Systematic Techniques to Find Problems Fast
Web Security Testing Cookbook
O'REILLY
Paco Hope & Ben Walther

Cooking with OWASP

Paco Hope
Technical Manager
Cigital, Inc.
<paco@cigital.com>

cigital

cigital
Software Confidence. Achieved.

Agenda

- Background / Motivation
- CAL9000
- WebScarab
- wsFuzzer

Motivation

“Phenomenal cosmic
POWER!
…itty bitty living space”

Attributes of OWASP Projects

Benefits	Limits
• Free • Open source • Minimal prerequisites • Minimal privileges • Mostly active	• Limited by OWASP attention span / enthusiasm • Might not apply to your needs • Experience the "Linux effect"

CAL9000

cigital
Software Confidence. Achieved.

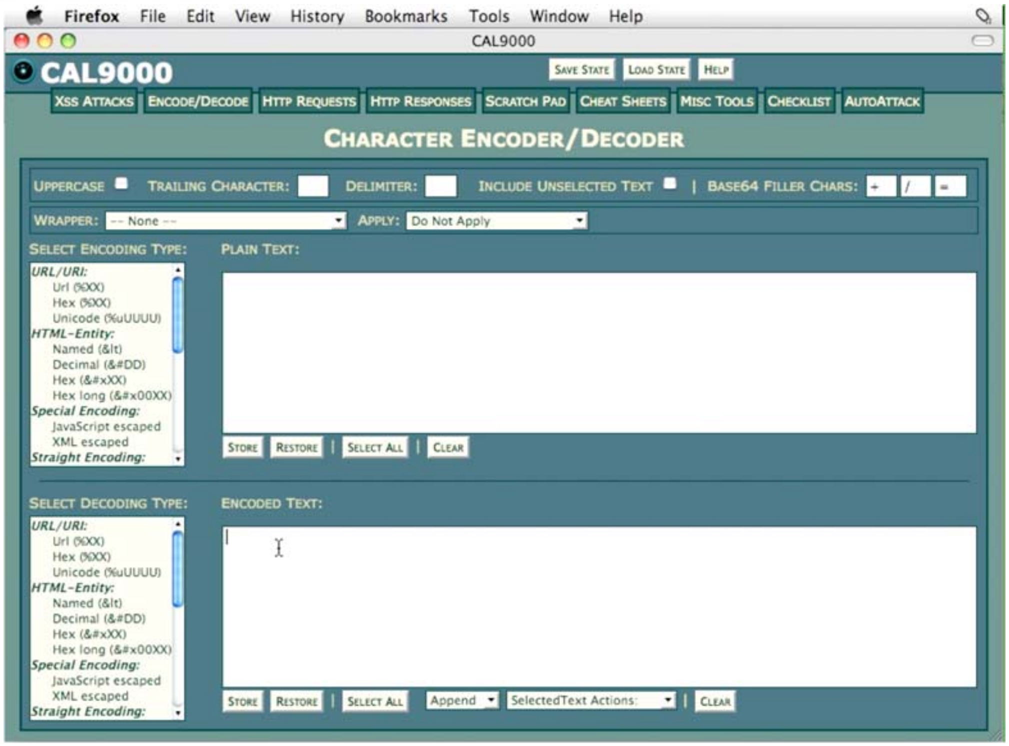
CAL9000

- Swiss Army Knife
- Encode
- Decode
- Hashes, etc.

- Just an HTML page and a bunch of JavaScript
- No installation
- No permissions
- Stick it on a thumb drive

cigital
Software Confidence. Achieved.

In Action



Base64 Filler Chars: + / =

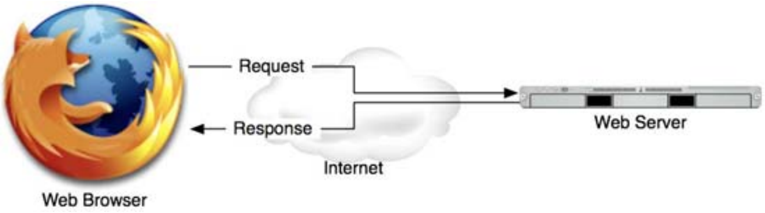
Wrapper: -- None --

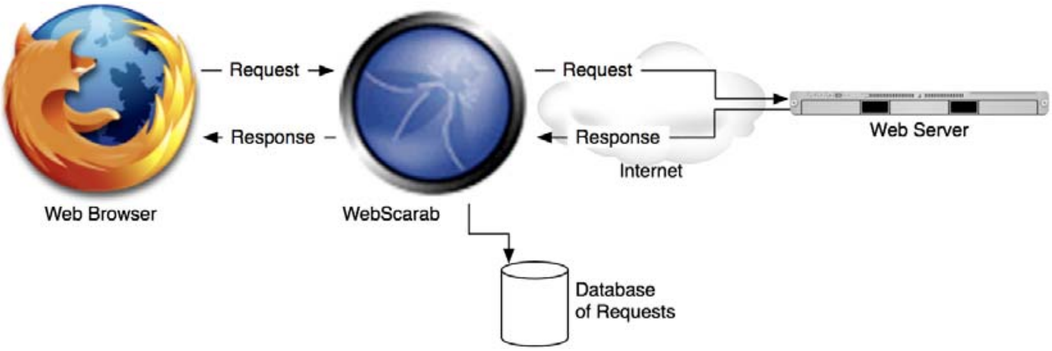
Apply: Do Not Apply

WebScarab

WebScarab

- Proxy
- Intercept requests
- Originate requests
- Session ID Analysis

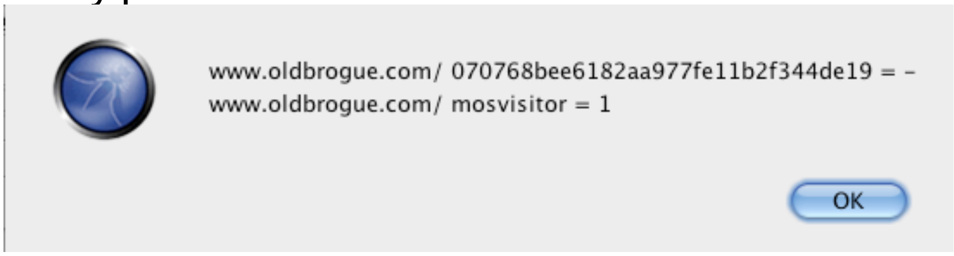




Session ID Analysis

- Fetch lots and lots of cookies
- Figure out where the Session IDs are
- Plot the values against time
- See any patterns?

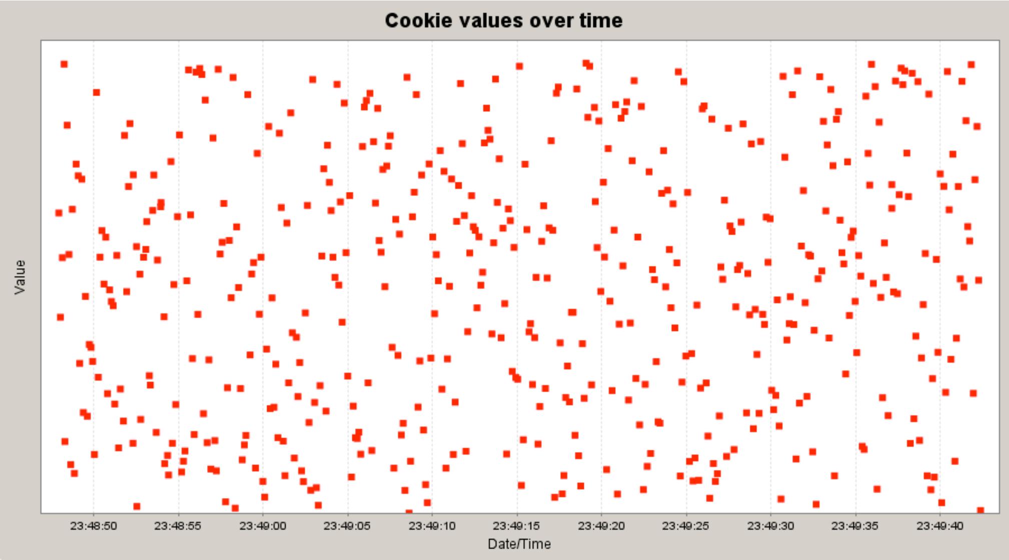
- Why does it matter?
- If I can guess / compute your session ID, I don't have to steal it
- I become YOU



```
www.oldbrogue.com/ 070768bee6182aa977fe11b2f344de19 = -
www.oldbrogue.com/ mosvisitor = 1
```

cigital
Software Confidence. Achieved.

Session ID Checking



wsFuzzer

Fuzz Testing Web Services

Fuzz Testing

- Random / semi-random permutations of input
- Great for APIs, structured documents, state machines, protocols
- Many free and commercial tools
- Important for future testing

wsFuzzer

Negatives

- Python based (complex prerequisite)
- Chatty (asks a bunch of questions)
- Interactive (not batched)
- Produces tons of false positives and undecided results

Positives

- Always finds something interesting
- Gives you a complete forensic record for reproduction and root-cause analysis
- Creates thousands of test cases that you wouldn't

In Action:

Config:

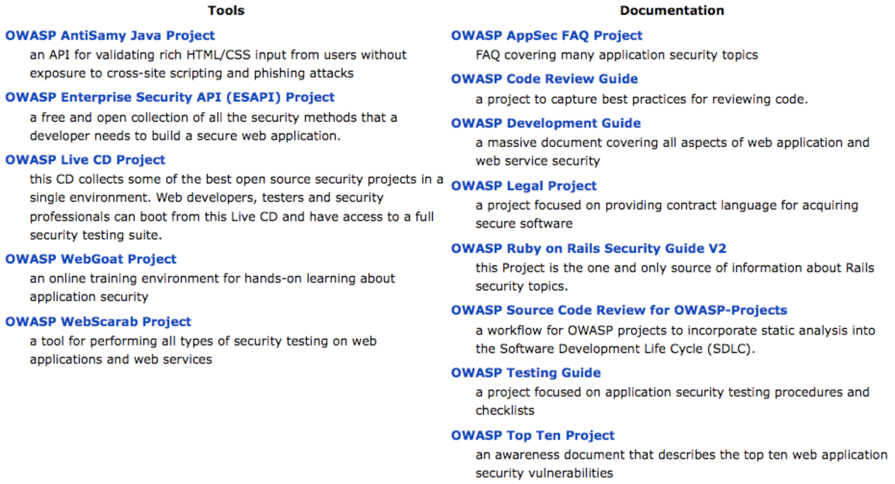
```
Mode = 3
dictionary = small.txt
host = bds.dev1.com:80
automate = yes
idsevasion = no
uri = /WebServiceBDS/
  DataService.asmx
simultaneous = yes
```

After Running

```
*** Outgoing HTTP headers **********************************************
POST /WebServiceBDS/DataService.asmx HTTP/1.1
Host: bds.dev1.com:80
User-Agent: WSFuzzer-1.9.2.1
Content-type: text/xml; charset="UTF-8"
Content-length: 1418
SOAPAction: "http://example.com/InsertBranchRecord"
*** Outgoing SOAP ******************************************
<?xml version="1.0" ?>
<soap:Body>
<InsertBranchRecord xmlns="http://example.com/">
<ParentBrokerID>1</ParentBrokerID>
<CompanyName>1</CompanyName>
<BusinessFormID>1</BusinessFormID>
<TaxID_SSN>1</TaxID_SSN>
</InsertBranchRecord>
</soap:Body>
</soap:Envelope>
*** Incoming HTTP headers ***********************************
HTTP/1.1 200 OK
Date: Tue, 24 Jun 2008 07:43:54 GMT
Server: Microsoft-IIS/6.0
MicrosoftOfficeWebServer: 5.0_Pub
Content-Type: text/xml; charset=utf-8
Content-Length: 1823
*** Incoming SOAP *******************************************
<?xml version="1.0" encoding="utf-8"?>
<soap:Body>
<InsertBranchRecordResponse xmlns="http://example.com/">
<InsertBranchRecordResult>
<resultcode>90080</resultcode>
<error>No Errors. Broker created successfully.</error>
</Results>
</TypedResultsDataSet>
</InsertBranchRecordResult>
</InsertBranchRecordResponse>
</soap:Body></soap:Envelope>
```

Closing Thoughts

- Security people don't think like testers
- Explore all the different options at owasp.org



Tools

OWASP AntiSamy Java Project
an API for validating rich HTML/CSS input from users without exposure to cross-site scripting and phishing attacks

OWASP Enterprise Security API (ESAPI) Project
a free and open collection of all the security methods that a developer needs to build a secure web application.

OWASP Live CD Project
this CD collects some of the best open source security projects in a single environment. Web developers, testers and security professionals can boot from this Live CD and have access to a full security testing suite.

OWASP WebGoat Project
an online training environment for hands-on learning about application security

OWASP WebScarab Project
a tool for performing all types of security testing on web applications and web services

Documentation

OWASP AppSec FAQ Project
FAQ covering many application security topics

OWASP Code Review Guide
a project to capture best practices for reviewing code.

OWASP Development Guide
a massive document covering all aspects of web application and web service security

OWASP Legal Project
a project focused on providing contract language for acquiring secure software

OWASP Ruby on Rails Security Guide V2
this Project is the one and only source of information about Rails security topics.

OWASP Source Code Review for OWASP-Projects
a workflow for OWASP projects to incorporate static analysis into the Software Development Life Cycle (SDLC).

OWASP Testing Guide
a project focused on application security testing procedures and checklists

OWASP Top Ten Project
an awareness document that describes the top ten web application security vulnerabilities