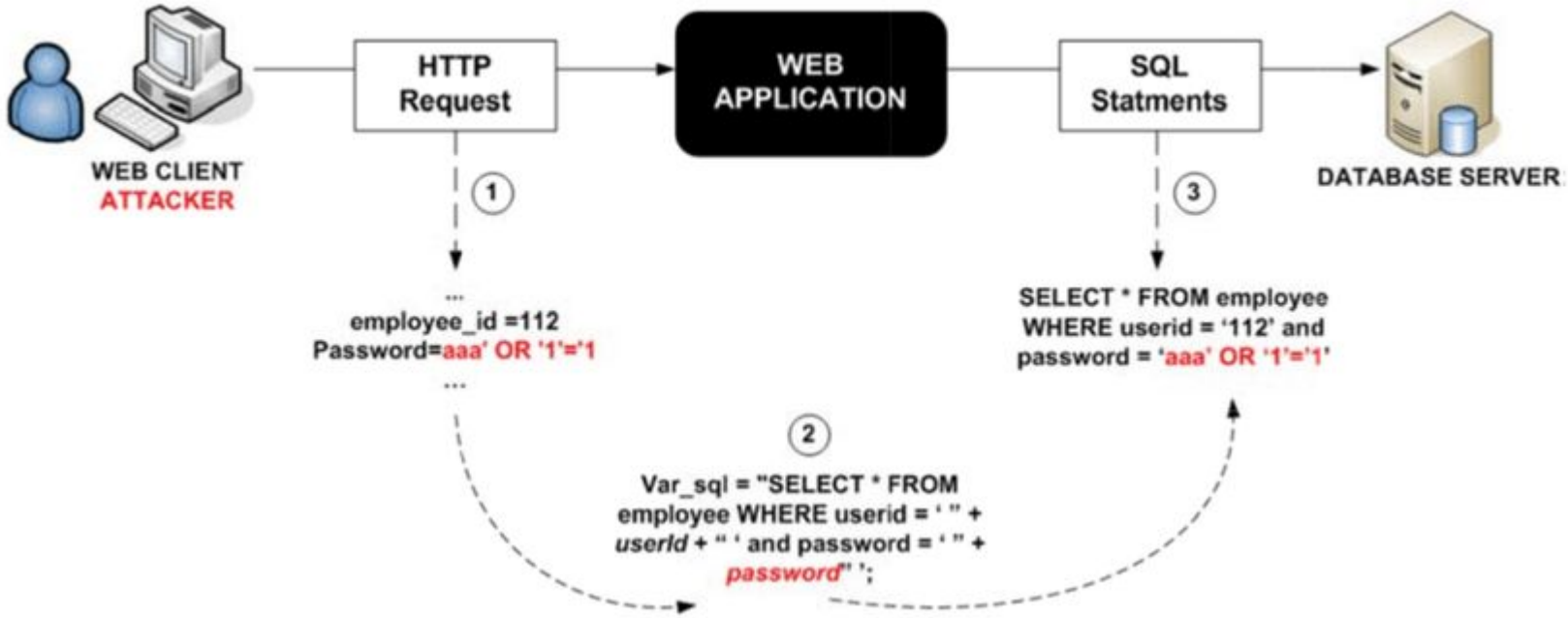
- Penyerang memasukkan `' OR 1=1 --` di kolom login, sehingga bisa masuk tanpa password.
- Kebocoran data nasabah bank karena kueri SQL tidak aman.

Jenis SQL Injection:

1. **Classic SQLi**: Manipulasi kueri langsung (contoh: UNION SELECT).
2. **Blind SQLi**: Menebak struktur database dari respons error/waktu tanggap.
3. **Boolean-based**: Mengeksploitasi logika TRUE/FALSE.



2. SQL Injection



Rakamin

2. SQL Injection

Dampak:

- Pencurian data sensitif (nomor KTP, rekening bank).
- Penghapusan atau modifikasi database.
- Takeover sistem (RCE - Remote Code Execution).

Mitigasi:

- **Prepared Statements**:

```
$stmt = $pdo->prepare('SELECT * FROM users WHERE email = :email');
$stmt->execute(['email' => $email]);
```

- **Input Validation**: Batasi input hanya ke format yang diizinkan (misal: email harus mengandung `@`).
- **ORM**: Gunakan ORM seperti Laravel Eloquent atau Django ORM untuk menghindari SQL mentah.

sumber

Rakamin

Perbandingan XSS vs SQL Injection

Aspek	XSS	SQL Injection
Target	Browser pengguna	Database server
Teknik Serangan	Skrip jahat di HTML/JS	Kueri SQL dimodifikasi
Dampak Umum	Pencurian sesi, phishing	Kebocoran data, penghapusan data
Tools Deteksi	OWASP ZAP, Burp Suite	SQLMap, Acunetix

Regulasi & Standar Indonesia

- **UU PDP No. 27/2022**: Wajib lindungi data pribadi dari kebocoran (termasuk via XSS/SQLi).
- **Permenkominfo No. 20/2016**: Keamanan sistem elektronik harus mencakup sanitasi input/output.

Rakamin

TERIMA KASIH