



Web 2.0 Testing

OWASP

31/07/2010

Chandrasekar Umapathy

CRISC, CISM, CBCP, CSSLP, LPT, CEH,
CHFI, ECSA, ENSA, CPTS, ISO27001
(LA)(I), ITIL, CCSA, and CCSE, CWNA,
BS25999,

OWASP Chennai Chapter Lead

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

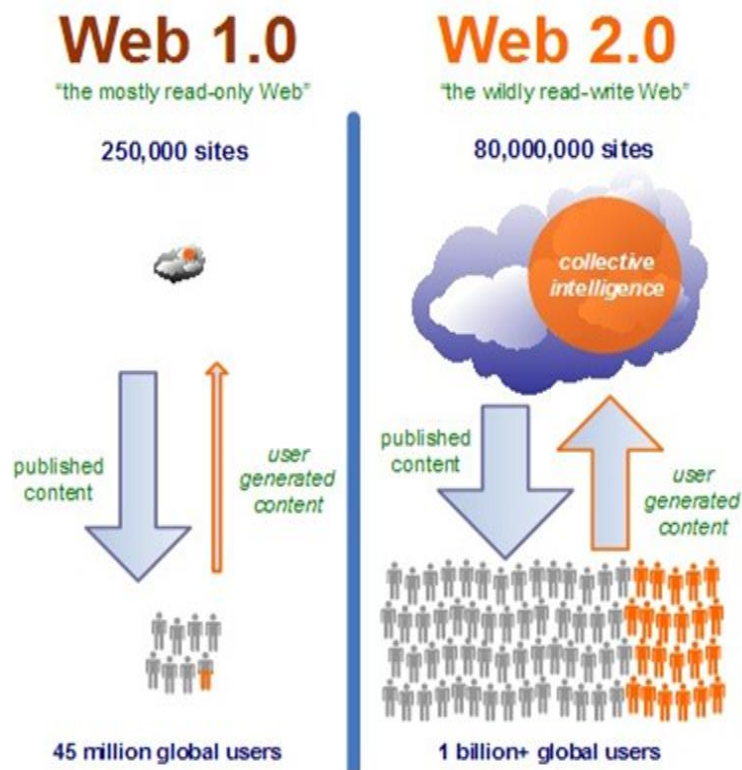
The OWASP Foundation

<http://www.owasp.org>

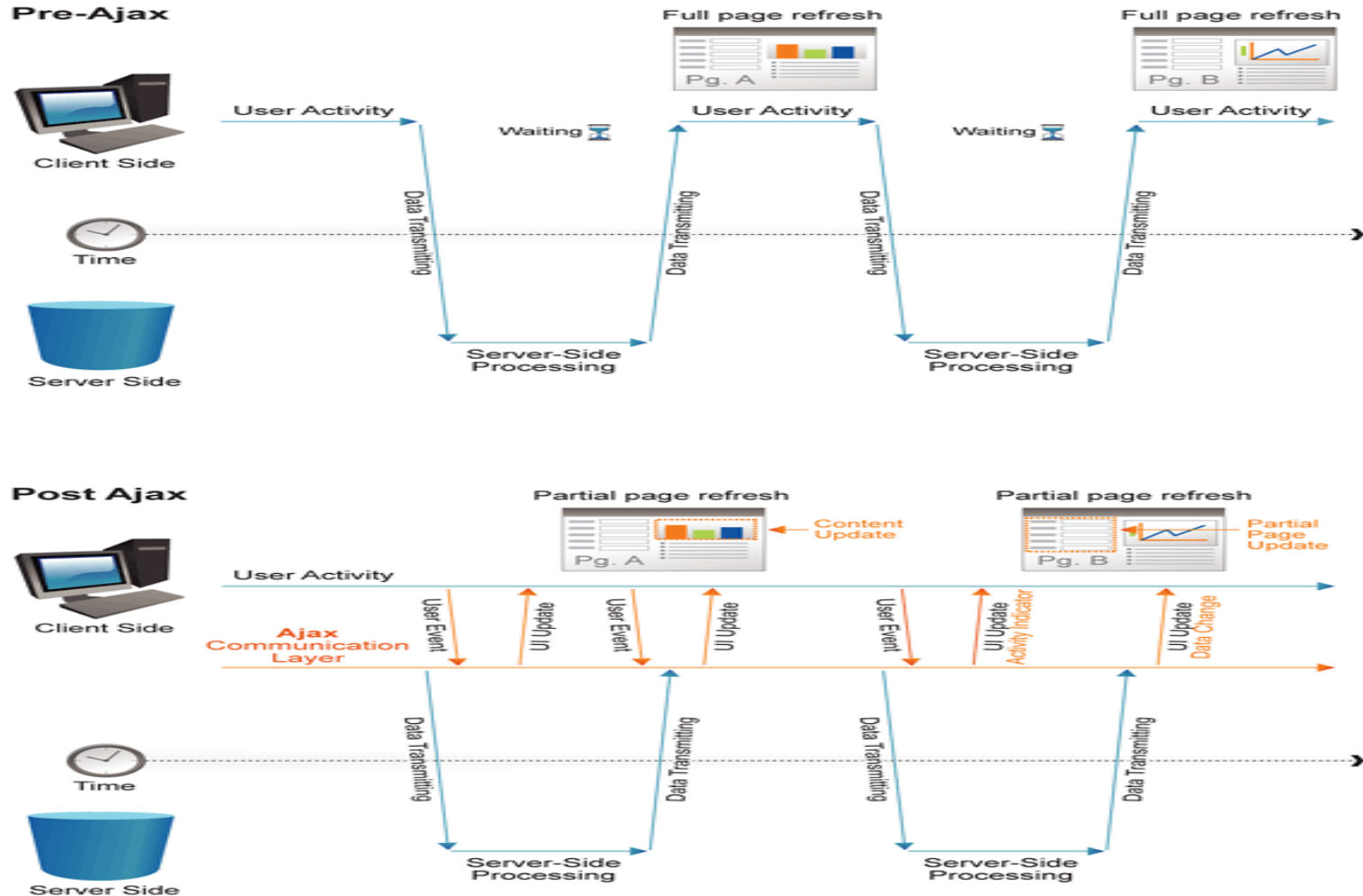
Agenda

- Increase in Web 2.0 Applications
- Traditional Web Model vs Ajax Web Model
- Hacking attempts on Web 2.0 Applications
- AJAX Real attacks examples
- Challenges in Web 2.0 Testing
- Approach to Address Security Testing Concerns
- Conclusion & Questions

Increase in Web 2.0 Applications



Traditional Vs New Web Model



Hacking attempts on Web 2.0 Applications

Facebook Accounts Hacked Sold

Facebook is not able to estimate how many more accounts may be compromised by other hackers.

Selling price : \$25 per 1000 accounts with ten friends or less, and \$45 per 1,000 for those accounts with more than ten friends.

MySpace

MySpace, an even larger social networking site with an estimated 250 million users, has been subverted on multiple occasions by malware attackers during the last year.

Impact: "In less than 24 hours, 'Samy' had amassed over 1 million friends on the popular online community"

Twitter

Twitter knocked offline by DDoS attack.

Popular micro blogging
Twitter was knocked offline for an extended period by massive distributed denial-of-service attacks.

Hacking Amazon's Cloud and Other Web 2.0 Threats

Amazon's cloud can be hacked for BitTorrent , and social network sites are hotbeds for cyber crime.



AJAX Real attacks examples

Group technologies means there are more elements to attack - increased attack surface

Application is delivered to the browser. The attacker controls the functionality of the application.

Ajax application is still a web application – traditional web attack techniques can be used.

Chances developers commit mistakes like exposing internal functions of the application.

New ways of interaction means more complexity.

Samy ,Jammanner Nduja - Webmail XSS worm

OWASP

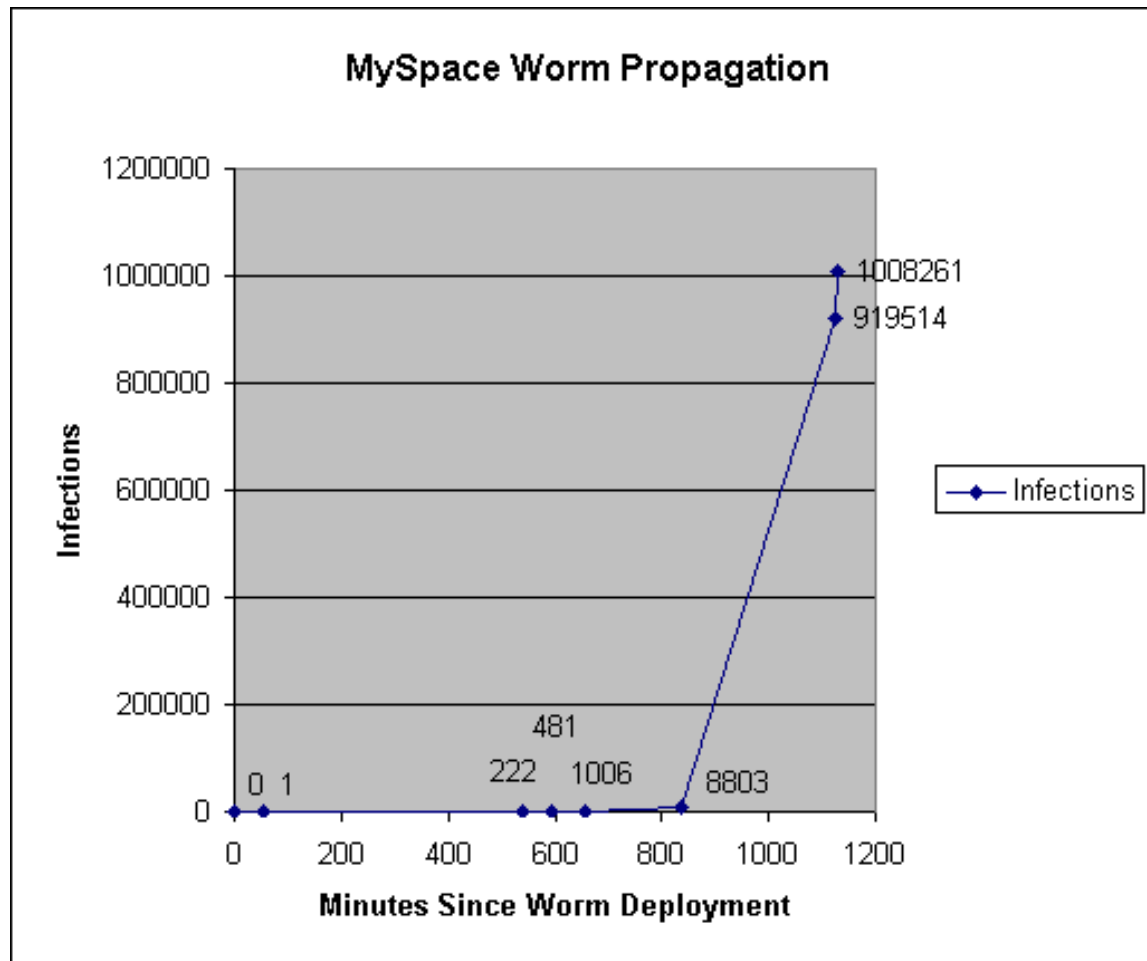


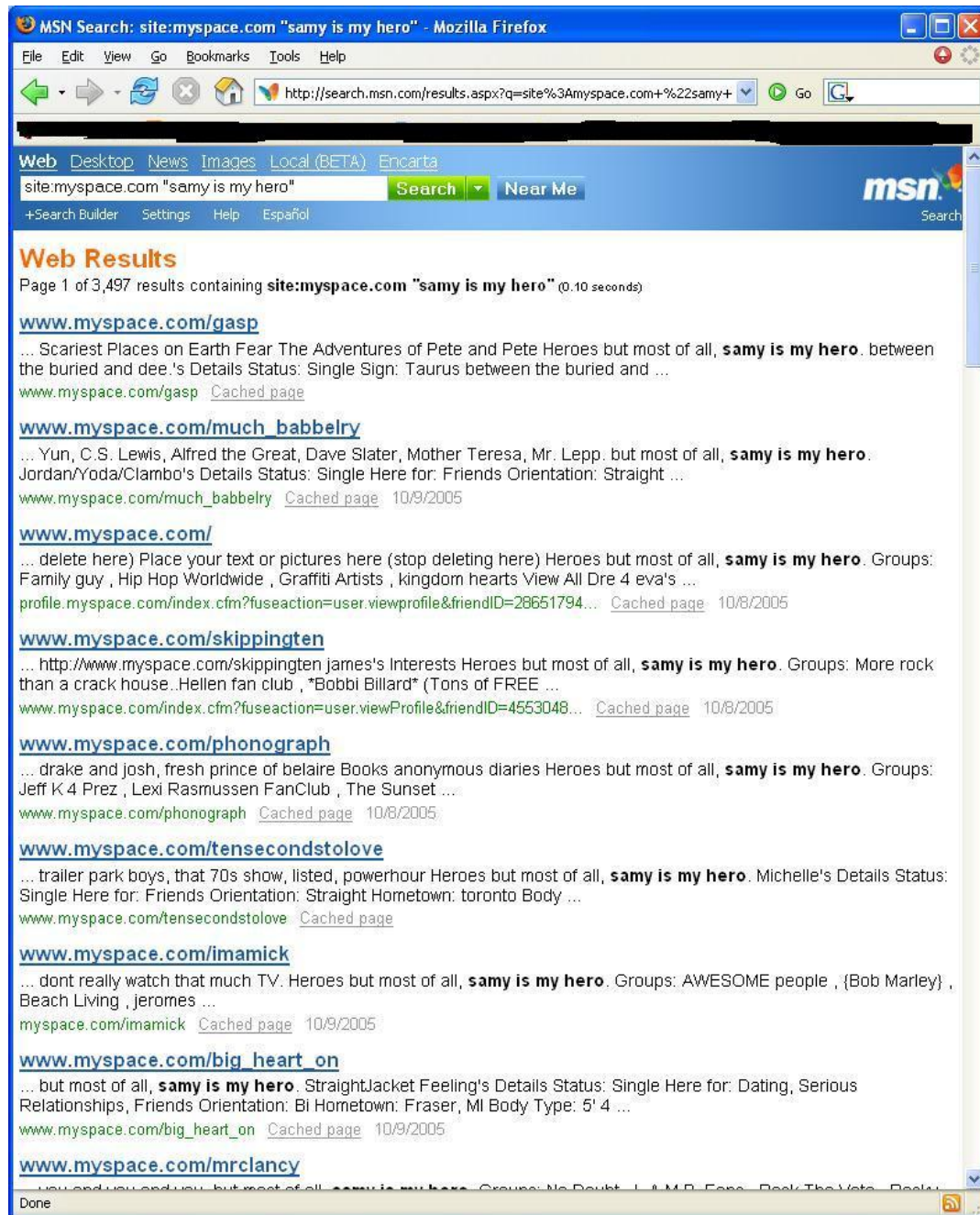
Ajax Security – Case Study – Samy worm

- Inserted HTML and JavaScript through MySpace's profile editor.
- Automated the friend selection process. Instead of someone selecting Samy as a friend, the worm automated the procedure with JavaScript.
- The result of the code injection made the visitor and all visitor friends to be friend Samy when visiting Samy's page. Samy automatically also became their "hero".
- Worm Source Code: <http://namb.la/popular/tech.html>

Ajax – Case Study – Samy worm (cont)

- **Impact:** “In less than 24 hours, 'Samy' had amassed over 1 million friends on the popular online community”





Screenshot showing list of Myspace profiles infected by Samy Worm



site:myspace.com "but most of all, samy is my hero"

Search

[Advanced](#) · [Options](#)

Web results 1-10 of 532

See also: [Images](#), [Video](#), [News](#), [Maps](#), [MSN](#), [More](#) ▼

[MySpace.com - w1z@rd - 28 - Male - The BIZ by way of the roach, North ...](#)

Heroes: **but most of all, samy is my hero**. Groups: David Sedaris Fans , Indigenous of the Western Hemisphere , THE GRASSROOTS GALLERY OF PHOTOGRAPHY , American Indian Movement , Institute ...

[profile.myspace.com/index.cfm?fuseaction=user.viewprofile&friendid=146247398](#) · [Cached page](#)

[MySpace.com - hannahsaurus♥rex - 45 - Female - 903984752, Alabama ...](#)

MySpace profile for hannahsaurus♥rex with pictures, videos, personal blog, interests, information about me and more

[profile.myspace.com/index.cfm?fuseaction=user.viewprofile&friendid=36178890](#) · [Cached page](#)

[MySpace.com - scott - 22 - Male - San Diego, CALIFORNIA - www.myspace ...](#)

... is the chosen one | Samy can set you free Add me as a friend samyismyhero Click here to go back. You may now view this profile. I like many books... **but most of all, samy is my hero**.

[profile.myspace.com/index.cfm?fuseaction=user.viewprofile&friendid=82471737](#) · [Cached page](#)

[MySpace.com - Harold Hunter - 31 - Male - Ny, NEW YORK - www.myspace ...](#)

... marques brown **but most of all, samy is my hero**. ...

[www.myspace.com/haroldhunter](#) · [Cached page](#)

[MySpace.com - Anniechica - 23 - Female - tucson, ARIZONA - www.myspace ...](#)

Heroes: **but most of all, samy is my hero**. hahahah wait whos Samy? But really my Mom and my Dad, with out them I would be nothing and have nothing.

[profile.myspace.com/index.cfm?fuseaction=user.viewprofile&friendid=252688](#) · [Cached page](#)

[MySpace.com - 4.0 - 300 - pockets - PSAT - 47 - Female - My ...](#)

Except for my grandfather, G.Canfield. Please do not send her rude messages or comments. It's not nice. **but most of all, samy is my hero**. ...

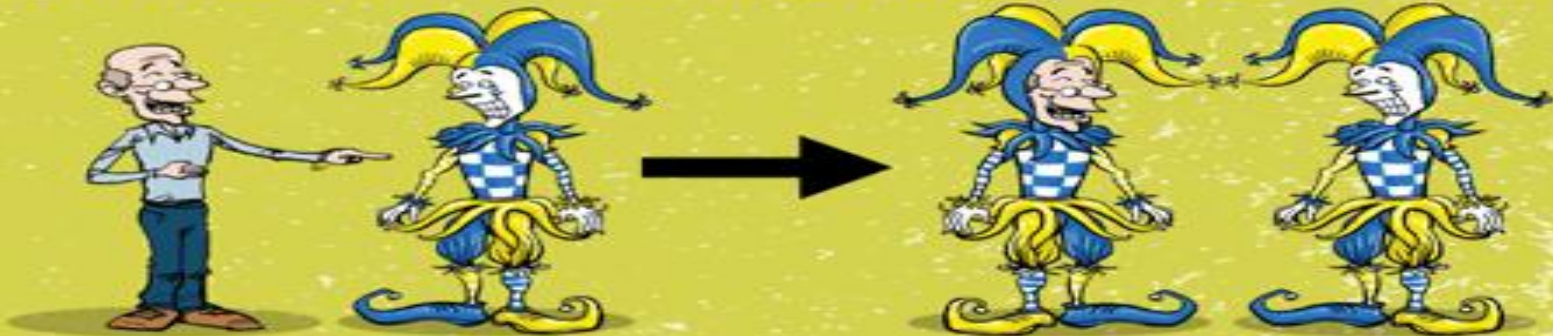
[profile.myspace.com/index.cfm?fuseaction=user.viewprofile&friendid=128925332](#) · [Cached page](#)

And today there are still Myspace accounts with Samy as a hero!

532 results with live.com

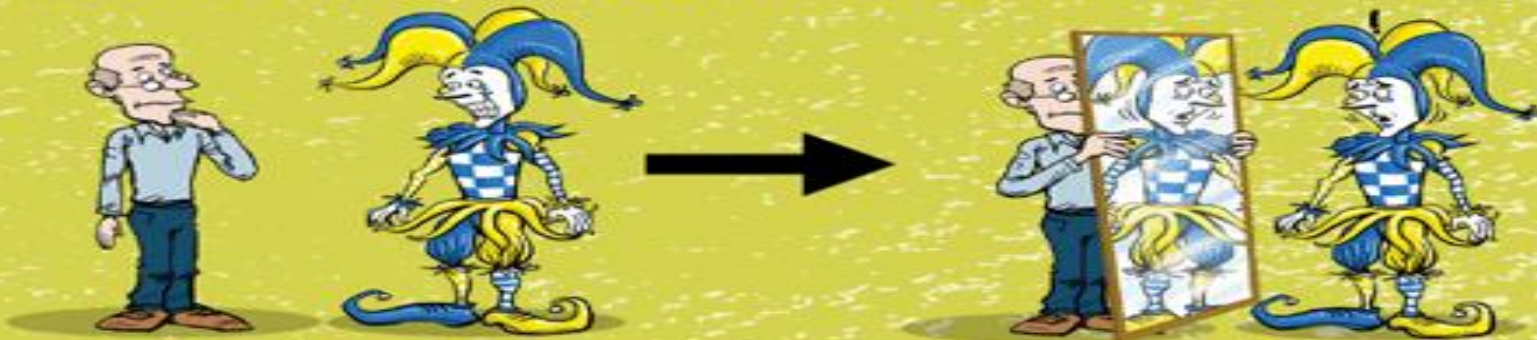
A Fool With a Tool is Still a Fool

DO NOT ANSWER A FOOL ACCORDING TO HIS FOLLY (Prov. 26:4)

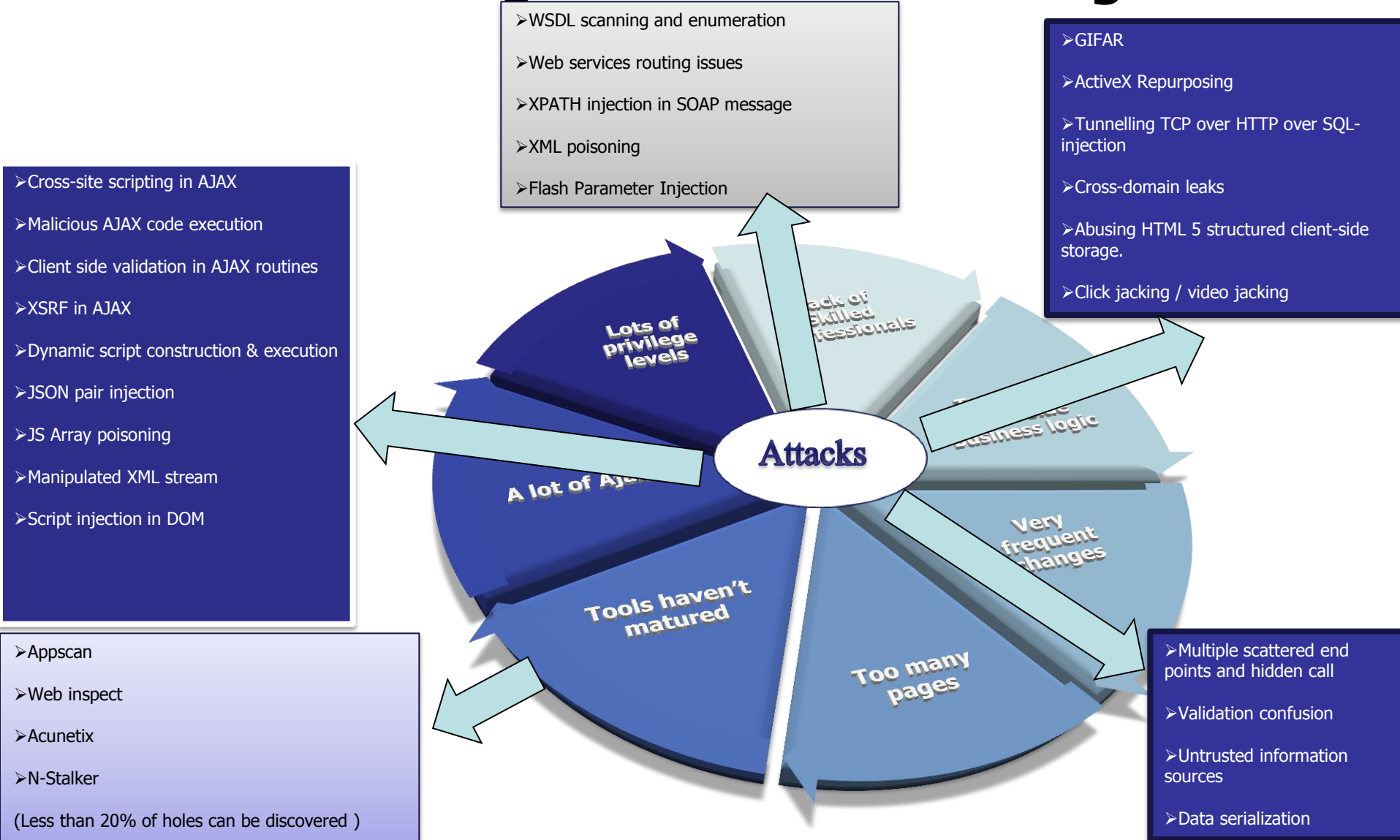


An unbeliever may be highly intelligent, but he has embraced an absurd worldview. He is "foolish" according to Scripture (Proverbs 1:7). We should not embrace his standard or we would be like him. But we should reflect his standard back to him, so that he may see the absurdity.

ANSWER A FOOL ACCORDING TO HIS FOLLY (Prov. 26:5)



Challenges in Web 2.0 Testing



Tester Vs Hacker



- Can only execute scripts which they know about.
- More Dependent on Tools
- Will have a standard testing frame work to test
- Work 5 days a week
- Mentally get disturbed during recession



- Find problems that's never reported by Testers.
- More towards hacking the business logic
- Will have a monetary frame work defined for every test
- Work continuously till they break
- Self-employed

Approach to Address Security Testing Concerns

Discovery

- Understand Business Process
- *Logic discovery*
- Dissecting application
- Enumeration of Services
- Threat Model

Assess

- Multiple scattered end points and hidden calls
- Untrusted information sources
- Data serialization
- Dynamic script construction & execution
- Script injection in DOM
- Cross-domain access and Callback
- Flash-based cross domain access
- Web services routing
- WSDL scanning and enumeration
- Discovering hidden calls
- Business logic flaws

Exploit

- XSS in AJAX
- XML poisoning
- Malicious AJAX code execution
- RSS / Atom injection
- Malicious AJAX code execution
- Client side validation in AJAX routines
- Web services routing issues
- Parameter manipulation with SOAP
- XPATH injection in SOAP message
- Flash Parameter Injection

Report

- Result Reporting
- Business Impact Analysis
- Benchmarking Application against Industry Standard
- Defect Remediation suggestions

Tools

*Httpprint - Web Server Fingerprinting Tool.
Datapipe_http- Raw/HTTP TCP Tunnelling.*

*Ajaxfinger - Ajax Fingerprinting Tool.
Nstools-Security ToolKit from Net-Square.*

Free Tools

Datapipe_http- Raw/HTTP TCP Tunneling .

Msnpawn-application Fingerprinting, Profiling & Assessment tool

*WsChess- Toolkit for Web Services Assessments and Defense.
HP SWF Scanner.*



Conclusion & Questions

Things to Remember

- Perform Threat Modeling
- Spend More time to understand the Business Logic
- Perform an effective manual testing rather than running automated tools
- Don't use a common testing approach
- Update your skills on new technologies

Next ?

