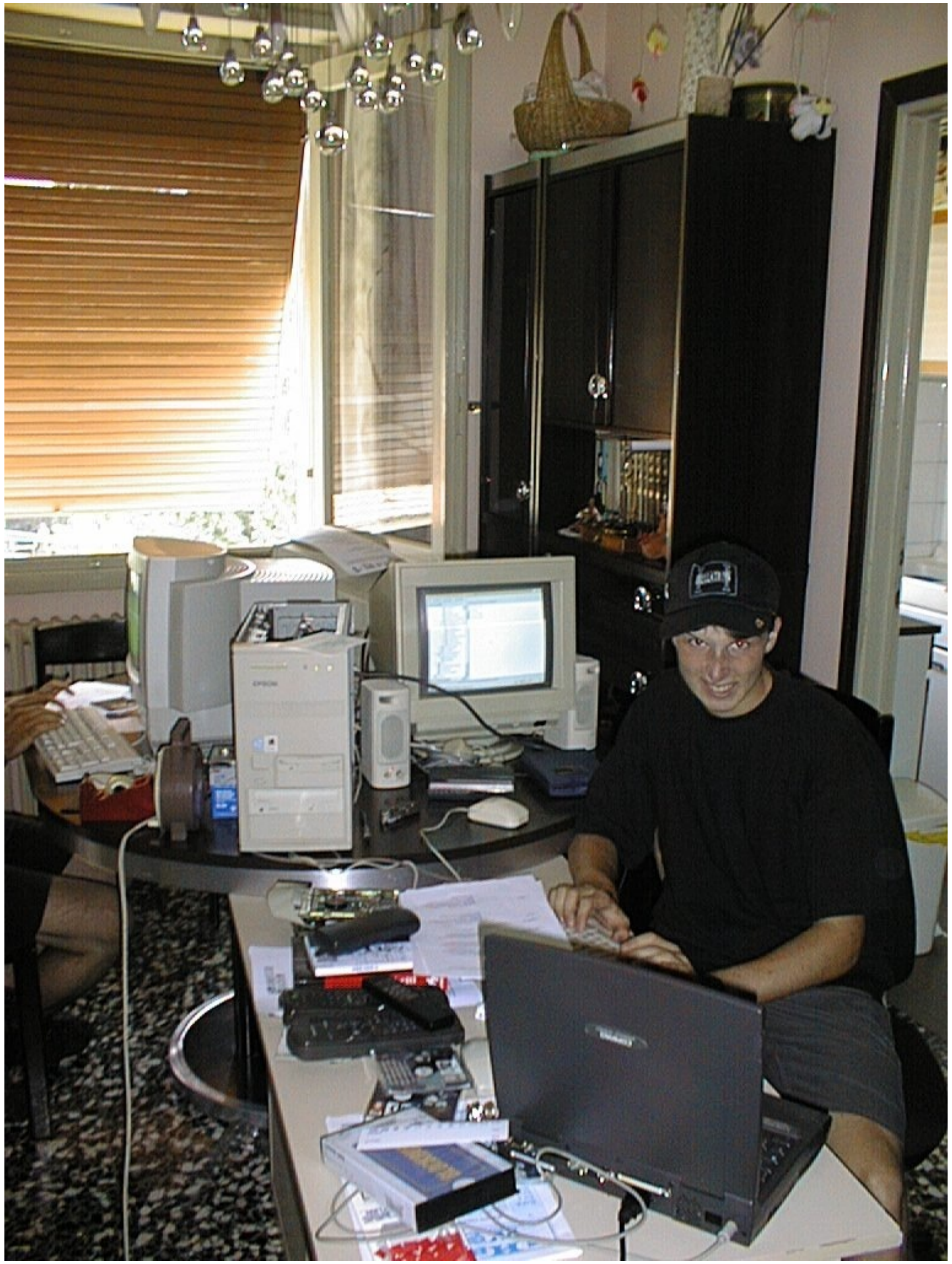
Leverage OpenSource to improve your security

luca@addepar.com

@_ikki

About Me - Past Life



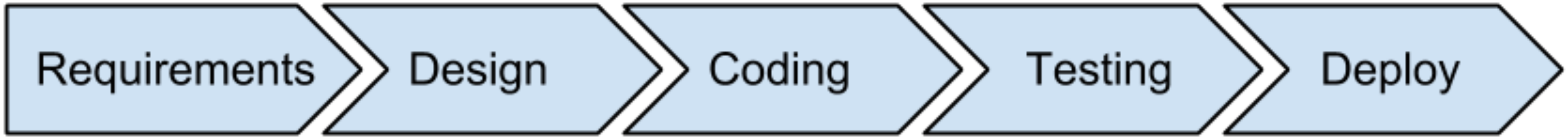
About Me - Now

organizations
considered
result
models
peer
widely
available
fields
making
various
use
Open
software
different
approach
variety
methods
customers
agendas
code
approaches
technology
Source
consider
authors
definition
applied
strategic
writing
released
share
online
view
communication
development
changes
principles
marketing
internet
distribution
public
free
term
centralized
content
determite
based
design
critical
describe
access
pricing
user
written
culture
www

open source

closed source

SDLC



Requirements

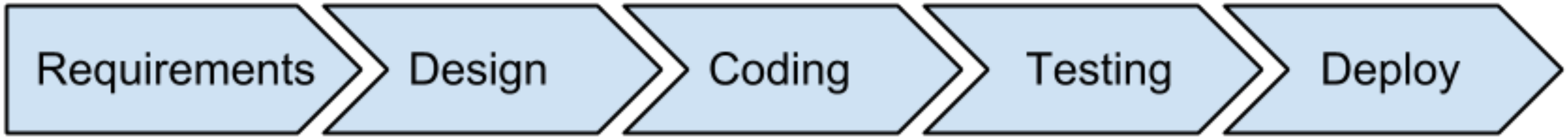
Design

Coding

Testing

Deploy

Secure SDLC

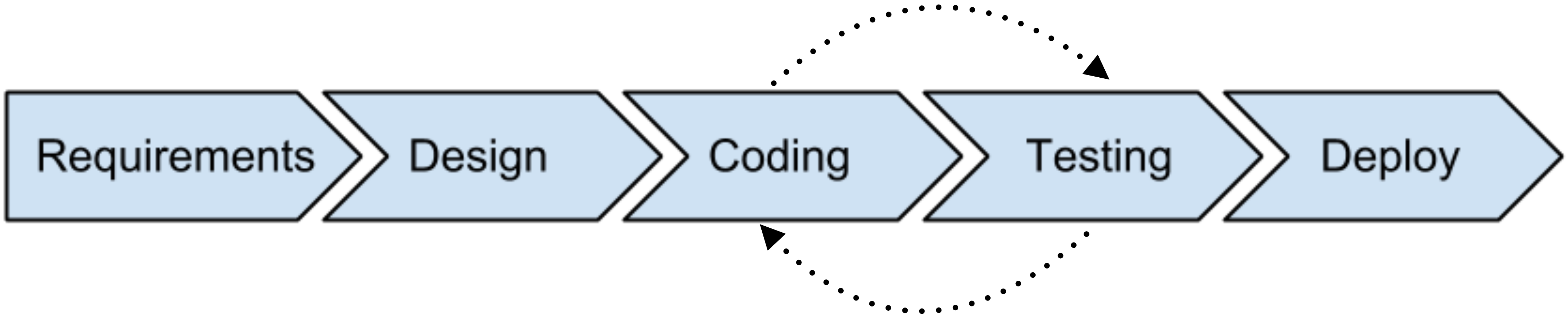


Requirements
Design
Coding
Testing
Deploy

- Security requirements
- Design reviews
- Training
- Risk assessments
- Attack surface reduction
- …

Phase 1

Secure SDLC



Requirements

Design

Coding

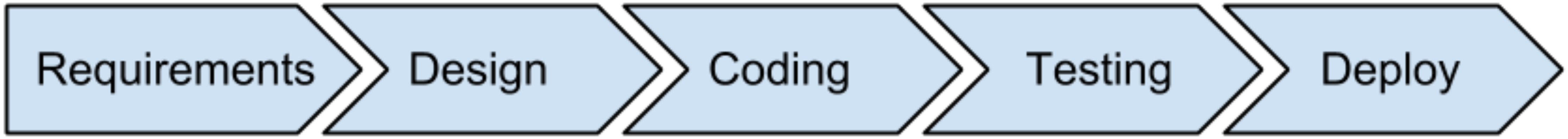
Testing

Deploy

- Secure Coding
- Dynamic Testing
- Static Analysis
- …

Phase 2

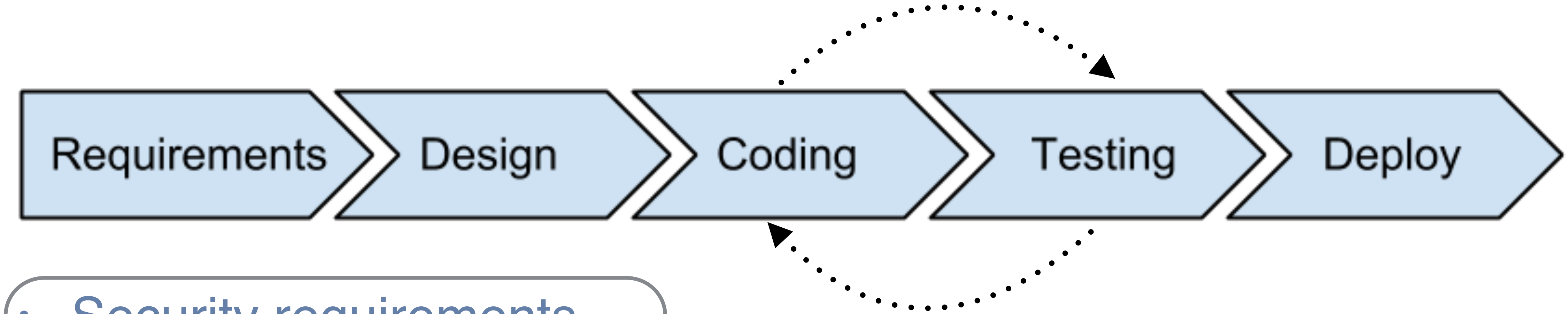
Secure SDLC



- Monitoring
- Audit trails
- …

Phase 3

Secure SDLC



Requirements

Design

Coding

Testing

Deploy

- Security requirements
- Design reviews
- Training
- Risk assessments
- Attack surface reduction
- …

Phase 1

- Secure Coding
- Dynamic Testing
- Static Analysis
- …

Phase 2

- Monitoring
- Audit trails
- …

Phase 3

Requirements, Design

Phase 1

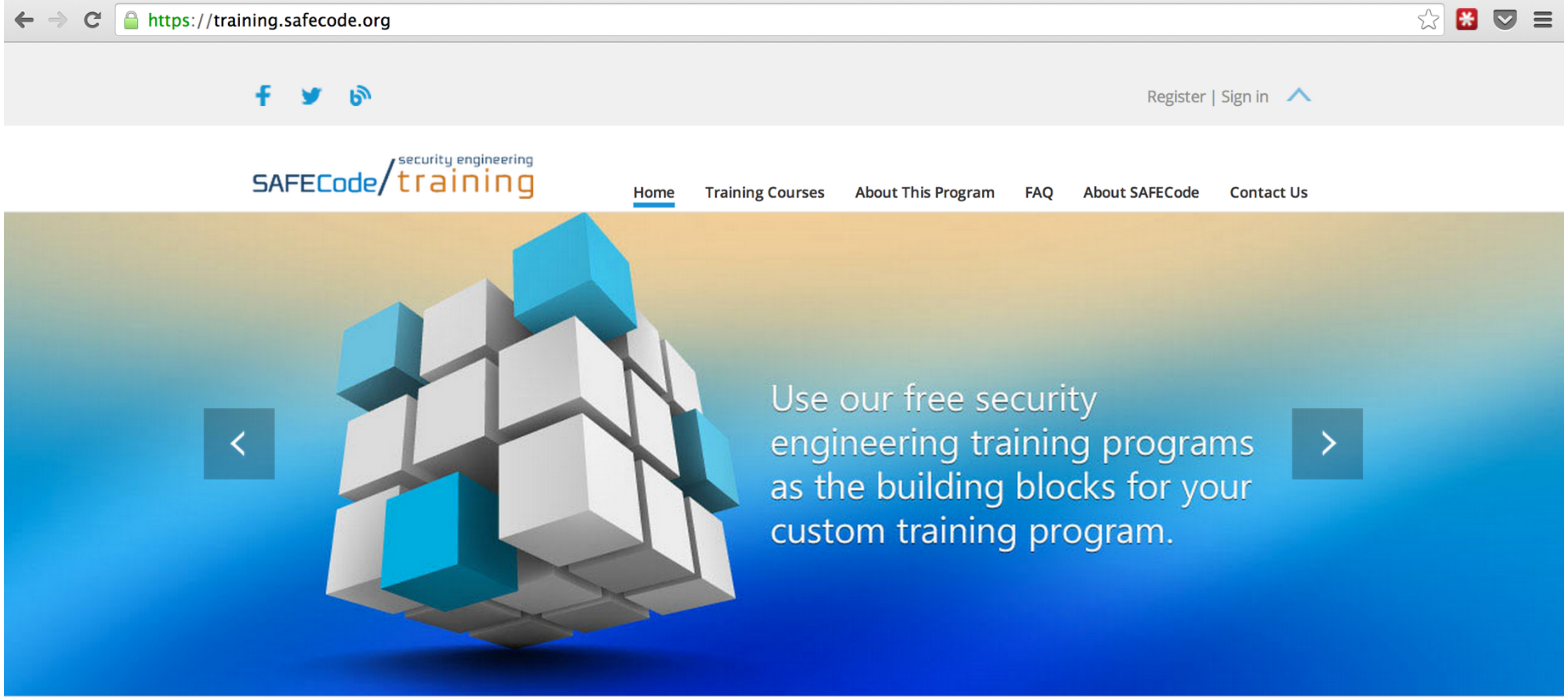
Training

“The foundation of secure software is writing secure code”
https://training.safecode.org/

- Traditional training
- Deliberately insecure applications
- CTF challenges

SAFECode - https://training.safecode.org/

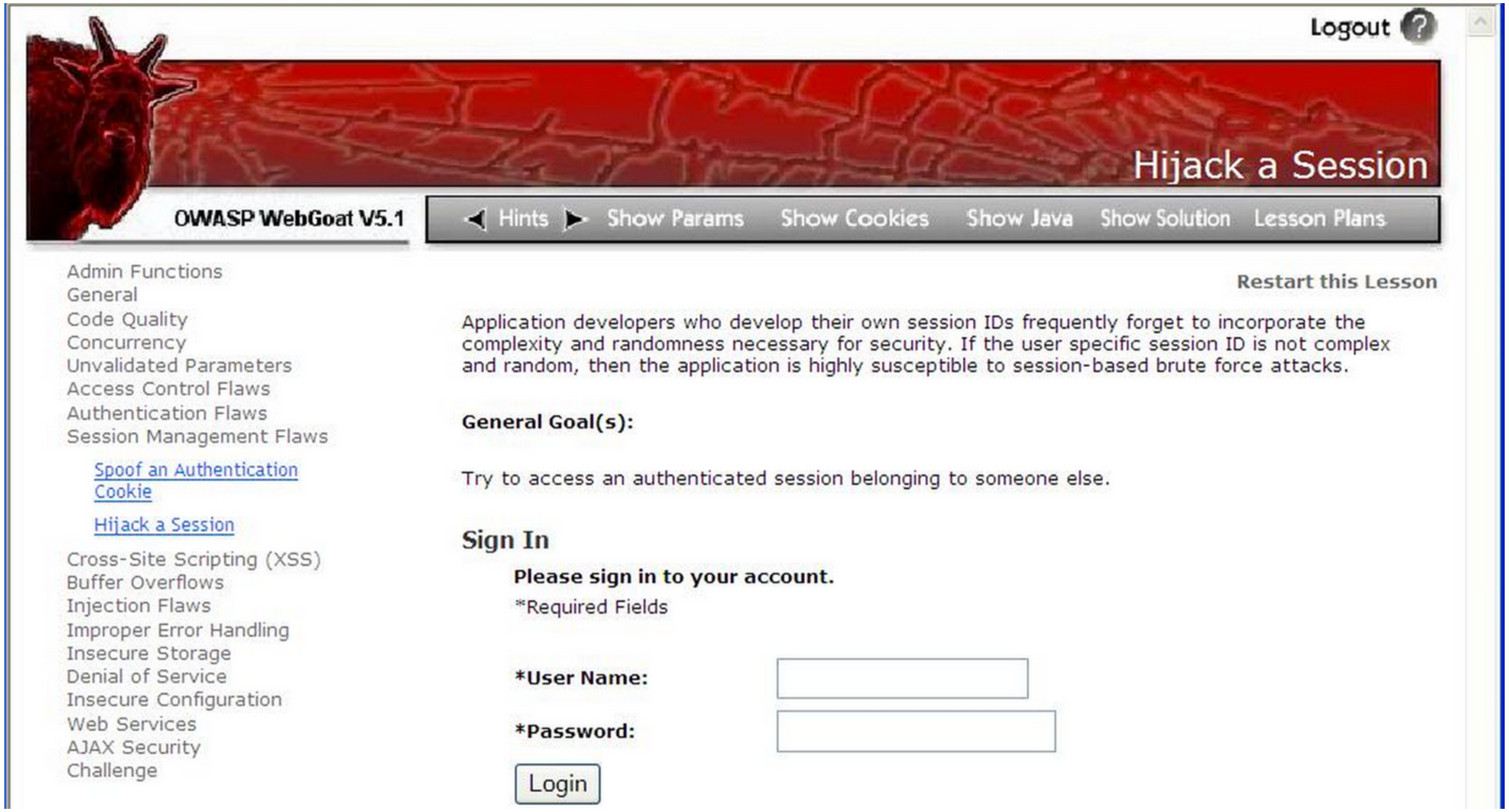
- Free On-Demand Training Courses
  - Released as Creative Commons 3.0
  - Examples: Secure Java Programming 101, Cross-Site Scripting 101, File Permissions, ….



Use our free security engineering training programs as the building blocks for your custom training program.

WebGoat - https://code.google.com/p/webgoat/

- Insecure J2EE app
  - Released as GPLv2, OWASP Project
  - Interactive teaching environment, with multiple lessons of increasing complexity



Application developers who develop their own session IDs frequently forget to incorporate the complexity and randomness necessary for security. If the user specific session ID is not complex and random, then the application is highly susceptible to session-based brute force attacks.

General Goal(s):

Try to access an authenticated session belonging to someone else.

Sign In

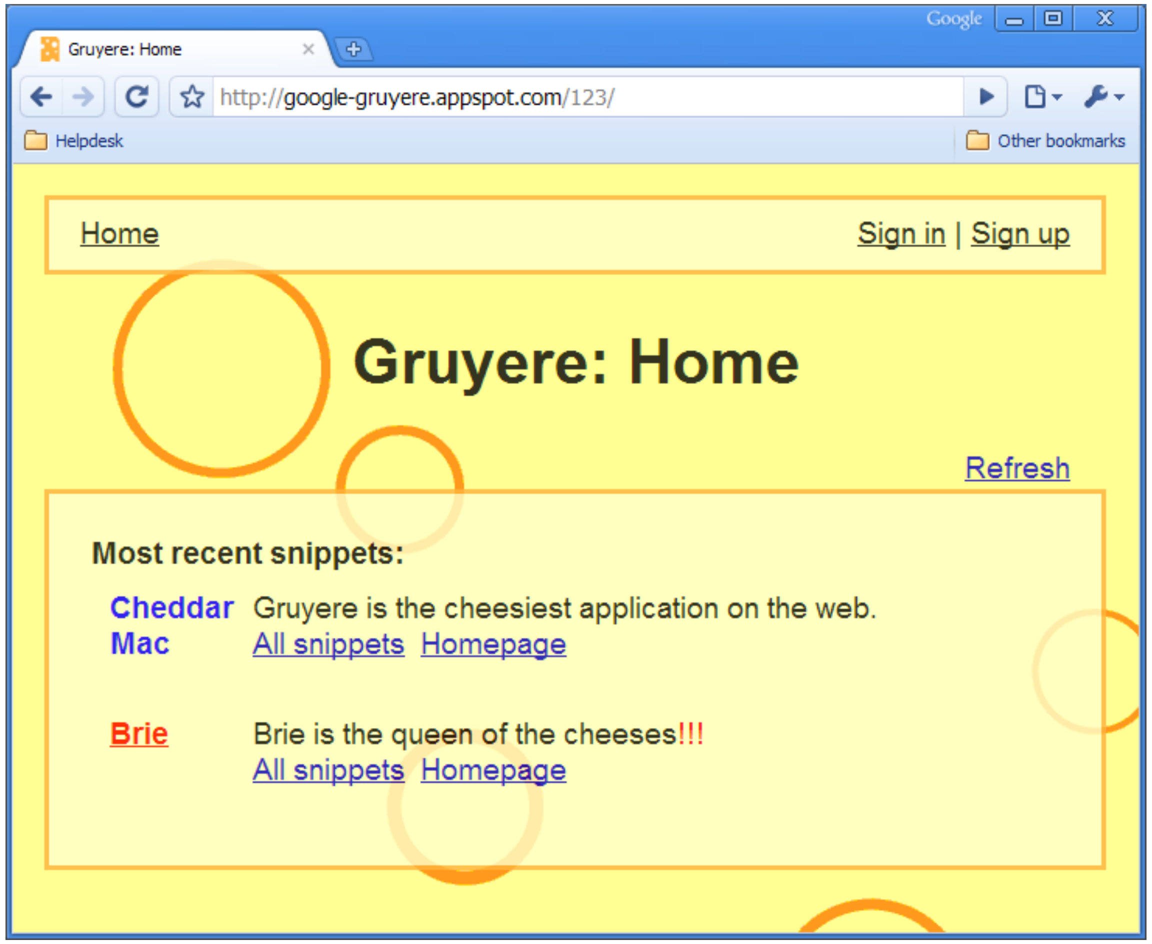
Please sign in to your account.

*Required Fields

***User Name:**

***Password:**

And many others



Home Sign in | Sign up

Gruyere: Home

Refresh

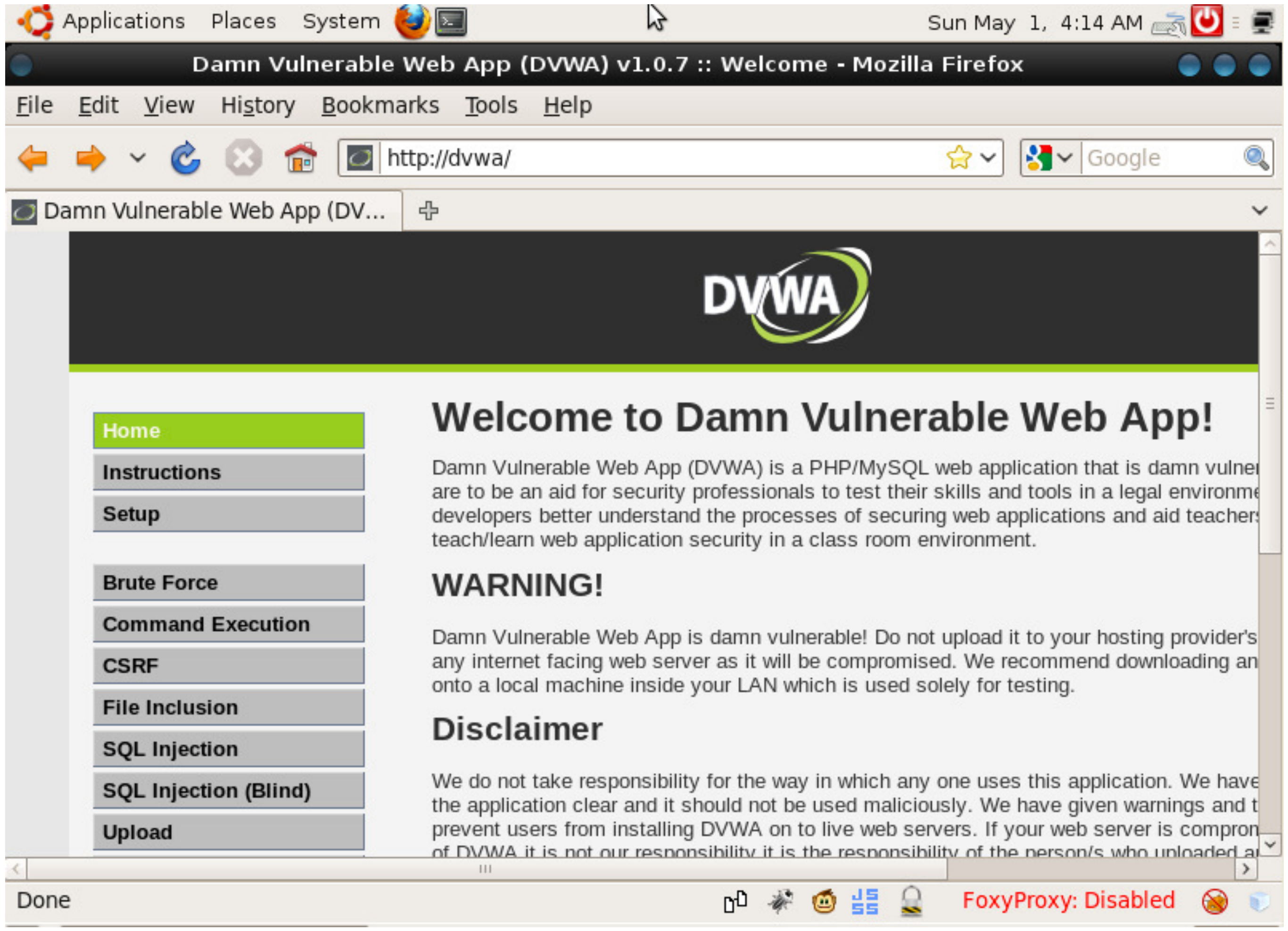
Most recent snippets:

Cheddar Mac Gruyere is the cheesiest application on the web.
All snippets Homepage

Brie Brie is the queen of the cheeses!!!
All snippets Homepage

Gruyere (Python)

DVWA (PHP)



Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulner
are to be an aid for security professionals to test their skills and tools in a legal environme
developers better understand the processes of securing web applications and aid teacher
teach/learn web application security in a class room environment.

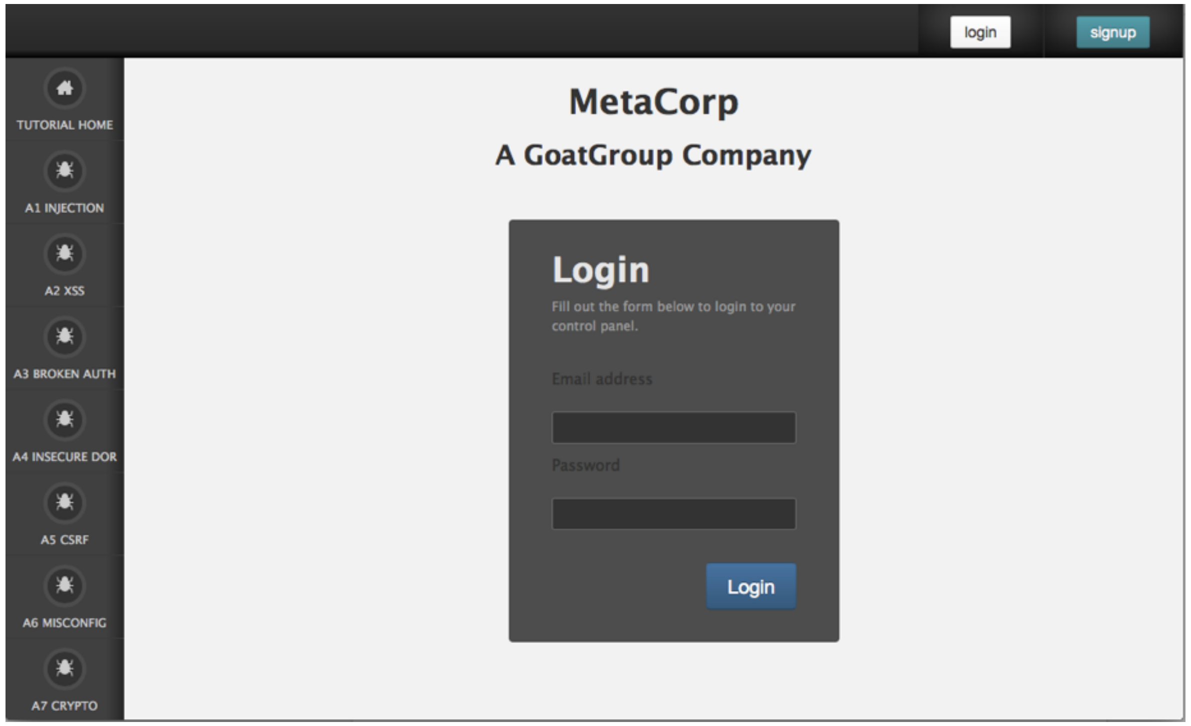
WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's
any internet facing web server as it will be compromised. We recommend downloading an
onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have
the application clear and it should not be used maliciously. We have given warnings and t
prevent users from installing DVWA on to live web servers. If your web server is compron
of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded a

And many others



MetaCorp

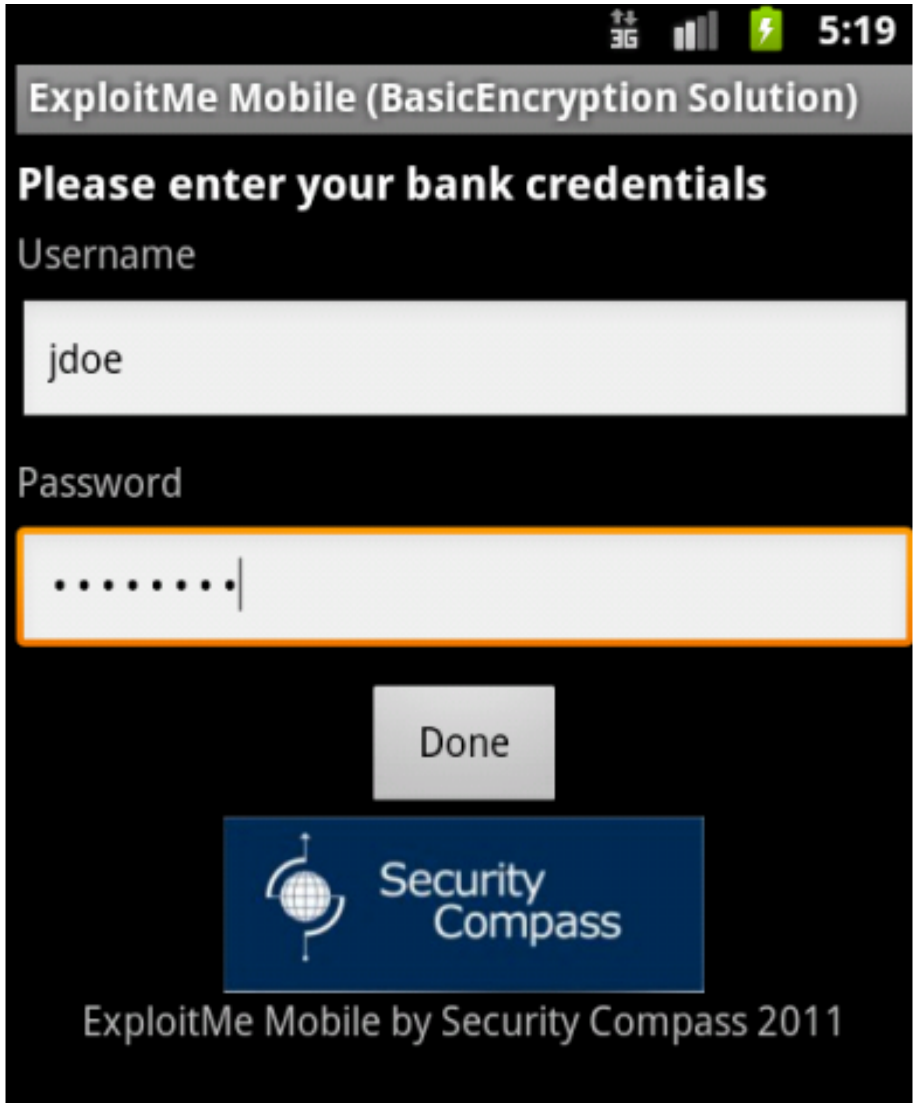
A GoatGroup Company

Login

Fill out the form below to login to your control panel.

Railsgoat (Ruby)

ExploitMe Mobile
(Java, Objective-C)



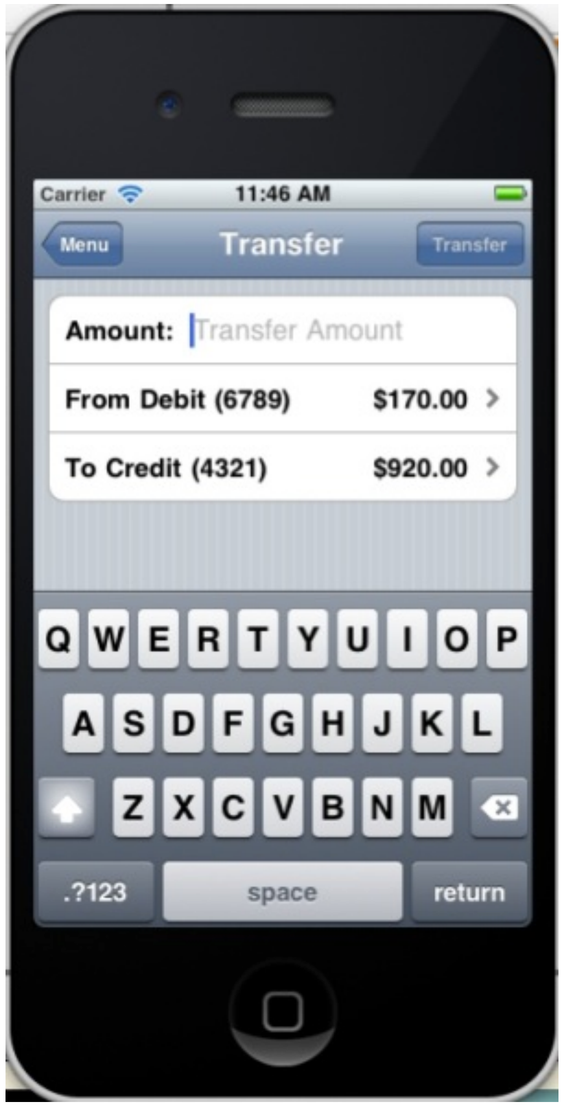
ExploitMe Mobile (BasicEncryption Solution)

Please enter your bank credentials

Username: jdoe

Password: ••••••••

ExploitMe Mobile by Security Compass 2011



Amount: Transfer Amount

From Debit (6789) $170.00

To Credit (4321) $920.00

Built-in Security

“The most effective way to bring security capabilities to developers is to have them built into the framework” OWASP Framework Security project

Still, not a silver-bullet:

1. Frameworks are not immune to bugs
2. Poor or inconsistent documentation
3. Negligence

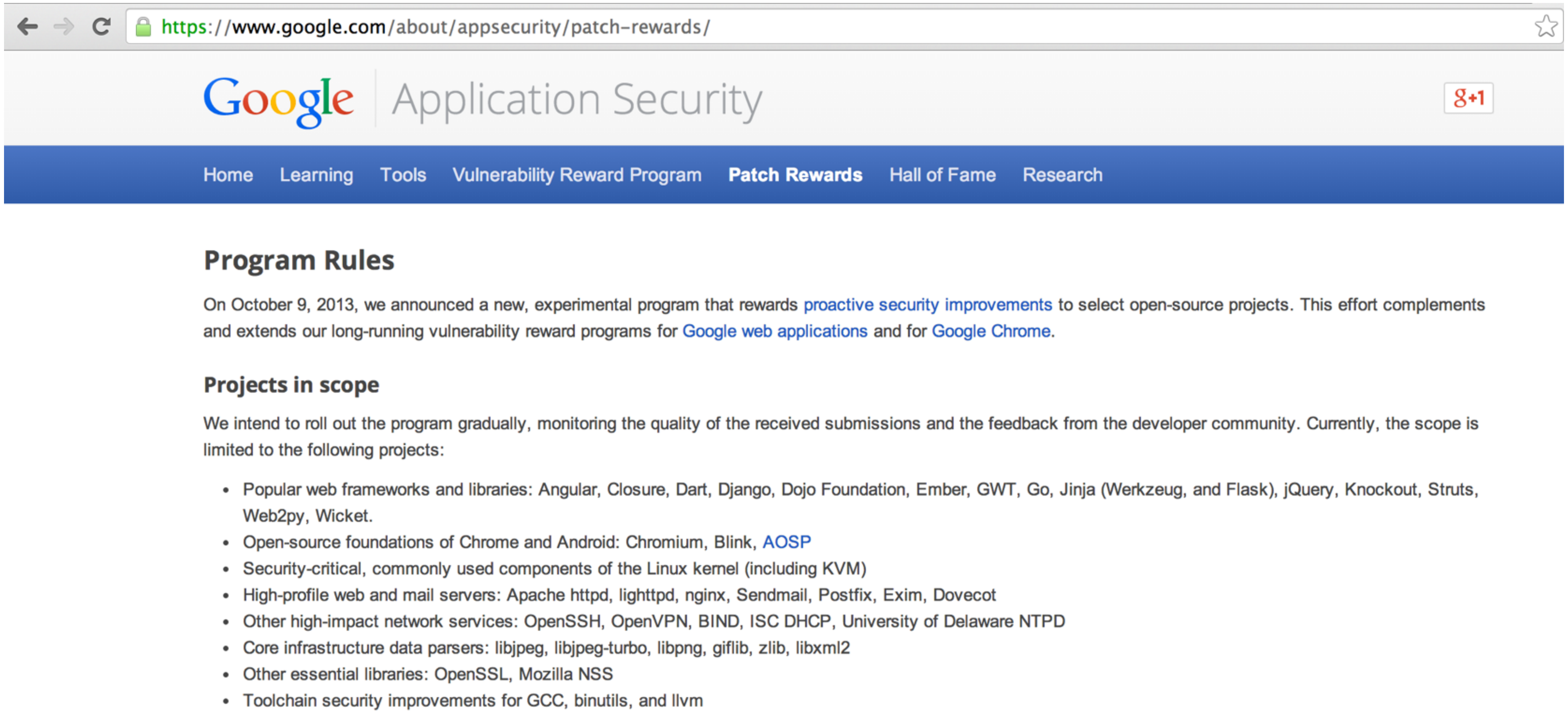
http://blog.nibblesec.org/2014/04/on-web-frameworks-built-in-security.html

How to choose a (secure) framework?

- Evaluate all security features and default settings
- Maturity of the project
- Project popularity
- Look for security advisories in Google, osvdb.org, etc.
  - No results ✗
  - Just few vulnerabilities in a few years ✓
  - Many software vulnerabilities ✗
- Time To Patch statistics

Security reward programs focused on OSS

- Google patch reward program
  - Focused on proactive security improvements for popular OSS projects
  - https://www.google.com/about/appsecurity/patch-rewards/
  - Eg: Ember, Angular, jQuery, …



https://www.google.com/about/appsecurity/patch-rewards/
Google Application Security
g+1
Home
Learning
Tools
Vulnerability Reward Program
Patch Rewards
Hall of Fame
Research

Program Rules

On October 9, 2013, we announced a new, experimental program that rewards proactive security improvements to select open-source projects. This effort complements and extends our long-running vulnerability reward programs for Google web applications and for Google Chrome.

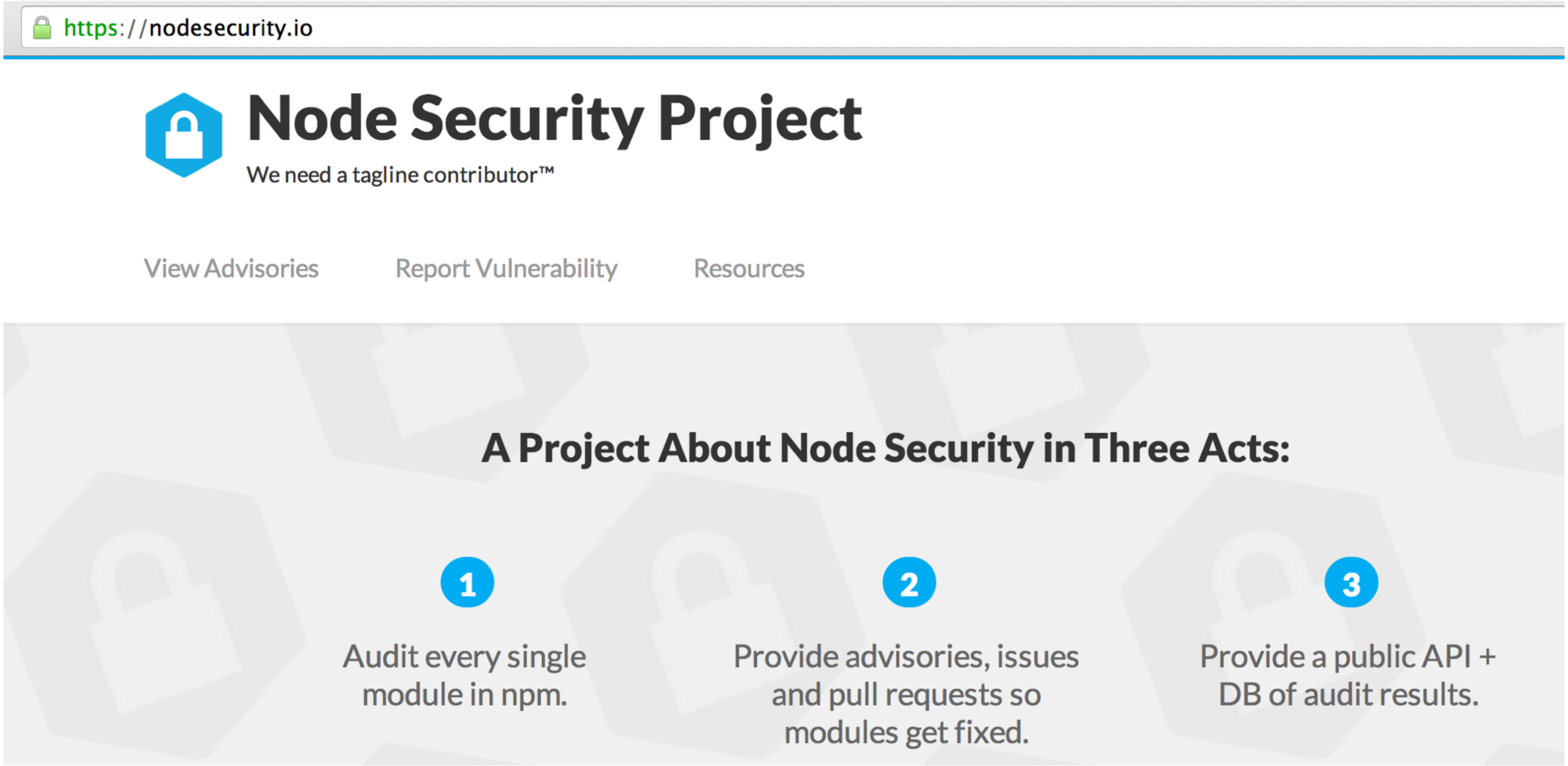
Projects in scope

We intend to roll out the program gradually, monitoring the quality of the received submissions and the feedback from the developer community. Currently, the scope is limited to the following projects:

- Popular web frameworks and libraries: Angular, Closure, Dart, Django, Dojo Foundation, Ember, GWT, Go, Jinja (Werkzeug, and Flask), jQuery, Knockout, Struts, Web2py, Wicket.
- Open-source foundations of Chrome and Android: Chromium, Blink, AOSP
- Security-critical, commonly used components of the Linux kernel (including KVM)
- High-profile web and mail servers: Apache httpd, lighttpd, nginx, Sendmail, Postfix, Exim, Dovecot
- Other high-impact network services: OpenSSH, OpenVPN, BIND, ISC DHCP, University of Delaware NTPD
- Core infrastructure data parsers: libjpeg, libjpeg-turbo, libpng, giflib, zlib, libxml2
- Other essential libraries: OpenSSL, Mozilla NSS
- Toolchain security improvements for GCC, binutils, and llvm

Community-based security reviews

- NodeSecurity Project
  - Audit NPM modules, fix bugs, write advisories
  - https://nodesecurity.io/



https://nodesecurity.io

Node Security Project

We need a tagline contributor™

A Project About Node Security in Three Acts:

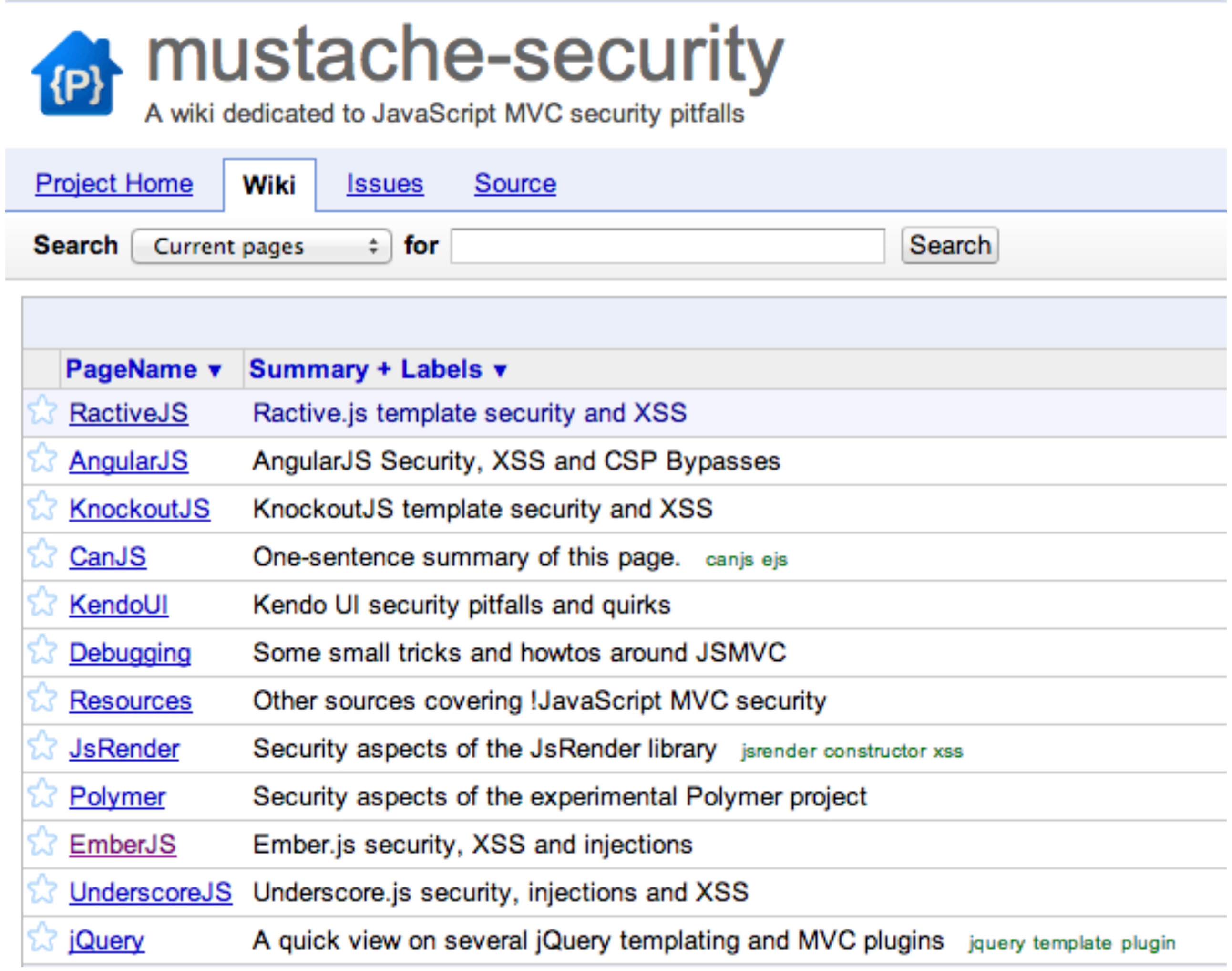
1 Audit every single module in npm.

2 Provide advisories, issues and pull requests so modules get fixed.

3 Provide a public API + DB of audit results.

Community-based security reviews

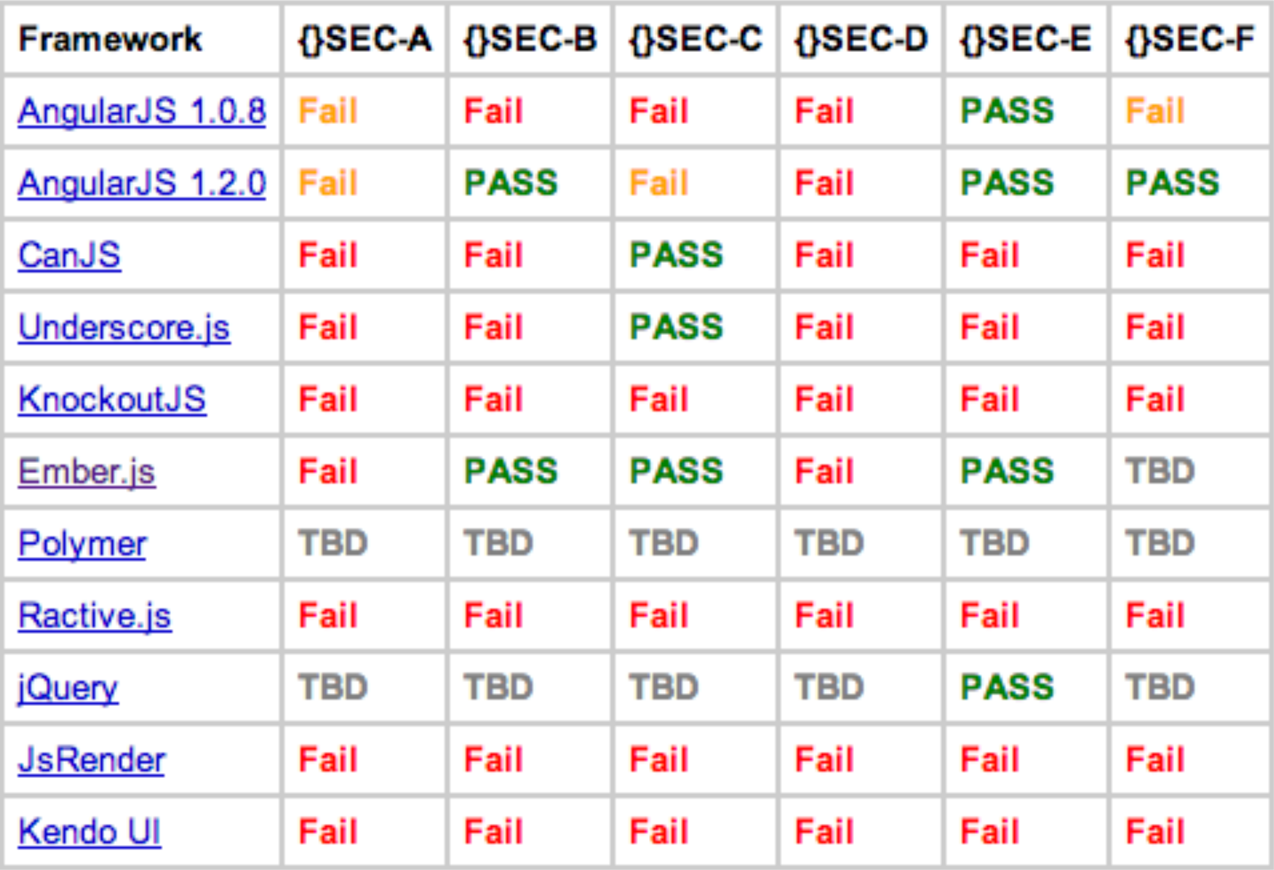
- Mustache-Security
  - A wiki dedicated to JavaScript MVC security pitfalls
  - https://code.google.com/p/mustache-security/



mustache-security

A wiki dedicated to JavaScript MVC security pitfalls

PageName ▾	Summary + Labels ▾
☆ RactiveJS	Ractive.js template security and XSS
☆ AngularJS	AngularJS Security, XSS and CSP Bypasses
☆ KnockoutJS	KnockoutJS template security and XSS
☆ CanJS	One-sentence summary of this page. canjs ejs
☆ KendoUI	Kendo UI security pitfalls and quirks
☆ Debugging	Some small tricks and howtos around JSMVC
☆ Resources	Other sources covering !JavaScript MVC security
☆ JsRender	Security aspects of the JsRender library jsrender constructor xss
☆ Polymer	Security aspects of the experimental Polymer project
☆ EmberJS	Ember.js security, XSS and injections
☆ UnderscoreJS	Underscore.js security, injections and XSS
☆ jQuery	A quick view on several jQuery templating and MVC plugins jquery template plugin



Framework	{}SEC-A	{}SEC-B	{}SEC-C	{}SEC-D	{}SEC-E	{}SEC-F
AngularJS 1.0.8	Fail	Fail	Fail	Fail	PASS	Fail
AngularJS 1.2.0	Fail	PASS	Fail	Fail	PASS	PASS
CanJS	Fail	Fail	PASS	Fail	Fail	Fail
Underscore.js	Fail	Fail	PASS	Fail	Fail	Fail
KnockoutJS	Fail	Fail	Fail	Fail	Fail	Fail
Ember.js	Fail	PASS	PASS	Fail	PASS	TBD
Polymer	TBD	TBD	TBD	TBD	TBD	TBD
Ractive.js	Fail	Fail	Fail	Fail	Fail	Fail
jQuery	TBD	TBD	TBD	TBD	PASS	TBD
JsRender	Fail	Fail	Fail	Fail	Fail	Fail
Kendo UI	Fail	Fail	Fail	Fail	Fail	Fail

IsTrueCryptAuditedYet?

- TrueCrypt
  - Very popular file and disk encryption software
  - Never been fully and independently audited
  - http://istruecryptauditedyet.com/

Code, Testing

Phase 2

Don't reinvent the wheel

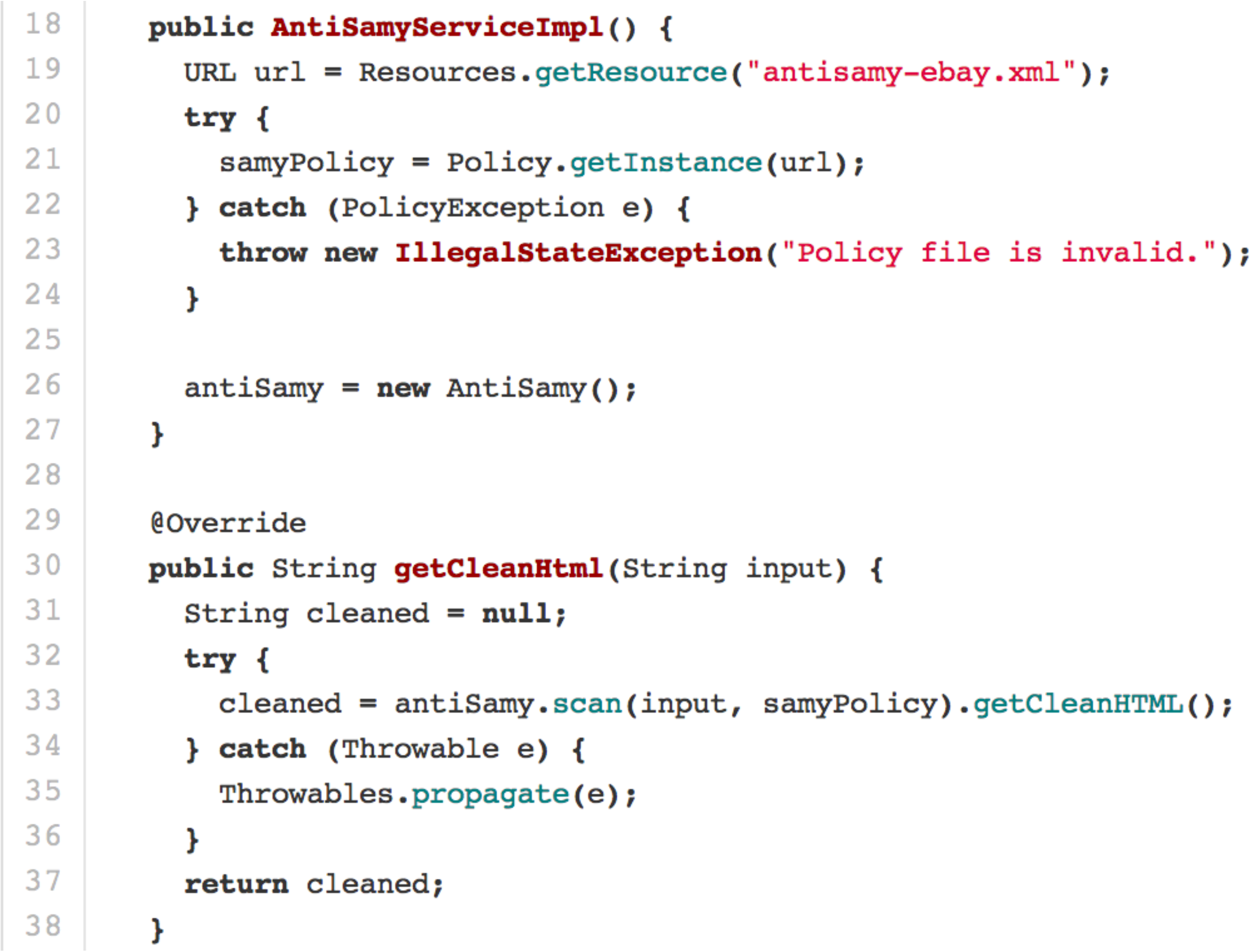
“When I was in college in the early 70s, I devised what I believed was a brilliant encryption scheme. […] Years later, I discovered this same scheme in several introductory cryptography texts […] as a simple homework assignment on how to use elementary cryptanalytic techniques to crack it” Phil Zimmermann

Really, don’t - especially for the following:

- Crypto (RNG, Hash functions, Enc/Dec schemas, …)
- Security features, such as input validation/output encoding

AntiSamy - https://code.google.com/p/owaspantisamy/

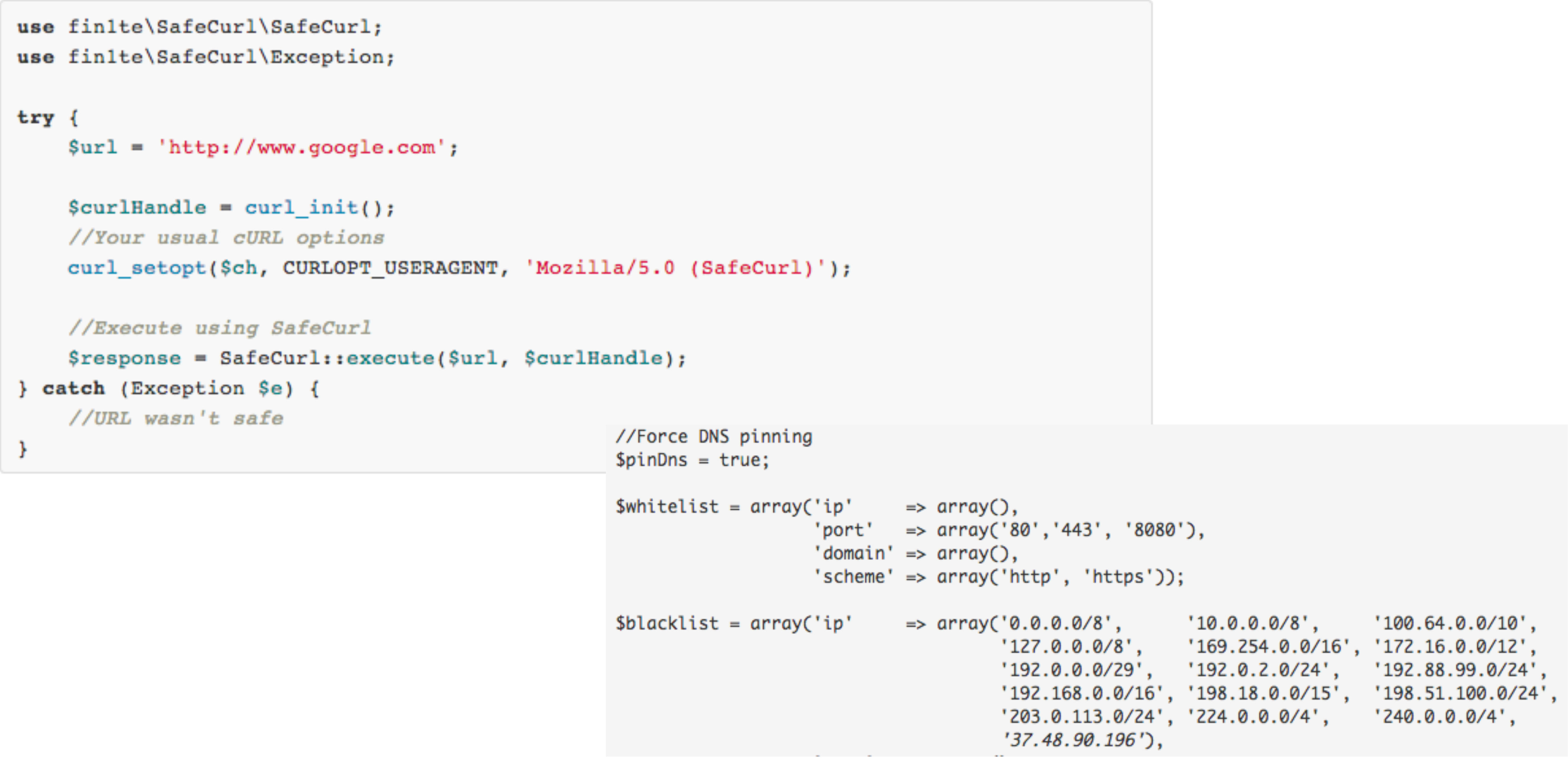
- Collection of APIs for validating rich user content
  - Released as BSD, OWASP Project
  - Useful to check whether user-supplied HTML/CSS is in compliance within an application's rules



```java
public AntiSamyServiceImpl() {
  URL url = Resources.getResource("antisamy-ebay.xml");
  try {
    samyPolicy = Policy.getInstance(url);
  } catch (PolicyException e) {
    throw new IllegalStateException("Policy file is invalid.");
  }

  antiSamy = new AntiSamy();
}

@Override
public String getCleanHtml(String input) {
  String cleaned = null;
  try {
    cleaned = antiSamy.scan(input, samyPolicy).getCleanHTML();
  } catch (Throwable e) {
    Throwables.propagate(e);
  }
  return cleaned;
}
```

SafeCURL - https://github.com/fin1te/safecurl

- A drop-in replacement for the ‘insecure’ curl_exec function in PHP
    - Useful to prevent Server-Side Request Forgery

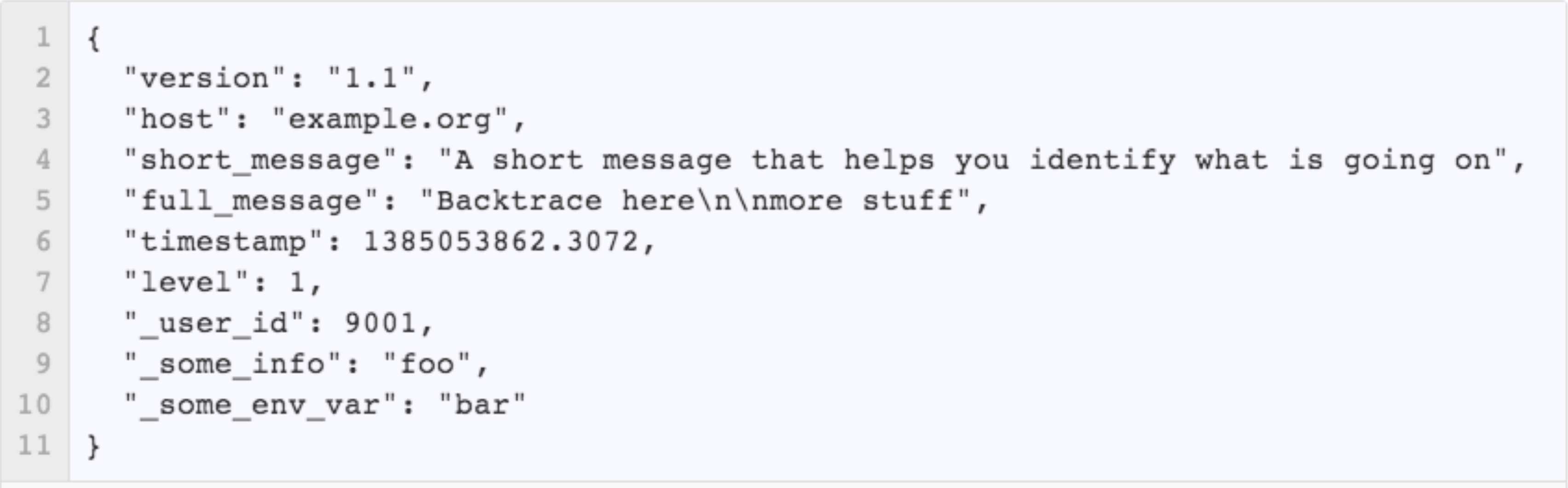


```
use fin1te\SafeCurl\SafeCurl;
use fin1te\SafeCurl\Exception;

try {
    $url = 'http://www.google.com';

    $curlHandle = curl_init();
    //Your usual cURL options
    curl_setopt($ch, CURLOPT_USERAGENT, 'Mozilla/5.0 (SafeCurl)');

    //Execute using SafeCurl
    $response = SafeCurl::execute($url, $curlHandle);
} catch (Exception $e) {
    //URL wasn't safe
}
```

```
//Force DNS pinning
$pinDns = true;

$whitelist = array('ip'     => array(),
                   'port'   => array('80','443', '8080'),
                   'domain' => array(),
                   'scheme' => array('http', 'https'));

$blacklist = array('ip'     => array('0.0.0.0/8',      '10.0.0.0/8',     '100.64.0.0/10',
                                     '127.0.0.0/8',    '169.254.0.0/16', '172.16.0.0/12',
                                     '192.0.0.0/29',   '192.0.2.0/24',   '192.88.99.0/24',
                                     '192.168.0.0/16', '198.18.0.0/15',  '198.51.100.0/24',
                                     '203.0.113.0/24', '224.0.0.0/4',    '240.0.0.0/4',
                                     '37.48.90.196'),
```

GELF Appenders - http://graylog2.org/gelf#libraries

- Extended Log Format for Apps
  - Structured
  - Chunking
  - Compression



```
{
  "version": "1.1",
  "host": "example.org",
  "short_message": "A short message that helps you identify what is going on",
  "full_message": "Backtrace here\n\nmore stuff",
  "timestamp": 1385053862.3072,
  "level": 1,
  "_user_id": 9001,
  "_some_info": "foo",
  "_some_env_var": "bar"
}
```

- Appenders available for many languages/frameworks
  - Java, Node.js, Ruby, Python, Perl, PHP, …<language that you'll never use>

Security Testing

“When you think that there are not more holes, relax and continue - sure you will find another” Cesar Cerrudo

KNOWN VULNERABILITIES
UNKNOWN VULNERABILITIES

Security Testing

There's a good news: you're defending the castle!

- Maximize the home-field advantage
  - You have source code
  - You know better your systems
  - You can make the attackers play with your rules

Maximize the home-field advantage

- Mix **source code** + **dynamic testing**
  - manual and semi-automatic

“Strategic” code review

- Define critical areas of your codebase, setup automatic alerts, review all changes

“Continuous” semi-automatic security testing

- Setup a dynamic web scanner to run for each candidate
- Customize the scanner to detect previously discovered vulnerabilities

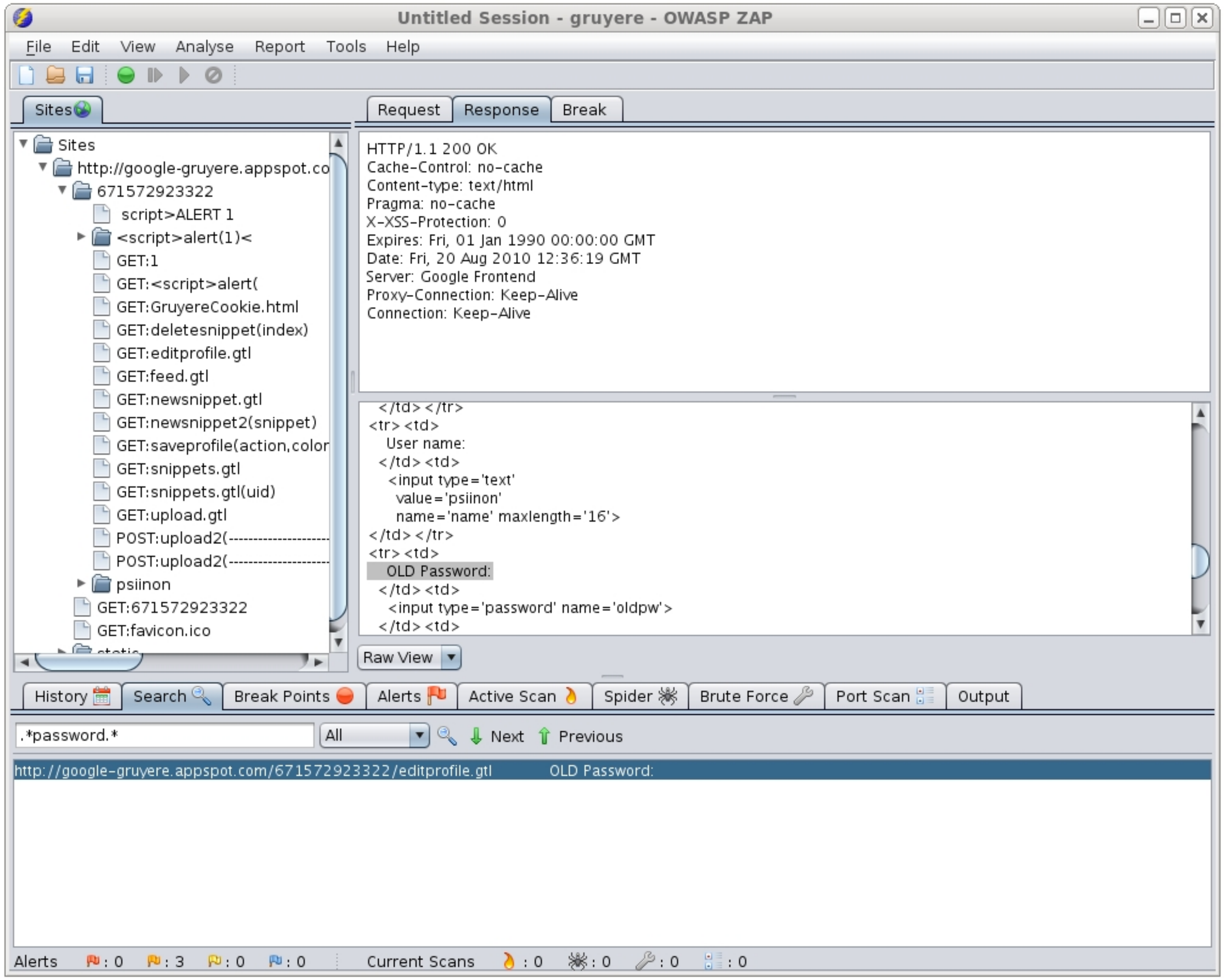
OWASP Testing Guide

- An open web application pentest methodology
- https://www.owasp.org/index.php/OWASP_Testing_Project
- V.4 is almost ready, currently in review phase

OWASP
The Open Web Application Security Project
OWASP Testing Guide v3.0
release
Creative Commons (CC) Attribution Share-Alike
Free version at http://www.owasp.org

OWASP ZED Attack Proxy Project

- Web application scanner and proxy for semi-automatic testing
- https://code.google.com/p/zaproxy


Untitled Session - gruyere - OWASP ZAP
File Edit View Analyse Report Tools Help
Sites
Request Response Break
Sites
http://google-gruyere.appspot.co
671572923322
script>ALERT 1
<script>alert(1)<
GET:1
GET:<script>alert(
GET:GruyereCookie.html
GET:deletesnippet(index)
GET:editprofile.gtl
GET:feed.gtl
GET:newsnippet.gtl
GET:newsnippet2(snippet)
GET:saveprofile(action,color
GET:snippets.gtl
GET:snippets.gtl(uid)
GET:upload.gtl
POST:upload2(--------------------
POST:upload2(--------------------
psiinon
GET:671572923322
GET:favicon.ico
static
Raw View
History Search Break Points Alerts Active Scan Spider Brute Force Port Scan Output
All
Next Previous
Alerts : 0 : 3 : 0 : 0 Current Scans : 0 : 0 : 0 : 0

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Content-type: text/html
Pragma: no-cache
X-XSS-Protection: 0
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Date: Fri, 20 Aug 2010 12:36:19 GMT
Server: Google Frontend
Proxy-Connection: Keep-Alive
Connection: Keep-Alive
```

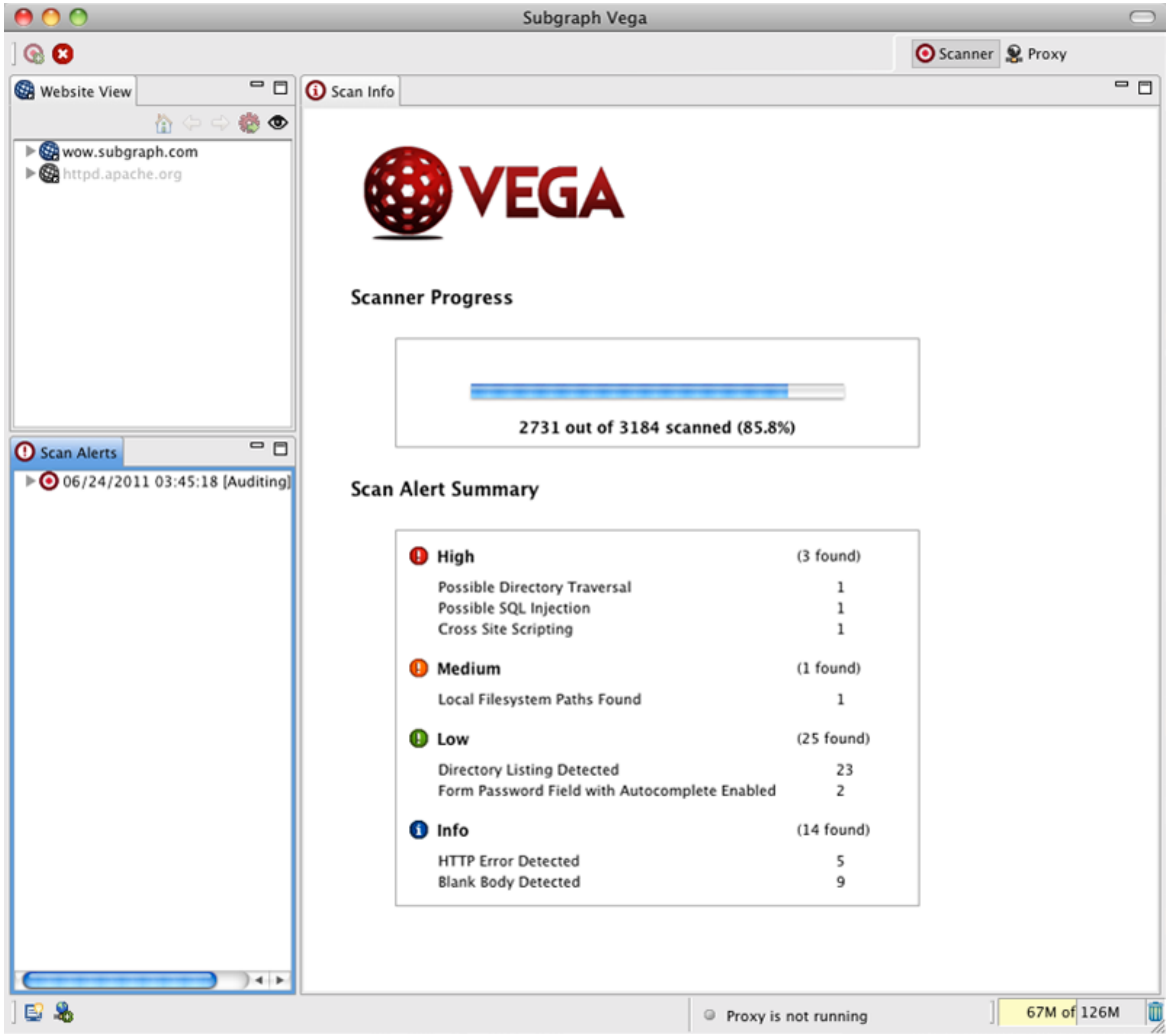
```
  </td></tr>
<tr><td>
    User name:
  </td><td>
   <input type='text'
     value='psiinon'
     name='name' maxlength='16'>
</td></tr>
<tr><td>
    OLD Password:
  </td><td>
   <input type='password' name='oldpw'>
  </td><td>
```

.*password.*

```
http://google-gruyere.appspot.com/671572923322/editprofile.gtl          OLD Password:
```

SUBGRAPH VEGA

- Web application vulnerability scanner
- https://subgraph.com/vega/



06/24/2011 03:45:18 [Auditing]

Scanner Progress

2731 out of 3184 scanned (85.8%)

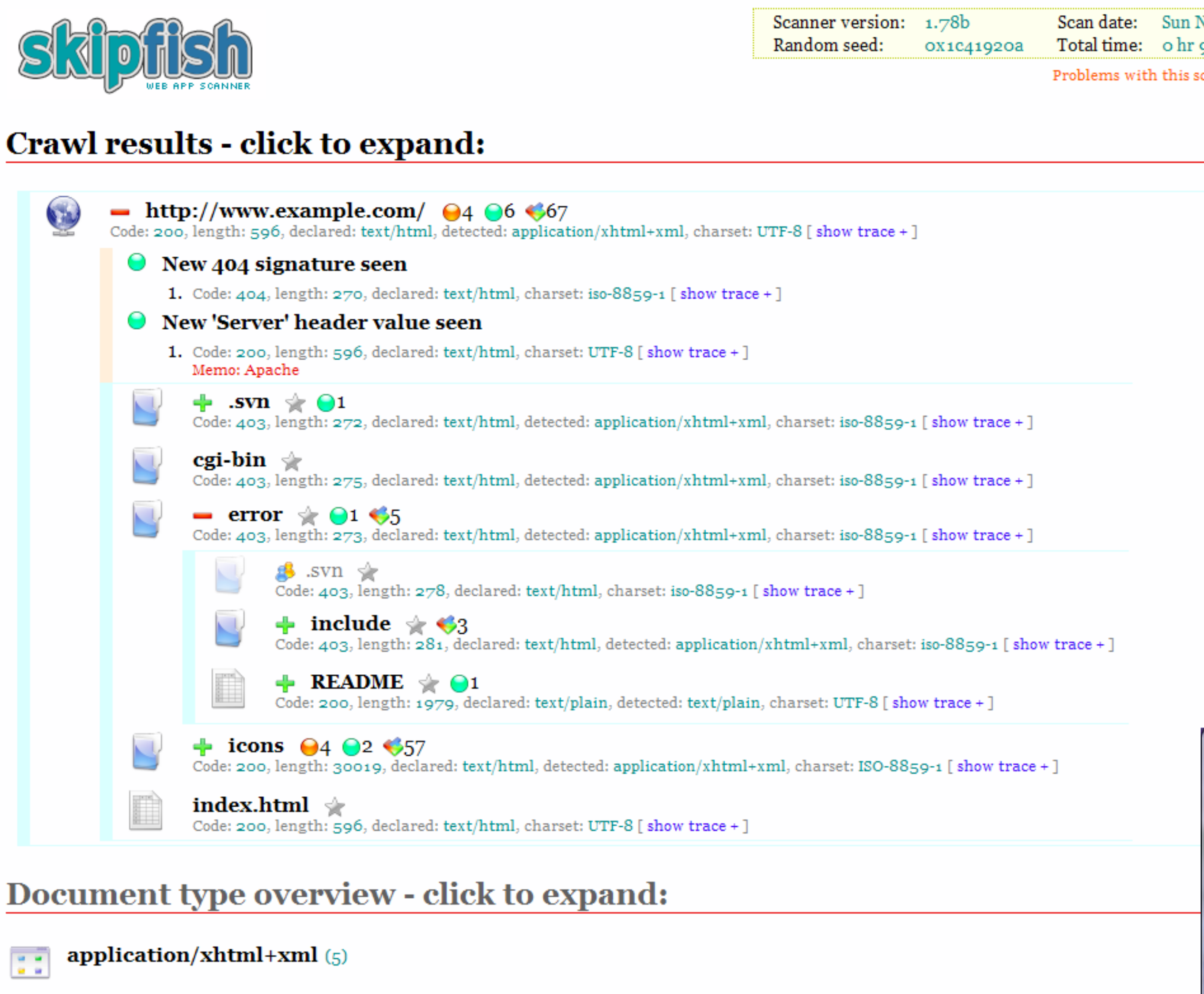
Scan Alert Summary

High	(3 found)
Possible Directory Traversal	1
Possible SQL Injection	1
Cross Site Scripting	1
Medium	(1 found)
Local Filesystem Paths Found	1
Low	(25 found)
Directory Listing Detected	23
Form Password Field with Autocomplete Enabled	2
Info	(14 found)
HTTP Error Detected	5
Blank Body Detected	9

Proxy is not running

67M of 126M

And many others



Scanner version: 1.78b Scan date: Sun Nov 21 23:40:36 2010
Random seed: 0x1c41920a Total time: 0 hr 9 min 8 sec 467 ms

Problems with this scan? Click here for advice.

Crawl results - click to expand:

http://www.example.com/ 4 6 67
Code: 200, length: 596, declared: text/html, detected: application/xhtml+xml, charset: UTF-8 [show trace +]

New 404 signature seen
1. Code: 404, length: 270, declared: text/html, charset: iso-8859-1 [show trace +]

New 'Server' header value seen
1. Code: 200, length: 596, declared: text/html, charset: UTF-8 [show trace +]
Memo: Apache

.svn 1
Code: 403, length: 272, declared: text/html, detected: application/xhtml+xml, charset: iso-8859-1 [show trace +]

cgi-bin
Code: 403, length: 275, declared: text/html, detected: application/xhtml+xml, charset: iso-8859-1 [show trace +]

error 1 5
Code: 403, length: 273, declared: text/html, detected: application/xhtml+xml, charset: iso-8859-1 [show trace +]

.svn
Code: 403, length: 278, declared: text/html, charset: iso-8859-1 [show trace +]

include 3
Code: 403, length: 281, declared: text/html, detected: application/xhtml+xml, charset: iso-8859-1 [show trace +]

README 1
Code: 200, length: 1979, declared: text/plain, detected: text/plain, charset: UTF-8 [show trace +]

icons 4 2 57
Code: 200, length: 30019, declared: text/html, detected: application/xhtml+xml, charset: ISO-8859-1 [show trace +]

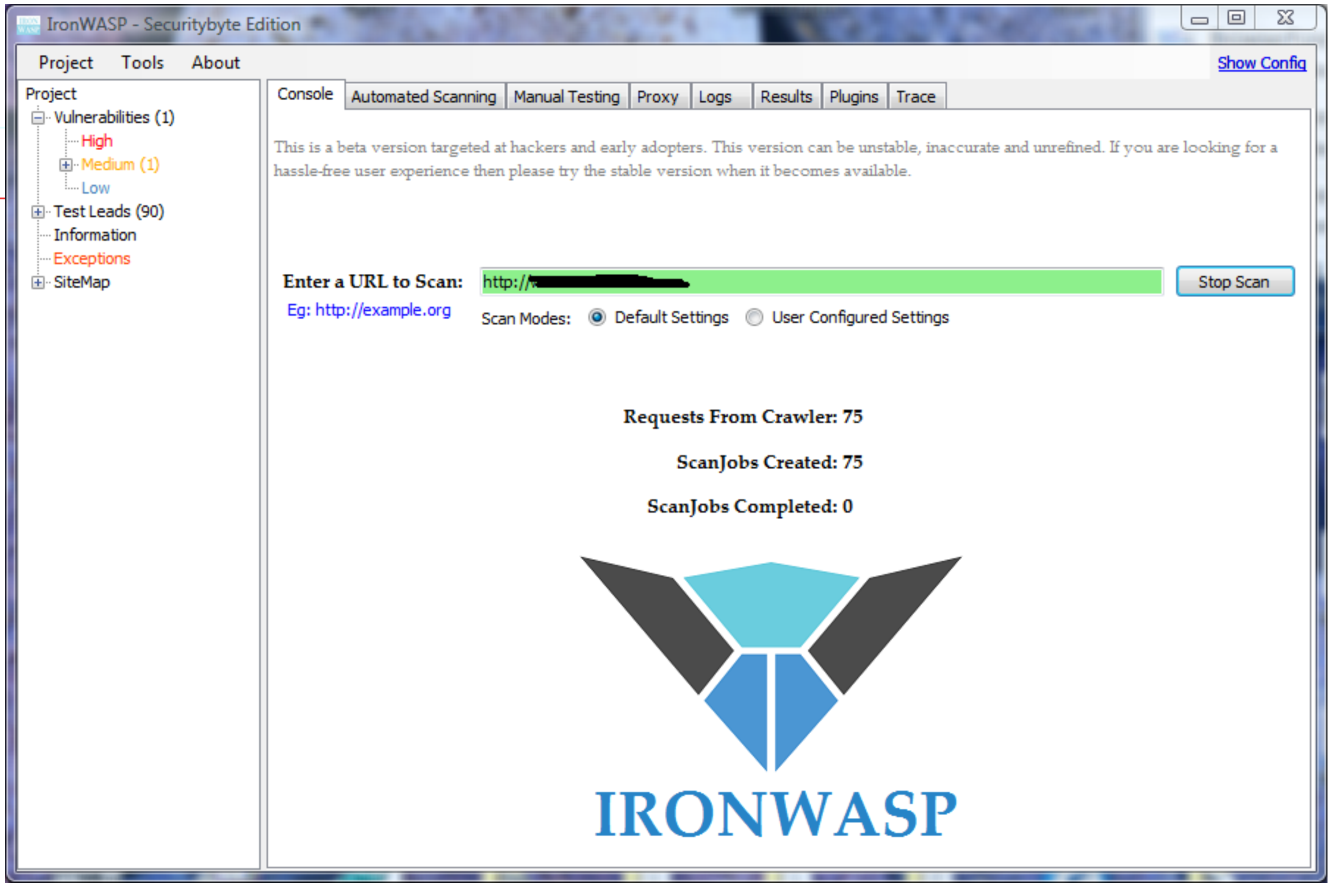
index.html
Code: 200, length: 596, declared: text/html, charset: UTF-8 [show trace +]

Document type overview - click to expand:

application/xhtml+xml (5)

SkipFish

IronWASP



This is a beta version targeted at hackers and early adopters. This version can be unstable, inaccurate and unrefined. If you are looking for a hassle-free user experience then please try the stable version when it becomes available.

Enter a URL to Scan: http://[redacted]

Eg: http://example.org

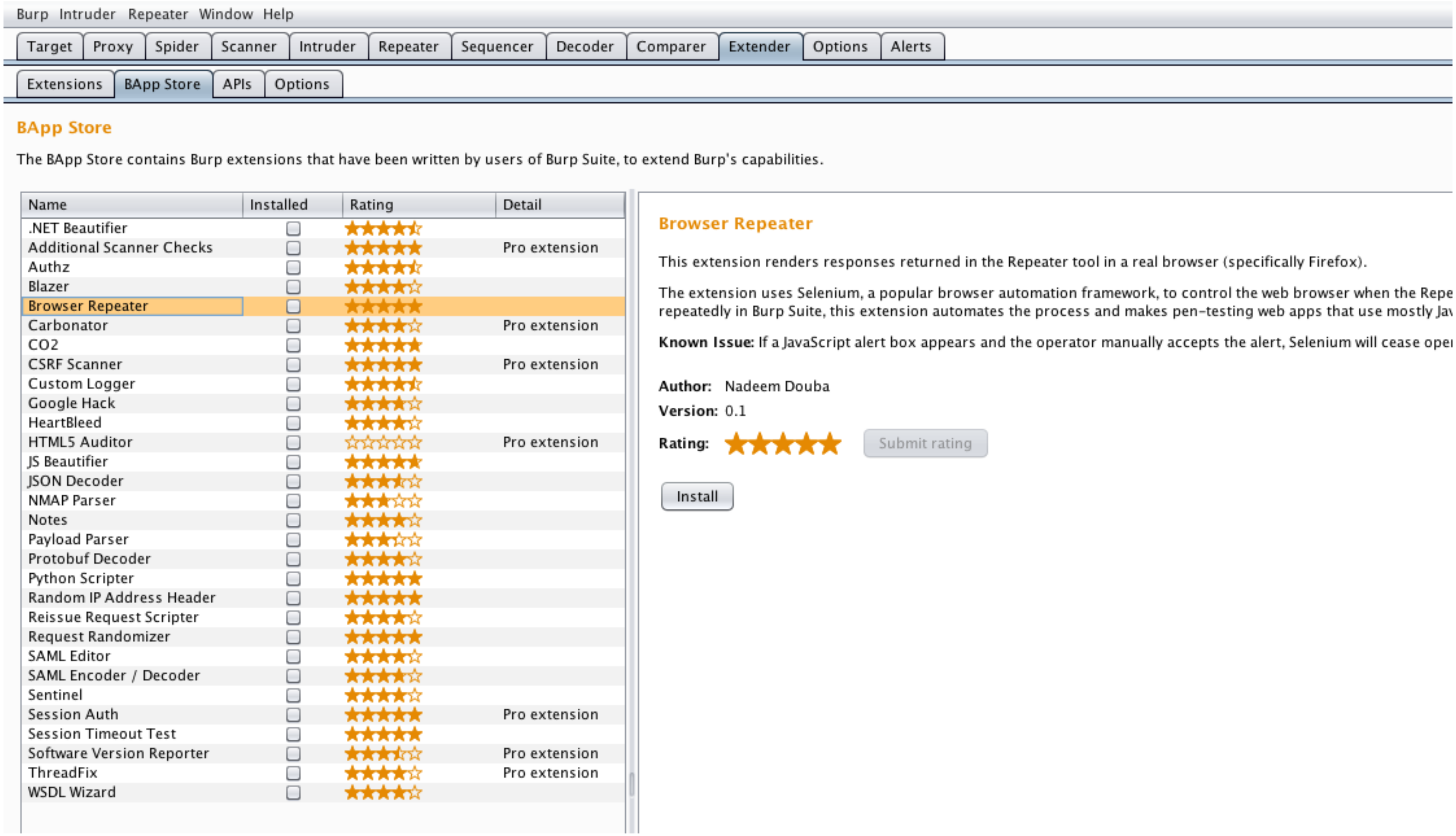
Scan Modes: ● Default Settings ○ User Configured Settings

Requests From Crawler: 75

ScanJobs Created: 75

ScanJobs Completed: 0

Even not open, have open plugins



BApp Store

The BApp Store contains Burp extensions that have been written by users of Burp Suite, to extend Burp's capabilities.

Name	Installed	Rating	Detail
.NET Beautifier	□	★★★★½	
Additional Scanner Checks	□	★★★★★	Pro extension
Authz	□	★★★★½	
Blazer	□	★★★★☆	
Browser Repeater	□	★★★★★	
Carbonator	□	★★★★☆	Pro extension
CO2	□	★★★★★	
CSRF Scanner	□	★★★★★	Pro extension
Custom Logger	□	★★★★½	
Google Hack	□	★★★★☆	
HeartBleed	□	★★★★☆	
HTML5 Auditor	□	☆☆☆☆☆	Pro extension
JS Beautifier	□	★★★★★	
JSON Decoder	□	★★★½☆	
NMAP Parser	□	★★★☆☆	
Notes	□	★★★★☆	
Payload Parser	□	★★★☆☆	
Protobuf Decoder	□	★★★★☆	
Python Scripter	□	★★★★★	
Random IP Address Header	□	★★★★★	
Reissue Request Scripter	□	★★★★☆	
Request Randomizer	□	★★★★★	
SAML Editor	□	★★★★☆	
SAML Encoder / Decoder	□	★★★★☆	
Sentinel	□	★★★★☆	
Session Auth	□	★★★★★	Pro extension
Session Timeout Test	□	★★★★★	
Software Version Reporter	□	★★★½☆	Pro extension
ThreadFix	□	★★★★☆	Pro extension
WSDL Wizard	□	★★★★☆	

Browser Repeater

This extension renders responses returned in the Repeater tool in a real browser (specifically Firefox).

The extension uses Selenium, a popular browser automation framework, to control the web browser when the Repe
repeatedly in Burp Suite, this extension automates the process and makes pen-testing web apps that use mostly Jav

Known Issue: If a JavaScript alert box appears and the operator manually accepts the alert, Selenium will cease ope

Author: Nadeem Douba

Version: 0.1

Rating: ★★★★★

BurpSuite

Insecure libraries

From the 2014 OpenSource Survey:

“Is open source governance keeping pace with growth of open source component usage?”
75% admit they don't have meaningful controls in place

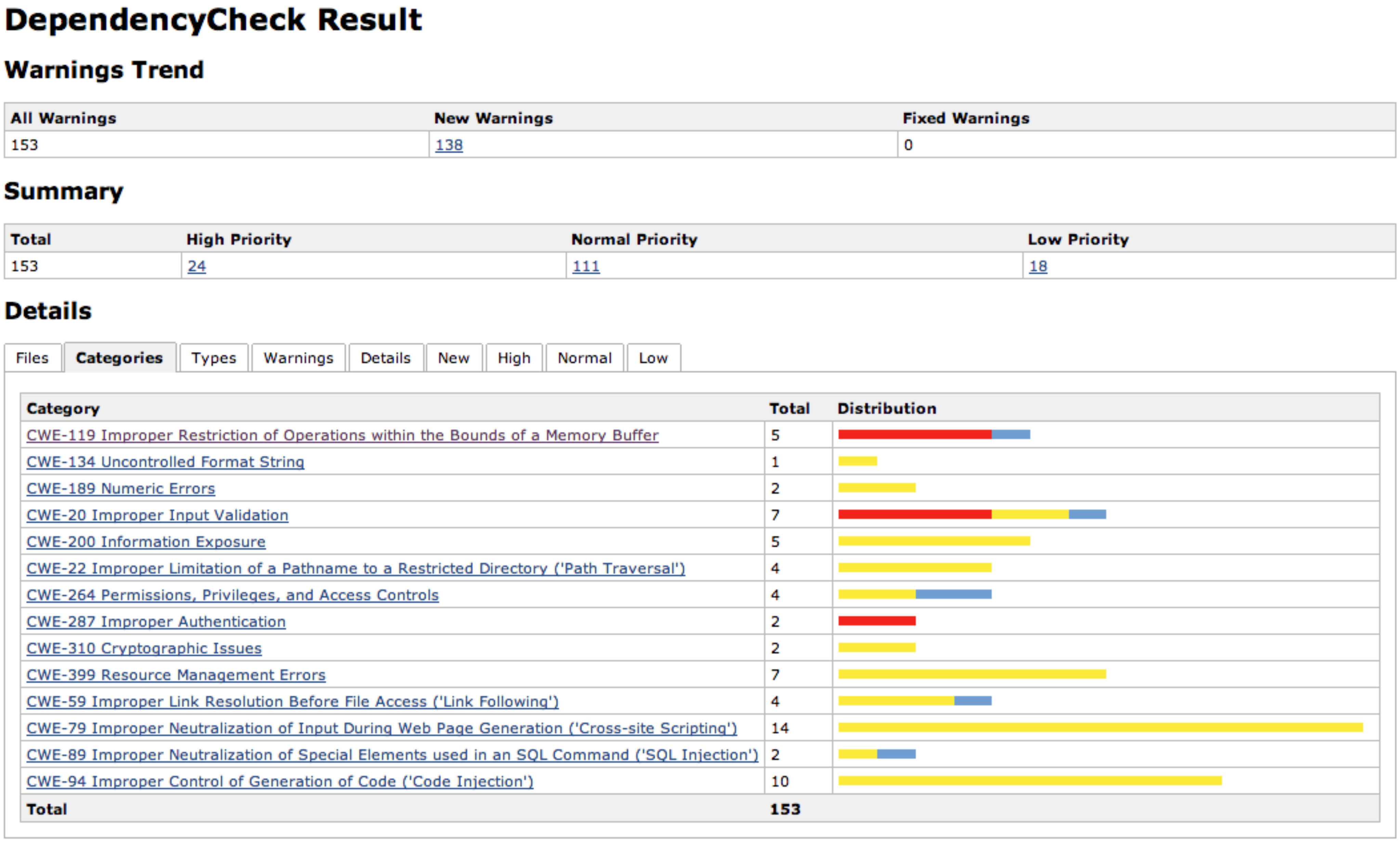
“Are components monitored for changes in vulnerability?”
6-in-10 said No

Governance in two steps, depending on your level of maturity:

1. Detect libraries with known vulnerabilities
2. Proactively prevent inclusion

OWASP Dependency-Check

- Java and .NET dependencies scanner
- https://github.com/jeremylong/DependencyCheck
- CLI, Maven, Ant, Jenkins



DependencyCheck Result

Warnings Trend

All Warnings	New Warnings	Fixed Warnings
153	138	0

Summary

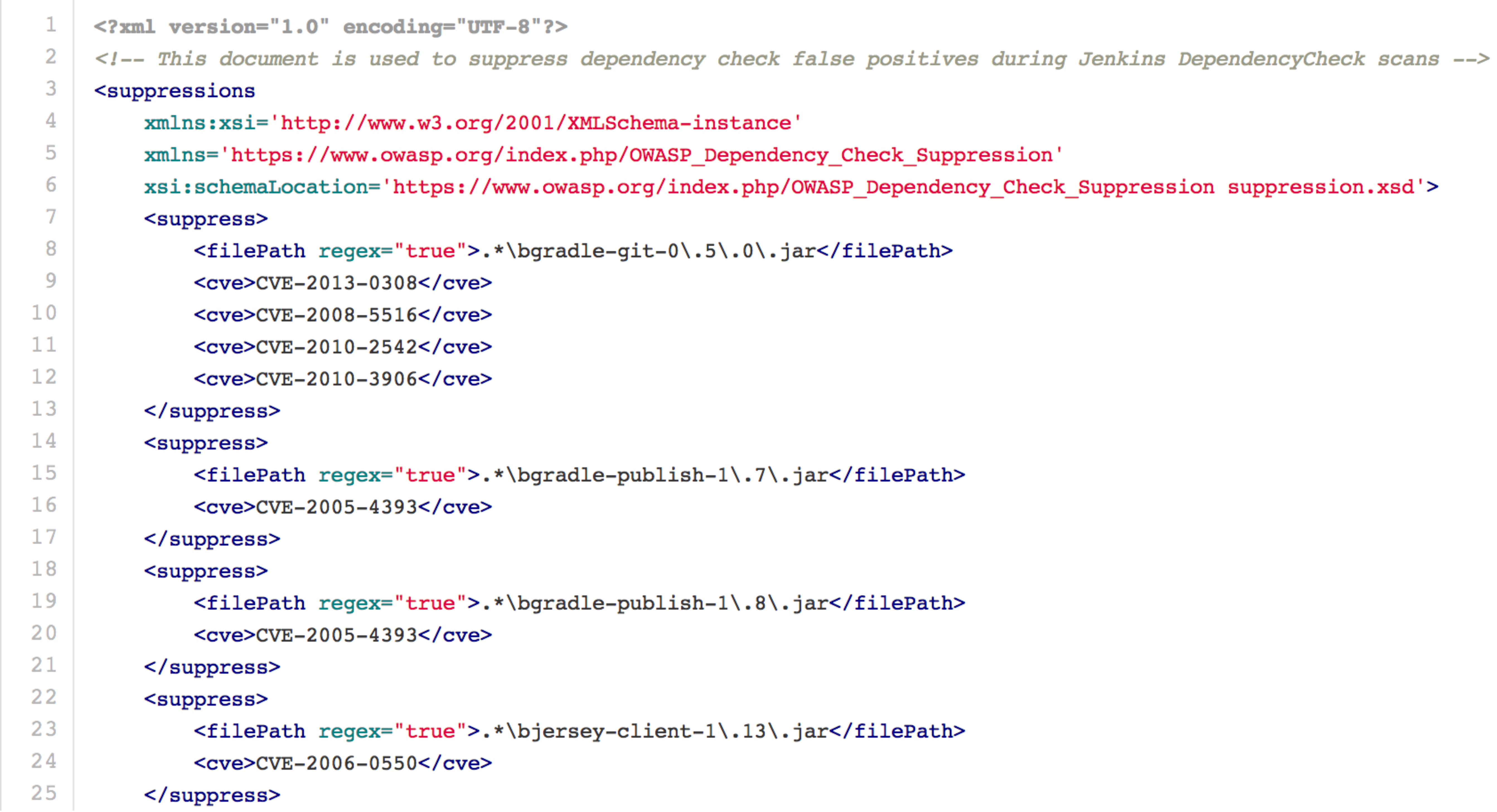
Total	High Priority	Normal Priority	Low Priority
153	24	111	18

Details

Category	Total	Distribution
CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer	5	🟥🟥🟥🟥🟦
CWE-134 Uncontrolled Format String	1	🟨
CWE-189 Numeric Errors	2	🟨🟨
CWE-20 Improper Input Validation	7	🟥🟥🟥🟥🟨🟨🟦
CWE-200 Information Exposure	5	🟨🟨🟨🟨🟨
CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	4	🟨🟨🟨🟨
CWE-264 Permissions, Privileges, and Access Controls	4	🟨🟨🟦🟦
CWE-287 Improper Authentication	2	🟥🟥
CWE-310 Cryptographic Issues	2	🟨🟨
CWE-399 Resource Management Errors	7	🟨🟨🟨🟨🟨🟨🟨
CWE-59 Improper Link Resolution Before File Access ('Link Following')	4	🟨🟨🟨🟦
CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14	🟨🟨🟨🟨🟨🟨🟨🟨🟨🟨🟨🟨🟨🟨
CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	2	🟨🟦
CWE-94 Improper Control of Generation of Code ('Code Injection')	10	🟨🟨🟨🟨🟨🟨🟨🟨🟨🟨
Total	**153**	

OWASP Dependency-Check

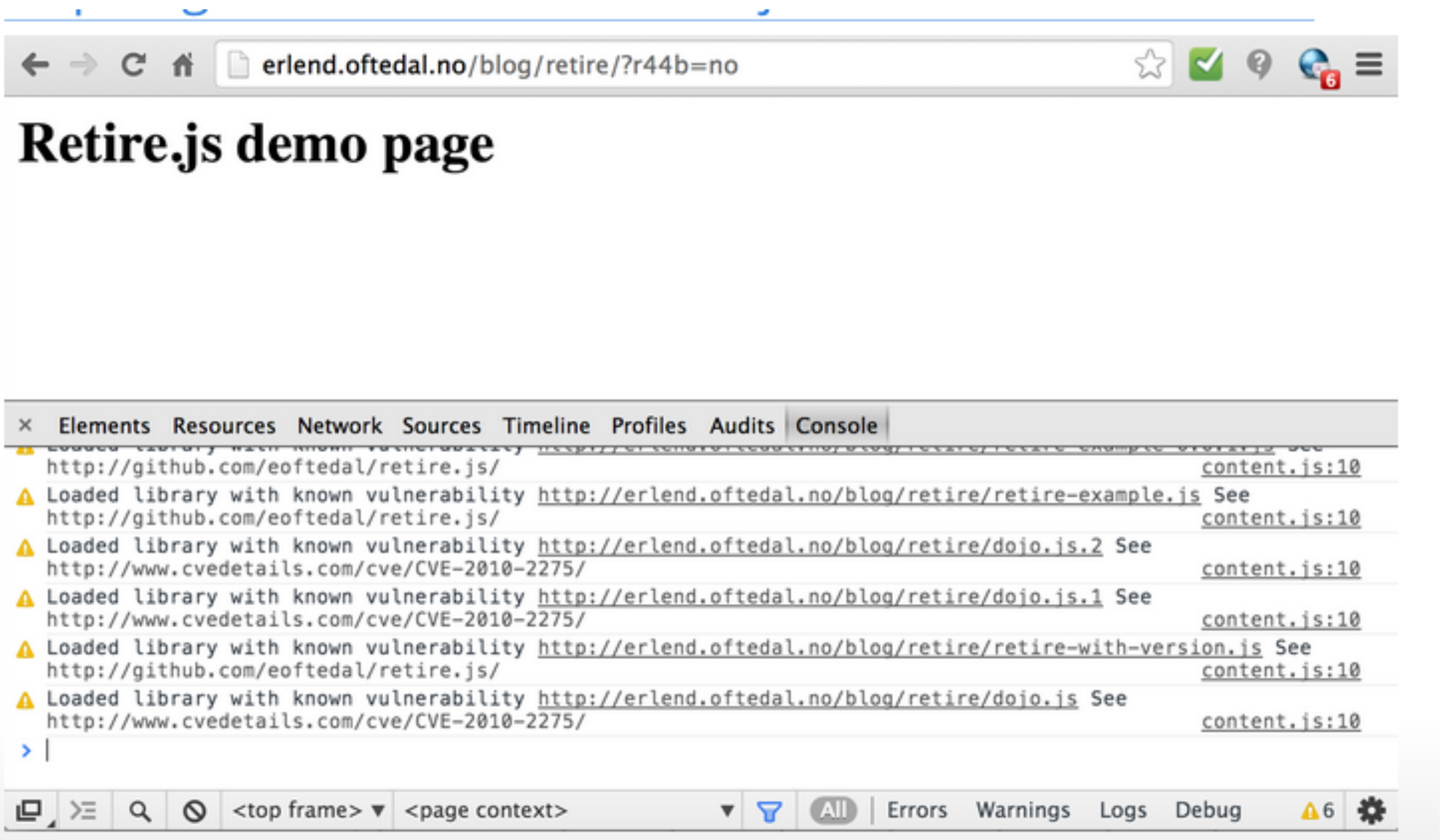
- Suppressions.xml



```xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- This document is used to suppress dependency check false positives during Jenkins DependencyCheck scans -->
<suppressions
    xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
    xmlns='https://www.owasp.org/index.php/OWASP_Dependency_Check_Suppression'
    xsi:schemaLocation='https://www.owasp.org/index.php/OWASP_Dependency_Check_Suppression suppression.xsd'>
    <suppress>
        <filePath regex="true">.*\bgradle-git-0\.5\.0\.jar</filePath>
        <cve>CVE-2013-0308</cve>
        <cve>CVE-2008-5516</cve>
        <cve>CVE-2010-2542</cve>
        <cve>CVE-2010-3906</cve>
    </suppress>
    <suppress>
        <filePath regex="true">.*\bgradle-publish-1\.7\.jar</filePath>
        <cve>CVE-2005-4393</cve>
    </suppress>
    <suppress>
        <filePath regex="true">.*\bgradle-publish-1\.8\.jar</filePath>
        <cve>CVE-2005-4393</cve>
    </suppress>
    <suppress>
        <filePath regex="true">.*\bjersey-client-1\.13\.jar</filePath>
        <cve>CVE-2006-0550</cve>
    </suppress>
```

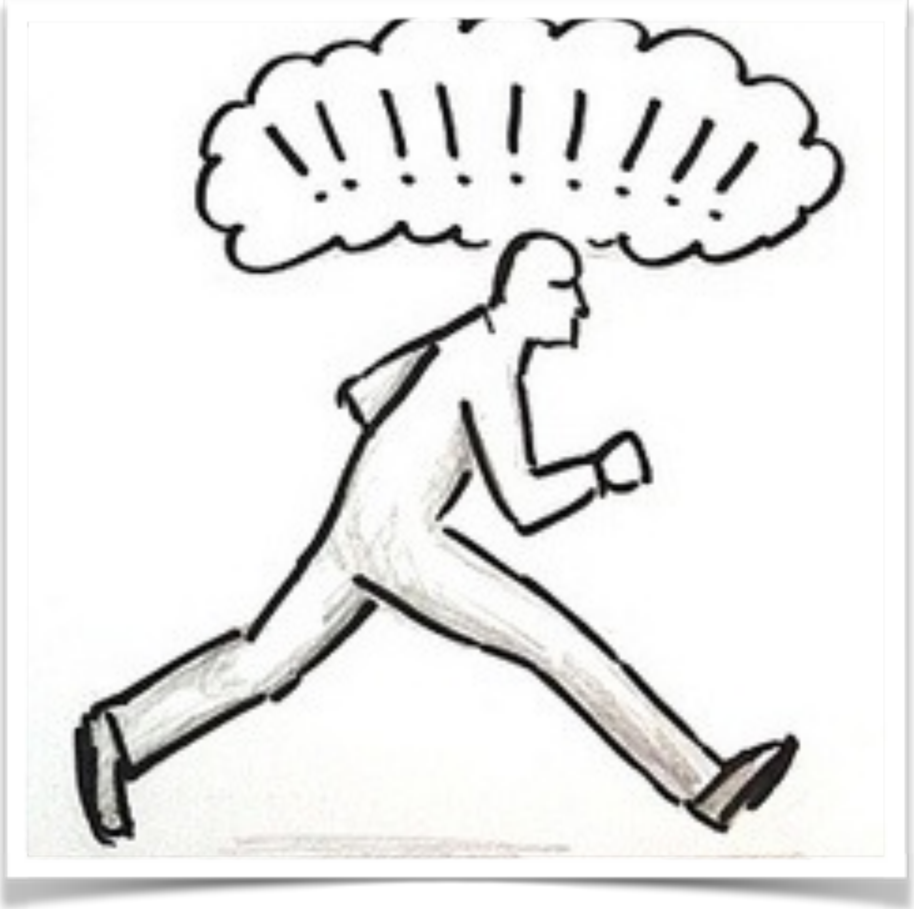
Retire.js

- JavaScript,NodeJS dependency scanner
- http://bekk.github.io/retire.js/
- CLI, Grunt, browser plugins



Retire.js demo page

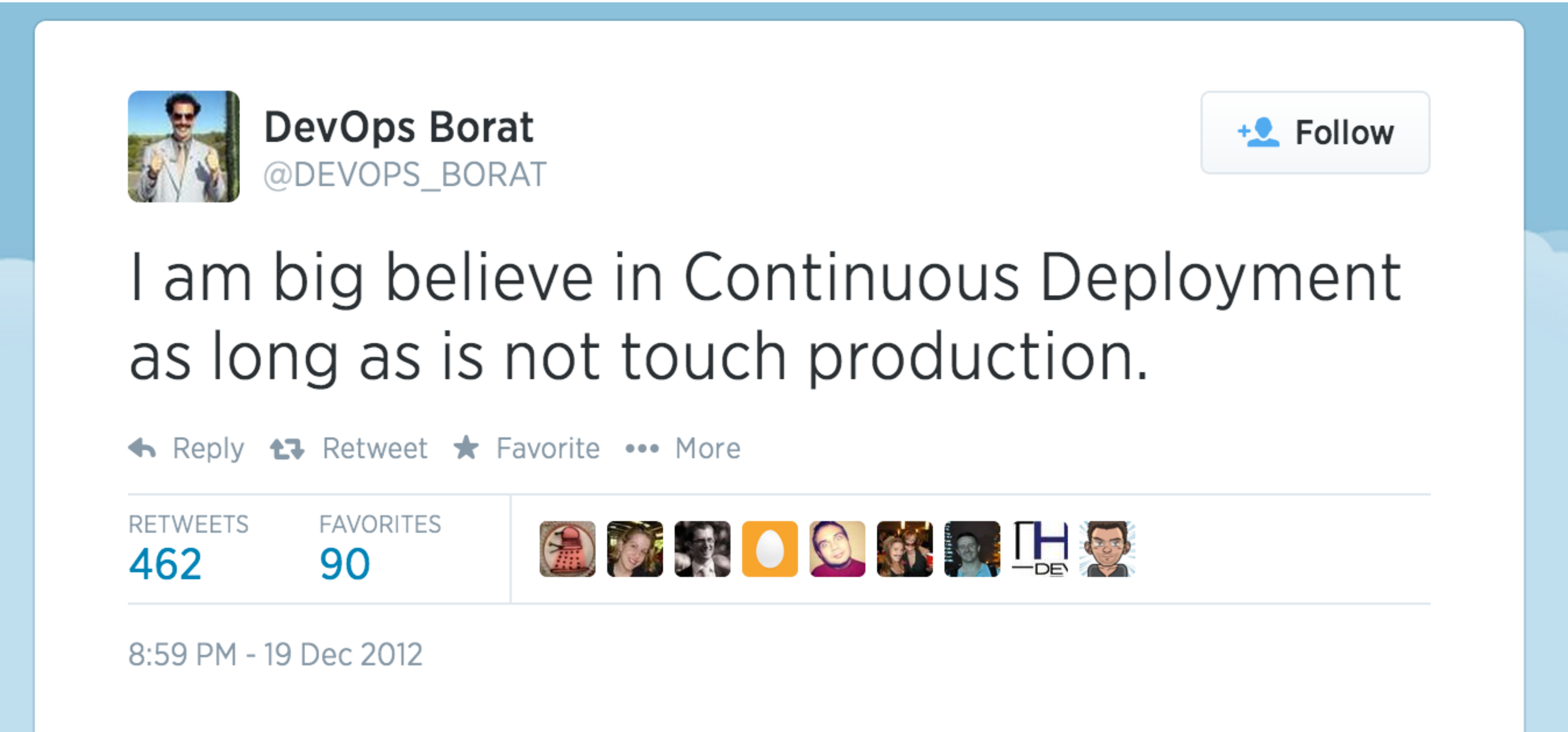
```
  http://github.com/eoftedal/retire.js/                                               content.js:10
⚠ Loaded library with known vulnerability http://erlend.oftedal.no/blog/retire/retire-example.js See
  http://github.com/eoftedal/retire.js/                                               content.js:10
⚠ Loaded library with known vulnerability http://erlend.oftedal.no/blog/retire/dojo.js.2 See
  http://www.cvedetails.com/cve/CVE-2010-2275/                                        content.js:10
⚠ Loaded library with known vulnerability http://erlend.oftedal.no/blog/retire/dojo.js.1 See
  http://www.cvedetails.com/cve/CVE-2010-2275/                                        content.js:10
⚠ Loaded library with known vulnerability http://erlend.oftedal.no/blog/retire/retire-with-version.js See
  http://github.com/eoftedal/retire.js/                                               content.js:10
⚠ Loaded library with known vulnerability http://erlend.oftedal.no/blog/retire/dojo.js See
  http://www.cvedetails.com/cve/CVE-2010-2275/                                        content.js:10
> |
```



Deploy (and maintain)

Phase 3

On continuous deployment



DevOps Borat
@DEVOPS_BORAT

I am big believe in Continuous Deployment as long as is not touch production.

RETWEETS 462

FAVORITES 90

8:59 PM - 19 Dec 2012

Logs

“Logs are your friend” A friend of mine

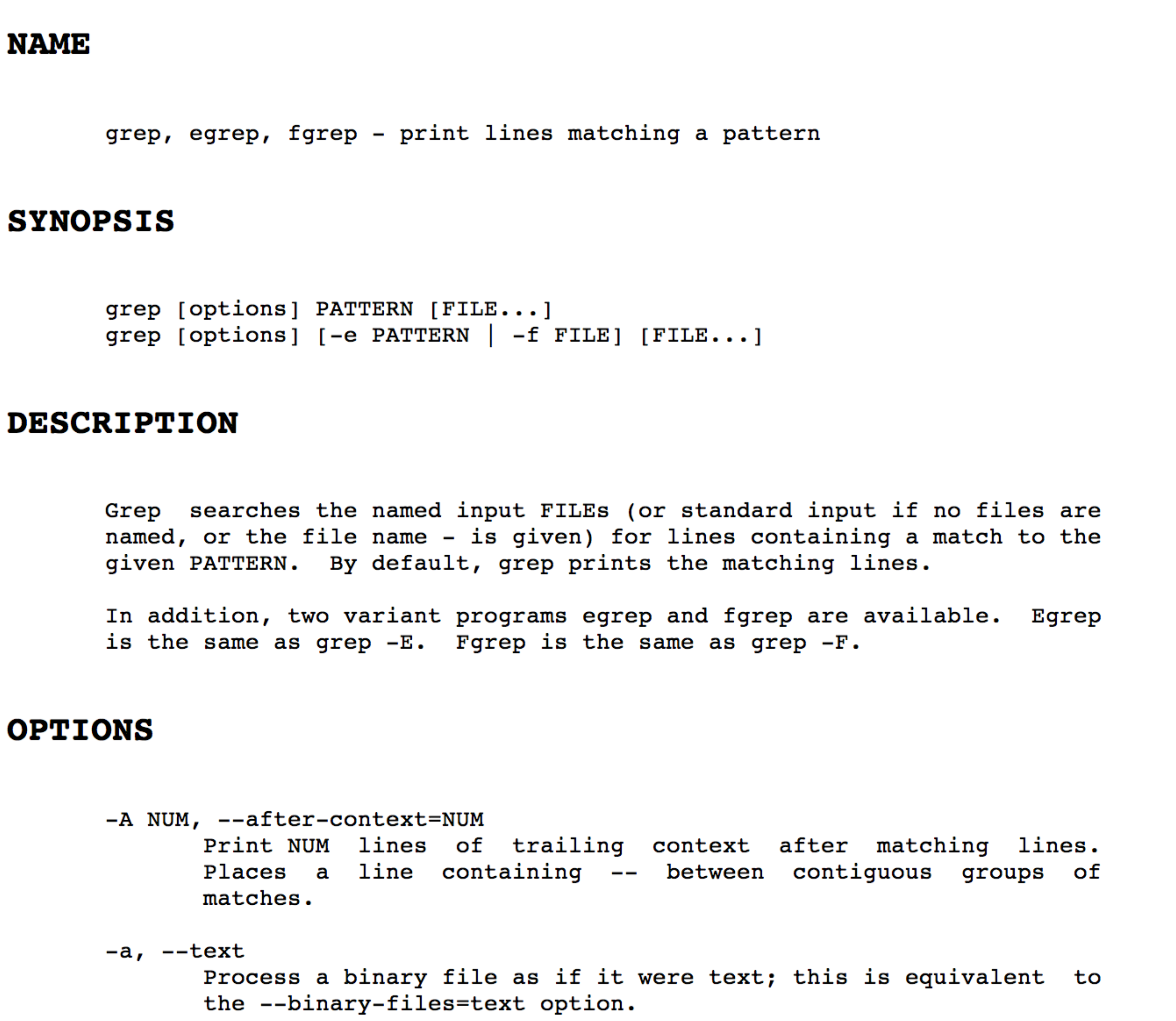
Prevent #Fails by:

- Having a centralized logging mechanism
- Having backups
- Using the same timezone for all servers
- Aggregating system and application logs

OSS Logs

- Having a centralized logging mechanism
  - **syslog-ng/rsyslog, GELF plugins**
- Having backups
  - **tar, rsync, ssh, …**
- Using the same timezone for all servers
  - **ntp**
- Aggregating system and application logs
  - **syslog-ng/rsyslog, GELF plugins**

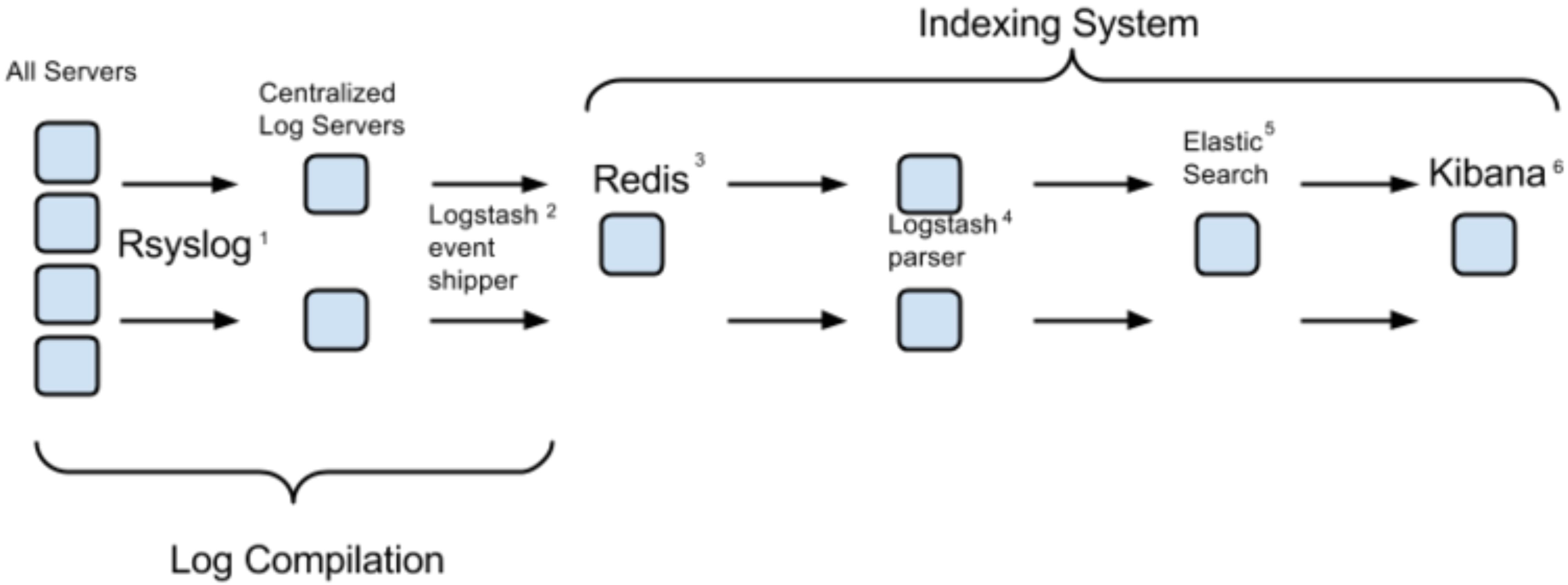
…and ‘grep’



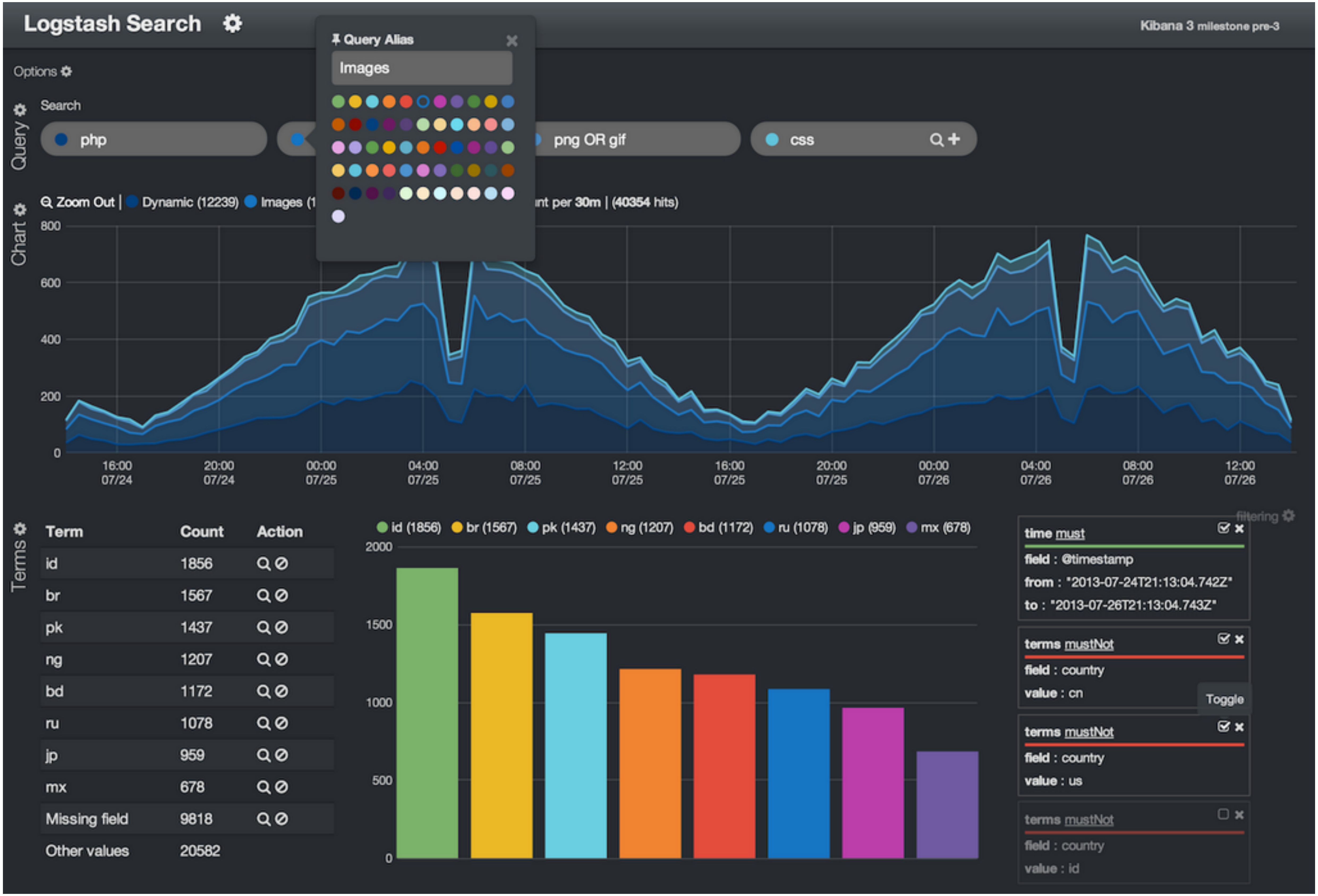
```
NAME

       grep, egrep, fgrep - print lines matching a pattern

SYNOPSIS

       grep [options] PATTERN [FILE...]
       grep [options] [-e PATTERN | -f FILE] [FILE...]

DESCRIPTION

       Grep  searches the named input FILEs (or standard input if no files are
       named, or the file name - is given) for lines containing a match to the
       given PATTERN.  By default, grep prints the matching lines.

       In addition, two variant programs egrep and fgrep are available.  Egrep
       is the same as grep -E.  Fgrep is the same as grep -F.

OPTIONS

       -A NUM, --after-context=NUM
              Print  NUM  lines  of  trailing  context  after  matching  lines.
              Places  a  line  containing  --  between  contiguous  groups  of
              matches.

       -a, --text
              Process a binary file as if it were text; this is equivalent  to
              the --binary-files=text option.
```

Logstash, ElasticSearch, Kibana

- Collect, parse, index, search logs
- http://logstash.net/
- http://www.elasticsearch.org/
- ELK stack now available for download



Logstash, ElasticSearch, Kibana



Term	Count	Action
id	1856	🔍 ⊘
br	1567	🔍 ⊘
pk	1437	🔍 ⊘
ng	1207	🔍 ⊘
bd	1172	🔍 ⊘
ru	1078	🔍 ⊘
jp	959	🔍 ⊘
mx	678	🔍 ⊘
Missing field	9818	🔍 ⊘
Other values	20582	

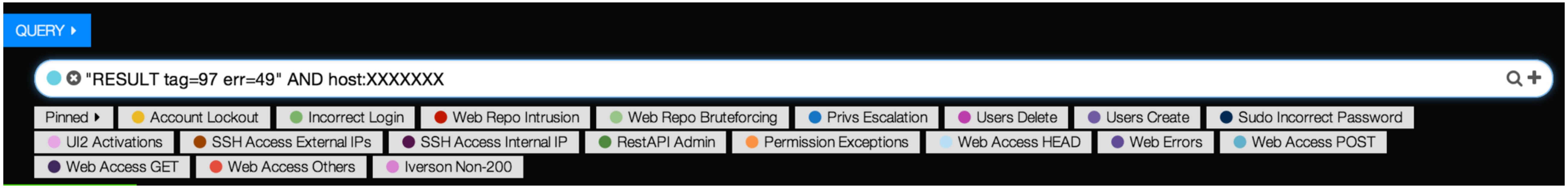
time must ☑ ✕
field : @timestamp
from : "2013-07-24T21:13:04.742Z"
to : "2013-07-26T21:13:04.743Z"

terms mustNot ☑ ✕
field : country
value : cn

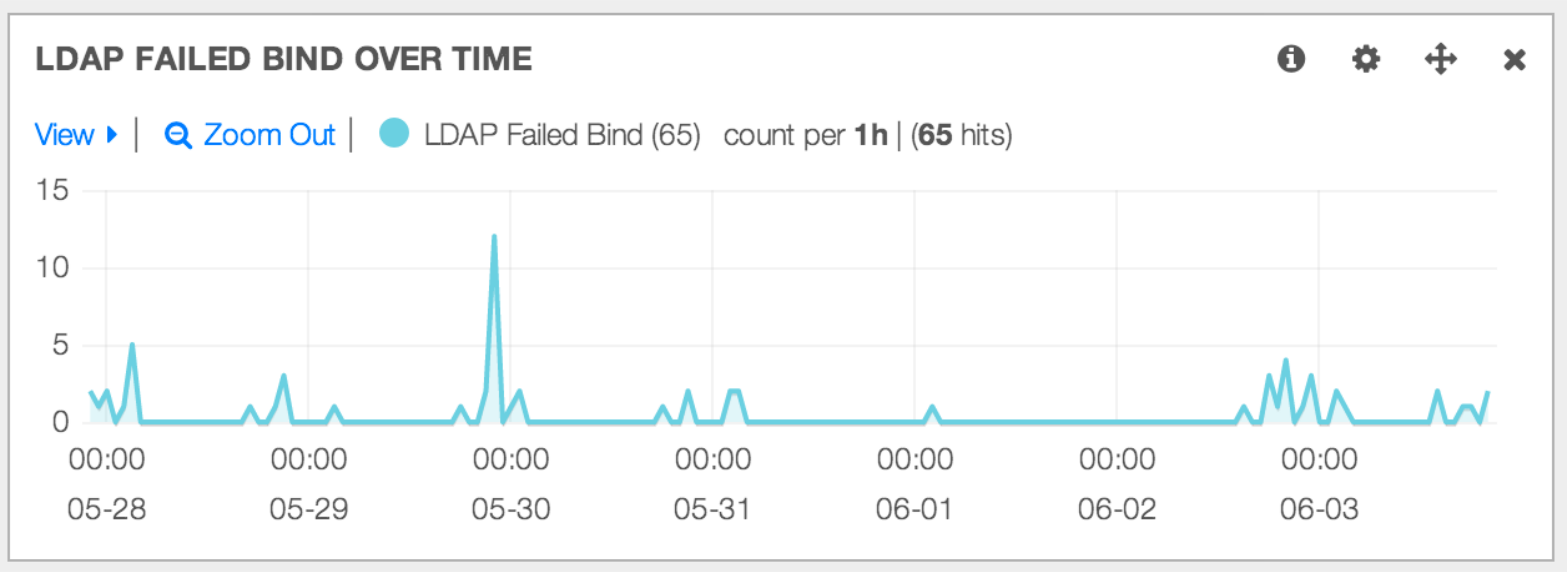
terms mustNot ☑ ✕
field : country
value : us

terms mustNot □ ✕
field : country
value : id

Logstash, ElasticSearch, Kibana



"RESULT tag=97 err=49" AND host:XXXXXXX


LDAP FAILED BIND OVER TIME

Attack surface monitoring

Continuous deployment requires continuous security:

- Determine your attack surface at a fast pace

    1. Collect all public IPs for your infrastructure
    2. Perform an Internet-facing portscan
    3. Perform services enumeration
    4. Send to InfoSec, DevOps, …
    5. Sleep 10
    6. Goto 1

Attack surface monitoring

- Collect all public IPs for your infrastructure
  - **For AWS: boto, cli53**
- Perform an Internet-facing portscan
  - **nmap**
- Perform services enumeration
  - **nmap**

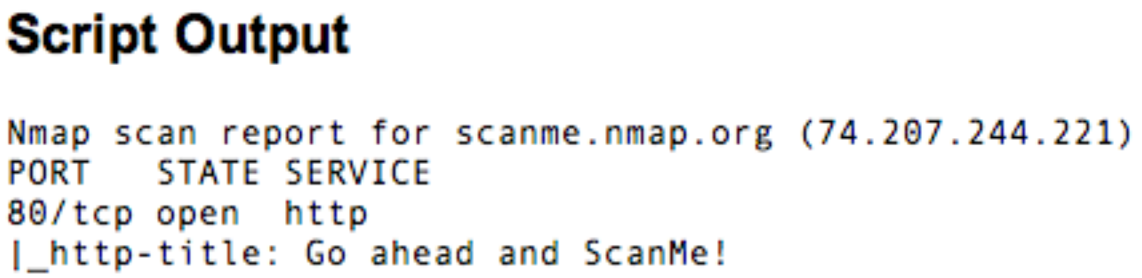
NMAP Pro Tips

- NMAP is a powerful tool with many settings
- http://nmap.org/, http://nmap.org/nsedoc/categories/default.html
- You can enhance it using **Nmap Scripting Engine**
    - Set of libraries/scripts built on top of standard LUA libs
        - 479 scripts, 111 libraries

```
#!/bin/bash
dirout=`date +%s`;
mkdir “/data/scans/$dirout”;

for i in `cat $1`; do
echo "Scanning $i"
nmap -sS -P0 -T4 -p- --script addepar-versioning.nse -oN /data/scans/$dirout/$i.tcp $i
echo "-----------------------------"
nmap -sU -P0 -T4 -F -oN /data/scans/$dirout/$i.udp $i
echo "-----------------------------"
done
```

NMAP Pro Tips

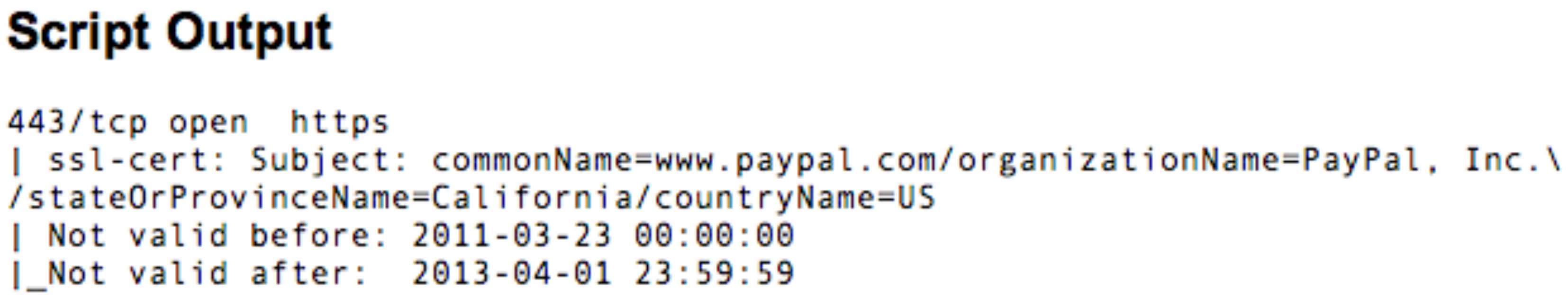
http-title.nse



Script Output

```
Nmap scan report for scanme.nmap.org (74.207.244.221)
PORT   STATE SERVICE
80/tcp open  http
|_http-title: Go ahead and ScanMe!
```

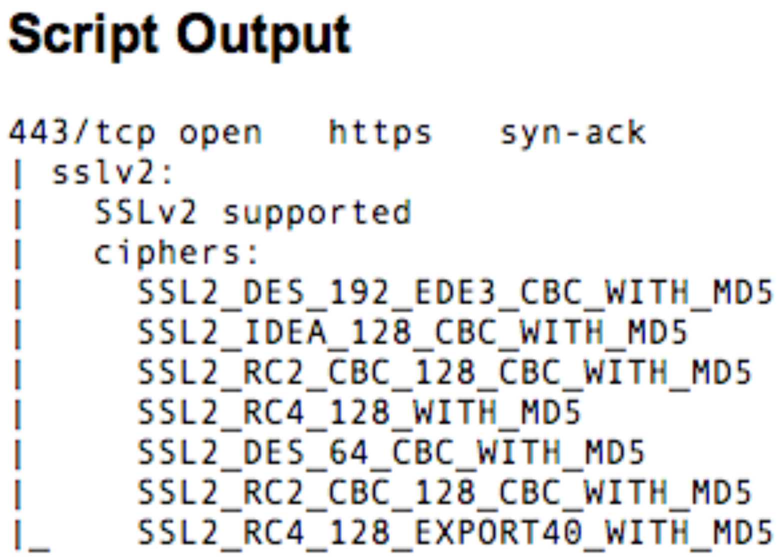
ssl-cert.nse



Script Output

```
443/tcp open  https
| ssl-cert: Subject: commonName=www.paypal.com/organizationName=PayPal, Inc.\
/stateOrProvinceName=California/countryName=US
| Not valid before: 2011-03-23 00:00:00
|_Not valid after:  2013-04-01 23:59:59
```

sslv2.nse

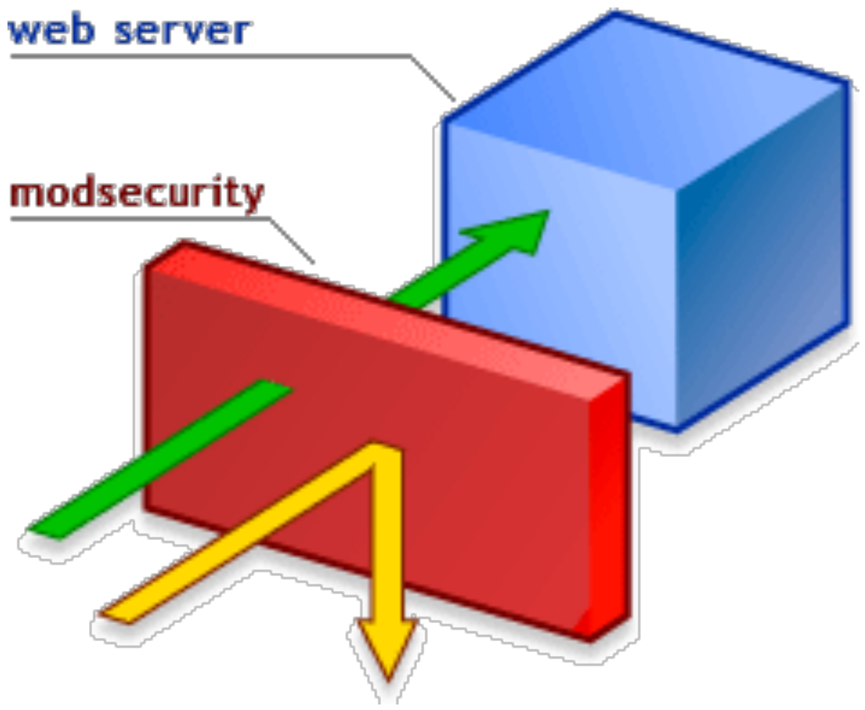


Script Output

```
443/tcp open   https   syn-ack
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_IDEA_128_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_CBC_128_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
```

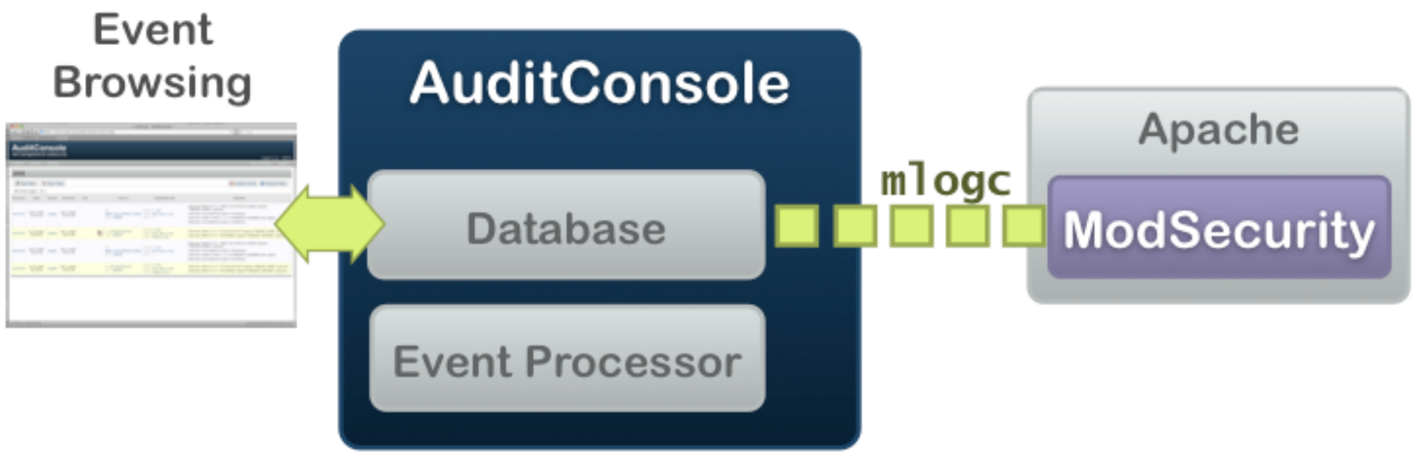
ModSecurity

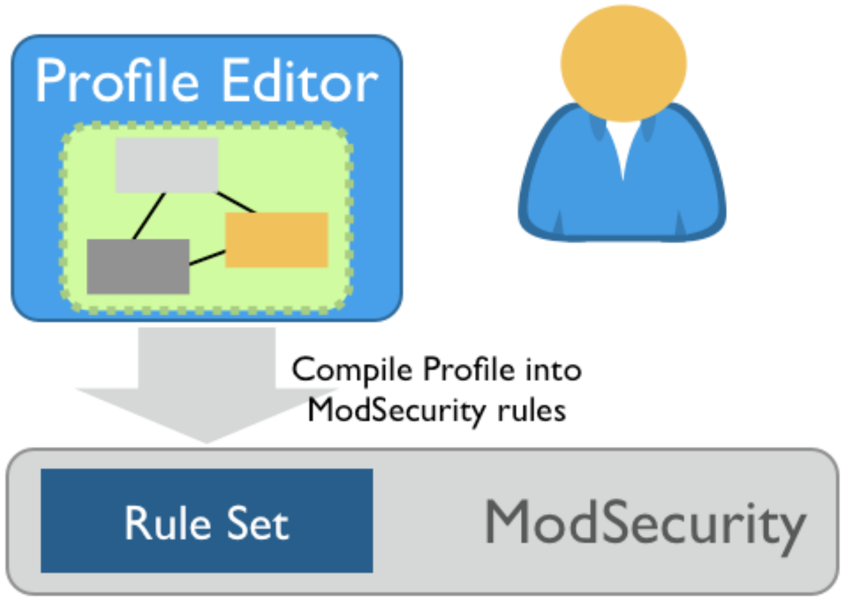
- **OpenSource Web Application Firewall**
  - https://www.modsecurity.org/
  - Supports Apache, Nginx and IIS
  - RegExp-based rules
  - Many use cases:
    - Filtering, online patching, data exfiltration prevention, …



ModSecurity ecosystem

- OpenSource Rules
    - OWASP Core Rules - https://github.com/SpiderLabs/owasp-modsecurity-crs
- Rules editors, logging and auditing tools





Thank You

- Questions?