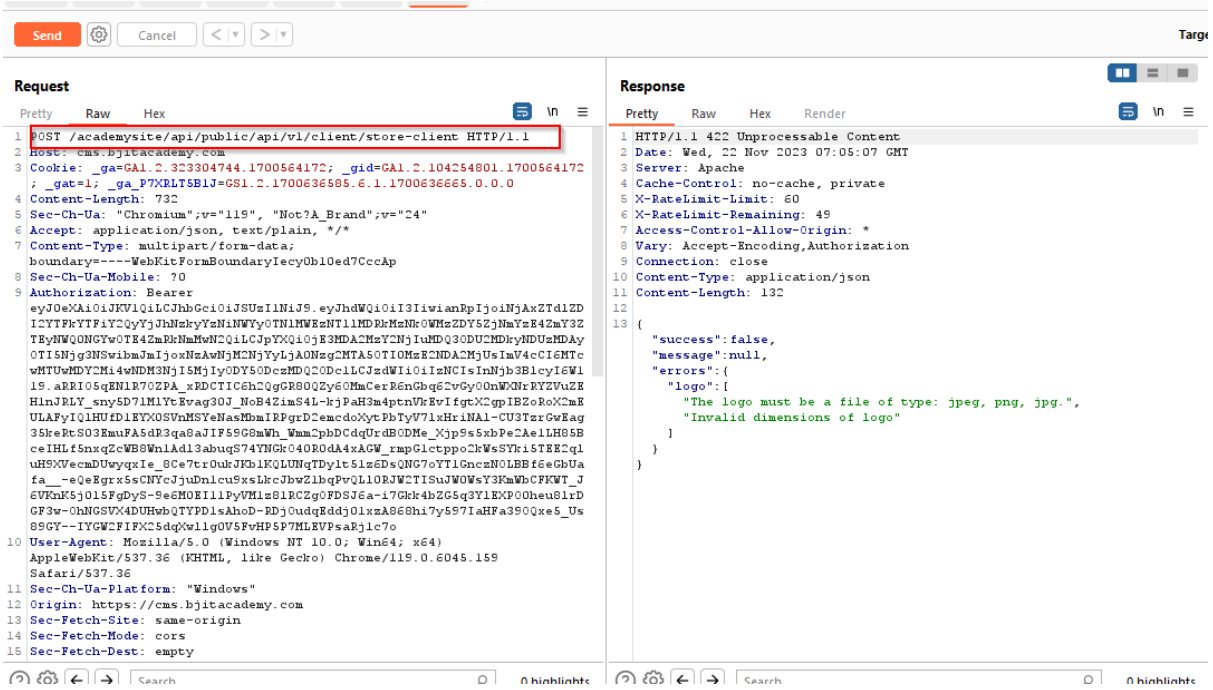
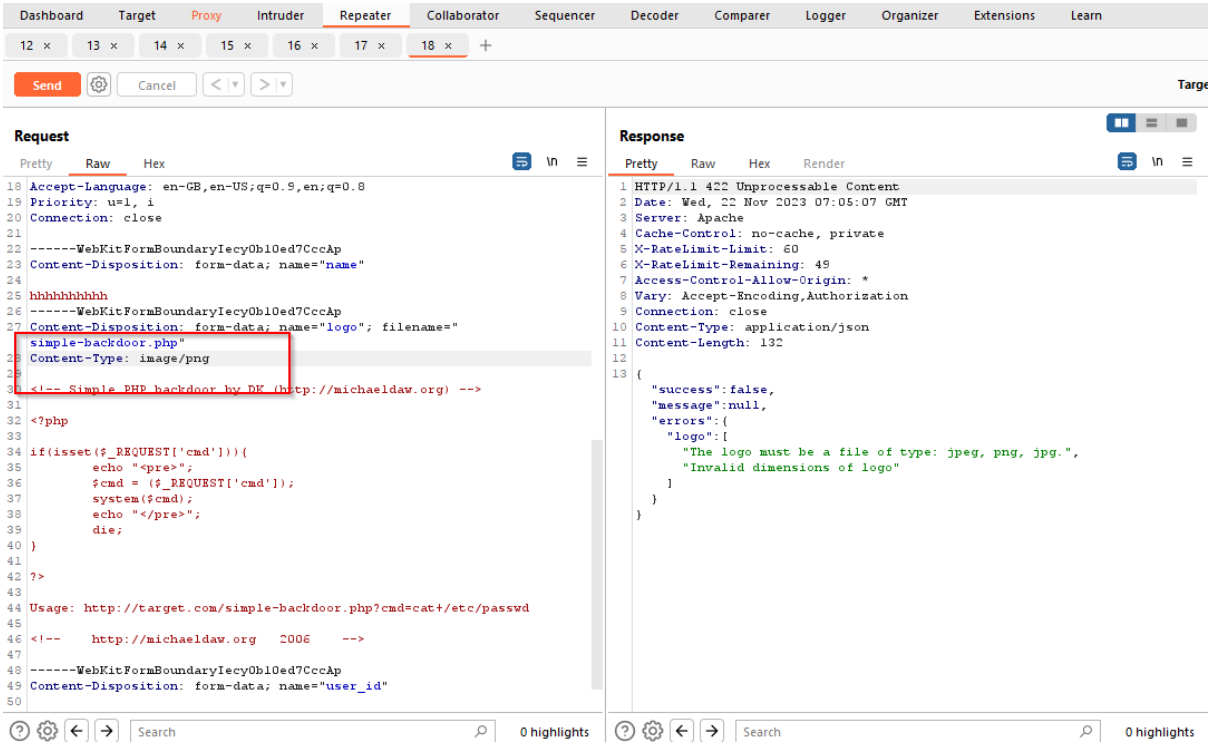
Name: Rushmia Ahmed
ID:30098
Course: Vulnerability Assessment & Penetration Testing
Submitted To: Sad Murshid khan Adon and Abdullah Al Nayeem.

File upload vulnerabilities:

Attempt1:

Title:Try to upload web shell via Content-Type restriction bypass in the add client section.
API:POST /academysite/api/public/api/v1/client/store-client HTTP/1.1.
Target:https://cms.bjitacademy.com
Steps:Login as SuperAdmin>Click Add client section >Try to upload .php file in logo section>Intercept on in burpsuite>Click save in the frontend>>capture request>>Modify .php file with Content-Type from application/octet-stream to **image/png**





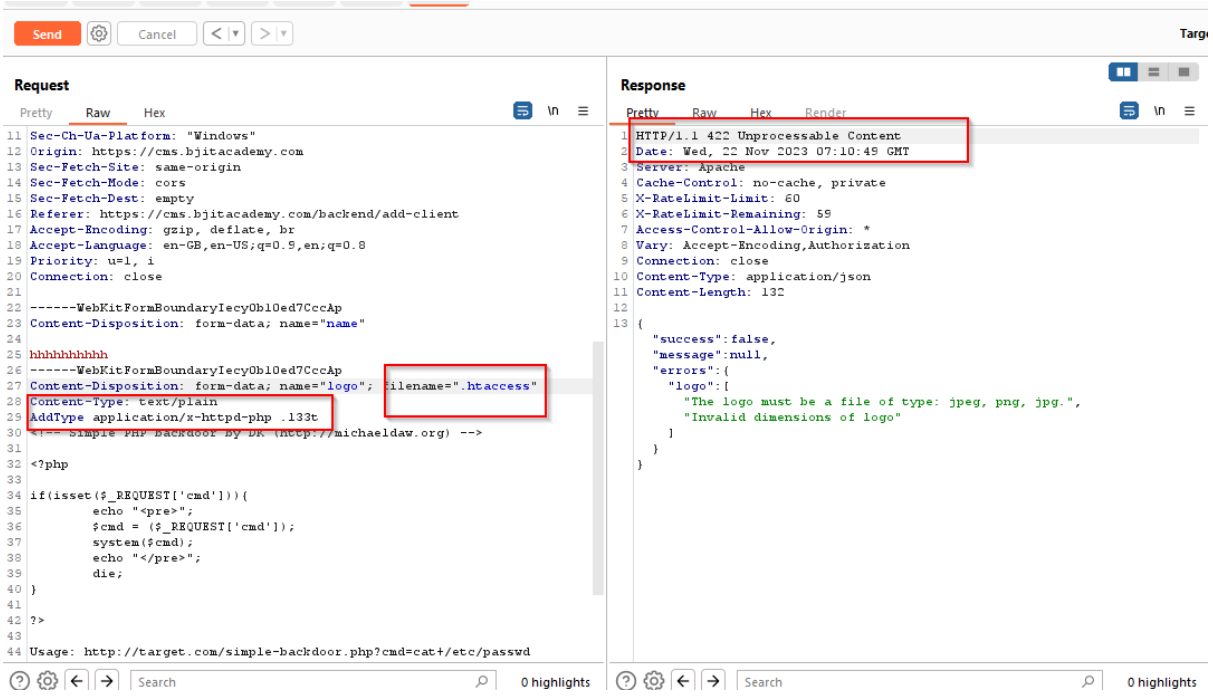
Attempt-2:

Title:Try to bypassed web shell due to a fundamental flaw in the configuration of this blacklist in the add client section.

API:POST /academysite/api/public/api/v1/client/store-client HTTP/1.1.

Target:https://cms.bjitacademy.com/

steps: Login as SuperAdmin>Click Add client section >Try to upload .php file in logo section>Intercept on in burpsuite>Click save in the frontend>>capture request>>Modify .php file into filename=".htaccess",make the **Content-Type** header to **text/plain,**replace the contents of php file with **AddType application/x-httpd-php .l33t**



Attempt-3:

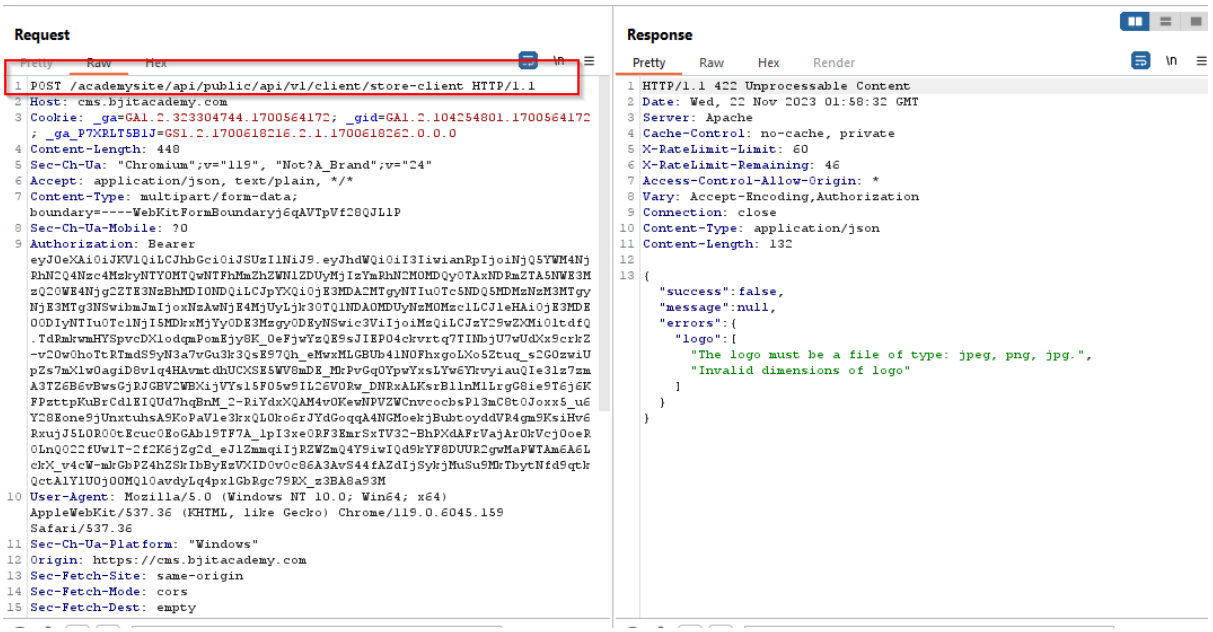
Title:Try to upload web shell via obfuscated file extension in the add client section.

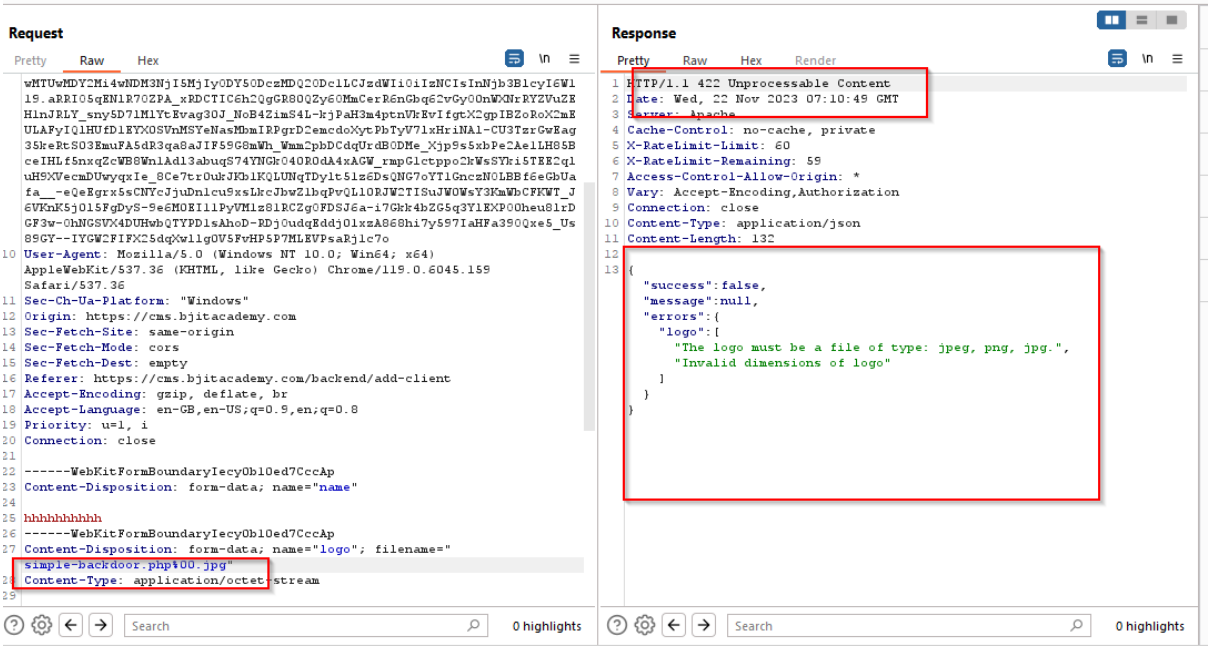
URL:POST /academysite/api/public/api/v1/client/store-client HTTP/1.1.

Target:https://cms.bjitacademy.com/

Steps:

Login as SuperAdmin>Click Add client section >Try to upload .php file in logo section>Intercept on in burpsuite>Click save in the frontend>>capture request>>Modify .php file into filename="**l.php%00.jpg**".





Attempt-4:

Title:Try to upload web shell via obfuscated file extension in the add client section.
API:POST /academysite/api/public/api/v1/client/store-client HTTP/1.1.
Target:https://cms.bjitacademy.com/

Steps:

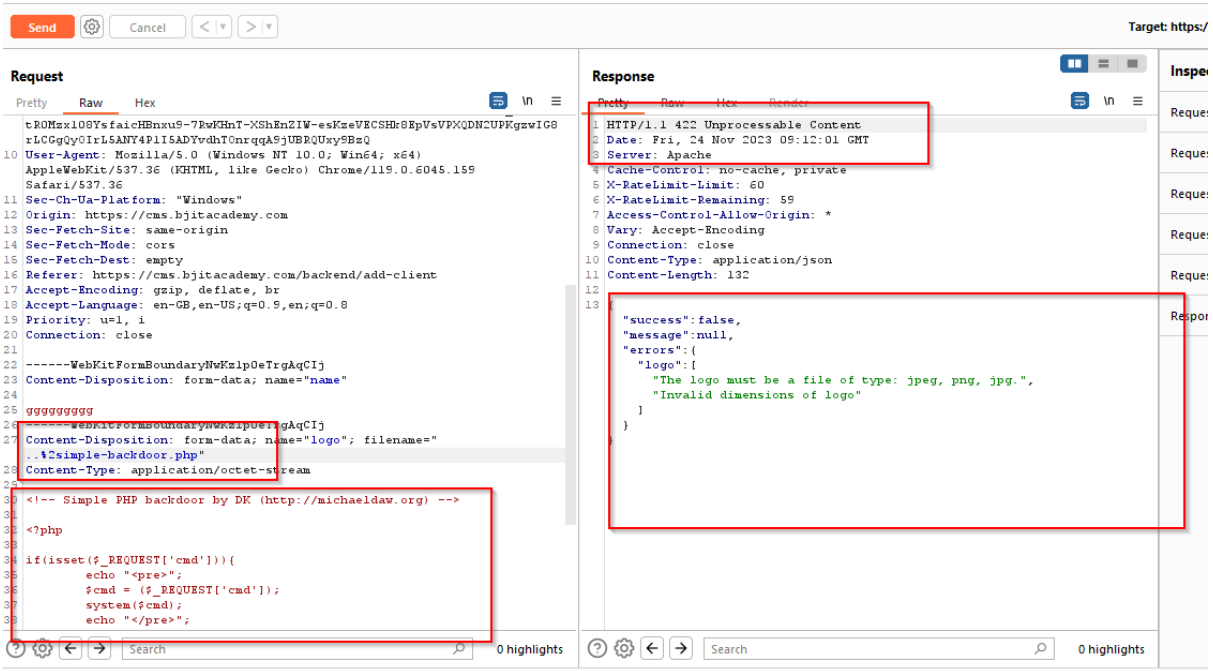
Capture POST /academysite/api/public/api/v1/client/store-client HTTP/1.1.>>Go to repeater>>Modify the filename with .php extension>>add web shell<?php echo system($_GET[‘command’])?>

Attempt-5:

API:POST /academysite/api/public/api/v1/client/store-client HTTP/1.1.
Target:https://cms.bjitacademy.com/

Steps:

Login as SuperAdmin>Click Add client section >Try to upload .php file in logo section>Intercept on in burpsuite>Click save in the frontend>>capture request>>Modify .php file into filename="**..%2simple-backdoor.php**".

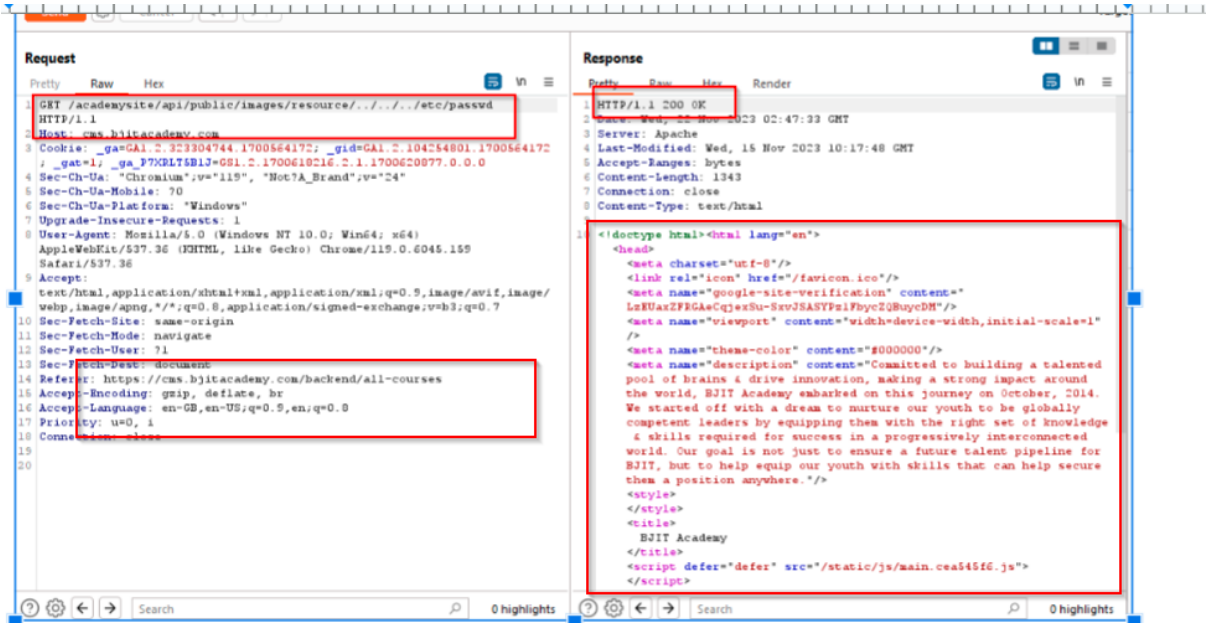


Path traversal:

Attempt-6:

Title: Changing particular filename to a different arbitrary file system
API:GET /academysite/api/public/images/resource/9lSP6cxyYoQT4PNiJoatUB0bH7pVInygVibSugac.jpg HTTP/1.
Target:https://cms.bjitacademy.com/

Steps:
Start burp suite>>>Go to the proxy section>> Click open browser option>>Login as SuperAdmin>Click All Courses section >Open any image in a new tab >>Go to the HTTP history in the proxy >>Collect the target url>>Send it to the repeater>>Modify filename="../../../etc/passwd".



Attempt-7:

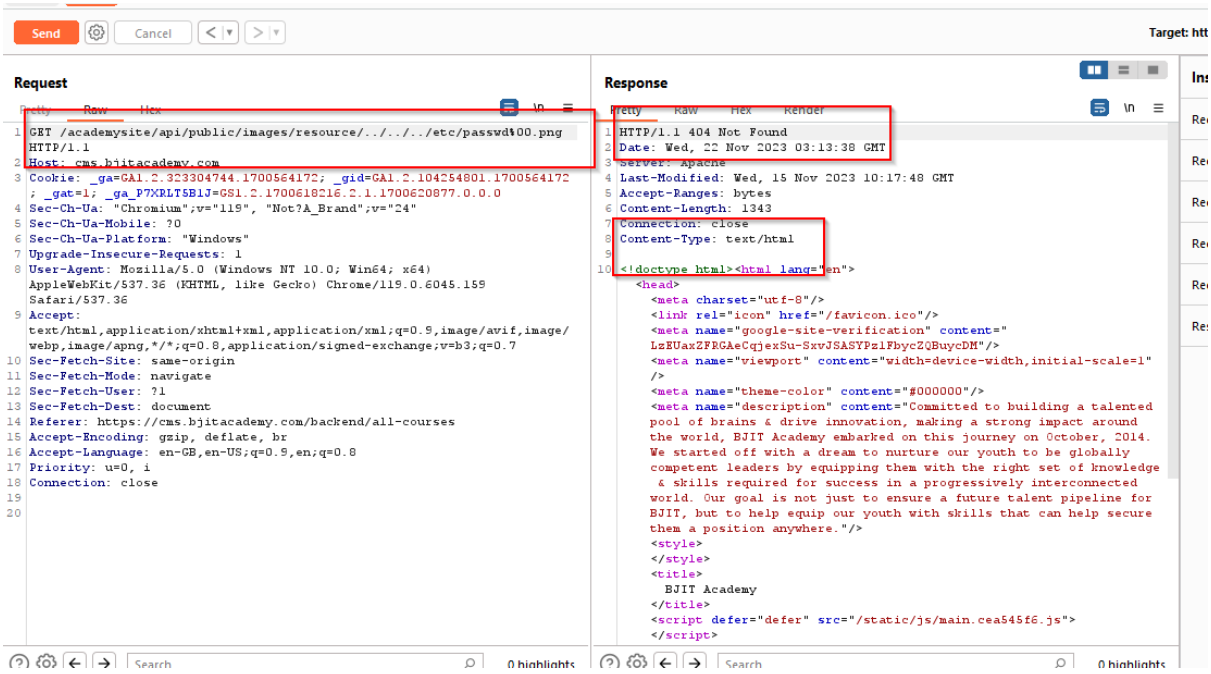
Title: Try to discover critical file path with with null byte bypass

API:GET /academysite/api/public/images/resource/9lSP6cxyYoQT4PNiJoatUB0bH7pVInygVibSugac.jpg HTTP/1.

Target:https://cms.bjitacademy.com/

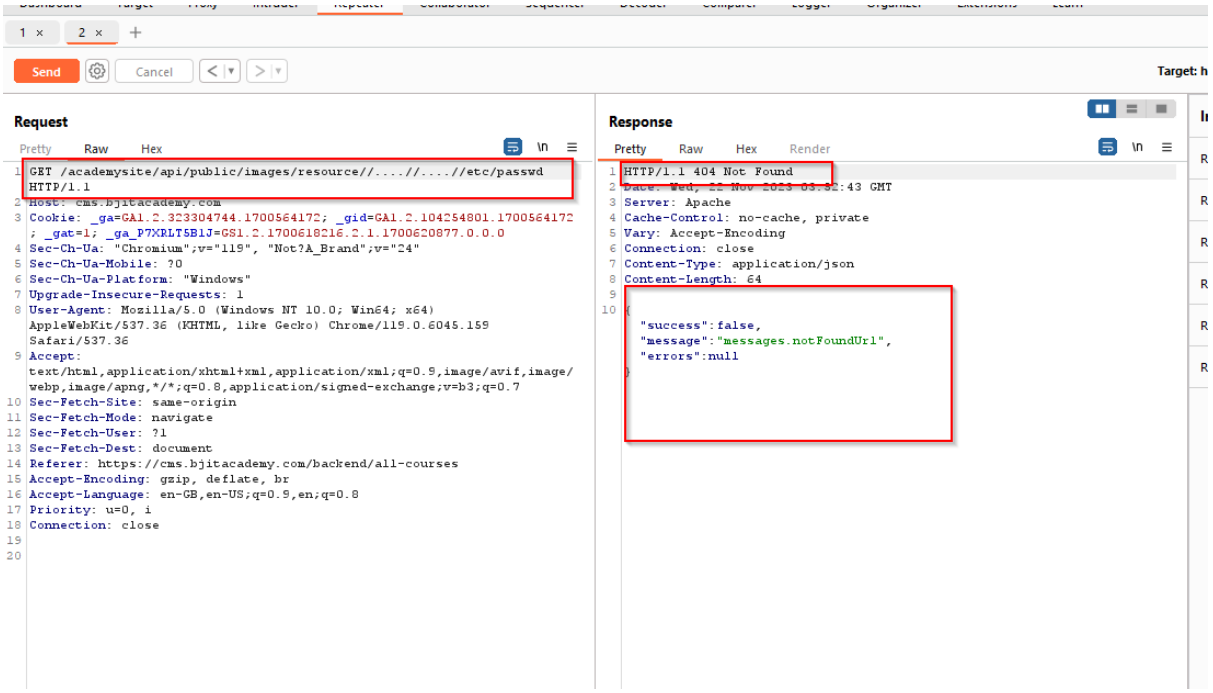
Steps:

Start burp suite>>>Go to the proxy section>> Click open browser option>>Login as SuperAdmin>Click All Courses section >Open any image in a new tab >>Go to the HTTP history in the proxy >>Collect the target url>>Send it to the repeater>>Modify filename="../../../etc/passwd%00.png".

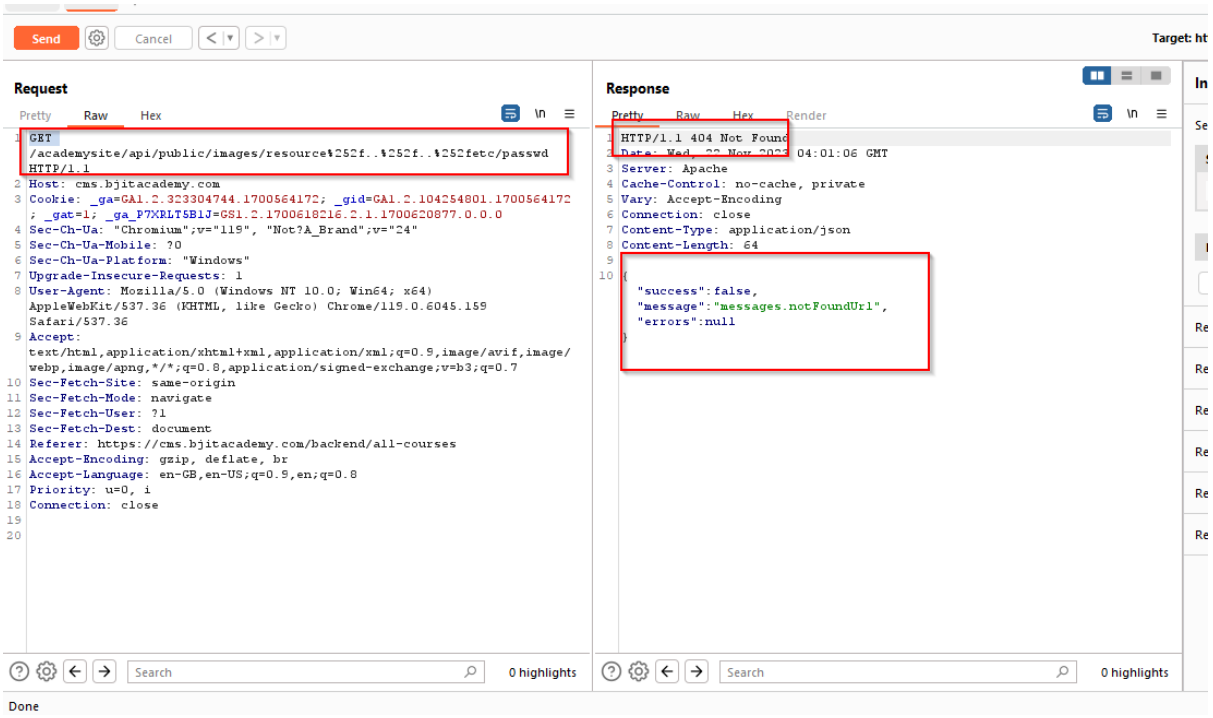


Attempt-8:

Title: Try to discover critical file path to check if traversal sequences stripped non-recursively or not
API:GET /academysite/api/public/images/resource/9lSP6cxyYoQT4PNiJoatUB0bH7pVInygVibSugac.jpg HTTP/1.
Target:https://cms.bjitacademy.com/
Steps:
Start burp suite>>>Go to the proxy section>> Click open browser option>>Login as SuperAdmin>Click All Courses section >Open any image in a new tab >>Go to the HTTP history in the proxy >>Collect the target url>>Send it to the repeater>>Modify filename="**//....//....//etc/passwd**".



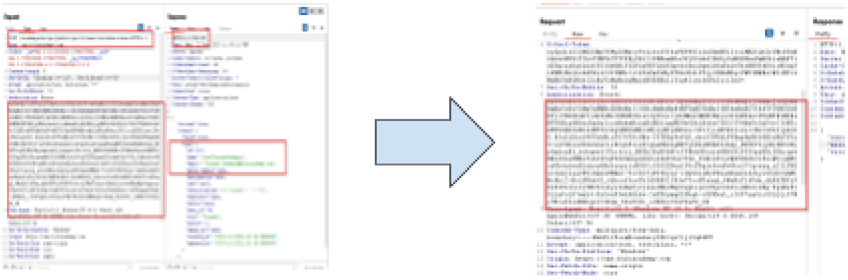
Attempt-9:
Title: Try to discover critical file path to check if traversal sequences stripped with superfluous URL-decode or not
API:GET /academysite/api/public/images/resource/9lSP6cxyYoQT4PNiJoatUB0bH7pVInygVibSugac.jpg HTTP/1.
Target:https://cms.bjitacademy.com/
Steps:
Start burp suite>>>Go to the proxy section>> Click open browser option>>Login as SuperAdmin>Click All Courses section >Open any image in a new tab >>Go to the HTTP history in the proxy >>Collect the target url>>Send it to the repeater>>Modify filename="**%252f..%252f..%252fetc/passwd**"



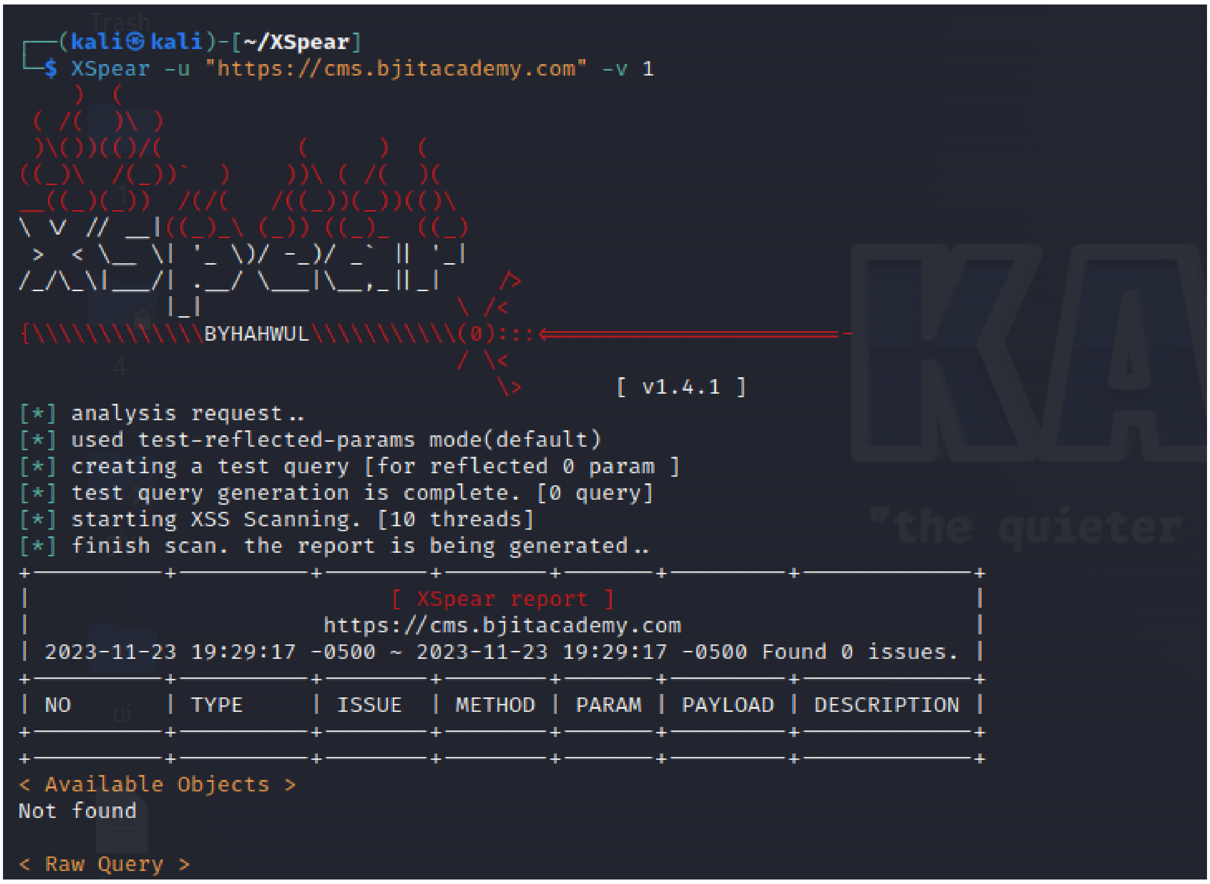
Information disclosure vulnerabilities

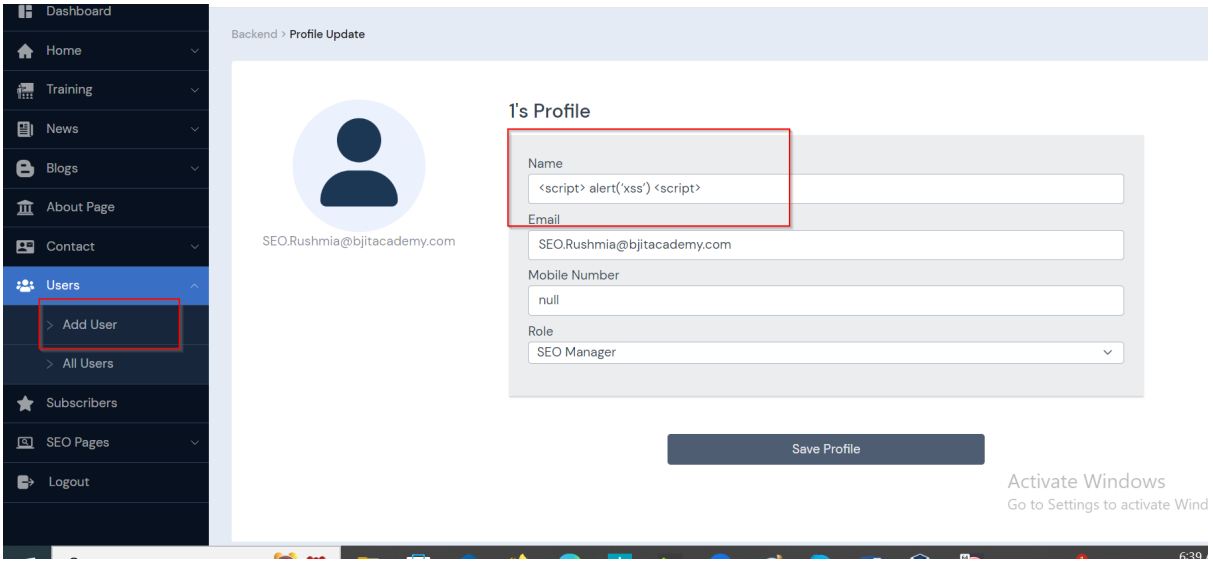
Attempt-10:
Title: Try to find critical information by using robots.txt
Target:https://cms.bjitacademy.com/
Steps:
Start burp suite>>>Go to the proxy section>> Click open browser option>>browse
https://cms.bjitacademy.com/robots.txt

Attempt-11:
Title: Try to Add user as Trainer using bearer token
Target:https://cms.bjitacademy.com/
Steps:
Capture trainer's token and copy it and exchange it to Superadmin's token in POST /academysite/api/public/api/v1/user/register HTTP/1.1



Cross-site scripting (XSS):
Attempt-12:
Title:TRY to find XSS vulnerability
Target:https://cms.bjitacademy.com/
Steps:
Open kali linux>>clone xSpear from github>>navigate to XSpear directory>>start scanning the **cms.bjitacademy.com** website





Command Injection:

Attempt-13:

Title: Check if add user section contains command injection with time delays

Target:https://cms.bjitacademy.com/

Steps:

Login as Super Admin>>go to Users>>Add User>>Capture Request>>Send to the Repeater>>modify name,email,role,certification,password,super_admin_id with ||ping+-c+10+127.0.0.1||