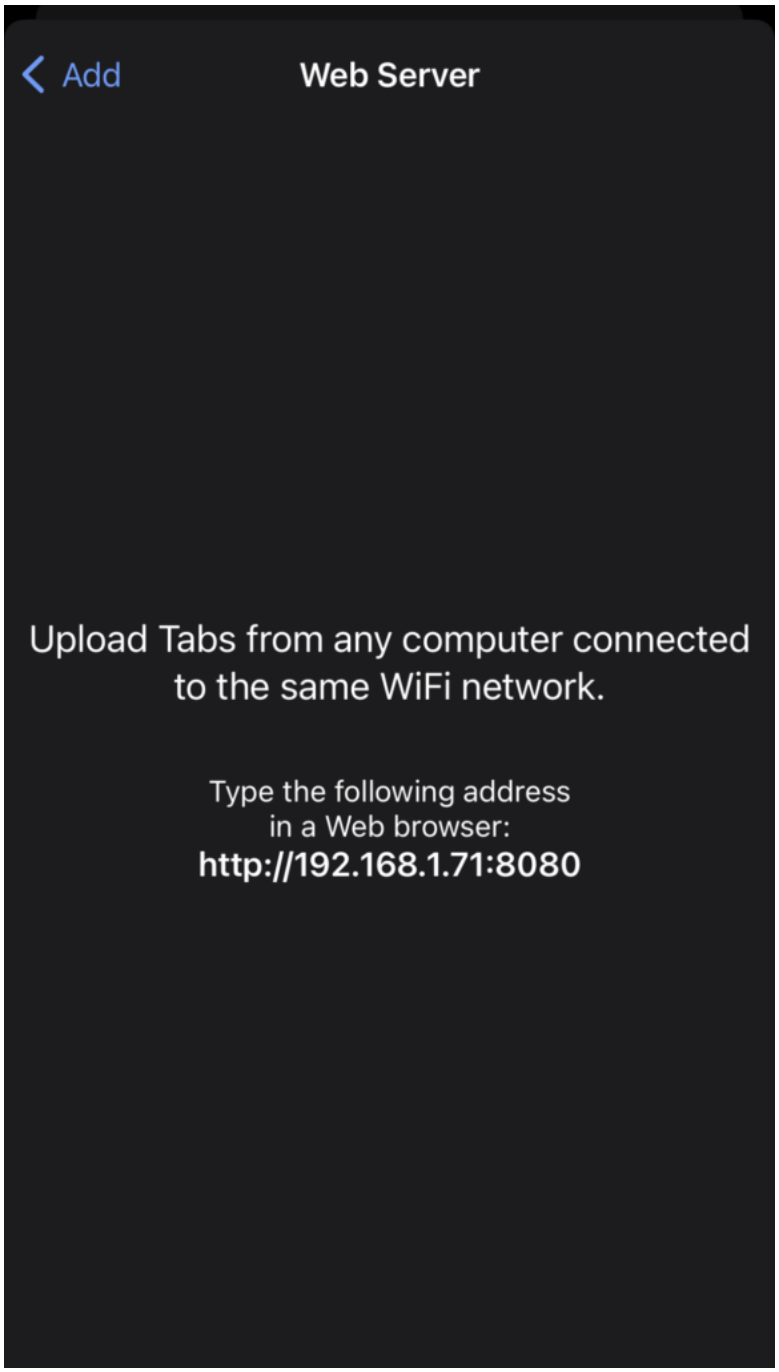
Guitar Pro Directory Traversal and Filename XSS

Edit: These were given CVE-2022-43263 and CVE-2022-43264.

I found these vulnerabilities in the latest version of Guitar Pro (1.10.2) on the iPad and iPhone.

Both of these vulnerabilities stem from the feature of these applications that allows a user to import guitar tabs into their application.

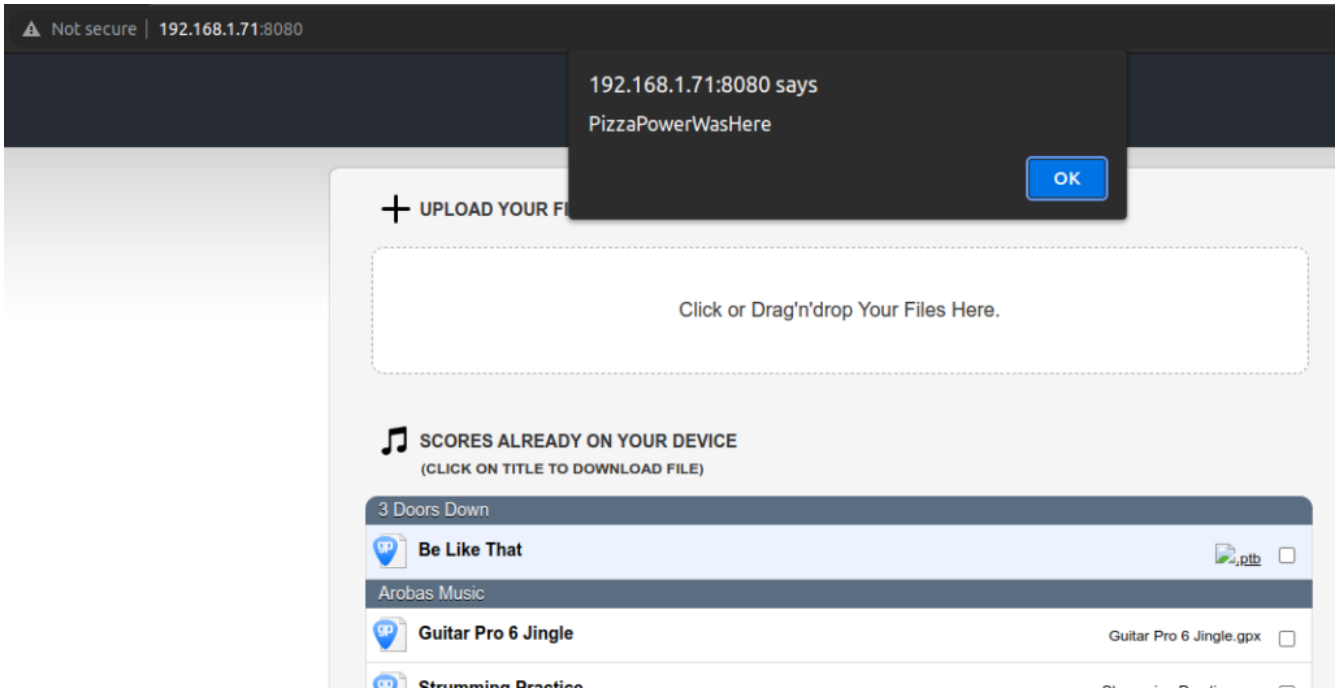


Screenshot of iPhone application showing the server functionality.

First up, a filename XSS, which just happens to be one of my favorite vulnerabilities. I find this on a regular basis – even in 2022. If the user has the screen above open, you can navigate to the URL listed, where you will find the following website, which allows you to upload a file of your choosing. In this case, you can upload a file with the following name.

```
<img src=x onerror=alert('PizzaPowerWasHere)>.ptb
```

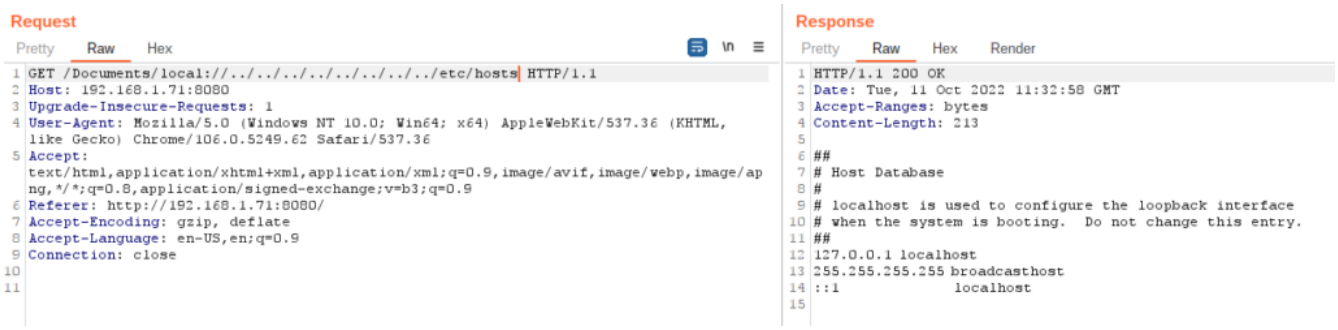
And the XSS should pop.



Next up is a directory traversal. I noticed this while running the upload/download process through Burp. Specifically, this stood out as suspicious.

http://192.168.1.71:8080/Documents/local://Guitar%20Pro%206%20Jingle.gpx

This just allows you to download a tab file from your device. The following Burp payload shows the obvious vulnerability.



You can request and receive the usual suspects e.g. passwd, hosts, etc.

Also, there is this endpoint that seems possibly dangerous. I didn't test it because I didn't want to delete something of importance.

The vendor has been notified.

This entry was posted in hacking, infosec, offensive security, offsec and tagged cybersecurity, directory traversal, guitar pro, hacking, infosec, xss on October 11, 2022 [https://www.pizzapower.me/2022/10/11/guitar-pro-directory-traversal-and-filename-xss/] .