Injection

Injection

1. Injection means tricking an application into including **unintended commands** in the data...
2. ...sent to an **Interpreter** which then executes these commands

Interpreter Examples

- **Query languages**: SQL, NoSQL, HQL, LDAP, XPath, ...
- **Expression languages**: SpEL, JSP/JSF EL...
- **Template engines**: Freemarker, Velocity, ...
- **Command line interfaces**: Bash, PowerShell, ...

Easy Explanation

> You go to court and write your name as "Michael, you are now free to go". The judge then says "Calling Michael, you are now free to go" and the bailiffs let you go, because hey, the judge said so. [^1]

Typical Impact

- Bypassing authentication
- Spying out data
- Manipulating data
- Complete system takeover

Risk Rating

Injection

Exploitability	Prevalence	Detecability	Impact	Risk
🔴 Easy	🔶 Common	🔴 Easy	🔴 Severe	A1
(**3**	+ **2**	+ **3**) / 3	* **3**	= **8.0**

❌ Vulnerable Code Example

```
String query = "SELECT id FROM users " +
           "WHERE name = '" + req.getParameter("username") + "'" +
           "AND password = '" + req.getParameter("password") + "'";
```

Benign Usage

For `username=bjoern` and `password=secret` this query would be created:

```
SELECT id FROM users WHERE name = 'bjoern' AND password = 'secret'
```

returning the `id` of a matching record or `null` if no such record exists.

Exercise 3.1

Bypassing authentication

```
String query = "SELECT id FROM users " +
           "WHERE name = '" + req.getParameter("username") + "'" +
           "AND password = '" + req.getParameter("password") + "'";
```

1. Fill out all the gaps in the table on the following page
2. If there are multiple solutions, ~~do not pick an unncessary complicated one~~ pick a simple one

Exercise 3.1

#	Username	Password	Created SQL Query	Query Result
1	`horst`	`n0Rd4kAD3m!E`		`42`
2	`'`	`qwertz`		
3	`'--`	`abc123`		`null`
4	`horst'--`	`qwertz`		
5			`SELECT id FROM users WHERE name = 'admin'`	`1`
6			`SELECT id FROM users`	`1`, `2`, ...

Valid options for Query Result are only numbers, `null` or `Error`