Owasp Security Shepherd Project

Tarik EL AOUADI

Owasp France Meeting – Jul 7th 2016

tarik.elaouadi@owasp.org

OWASP

The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

- Tarik EL AOUADI (tarik.elaouadi@owasp.org)
  - +5 years of software development
    - Accenture, Bull, …
  - +5 years of software security
    - Consulting, code review, pentesting, training
  - Owasp Morocco Chapter Co-Leader
    - Speaker & Training Manager
    - Owasp Morocco Cyber Security Conference 2016
      - Marrakech (Nov 25th, 26th)
  - Entrepreneur (Adam Ridson)
    - Improving Software Security

Adam Ridson
IMPROVING SOFTWARE SECURITY
RECHERCHE - INNOVATION - DÉVELOPPEMENT SÉCURISÉ - OPTIMISATION - NORMALISATION

- Owasp Security Shepherd Project

The OWASP Security Shepherd project is a web and mobile application security training platform. Security Shepherd has been designed to foster and improve security awareness among a varied skill-set demographic. The aim of this project is to take AppSec novices or experienced engineers and sharpen their penetration testing skillset to security expert status

Covered AppSec topics

OWASP
The Open Web Application Security Project

- The Security Shepherd project covers the following web and mobile application security topics

- SQL Injection
- Broken Authentication and Session Management
- Cross Site Scripting
- Insecure Direct Object Reference
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross Site Request Forgery
- Unvalidated Redirects and Forwards
- Poor Data Validation
- Insecure Data Storage
- Unintended Data Leakage
- Poor Authentication and Authorisation
- Broken crypto
- Client Side Injection
- Lack Of Binary Protections

Detailed explaination

OWASP
The Open Web Application Security Project

Admin

Scoreboard

Lessons

- XBroken Crypto
- XBroken Session Management
- XClient Side Injection
- XContent Provider Leakage
- XCross Site Request Forgery
- XCross Site Scripting
- XFailure to Restrict URL Access
- XInsecure Cryptographic Storage
- XInsecure Data Storage
- XInsecure Direct Object References
- XPoor Authentication
- XPoor Data Validation
- XReverse Engineering
- XSecurity Misconfiguration
- XSQL Injection

Submit Result Key Here... Submit

SQL Injection Lesson

Injection flaws, such as SQL injection, occur when hostile data is sent to an interpreter as part of a command or quer y. The hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data. Inje ctions attacks are of a high severity. Injection flaws can be exploited to remove a system's confidentiality by accessin g any information held on the system. These security risks can then be extended to execute updates to existing data affecting the systems integrity and availability. These attacks are easily exploitable as they can be initiated by anyon e who can interact with the system through any data they pass to the application.

The following form's parameters are concatenated to a string that will be passed to a SQL server. This means that the data can be interpreted as part of the code.

The objective here is to modify the result of the query with SQL Injection so that all of the table's rows are returned. T his means you want to change the boolean result of the query's WHERE clause to return true for every row in the tabl e. The easiest way to ensure the boolean result is always true is to inject a boolean 'OR' operator followed by a true st atement like 1 = 1.

If the parameter is been interpreted as a string, you can escape the string with an apostrophe. That means that everyt hing after the apostrophe will be interpreted as SQL code.

Hide Lesson Introduction

Exploit the SQL Injection flaw in the following example to retrieve all of the rows in the table. The lesson's solution key will be found in one of these rows! The results will be posted beneath the search form.

Please enter the user name of the user that you want to look up

Get this user

Competitive Learning

OWASP
The Open Web Application Security Project

1st:	dcua 36 15 6	3941
2nd:	NULL Life 18 12	3558
3rd:	arusell 2 2 3	3053
4th:	andro1de 1 3	2996
5th:	micaman 1 1 1	2966
6th:	Insanity 3 10 2	2909
7th:	longerthan5characters 1 2 3	2878
8th:	aiacobelli 1 1	2516
9th:	ottucsakj 3 3 2	2501
10th:	mfocuz 2 4	2084

Easy configuration

OWASP
The Open Web Application Security Project

Download

OWASP
The Open Web Application Security Project

- https://www.owasp.org/index.php/OWASP_Security_Shepherd
- https://github.com/OWASP/SecurityShepherd
- https://github.com/OWASP/SecurityShepherd/releases/tag/v3.0v (latest release)

Demo

OWASP
The Open Web Application Security Project