

Motivation

The famous "Little Bobby Tables" comic shows what can happen when websites fail to handle user input properly: systems can break or important data can be lost. In real life, these flaws can cause stolen information, financial damage, and serious privacy concerns. This project turns Bobby's fictional school database into an intentionally vulnerable website that helps users learn about web security through safe, hands-on experience



SQL Injection

- What if someone could unlock a vault of private data and trick a website into revealing its secrets just by typing sneaky sentences?
- SQL Injection happens when a hacker puts special text into a search box or login field to manipulate the database behind the scenes.

Search Teacher:

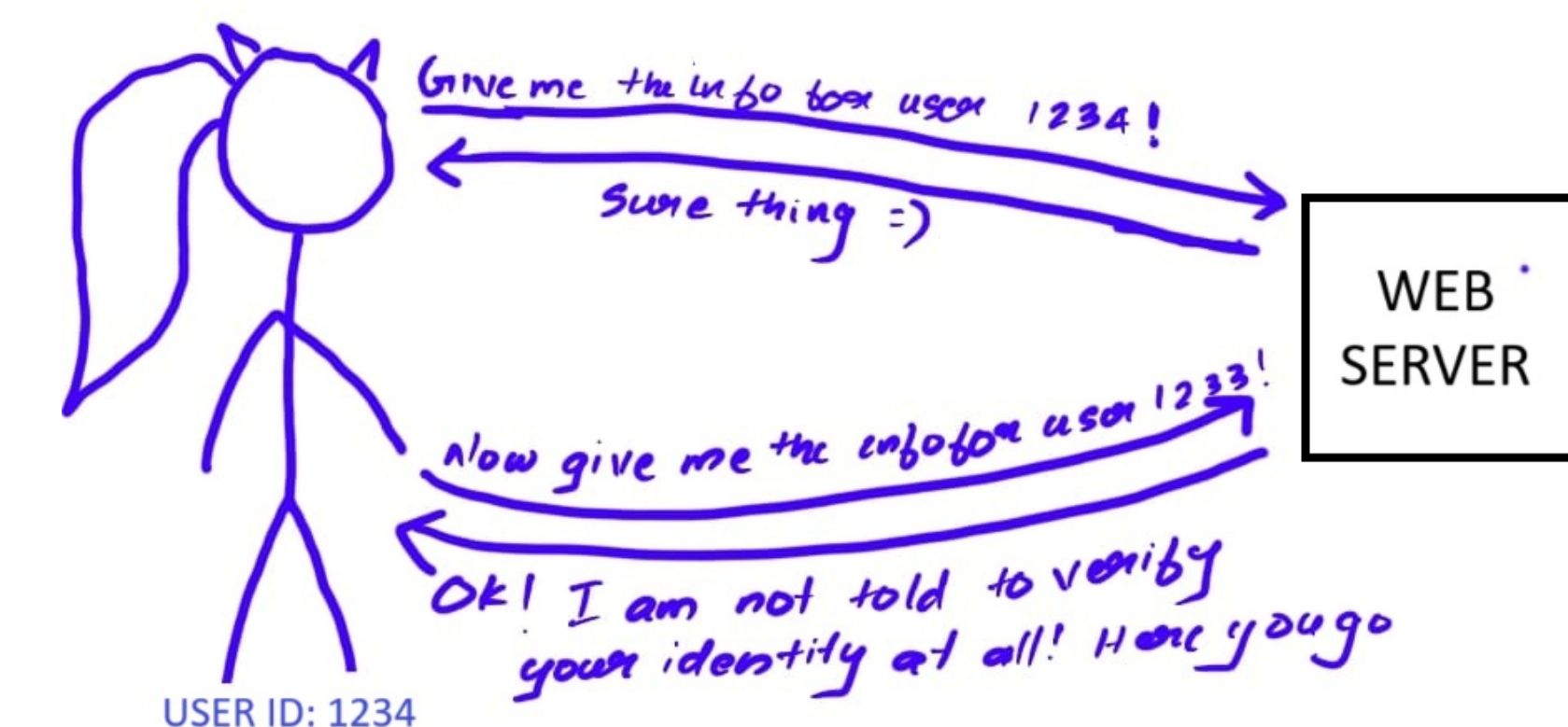

```
SELECT * FROM table_name WHERE column_name = 'Bobby';
```

Search Teacher:


```
SELECT * FROM table_name WHERE column_name = '' or 1=1 -- ;
```

IDOR (Insecure Direct Object Reference)

- Imagine everyone has their own locker, but all it takes to open someone else's is changing a number on the door.
- When websites use predictable URLs or IDs without checking who's asking, attackers can just try other numbers and see private info that's not theirs without logging in as someone else.



Security Misconfiguration

- It's like locking your front door and putting a security alarm on your front door, but leaving your windows wide open.
- Systems often have hidden settings or default features that need to be locked down. If they're left open attackers can sneak in without breaking anything.

