www.pandoralabs.net

PANDORA SECURITY LABS

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

OWASP TOP 10: #3 Cross-Site Scripting (XSS)

By @isaacsabas

PANDORA SECURITY LABS

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

www.pandoralabs.net

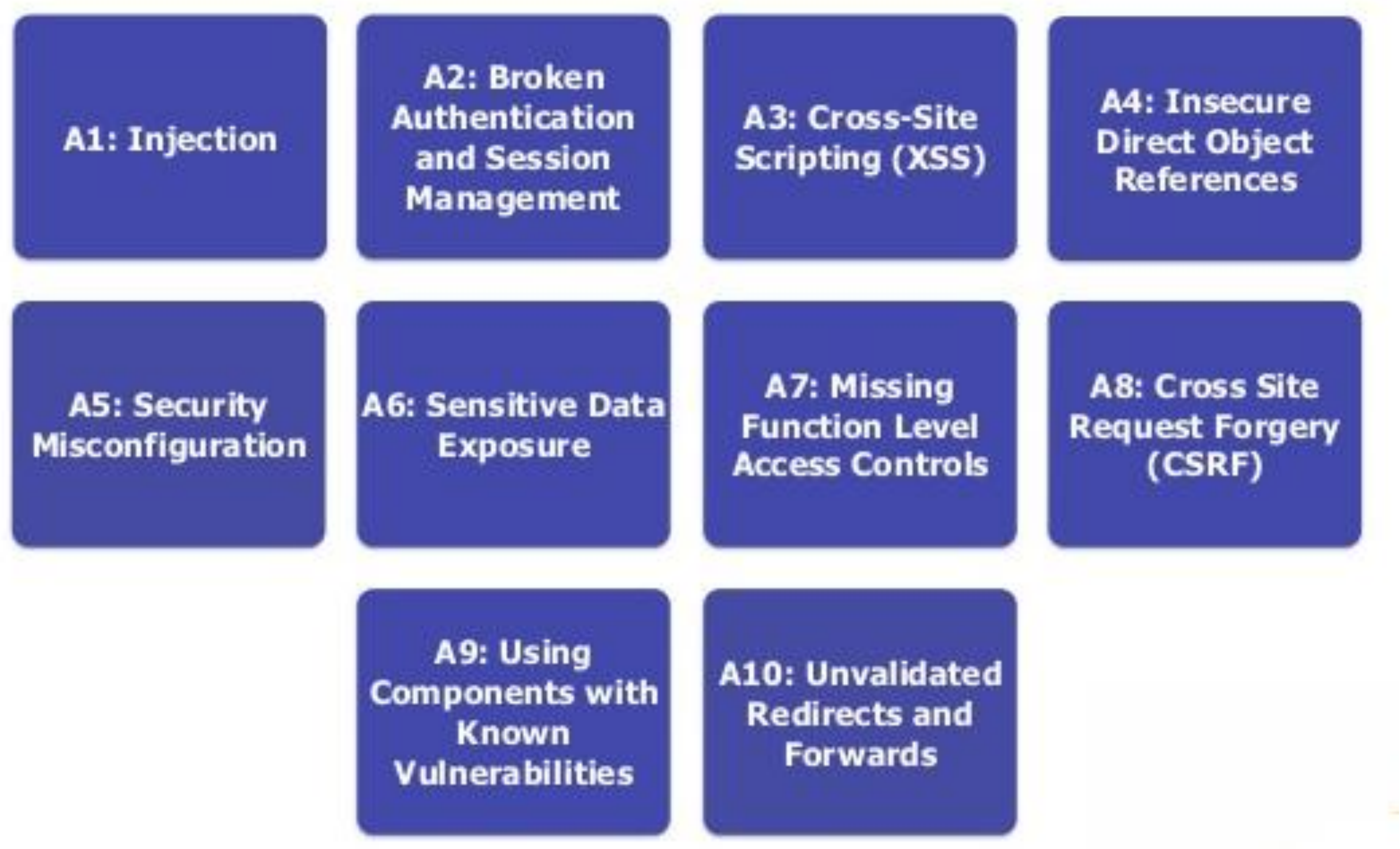
We are a Security-as-a-Service company

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)

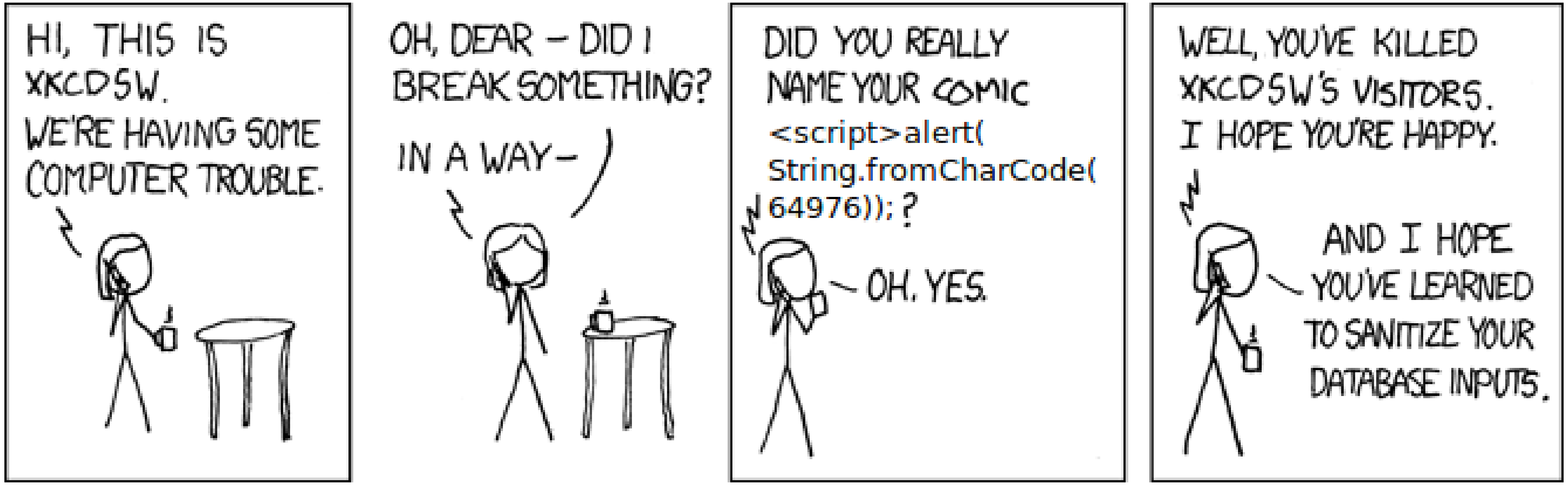
A9: Using Components with Known Vulnerabilities

A10: Unvalidated Redirects and Forwards

OWASP #3

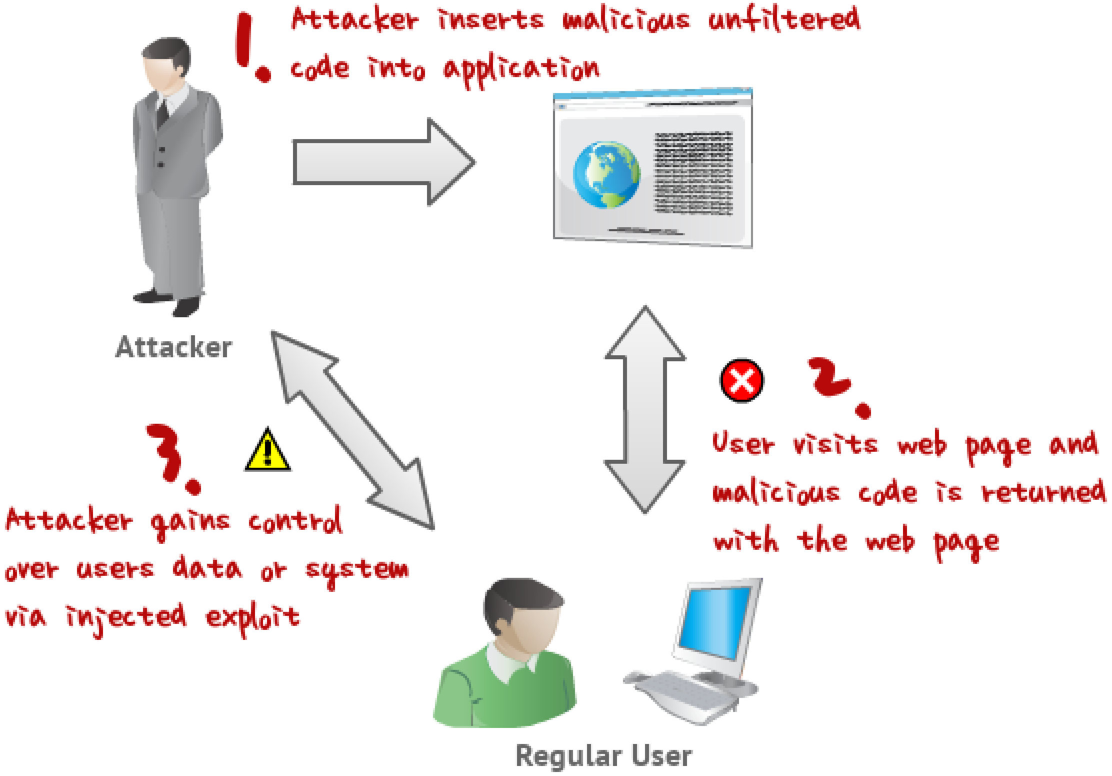
Cross-Site Scripting (XSS)

OWASP Top 10 Vulnerabilities


HI, THIS IS XKCDSW. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID I BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR COMIC <script>alert(String.fromCharCode(64976)); ?
OH. YES.
WELL, YOU'VE KILLED XKCDSW'S VISITORS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

What is XSS?

Where it all began.


1. Attacker inserts malicious unfiltered code into application
Attacker
2. User visits web page and malicious code is returned with the web page
3. Attacker gains control over users data or system via injected exploit
Regular User

How does XSS work?

How does one exploit a XSS vulnerability?

Type of XSS Attacks

1. Reflected XSS
2. Stored XSS
3. DOM-based XSS

What are the risks with XSS?

1. Compromise of victim’s user account
2. Exfiltration of data from target web application
3. Defacement
4. Redirection to malicious site or phishing site
5. Malware download

How to prevent the XSS flaws?

1. Use well supported framework
2. Output encoding
3. Use *HttpOnly* attribute for cookies
4. Input validation

Go to http://www.securesavingsbank.com

EXPLOIT DEMO

How simple it is to test for a XSS vulnerability.

Demo

1. Use the main search box to validate basic XSS flaws
2. Use vulnerability to construct a link that will redicrect the user to a "malicious" site.
3. Steal victim's cookies using XSS.

TIME FOR

Q&A

OWASP Top 10 – Cross-Site Scripting

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 Cross-Site Scripting Menu
    1. Answer Stages 1,3 and 5.

OWASP #3

Cross-Site Scripting (XSS)

OWASP Top 10 Vulnerabilities

www.pandoralabs.net

PANDORA
SECURITY LABS

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

OWASP TOP 10: #3 Cross-Site Scripting (XSS)

By @isaacsabas