Viraj Mota (Follow)

Sep 2, 2020 · 1 min read · ▶ Listen

🔖 Save   ✕ ⊙ in 🔗

Full path disclosure

Hello **Techie**,

Hope you are doing well, So today discussion is about well known bug i.e: Full Path disclosure.

Although, It is low/medium in severity depends upon attack vector (Looping this issue with another).

In Owasp TOP 10 category comes under

Vulnerability Category: **A6- Security Misconfiguration**

Without further delay, I am sharing well known bug which i got in one of well known product.

Let's take site name as **redacted**.com, So normally we found full path in error message.

But the question is how we can get those ?

Here, **I achieved this error message by playing with sessions timeout features.**

Steps to reproduce:

1. Login into product.

http://redacted.com

2. Next, Once you login into product, Leave the session for more than 2 hours once server automatically terminate the current session.

3. After, Session terminate i got the error message like "session timeout" and also even with that internal path disclose where file reside.
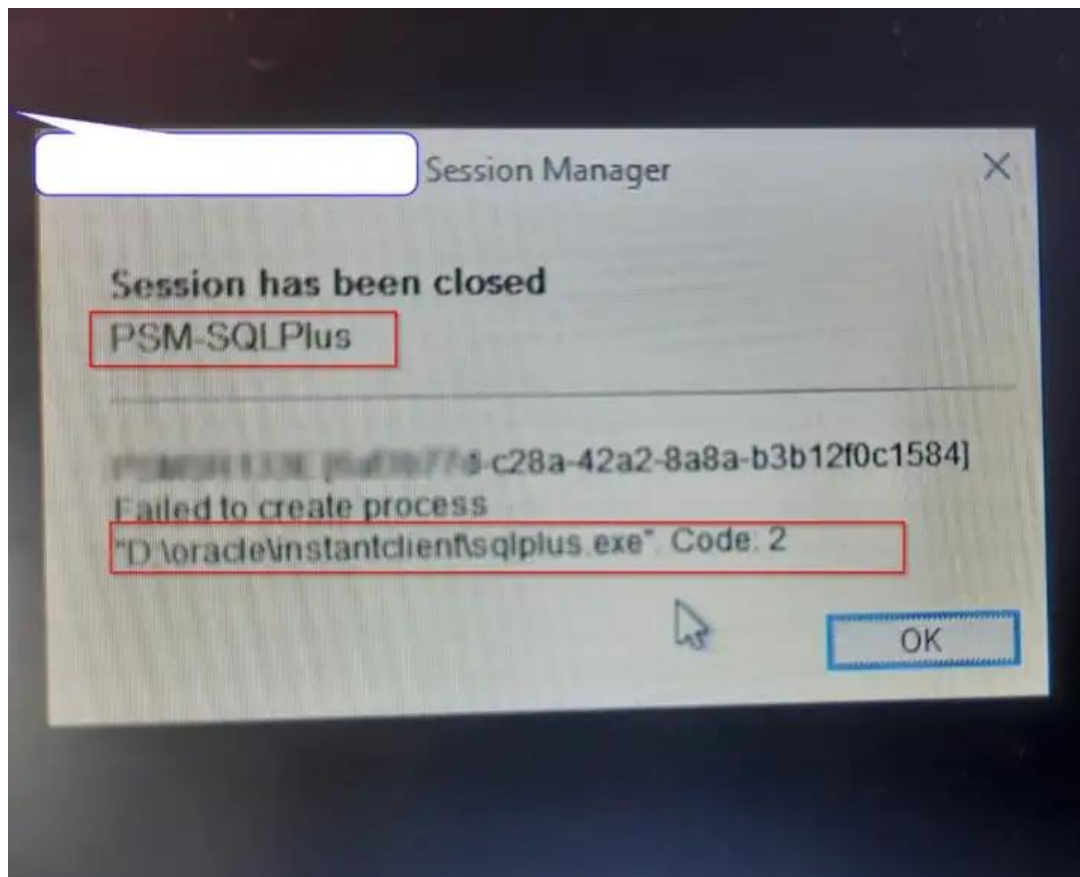
It work for me, Hope in your case works too.

👏 13 | 💬

After this, submit to them and got the appreciation from them.

Rewards: Got appreciation and recommendation.

Conclusion -

"When an active session is closed due to timeout on user's inactivity, the error message contain the path of connection component."

Keep Hacking,

Viraj Mota

Hacking   Product   Hackathons   Tech   Motivation