

# XSS and SQL Injection

sigpwny{do\_you\_pronounce\_it\_as\_sql\_or\_sql}

**XSS**

# What is XSS (Cross Site Scripting)

- User adds their own javascript code that is then executed
- Takes advantage of `<script>` tags, which allow javascript code to be written in the middle of content
  - If user input is used directly, they can insert these tags to write their own code in the middle of your web application

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

</html>
```

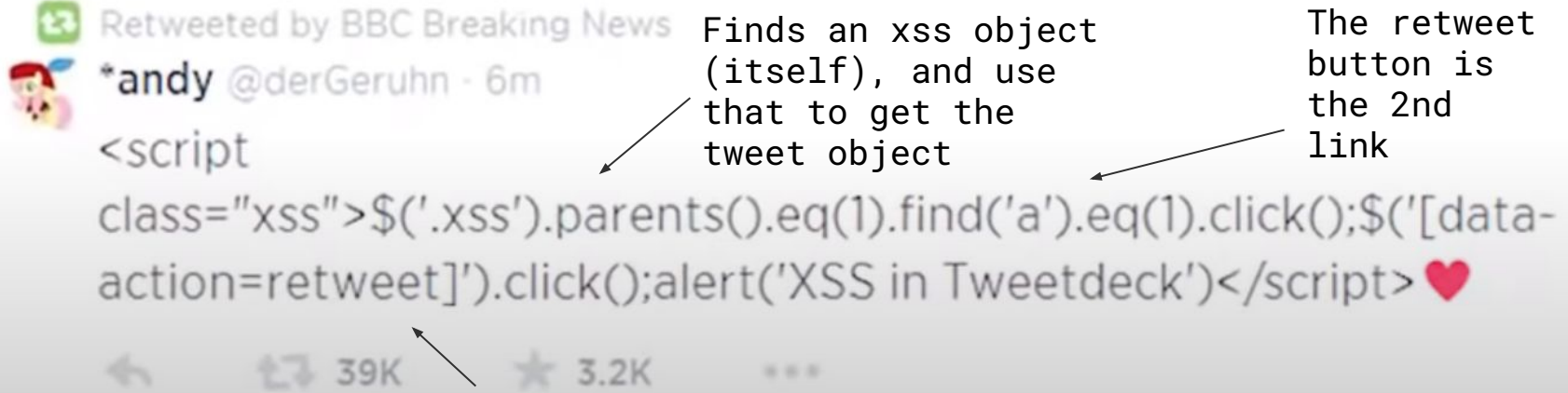
# The Self Retweeting Tweet

Retweeted by BBC Breaking News

\*andy @derGeruhn · 6m

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

← 39K 3.2K ...



Confirms the action

URL

# *FourOrFour*

URL

# What if script tags are filtered?

- Other html tags have javascript attributes you can force into running
  - The img tag onerror attribute will always run if given a bad address
  - Buttons will likely be less commonly available
- Check if input is being taken from the url
  - If so you may be able to alter one of the parameters there
- Remember to take a look at the source-code, that will tell you immediately how any input is being collected (though you won't be able to see any processing done on the backend)

# SQL Injection



```
SELECT * FROM Users WHERE username = "_____"
```

What can we put in the blank to return all the users?

Hint: We want to match at every entry in the table

Test another case that will always be true

Put something to finish the query they wanted to make, what it is shouldn't matter.

```
a" OR 1==1; --
```

Start a comment to ignore the rest of the line

```
SELECT * FROM Users WHERE username = "a" OR 1==1 --"
```

What if the query you want to run doesn't look like the one they wanted you to run?

By adding a semicolon, you can add a completely separate statement at the end (; DROP TABLE \_\_\_\_)

*NOTE: This usually won't work, but it's worth a try*

However, you'll still only be able to see what is returned to you by the webpage (i.e. if you were getting 3 fields and you need 4, do it in 2 batches)

