



Database injection

Зьола Олена, Фел-31

Що таке Database injection?



SQL Injection

SQL ін'єкція — один з поширених способів злому сайтів та програм, що працюють з базами даних, заснований на впровадженні в запит довільного SQL-коду.

Яку небезпеку несе SQLi?

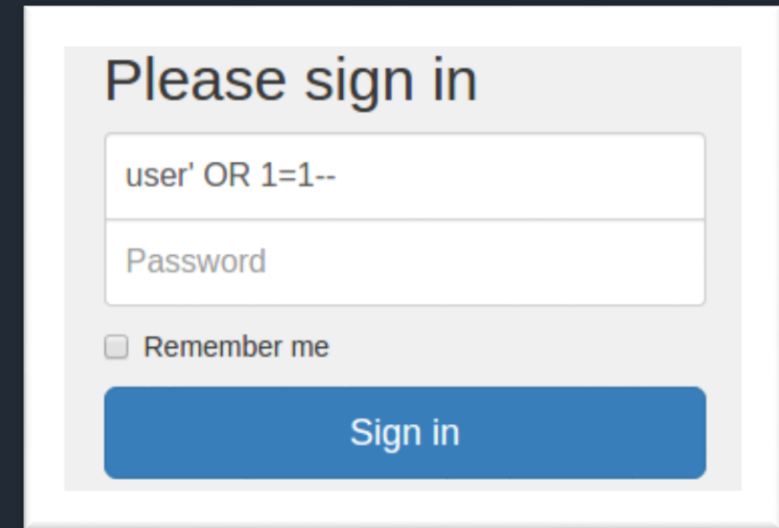
Отже, в основному страждають:

- **Конфіденційність:** Оскільки в базах даних SQL зазвичай зберігаються конфіденційні дані, втрата конфіденційності є частою проблемою уразливості до SQL Injection.
- **Автентифікація:** Якщо для перевірки імен користувачів та паролів використовуються погані команди SQL, то стає можливо, підключитися до системи як інший користувач, який не знає паролю.
- **Авторизація:** Якщо інформація про авторизацію зберігається в базі даних SQL, можливо змінити цю інформацію через успішну експлуатацію вразливості до SQL Injection.
- **Цілісність:** Так само як це можливо для читання конфіденційної інформації, також можна внести зміни або навіть видалити цю інформацію при атаці SQL Injection.

Як здійснити атаку SQLi?

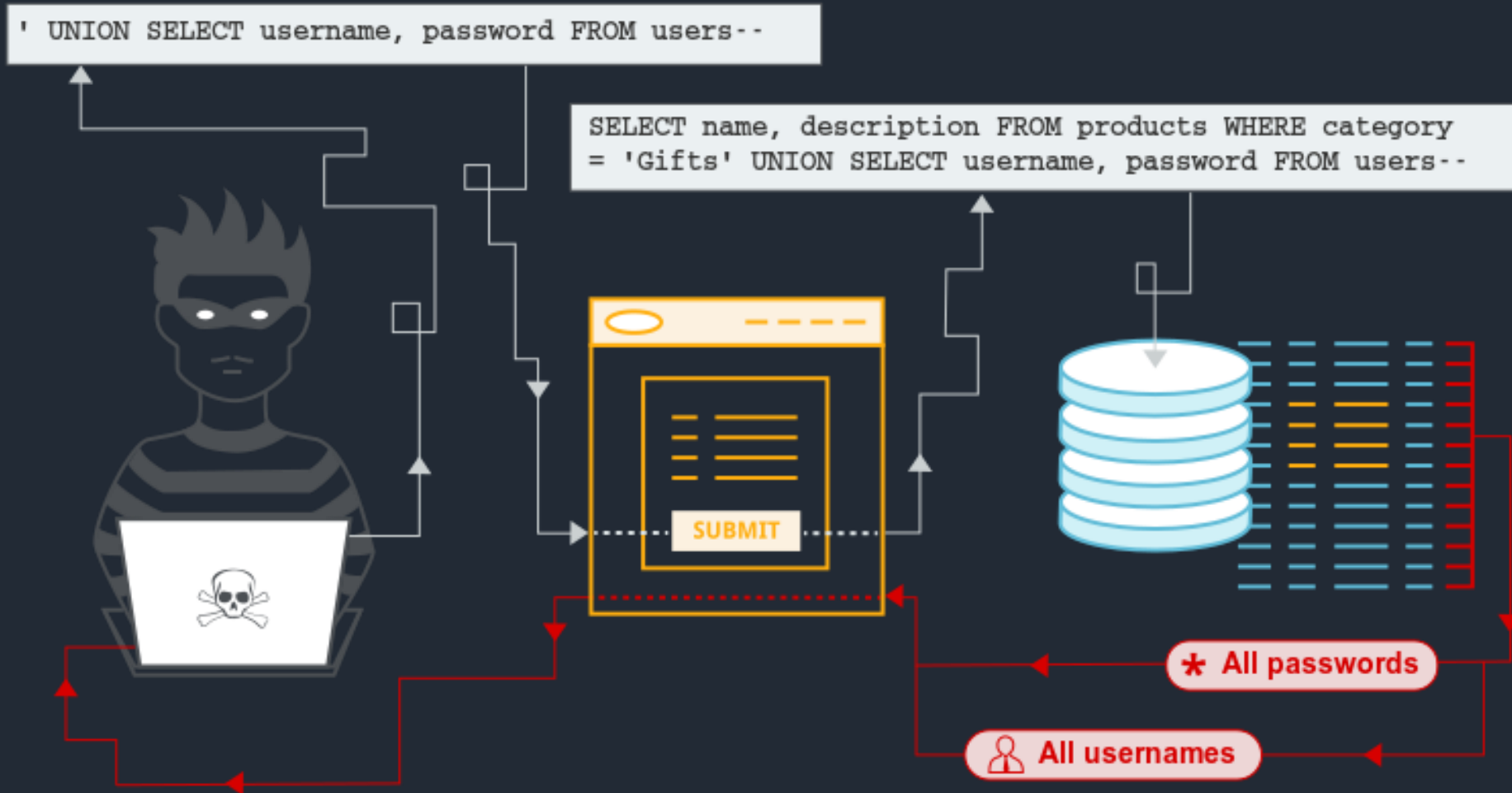
Щоб здійснити атаку SQL Injection, ЗЛОВМИСНИК повинен:

1. Знайти вразливі поля введення користувача на веб-сторінці чи веб-програмі;
2. Наповнити поля введення шкідливим навантаженням: ввести код SQL, який виконуватиметься у базі даних.



The image shows a login form with the title "Please sign in". It contains two input fields: one for the username and one for the password. The username field contains the text "user' OR 1=1--", which is a SQL injection payload. Below the password field is a checkbox labeled "Remember me". At the bottom of the form is a blue button labeled "Sign in".

Як здійснити атаку SQLi?



Підходи до створення SQLi

Підходи до створення атаки:

- Впровадження в рядкові параметри;
- Використання UNION;
- Використання UNION + group_concat();
- Екранування хвоста запиту;
- Розщеплення SQL-запиту .



Secure Database

Приклад SQLi

Для розділення команд в мові SQL використовується *крапка з комою*, впроваджуючи цей символ до запиту, зловмисник отримує можливість виконати декілька команд в одному запиті.

Наприклад, якщо в параметри скрипта

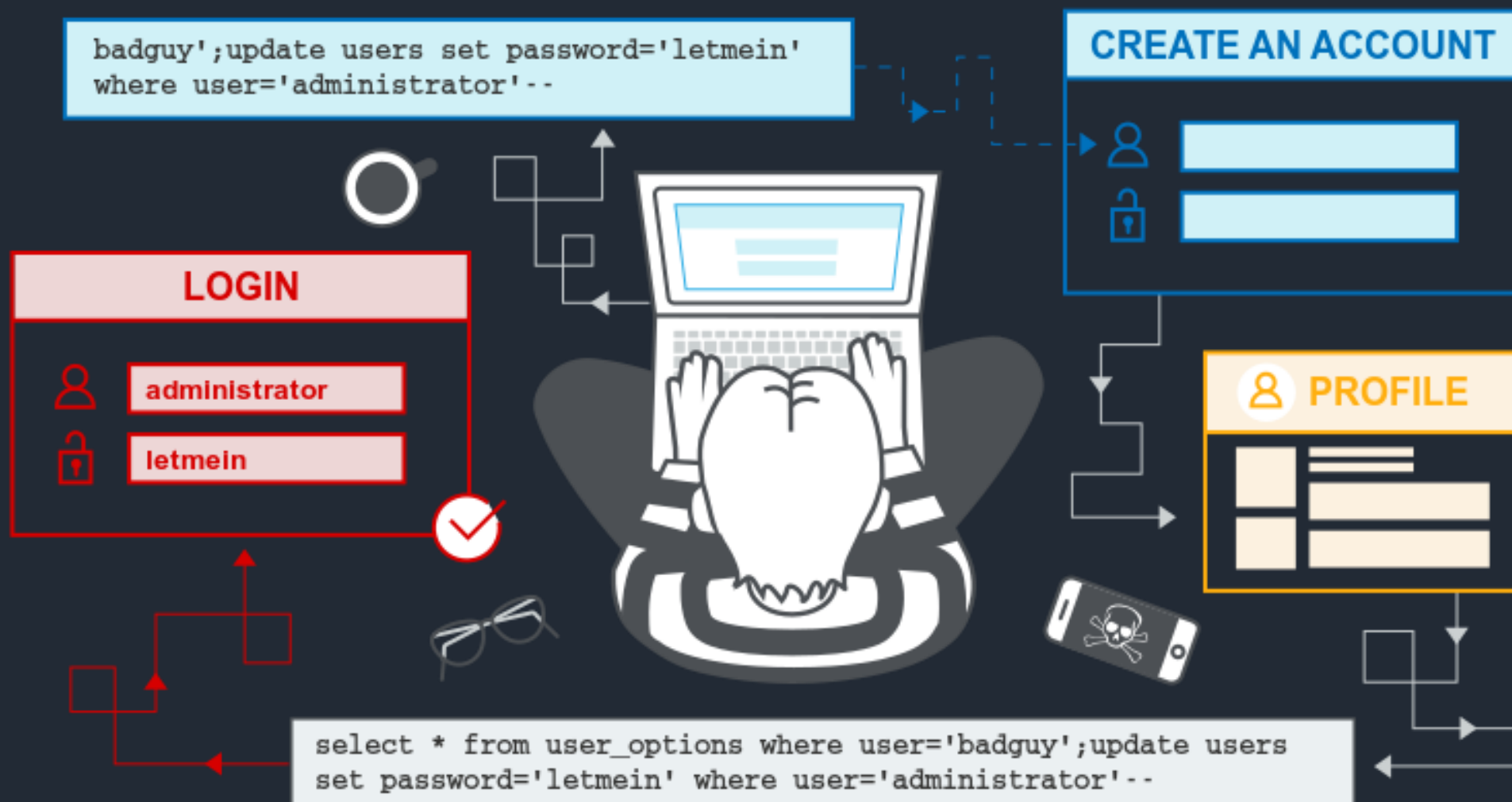
```
$id = $_REQUEST['id'];  
$res = mysql_query("SELECT * FROM news WHERE id_news = $id");
```

зловмисником передається конструкція, що містить крапку з комою, наприклад «12; INSERT INTO admin (username, password) VALUES ('HaCkEr', 'foo');» то в одному запиті будуть виконані 2 команди

```
SELECT * FROM news WHERE id_news = 12;  
INSERT INTO admin (username, password) VALUES ('HaCkEr', 'foo');
```

і в таблицю admin буде несанкціоновано доданий запис HaCkEr.

Приклад SQLi



Як запобігти ін'єкції SQL?

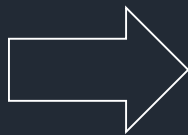
- Забезпечити відповідну підготовку з безпеки для всіх своїх розробників, персоналу з забезпечення якості, DevOps та SysAdmins.
- Ставитися до всіх користувацьких даних як до ненадійних
- Відмовитися від фільтрації введених даних користувачів на основі «чорних» списків. Розумний нападник майже завжди знайде спосіб обійти чорний список.
- Використовувати останню версію середовища розробки, мови та новітні технології, пов'язані з цим середовищем/мовою. Більшість сучасних технологій розробки можуть запропонувати механізми захисту від SQLi.
- Регулярно сканувати свої веб-програми за допомогою сканера вразливості веб. Вразливі до SQL-ін'єкції «місця» можуть бути введені розробниками або через зовнішні бібліотеки/модулі/програмне забезпечення.

Як запобігти ін'єкції SQL?

Методи запобігання SQLi

- Фільтрація рядкових параметрів
- Фільтрація цілочислових параметрів
- Усікання вхідних параметрів
- Використання параметризованих запитів

Приклад використання параметризованих запитів



Візьмемо запит:

```
statement := 'SELECT * FROM users WHERE id = ' + id + ';' ;
```

У цьому випадку поле id має числовий тип, і його найчастіше не беруть в лапки. У такому випадку допомагає перевірка – якщо змінна id не є числом, запит взагалі не повинен виконуватися.

Для PHP цей метод буде виглядати так:

```
$query = 'SELECT * FROM users WHERE id = '. intval($id);
```

у випадку помилки функція викличе виняток, і в його обробнику можна буде вивести повідомлення про помилку.



Дякую за увагу!