# IT666 – Web Attacks Lab 2/10/2021

# [RJS1070@wildcats.unh.edu](mailto:RJS1070@wildcats.unh.edu) Ryan J. Skelly

Lab Report: Answer the following 20 questions (5 points each) from the Hacksplaining site

1: List 3 attacks the Hacksplaining assigns the prevalence as RARE.

1. Dom Based Cross Site Scripting
2. Session Fixation
3. XML External Entities

2: List one of the two attacks the Hacksplaining assigns the exploitability as DIFFICULT.

Ensuring Correct Encryption

3: List 3 attacks the Hacksplaining assigns the impact as DEVASTATING.

1. Password Mismanagement
2. Privilege Escalation
3. Weak Session ID

4: True/False: Does Hacksplaining assign any attacks as COMMON, EASY, and DEVASTATING?

No, It doesn’t … False?

5: Which injection attack allows an attacker to run arbitrary statements on a database?

SQL Injection

6: Which protection will protect all 3 XSS variants?

1. Escape Dynamic Content
2. Whitelist Values
3. Implement a Content-Security Policy
4. Sanitize HTML
5. Use a JavaScript Framework
6. Audit Your Code Carefully
7. Parse JSON Carefully
8. Detect Unsafe Code Using Development Tools
9. Don’t Use URI Fragments at All!

7: By exploiting XSS hackers have spread worms on social media sites like Facebook, Twitter and YouTube.

True

8: How would running your server in a chroot jail limit the impact of command execution vulnerabilities?

It restricts which directories the web-server process can access, limiting the damage an attacker can do.

9: List three clickjacking protections

1. X-frame-options
2. Content-security-policy
3. Frame-Killing JavaScript

10: Why is it a good idea to restrict what directories on disk your web server can access?

It restricts the harm an attacker could do, if they manage to find a way to access the disk through a server vulnerability.

11: True or False: if a page isn’t linked to anywhere on your site, it can’t be accessed by an attacker.

False

12: The Let's Encrypt project - sponsored by Mozilla, Facebook, and the Electronic Frontier Foundation - aims to make encryption ubiquitous across the web by eliminating which three tasks?

1. Payment
2. Web server configuration
3. Certificate renewal
4. Secure key storage

13: True or False: User enumeration vulnerabilities allow hackers to circumvent your login screen.

True

14: True or False: Privilege escalation vulnerabilities are system flaws that grant a malicious user excessive or wrong permissions after they have authenticated themselves. (These are distinct from session hijacking vulnerabilities that allow an attacker to impersonate another user.)

True

15: What two are good methods of generating session IDs?

1. UUIDs.
2. User IDs.
3. Login time in milliseconds.
4. Strong random numbers.

16: How can you ensure cookies are not tampered with?

1. Mark them as HTTP-only cookies.
2. Only send the cookies over HTTPS.
3. Encrypt them.
4. Use a digital signature.

17: Which protection mitigates both XML Bomb and XML External Entity attacks?

1. Disable Parsing of Inline DTDs
2. Consider Making XML Parsing Asynchronous
3. Throttle Uploads Per Client
4. Limit the Permissions of Your Web Server Process

18: Why is it important to separate code and configuration?

1. So you can deploy the same code in different environments without sharing access credentials.
2. Configuration files are always encrypted.
3. It helps enforce a strong password policy.

19: Toxic dependencies. Why is an ad-hoc build process a security risk?

1. If you can’t be sure what software you are running, you can’t be sure it is secure.
2. You will not be able use encryption.
3. It limits the file sizes you can deploy to servers.

20: List 5 things you should NOT Log

1. Usernames & Passwords
2. Encryption & API Keys
3. Session IDs and cookies
4. Email Addrs
5. Credit and CVV Info