# The OWASP Top 10

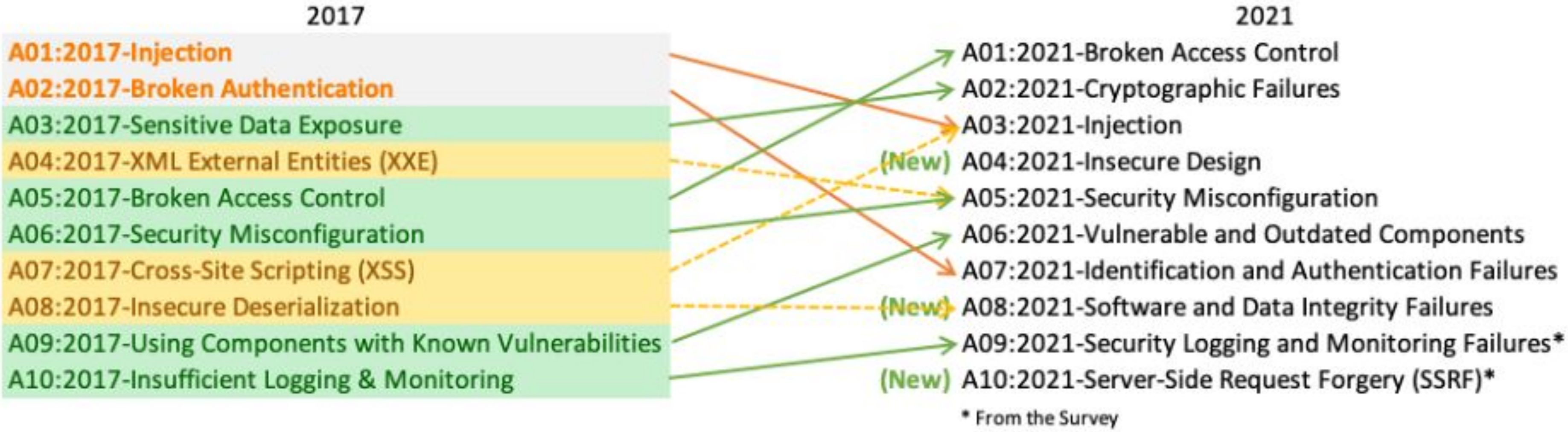
OSIRIS Lab
2/8/2023

# The OWASP Foundation

- The **O**pen **W**eb **A**pplication **S**ecurity **P**roject
  - Nonprofit foundation, international community
  - 250+ local chapters, 4500+ sponsors
- Guides and tools
  - Top Ten
  - Web Security Testing Guide (WSTG)
  - Mobile Application Security (MAS)
  - Zed Attack Proxy (ZAP)

# OWASP Top Ten

- Highlights the ten most critical security vulnerabilities with web applications



2017

A01:2017-Injection

A02:2017-Broken Authentication

A03:2017-Sensitive Data Exposure

A04:2017-XML External Entities (XXE)

A05:2017-Broken Access Control

A06:2017-Security Misconfiguration

A07:2017-Cross-Site Scripting (XSS)

A08:2017-Insecure Deserialization

A09:2017-Using Components with Known Vulnerabilities

A10:2017-Insufficient Logging & Monitoring

2021

A01:2021-Broken Access Control

A02:2021-Cryptographic Failures

A03:2021-Injection

(New) A04:2021-Insecure Design

A05:2021-Security Misconfiguration

A06:2021-Vulnerable and Outdated Components

A07:2021-Identification and Authentication Failures

(New) A08:2021-Software and Data Integrity Failures

A09:2021-Security Logging and Monitoring Failures*

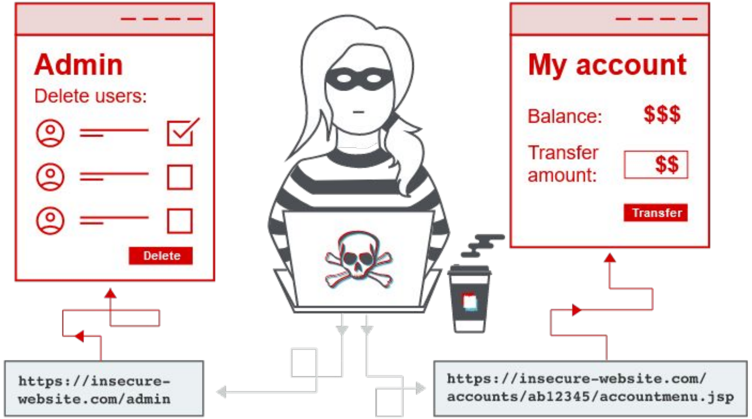
(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

# A01 Broken Access Control

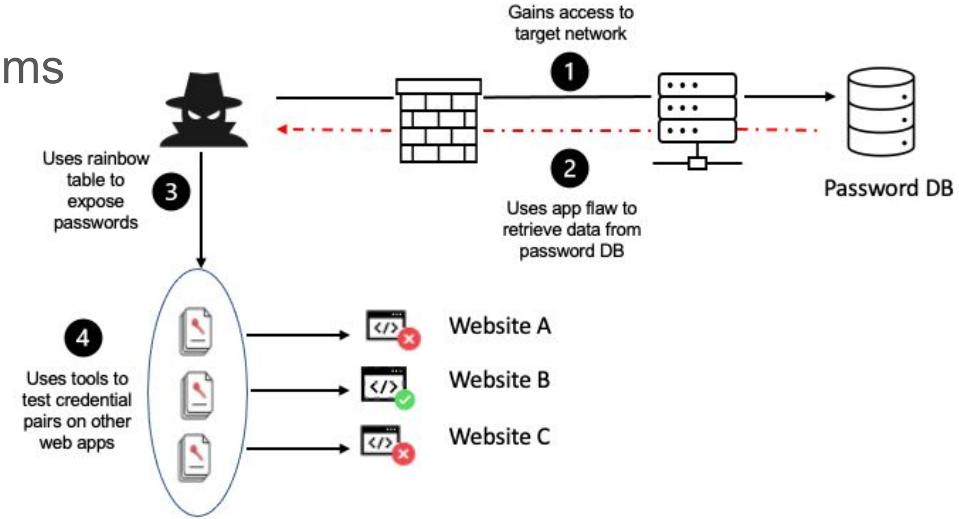
- Users have unintended permissions
  - Information disclosure
  - Unauthorized actions
  - Privilege escalation

- Insecure Direct Object Reference (IDOR)
  - /profile/1
  - /profile/2
- Cross Site Request Forgery (CSRF)
  - iframes,


Admin
Delete users:
Delete
My account
Balance: $$$
Transfer amount: $$
Transfer
https://insecure-website.com/admin
https://insecure-website.com/accounts/ab12345/accountmenu.jsp

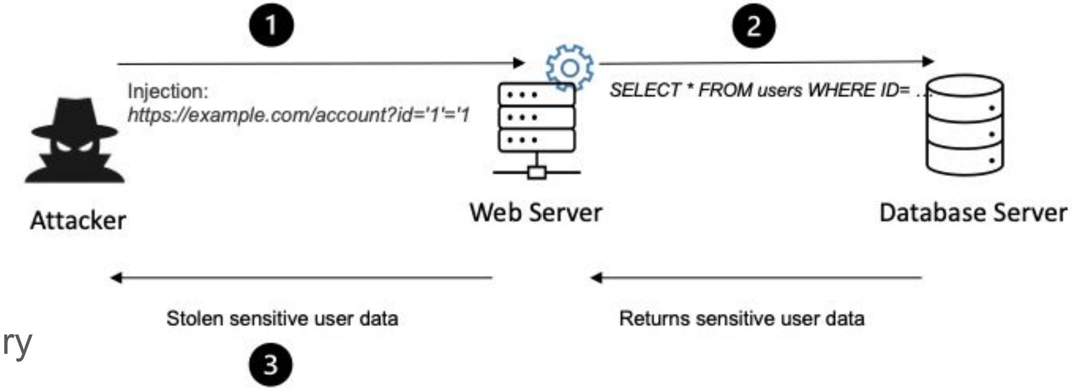
# A02 Cryptographic Failures

- Weak password restrictions
  - “password123”, “qwerty”
- Storing plaintext passwords
  - Hash them!
- Using poor cryptographic algorithms
  - MD5, SHA-1, ECB
- “Don’t roll your own crypto”


Gains access to target network
1
2
Uses app flaw to retrieve data from password DB
Password DB
Uses rainbow table to expose passwords
3
4
Uses tools to test credential pairs on other web apps
Website A
Website B
Website C

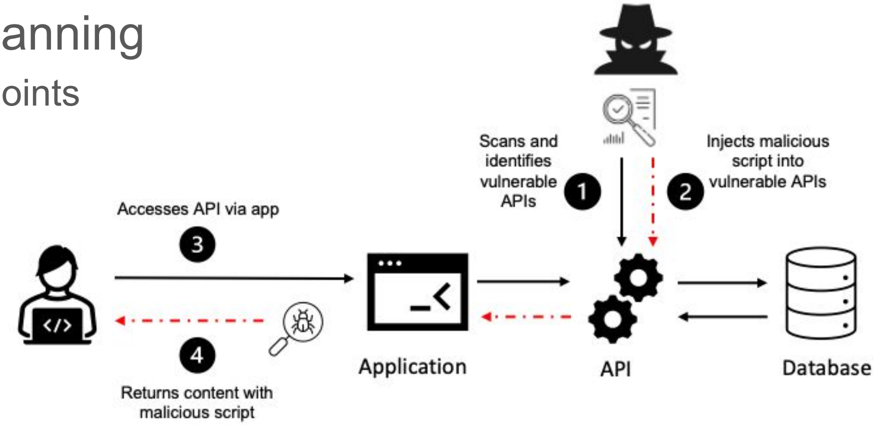
# A03 Injection

- Poor validation, filtering, or sanitization of user input
- Do not trust user input
- Many types of injections
  - SQL
  - Server-side templates
  - Command injection
  - Object Graph Navigation Library
    - Equifax


1
Injection:
https://example.com/account?id='1'='1
2
SELECT * FROM users WHERE ID= ...
Attacker
Web Server
Database Server
Stolen sensitive user data
Returns sensitive user data
3

# A04 Insecure Design

- Different from security misconfiguration
- Design and architectural flaws
  - Missing protection requirements or security controls
    - Confidentiality, integrity, availability (CIA)
- Occurs due to lack of resources for planning
  - Mobile apps, client-side JS, exposed endpoints


Scans and identifies vulnerable APIs
1
2
Injects malicious script into vulnerable APIs
Accesses API via app
3
</>
4
Returns content with malicious script
Application
API
Database

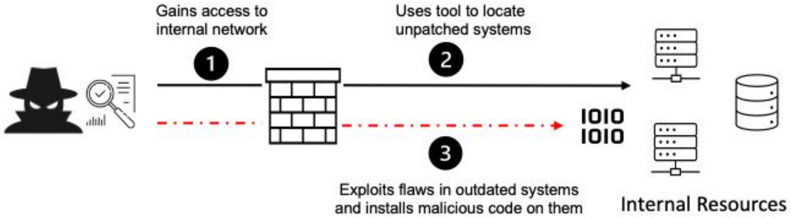
# A05 Security Misconfiguration

Anything that may have been misconfigured or missing configuration

- S3 buckets with public permission
- Default credentials
  - Common with devices: cameras, TVs, routers
- Mistakes with certain frameworks
  - WordPress
    - WPScan
  - Nginx
    - Alias directive

# A06 Vulnerable and Outdated Components

- Release of common vulnerabilities and exposures (CVEs)
  - exploitdb
- Researchers/vendors may disclose findings
  - Zero-days


Gains access to internal network
1
Uses tool to locate unpatched systems
2
1010
1010
3
Exploits flaws in outdated systems and installs malicious code on them
Internal Resources

Prevention

- Frequently update, remove unused dependencies
- Know used libraries, components, technologies
  - npm packages

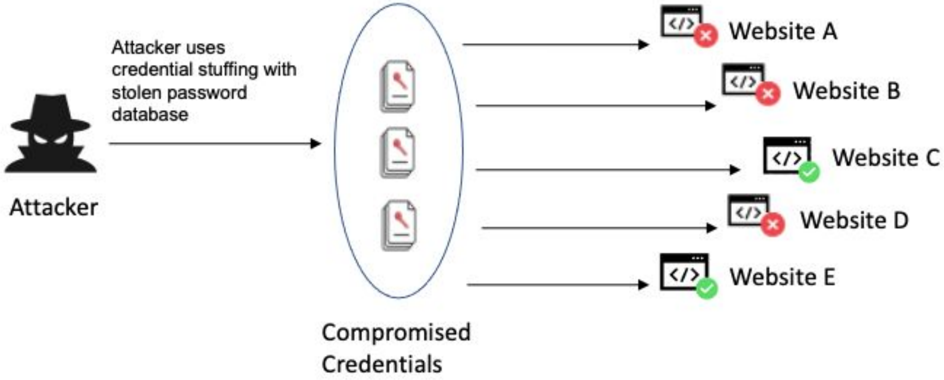
# A07 Identification and Authentication Failures

Related to A01 Broken Access Control

- Authn vs authz
  - Authentication vs authorization

Attacks:

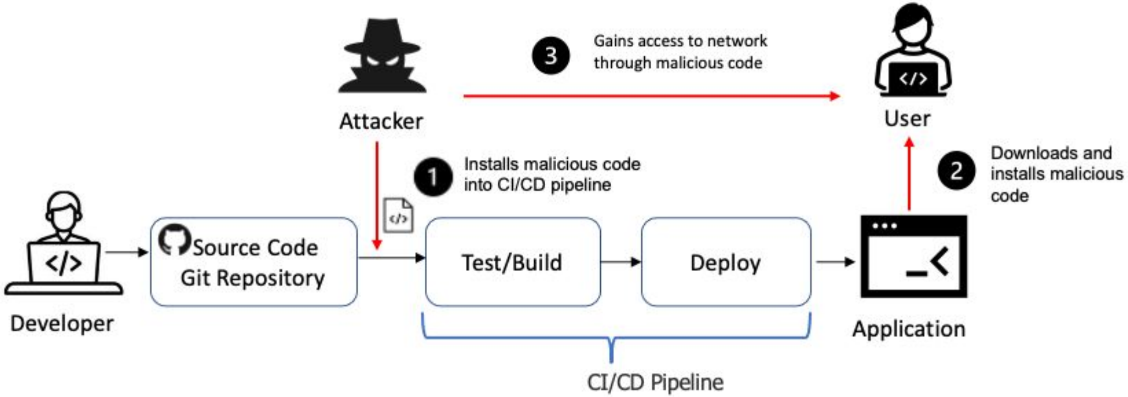
- Brute forcing
- Password spraying
- Session hijacking
- CSRF



# A08 Software and Data Integrity Failures

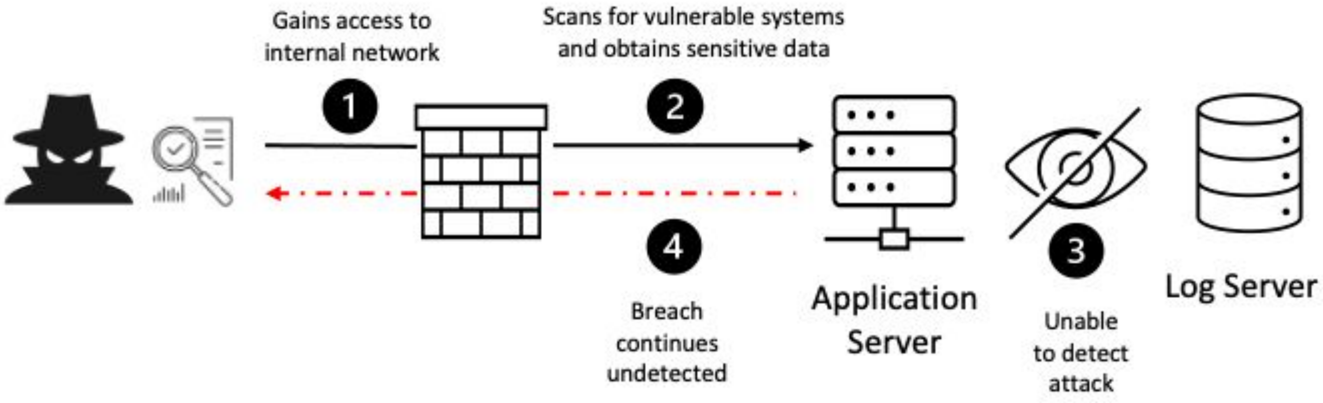
Similar to A06 Vulnerable and Outdated Components

- Unchecked CI/CD pipeline
- Checking correct files are downloaded with integrity checks
  - Hashing
- Using trustworthy libraries/dependencies


Attacker
3
Gains access to network through malicious code
User
1
Installs malicious code into CI/CD pipeline
2
Downloads and installs malicious code
Developer
Source Code Git Repository
Test/Build
Deploy
Application
CI/CD Pipeline

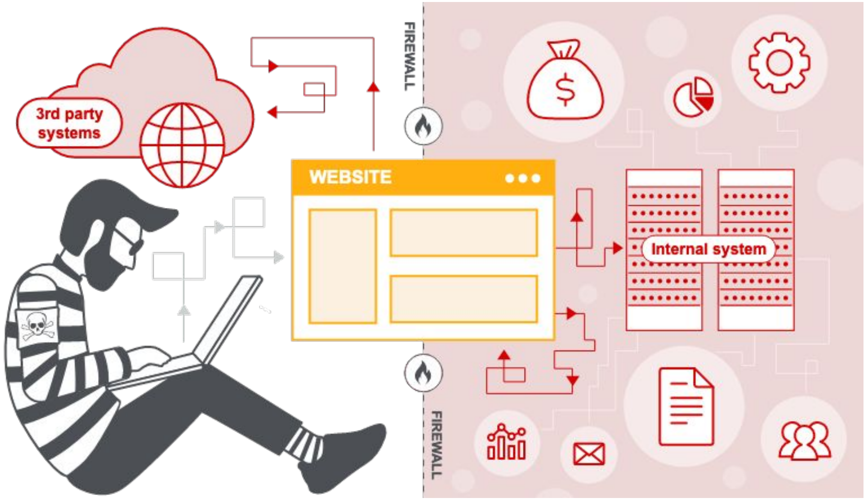
# A09 Security Logging and Monitoring Failures

- Required for security teams and to catch threats
- Typically a high number of false positives
  - Better than false negatives
- Logs can help trace an attacker’s path or attempts


Gains access to internal network
1
Scans for vulnerable systems and obtains sensitive data
2
4
Breach continues undetected
Application Server
3
Unable to detect attack
Log Server

# A10 Server-Side Request Forgery (SSRF)

- When an attacker can have the server make requests
  - Can hit internal local IPs
- Instance metadata
  - 169.254.169.254
  - Leak AWS credentials
    - CapitalOne



# Conclusion

- Only the top 10 vulnerabilities
- OWASP Juice Shop
  - Play around with http://hacknight.osiris.bar:3000/
  - Tutorial mode
    - If things break tell Rachel
- Low-hanging fruit
  - /robots.txt
  - admin’ or 1 -- ;
  - <script>alert(1)</script>