LATERAL | SECURITY

Information Security Specialists

OWASP
Testing Web Services

Presenter: Nick von Dadelszen
Date: 13th July 2009
Company: Lateral Security (IT) Services Limited

LATERAL | SECURITY

Company Overview

- Company
  - Lateral Security (IT) Services Limited
  - Founded in April 2008, HQ in Woodward Street, Wellington
  - Directors, Nick von Dadelszen and Ratu Mason
- Services
  - Information security testing (design, architecture, penetration testing, security controls, policy and compliance)
  - Lifecycle auditing (design, pre prod, post prod)
  - Regular ongoing testing programs
- Differentiators
  - True vendor independence
  - Security testing is our unique specialty
  - Very highly skilled staff

LATERAL | SECURITY

Agenda

- Why Web Services testing is important
- How To Test Web Services
  - Information Gathering
  - Service Testing
- Common Web Services Issues
- Useful Tools
- Tips and tricks
- WS-Security

LATERAL | SECURITY

Why WS Testing Is Important

- Web services and SOAP-based apps are getting more and more common
- Only data is passed through web services so more reliance on client for processing
- Number one rule of application security is:

DO NOT TRUST THE CLIENT

LATERAL | SECURITY

WS Testing versus Standard App Testing

- Many common areas:
  - Authentication
  - Session management
  - Data validation
  - Business logic
  - Information disclosure
- Some unique areas:
  - XML parser issues
  - XML content issues
- More focus required on level of client trust

LATERAL | SECURITY

How To Test Web Services

- Standard testing approach
  - Information gathering
    - Service discovery
    - Method discovery
  - Service testing
    - Standard web application tests
    - Web Services specific tests

LATERAL | SECURITY

Web Services Discovery

- Search engines
  - inurl:WSDL inurl:/ws inurl:/axis/services
  - filetype:asmx filetype:jws
  - Always interesting to search for terms like Admin and StopService
- Site crawling
- Behaviour investigation
  - Intercept the client to observe standard behaviour
  - If the client is a thick application you may need some trickery to do this (SSL certs, WM networks, reverse proxies)

LATERAL | SECURITY

Google Search For Web Services

Google

inurl:.asmx site:.nz

Search

Advanced Search
Preferences

Search: the web pages from New Zealand

Web Show options... Results **1** - **10** of about **1,130** for **inurl:.asmx site:.nz**. (**0.25** seconds)

CoreServices Web Service
CoreServices. The following operations are supported. For a formal definition, please review the Service Description. **...**
youtxt.co.nz/CoreServices.**asmx** - Cached - Similar

WidgetWebService Web Service
SOAP 1.1. The following is a sample SOAP 1.1 request and response. The placeholders shown need to be replaced with actual values. **...**
www.hito.org.nz/WidgetWebService.**asmx**?op... - Cached - Similar

CustomerEstimateService Web Service
SOAP 1.1. The following is a sample SOAP 1.1 request and response. The placeholders shown need to be replaced with actual values. **...**
https://secure.mainfreight.co.nz/.../CustomerEstimateService.**asmx**?... - Cached - Similar

cManagerService Web Service
cManagerService. Click here for a complete list of operations. GetPageByUrl. Test. To test the operation using the HTTP POST protocol, click the 'Invoke' **...**
www.formway.co.nz/cManagerService.**asmx**?op... - Cached - Similar

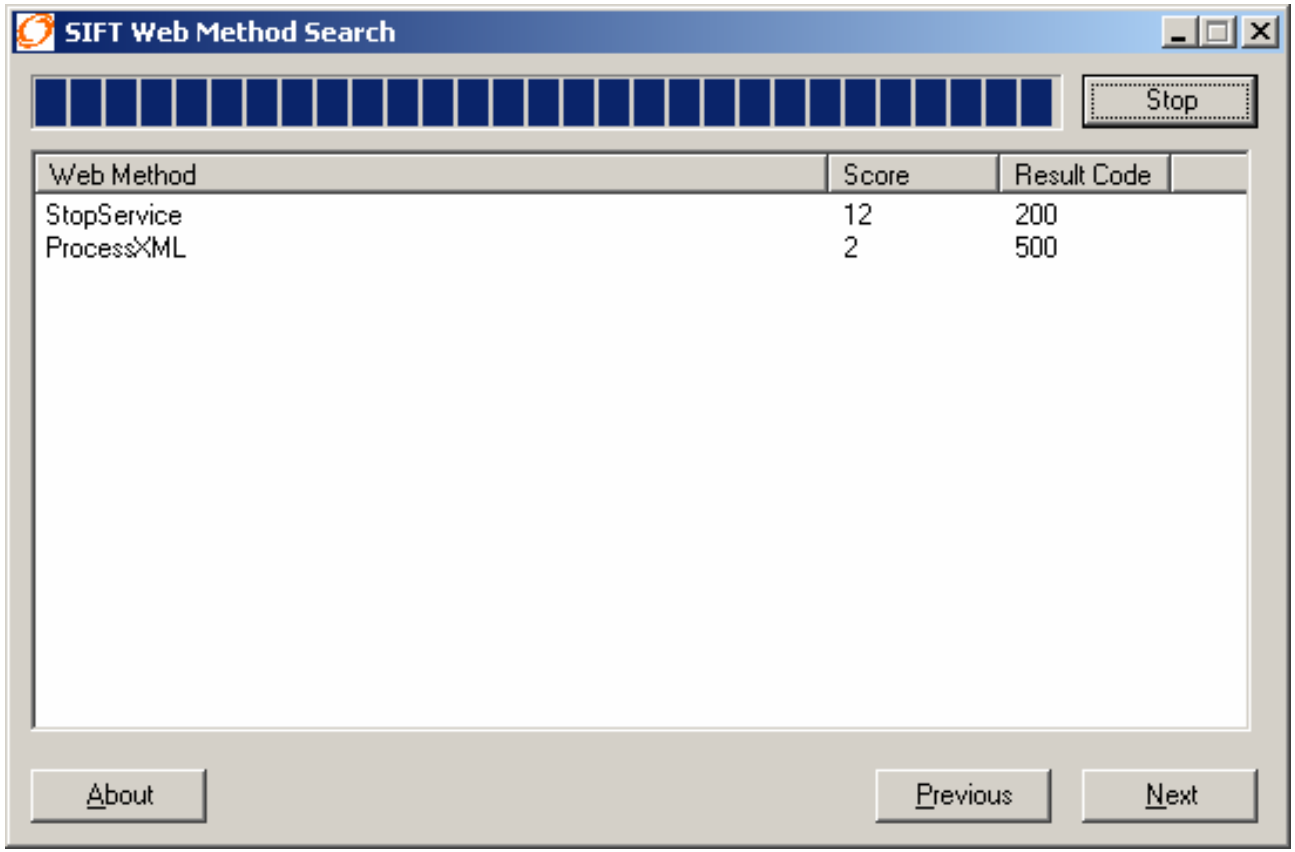
LATERAL | SECURITY

Method Discovery

- To discover available methods:
  - WSDL interrogation
  - Behaviour investigation
  - Method brute forcing
- Potential Issue - Insecure method leakage
  - WSDL containing methods that shouldn't be public
  - Private method brute-forcing
- Tool
  - SIFT Web Method Search

LATERAL | SECURITY

Demo – Web Method Discovery



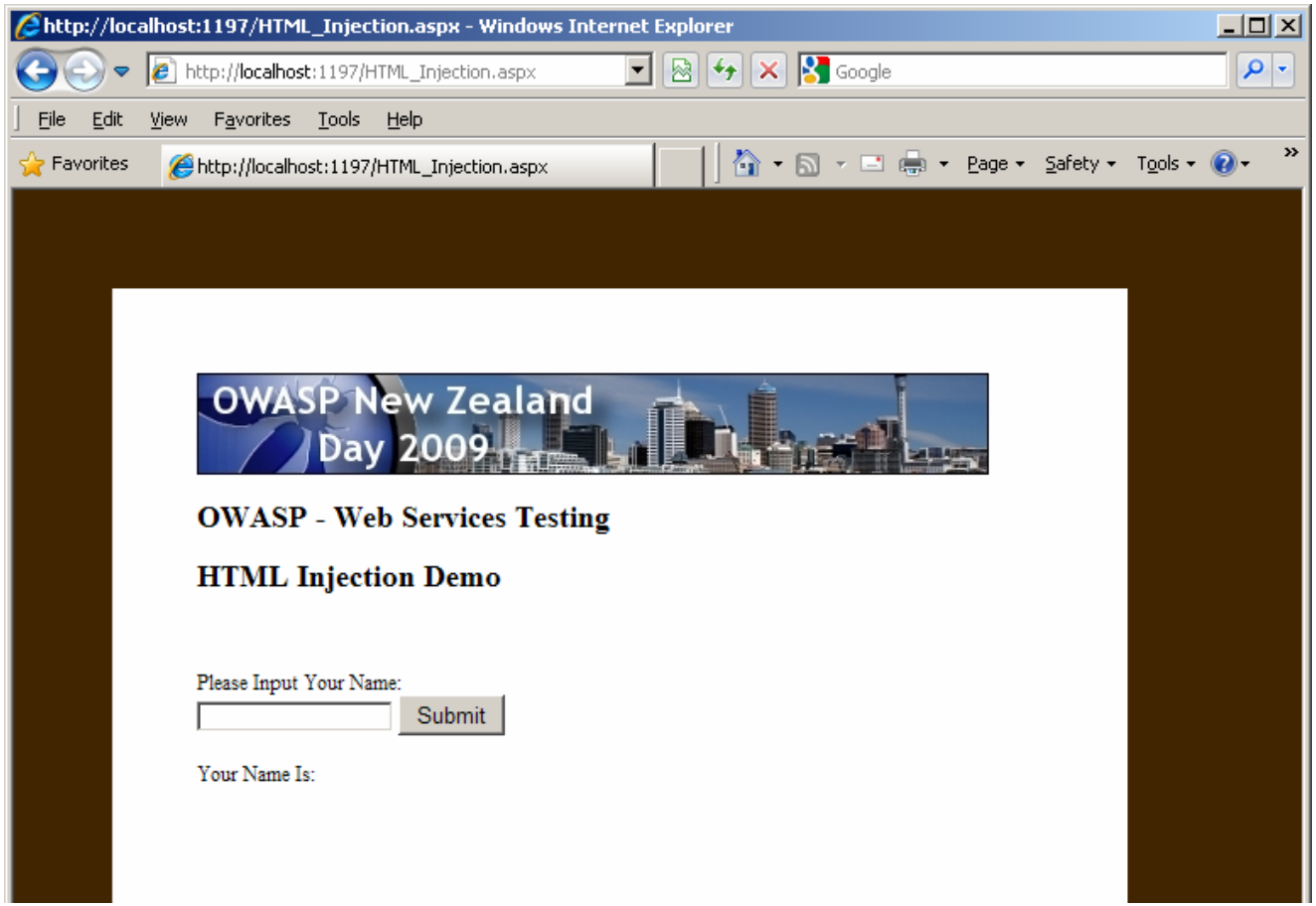
LATERAL | SECURITY

Web Services Mapped To OWASP Top Ten

- A1 – Cross site scripting (XSS)
  - XSS attacks can be propagated through web services
  - Depends on the consuming application
  - If the application parses HTML then this can be an issue
- A2 – Injection flaws
  - All still possible:
    - SQL, XPATH, XML, LDAP
  - Depends on how the web service uses input

LATERAL | SECURITY

Demo – HTML Injection



LATERAL SECURITY

Top Ten Continued

- A3 – Malicious file execution
  - Again depends on how the web service uses input
  - Some web services allow attachments
- A4 – Insecure direct object reference
  - Still an issue based on web service logic
- A5 – Cross site request forgery (CSRF)
  - More of an issue with AJAX than traditional web services, but SOAP can be called from a browser (JavaScript SOAP client)

LATERAL | SECURITY

Top Ten Continued

- A6 – Information leakage and improper error handling
  - Common problem with web services, errors often leak information
- A7 – Broken authentication and session management
  - Sensitive methods can be exposed without authentication
  - Other standard authentication issues apply (ability to brute force etc)
  - If session management is used, same issues apply

LATERAL | SECURITY

Top Ten Continued

- A8 – Insecure cryptographic storage
  - Still an issue based on web service logic
- A9 – Insecure communications
  - The use of SSL and its proper configuration is important for Web Services
- A10 – Failure to restrict URL access
  - Restricting access to Web Service URLs to only authorised consumers is an issue

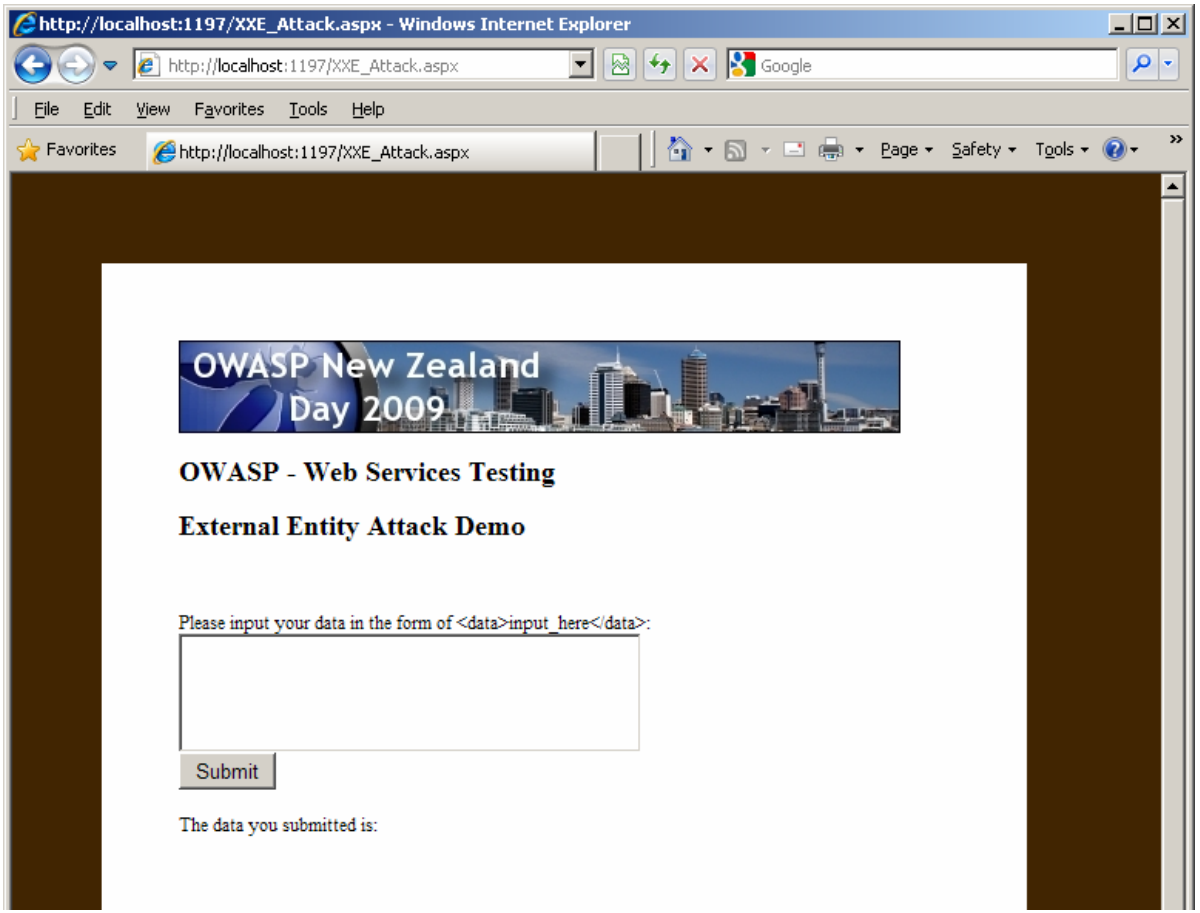
LATERAL | SECURITY

Web Service Specific Tests

- XML Issues
  - External entity issues
  - Malformed XML
  - Recursive XML
  - XML Entity Expansion
  - XML Attribute Blowup
  - Overlarge XML
  - CDATA injection
- WS-Routing issues

LATERAL | SECURITY

Demo – XXE Attack



LATERAL | SECURITY

XML Entity Expansion

```
<?xml version="1.0"?>
<!DOCTYPE root [
<!ENTITY ha "Ha !">
<!ENTITY ha2 "&ha; &ha;">
<!ENTITY ha3 "&ha2; &ha2;">
<!ENTITY ha4 "&ha3; &ha3;">
<!ENTITY ha5 "&ha4; &ha4;">
...
<!ENTITY ha128 "&ha127; &ha127;">
]>
<root>&ha128;</root>
```

LATERAL | SECURITY

Common WS Issues Found

- Insecure functionality leaked through WSDL
- XML Parser Issues
  - XXE
  - Recursive and overlarge payloads
- XML/Xpath injection
- Information disclosure through error messages

- Too much trust of client side application

LATERAL | SECURITY

Useful Tools

- Useful tools for testing web services are:
  - WebScarab (of course)
  - Foundstone WSDigger
  - SIFT Web Method Search
  - Firebug browser plugin (for AJAX testing)
  - PocketSOAP
  - SoapUI
  - Your favourite scripting language

LATERAL | SECURITY

Tips and Tricks

- Always search the WSDL for unused functions
- Look very closely at reliance on client for security and business logic
- HTML gets encoded when placed into XML so by pre-encoding you may be able to circumvent validation
- ASP.Net Web Services do not get automatically validated
- Watch for custom-built XML or JSON

LATERAL | SECURITY

But What About WS-Security?

- WS-Security provides integrity and confidentiality for SOAP messages (through encryption and mac-ing)
- Just like SSL on a standard web application, it doesn't stop most attacks
- If I can legitimately consume a Web Service, I can legitimately attack one too

LATERAL | SECURITY

Contact Details

Thank you

Lateral Security (IT) Services Limited
2 Woodward Street (level 5)
PO Box 11785, Wellington 6011, New Zealand

Phone: +64 4 4999756
Presenter: nick@lateralsecurity.com
Web: www.lateralsecurity.com

LATERAL | SECURITY