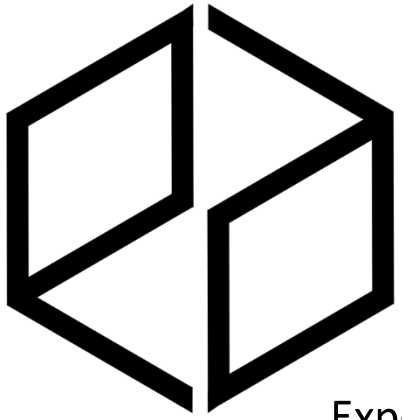
www.pandoralabs.net

PANDORA
SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

OWASP TOP 10: #7 Missing Function Access Control

By @isaacsabas



PANDORA
SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

www.pandoralabs.net

We are a Security-as-a-Service company

Providing businesses with on-demand IT security controls for them to meet their 24x7 security strategies & requirements.

We Make IT Secure

OWASP

Open Web Application Security Project


A1: Injection
A2: Broken Authentication and Session Management
A3: Cross-Site Scripting (XSS)
A4: Insecure Direct Object References
A5: Security Misconfiguration
A6: Sensitive Data Exposure
A7: Missing Function Level Access Controls
A8: Cross Site Request Forgery (CSRF)
A9: Using Components with Known Vulnerabilities
A10: Unvalidated Redirects and Forwards

OWASP #7

Missing Function Access Control

OWASP Top 10 Vulnerabilities

Flaws in the web application that allows access to functions that needs authorization before allowing privileges.

Missing Function Access Control

What is it?

How is this vulnerability exploited?

1. No secure access model
   - User X should only have access to function A
2. Action are passed via URL
   - *http://www.example.com/?post=434&**action=view***
   - *http://www.example.com/post/434?**action=modify***

What are the Risks When Exploited?

- Administrative function access to unauthorized users
- Data manipulation and data theft (same as IDOR)
  - Change of database content (e.g. change of delivery address)
  - Delete database entry (e.g. another user account, invoice, etc.)
  - Loss of profits (e.g. access to promo codes or gift certificates)

How do I Prevent Such Vulnerability?

- Deny access to all functionality by default
- Use access control lists (or access control model) and role based authentication mechanism
- Don’t just hide functions

Go to http://www.securesavingsbank.com

EXPLOIT DEMO

How simple it is to test for a missing function access control vulnerability.

TIME FOR

Q&A

OWASP Top 10 – Missing Function Access Control

Go download WebGoat

https://github.com/WebGoat/WebGoat-Legacy

TRY IT YOURSELF

Some homework for you to learn a bit more.

WebGoat Installation How-To

1. Download Java VM, JDK 1.7
2. Download WebGoat: https://webgoat.atlassian.net/builds/browse/WEB-WGM/latestSuccessful/artifact/shared/WebGoat-Embedded-Tomcat/WebGoat-6.0.1-war-exec.jar
3. Run the .jar file:
    1. java -jar WebGoat-6.0-exec-war.jar
4. Then navigate in your browser to: (http://localhost:8080/WebGoat)
5. Login using guest account
6. Go to Access Control Flaws and complete the following exercises:
    1. Stage 1

OWASP #7

Missing Function Access Control

OWASP Top 10 Vulnerabilities

www.pandoralabs.net

PANDORA
SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

OWASP TOP 10: #7 Missing Function Access Control

By @isaacsabas