Opportunities on OWASP Top 10

Kwaku Sarpong Manu

OWASP

The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

- Computer Engineer
- System Analyst
- Application and Communications Security Researcher
- I might know how to hack. Emphasis on *might*

OWASP
The Open Web Application Security Project

- Outline
  - Background to OWASP Top 10
  - Trends and Observations
  - Analysis
  - Recommendations

Background

OWASP
The Open Web Application Security Project

- The OWASP Top 10 has become the standard security awareness document for developers
- It represents a broad consensus about the most critical security risks to web applications.
- Original Top 10 released in 2003 and then roughly every 3 years since.
- The product is focused on observed security vulnerabilities in applications based off testing and survey by App-Sec-Dev community members

Top 10: Trends

OWASP
The Open Web Application Security Project

2013	2017
Injection	Injection
Broken Authentication & Session Mgmt	Broken Authentication
Cross-Site Scripting (XSS)	Sensitive Data Exposure

Top 10: Trends

OWASP
The Open Web Application Security Project

2021
Broken Access Control
Cryptographic Failures
Injection
Insecure Design
Security Misconfigurations

Top 10: Core Trends

OWASP
The Open Web Application Security Project

- Data is the new oil (not gold). IMO !
- Data is the most valuable and vulnerable resource
- Cyber incidents have a concentric target. All the hackers want your data and escalated privileges
- Most exploits are escalating to unauthorised access, confidentiality breaches and privacy attacks

Opportunities: Who f'ed up?

OWASP
The Open Web Application Security Project

- The developers. As usual
- Re/use of vulnerable components
- Weak package inspection
- Flawed design logic on custom modules (esp. authentication and access control)

Opportunities: What Do We Do?

OWASP
The Open Web Application Security Project

- Code Audit and Inspection
- Encourage use of SDLCs that enable flexible & frequent testing
- Utilise enhanced data security controls (e.g. Access & authorisation controls)
- Ensuring strict or best-possible compliance with cyberspace standards

Endnote

OWASP
The Open Web Application Security Project

- Architecture and Resource allocation have improved esp. with flexible cloud services.
- Availability Attacks are less attractive for the typical threat actor
- Data has infinite upward value
- Confidentiality Attacks are gaining notoriety
- Attackers have many advantages

Endnote

OWASP
The Open Web Application Security Project

- Don’t drop the soap! Defenders must keep defending.
- Privacy and data protections are the crux of future security developments, problems and solutions
- Application security is everyone’s job. Devs screw up but so do users
- We may not win, but we lose if we stop fighting

OWASP
The Open Web Application Security Project

THANK YOU

This production does not represent the opinions of any specific organisation, regardless of any known affiliations of the author.