JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Web Application Vulnerabilities

VULNERABILITY MANAGEMENT

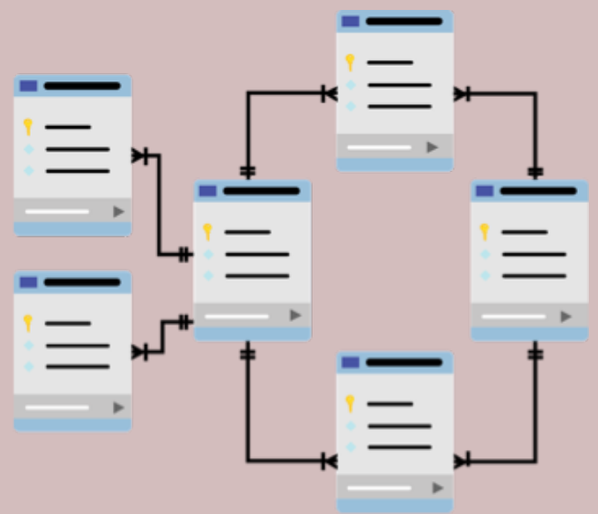
Web Application Vulnerabilities

- Injection Attacks
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Injection Attacks

- Send commands through a web server to a backend system, bypassing the normal security controls
- Most commonly done as an SQL inject
- Prevent this through input validation and using least privilege for the databases



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

SQL Injection Attacks

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

User ID: jason

Password: mypassword

```
select * from Users where user_id= ‘jason’ and password = ‘mypassword’
```

User ID: ' OR 1=1; /*

Password: */--

```
select * from Users where user_id= ‘` OR 1 = 1; /* ‘ and password =‘ */--’
```

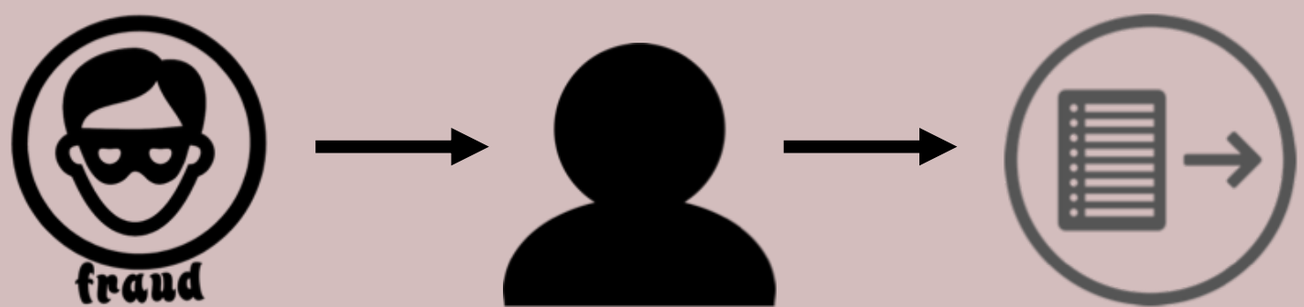
Cross-Site Scripting (XSS)

- Attacker embeds scripting commands on a website that is executed by a regular user without knowing it
- Victim in this case is the regular user, not the server
- If one of these are discovered during a scan, you need to work with the developer to fix the code and setup proper controls to prevent it in the future

Cross-Site Request Forgery

- Attacker forces a user to execute actions on web server which they authenticated

- Attacker cannot see web server's response, but this attack can be used to have victim transfer funds, change their password, etc.



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Web Application Scans

- Nessus and Qualysguard can scan for web vulnerabilities, but they aren't specialized (like Nikto) to do it