
meetup

“I admit it’s getting better,
a little better all the time.
It can’t get more worse!”

- The Beatles

CONTINUOUS SECURITY

Continuous Delivery Amsterdam - October 2017

HELLO!

I am Arjan Gelderblom

I can be reached at

a.gelderblom@first8.nl

https://keybase.io/bloged


KAUAI
BRUCON


FIRST 8

WHY?

Why burden developers with security?

“To a hacker, you're just an IP address. You get hit because you let yourself be an easy mark.”

- Ira Winkler

Software Development Life Cycle

design

code

test

deploy

Software Development Life Cycle

design

code

test

deploy

Software Development Life Cycle

design

code

test

deploy

DEVSECOPS

Adding Sec to DevOps

stackoverflow

https://www.helpnetsecurity.com/2017/10/03/secure-coding-java/

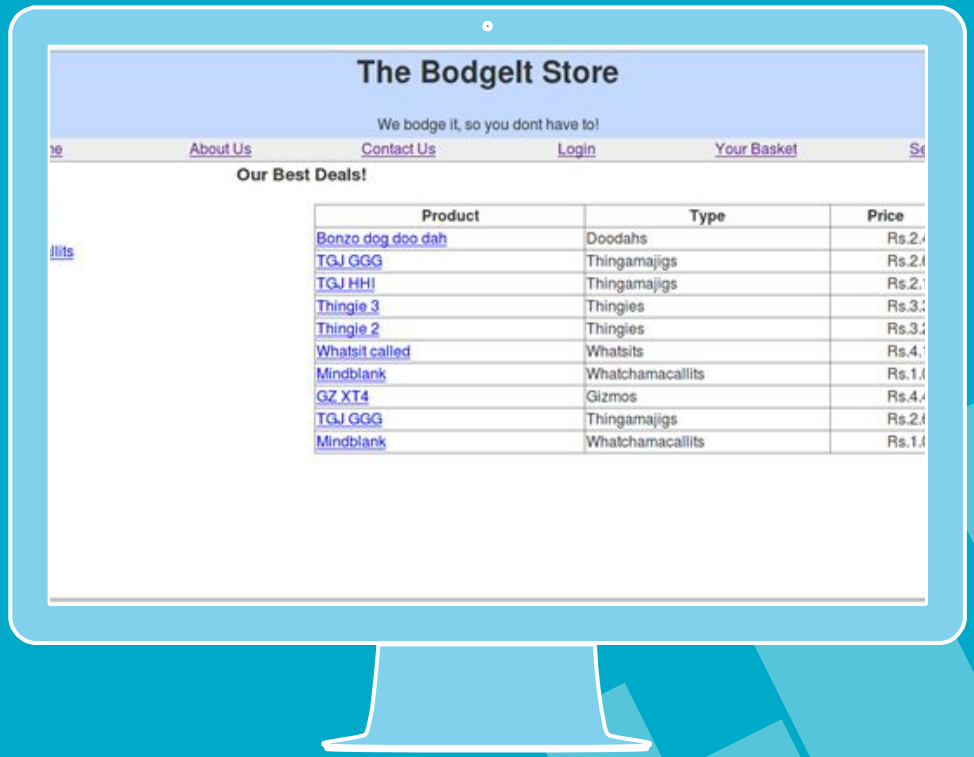
Secure or not?

```
public static int stringCompare(String orig, String input) {
    char[] charArray1 = orig.toCharArray();
    char[] charArray2 = input.toCharArray();

    int length = charArray2.length;

    int k = 0;
    while (k < lim) {
        if (charArray1[k] != charArray2[k]) {
            return charArray1[k] - charArray2[k];
        }
        k++;
    }
    return 0;
}
```

https://embedi.com/files/white-papers/silent-bob-is-silent.pdf

STARTING POINT

The Bodgeit Store



https://github.com/psiinon/bodgeit

OUR INITIAL PIPELINE

SOURCE CODE

You Built a Slack Bot

TO READ YOUR TEAM THE NEWS

and It Told Everyone Everything

http://observer.com/2016/04/slack-bot-benedict-arnold/
https://labs.detectify.com/2016/04/28/slack-bot-token-leakage-exposing-business-critical-information/

```
"text": "<!here|@here> You can use my email for the XXXXXXX, and `AwezGrowth` as the password.",
"permalink": "https://xxxxxxx.slack.com/archives/dev-growth/p14573712121219",
"user": "U06A19PDF",
"username": "flarsson",
```


Executable File

```
1  #!/bin/ba
```


```
{"type":"message","user":"U0552AAL9","username":"way","ts":"1450309434.000164","text":"<@U01AUU
A2BA>: what's the vimeo password again?","channel":

"next":{"user":"U01AUUA2BA","username":"jen","ts":"1450309910.000165","type":"message","text":"
banana12"}
```


'8d408"

```
8  heroku config:add HUBOT_SLACK_TOKEN="xoxp-2446364950-2445644913-25778          3a"
```

Tree: 92 16... / Procfile

Wiring

1 contributor


```
{"title":"","value":"hey there! to connect to our database, here is the connection info. Host:
X.X.X.X Username: fala-ade23 password: csAdd12dsw Database: dms_all_125","short":false}
```


2 lines (1 sloc) | 139 Bytes | Raw | Blame | History

```
1  web: asana-task-bot -slack-key xoxp-2182767778-3338739518-177355          -asana-key 0/e7e6e2cb8cd646          e1 -port $PORT
```

The sensitive information in these examples has been modified or redacted

gittyleaks

Scanning source control.

https://github.com/kootenpv/gittyleaks

gittyleaks

```
node {
    stage('gittyleaks') {
            sh 'export LC_ALL=C'
            sh 'gittyleaks -l git@github.com:psiinon/bodgeit.git'
    }
}
```

gittyleaks

```
agelderblom@asterix:~/tmp.opentechday/bdd-security$ gittyleaks -l git@github.com:psiinon/bodgeit.git
```

https://asciinema.org/a/05zYKyQkOO8iidwxpPlW2jI8z

FindBugs + FindSecBugs

Static code analysis

http://findbugs.sourceforge.net/
http://find-sec-bugs.github.io/

FindBugs + FindSecBugs

```
node {
    stage('findbugs') {
        sh 'findbugs -textui target/project.jar'
    }
}
```

FindBugs + FindSecBugs

```
M D SF: Switch statement found in org.eclipse.jdt.internal.compiler.lookup.SourceTypeBinding.getNullDefault() where default case is missing  At SourceTypeBinding.java:[lines 1329-1335]
M D SF: Switch statement found in org.eclipse.jdt.internal.compiler.lookup.SourceTypeBinding.getNullDefault() where one case falls through to the next case  At SourceTypeBinding.java:[lines 1331-1334]
M V EI2: new org.eclipse.jdt.internal.compiler.ast.FieldReference(char[], long) may expose internal representation by storing an externally mutable object into FieldReference.token  At FieldReference.java:
[line 63]
M D SF: Switch statement found in org.eclipse.jdt.internal.compiler.ast.FieldReference.postConversionType(Scope) where default case is missing  At FieldReference.java:[lines 566-589]
M D SF: Switch statement found in org.eclipse.jdt.internal.compiler.ast.FieldReference.resolveType(BlockScope) where default case is missing  At FieldReference.java:[lines 645-651]
M D RCN: Redundant nullcheck of synthLocal, which is known to be non-null in org.eclipse.jdt.internal.compiler.lookup.NestedTypeBinding.addSyntheticArgumentAndField(ReferenceBinding)  Redundant null check
at NestedTypeBinding.java:[line 121]
M V EI: org.eclipse.jdt.internal.compiler.lookup.NestedTypeBinding.syntheticEnclosingInstances() may expose internal representation by returning NestedTypeBinding.enclosingInstances  At NestedTypeBinding.j
ava:[line 234]
M V EI: org.eclipse.jdt.internal.compiler.lookup.NestedTypeBinding.syntheticOuterLocalVariables() may expose internal representation by returning NestedTypeBinding.outerLocalVariables  At NestedTypeBinding
.java:[line 255]
M V EI: org.eclipse.jdt.internal.compiler.lookup.NestedTypeBinding.syntheticEnclosingInstanceTypes() may expose internal representation by returning NestedTypeBinding.enclosingTypes  At NestedTypeBinding.j
ava:[line 250]
M V EI: org.eclipse.jdt.internal.compiler.lookup.ElementValuePair.getName() may expose internal representation by returning ElementValuePair.name  At ElementValuePair.java:[line 98]
M V EI2: new org.eclipse.jdt.internal.compiler.lookup.ElementValuePair(char[], Object, MethodBinding) may expose internal representation by storing an externally mutable object into ElementValuePair.name
At ElementValuePair.java:[line 89]
M B BIT: Check for sign of bitwise operation in org.eclipse.jdt.internal.compiler.lookup.ElementValuePair.getValue(Expression)  At ElementValuePair.java:[line 77]
M V EI2: new org.eclipse.jdt.internal.compiler.lookup.AnnotationBinding(ReferenceBinding, ElementValuePair[]) may expose internal representation by storing an externally mutable object into AnnotationBindi
ng.pairs  At AnnotationBinding.java:[line 184]
M V EI: org.eclipse.jdt.internal.compiler.lookup.AnnotationBinding.getElementValuePairs() may expose internal representation by returning AnnotationBinding.pairs  At AnnotationBinding.java:[line 215]
M V EI: org.eclipse.jdt.internal.compiler.lookup.LocalTypeBinding.constantPoolName() may expose internal representation by returning LocalTypeBinding.constantPoolName  At LocalTypeBinding.java:[line 153]
M V EI: org.eclipse.jdt.internal.compiler.lookup.LocalTypeBinding.sourceName() may expose internal representation by returning LocalTypeBinding.sourceName  At LocalTypeBinding.java:[line 284]
M V EI2: org.eclipse.jdt.internal.compiler.lookup.LocalTypeBinding.setConstantPoolName(char[]) may expose internal representation by storing an externally mutable object into LocalTypeBinding.constantPoolN
ame  At LocalTypeBinding.java:[line 254]
M V EI: org.eclipse.jdt.internal.compiler.lookup.BinaryTypeBinding.availableMethods() may expose internal representation by returning BinaryTypeBinding.methods  At BinaryTypeBinding.java:[line 345]
M V EI: org.eclipse.jdt.internal.compiler.lookup.BinaryTypeBinding.typeVariables() may expose internal representation by returning BinaryTypeBinding.typeVariables  At BinaryTypeBinding.java:[line 1821]
M V EI: org.eclipse.jdt.internal.compiler.lookup.BinaryTypeBinding.fields() may expose internal representation by returning BinaryTypeBinding.fields  At BinaryTypeBinding.java:[line 910]
M V EI: org.eclipse.jdt.internal.compiler.lookup.BinaryTypeBinding.methods() may expose internal representation by returning BinaryTypeBinding.methods  At BinaryTypeBinding.java:[line 1352]
M V EI: org.eclipse.jdt.internal.compiler.lookup.BinaryTypeBinding.memberTypes() may expose internal representation by returning BinaryTypeBinding.memberTypes  At BinaryTypeBinding.java:[line 1324]
M V EI: org.eclipse.jdt.internal.compiler.lookup.BinaryTypeBinding.superInterfaces() may expose internal representation by returning BinaryTypeBinding.superInterfaces  At BinaryTypeBinding.java:[line 1791]
M V EI: org.eclipse.jdt.internal.compiler.lookup.BinaryTypeBinding.unResolvedFields() may expose internal representation by returning BinaryTypeBinding.fields  At BinaryTypeBinding.java:[line 1936]
M V EI: org.eclipse.jdt.internal.compiler.lookup.BinaryTypeBinding.availableFields() may expose internal representation by returning BinaryTypeBinding.fields  At BinaryTypeBinding.java:[line 285]
M D SF: Switch statement found in org.eclipse.jdt.internal.compiler.lookup.BinaryTypeBinding.scanTypeForNullDefaultAnnotation(IBinaryType, PackageBinding, BinaryTypeBinding) where default case is missing
At BinaryTypeBinding.java:[lines 1683-1688]
M V EI2: new org.eclipse.jdt.internal.compiler.ast.MemberValuePair(char[], int, int, Expression) may expose internal representation by storing an externally mutable object into MemberValuePair.name  At Mem
berValuePair.java:[line 42]
M V EI: org.eclipse.jdt.internal.compiler.ast.SingleMemberAnnotation.memberValuePairs() may expose internal representation by returning SingleMemberAnnotation.singlePairs  At SingleMemberAnnotation.java:[l
ine 50]
H C RpC: Repeated conditional test in org.apache.tomcat.websocket.WsSession.removeMessageHandler(MessageHandler)  At WsSession.java:[line 315]
H C RpC: Repeated conditional test in org.apache.tomcat.websocket.WsSession.removeMessageHandler(MessageHandler)  At WsSession.java:[line 321]
```

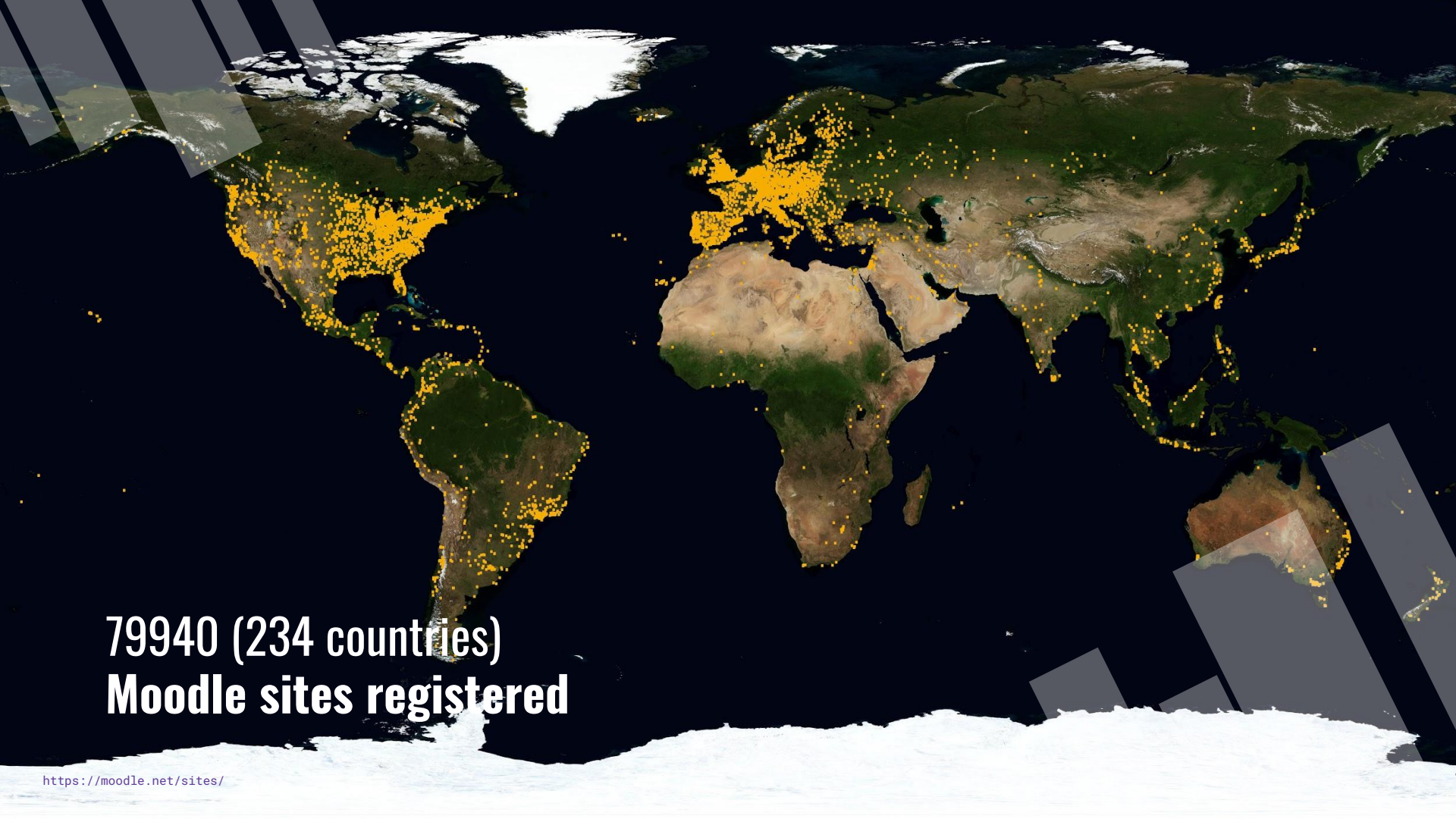
https://asciinema.org/a/8vgl8gsfj1qhevnr9c6285gkf

CURRENT PIPELINE

TESTING

Ever wanted to hack a University?

http://netanelrub.in/2017/03/20/moodle-remote-code-execution/
https://threatpost.com/critical-moodle-vulnerability-could-lead-to-server-compromise/124446/



https://moodle.net/sites/

ZAPROXY

ZED Attack Proxy

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

ZAPROXY

ZED Attack Proxy

```
node {
    stage('zap-baseline') {
        sh 'docker run -t owasp/zap2docker-stable zap-baseline.py -t http://172.17.0.2:8080/bodgeit'
    }
}
```

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

ZAPROXY

ZED Attack Proxy

```
agelderblom@asterix:~$ docker run -t owasp/zap2docker-stable zap-baseline.py -t http://172.17.0.2:8080/bodgeit
_XSERVTransmkdir: ERROR: euid != 0,directory /tmp/.X11-unix will not be created.
Apr 19, 2017 6:29:17 PM java.util.prefs.FileSystemPreferences$1 run
INFO: Created user preferences directory.
```

https://asciinema.org/a/1s2telu6m7vsd4uzxoursd8pt

gauntlt

Be Mean To Your Code And Like It

gauntlt

```
@slow
Feature: simple nmap attack (sanity check)

  Background:
       Given "nmap" is installed
       And the following profile:
       | name  | value        |
       | hostname | 172.17.0.2 |

  Scenario: Verify server is available on standard web ports
       When I launch an "nmap" attack with:
       """
       nmap -p 8080,443 <hostname>
       """
       Then the output should match /8080.tcp\s+open/
       And the output should not match:
       """
       443/tcp\s+open
"""
```

gauntlt

```
node {
    stage('gauntlt') {
        sh 'gauntlt custom/*/*.attack'
    }
}
```

gauntlt

https://asciinema.org/a/2tfc8bfzygw6j6xvjgn2pvnia

inspec

Inspect Your Infrastructure

inspec

```
title '/port-8080 open'

# you add controls here
control "port 8080" do                          # A unique ID for this control
  impact 0.7                                    # The criticality, if this control fails.
  title "Port 8080 should be listening"         # A human-readable title
  desc "Checking the port public port ..."      # Describe why this is needed
  tag data: "port"                              # A tag allows you to associate key
  tag "security"                                # information to the test
  ref "Document A-12", url: 'http://...'        # Additional references

  describe port(8080) do                        # Actual test
       it { should be_listening }
  end
end
```

https://github.com/chef/inspec/blob/master/docs/profiles.md

inspec

```
node {
    stage('inspec') {
        sh 'inspec exec inspec/example/ -t docker://f782c7f0a177'
    }
}
```

inspec

https://asciinema.org/a/4ft5iso3jhu8vbh6shnatr1nk

BDD Security

Security Testing Framework

```
@cwe-295-auth
Scenario: Present the login form itself over an HTTPS connection
  Given a new browser instance
  And the client/browser is configured to use an intercepting proxy
  And the proxy logs are cleared
  And the login page is displayed
  And the HTTP request-response containing the login form
  Then the protocol should be HTTPS
```

https://www.continuumsecurity.net/bdd-security/

BDD Security

BDD-Security

```
144156 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Format String Error
144156 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin CRLF Injection
144156 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Parameter Tampering
144156 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Cross Site Scripting (Persistent) - Prime
144156 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Cross Site Scripting (Persistent) - Spider
144156 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Script Active Scan Rules
144156 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Source Code Disclosure - SVN
144156 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Source Code Disclosure - /WEB-INF folder
144156 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Remote Code Execution - Shell Shock
144156 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Anti CSRF Tokens Scanner
144156 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Heartbleed OpenSSL Vulnerability
144156 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Cross-Domain Misconfiguration
144157 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Source Code Disclosure - CVE-2012-1823
144157 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Remote Code Execution - CVE-2012-1823
144157 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Session Fixation
144157 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin SQL Injection - MySQL
144157 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin SQL Injection - Hypersonic SQL
144157 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin SQL Injection - Oracle
144157 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin SQL Injection - PostgreSQL
144157 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin [illegible] Injection
144157 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin [illegible] External Entity Attack
144157 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin [illegible] Padding Oracle
144157 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin [illegible] Session Language Injection
144157 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Backup File Disclosure
144157 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Integer Overflow Error
144157 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Insecure HTTP Method
144157 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin HTTP Parameter Pollution scanner
144158 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Possible Username Enumeration
144158 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Source Code Disclosure - Git
144158 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Source Code Disclosure - File Inclusion
144158 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Httpoxy - Proxy Header Misuse
144158 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin LDAP Injection
144158 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin SQL Injection - SQLite
144158 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Example Active Scanner: Denial of Service
144158 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin An example active scan rule which loads data from a file
144158 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Relative Path Confusion
144158 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin User Agent Fuzzer
144158 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin HTTP Only Site
144158 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Proxy Disclosure
144158 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin HTTPS Content Available via HTTP
144158 [ZAP-ProxyThread-74] INFO org.parosproxy.paros.core.scanner.PluginFactory  - loaded plugin Cookie Slack Detector
> Building 84% > :test > 185 tests completed, 28 failed, 112 skipped
```

https://asciinema.org/a/8ixx15uydulugvw1syohgb03g

beaker

Cloud enabled acceptance testing

https://github.com/puppetlabs/beaker

CURRENT PIPELINE

Maven

BDD-Security

ZAPROXY

checkout | analysis | build | test | deploy

EXTERNAL DEPENDENCIES

https://en.wikipedia.org/wiki/Equifax#May.E2.80.93July_2017_security_breach

OpenVAS

Vulnerability scanning and vulnerability management

Dashboard

Tasks by Severity Class (Total: 0)

Tasks by status (Total: 0)

CVEs by creation time (Total: 0)

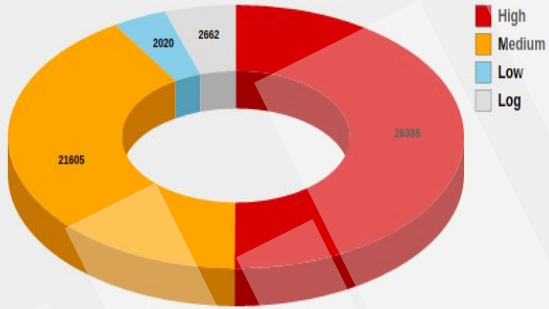
CVEs *Total CVEs*

Want big impact?
USE BIG IMAGE.

Hosts topology

No hosts with topology selected

NVTs by Severity Class (Total: 52672)



cvechecker

Vulnerability scanning and vulnerability management

https://github.com/sjvermeu/cvechecker

cvechecker

```
node {
    stage('cvechecker') {
        sh 'find / -type f -perm -o+x > scanlist.txt'
        sh 'echo "/proc/version" >> scanlist.txt'
        sh 'cvechecker -b scanlist.txt'
        sh 'cvechecker -r'
    }
}
```

https://github.com/sjvermeu/cvechecker

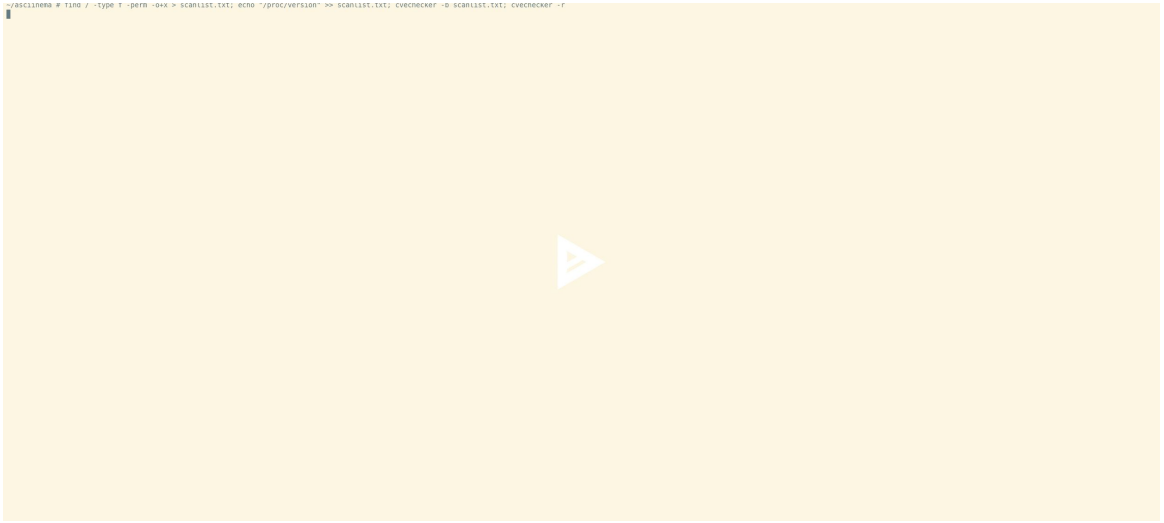
cvechecker

```
# find / -type f -perm -o+x > scanlist.txt; echo "/proc/version" >> scanlist.txt; cvechecker -b scanlist.txt; cvechecker -r
find: `/proc/2998/task/2998/fd/5': No such file or directory
find: `/proc/2998/task/2998/fdinfo/5': No such file or directory
find: `/proc/2998/fd/5': No such file or directory
find: `/proc/2998/fdinfo/5': No such file or directory
Searching for known software titles...
 - Found match for /usr/bin/rpcgen:     cpe:/a:gnu:glibc:2.19:::
 - Found match for /usr/bin/mkfifo:     cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/head:       cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/chcon:      cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/perlivp:    cpe:/a:perl:perl:5.20.2:::
 - Found match for /usr/bin/csplit:     cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/gencat:     cpe:/a:gnu:glibc:2.19:::
 - Found match for /usr/bin/id: cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/cksum:      cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/unzip:      cpe:/a:info-zip:unzip:1.0:::
 - Found match for /usr/bin/nohup:      cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/base64:     cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/tee:        cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/chattr:     cpe:/a:ext2_filesystems_utilities:e2fsprogs:1.42.12:::
 - Found match for /usr/bin/groups:     cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/gpg-zip:    cpe:/a:gnupg:gnupg:1.4.18:::
 - Found match for /usr/bin/du: cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/shuf:       cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/as: cpe:/a:gnu:binutils:2.25:::
 - Found match for /usr/bin/join:       cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/zipinfo:    cpe:/a:info-zip:zip:4.9.2:::
 - Found match for /usr/bin/install:    cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/cut:        cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/expand:     cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/make:       cpe:/a:gnu:make:4.0:::
 - Found match for /usr/bin/unzipsfx:   cpe:/a:info-zip:unzip:2.3:::
 - Found match for /usr/bin/od: cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/logname:    cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/link:       cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/dircolors:  cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/sprof:      cpe:/a:gnu:glibc:2.19:::
 - Found match for /usr/bin/uniq:       cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/xargs:      cpe:/a:gnu:findutils:4.4.2:::
 - Found match for /usr/bin/paste:      cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/oldfind:    cpe:/a:gnu:findutils:4.4.2:::
 - Found match for /usr/bin/whoami:     cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/nice:       cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/locale:     cpe:/a:gnu:glibc:2.19:::
 - Found match for /usr/bin/tty:        cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/unlink:     cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/ptx:        cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/pathchk:    cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/who:        cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/comm:       cpe:/a:gnu:coreutils:8.23:::
 - Found match for /usr/bin/getent:     cpe:/a:gnu:glibc:2.19:::
 - Found match for /usr/bin/runcon:     cpe:/a:gnu:coreutils:8.23:::
```

https://asciinema.org/a/6xtccj8r0qjihh94ui1gu92ma

https://alpinelinux.org/

Alpine Linux



https://asciinema.org/a/34ihmet34cd4ly523pfaml2uu

OWASP Dependency Check

https://www.owasp.org/index.php/OWASP_Dependency_Check

OWASP Dependency Check

```
node {
    stage('cvechecker') {
        sh 'mvn org.owasp:dependency-check-maven:1.4.5:aggregate'
    }
}
```

OWASP Dependency Check

```
agelderblom@asterix:~/tmp.opentechday/demo-insecure-project$ mvn org.owasp:dependency-check-maven:1.4.5:aggregate
[INFO] Scanning for projects...
[INFO]
[INFO] ------------------------------------------------------------------------
[INFO] Building Demo Insecure Project 1.0.0-SNAPSHOT
[INFO] ------------------------------------------------------------------------
[INFO]
[INFO] --- dependency-check-maven:1.4.5:aggregate (default-cli) @ demo-insecure-project ---
[INFO] Checking for updates
[INFO] Skipping NVD check since last check was within 4 hours.
```

https://asciinema.org/a/6ytzredroiwvifzude45n3bcm

http://www.networkworld.com/article/3162232/security/that-hearbleed-problem-may-be-more-pervasive-than-you-think.html

Updates

Base images & dependencies

OPEN INFORMATION

OWASP
Open Web Application Security Project

OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

https://www.owasp.org
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Training

OWASP WebGoat

OWASP SecurityShepherd

https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
https://www.owasp.org/index.php/OWASP_Security_Shepherd

Software Development Life Cycle

design

code

test

deploy

TAKEAWAYS

THANKS!

Any questions?

You can find me at

 a.gelderblom@first8.nl

 https://www.first8.nl/nieuws-overzicht


meetup