ZAPping your Applications

OWASP
The Open Web Application Security Project

Aaron Guzman
ZAP Evangelist
Aaron.guzman@owasp.org

OWASP
The Open Web Application Security Project

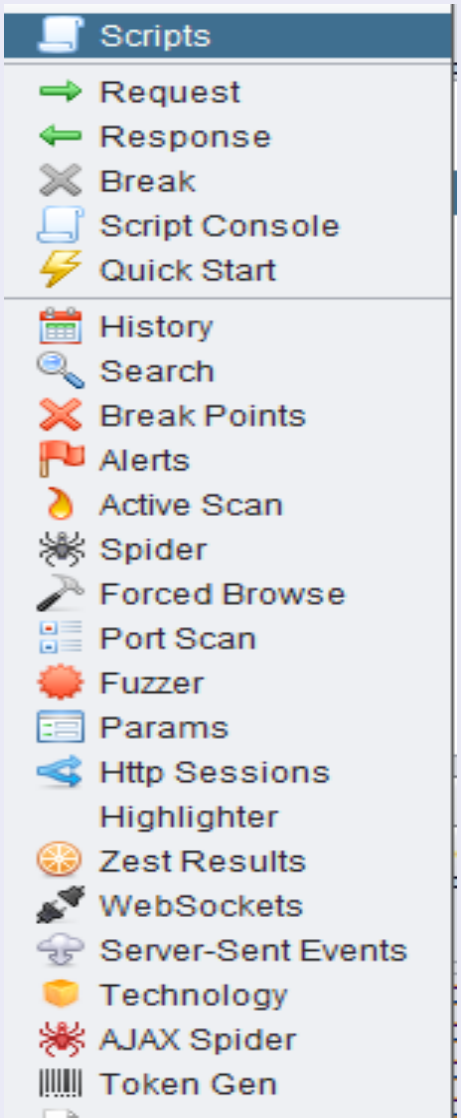
Me?

- ✓ Born and Raised in Cali
- ✓ Pizza<3
- ✓ CSA Board, OWASP, HTCIA 1st VP
- ✓ Motivated with tons of goals to complete
- ✓ Some people say I'm paranoid, I just say I enjoy my privacy :)
- ✓ I ~~ride~~ rode a motorcycle(Fri 13th)

OWASP
The Open Web Application Security Project

What is ZAP?

- ✓ Web App Testing Tool
- ✓ Forked off of older OWASP tools such as Dirbuster and Paros Proxy
- ✓ Can test apps actively or passively
- ✓ Active community
- ✓ Known for its ease of use
- ✓ Open source and Free
- ✓ Cross Platform
- ✓ Lots of features



Everyone loves Features

- ✓Plug-n-hack
- ✓Quick Start
- ✓Custom Fuzzing
- ✓Active scanning
- ✓Custom bruteforcing
- ✓Passively scan
- ✓Specify Modes
- ✓Spidering
- ✓Login/Logout Params
- ✓Ajax Spidering
- ✓Daemon Mode
- ✓Break Points
- ✓API Available
- ✓Scripting

Stay Tuned...more to come!

OWASP
The Open Web Application Security Project

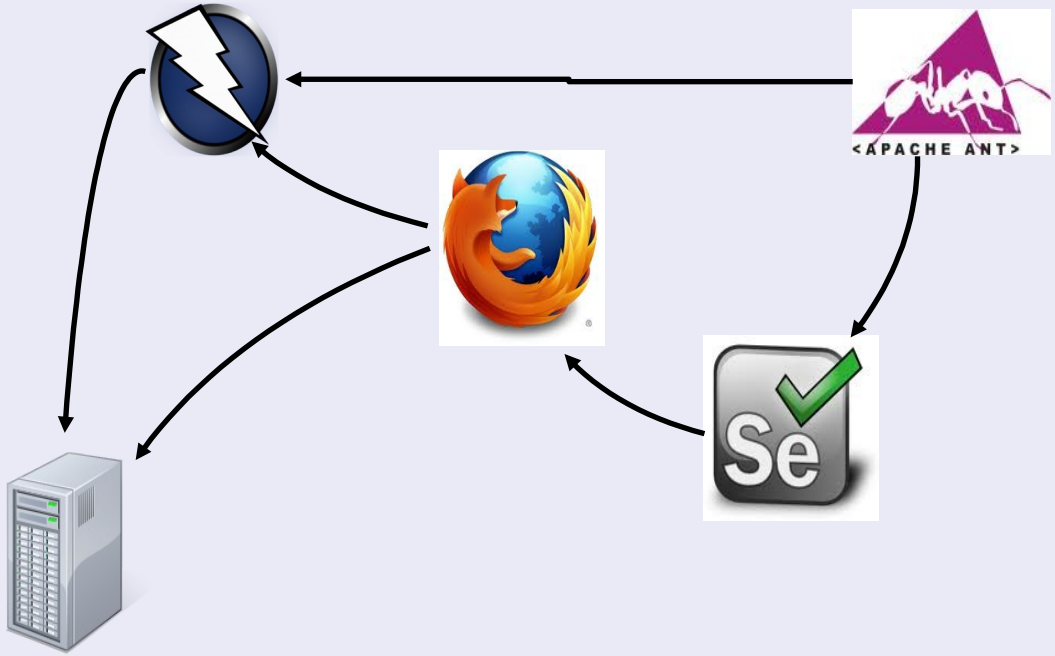
Demo Time

OWASP
The Open Web Application Security Project

Regression Testing

- Using Zest
- Plug-n-Hack record option
- Using Selenium w/Ant Build Server
- Helps the Security Guy show Devs what exactly was done to find the vulnerability

Security Regression Testing



http://code.google.com/p/zaproxy/wiki/SecRegTests

OWASP
The Open Web Application Security Project

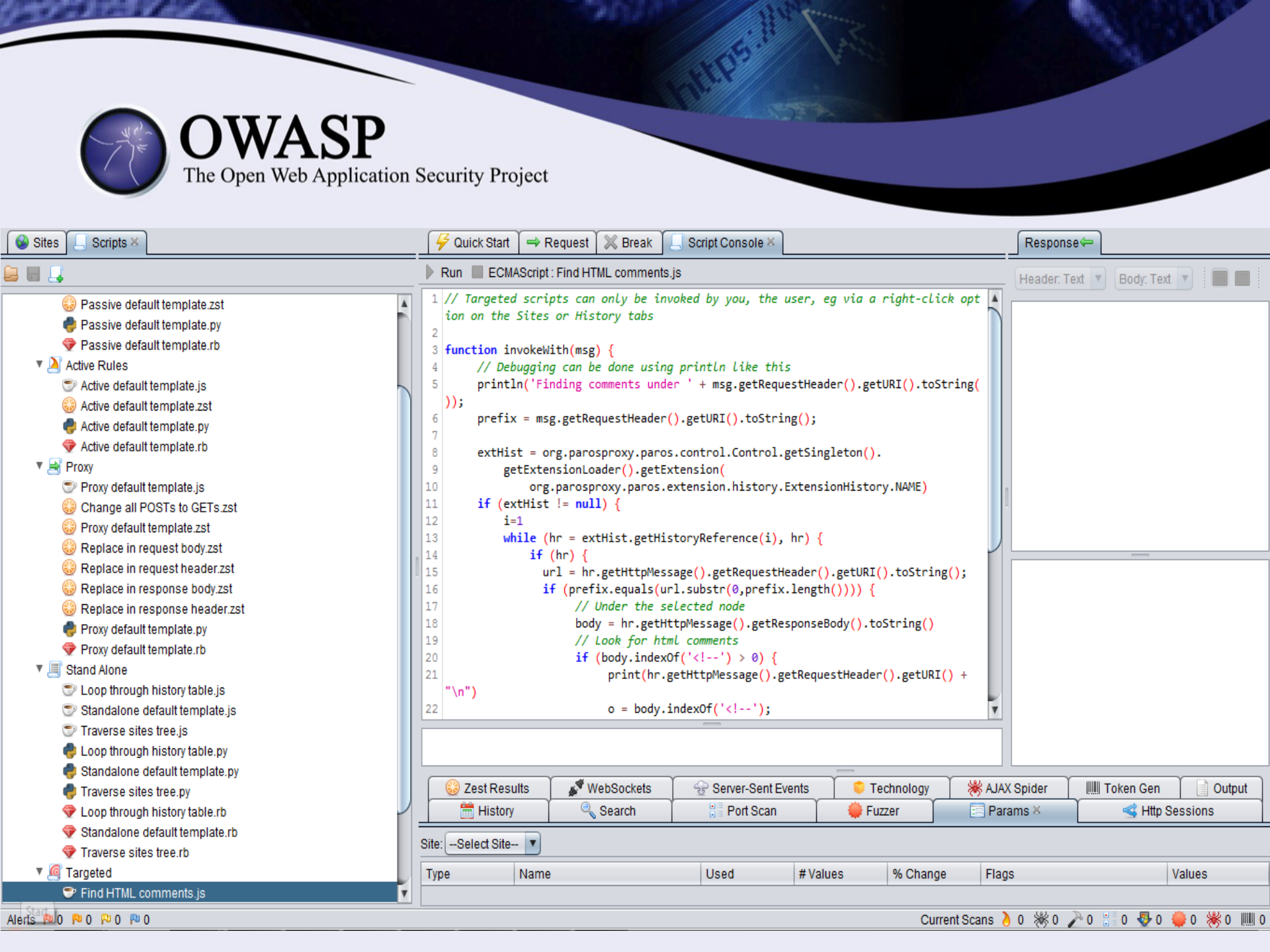
Zest Scripts

- Built in, same script types
- Graphical way to write scripts
- Right click everywhere!
- Effectively ZAP's macro language
- Implement JSR 223
- https://developer.mozilla.org/en-US/docs/zest

OWASP
The Open Web Application Security Project

Automation

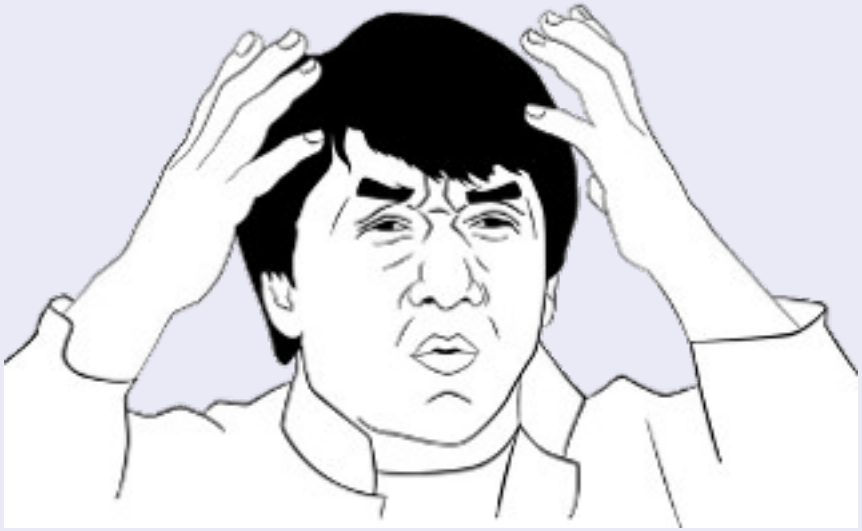
- Using Zest, Python, Ruby, JavaScript in Scripts tab (script generation add-on)
- Templates Available
- Using daemon mode
- Threadfix (Denim Group) tasker to automate scans
- Great for QA teams


OWASP
The Open Web Application Security Project
Sites
Scripts
Passive default template.zst
Passive default template.py
Passive default template.rb
Active Rules
Active default template.js
Active default template.zst
Active default template.py
Active default template.rb
Proxy
Proxy default template.js
Change all POSTs to GETs.zst
Proxy default template.zst
Replace in request body.zst
Replace in request header.zst
Replace in response body.zst
Replace in response header.zst
Proxy default template.py
Proxy default template.rb
Stand Alone
Loop through history table.js
Standalone default template.js
Traverse sites tree.js
Loop through history table.py
Standalone default template.py
Traverse sites tree.py
Loop through history table.rb
Standalone default template.rb
Traverse sites tree.rb
Targeted
Find HTML comments.js
Quick Start
Request
Break
Script Console
Response
Run
ECMAScript : Find HTML comments.js
Header: Text
Body: Text
1 // Targeted scripts can only be invoked by you, the user, eg via a right-click option on the Sites or History tabs
2
3 function invokeWith(msg) {
4 // Debugging can be done using println like this
5 println('Finding comments under ' + msg.getRequestHeader().getURI().toString());
6 prefix = msg.getRequestHeader().getURI().toString();
7
8 extHist = org.parosproxy.paros.control.Control.getSingleton().
9 getExtensionLoader().getExtension(
10 org.parosproxy.paros.extension.history.ExtensionHistory.NAME)
11 if (extHist != null) {
12 i=1
13 while (hr = extHist.getHistoryReference(i), hr) {
14 if (hr) {
15 url = hr.getHttpMessage().getRequestHeader().getURI().toString();
16 if (prefix.equals(url.substr(0,prefix.length()))) {
17 // Under the selected node
18 body = hr.getHttpMessage().getResponseBody().toString()
19 // Look for html comments
20 if (body.indexOf('<!--') > 0) {
21 print(hr.getHttpMessage().getRequestHeader().getURI() + "\n")
22 o = body.indexOf('<!--');
Zest Results
WebSockets
Server-Sent Events
Technology
AJAX Spider
Token Gen
Output
History
Search
Port Scan
Fuzzer
Params
Http Sessions
Site: --Select Site--
Type
Name
Used
Values
% Change
Flags
Values
Alerts
Current Scans

OWASP
The Open Web Application Security Project

Active Community

- https://groups.google.com/forum/#!forum/zaproxy-users
- https://groups.google.com/forum/#!forum/zaproxy-develop
- http://code.google.com/p/zaproxy/wiki/ZapEvangelists
- http://sourceforge.net/projects/zaproxy/files/weekly/



Why wouldn't you want to use ZAP??

OWASP
The Open Web Application Security Project

Questions?

Aaron.guzman@owasp.org

http://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project