OCTOBER 19, 2021

OWASP TOP 10

Web Exploitation

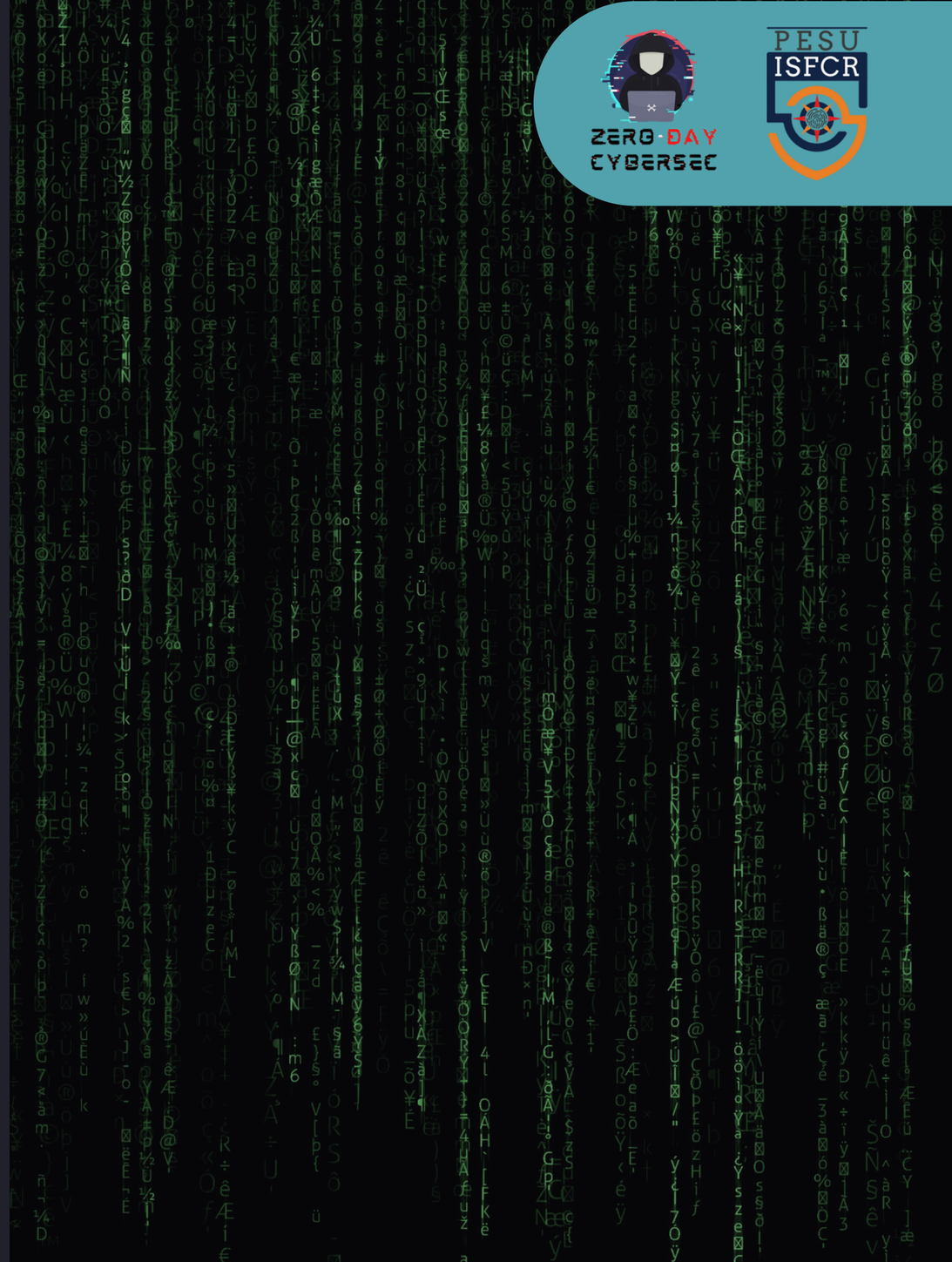
Workshop Overview

Points of Discussion

About OWASP

Top 10 Vulnerabilities

Demo



Introduction

What is OWASP?

The Open Web Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software.

Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web.

What is OWASP Top 10?

and why is it important?

The OWASP Top 10 is a standard awareness document for developers and web application security.

It represents a broad consensus about the most critical security risks to web applications.

Using the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture into one that produces more secure code.

Top 10
Vulnerabilities

1. BROKEN ACCESS CONTROL
2. CRYPTOGRAPHIC FAILURES
3. INJECTION
4. INSECURE DESIGN
5. SECURITY MISCONFIGURATION
6. OUTDATED COMPONENTS
7. AUTHENTICATION FAILURES
8. DATA INTEGRITY FAILURES
9. MONITORING FAILURES
10. SERVER-SIDE REQUEST FORGERY

Broken Access Control

94% of applications were tested for some form of broken access control.

Attack

PARAMETER TAMPERING
CORS MISCONFIGURATION
ELEVATION OF PRIVILEGE
API MISUSE
METADATA MANIPULATION

Prevention

DENY BY DEFAULT
MINIMIZING CORS
RECORD OWNERSHIP
RATE LIMIT API
STATELESS JWT

HTTPS://EXAMPLE.COM/APP/ACCOUNTINFO?ACCT=NOTMYACCT

Cryptographic Failures

PROTECTION NEEDS OF DATA IN TRANSIT AND AT REST

Protocol Security - HTTP vs HTTPS
Encryption Standards - MD5 vs SHA256
Weak Keys - JWT
Seeded Keys

Injection

Attackers try to exploit inputs to manipulate DB queries

Unsanitized Inputs

Use LIMITS to reduce information sent

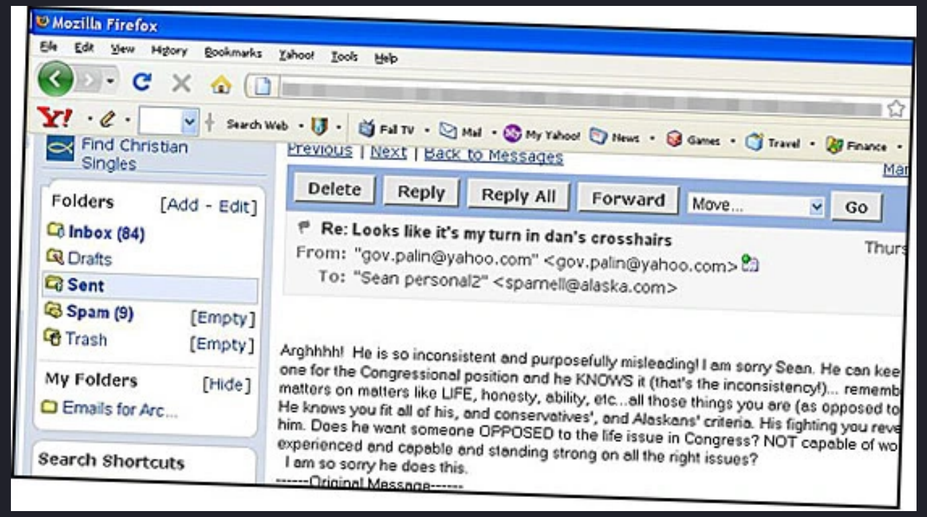
String query = "SELECT * FROM accounts WHERE custID='" + request.getParameter("id") + "'";

http://example.com/app/accountView?id=19

http://example.com/app/accountView?id=' or '1'='1

Insecure Design

INSECURE DESIGN VS IMPLEMENTATION



Questions and Answers - Credential recovery

A e-commerce website has no protection against bots buying products to resell at auction sites.

DevSecOps

Security Frameworks - NIST, ISO

Security Misconfiguration

Wrongly configured softwares

DEFAULT CREDENTIALS
UNNECESSARY FEATURES
ERROR HANDLING

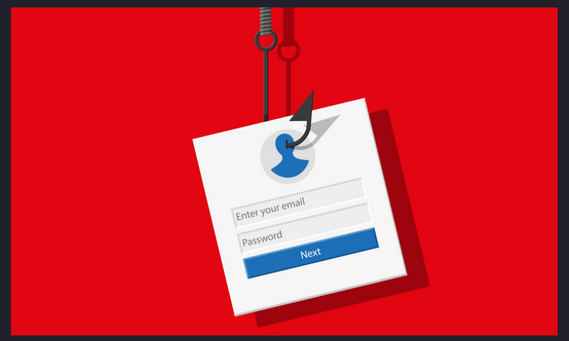
SEGMENTED ARCHITECTURE
MINIMAL PLATFORM
QA AND TESTING

Vulnerable and Outdated Components

SHADOW BROKERS

UNKNOWN VERSIONS
UNSUPPORTED/ OUTDATED
VULNERABILITY SCANNING
COMPATIBILITY

UPDATING / PATCHING
INVENTORY THE VERSIONS
OFFICIAL RELEASES
REMOVE UNUSED SOFTWARES

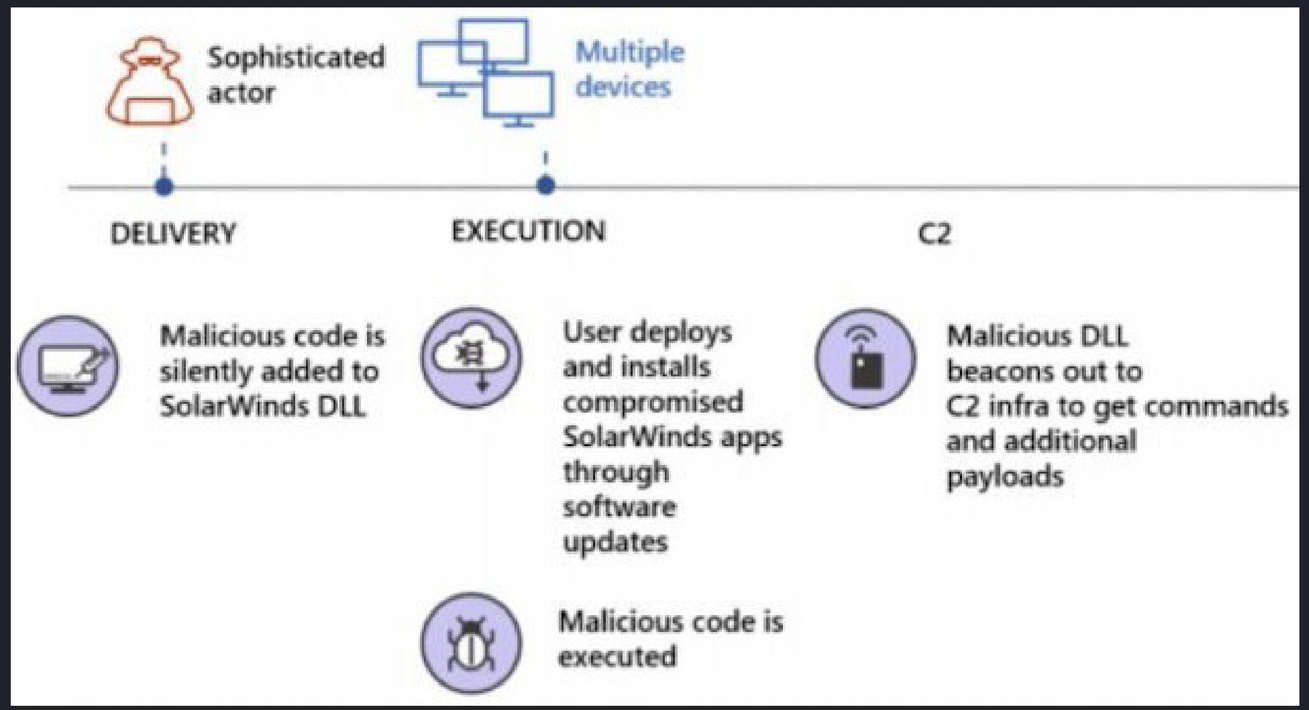


Identification and Authentication Failures

BRUTE FORCE ATTACKS
PERMITTING WEAK PASSWORDS
INSECURE SESSION IDENTIFIERS
NO MFA

MULTI FACTOR AUTHENTICATION
DELAY FAILED LOGIN ATTEMPTS
SESSION ID SECURITY

Software and Data Integrity Failures



UNTRUSTED UDPATES
UNUSED PLUGINS

DEPENDENCY CHECKS
DIGITAL SIGNATURES

Security Logging and Monitoring Failures

ERROR LOGGING
LOGGIGG LOGIN
ATTEMPTS

LOG AND STORE SECURELY

Server-Side Request Forgery

SSRF FLAWS OCCUR WHENEVER A WEB APPLICATION IS FETCHING A REMOTE RESOURCE WITHOUT VALIDATING THE USER-SUPPLIED URL.

DENY BY DEFAULT
SANITIZE INPUT
NO RAW RESPONSES

Demo and Q&A

Any doubts / queries ?

https://application.security/free/owasp-top-10

THANK YOU!

VISIT US SOON.