CodePath

Week 3

CS 4760 F18
Christopher Raley

Codepath Homework

Security Shepherd (Challenges 0-4)

No CTF

Topics

Week 3

Readings available on CodePath Course website

- **Cross-Site Scripting (XSS)**
- Clickjacking
- HTML Tags

Cross-Site Scripting (XSS)

- Ranked #3 security threat by OWASP
- Majority of websites like to use JavaScript
- Users can inject their own scripts if the input on websites are not ***properly*** sanitized
    - Another example of injection attack
        - Recall SQLi last week

Cross-Site Scripting (XSS)

- Attackers can steal your cookies or other private data
- Cookies here in this case will be like session ID’s
- Can be any script injection, but most commonly Javascript
    - Majority of web applications use it

Cross-Site Scripting (XSS)

1. Persistent XSS
    a. Originates from website's database
2. Reflected XSS
    a. Originates from client-side request
3. DOM-based XSS
    a. Cross between persistent and reflected

Why is this relevant?

A Year Later, XSS Vulnerability Still Exists in eBay

```
<SCRIPT>alert('XSS')</SCRIPT>
<IMG SRC="#" ONERROR="alert('XSS')"/>
<INPUT TYPE="BUTTON" ONCLICK="alert('XSS')"/>
<IFRAME SRC="javascript:alert('XSS');"></IFRAME>
```

Lab 3

XSS