OWASP Top 10 – 2013

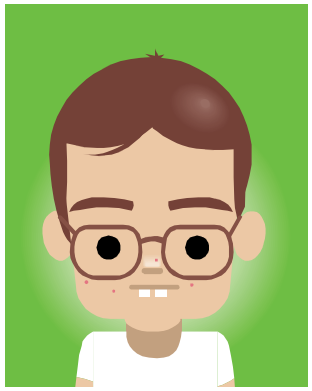
The Top 10 Most Critical Web Application Security Risks

Johnny Cho (조민재)
OWASP Korea Chapter Board Member

johnny.cho@owasp.org

The OWASP Foundation
http://www.owasp.org/

발표자 소개



- OWASP Korea 챕터 이사
- Yahoo! Korea, NHN, Penta Security, Cisco Korea 등 기업체 경력 15년
- SW개발 보안 및 인프라 보안 전문가
- OWASP Top 10 2010 번역 참여
- 2004년부터 OWASP projects 에 관심

발표내용

- Top 10 Project
- Top 10 for 2013
- Top 10 for 2013 한글 번역
- Q&A

Top 10 Project

- started in 2003
- Released on 2004, 2007, 2010
- 2013 Release Candidate is available.

Jeff Williams

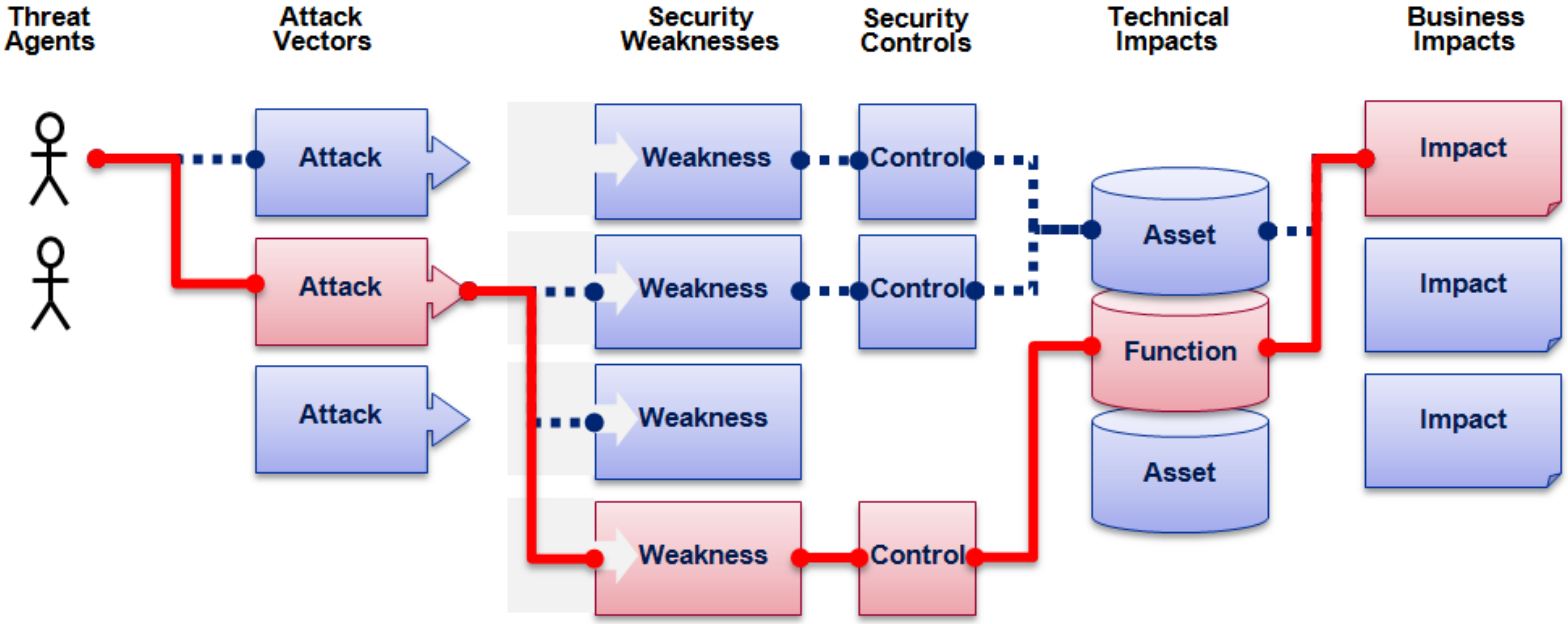
ASPECT SECURITY
Application Security Specialists

Dave Wichers

Top 10 Project

- It's About Risks, Not Just Vulnerabilities
- New title is : "The Top 10 Most Critical Web Application Security Risks"
- Based on the OWASP Risk Rating Methodology
- Used to prioritize Top 10
- Various Data Sources
  - Aspect Security, HP(Fortify&WebInspect), Minded Security, Softtek, TrustWave Spiderlab, Veracode, WhiteHat Security

OWASP Top 10 Risk Rating Methodology



Threat Agent	Attack Vector	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact
	Easy	Widespread	Easy	Severe	
?	Average	Common	Average	Moderate	?
	Difficult	Uncommon	Difficult	Minor	
	1	2	2	1	
		1.66	*	1	

Injection Example

1.66
weighted risk rating

OWASP Top10 Risk (2004 ~ 2010)

	2004	2007	2010
A1	Unvalidated Input (New, Removed in 2007)	Cross Site Scripting (A4→A1)	Injection (A2→A1)
A2	Broken Access Control (New, Removed in 2007)	Injection Flaws (A6→A2)	Cross Site Scripting (A1→A2)
A3	Broken Authentication and Session Management (New)	Malicious File Execution (New, Removed in 2010)	Broken Authentication and Session Management (A7→A3)
A4	Cross Site Scripting (New)	Insecure Direct Object Reference (New)	Insecure Direct Object Reference (A4→A4)
A5	Buffer Overflow (New, Removed in 2007)	Cross Site Request Forgery (New)	Cross Site Request Forgery (A5→A5)
A6	Injection Flaws (New)	Information Leakage and Improper Error Handling (New, Removed in 2010)	Security Misconfiguration (New)
A7	Improper Error Handling (New)	Broken Authentication and Session Management (A3→A7)	Insecure Cryptographic Storage (A8→A7)
A8	Insecure Storage (New)	Insecure Cryptographic Storage (New)	Failure to Restrict URL Access (A10→A8)
A9	Application Denial of Service (New, Removed in 2007)	Insecure Communications (New, Removed in 2010)	Insufficient Transport Layer Protection (New)
A10	Insecure Configuration Management (New, Removed in 2007)	Failure to Restrict URL Access (New)	Unvaildated Redirects and Forwards (New)

OWASP Top Ten (2013 Edition)

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

OWASP
The Open Web Application Security Project
http://www.owasp.org

Mapping from 2010 to 2013 Top 10

OWASP Top 10 – 2010 (Previous)		OWASP Top 10 – 2013 (New)
A1 – Injection	=	A1 – Injection
A3 – Broken Authentication and Session Management	↑	A2 – Broken Authentication and Session Management
A2 – Cross Site Scripting (XSS)	↓	A3 – Cross Site Scripting (XSS)
A4 – Insecure Direct Object Reference	=	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	↑	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage - Merge with A9 →	+	A6 – Sensitive Data Exposure (NEW)
A8 – Failure to Restrict URL Access – Broaden into →	+	A7 – Missing Function Level Access control (NEW)
A5 – Cross-Site Request Forgery (CSRF)	↓	A8 – Cross-Site Request Forgery (CSRF)
<Buried in A6: Security Misconfiguration>	+	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	=	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	-	Merged with 2010-A7 into new 2013-A6

What Changed From 2010 to 2013 ?

1. Broken Authentication and Session Management
   - 2010-A3 → 2013-A2
2. CSRF
   - 2010-A5 → 2013-A8
3. 

2013-A7: Missing Function Level Access Control
   · 2010-A8: Failure to Restrict URL Access
4. 

2013-A6: Sensitive Data Exposure
   - 2010-A7: Insecure Cryptographic Storage & 2010-A9:Insufficient Transport Layer Protection
   - Adding browser side sensitive data risks
5. 

2013-A9: Using Known Vulnerable Components
   - A part of 2010-A6:Security Misconfiguration
   - The growth/depth of component based development

어떻게 대처해볼 것인가?

- 시큐어 코딩
  - OWASP 가이드 문서 : 개발 가이드, 테스팅 가이드 등
    - https://www.owasp.org/index.php/OWASP_Guide_Project
  - OWASP ASVS(Application Security Verification Standard) 활용
    - https://owasp.org/index.php/ASVS
  - 각 조직에 맞는 표준 보안 컴포넌트 사용
    - OWASP ESAPI(Enterprise Security API)
    - http://www.owasp.org/index.php/ESAPI
- 어플리케이션 검토(Review)
  - 개발보안전문가에게 어플리케이션의 보안 검토를 맡겨본다.
  - OWASP의 가이드라인에 따라 직접 검토해본다.
    - OWASP 코드리뷰 가이드: http://www.owasp.org/index.php/Code_Review_Guide
    - OWASP 테스팅 가이드: http://www.owasp.org/index.php/Testing_Guide

Top 10 for 2013 한글 번역

- Top 10 한글 번역
  - 2004 : 배상우(Jeremy Bae)
  - 2007 : SECURITY PLUS
- Top 10 for 2013 한글 번역
  - OWASP Korea 챕터 공식 프로젝트
    - 프로젝트 진행/감수 : 조민재
    - 번역자(12명) : 송창기, 전영재, 송보영, 김태일, 김병효, 정홍순, 김효근, 박정훈, 유정호, 정가람, 성영모, 허성무
  - 5월 중 출간 목표
    - 영문판 5월 1일 출간 예정

Q & A
Suggestion