
OMU
HACKERS

Announcements

- Apologies for last week
- Red vs Blue - thanks!
- Lanyards


PUB
QUIZ
Monday, 4 December 2023
Doors 7:30pm | Upstairs at Firebug Bar
FREE ENTRY!
Teams of up to 6
Free club night afterwards
Dedicated bar
Prizes to be won!
OMU HACKERS
FIREBUGBAR.CO.UK
TWITTER.COM/FIREBUGBAR
FIRE BUG
1 MILLSTONE LANE - LEICESTER - LE1 5JN
EST 2012

OMU HACKERS


YOU ARE INVITED TO THE
DMU HACKERS XMAS MEAL
THURSDAY DECEMBER 14 7:00 PM 2023
2 Courses £20.50 | 3 Courses £23.50
Join us for a nice meal after the last session of the term! +1s are encouraged, so bring a flatmate, friend or partner along if you wish!
DMU HACKERS
THE SOAR POINT


hackers.dmu
@dmuhackers
DMU
HACKERS
The OWASP Top 10

Don't do illegal shit

OWASP
Open Web Application Security Project

What is OWASP?

- Open Web-App Security Project
- Non-Profit focused on being a free resource for identifying, understanding and mitigating web vulnerabilities

OWASP
Open Web Application Security Project

What is OWASP?

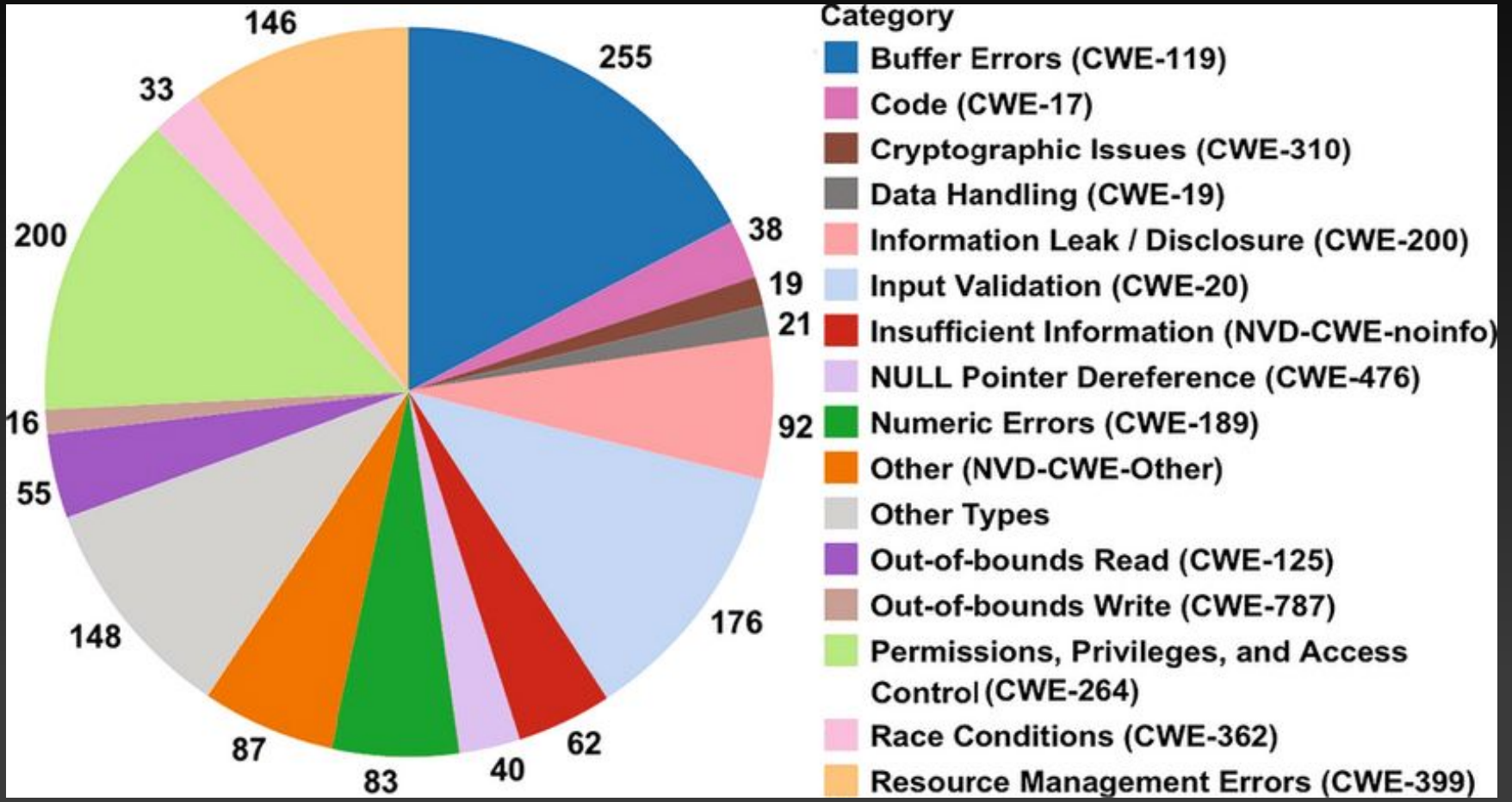
- Worldwide community of professionals from security and development backgrounds
- Vendor-neutral - try to give advice as widely as possible
- Most famous for their 'Top 10'

OWASP Top 10

- Represents the most critical security risks to web applications
- Industry Standard
- Regularly updated
- Was identified using CWEs

Root of an issue, as opposed to CVEs which are specific issues with a piece of software

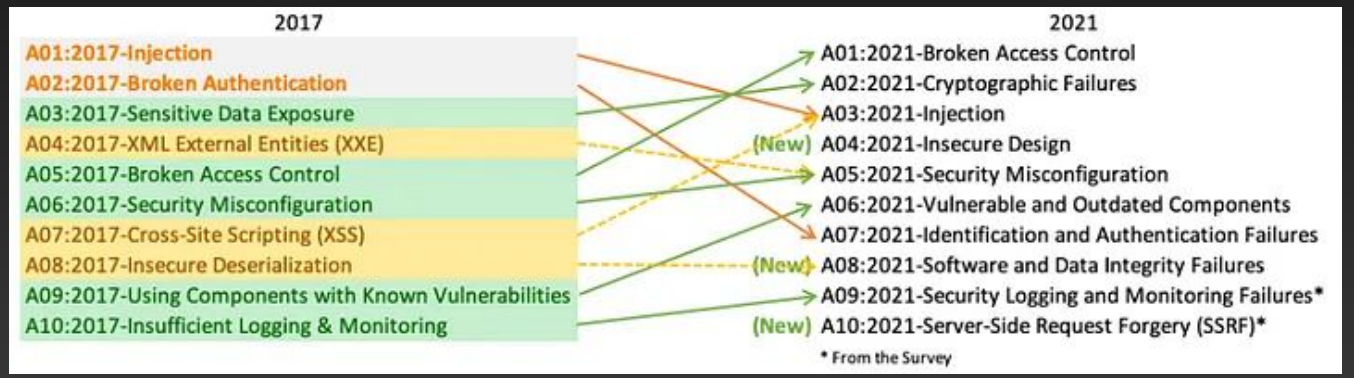
Common Weakness Enumeration (CWE)



OWASP top 10

- Been published since 2004!
- Updates every 3-4 years to fit current trends

OWASP Top 10 2004 (old)	OWASP Top 10 2007 (New)
A4. Cross Site Scripting (XSS)	A1. Cross Site Scripting (XSS)
A6. Injection Flaws	A2. Injection Flaws
	A3. Malicious File Execution (NEW)
A2. Broken Access Control (split in 2007 T10)	A4. Insecure Direct Object Reference
	A5. Cross Site Request Forgery (CSRF) (NEW)
A7. Improper Error Handling	A6. Information Leakage and Improper Error Handling
A3. Broken Authentication and Session Management	A7. Broken Authentication and Session Management
A8. Insecure Storage	A8. Insecure Cryptographic Storage
Discussed under A10. Insecure Configuration Management	A9. Insecure Communications (NEW)
A2. Broken Access Control (split in 2007 T10)	A10. Failure to Restrict URL Access
A1. Unvalidated Input	<removed in 2007>
A5. Buffer Overflows	<removed in 2007>
A9. Denial of Service	<removed in 2007>
A10. Insecure Configuration Management	<removed in 2007>



OWASP Top 10 (2021)

A1:2021 Broken Access Control

- Any kind of bypassing authorisation measures

IDOR (Insecure Direct Object References)
`?user=fred` to `?user=admin`

Using a misconfigured API
(e.g no password)

Accessing unauthorised functions
(e.g finding the admin panel)

Token theft + manipulation
(e.g stealing session cookies)

OMU HACKERS

A2:2021 Cryptographic Failures

- Any problem as a result of weak/lack of cryptography!

Data transmitted in cleartext (HTTP, SMTP, FTP)

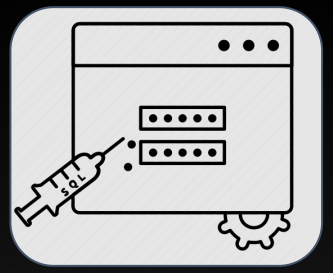
Bad key management (key reuse, using them too long, storing insecurely)

Hardcoding encryption keys

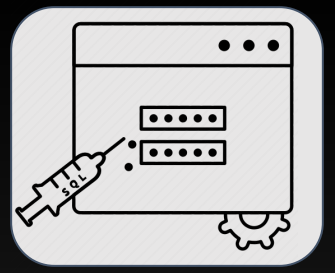
Weak/Deprecated ciphers in use (e.g MD5, SHA1)

Storing passwords in plaintext!!!!

OMU HACKERS



A3:2021 Injection



- A result of unsanitised input in forms
- Can return juicy data for the attacker!

SQL Injection
`' or 1=1;`

Cross-Site Scripting (XSS)
`<script>alert('XSS')</script>`

LDAP Injection
`*)(cn=*))(|(cn=*`

Command Injection
`?command='ls -la'`

OMU HACKERS

A4:2021 Insecure Design

- Talks about security flaws at the design stage
- All about encouraging secure design

Threat Modelling

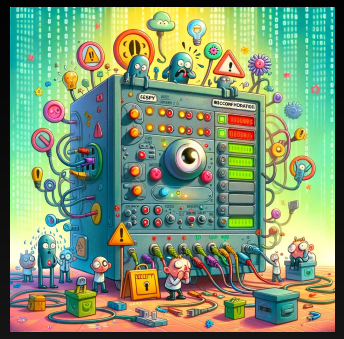
Secure By Default

This whole one is a bit wishy washy but try to appreciate what it's getting at?!?!

Risk Analysis

Design for Failure

OMU HACKERS



A5:2021 Security Misconfiguration

- Talking about general misconfigurations
- Not vulnerabilities in design as such, more 'stuff that should be done that hasn't been'

Default account usernames/passwords

Software out of date/vulnerable to known exploits

Mostly prevented by adhering to 'least privilege'

Unnecessary features are enabled (ie open ports)

For upgraded systems: not enabling latest security features

OMU HACKERS

A6:2021 Vulnerable and Outdated Components

- Involves risks of using vulnerable & outdated components
- Secure management & updating 3rd party modules

Outdated Software

Unpatched Vulnerabilities

Deprecated Frameworks

Insecure Third-Party Plugins

Legacy Code

OMU HACKERS

A7:2021 Identification and Authentication Failures

- Any kind of failure to authenticate a user

Brute Force attacks (stopped by limiting login attempts over x time)

Weak/Well known passwords (anything in `rockyou.txt`)

Not validating SSO tokens

Credential Stuffing

Weak password recovery processes

OMU HACKERS

A8:2021 Software and Data Integrity Failures

- Where data isn't validated correctly
- Risks from failing to keep the integrity of software and data

Insecure Software Updates

Data Intercepted By Lack Of Encryption

Running Unsigned Code

Using Unverified External Dependencies

Lack of Data Input Validation

OMU HACKERS

A9:2021 Security Logging and Monitoring Failures

- Either events not logged properly or events that are logged are insecurely stored
- Not much CVE/CVSS data - it's a complex problem not attributable to a specific event often

Auditable events (valid/invalid logins, high value transactions) not logged

Logs only stored locally and not replicated elsewhere

Incident Response processes not in place/inadequate

Warnings/Errors either logged unclearly or not at all

Scans (e.g NMAP) don't trigger alerts

OMU HACKERS

A10:2021 Server-Side Request Forgery (SSRF)

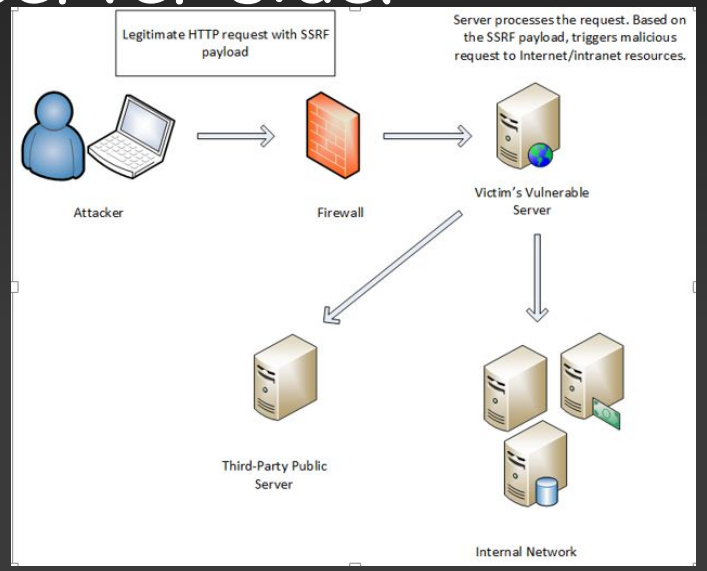
- Happens when the server doesn't validate the data given to it
- Exploitable through tools like BurpSuite, Caido, OWASP Zap
- Prevented by validating bits server side!

Ability to access files if network not properly segmented

Bypassing Firewall Protections

Prevented by whitelisting URLs that can access resources

Internal Network Scanning



Session-Related Task:

OWASP Top 10 - 2021

https://tryhackme.com/room/owasptop102021