

Exploring security in day-to-day testing

Richard Adams

About me

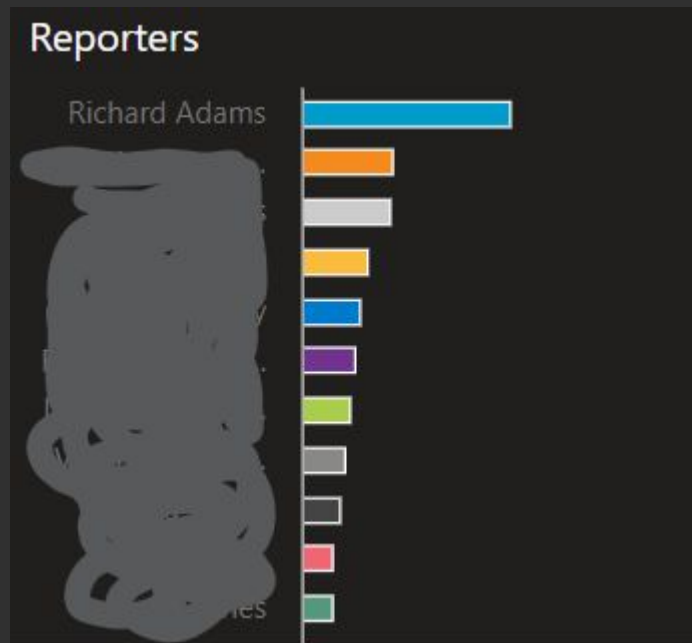
- Based in Scotland.
- Started testing in 2008.
- Had a bunch of roles & job titles.
- Work for Motorola Solutions.
- Currently have a number of hats.
 - “Cyber Champion”
 - “QA Champion”
 - Senior Quality Engineer
- Identify as manual exploratory tester.

Getting Started

My journey into security testing

I found bugs

Starting as a tester



Time to upskill

Improving as a tester



MINISTRY OF TESTING

Cyber Champion

Joining Motorola Solutions
Cyber Champion program



Labs and CTF

Online learning resources

CMD+CTRL REGIONAL WINNERS					
TEAM	RANK	NAME	REGION	POINTS	CHALLENGES
			NA	7045	30
			NA	6095	27
			NA	5145	25
		Richard Adams	EMEA	6095	27
			EMEA	5445	27
			EMEA	4295	21

```
java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:634) at  
org.apache.tomcat.util.threads.TaskThread$WrappingRunnable.run(TaskThread.java:63) at java.lang.Thread.run(Thread.java:759)
```



00:25:51 | Note - Comment

Performed similar attack again:

<https://13-52-213-237-shred.vulnerablesites.net/Shred/catalog?category=BOARDS>; DROP ALL --

((Error executing SQL query: SELECT id, category, price, name, description, photoURL FROM Products WHERE category='BOARDS'; DROP ALL -- ORDER BY price))

Details: com.fjordengineering.store.util.SecurityException: SELECT id, category, price, name, description, photoURL FROM Products WHERE category='BOARDS'; DROP ALL -- ORDER BY price at com.fjordengineering.store.dao.ProductDao.getProductsByCategory(ProductDao.java:168) at com.fjordengineering.store.actions.catalog.ViewCatalogAction.execute(ViewCatalogAction.java:24) at



00:27:41 | Note - Problem

Information disclosure by tampering with URL:

<https://13-52-213-237-shred.vulnerablesites.net/Shred/catalog?category=BOARDS' OR category='BOARDS>

Revealed all the categories



00:31:28 | Video - Problem



Modified HTML so that I could submit the hidden form.

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 viewing my order.

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

Then...

URL Manipulation

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

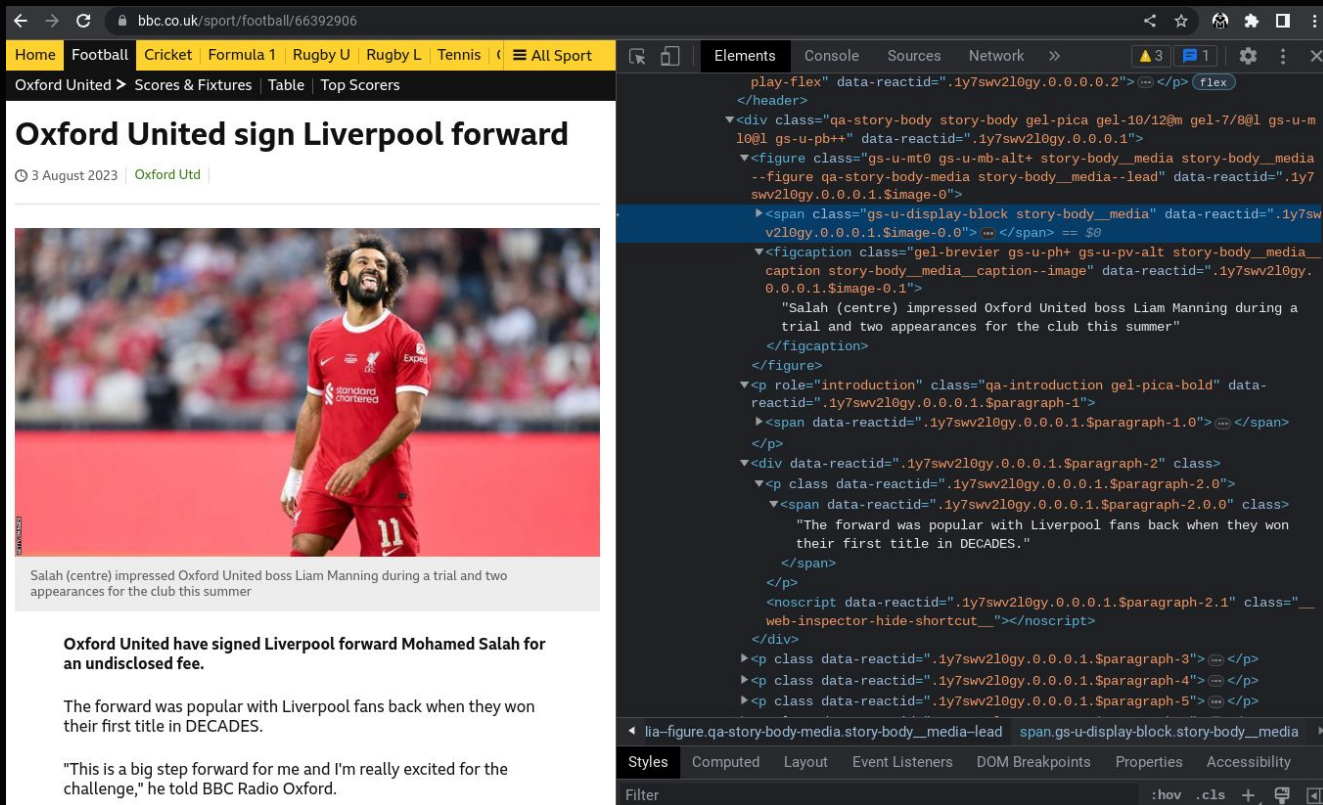
Bookmark URLs	Modify URLs	Elevation of Privileges
<ul style="list-style-type: none">• Can you access them without logging in?• Can you access admin panel as normal user?	<p><code>?isAdmin=false → ?isAdmin=true</code></p> <p><code>/user/1234/edit → /user/1122/edit</code></p> <p><code>/photo/567/view → /photo/567/edit</code></p>	<p>Elevation of privileges security bugs are where you can do something beyond what your user account should be allowed to do.</p>

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



The screenshot shows a web browser displaying a news article from BBC Sport. The article is titled "Oxford United sign Liverpool forward" and is dated 3 August 2023. The main image shows Mohamed Salah in a red Liverpool kit. The article text states that Salah impressed Oxford United boss Liam Manning during a trial and two appearances for the club this summer. Below the image, it is reported that Oxford United have signed Liverpool forward Mohamed Salah for an undisclosed fee. The forward was popular with Liverpool fans back when they won their first title in DECADES. Salah said, "This is a big step forward for me and I'm really excited for the challenge," he told BBC Radio Oxford.

The Chrome DevTools Elements panel is open on the right, showing the HTML structure of the page. The selected element is a `span` with the class `gs-u-display-block story-body_media`. The parent element is a `figure` with the class `gs-u-mt0 gs-u-mb-alt+ story-body_media story-body_media`. The `figure` element contains a `img` element and a `figcaption` element. The `figcaption` element contains the text "Salah (centre) impressed Oxford United boss Liam Manning during a trial and two appearances for the club this summer". The `figure` element is part of a `div` with the class `qa-story-body story-body gel-pica gel-10/12@m gel-7/8@l gs-u-m10@l gs-u-pb++`. The `div` element is part of a `header` element. The `header` element is part of a `play-flex` element with the data-reactid `.1y7swv2l0gy.0.0.0.2`.

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

The screenshot shows the Chrome DevTools Network tab. The selected resource is `?activity=html`. The **Payload** tab is active, displaying the following data:

- Query String Parameters:** `activity: html`
- Form Data:**
 - `fname: Richard`
 - `sname: Adams`
 - `age: 39`
 - `attending: Yes`
 - `submitForm: Submit`

Postman

The screenshot shows the Postman interface for a **POST** request to `https://www.r-adams.co.uk/workshop/?activity=html`. The **Body** tab is selected, and the `x-www-form-urlencoded` format is chosen. The request body is displayed as a table:

Key	Value
<input checked="" type="checkbox"/> <code>fname</code>	<code>Richard</code>
<input checked="" type="checkbox"/> <code>sname</code>	<code>Adams</code>
<input checked="" type="checkbox"/> <code>age</code>	<code>not old</code>
<input checked="" type="checkbox"/> <code>attending</code>	<code>Yes</code>
<input checked="" type="checkbox"/> <code>submitForm</code>	<code>Submit</code>

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:

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:

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:

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

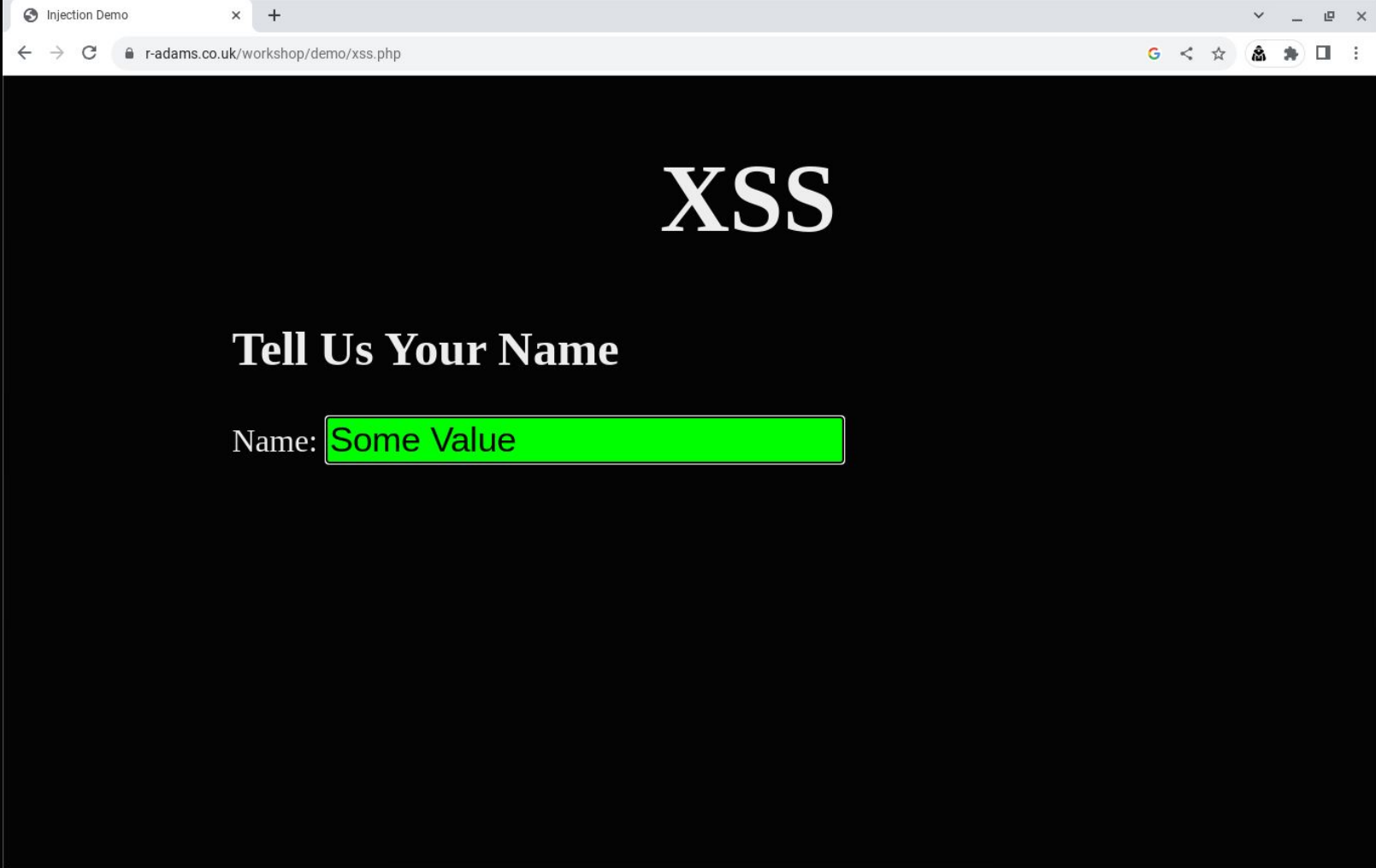
Test Data

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 x +

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

```
<!DOCTYPE html>
<html lang="en">
  <head>
  </head>
  <body>
    <h1>XSS</h1>
    <h2>Tell Us Your Name</h2>
    <p>Hello Some Value</p>
    <p style="font-size:0.6em;">https://r-
adams.co.uk/workshop/demo/xss.php?name=Some+Value</p>
    <form method="GET">
    </form>
  </body>
</html>
```

html body

Styles Computed Layout Event Listeners Properties >>

Filter Show all

Console Issues What's New Search X

top Filter Default levels

1 Issue: 1

Using our test data

Name:

```
Rich<script>alert('XSS')</script>
```

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
 - 487836128054750366286127688929561046618/snippets.gtl
 - GET:cheese.png
 - GET:lib.js
 - GET:login
 - GET:login(pw,uid)**
 - GET:newsnippet.gtl
 - GET:newsnippet2(snippet)
 - GET:snippets.gtl
 - GET:487836128054750366286127688929561046618/snippets.gtl
 - GET:favicon.ico

GET
https://google-gruyere.appspot.com/487836128054750366286127688929561046618/snippets.gtl
ch&pw=Admin...
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_0_0; rv:89.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.8,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive

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

Cross Site Scripting (Persistent)

Alerts (11)

- Cross Site Scripting (Persistent)
 - GET: https://google-gruyere.appspot.com/487836128054750366286127688929561046618/snippets.gtl**
 - Cross Site Scripting (Reflected)
 - GET: https://google-gruyere.appspot.com/487836128054750366286127688929561046618/snippets.gtl
 - X-Frame-Options Header Not Set (6)
 - Absence of Anti-CSRF Tokens (3)
 - Cookie No HttpOnly Flag
 - Cookie Without SameSite Attribute

Cross Site Scripting (Reflected)

URL: https://google-gruyere.appspot.com/487836128054750366286127688929561046618/snippets.gtl
Risk: High
Confidence: Medium
Parameter: snippet
Attack:
Evidence:
CWE ID: 79
WASC ID: 8
Source: Active (10014) - Cross Site Scripting (Persistent)

Dashboard Session SCA Proxy R-Builder R-Attacker Macro IOOS

Generate report Scan in runtime Reset

▶ <https://www.r-adams.co.uk/workshop/demo/xss.php?name=A+safe+value>

All Vulns

13	8	5	0	3
ATTACKS	FINDINGS	HIGH	MEDIUM	LOW

⚠ Vulnerability detected
 Attack: XSS - Unfiltered <script> tag
 URL: <https://www.r-adams.co.uk/workshop/demo/xss.php?name=A+safe+value>
 Proof: `<script>alert(ptk_xss_1)</script>`
[Details](#)

⚠ Vulnerability detected
 Attack: XSS - Script tag after noscript tag
 URL: <https://www.r-adams.co.uk/workshop/demo/xss.php?name=A+safe+value>
 Proof: `</noscript><script>alert(ptk_xss_2)</script>`
[Details](#)

⚠ Vulnerability detected
 Attack: XSS - Svg tag with animation event
 URL: <https://www.r-adams.co.uk/workshop/demo/xss.php?name=A+safe+value>
[Details](#)

Tell Us Your

Hello A safe value

<https://r-adams.co.uk/workshop/demo/xss.php?name=A+safe+value>

Name: A safe value

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