Narzędzia OWASP dla developerów OWASP ESAPI & AppSensor

Wojciech Dworakowski
OWASP Poland Chapter Leader
SecuRing
wojciech.dworakowski@owasp.org
+48506184550

OWASP
2011-11-23

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

Wybrane projekty OWASP

	DETECT	PROTECT	LIFE-CYCLE
Documentation	Top10 ASVS Testing Guide Code Review Guide	Development Guide Secure Coding Practices – Quick Reference	OpenSAMM
Tools	WebScarab Zed Attack Proxy JBroFuzz	**ESAPI** **AppSensor** ModSecurity Core Ruleset	WebGoat Education Project

~140+ Projektów

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

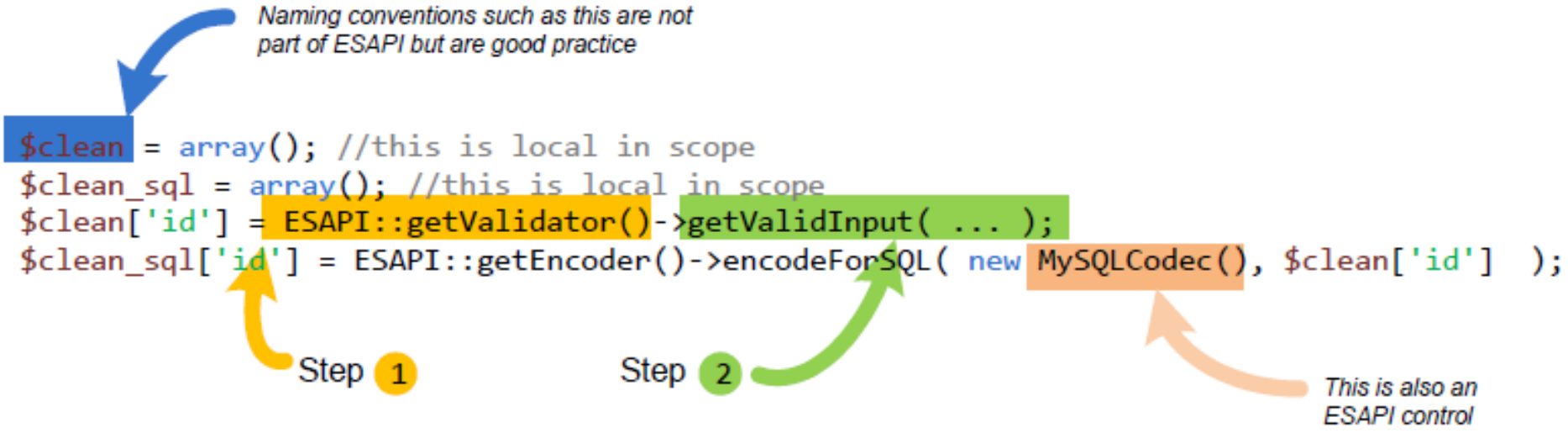
Problemy

- Typowy projekt programistyczny:
  - Brak czasu na bezpieczeństwo aplikacji
  - Brak wiedzy wśród programistów
  - Brak spójnej implementacji zabezpieczeń
  - Rozwijanie wielu aplikacji w wielu językach
- Rezultat
  - Podatności wykrywane (lub nie) podczas testów przed wdrożeniem
  - Niespójne implementacje zabezpieczeń
  - Zabezpieczenia, które da się obejść
  - …

OWASP ESAPI

- *„a free and open collection of all the security methods that a developer needs to build a secure web application”*
- Biblioteka zabezpieczeń
- Stworzone przez ekspertów
- Darmowe (licencja BSD)
- Łatwe do zintegrowania z aplikacją

Przykład



Źródło: OWASP ESAPI Datasheet

ESAPI vs Top 10

Top 10	ESAPI
A1: Injection	Encoder
A2: Cross-Site Scripting (XSS)	Encoder, Validator
A3: Broken Authentication and Session Management	Authenticator, User, HTTPUtilities
A4: Insecure Direct Object Reference	AccessReferenceMap, AccessController
A5: Cross Site Request Forgery	User (CSRF Token)
A6: Security Misconfiguration	SecurityConfiguration
A7: Insecure Cryptographic Storage	Encryptor
A8: Failure to Restrict URL Access	AccessController
A9: Insufficient Transport Layer Protection	HTTPUtilities (Secure Cookie, Channel)
A10: Unvalidated Redirects and Forwards	AccessController

Wspierane platformy

- J2EE,
- .NET,
- Classic ASP,
- Python,
- PHP („alpha”)
- ColdFusion & CFML
- JavaScript
- Ruby, …

Gdzie zacząć?

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

http://esapi.org/

http://code.google.com/p/owasp-esapi-java/ → Wiki

https://www.owasp.org/index.php/ESAPI-Building

https://www.owasp.org/index.php/ESAPI-BuildingWithEclipse

http://www.jtmelton.com/2010/08/17/the-owasp-top-ten-and-esapi-final-summary/

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

(beta!)

OWASP AppSensor

OWASP

Problem

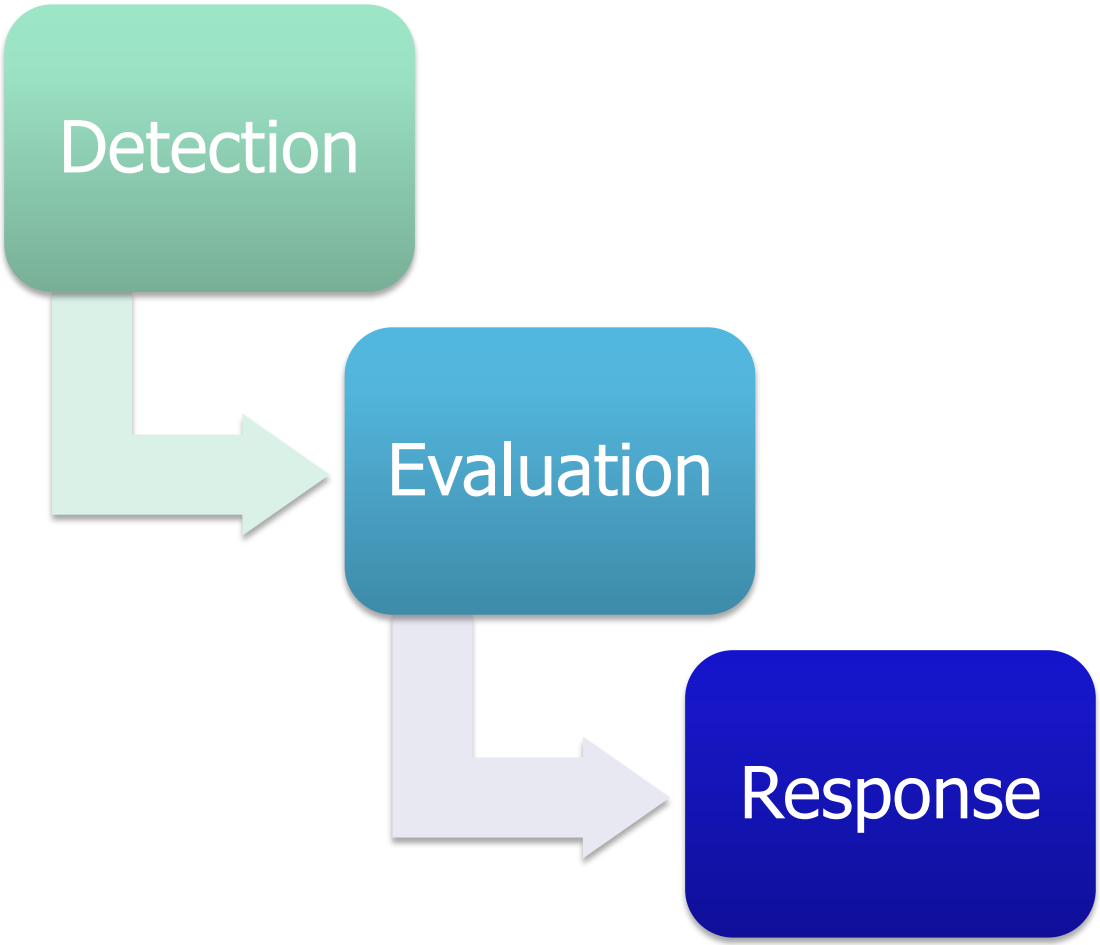
Jak chronić aplikację webową?

- Firewall (tradycyjny)
  - przepuści wszystko na port 80, 443, …
- Firewall + „deep packet inspection”
  - Nie zna specyfiki aplikacji
  - Zablokuje ataki na środowisko ale nie na aplikacje
- Web Application Firewall
  - Nie rozumie kontekstu
  - http://www.bank.com/AccountDetails?id=567896

OWASP AppSensor

- Application Based Intrusion Detection
- Wykrywa i odpowiada na ataki
- WAF ale „wszyty” w kod aplikacji
- Może rozumieć kontekst aplikacji i specyfikę biznesu
- Może być zintegrowany metodami uwierzytelnienia i repozytorium użytkowników
- Ponad 50 detection points / 15 sposobów reakcji

OWASP AppSensor



Detection Points

Exception	# Detection Points
Request	4
Authentication	11
Access Control	6
Session	4
Input	2
Encoding	2
Command Injection	4
File IO	2
User Trend	4
System Trend	3

Signature based

Behavior based

Przykłady

ACE1	Modifying URL Arguments Within a GET For Direct Object Access Attempts
Exception Type	AccessControlException
Description	The application is designed to use an identifier for a particular object, such as using categoryID=4 or user=guest within the URL. A user modifies this value in an attempt to access unauthorized information. This exception should be thrown anytime the identifier received from the user is not authorized due to the identifier being nonexistent or the identifier not authorized for that user.
Considerations	
Example(s)	The user modifies the following URL from site.com/viewpage?page=1&user=guest to site.com/viewpage?page=22&user=admin

UT2	Speed Of Application Use
Exception Type	UserTrendException
Description	The speed of requests from a user indicates that an automated tool is being used to access the site. The use of a tool may indicate reconnaissance for an attack or attempts to identify vulnerabilities in the site.
Considerations	Search spiders may request large quantities of pages from the unauthenticated portion of the website. However, any scripted tool requesting large quantities of pages within the authenticated portion of the site would be suspicious.
Example(s)	The user utilizes an automated tool to request hundreds of pages per minute.

Jak zintegrować z własnym kodem?

```
// This example snippet might be placed on a jsp that
// handles HTTP 404 errors.
// When the page is accessed, this code notifies AppSensor
// that an invalid page request was made.
// Notice that the exception is created, not thrown

new AppSensorException("ACE3", "Invalid request", "Attacker is
   requesting a non-existent (404) page (" + requestedURI + ")");
```

```
// This example snippet might be placed in request handling code
// that expects a form POST to occur (not a GET, not a PUT, etc).
// This code notifies AppSensor that an type of HTTP request was
// made.

AttackDetectorUtils.verifyValidRequestMethod(request,
   AttackDetectorUtils.POST);
```

Response Actions

Category		Response	
Type	Description	ID	Description
Silent	User unaware of application's response	ASR-A	Logging Change
		ASR-B	Administrator Notification
		ASR-C	Other Notification
		ASR-N	Proxy
Passive	Changes to user experience but nothing denied	ASR-D	User Status Change
		ASR-E	User Notification
		ASR-F	Timing Change
Active	Application functionality reduced for user(s)	ASR-G	Process Terminated
		ASR-H	Function Amended
		ASR-I	Function Disabled
		ASR-J	Account Logout
		ASR-K	Account Lockout
		ASR-L	Application Disabled
Intrusive	User's environment altered	ASR-M	Collect Data from User

Gdzie zacząć?

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

https://www.owasp.org/images/2/2f/OWASP_AppSensor_Beta_1.1.pdf

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

http://www.jtmelton.com/2010/11/10/application-intrusion-detection-with-owasp-appsensor/