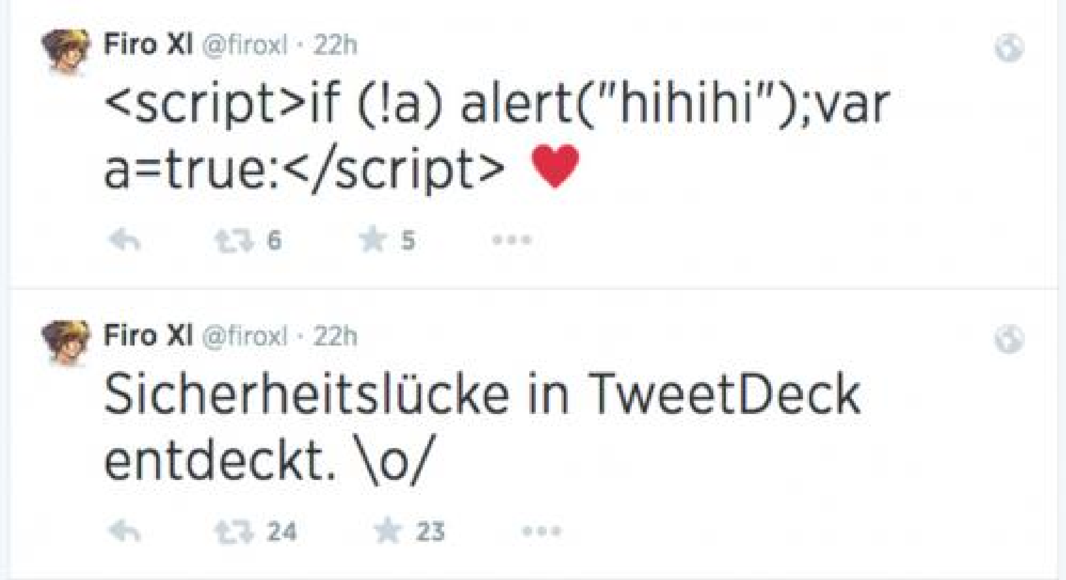
How the love of one teenager brought Tweetdeck to its knees

June 13 2014, by Bill Buchanan

TweetDeck, a Twitter app with millions of users, is back online after a rather surprising security scare. For several hours, the service was taken down all because a 19-year-old user tried to add a cute heart to his messages.

It seems that Florian, a budding young programmer from Austria, had run a small amount of code in the TweetDeck interface in an attempt to add a heart icon at the end of his tweets.



Firo XI @firoxl · 22h

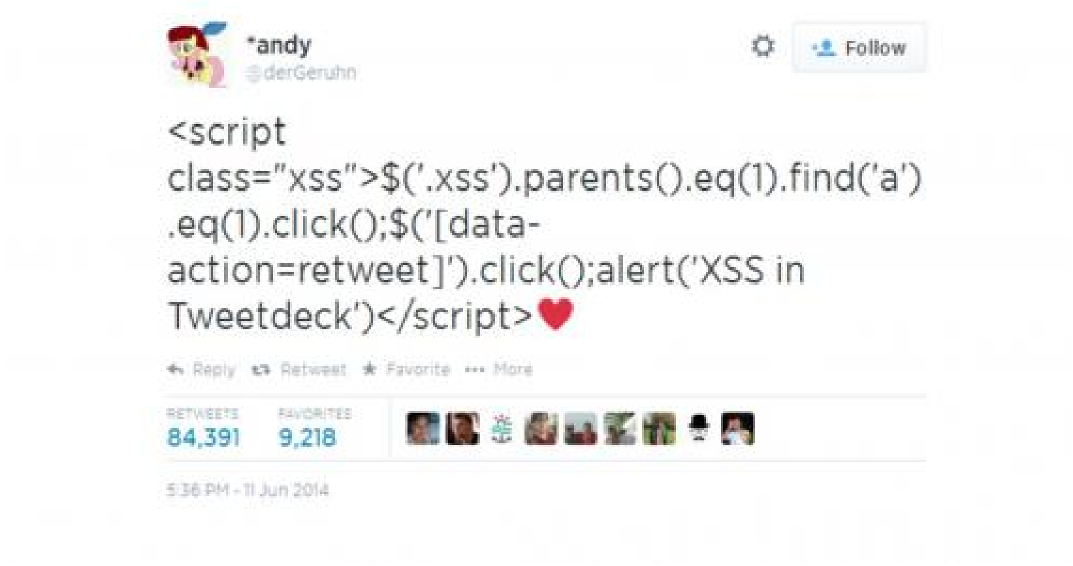
```
<script>if (!a) alert("hihihi");var a=true:</script> ♥
```

Firo XI @firoxl · 22h

Sicherheitslücke in TweetDeck entdeckt. \o/

Florian reveals his discovery. Credit: Twitter

Once Florian realised he had found a weakness in TweetDeck that would allow him to introduce a heart, he announced it triumphantly to the world. He says that he tried to alert Twitter, which owns the service, to the weakness but received no response.



*andy
@derGeruhn

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

RETWEETS 84,391
FAVORITES 9,218

5:36 PM - 11 Jun 2014

A lot of retweets for @derGeruhn. Credit: Twitter

That worm sent out a line of code out as a tweet from a Twitter account and caused tens of thousands of users to automatically retweet without realising. The account that had the original tweet, @derGeruhn, is owned by a German student called Andy Perdana. It's not known if he was deliberately involved or had his account hijacked.

Tweetdeck picked up the tweet and retweeted it to anyone with the app open on their machine. It was then retweeted around 80,000 times, including by the BBC, which retweeted to ten million followers.

It was just like the old days, when worms would infect systems and hog them to the point that they became unusable. In this case, Twitter stepped in, and switched off the function that allowed the messages to be retweeted.

What's up with the web?

At the moment it seems security threats are emerging on some of the biggest sites every day and this is at least in part due to how we run websites these days.

As more and more services are hosted in the cloud and more code is run on web servers, we are using HTML and JavaScript more than ever. In the past, software development teams would spend a great deal of time testing their programs to destruction to spot weaknesses but these programming languages were never designed to be secure.

To make things worse, the teams who are writing web-based code often have little training in how to actually test their applications. Code that is run on Windows or Mac programs are rigorously tested but those run on the web are not. Programmers who test their own programs often do not exercise them in a way that will make them break so they miss important problems.

The TweetDeck hack was about as simple they come, it just exploited a flaw that had been overlooked in testing. As Florian himself pointed out, he should never have been allowed to introduce his loved-up code in the first place.

The code that runs on web servers is often quite messy so security needs to be taught from day one. Software development teams must learn how to secure their code, especially by checking data input at the gate. They should know that users should never be allowed to add code without it being checked first.

For some reason, we often don't teach security to software developers, especially in an understanding of how to handle exceptions in user input or from external systems, and how we encrypt data. This lack of understanding often leads to passwords and user credentials not be stored in a secure way.

This has got to change. Luckily, in this case, there was no real damage done, but if a single teenager can prompt the collapse of one of the biggest names on the web, we should really be taking away a serious warning about security.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Provided by The Conversation

Citation: How the love of one teenager brought Tweetdeck to its knees (2014, June 13) retrieved 18 April 2024 from https://phys.org/news/2014-06-teenager-brought-tweetdeck-knees.html