Week 3 – Command Injection

Introduction to Offensive Security

Command Injection?

- Everybody loves command line utilities
- User input could often be passed in as arguments
  - Media conversion
  - Text to speech
  - Basically anything that has a nice CLI but no API for the language youre in
    - Or even if it does have an API…

Command Injection?

- Example: `ffmpeg -i '$url' … out.mp4`
- If URL is attacker-controlled and not sanitized…
  - Same "essential" issue as SQLi
- Unlike SQL, `system/exec/pass_thru`/etc. dont limit the number of commands per call

Command Injection

```
ffmpeg -i '$url' … out.mp4
```

```
$url = "'; rm -rf --no-preserve-root /;"
```

Demo

Bypassing Character Restrictions

- Often times certain characters will be limited to make the injection harder
  - spaces
  - semicolon
- Spaces can be replaced with ${IFS}
  - Shell environment variable which almost always contains space
- Semicolons
  - Usually able to be replaced with && or ||

Testing for Cmd Injection

- Much like SQLi, its often blind
- Entering some combination of quotes, semicolons, etc. is usually the best thing to get started
- Its usually pretty obvious based off of the purpose of the website
  - Again, media conversion is a big one
  - Also, networking tools (ping, traceroute, etc.)