Web 2.0 Testing

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

OWASP
31/07/2010

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

Web 1.0
"the mostly read-only Web"
250,000 sites

Web 2.0
"the wildly read-write Web"
80,000,000 sites

published content
user generated content

45 million global users

1 billion+ global users

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

532 results with live.com
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.
Challenges in Web 2.0 Testing

- Cross-site scripting in AJAX
- Malicious AJAX code execution
- Client side validation in AJAX routines
- XSRF in AJAX
- Dynamic script construction & execution
- JSON pair injection
- JS Array poisoning
- Manipulated XML stream
- Script injection in DOM

- Appscan
- Web inspect
- Acunetix
- N-Stalker

(Less than 20% of holes can be discovered)

- WSDL scanning and enumeration
- Web services routing issues
- XPATH injection in SOAP message
- XML poisoning
- Flash Parameter Injection

- GIFAR
- ActiveX Repurposing
- Tunnelling TCP over HTTP over SQL-injection
- Cross-domain leaks
- Abusing HTML 5 structured client-side storage.
- Click jacking / video jacking

- Multiple scattered end points and hidden call
- Validation confusion
- Untrusted information sources
- Data serialization
Tester Vs Hacker

- Can only execute scripts which they know about.
- More Dependent on Tools
- Will have a standard testing framework 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 framework 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
- Multiple scattered endpoints 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

**Assess**
- 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

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

**Report**
Tools

Free Tools

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

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

Datapipe_http - Raw/HTTP TCP Tunneling.
Msnpawn-application Footprinting, Profiling & Assessment tool

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