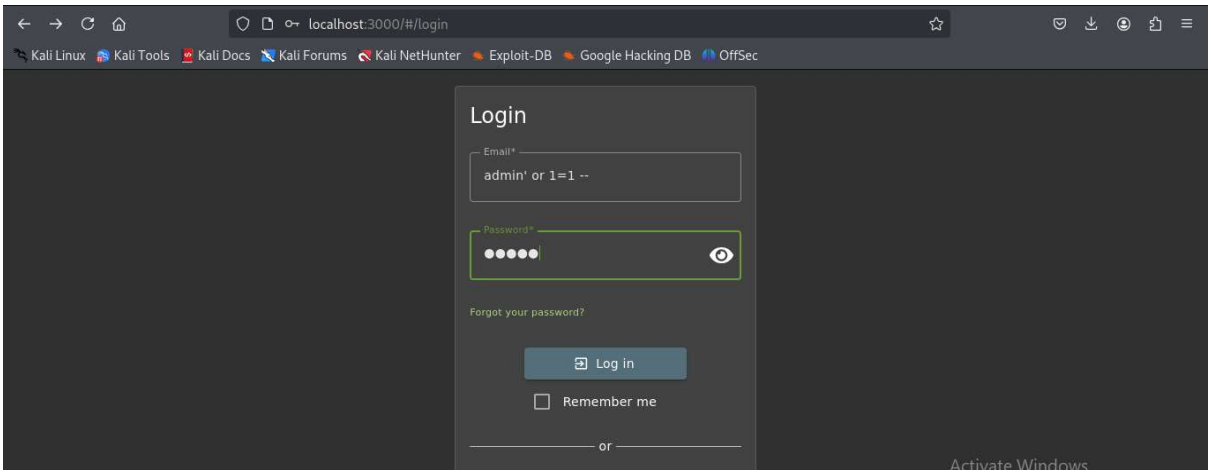
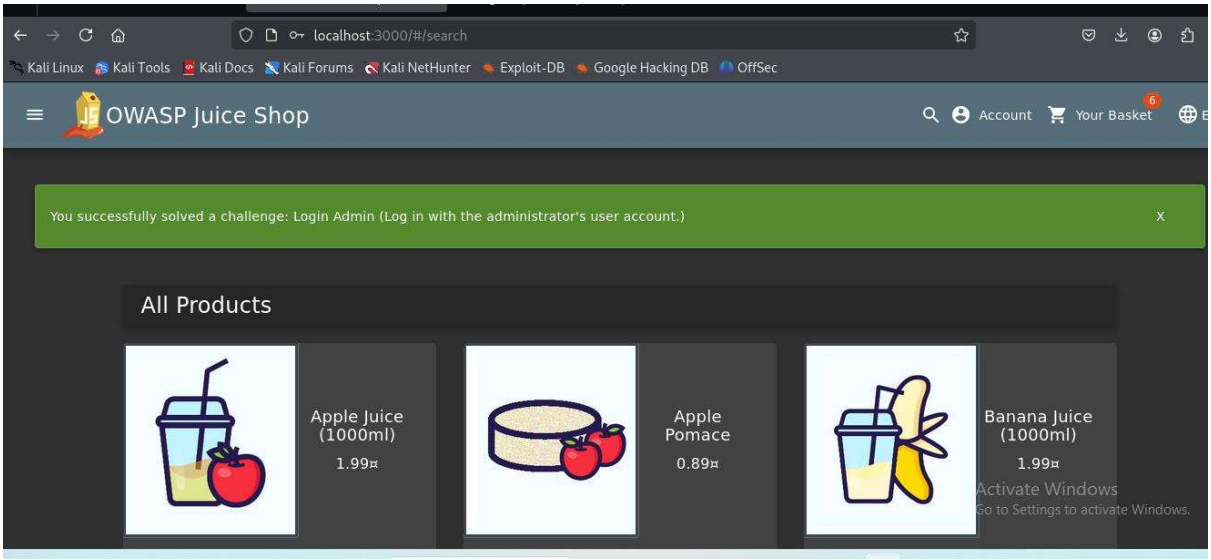
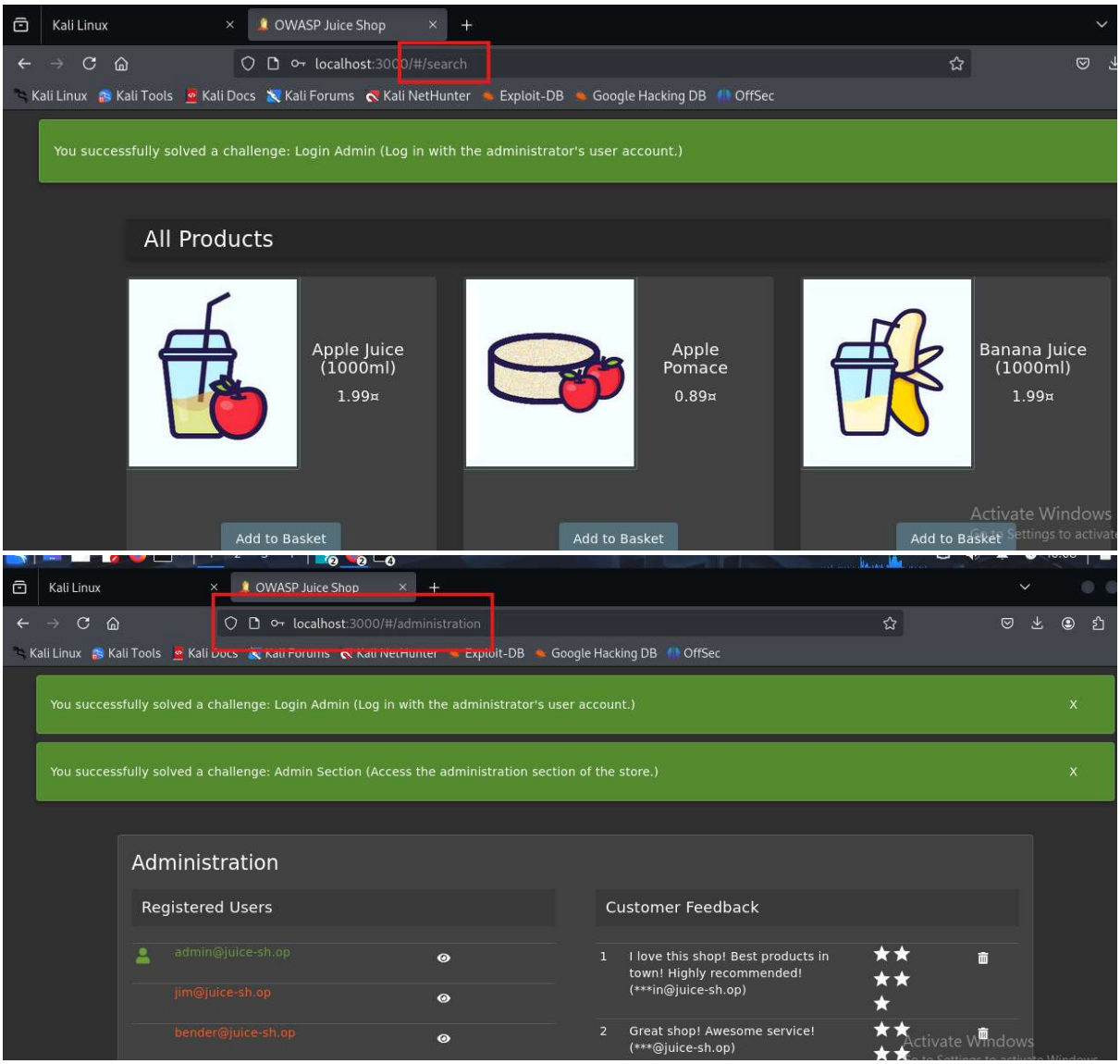
1)SQL injection : Accesing admin account using sql injection

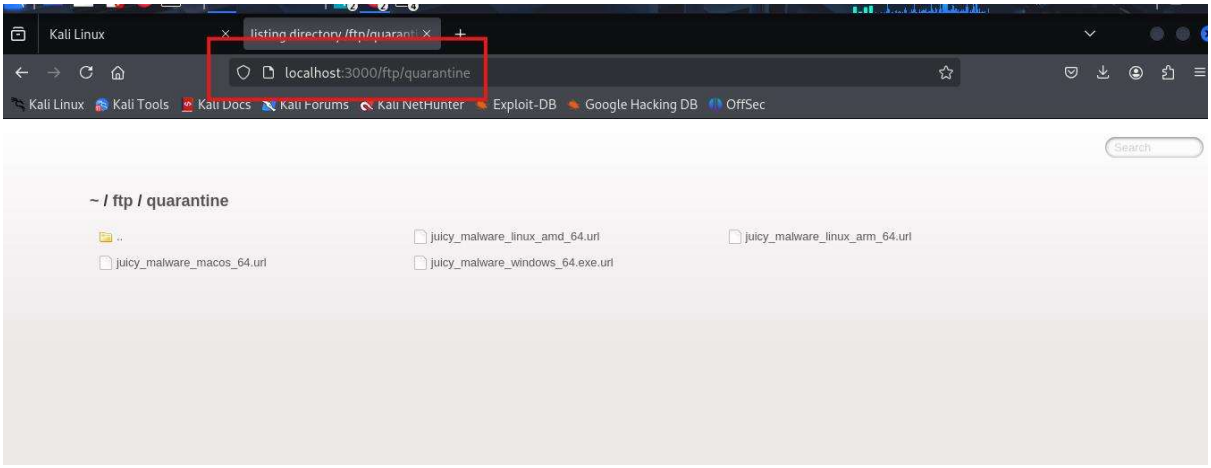


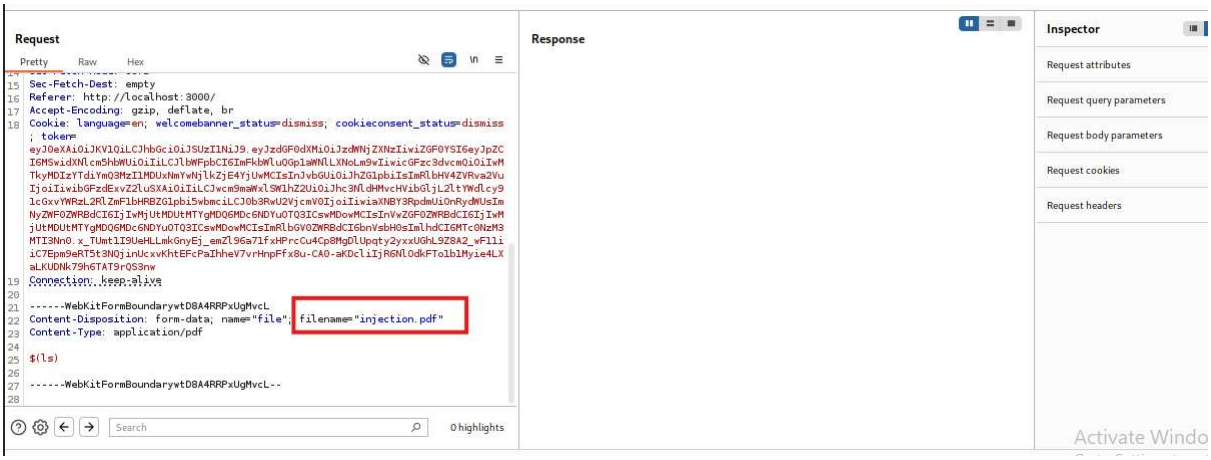


2)Broken Access Control : Changing the search to administration in the url we got the adminsitration details

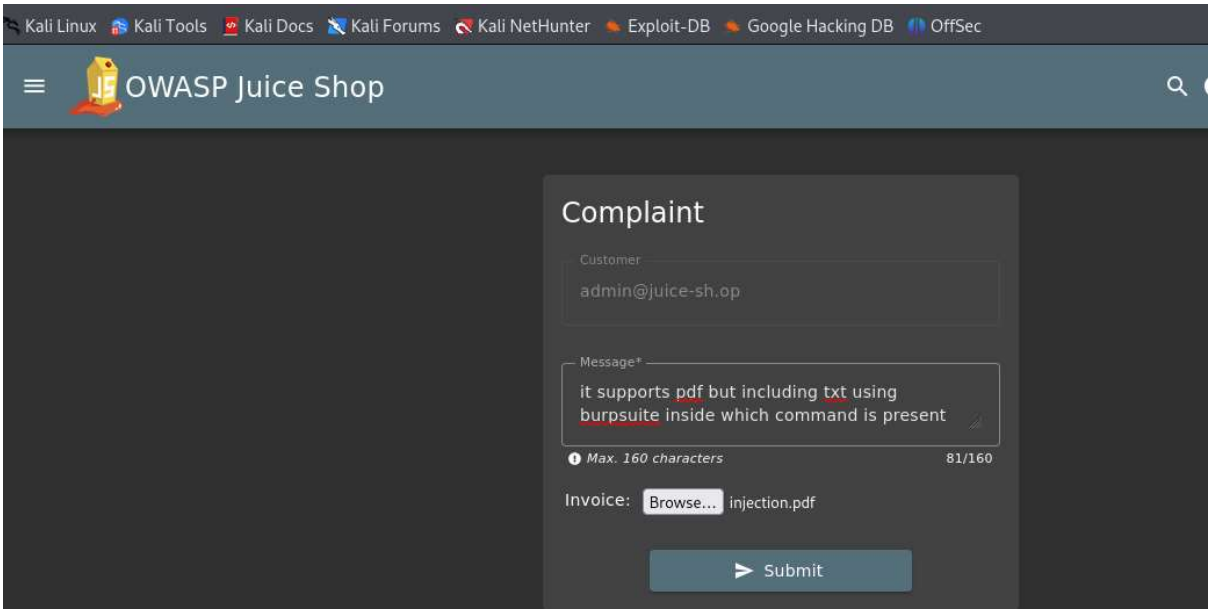


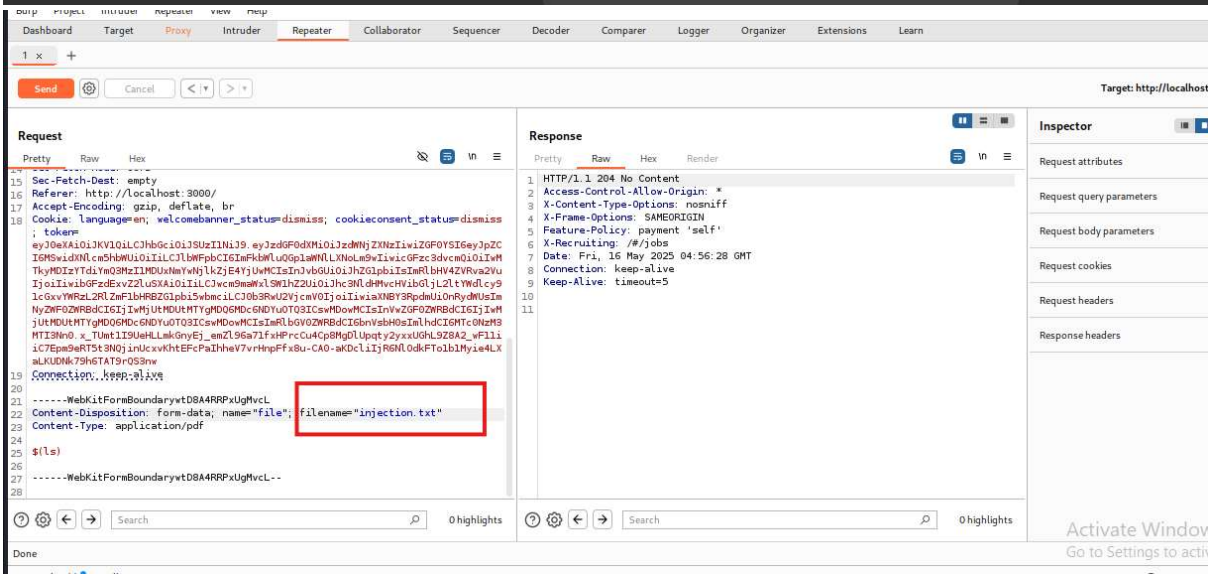
3)Directory Traversal : Using directory traversal we got the files inside the ftp folders

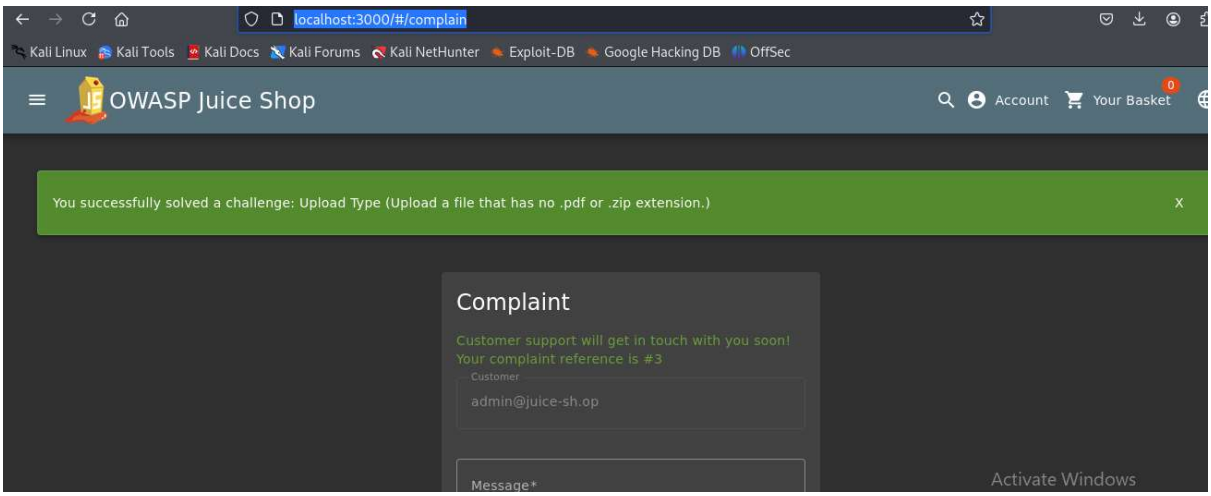

Kali Linux
localhost:3000/ftp/quarantine
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Search
~ / ftp / quarantine
..
juicy_malware_linux_amd_64.url
juicy_malware_linux_arm_64.url
juicy_malware_macos_64.url
juicy_malware_windows_64.exe.url


Request
Pretty
Raw
Hex
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy9lcGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjUtMDUtMTYgMDQ6MDc6NDYuOTQ3ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjUtMDUtMTYgMDQ6MDc6NDYuOTQ3ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTc0NzM3MTI3Nn0.x_TUmtlI9UeHLLmkGnyEj_emZl96a7lfxHPrcCu4Cp8MgDlUpqty2yxxUGhL9Z8A2_wFlliC7Epm9eRT5t3NQjinUcxvKhtEFcPaIhheV7vrHnpFfx8u-CA0-aKDcliIjR6Nl0dkFTolblMyie4LXaLKUDNk79h6TAT9rQS3nw
Connection: keep-alive
------WebKitFormBoundarywtD8A4RRPxUgMvcL
Content-Disposition: form-data; name="file"; filename="injection.pdf"
Content-Type: application/pdf
$(ls)
------WebKitFormBoundarywtD8A4RRPxUgMvcL--
Search
0 highlights
Response
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Activate Windo

4) File inclusion and command injection : Injected a txt file which is not allowed as here only pdf and zip is allowed so using burpsuite modified the request and uploaded the txt file and that file includes the command ls which can be executed







5)Information disclosure : Using curl we got details about header response as we can see here in Access-Control-Allow-Origin its using * which should be not used