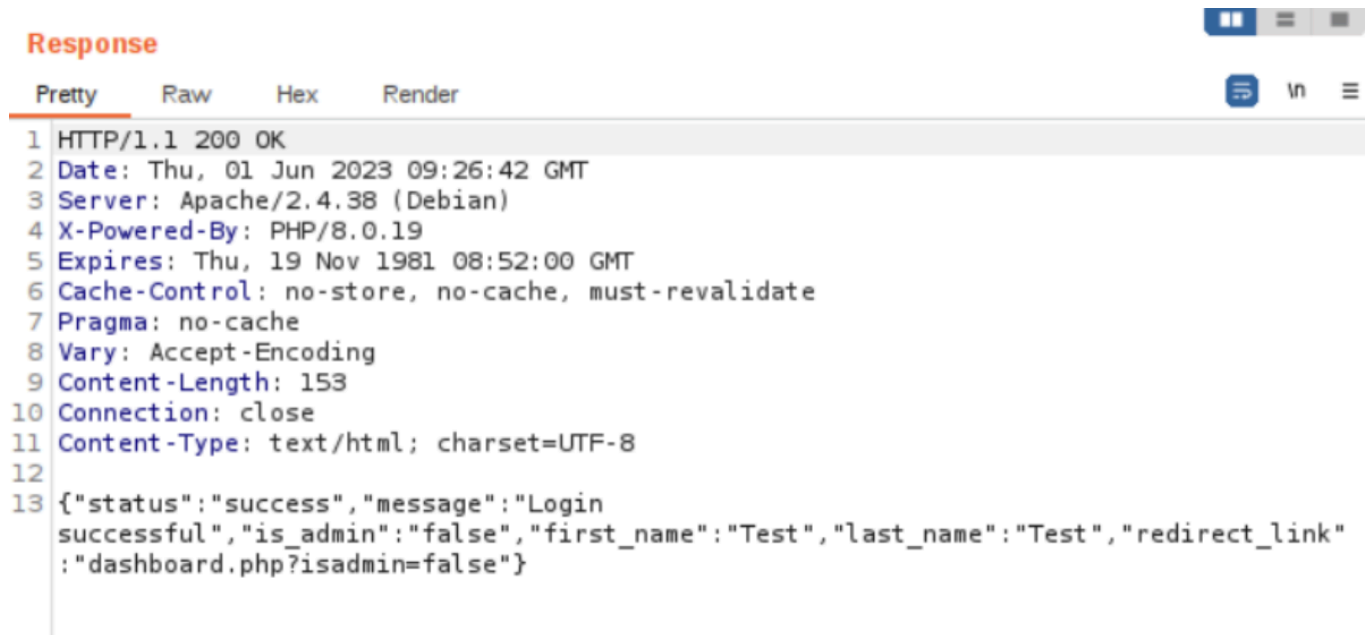


OWASP Broken Access Control

Task 4

Question 1 :

the type of server is Apache as seen below



The screenshot shows a web browser's developer tools with the 'Response' tab selected. The response is an HTTP 200 OK from Apache/2.4.38 (Debian). The response body is a JSON object indicating a successful login.

```
1 HTTP/1.1 200 OK
2 Date: Thu, 01 Jun 2023 09:26:42 GMT
3 Server: Apache/2.4.38 (Debian)
4 X-Powered-By: PHP/8.0.19
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 153
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12
13 {"status": "success", "message": "Login
    successful", "is_admin": "false", "first_name": "Test", "last_name": "Test", "redirect_link"
    : "dashboard.php?isadmin=false"}
```

Question 2: name of the parameter in the JSON response from the login request that contains a redirect link

the answer is: redirect_link as shown below:



The screenshot shows a web browser's developer tools with the 'Response' tab selected. The response is an HTTP 200 OK from Apache/2.4.38 (Debian). The response body is a JSON object indicating a successful login. The 'redirect_link' parameter is highlighted in blue.

```
1 HTTP/1.1 200 OK
2 Date: Mon, 04 Aug 2025 22:09:25 GMT
3 Server: Apache/2.4.38 (Debian)
4 X-Powered-By: PHP/8.0.19
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 156
10 Keep-Alive: timeout=5, max=100
11 Connection: Keep-Alive
12 Content-Type: text/html; charset=UTF-8
13
14 {"status": "success", "message": "Login successful", "is_admin": "false", "first_name": "brian", "last_name": "maitho", "redirect_link": "dashboard.php?isadmin=false"}
```

Question 4: What Burp Suite module allows us to capture requests and responses between ourselves and our target?

The answer is proxy as shown below:

What Burp Suite module allows us to capture requests and responses between ourselves and our target?

Proxy

✓ Correct Answer

Question 5: What is the admin's email that can be found in the online users' table?

The answer is gotten by sending the login request to the repeater and the email is displayed in the response as shown below:

The screenshot displays a web browser window with a 'Request' tab on the left and a 'Response' tab on the right. The 'Request' tab shows the following details:

- URL: GET /dashboard.php HTTP/1.1
- Host: 10.10.179.210
- Upgrade-Insecure-Requests: 1
- User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.0.0 Safari/537.36
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;vrb;q=0.7
- Referer: http://10.10.179.210/login.php
- Accept-Encoding: gzip, deflate, br
- Accept-Language: en-US,en;q=0.9
- Cookie: PHPSESSID=726391f80ca47c090
- Connection: Keep-Alive

The 'Response' tab shows the following details:

- Keep-Alive: timeout=5, max=100
- Connection: Keep-Alive
- Content-Type: text/html; charset=UTF-8
- Cache-Control: no-cache
- Server: Apache/2.4.18 (Ubuntu)
- Set-Cookie: PHPSESSID=726391f80ca47c090

The response body is an HTML document titled 'Dashboard'. It includes a navigation bar with a 'Logout' link, a main content area with a 'Welcome, Brian' message, a 'Status Update Test' section, and a 'Report the bugs' section. The footer contains a table with the text 'Online users' and a list of users: 'admin@admin.com' and 'brayon@gmail.com'.

Task 5 questions and answers:

Answer the questions below

What kind of privilege escalation happened after accessing admin.php?

Vertical

✓ Correct Answer

What parameter allows the attacker to access the admin page?

isadmin

✓ Correct Answer

What is the flag in the admin page?

THM{I_C4n_3xpl01t_B4c}

✓ Correct Answer