OWASP Review

Amherst Security Group

June 14, 2017

Robert Hurlbut

RobertHurlbut.com • @RobertHurlbut

Robert Hurlbut

Software Security Consultant, Architect, and Trainer

- Owner / President of Robert Hurlbut Consulting Services
- Microsoft MVP – Developer Security 2005-2009, 2015, 2016
- (ISC)2 CSSLP 2014-2017
- Co-host with Chris Romeo – Application Security Podcast

Contacts

Web Site: https://roberthurlbut.com

Twitter: @RobertHurlbut, @AppSecPodcast

ROBERT HURLBUT CONSULTING SERVICES

securedevelop.NET

Agenda

OWASP – what is it?

OWASP – Lots of projects!

OWASP Top 10

OWASP ASVS v3.0

OWASP Top 10 Proactive Controls v2

OWASP Summit 2017

OWASP

Open Web Application Security Project (OWASP) is not-for-profit organization focused on improving the security of software and helping people and organizations make informed decisions about true application security risks

Everyone welcome to participate in OWASP

All materials available under free and open software licenses

Search

Home
About OWASP
Acknowledgements
Advertising

Welcome to OWASP

the free and open software security community

- Dependency Check
- Proactive Controls
- ZAP Proxy
- Cheat Sheets
- Top 10
- OWTF
- ASVS
- SAMM
- Development Guide
- AppSensor
- Testing Guide
- ModSecurity Ruleset
- **More...**

OWASP – Lots of projects!

Dependency Check

Top 10

Proactive Controls

ZAP (Zed Attack Proxy)

Cheat Sheets

OWTF (Offensive Web Testing Framework)

ASVS (Application Security Verification Standard)

SAMM (Software Assurance Maturity Model)

OWASP Top 10 (2013)

Updated every 3-4 years

A1 - Injection
A2 - Broken Authentication and Session Management
A3 - Cross Site Scripting (XSS)
A4 - Insecure Direct Object References
A5 - Security Misconfiguration
A6 - Sensitive Data Exposure
A7 - Missing Function Level Access Control
A8 - Cross-Site Request Forgery
A9 - Using Components with Known Vulnerabilities
A10 - Unvalidated Redirects and Forwards

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

OWASP Top 10 2017 – under review

A1-Injection
A2-Broken Authentication and Session Management
A3-Cross-Site Scripting (XSS)
A4-Broken Access Control
A5-Security Misconfiguration
A6-Sensitive Data Exposure
A7-Insufficient Attack Protection (new)
A8-Cross-Site Request Forgery (CSRF)
A9-Using Components with Known Vulnerabilities
A10-Underprotected APIs (new)

https://www.owasp.org/index.php/Top_10_2017-Top_10

OWASP ASVS v3.0 (2015)

OWASP Application Security Verification Standard (ASVS) provides basis for testing web application technical security controls and provides developers list of requirements for secure development

Use as:

- Metric
- Guidance
- During procurement

https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

OWASP ASVS v3.0 (2015)

V1: Architecture, design and threat modelling
V2: Authentication Verification Requirements
V3: Session Management Verification Requirements
V4: Access Control Verification Requirements
V5: Malicious input handling verification requirements
V7: Cryptography at rest verification requirements
V8: Error handling and logging verification requirements
V9: Data protection verification requirements

https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

OWASP ASVS v3.0 (2015)

V10: Communications security verification requirements

V11: HTTP security configuration verification requirements

V13: Malicious controls verification requirements

V15: Business logic verification requirements

V16: Files and resources verification requirements

V17: Mobile verification requirements

V18: Web services verification requirements

V19. Configuration

https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

OWASP Top 10 Proactive Controls v2 (2016)

Help for fixing Top 10 "Attacks"

- C1 - Verify for Security Early and Often
- C2 - Parameterize Queries
- C3 - Encode Data
- C4 - Validate All Inputs
- C5 - Implement Identity and Authentication Controls
- C6 - Implement Appropriate Access Controls
- C7 - Protect Data
- C8 - Implement Logging and Intrusion Detection
- C9 - Leverage Security Frameworks and Libraries
- C10 - Error and Exception Handling

https://www.owasp.org/index.php/OWASP_Proactive_Controls

OWASP Summit 2017

This week – June 12-16, Woburn Forest Center Parcs, Bedfordshire, UK

150+ organizers and participants meeting for the week to discuss about many OWASP projects

https://owaspsummit.org

Resources - Tools

OWASP Application Security Verification Standard (ASVS)

https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

OWASP Proactive Controls 2016

https://www.owasp.org/index.php/OWASP_Proactive_Controls

Questions?

Contacts

Web Site: https://roberthurlbut.com

Twitter: @RobertHurlbut, @AppSecPodcast

Email: robert at roberthurlbut.com

ROBERT HURLBUT CONSULTING SERVICES

securedevelop.NET