



OWASP

Open Web Application
Security Project

Application Security Verification Standard

Wojciech Dworakowski, SecuRing

login: Wojciech Dworakowski



CONNECT. LEARN. GROW.

- OWASP Poland Chapter Leader
- OWASP = Open Web Application Security Project
- Cel: Podnoszenie świadomości w zakresie bezpieczeństwa aplikacji



- Testowanie i doradztwo dotyczące bezpieczeństwa aplikacji i systemów IT

Agenda

- Bezpieczeństwo aplikacji – Wyzwania
 - Definiowanie wymagań
 - Zakres testów bezpieczeństwa
- Przedstawienie ASVS
- Case study
- Podsumowanie



CONNECT.

LEARN.

GROW.

BEZPIECZEŃSTWO APLIKACJI - WYZWANIA



OWASP
Open Web Application
Security Project

„Wishful thinking”

Sponsor projektu

- To jasne że ma być bezpiecznie!
- Mamy dobry zespół
- Wykonawcą jest doświadczoną firmą, z pewnością wiedzą co robią

Project Manager

- Zatrudniamy doświadczonych programistów
- Nie otrzymaliśmy żadnych szczegółowych wytycznych
- Pewnie ryzyko będzie ograniczone innymi metodami

Programista

- Bezpieczeństwo zapewnia framework
- **Ja nie zajmuję się bezpieczeństwem tylko programowaniem**



Hipotetyczny przykład

Aplikacja płatności mobilnych

- Transmisja jest zabezpieczona SSL-em
- ...ale certyfikat serwera nie jest weryfikowany
- **Czy może to wykorzystać intruz, który ma dostęp do tej samej sieci WiFi?**
- Jaki będzie koszt poprawienia tego błędu?

Przykład 2

- Historia transakcji przechowywana offline, w postaci szyfrowanej
- Zarówno do odblokowania offline jak i do uwierzytelnienia online służy 4-cyfrowy PIN
- Aplikacja mobilna blokuje się po 3 próbach
- **Czy może to wykorzystać intruz który „pożyczył” telefon?**
- Jaki będzie koszt poprawienia tego błędu?



Software Security Development Lifecycle

Wymagania

Definiowanie

Projektowanie

Wykonanie

Wdrażanie

- Identyfikacja ryzyka
- Do kluczowych ryzyk są dobierane zabezpieczenia
- Zdefiniowanie **wymagań**

- **Wymagania** są weryfikowane w projekcie

- Testy jednostkowe zabezpieczeń i poprawności kodu (według przyjętych **wymagań**)

- Testy odbiorcze – w zakresie odpowiadającym przyjętym **wymaganiom**




Jak definiować wymagania?

- Najlepiej na podstawie analizy ryzyka
 - Modelowanie zagrożeń
- Czy istnieje „droga na skróty”?
 - – Można oprzeć się na ogólnych wytycznych („zasadach dobrej praktyki”)
 - Trzeba pamiętać że są one dobre w ogólnym przypadku
 - ...a każda aplikacja ma swoją specyfikę



Zakres testów bezpieczeństwa

- Testy „ad hoc”
- Znaleziono N podatności 
- ale...
- Czy znaleziono wszystkie istotne podatności?
- Czy testy objęły wszystkie istotne zagrożenia?
- Czy szukano tam gdzie trzeba?
- Czy test symuluje realne zagrożenie (atak)?

Definiowanie zakresu testów bezpieczeństwa

- Najlepiej – w oparciu o wymagania lub ryzyko
 - Więcej: <http://www.slideshare.net/wojdwo/testowanie-bezpieczestwa-jak-dostosowa-zakres-do-realnych-zagroe-i-budetu>
- Droga na skróty
 - Checklista ogólnych „zasad dobrej praktyki”
 - Dostosowana do specyfiki aplikacji



CONNECT.

LEARN.

GROW.

APPLICATION SECURITY VERIFICATION STANDARD



OWASP
Open Web Application
Security Project

ASVS

- Projekt fundacji OWASP
 - Wersja 1: w 2007 (tłumaczenie na polski)
 - Wersja 2: 2013
- https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project#tab=Downloads
- Lista kontrolna typowych zabezpieczeń
 - Pogrupowana na zakresy (uwierzytelnienie, autoryzacja, walidacja, ...)
 - Kilka poziomów



Poziomy ASVS

- 2007: W zależności od metody badania

Poziom 1 - Weryfikacja automatyczna
Poziom 1A - Skanowanie dynamiczne (częściowa weryfikacja automatyczna)
Poziom 1B - Skanowanie kodu źródłowego (częściowa weryfikacja automatyczna)
Poziom 2 - Weryfikacja ręczna
Poziom 2A - Test bezpieczeństwa (częściowa weryfikacja ręczna)
Poziom 2B - Przegląd kodu (częściowa weryfikacja ręczna)
Poziom 3 - Weryfikacja projektu
Poziom 4 - Weryfikacja wewnętrzna

- 2013: W zależności od profilu ryzyka

Level 0: Cursors
Level 1: Opportunistic
Level 2: Standard
Level 3: Advanced

**Dobór metody badania:
tak żeby osiągnąć cel**

Poziomy ASVS

- **Level 0 (Cursory)** – aplikacja przeszła jakiś (nieuporządkowany) rodzaj weryfikacji.
- **Level 1 (Opportunistic)** – odpowiednio chroni się przed podatnościami które są łatwe do wykrycia.
- **Level 2 (Standard)** – j.w. + odpowiednio chroni się przed powszechnymi podatnościami, których istnienie powoduje średnie lub wysokie ryzyko.
- **Level 3 (Advanced)** – j.w. + odpowiednio chroni się przed wszystkimi zaawansowanymi podatnościami oraz wykazuje zasady dobrego projektowania.

Grupy wymagań (rozdziały)

- V1. Authentication
- V2. Session Management
- V3. Access Control
- V4. Input Validation
- V5. Cryptography (at Rest)
- V6. Error Handling and Logging
- V7. Data Protection
- V8. Communication Security
- V9. HTTP Security
- V10. Malicious Controls
- V11. Business Logic
- V12. Files and Resources
- V13. Mobile



V8: Communications Security Verification Requirements

The table below defines the corresponding verification requirements that apply for each of the verification levels. Verification requirements for Level 0 are not defined by this standard.

COMMUNICATIONS SECURITY VERIFICATION REQUIREMENT	LEVELS		
	1	2	3
V8.1 Verify that a path can be built from a trusted CA to each Transport Layer Security (TLS) server certificate, and that each server certificate is valid.	✓	✓	✓
V8.2 Verify that TLS is used for all connections (including both external and backend connections) that are authenticated or that involve sensitive data or functions.		✓	✓
V8.3 Verify that backend TLS connection failures are logged.		✓	✓

AUTHENTICATION VERIFICATION REQUIREMENT		LEVELS		
		1	2	3
V1.9	Verify all authentication controls are enforced on the server side.		✓	✓
V1.10	Verify password entry fields allow or encourage the use of passphrases, and do not prevent long passphrases or highly complex passwords being entered, and provide a sufficient minimum strength to protect against the use of commonly chosen passwords.		✓	✓
V1.11	Verify all account management functions (such as registration, update profile, forgot username, forgot password, disabled / lost token, help desk or		✓	✓

V11.9 Verify the application has additional authorization (such as step up or adaptive authentication) for lower value systems, and / or segregation of duties for high value applications to enforce anti-fraud controls as per the

	✓	✓
--	---	---

V13.4 Verify that sensitive data is not stored in SQLite database on the device.

✓	✓	✓
---	---	---

Który poziom?

- Zależy od ekspozycji aplikacji na ryzyko
- Ściąga w dodatku A

INDUSTRYSEGMENT	THREAT PROFILE	SUGGESTED ASVS LEVEL
Finance and Insurance	Although this segment will experience attempts from opportunistic attackers, it is often viewed as a high value target by motivated attackers and attacks are often financially motivated. Commonly, attackers are looking for sensitive data or account credentials that can be used to commit fraud or to benefit directly by leveraging money movement functionality built into applications	<i>Level 1: all Internet-accessible applications.</i>
		<i>Level 2: applications that contain sensitive information like credit card numbers, personal information, can move limited amounts of</i>

ASVS trzeba dostosować do specyfiki aplikacji

- Nie wszystkie wymagania zawsze mają sens

V2.3	Verify that sessions timeout after a specified period of inactivity.	✓	✓	
V2.4	Verify that all pages that require authentication to access them have logout links.	✓	✓	

- Nie jest to lista kompletna dla każdej aplikacji, tylko zbiór uniwersalnych zasad dobrej praktyki

Podsumowanie

- ASVS pomaga uporządkować bezpieczeństwo aplikacji
 - Definiowanie wymagań (w tym нефункциональных)
 - Określenie zakresu testów bezpieczeństwa
- Baza, punkt wyjściowy
- Listę wymagań / sprawdzeń trzeba dostosowywać do specyfiki aplikacji



OWASP

Open Web Application
Security Project



PYTANIA

