CSCI 3330 Cybersecurity

Word of the day

LARVAL STAGE n. Describes a period of monomaniacal concentration on coding apparently passed through by all fledgling hackers. Common symptoms include the perpetration of more than one 36-hour hacking run in a given week; neglect of all other activities including usual basics like food, sleep, and personal hygiene; and a chronic case of advanced bleary-eye. Can last from 6 months to 2 years, the apparent median being around 18 months. A few so afflicted never resume a more ‘normal’ life, but the ordeal seems to be necessary to produce really wizardly (as opposed to merely competent) programmers. A less protracted and intense version of larval stage (typically lasting about a month) may recur when one is learning a new OS or programming language.

XSS: three types

1) ?
2) ?
3) ?

XSS: three types

1) Non-persistent
2) Persistent
3) DOM-based

File systems

- What is a directory?

Directories

- A special file
- A list of links to files (including directories)
- Two special links

Special links

- . – current directory
  - Where have we seen these before?
- .. – parent directory (with one exception)
  - Where have we seen these before?

Special links

- . – current directory
  - Firewall evasion, escaping getopt CLI
- .. – parent directory (with one exception)
  - Directory traversal attacks

What is a path?

- A string of file names separated by slashes
- Provides route to file
- / means start at root
- Otherwise, relative to current working directory

Informed by the above experimentation about which attempts succeeded and which failed, speculate using pseudocode or code in any language what you think the service's code for writing uploaded files to the file system might look like, highlighting the vulnerability.

- Premise: absolute path directory traversal attacks failed but relative paths succeeded

```
def save_file(f, name):
    with open('/mnt/out/' + name, 'wb') as fout:
        fout.write(f.read())
```

```
def save_file(f, name): # what if name is a path?
    with open('/mnt/out/' + name, 'wb') as fout:
        fout.write(f.read())
```

- We see paths everywhere
- https://www.bowdoin.edu/academics/../../../../../academics/index.html
- https://athletics.bowdoin.edu/news/2025/../2025/./../../9/28/consistent-scores-lead-womens-golf-to-eighth-at-williams-invitational.aspx

Cross-site request forgeries (CSRF)

- Same origin policy: scripts from one origin should not be able to read or manipulate content from another origin

Cross-site request forgeries (CSRF)

- Same origin policy: scripts from one origin should not be able to read or manipulate content from another origin
- But… you can still submit content

Demo

- https://jeffreyknockel.com/csrf.html
- https://tildesites.bowdoin.edu/~j.knockel/gradebook.php

Mitigations

- CSRF tokens
- Sec-Fetch-Site
  - cross-site
  - same-origin (same scheme, host, and port)
  - same-site (same pay-level domain)
  - none

Assignment 3

- Deadline: October 2, 2025, 10:00pm
- Unix permissions, SQL, and SQL injection vulnerabilities
  https://tildesites.bowdoin.edu/~j.knockel/csci3330f25/assignment3.pdf