Exploring security in day-to-day testing

Richard Adams

About me

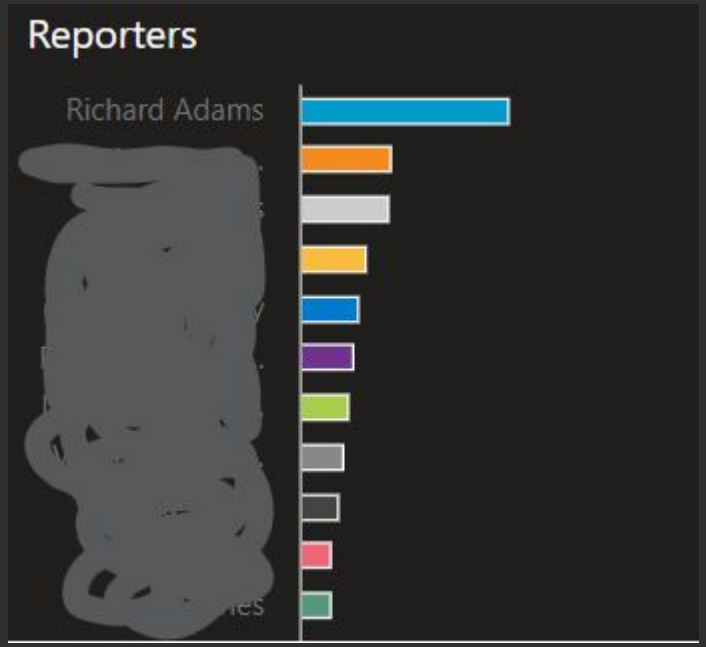
- Based in Scotland.
- Started testing in 2008.
- Had a bunch of roles & job titles.
- Work for Motorola Solutions.
- Currently have a number of hats.
  - “Cyber Champion”
  - “QA Champion”
  - Senior Quality Engineer
- Identify as manual exploratory tester.

Getting Started

My journey into security testing

I found bugs

Starting as a tester



Time to upskill

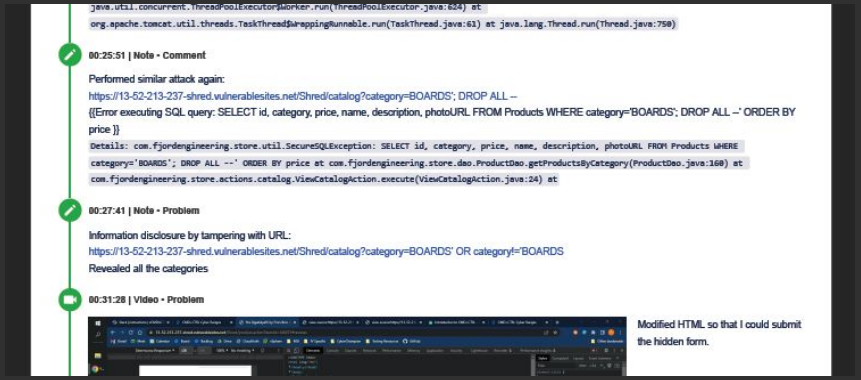
Improving as a tester

Cyber Champion

Joining Motorola Solutions Cyber Champion program

Labs and CTF

Online learning resources



What I’ve learnt

My key takeaways

- Some of this is straight forward
  - Some of this is still quite hard
- Suits me, a manual exploratory tester
- ~~I find bugs~~ I missed many bugs that I could have caught
  - I wish I’d thought like this 13-15 years ago...

Why should we invest our time?

Business Case

Why should we care?

- Bugs hit in production can hurt the business.
- Fixing bugs earlier is cheaper.
- … so the industry shifts left 😎

- Security bugs hit in production can ***really*** hurt the business.
- Fixing security bugs earlier is cheaper.
- … so the industry outsources at the end of a project? 😟

Security testing is just testing…

So let’s shift that left too!

Security testing in our day to day

Planning

Security in our day-to-day activities

- Ask questions
- Challenge assumptions.
- Look for edge cases in the design.
- Be a tester.

Scenarios

Security in our day-to-day activities

Given I am logged in as a standard user.

When I try to access the URL for the admin panel.

Then…

Given I am am viewing my order.

When I change the order number to someone else's order

Then…

URL Manipulation

`https://mysite.com/userPanel/orders/375/view`

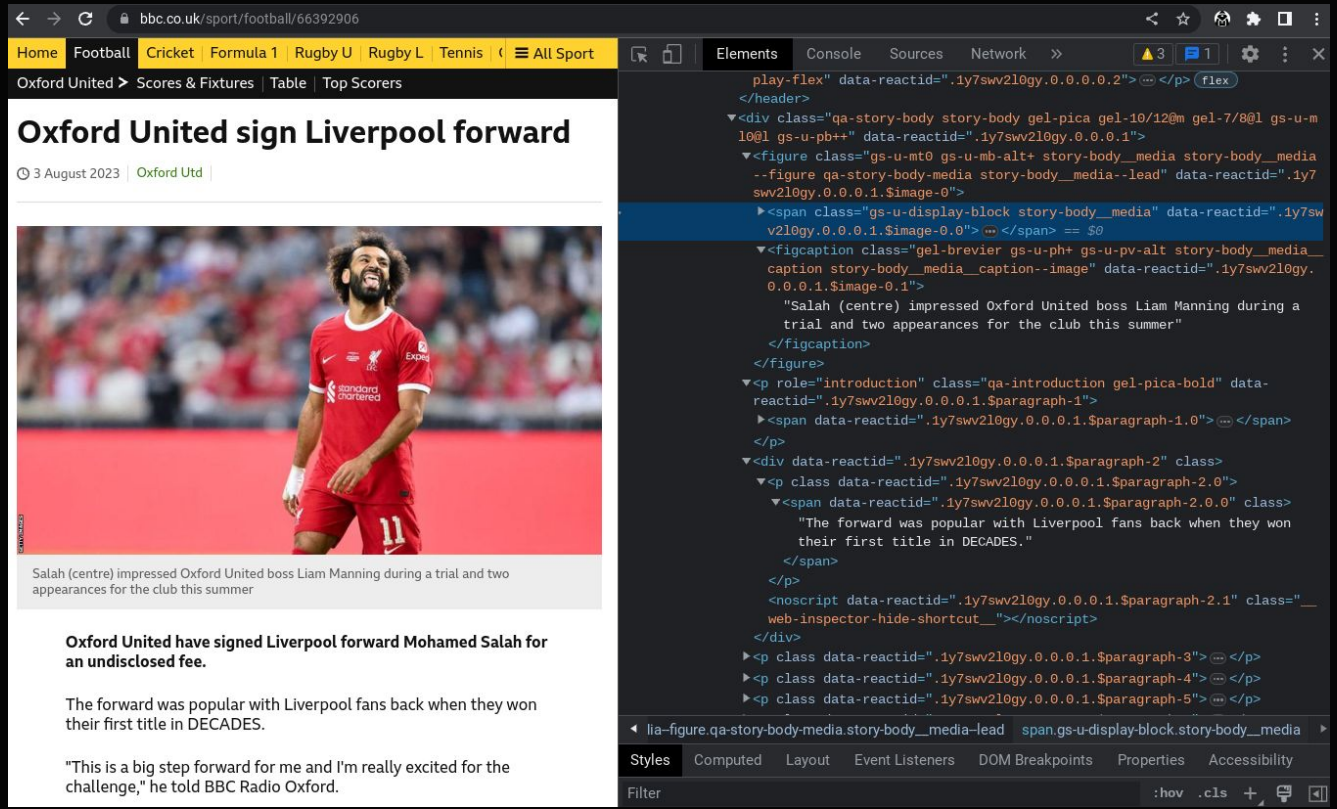
Bookmark URLs	Modify URLs	Elevation of Privileges
• Can you access them without logging in? • Can you access admin panel as normal user?	?isAdmin=false → ?isAdmin=true /user/1234/edit → /user/1122/edit /photo/567/view →/photo/567/edit	Elevation of privileges security bugs are where you can do something beyond what your user account should be allowed to do.

Test beyond UI

Security in our day-to-day activities

Bypass UI validation using your browser dev tools or custom requests

Chrome Dev Tools lets you modify HTML of pages you are viewing

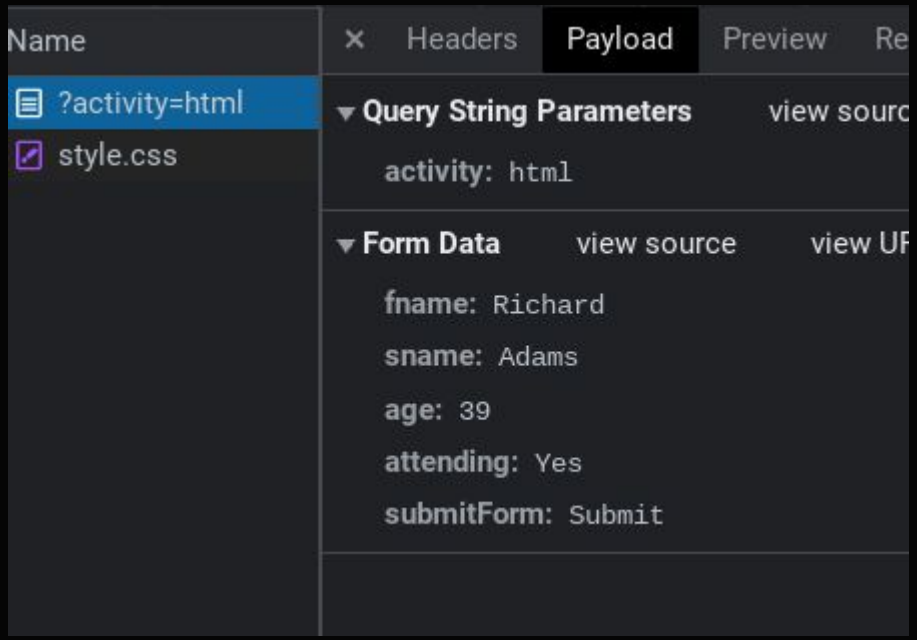


Modify the HTML (or Javascript)

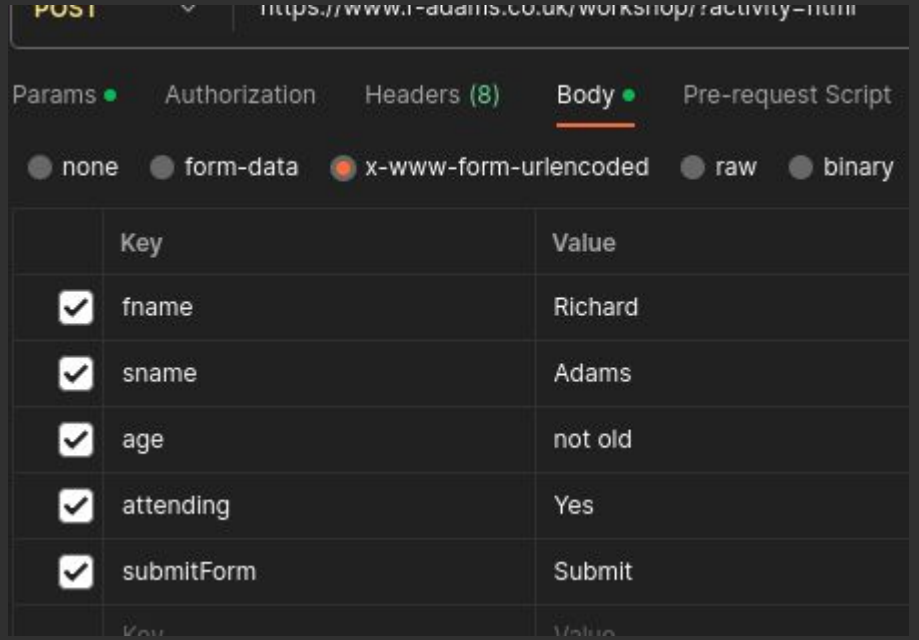
```
<h1>User Panel</h1>
▼<form method="post">
  <h2>Update your Bio</h2>
  <input name="id" type="hidden" value="2"> == $0
  <textarea name="mybio" rows="6" cols="50">Nothing but a 'lowly' user.</textarea>
  <br>
  <input name="submit" type="submit" value="Submit">
</form>
<p class="message"></p>
</div>
```

- Hidden fields can be fun to tinker with!
- Can you change a number control into a text box?
- Try removing “required” or min/max values

Chrome Dev Tools



Postman



Use Test Data

Security in our day-to-day activities

- Perform basic attacks:
  - SQL injection
  - XSS
  - Remote command injection
  - Much more
- Expand your test data
- Use cheat sheets

Part I: Override Filtering

Filter By: user GO

My code is running the following SQL command:

SELECT * FROM demo WHERE role = 'user' OR role = 'admin'

Username	Role	Comment
admin	admin	I am admin. Bow before me!
testuser	user	I am a test user, here for testing.
demo	user	My slogan

Part I: Override Filtering

Filter By: GO
You typed in: user

My code is running the following SQL command:

SELECT * FROM demo WHERE role = 'user'

Username	Role	Comment
testuser	user	I am a test user, here for testing.
demo	user	My slogan

Test Data

A great “go to” for SQL injection

Which one depends on your database tech & SQL code:

```
’ OR 1 > 0 -- comment
” OR 1 > 0 -- comment
” OR 1 > 0 # comment
```

(and a few more variations)

Part I: Override Filtering

Filter By: user' OR 1>0 -- comment GO
You typed in: user

My code is running the following SQL command:

SELECT * FROM demo WHERE role = 'user'

Username	Role	Comment
testuser	user	I am a test user, here for testing.
demo	user	My slogan

Part I: Override Filtering

Filter By: GO
You typed in: user' OR 1>0 -- comment

My code is running the following SQL command:

SELECT * FROM demo WHERE role = 'user' OR 1>0 -- comment'

Username	Role	Comment
admin	admin	I am admin. Bow before me!
Ninja1234	ninja	I am hidden in the darkness. You cannot see me.
testuser	user	I am a test user, here for testing.
demo	user	My slogan

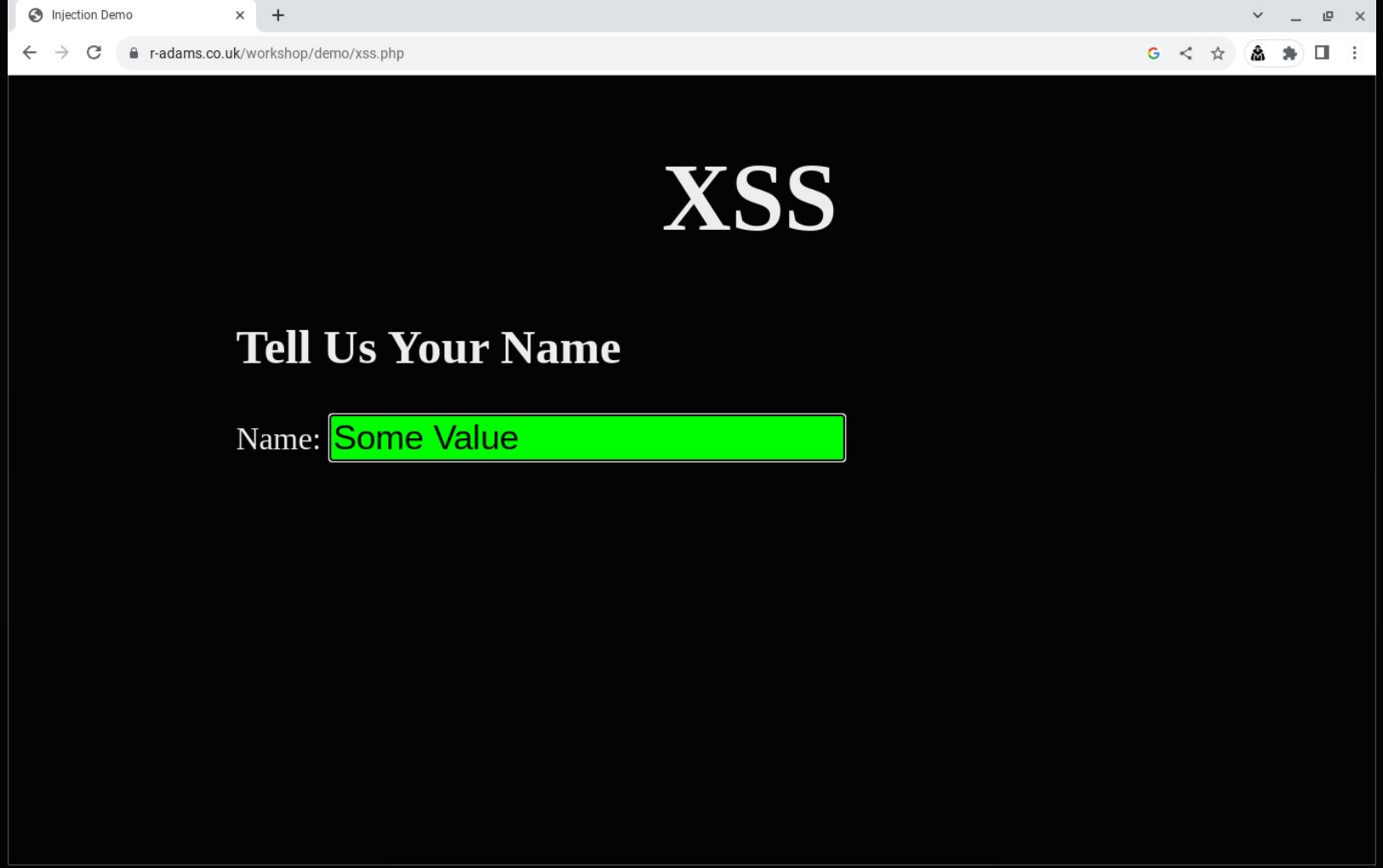
Test Data

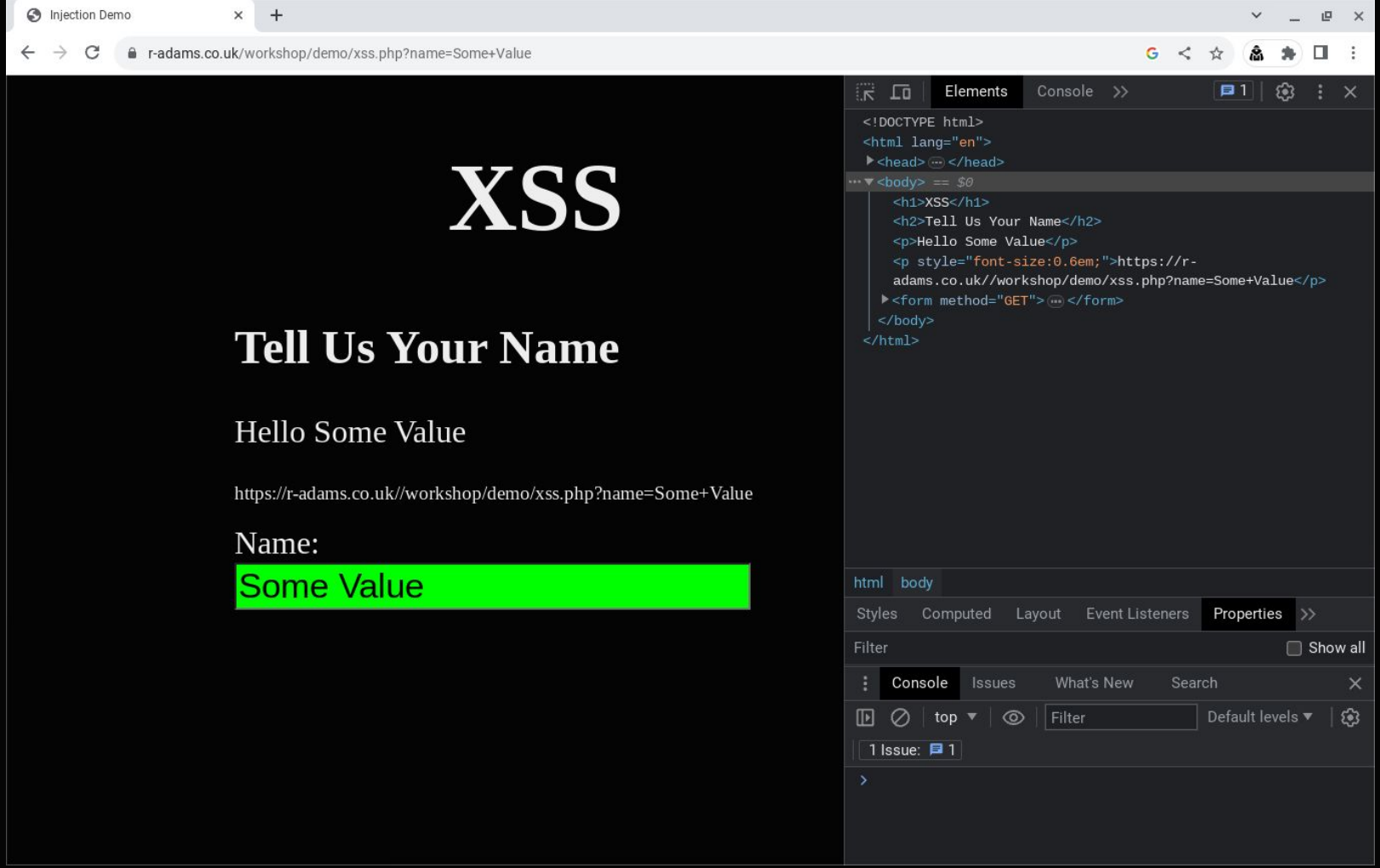
A great “go to” for XSS
(Cross Site Scripting)

Can you get an alert to pop up?

<script>alert(‘XSS’)</script>

Lots of variations available


Injection Demo
r-adams.co.uk/workshop/demo/xss.php
XSS
Tell Us Your Name
Name:
Some Value


Injection Demo
r-adams.co.uk/workshop/demo/xss.php?name=Some+Value
XSS
Tell Us Your Name
Hello Some Value
https://r-adams.co.uk//workshop/demo/xss.php?name=Some+Value
Name:
Some Value
Elements
Console
<!DOCTYPE html>
<html lang="en">
<head> </head>
<body> == $0
<h1>XSS</h1>
<h2>Tell Us Your Name</h2>
Hello Some Value
https://r-adams.co.uk//workshop/demo/xss.php?name=Some+Value
<form method="GET"> </form>
</body>
</html>
html
body
Styles
Computed
Layout
Event Listeners
Properties
Filter
Show all
Console
Issues
What's New
Search
top
Filter
Default levels
1 Issue: 1

Using our test data

We find a XSS bug

Tools

Security in our day-to-day activities

- Point scanners at your environment
  - Tenable Nessus
  - Open VAS
- Use tools to look for potential defects in running web app

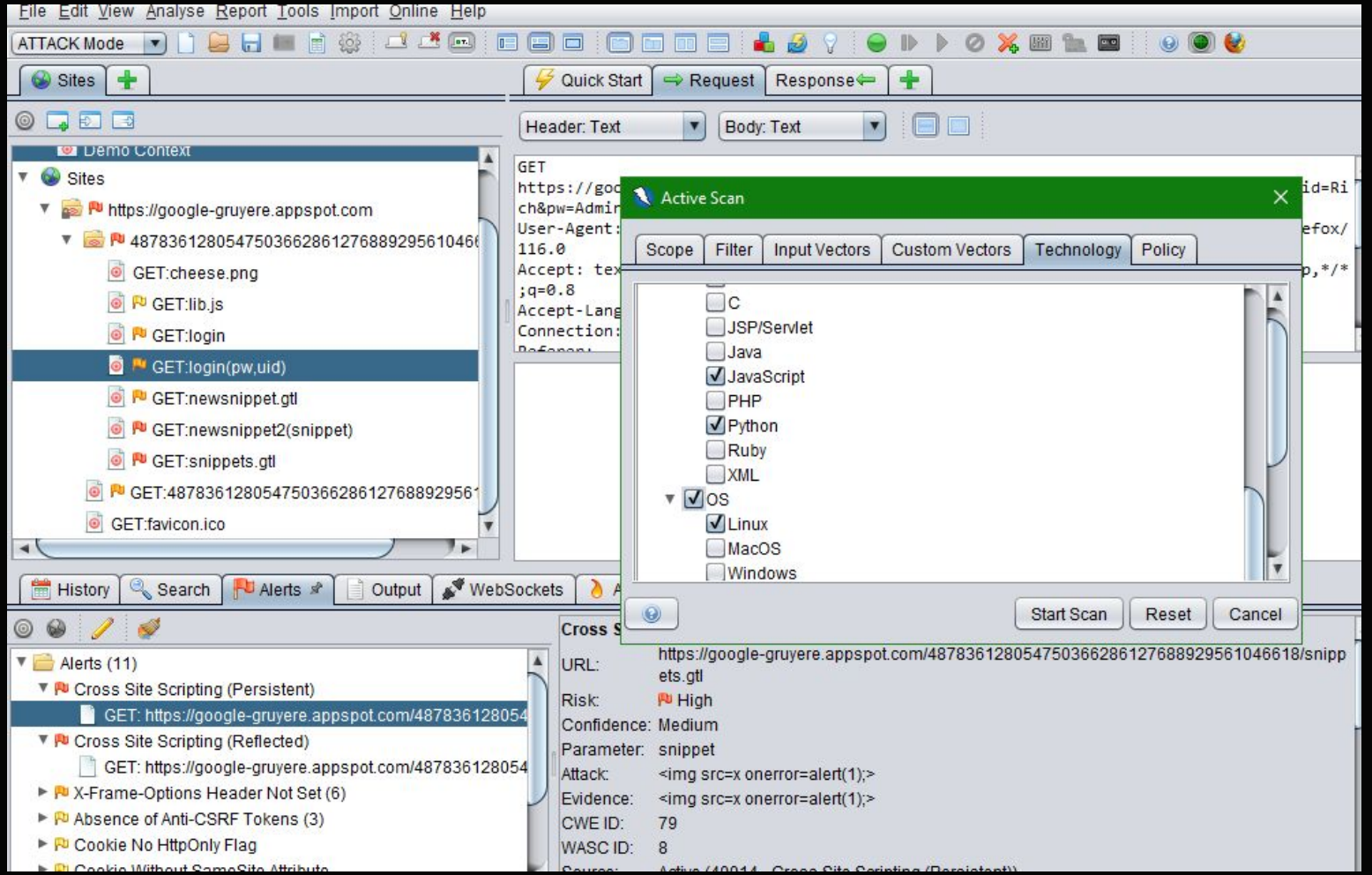
SSP ZAP

Zed Attack Proxy
Formerly OWASP ZAP

- Available for free
- https://www.zaproxy.org/
- Use it during standard testing.
- Monitor the pages to spot vulnerabilities.
- Attack mode will proactively make attacks.
- An alternative is Burp Suite
- Also OWASP Pen Test Kit browser extension

WARNING: Don’t use attack mode in production!

WARNING: It is not user friendly.

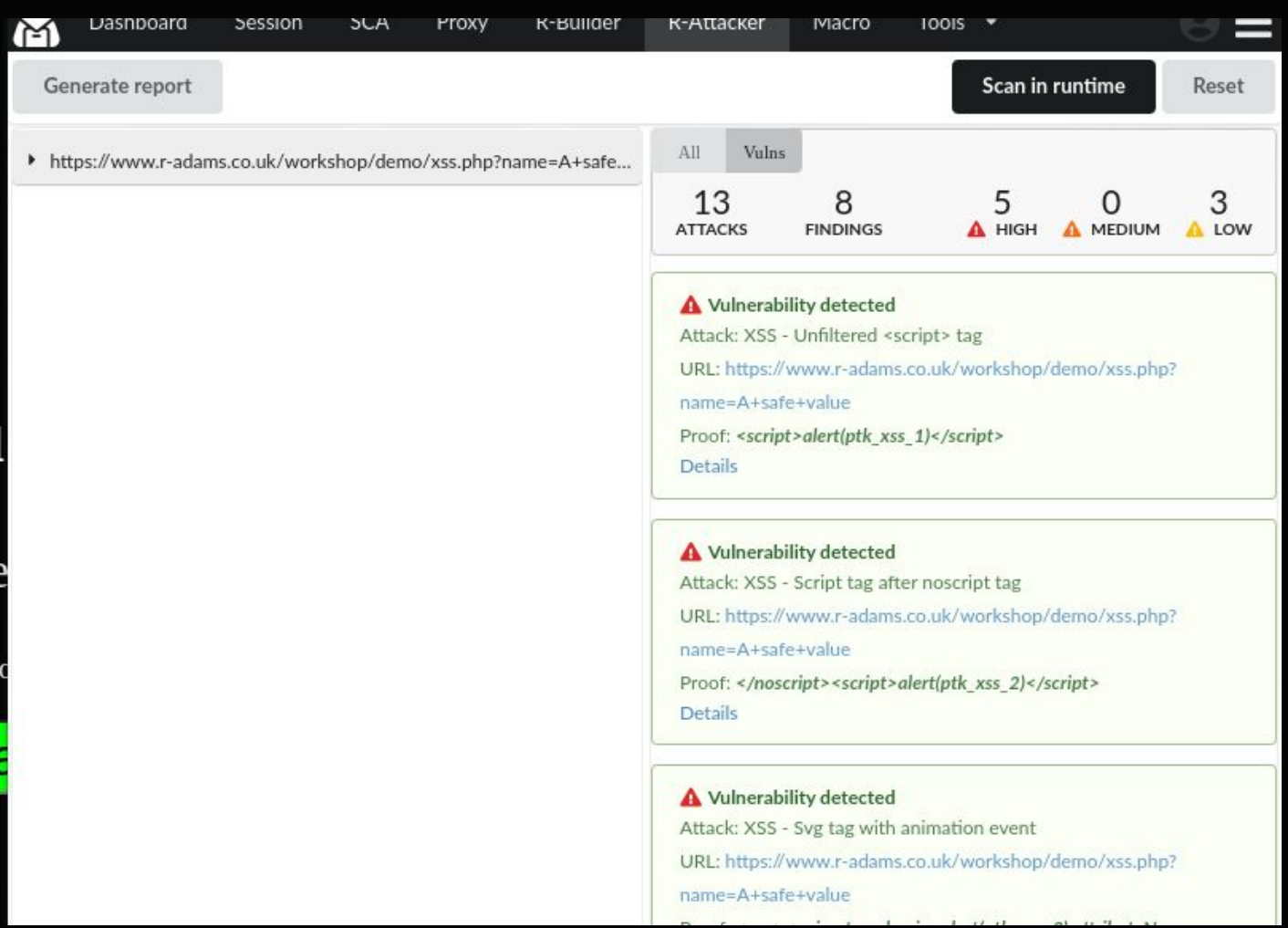

File Edit View Analyse Report Tools Import Online Help
ATTACK Mode
Sites
Quick Start
Request
Response
Header: Text
Body: Text
Demo Context
Sites
https://google-gruyere.appspot.com
GET:cheese.png
GET:lib.js
GET:login
GET:login(pw,uid)
GET:newsnippet.gtl
GET:newsnippet2(snippet)
GET:snippets.gtl
GET:favicon.ico
Active Scan
Scope
Filter
Input Vectors
Custom Vectors
Technology
Policy
C
JSP/Servlet
Java
JavaScript
PHP
Python
Ruby
XML
OS
Linux
MacOS
Windows
Start Scan
Reset
Cancel
History
Search
Alerts
Output
WebSockets
Alerts (11)
Cross Site Scripting (Persistent)
GET: https://google-gruyere.appspot.com/487836128054
Cross Site Scripting (Reflected)
GET: https://google-gruyere.appspot.com/487836128054
X-Frame-Options Header Not Set (6)
Absence of Anti-CSRF Tokens (3)
Cookie No HttpOnly Flag
URL: https://google-gruyere.appspot.com/48783612805475036628612768892956104661 8/snippets.gtl
Risk: High
Confidence: Medium
Parameter: snippet
Attack: <img src=x onerror=alert(1);>
Evidence: <img src=x onerror=alert(1);>
CWE ID: 79
WASC ID: 8

Tell Us You

Hello A safe value

https://r-adams.co.uk//worksho

Name: A safe va



Let’s pull this all together

Starting point for security testing

Question security in planning

Use Chrome Dev Tools to explore beyond what is shown on page.

Add SQL injection & XSS etc to your test data - cheat sheets are available online!

Use SSP ZAP to do a lot of the work for you!

Practice & learn

Use free resources to practice

OWASP Juice Shop

Google Gruyere

HackThisSite.org

Rich Adams Security Testing Activities

… and many more

Thank you!

Workshop @ 9am :: AMA @ 2pm