mehedishakeel

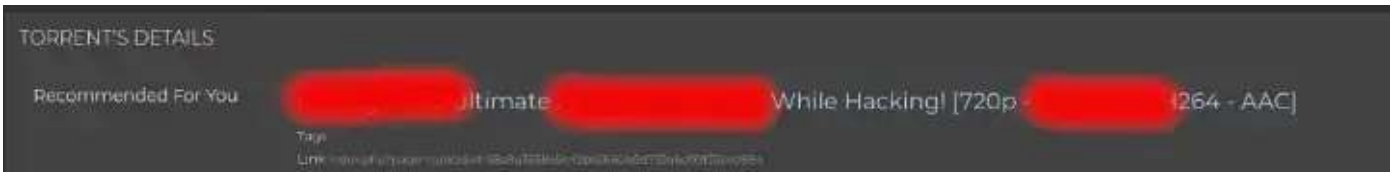
Oct 6, 2022 · 3 min read · Listen

Found XSS & Open Redirect Vulnerability in CrazyHD Torrent Website

CrazyHD is one of the famous torrent websites in Bangladesh and India. People get pirated movies, paid courses, software, and more in this torrent.

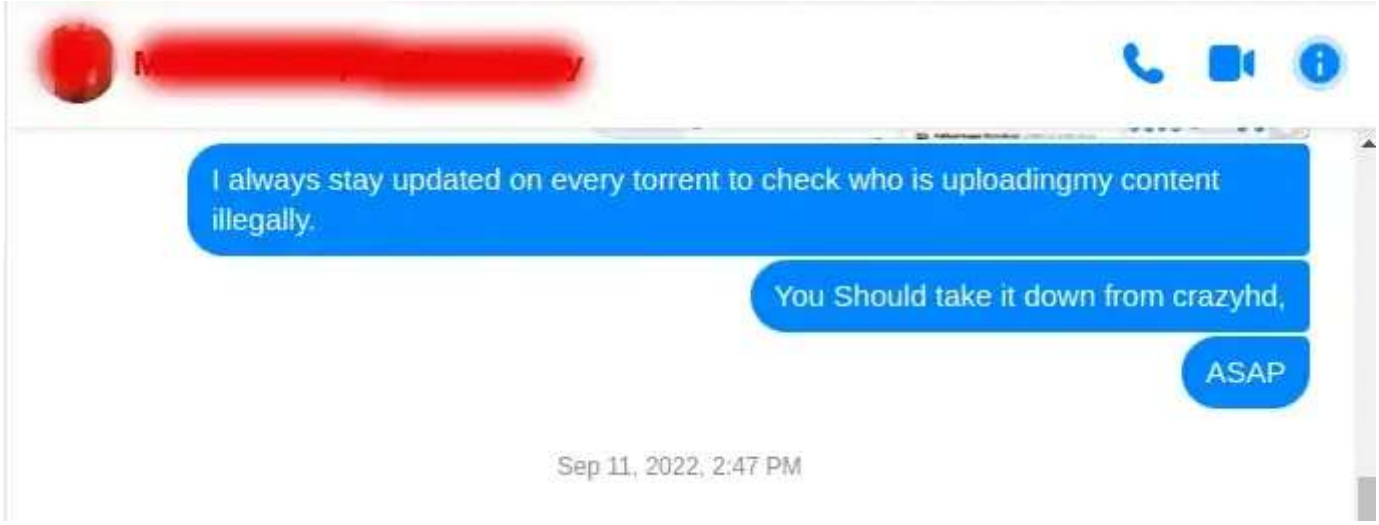
Story Behind Pentesting CrazyHD

One day I logged into my account on that CrazyHD torrent and I don't know why I search my name "Mehedi Shakeel" in the search box. As a search result, I found someone uploaded some of my paid courses there.



> *I didn't like that, because most of my paid courses I gave for free by making giveaways occasionally from my youtube channels and websites but some one uploaded it on CrazyHD for free.*

So, I start finding out who the guy is responsible for this. For information gathering I collect every detail of that guy like phone numbers, email, addresses, social media accounts, and more, Then I asked him to remove the course from there by sending him messages on social media but he didn't reply.



> *So i thought lets try to **Hack into CrazyHD** torrent website.*

I start digging the **CrazyHD** website by enumerating subdomains and got the following results.

```
[INF] Enumerating subdomains for crazyhd.com
news.crazyhd.com
crazyhd.com
core.crazyhd.com
z.crazyhd.com
siena.crazyhd.com
www.crazyhd.com
```

Then I start visiting those subdomains, enumerating internal files, technologies used in these subdomains, and others. In one word “Recon”. I found couple of interesting files named “License”, “Readme” and more.

```
Target: https://core.crazyhd.com/

[02:26:33] Starting:
[02:26:56] 200 -    1KB - /LICENSE.txt
[02:26:57] 200 -    5KB - /README.txt
[02:27:03] 200 -   18B  - /account.php
```

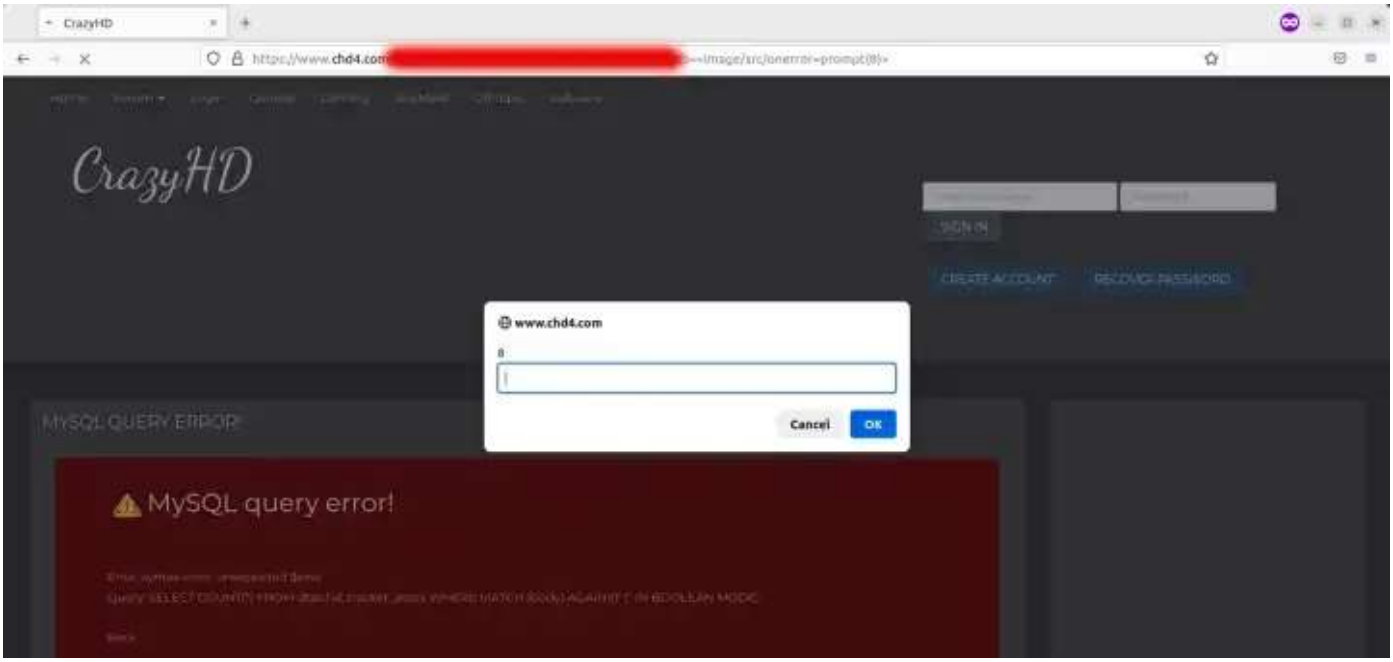
Reviewing those files I found that this **CrazyHD** torrent site uses **XBTIT Torrent Tracker** as its core application. So, I just simply google it and found some interesting vulnerability records of this xbtit application in the older versions from an article published in 2018.

Multiple Vulnerabilities in XBTIT Torrent Tracker

SEPTEMBER 3, 2018

I take those vulnerabilities as a guide and tried to find some of those vulnerabilities on the latest versions, and there is an (XSS) Reflected Cross Site Scripting. vulnerability in the latest version of this xbtit application.

After getting that vulnerability, I start digging the CrazyHD website manually and found a parameter that is vulnerable to Open Redirect Vulnerability.



So, after that, I deiced to use these vulnerabilities to hack the guy's credentials who uploaded my courses on CrazyHD Torrent and delete my courses by myself. But Suddenly, I got a message in my Facebook inbox :

> *Ok then. From next time I try to not upload your paid course in servers.*

That message makes me stop going further.

A quick suggestion: Before using any torrent based pirated website for pirated content like software, videos, movies, or e-books make sure to open them in a safe environment and do not use your daily driver web browser where you saved your other online account credentials.

I published a video PoC of those vulnerabilities on my Facebook page and my LinkedIn profile. You can watch that post on my profile. Thanks!

Xss Vulnerability Xss Attack Hacking Torrent Site Hacking Training