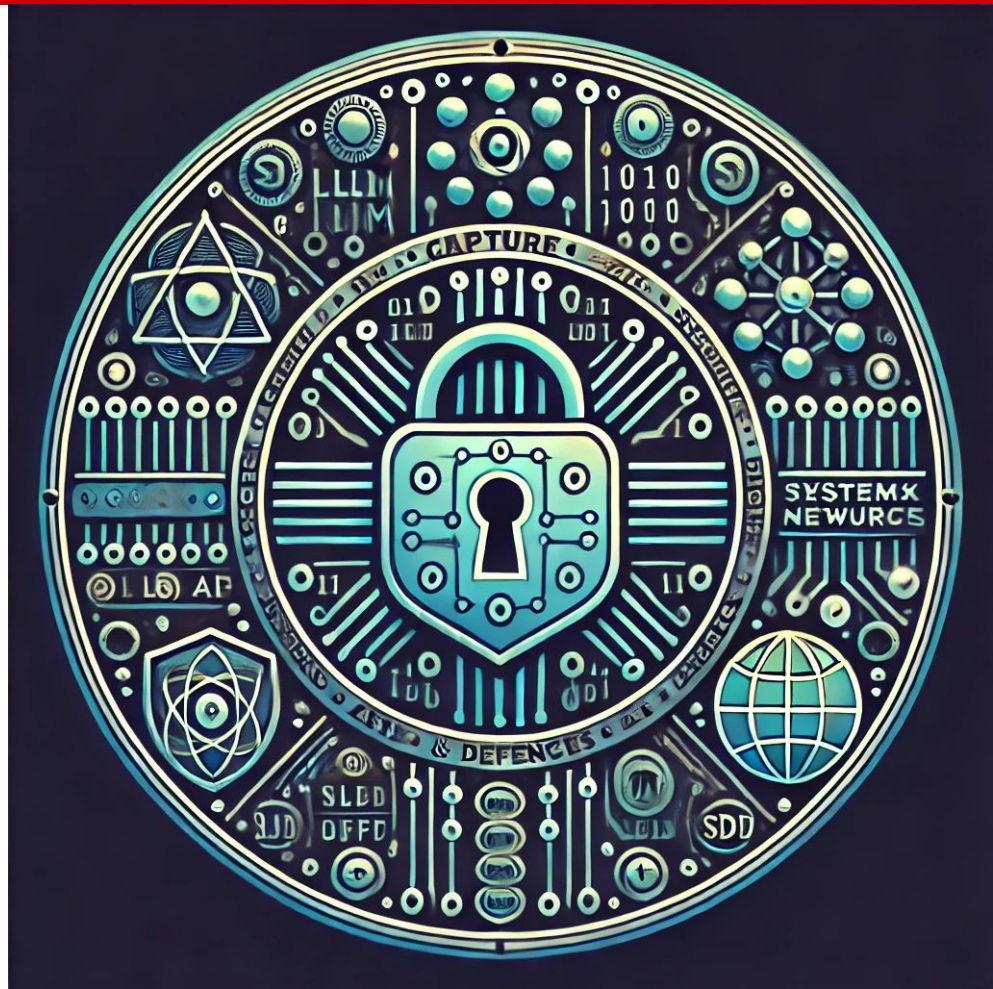
CSC-537
Systems Attacks and Defenses Vulnerabilities

Alexandros Kapravelos
akaprav@ncsu.edu

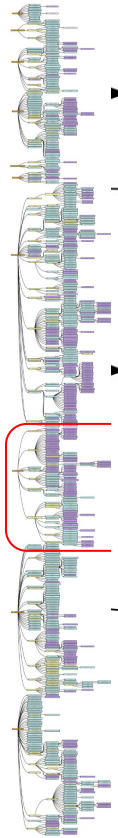


How do we communicate vulnerabilities?

- Common Weakness Enumeration (CWE)
- Common Vulnerabilities and Exposures (CVE)

NIST National Vulnerability Database

CVE feed



79 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

91 - XML Injection (aka Blind XPath Injection)

93 - Improper Neutralization of CRLF Sequences ('CRLF Injection')

94 - Improper Control of Generation of Code ('Code Injection')

80 - Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

81 - Improper Neutralization of Script in an Error Message Web Page

83 - Improper Neutralization of Script in Attributes in a Web Page

84 - Improper Neutralization of Encoded URI Schemes in a Web Page

85 - Doubled Character XSS Manipulations

86 - Improper Neutralization of Invalid Characters in Identifiers in Web Pages

87 - Improper Neutralization of Alternate XSS Syntax

113 - Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting')

1336 - Improper Neutralization of Special Elements Used in a Template Engine

95 - Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection')

96 - Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection')

source

How to report a vulnerability?

- Bug bounty programs
- A `security.txt` file on the website at `/.well-known/security.txt` (RFC 9116)
- Direct organization channels
  - An existing issue tracking system
  - Generic email addresses such as `security@` or `abuse@`
  - Social media

Memory and Resource Management

- NULL Pointer Dereference
- Integer Overflow
- Race Conditions
- Memory Buffer Bounds Violations
  - Overflows
  - Memory corruption
- Out-of-bounds Write
- Out-of-bounds Read
- Use After Free

Injection Vulnerabilities

- SQL injection
- Command injection
- Cross-site scripting (XSS)
- Code injection

Security misconfigurations

- Default credentials
- Default settings risks
- Cloud storage misconfigurations (exposed S3 buckets)
- Permission Problems
- Error Handling
- Filesystem exposure (directory listing, code leaks, internal file structures, etc)

Component Vulnerabilities

- Package Dependencies
  - Malicious packages
  - Dependency confusion
  - Vulnerable libraries
- Development Tools
  - Compromised build systems, build tools, and CI/CD pipelines
  - Compromised development stack (editor, frameworks, dev tools)
- Configuration management tools (Ansible, Puppet, etc)
- Package management software and ecosystems

Broken Access Control

- Missing Authentication for Critical Functions
- Improper Authentication
- Use of Hard-coded Credentials
- Missing Authorization
- Incorrect Authorization

Cryptographic Failures

- Insufficient entropy
- Pseudo-Random Number Generator (PRNG) problems
- Protocol Vulnerabilities (downgrade attacks, etc)
- Encryption Issues

SANS CWE Top 25

Rank	ID	Name
1	CWE-787	Out-of-bounds Write
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
4	CWE-416	Use After Free
5	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
6	CWE-20	Improper Input Validation
7	CWE-125	Out-of-bounds Read
8	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
9	CWE-352	Cross-Site Request Forgery (CSRF)
10	CWE-434	Unrestricted Upload of File with Dangerous Type

source

MITRE CWE Top 25

1. Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
   CWE-79 | CVEs in KEV: 3 | Rank Last Year: 2 (up 1) ▲
2. Out-of-bounds Write
   CWE-787 | CVEs in KEV: 18 | Rank Last Year: 1 (down 1) ▼
3. Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
   CWE-89 | CVEs in KEV: 4 | Rank Last Year: 3
4. Cross-Site Request Forgery (CSRF)
   CWE-352 | CVEs in KEV: 0 | Rank Last Year: 9 (up 5) ▲
5. Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
   CWE-22 | CVEs in KEV: 4 | Rank Last Year: 8 (up 3) ▲
6. Out-of-bounds Read
   CWE-125 | CVEs in KEV: 3 | Rank Last Year: 7 (up 1) ▲
7. Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
   CWE-78 | CVEs in KEV: 5 | Rank Last Year: 5 (down 2) ▼
8. Use After Free
   CWE-416 | CVEs in KEV: 5 | Rank Last Year: 4 (down 4) ▼
9. Missing Authorization
   CWE-862 | CVEs in KEV: 0 | Rank Last Year: 11 (up 2) ▲
10. Unrestricted Upload of File with Dangerous Type
    CWE-434 | CVEs in KEV: 0 | Rank Last Year: 10

source

https://owasp.org/Top10/

kinda arbitrary :)

Lab 01

Pick a CWE from cwe.mitre.org

Find a code example of that CWE
Find a vulnerability of that CWE

} Find any LLM (chatgpt, gemini, claude, etc) that does not detect it!

`https://www.cvedetails.com/vulnerability-list/cwe-55/vulnerabilities.html`

Submit your report here: https://forms.gle/12vLetVmszDf5qwNA

📅 Use the report template from `labs` channel on discord 📅