Secure your web applications from Cross Site Scripting (XSS)

Anwar Mohammed

FedCASIC Conference

Apr 12, 2017 - Suitland, MD

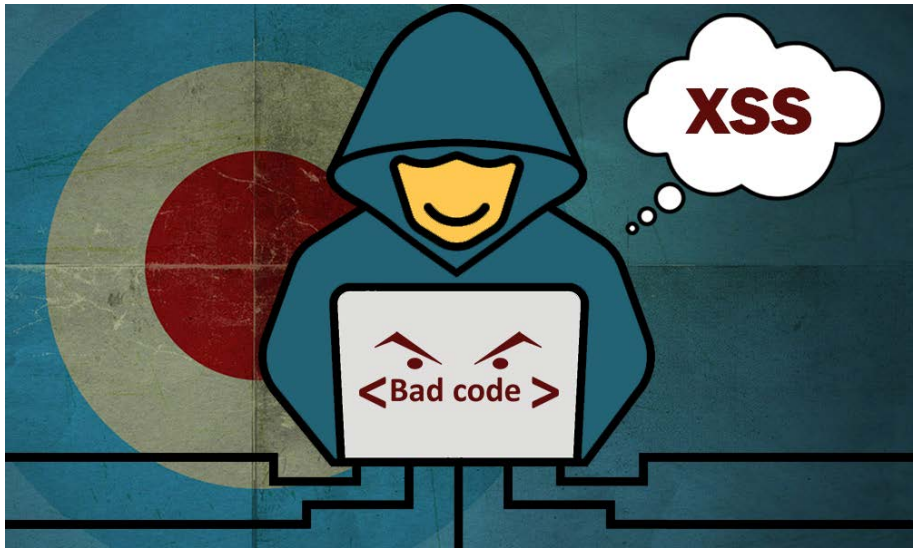
Cross-Site Scripting: Outline

- Definition
- Impact
- Types
- Techniques
- Tools
- Testing
- Demo
- Defense

What is Cross-Site Scripting?

- Cross-Site Scripting aka “XSS” or “CSS”

- Attackers inject malicious code (JavaScript, VBScript, ActiveX, HTML, Flash) for execution on a victim's system by hiding it within legitimate requests



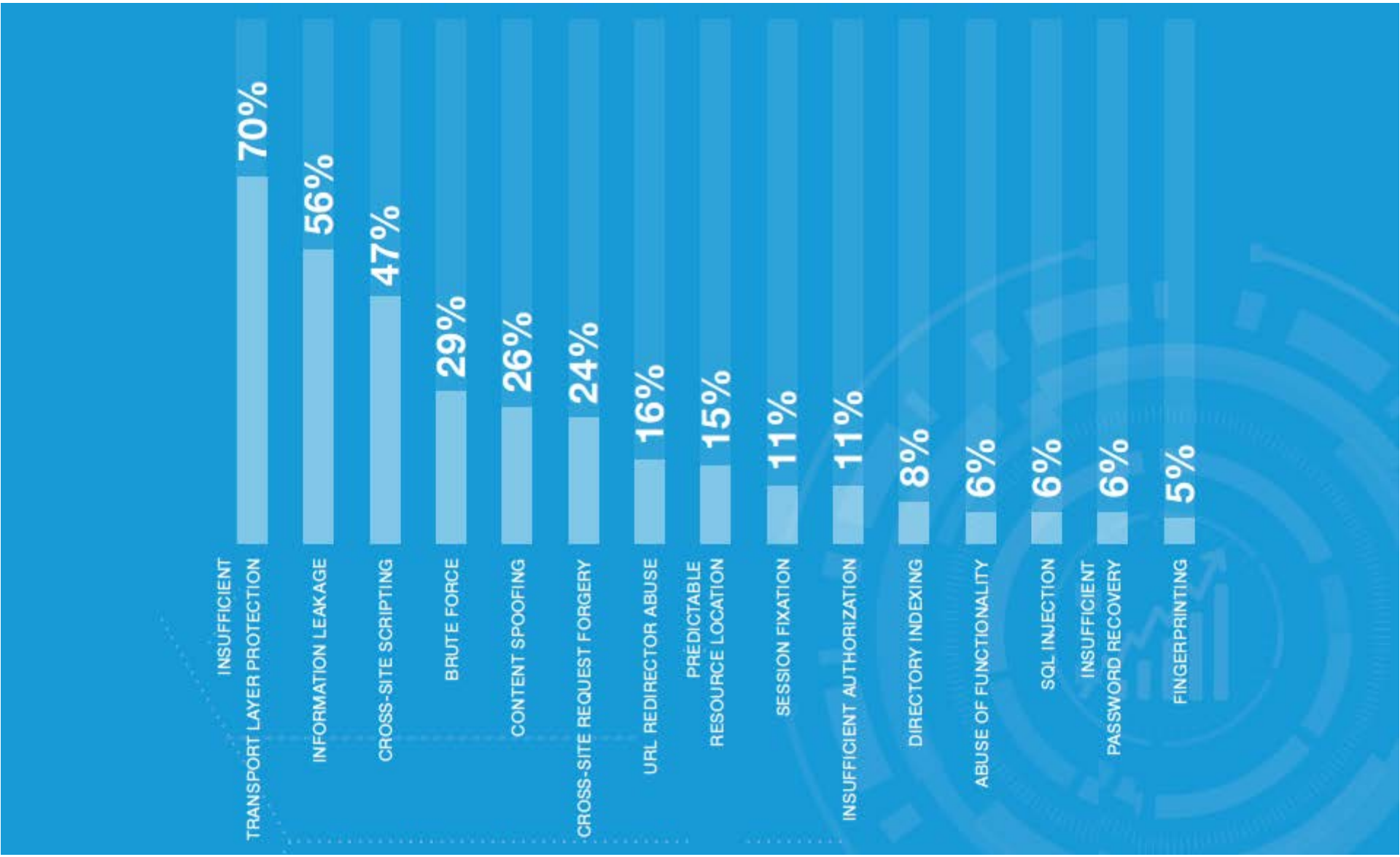
Conditions for XSS

A Web application accepts user input

The input is used to create dynamic content

The input is sufficiently validated

Top 15 Vulnerability List



White Hat Security Report 2016

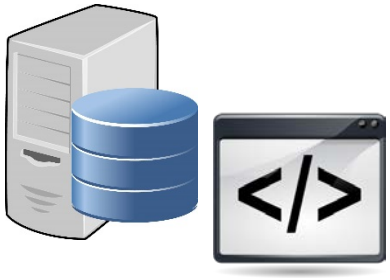
https://www.whitehatsec.com/info/website-stats-report-2016-wp/

XSS: Real World examples

Players in XSS

Client/Users
Any type of customer
Anonymous user

Attacker/hacker
Anonymous Internet User
Malicious Internal User



Company's Web server
Internal/External Web applications

XSS Types

- **Stored XSS**

  Persistent or Type I
  [blogs]

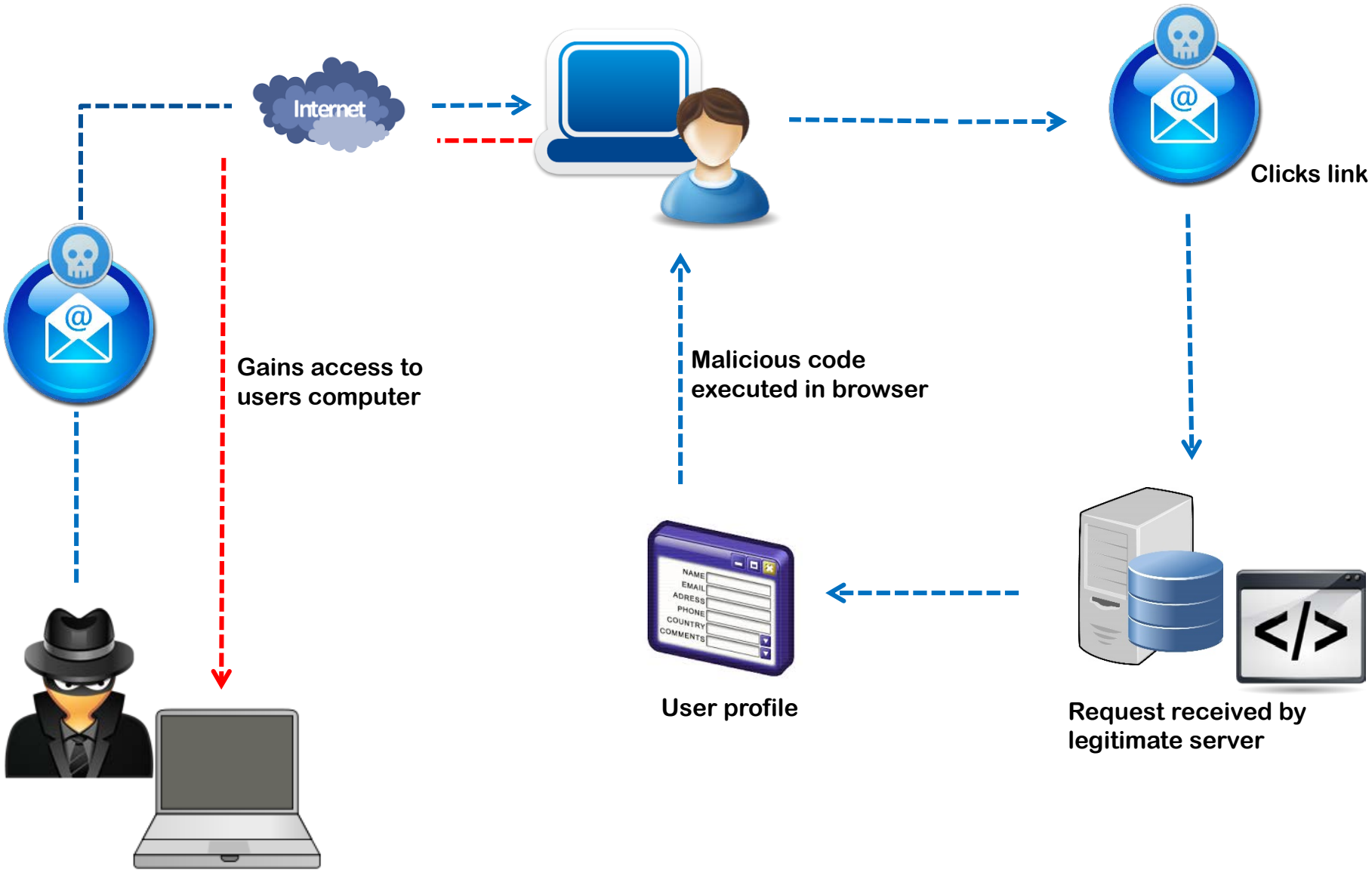
- **Reflected XSS**

  Non-Persistent or Type II
  [phishing]

- **DOM-based**

  Variant of both persistent, reflected;
  Malicious JavaScript is executed after page load

XSS: Email Attack



XSS Attack Payload

XSS Can result in…

- Session Hijacking
- Site Defacement
- Site Redirection
- Phishing
- Data Theft
- Keystroke Logging
- Network Scanning

Demo

Disclaimer

Hacking is illegal and should not be performed.

Penetration Testing is an agreed form of audit between two parties and should be bound in writing defining the scope and nature of what is to be audited.

Certified Ethical Hacker.

Common XSS Tools

WebInspect

IBM Rational

N-stalker

OWASP ZAP

Acunetix

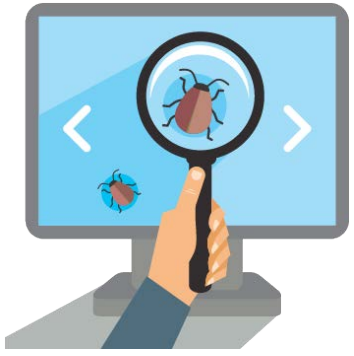
Firefox add-ons (Hackbar, XSS ME)

W3AF - Web App Attack and Audit Framework.

Testing for XSS

- Test all pages that display input originating from users
- Test by inserting malicious script or characters to see if they are ultimately displayed back to the user
- Examine code to ensure that application data is HTML encoded before being rendered to users
- Very easy to discover XSS via dynamic testing
- Test each input to see if data gets rendered back to the user.

<script>alert('XSS')</script>



Preventing XSS: Input Validation

Please enter your phone number

Phone No Formats
1234567890
123-456-7890
(123) 456-7890
123.456.7890
123 456 7890
+1-123-456-7890

Please enter your phone number

123 – 456 – 7890

- Accept known good (“whitelist” or +ve validation)
- Reject known bad (“blacklist” or -ve validation)
- Sanitize (change input to acceptable format)

Preventing XSS: Output Encoding/Escaping

Characters will still render in a browser correctly; escaping simply lets the interpreter know the data is not meant to be executed.

Characters	Description	HTML Entity	Entity number
	Non-breaking space		
	Less than	&lt;	&#60;
>	Greater than	&gt;	&#62;
&	Ampersand	&amp;	&#38;
!	Exclamation mark	&excl;	&#33;
"	Quotation mark	&quot;	&#34;
#	Number sign	&num;	&#35;
%	Percent sign	&percnt;	&#37;
‘	Open single quote	&lsquo;	&#8216;
’	Close single quote	&rsquo;	&#8217;

<script> gets converted to **<script>**

XSS: Summary

- A code injection attack due to insecure handling of user input.
- Allows attacker to execute malicious code in a victim's browser.
- Compromises security of both the website and its users.
- Persistent, Reflected, DOM-based types: performed in different ways but same effect.
- Best way of preventing is to perform secure input handling in both client-side and server-side code.

Know the vulnerabilities

- OWASP
  (http://www.owasp.org)
- National Vulnerability Database
  (http://nvd.nist.gov)
- Vulnerability Notes Database
  (https:// www.kb.cert.org/vuls/)
- SANS Top 20
  (www.sans.org/critical-security-controls/)
- White Hat security
  (www.whitehatsec.com)

Questions?

Anwar Mohammed

Program Manager

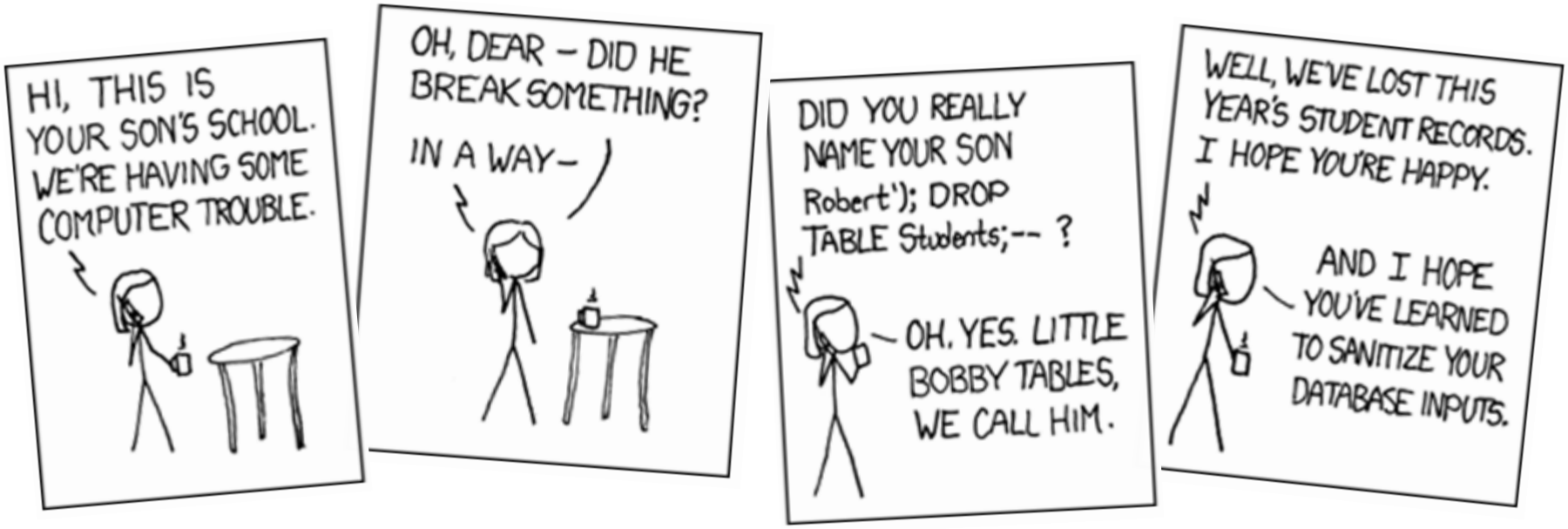
Software Quality Assurance

919.541.7308

amohammed@rti.org

Behind every successful Coder
there is an even more successful De-coder to understand that code
- Anonymous

Exploits of a mom



Source: http://xkcd.com/327/