www.pandoralabs.net

### PANDORA SECURITY LABS

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

OWASP TOP 10: #10 Unvalidated Redirects & Forwards By @isaacsabas



We are a Security-as-a-Service company

Expert advice. Experience advantage. Proactive Security Solutions Through Cutting-Edge Research. www.pandoralabs.net Providing businesses with on-demand IT security controls for them to meet their 24x7 security strategies & requirements.

We Make IT Secure



Who we are. Why we exist.



# Open Web Application Security Project



OWASP Top 10 – Sensitive Data Exposure

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 Top 10 – Sensitive Data Exposure

## OWASP #10 Unvalidated Redirects & Forwards

**OWASP Top 10 Vulnerabilities** 



Weakness in a web application that allows users to control which site you are redirected to by altering a user supplied parameter.

### Unvalidated Redirects & Forwards

What is it?



#### How is this vulnerability exploited?

- URL parameter not being validated
- Inserting URLs through GET parameters or other embedded components



#### How do I Prevent Such Vulnerability?

- Avoid redirects based on user parameters
- If you need to redirect, avoid using any user-supplied data to determine which site to be redirected to.
- Have a method to verify the target URL and verify that the user does in fact need to be redirected.

#### Go to http://www.securesavingsbank.com

## **EXPLOIT DEMO**

How simple it is to test for a Unvalidated Redirect vulnerability.

PANDORA SECURITY LABS

## TIME FOR Q&A

**OWASP Top 10 – Sensitive Data Exposure** 



## OWASP #10 Unvalidated Redirects & Forwards

**OWASP Top 10 Vulnerabilities** 



www.pandoralabs.net

### PANDORA SECURITY LABS

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

OWASP TOP 10: #10 Unvalidated Redirects & Forwards By @isaacsabas