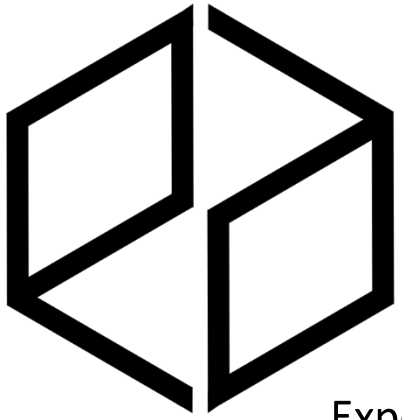
www.pandoralabs.net

PANDORA
SECURITY LABS

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

OWASP TOP 10: #8 Cross-Site Request Forgery (CSRF)

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 #8

Cross-Site Request Forgery (CSRF)

OWASP Top 10 Vulnerabilities

Weakness in a web application that allows attacker to force a user to unknowingly perform certain actions.

Cross-Site Request Forgery (CSRF)

What is it?

Samples

- Get a user to post something (e.g.Facebook/Twitter posts)
- Make user make certain payments or purchase

What are the Risks When Exploited?

- Reputation
- Financial Loss

How is this vulnerability exploited?

1. The web application allows requests to originate from servers other than itself.
2. There is no unique token that is tied to a user session.

How do I Prevent Such Vulnerability?

- Make sure that all request should only come from your server (or allowed servers)
- Issue tokens to each session

Go to http://www.securesavingsbank.com

EXPLOIT DEMO

How simple it is to test for a CSRF vulnerability.

TIME FOR

Q&A

OWASP Top 10 – Cross-Site Request Forgery (CSRF)

OWASP #8

Cross-Site Request Forgery (CSRF)

OWASP Top 10 Vulnerabilities

www.pandoralabs.net

PANDORA
SECURITY LABS

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

OWASP TOP 10: #8 Cross-Site Request Forgery (CSRF)

By @isaacsabas