



KEAMANAN APLIKASI WEB

endy.muhardin@gmail.com



TENTANG SAYA

.....

- Endy Muhardin
- <http://software.endy.muhardin.com>
- endy.muhardin@gmail.com
- github.com/endymuhardin
- +62 812 98000 468
- @endymuhardin
- [fb.com/endy.muhardin](https://www.facebook.com/endy.muhardin)

AGENDA TRAINING

- Konsep Web Security
 - Asset
 - Threat
 - Vulnerability
 - Attack
 - Countermeasure
- Vulnerability
 - Input Validation
 - Authentication
 - Authorization
 - Session Management
 - Parameter Manipulation
 - Exception Management
 - Auditing and Logging

AGENDA TRAINING

- Attack
 - Cross Site Scripting
 - Cross Site Request Forgery
 - SQL Injection
 - Path Traversal
 - HTTP Response Splitting
- Countermeasures
 - Understand Issues
 - Validate Input
 - Prevent Automation
 - Slow down
 - Throttling
 - Lockout

AGENDA TRAINING

- Security-aware Software Development Life Cycle
 - Threat Model
 - Test Plan Preparation
 - Test Execution
 - Test Automation
 - Continuous Delivery

REFERENSI

- OWASP Web Top Ten Security Risk
 - https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
 - https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet
- OWASP Mobile Top Ten Risk
 - https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#Top_Ten_Mobile_Risks
- OWASP AppSecUSA 2015
 - https://www.youtube.com/playlist?list=PLpr-xdpM8wG93dG_L9QKs0W1cD-esQEzU
- Other
 - https://danielmiessler.com/projects/webappsec_testing_resources/

REFERENSI

- OWASP Developer Guide
 - <https://github.com/OWASP/DevGuide>
- OWASP Testing Guide
 - https://www.owasp.org/images/5/52/OWASP_Testing_Guide_v4.pdf
- OWASP Code Review Guide
 - https://www.owasp.org/images/2/2e/OWASP_Code_Review_Guide-V1_1.pdf
- OWASP Application Security Verification Standard Project
 - <https://www.owasp.org/images/6/67/OWASPAplicationSecurityVerificationStandard3.0.pdf>
- OWASP Cheat Sheet
 - https://www.owasp.org/images/9/9a/OWASP_Cheatsheets_Book.pdf

APLIKASI UNTUK MENGETES

- Zap Proxy
 - <https://github.com/zaproxy/zaproxy>
- OWASP Offensive Web Testing Framework
 - https://www.owasp.org/index.php/OWASP_OWTF
- Browser Exploitation Framework (BeEF)
 - <http://beefproject.com/>

APLIKASI YANG DITES (INSTALL SENDIRI)

- OWASP Web Goat
 - <https://github.com/WebGoat>
- Damn Vulnerable Web Application
 - <http://www.dvwa.co.uk/>
- BodgeIt
 - <https://github.com/psiinon/bodgeit>
- Securibench
 - <http://suif.stanford.edu/~livshits/securibench/>
- Google Gruyere
 - <http://google-gruyere.appspot.com/part1>

APLIKASI UNTUK DITES (SERVICE)

- Zero Bank
 - <http://zero.webappsecurity.com/>
- Hack Me
 - <https://hack.me/>
- Hack This Site
 - <https://www.hackthissite.org/>

AUTOMATION TOOLS

- ZAP Web Driver
 - <https://github.com/continuumsecurity/zap-webdriver>
- BDD Security
 - <http://www.continuumsecurity.net/bdd-intro.html>
- GDS PMD Security Rule
 - <https://github.com/GDSSecurity/GDS-PMD-Security-Rules>



OWASP TOP 10

- Injection
- Authentication & Session
- XSS
- Direct Object References
- Misconfiguration
- Data Exposure
- Access Control
- CSRF
- Components
- Redirect & Forward

“

The only source of knowledge is
experience.

-Albert Einstein

HANDS ON SESSION

- Instalasi Aplikasi Test
- Menjalankan Penetration Test
 - OWASP Top 10
- Memperbaiki Aplikasi



DEVELOPMENT PROCESS

- Threat Model
- Membuat Test Plan
- Menjalankan Test
- Mengotomasi Test
- Continuous Delivery

THREAT MODEL

- Memahami OWASP Top 10
- Memahami Kelemahan Aplikasi (Vulnerability)
- Memahami Cara Kerja Serangan (Attack)
- Memahami Cara Menangkal
- Memahami Cara Pencegahan

PEMBUATAN TEST PLAN

- Daftar Threat Model yang akan dites
- Prosedur Pengetesan
 - User dan Role
 - Fitur yang akan dites
 - Langkah-langkah
- Data Sampel
- Analisa Hasil
 - Kriteria Sukses
 - Kriteria Gagal

MENJALANKAN TEST

- Jadwal Pengetesan
- Persiapan Tes
- Laporan Hasil Tes
- Tindak Lanjut Perbaikan

OTOMASI TEST

- Persiapan Environment
- Deployment Aplikasi
- Inisialisasi Test Data
- Pembuatan Script Pengetesan
- Eksekusi Script Pengetesan
- Integrasi dengan Build Tools

CONTINUOUS DELIVERY

- Continuous Integration
 - Version Control
 - Build Server
 - Deployment Target
 - Issue Tracker
 - Notifikasi
- Migration Script
- Blue / Green Deployment
- Chaos Monkey

“

Terima Kasih