

Server Site Request Forgery Lab-03

M.Gobi Shankar

CB.SC.P2CYS23019

SSRF with blacklist-based input filter

In this lab we trying access the /admin panel and delete the user carlos , But if we enter the URL it will give us a reply as URL blocked since the keyword admin is blacklisted, So we need to obfuscate the key term and then only we can access the admin panel.

The image shows the Burp Suite interface. The 'Request' tab is selected, displaying a POST request to /product/stock. The 'Response' tab is also visible, showing a 400 Bad Request response with the message: "External stock check blocked for security reasons". The request body contains a 'stockApi' parameter with the value 'http://127.0.0.1/'.

http://127.1/%25%36%31dmin

The image shows the WebSecurity Academy lab interface. The 'Request' tab is selected, displaying a POST request to /product/stock. The 'Response' tab is also visible, showing a 200 OK response with the message: "WebSecurity Academy SSRF with blacklist-based input filter". The request body contains a 'stockApi' parameter with the value 'http://127.1/%25%36%31dmin'.

Lab Completed Successfully.

The image shows a screenshot of a Kali Linux virtual machine. The browser window displays the WebSecurity Academy lab completion screen. The lab title is "SSRF with blacklist-based input filter". The status is "LAB Solved". A congratulatory message says "Congratulations, you solved the lab!". Below this, there is a section for "Giant Grasshopper" with a rating of 4 stars and a price of \$19.05. The background image shows a person looking at a large grasshopper.