

OWASP Top 10 - 2021

Introduction

The OWASP Top 10 - 2021 course on TryHackMe provided an in-depth learning experience on the ten most critical web security risks identified by the Open Web Application Security Project (OWASP). This training involved both theoretical learning and practical exercises to exploit and mitigate these vulnerabilities. The completion of this course enhances our ability to identify, understand, and protect against common web application security threats.

Introduction to the OWASP Top 10 - 2021 vulnerabilities and their significance in web security.

Accessing Machines

Instructions on how to set up and access the virtual machines required for the practical exercises.

Broken Access Control

Task: Learn about broken access control, where users can act outside of their intended permissions.

Challenge: Practical exploitation of Insecure Direct Object References (IDOR).

Cryptographic Failures

Task: Understand issues related to cryptography, such as weak encryption and improper key management.

Supporting Material 1 & 2: Supplementary content to reinforce understanding.

Challenge: Exploit cryptographic weaknesses in a given scenario.

Injection

Task: Explore various types of injection attacks, such as SQL, NoSQL, and command injection.

Command Injection: Specific focus on exploiting command injection vulnerabilities.

Insecure Design

Task: Learn about the importance of secure design principles and the risks associated with poor design.

Security Misconfiguration

Task: Identify and exploit security misconfigurations, which are often due to incomplete or improper configurations.

Vulnerable and Outdated Components

Task: Recognize the dangers of using components with known vulnerabilities.

Exploit: Practical exploitation of a system using outdated components.

Lab: Hands-on lab to reinforce learning.

Identification and Authentication Failures

Task: Understand the importance of robust authentication mechanisms to prevent unauthorized access.

Practical Exercise: Implement and test secure authentication practices.

Software and Data Integrity Failures

Task: Focus on ensuring the integrity of software and data.

Software Integrity Failures: Specific examples of software integrity issues.

Data Integrity Failures: Practical scenarios highlighting data integrity vulnerabilities.

Security Logging and Monitoring Failures

Task: Learn the significance of effective logging and monitoring in detecting and responding to security incidents.

Server-Side Request Forgery (SSRF)

Task: Explore SSRF vulnerabilities, where an attacker can make requests to unintended destinations on behalf of the server.

cs-sa07-24019

John_Mbithi_Mutave

tryhackme.com/r/room/owasp_top102021

Title	Target IP Address	Expires
owasp_top10_2021_v1.2	10.10.110.107	15min 28s

Task 22 10. Server-Side Request Forgery (SSRF)

Task 23 What Next?

What Next?
Why not enroll in our [beginner-level pathway](#) or [find another room](#) to complete?

Answer the questions below

Read the above!

No answer needed ✓ Correct Answer

Created by tryhackme, munra, 1337rce
Room Type: Free Room, Anyone can deploy virtual machines in the room (without being subscribed)!
Users in Room: 78,901
Created: 472 days ago

Copyright TryHackMe 2018-2024

Activate Windows
Go to Settings to activate Windows.

68°F Partly cloudy

tryhackme.com/r/room/owasp_top102021

Title	Target IP Address	Expires
owasp_top10_2021_v1.2	10.10.110.107	16min 7s

Woop woop! Your answer is correct

Woop woop! Your answer is correct

Answer the questions below

Explore the website. What is the only host allowed to access the admin area?
localhost ✓ Correct Answer Hint

Check the "Download Resume" button. Where does the server parameter point to?
secure-file-storage.com ✓ Correct Answer

Using SSRF, make the application send the request to your AttackBox instead of the secure file storage. Are there any API keys in the intercepted request?
THM[Hello_I'm_just_an_API_key] ✓ Correct Answer

Going the Extra Mile: There's a way to use SSRF to gain access to the site's admin area. Can you find it?

Note: You won't need this flag to progress in the room. You are expected to do some research in order to achieve your goal.

No answer needed ✓ Correct Answer

Task 23 What Next?

Activate Windows
Go to Settings to activate Windows.

68°F Partly cloudy

cs-sa07-24019

John_Mbithi_Mutave

tryhackme.com/r/room/owasp_top10_2021

Title	Target IP Address	Expires
owasp_top10_2021_v1.2	10.10.110.107	17min 19s

Woop woop! Your answer is correct

Common payloads: in web applications, it's common for attackers to use known payloads. Detecting the use of these payloads can indicate the presence of someone conducting unauthorised/malicious testing on applications.

Just detecting suspicious activity isn't helpful. This suspicious activity needs to be rated according to the impact level. For example, certain actions will have a higher impact than others. These higher-impact actions need to be responded to sooner; thus, they should raise alarms to get the relevant parties' attention.

Put this knowledge to practice by analysing the provided sample log file. You can download it by clicking the [Download Task Files](#) button at the top of the task.

Answer the questions below

What IP address is the attacker using?

49.99.13.16

Correct Answer Hint

What kind of attack is being carried out?

Brute Force

Correct Answer Hint

Task 22 10. Server-Side Request Forgery (SSRF)

Task 23 What Next?

Activate Windows Go to Settings to activate Windows

Created by Room Type Users in Room Created

68°F Partly cloudy Search

tryhackme.com/r/room/owasp_top10_2021

Title	Target IP Address	Expires
owasp_top10_2021_v1.2	10.10.110.107	18min 48s

Woop woop! Your answer is correct

Session Storage
IndexedDB
Web SQL
Cookies
http://10.10.110.92:8080/
Trust Tokens

What is the name of the website's cookie containing a JWT token?

jwt-session

Correct Answer

Use the knowledge gained in this task to modify the JWT token so that the application thinks you are the user "admin".

No answer needed

Correct Answer

What is the flag presented to the admin user?

THM[Dont_take_cookies_from_strangers]

Correct Answer

Task 21 9. Security Logging and Monitoring Failures

Task 22 10. Server-Side Request Forgery (SSRF)

Task 23 What Next?

Activate Windows Go to Settings to activate Windows

68°F Partly cloudy Search

9:20 AM 6/21/2024

cs-sa07-24019

John_Mbithi_Mutave

tryhackme.com/r/room/owasp_top10_2021_v1.2

Title	Target IP Address	Expires
owasp_top10_2021_v1.2	10.10.110.107	19min 42s

The problem is that an attacker somewhere down the jquery library repository, every could change the content of <https://code.jquery.com/jquery-3.6.1.min.js> to inject malicious code. As a result, anyone visiting your website would now pull the malicious code and execute it into their browsers unknowingly. This is a software integrity failure as your website makes no checks against the third-party library to see if it has changed. Modern browsers allow you to specify a hash along the library's URL so that the library code is executed only if the hash of the downloaded file matches the expected value. This security mechanism is called Subresource Integrity (SRI), and you can read more about it [here](#).

The correct way to insert the library in your HTML code would be to use SRI and include an integrity hash so that if somehow an attacker is able to modify the library, any client navigating through your website won't execute the modified version. Here's how that should look in HTML:

```
<script src="https://code.jquery.com/jquery-3.6.1.min.js" integrity="sha256-o88AwQnZB+VDvE9tvIXrMQaPlFFSUTR+n1dQm1LuPXQ=" crossorigin="anonymous"></script>
```

You can go to <https://www.srihash.org/> to generate hashes for any library if needed.

Answer the questions below

What is the SHA-256 hash of <https://code.jquery.com/jquery-1.12.4.min.js>?

sha256-ZosEbRLbNQzLpnKlkEdrPv7I0y9C27hHQ+Xp8a4MxAQ=

✓ Correct Answer Hint

Task 20 ○ Data Integrity Failures

Task 21 ○ 9. Security Logging and Monitoring Failures

Task 22 ○ 10. Server-Side Request Forgery (SSRF)

Activate Windows
Go to Settings to activate Windows.

tryhackme.com/r/room/owasp_top10_2021_v1.2

Title	Target IP Address	Expires
owasp_top10_2021_v1.2	10.10.110.107	20min 14s

Woop woop! Your answer is correct

Software and Data Integrity Failures

This vulnerability arises from code or infrastructure that uses software or data without using any kind of integrity checks. Since no integrity verification is being done, an attacker might modify the software or data passed to the application, resulting in unexpected consequences. There are mainly two types of vulnerabilities in this category:

- Software Integrity Failures
- Data Integrity Failures

Answer the questions below

Read the above and continue!

No answer needed

✓ Correct Answer

Task 19 ○ Software Integrity Failures

Task 20 ○ Data Integrity Failures

Task 21 ○ 9. Security Logging and Monitoring Failures

Task 22 ○ 10. Server-Side Request Forgery (SSRF)

Activate Windows
Go to Settings to activate Windows.

Task 23 ○ What Now?

68°F
Partly cloudy

Search

9:19 AM
6/21/2024

cs-sa07-24019

John_Mbithi_Mutave

tryhackme.com/r/room/owasp_top102021

Title	Target IP Address	Expires
owasp_top10_2021_v1.2	10.10.110.107	20min 34s

Woop woop! Your answer is correct

Let's understand this with the help of an example, say there is an existing user with the name `admin`, and we want access to their account, so what we can do is try to re-register that username but with slight modification. We will enter "admin" without the quotes (notice the space at the start). Now when you enter that in the username field and enter other required information like email id or password and submit that data, it will register a new user, but that user will have the same rights as the admin account. That new user will also be able to see all the content presented under the user `admin`.

To see this in action, go to <http://10.10.110.107:8088> and try to register with `darren` as your username. You'll see that the user already exists, so try to register "darren" instead, and you'll see that you are now logged in and can see the content present only in darren's account, which in our case, is the flag that you need to retrieve.

Answer the questions below

What is the flag that you found in darren's account?

Answer format: *****

Submit

Now try to do the same trick and see if you can log in as `arthur`.

No answer needed

Complete

What is the flag that you found in arthur's account?

d9ac0f7db4fd460ac3edeb75d75e16e

Correct Answer

Activate Windows

Go to Settings to activate Windows

tryhackme.com/r/room/owasp_top102021

Title	Target IP Address	Expires
owasp_top10_2021_v1.2	10.10.110.107	21min 13s

Woop woop! Your answer is correct

- Brute force attacks:** If a web application uses usernames and passwords, an attacker can try to launch brute force attacks that allow them to guess the username and password using multiple authentication attempts.
- Use of weak credentials:** Web applications should set strong password policies. If applications allow users to set passwords such as "password1" or common passwords, an attacker can easily guess them and access user accounts.
- Weak Session Cookies:** Session cookies are how the server keeps track of users. If session cookies contain predictable values, attackers can set their own session cookies and access users' accounts.

There can be various mitigation for broken authentication mechanisms depending on the exact flaw:

- To avoid password-guessing attacks, ensure the application enforces a strong password policy.
- To avoid brute force attacks, ensure that the application enforces an automatic lockout after a certain number of attempts. This would prevent an attacker from launching more brute-force attacks.
- Implement Multi-Factor Authentication. If a user has multiple authentication methods, for example, using a username and password and receiving a code on their mobile device, it would be difficult for an attacker to get both the password and the code to access the account.

Answer the questions below

I've understood broken authentication mechanisms.

No answer needed

Correct Answer

tryhackme.com/r/room/owasp_top102021

Title	Target IP Address	Expires
owasp_top10_2021_v1.2	10.10.110.107	21min 13s

Woop woop! Your answer is correct

cs-sa07-24019

John_Mbithi_Mutave

tryhackme.com/r/room/owasptop102021

Title	Target IP Address	Expires
owasp_top10_2021_v1.2	10.10.110.107	22min 33s

Task 13 6. Vulnerable and Outdated Components

Vulnerable and Outdated Components

Occasionally, you may find that the company/entity you're pen-testing is using a program with a well-known vulnerability.

For example, let's say that a company hasn't updated their version of WordPress for a few years, and using a tool such as [WPScan](#), you find that it's version 4.6. Some quick research will reveal that WordPress 4.6 is vulnerable to an unauthenticated remote code execution(RCE) exploit, and even better, you can find an exploit already made on [Exploit-DB](#).

As you can see, this would be quite devastating because it requires very little work on the attacker's part. Since the vulnerability is already well known, someone else has likely made an exploit for the vulnerability already. The situation worsens when you realise that it's really easy for this to happen. If a company misses a single update for a program they use, it could be vulnerable to any number of attacks.

Answer the questions below

Read about the vulnerability.

No answer needed ✓ Correct Answer

Task 14 Vulnerable and Outdated Components - Exploit

Task 15 Vulnerable and Outdated Components - Lab

Activate Windows
Go to Settings to activate Windows

68°F Partly cloudy

tryhackme.com/r/room/owasptop102021

Title	Target IP Address	Expires
owasp_top10_2021_v1.2	10.10.110.107	22min 55s

THM{Just_a_tiny_misconfiguration} as part of the challenge top 10 vulnerabilities list.

Navigate to <http://10.10.110.107:86> and try to exploit the security misconfiguration to read the application's source code.

Answer the questions below

Navigate to <http://10.10.110.107:86/console> to access the Werkzeug console.

No answer needed ✓ Correct Answer

Use the Werkzeug console to run the following Python code to execute the `ls -l` command on the server:

```
import os; print(os.popen("ls -l").read())
```

What is the database file name (the one with the .db extension) in the current directory?

todo.db ✓ Correct Answer

Modify the code to read the contents of the `app.py` file, which contains the application's source code. What is the value of the `secret_flag` variable in the source code?

THM{Just_a_tiny_misconfiguration} ✓ Correct Answer 💡 Hint

Task 13 6. Vulnerable and Outdated Components

Activate Windows
Go to Settings to activate Windows

68°F Partly cloudy

tryhackme.com/r/room/owasptop102021

9:17 AM 6/21/2024

cs-sa07-24019

John_Mbithi_Mutave

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "tryhackme.com/r/room/owasp_top102021". The page displays a challenge titled "owasp_top10_2021_v1.2" with a target IP address of 10.10.10.107 and an expiration time of 24min 4s. A green notification bar at the top right says "Woop woop! Your answer is correct". Below the title, there is a text block about insecure design vulnerabilities and a link to the "SSDLC room".

Practical Example

Navigate to <http://10.10.10.107:85> and get into joseph's account. This application also has a design flaw in its password reset mechanism. Can you figure out the weakness in the proposed design and how to abuse it?

Answer the questions below

Try to reset joseph's password. Keep in mind the method used by the site to validate if you are indeed joseph.

No answer needed

✓ Correct Answer

What is the value of the flag in joseph's account?

THM{Not_3ven_c4tz_c0uld_sav3_!l}

✓ Correct Answer

Hint

Task 12 ○ 5. Security Misconfiguration

Task 13 ○ 6. Vulnerable and Outdated Components

Activate Windows
Go to Settings to activate Windows

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "tryhackme.com/r/room/owasp_top102021". The page displays a challenge titled "owasp_top10_2021_v1.2" with a target IP address of 10.10.10.107 and an expiration time of 24min 45s. A red button labeled "Terminate" is visible. Below the title, there is a text block asking about a strange text file in the root directory.

Answer the questions below

What strange text file is in the website's root directory?

drpepper.txt

✓ Correct Answer

How many non-root/non-service/non-daemon users are there?

0

✓ Correct Answer

What user is this app running as?

apache

✓ Correct Answer

What is the user's shell set as?

/sbin/nologin

✓ Correct Answer

What version of Alpine Linux is running?

3.16.0

✓ Correct Answer

Hint

Activate Windows
Go to Settings to activate Windows

Task 11 ○ 4. Insecure Design

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "tryhackme.com/r/room/owasp_top102021". The page displays a challenge titled "owasp_top10_2021_v1.2" with a target IP address of 10.10.10.107 and an expiration time of 24min 45s. A red button labeled "Terminate" is visible. Below the title, there is a text block asking about the version of Alpine Linux running.

cs-sa07-24019

John_Mbithi_Mutave

tryhackme.com/t/room/owasp_top10_2021_v1.2

Title	Target IP Address	Expires
owasp_top10_2021_v1.2	10.10.110.107	34min 40s

Rejected, and the application throws an error.

- Stripping input:** If the input contains dangerous characters, these are removed before processing.

Dangerous characters or input is classified as any input that can change how the underlying data is processed. Instead of manually constructing allow lists or stripping input, various libraries exist that can perform these actions for you.

Answer the questions below

I've understood Injection attacks.

No answer needed ✓ Correct Answer

Task 10 ✓ 3.1. Command Injection

Task 11 ✓ 4. Insecure Design

Task 12 ✓ 5. Security Misconfiguration

Task 13 ✓ 6. Vulnerable and Outdated Components

Task 14 ✓ Vulnerable and Outdated Components - Exploit

Activate Windows
Go to Settings to activate Windows. 

tryhackme.com/t/room/owasp_top10_2021_v1.2

Title	Target IP Address	Expires
owasp_top10_2021_v1.2	10.10.110.107	35min 4s

Have a look around the web app. The developer has left themselves a note indicating that there is sensitive data in a specific directory.

What is the name of the mentioned directory?

/assets ✓ Correct Answer 💡 Hint

Navigate to the directory you found in question one. What file stands out as being likely to contain sensitive data?

webapp.db ✓ Correct Answer

Use the supporting material to access the sensitive data. What is the password hash of the admin user?

Geee9b7ef19179a06954edd0f6c05ceb ✓ Correct Answer

Crack the hash.

What is the admin's plaintext password?

qwertyuiop ✓ Correct Answer 💡 Hint

Log in as the admin. What is the flag?

THM{Yzc2YjdkMjE5N2VjMzNhOTE3NjdIMjdI} ✓ Correct Answer

Activate Windows
Go to Settings to activate Windows. 

Task 9 ✓ 3. Injection

cs-sa07-24019

John_Mbithi_Mutave

Screenshot of a web browser showing two challenges from the CSA2-2024 challenge set.

The top section shows the CrackStation password cracking interface. A user has entered the hash `6eea9b7ef19179a06954edd0f6c05ceb` and selected "md5". The result is shown as "qwertyuop". A reCAPTCHA verification is present.

The bottom section shows the TryHackMe challenge interface for challenge 10. The challenge title is "owasp_top10_2021_v1.2". The user has entered the hash `6eea9b7ef19179a06954edd0f6c05ceb` and selected "md5". The result is shown as "password". A green notification bar says "Woohoo! Your answer is correct".

Both screenshots show a Windows taskbar at the bottom with various icons and system status.

cs-sa07-24019

John_Mbithi_Mutave

Title Target IP Address Expires

owasp_top10_2021_v1.2 10.10.110.107 52min 42s

4|Keith Wayman|4972 1604 3381 8885|12e7a36c0710571b3d827992f4cfe679
5|Annett Scholz|5400 1617 6508 1166|e2795fc96af3f4d6288906a90a52a47f

We can see from the table information that there are four columns: `custID`, `custName`, `creditCard` and `password`. You may notice that this matches up with the results. Take the first row:

0|Joy Paulson|4916 9012 2231 7905|5f4dcc3b5aa765d61d8327deb882cf99

We have the custID (0), the custName (Joy Paulson), the creditCard (4916 9012 2231 7905) and a password hash (5f4dcc3b5aa765d61d8327deb882cf99). In the next task, we'll look at cracking this hash.

Answer the questions below

Read and understand the supporting material on SQLite Databases.

No answer needed

✓ Correct Answer

Task 7 ○ Cryptographic Failures (Supporting Material 2)

Task 8 ○ Cryptographic Failures (Challenge)

Activate Windows

Go to Settings to activate Windows

Task 9 ○ 3. Injection

Title Target IP Address Expires

owasp_top10_2021_v1.2 10.10.110.107 53min 5s

eavesdropper trying to capture your network packets won't be able to recover the content of your email addresses. When we encrypt the network traffic between the client and server, we usually refer to this as **encrypting data in transit**.

- Since your emails are stored in some server managed by your provider, it is also desirable that the email provider can't read their client's emails. To this end, your emails might also be encrypted when stored on the servers. This is referred to as **encrypting data at rest**.

Cryptographic failures often end up in web apps accidentally divulging sensitive data. This is often data directly linked to customers (e.g. names, dates of birth, financial information), but it could also be more technical information, such as usernames and passwords.

At more complex levels, taking advantage of some cryptographic failures often involves techniques such as "Man in The Middle Attacks", whereby the attacker would force user connections through a device they control. Then, they would take advantage of weak encryption on any transmitted data to access the intercepted information (if the data is even encrypted in the first place). Of course, many examples are much simpler, and vulnerabilities can be found in web apps that can be exploited without advanced networking knowledge. Indeed, in some cases, the sensitive data can be found directly on the web server itself.

The web application in this box contains one such vulnerability. To continue, read through the supporting material in the following tasks.

Answer the questions below

Read the introduction to Cryptographic Failures and deploy the machine.

No answer needed

✓ Correct Answer

Task 6 ○ Cryptographic Failures (Supporting Material 1)

Task 7 ○ Cryptographic Failures (Supporting Material 2)

Finance headline
New EU sanction...

8:46 AM 6/21/2024

tryhackme.com/r/room/owasp102021

Title	Target IP Address	Expires
owasp_top10_2021_v1.2	10.10.110.107	53min 30s

No answer needed ✓ Correct Answer

Deploy the machine and go to <http://10.10.110.107> - Login with the username **noot** and the password **test1234**.
No answer needed ✓ Correct Answer

Look at other users' notes. What is the flag?
flag{fivefourthree} ✓ Correct Answer Hint

Task 5 2. Cryptographic Failures

Task 6 Cryptographic Failures (Supporting Material 1)

Task 7 Cryptographic Failures (Supporting Material 2)

Task 8 Cryptographic Failures (Challenge)

Task 9 3. Injection

Task 10 3.1. Command Injection

Activate Windows Go to Settings to activate Windows

SVK - UKR Game score

tryhackme.com/r/room/owasp102021

Cloud Try Hack Me Dashboard Learn Compete Other Access Machines Woop woop! Your answer is correct

Websites have pages that are protected from regular visitors. For example, only the site's admin user should be able to access a page to manage other users. If a website visitor can access protected pages they are not meant to see, then the access controls are broken.

A regular visitor being able to access protected pages can lead to the following:

- Being able to view sensitive information from other users
- Accessing unauthorized functionality

Simply put, broken access control allows attackers to bypass **authorisation**, allowing them to view sensitive data or perform tasks they aren't supposed to.

For example, a **vulnerability was found in 2019**, where an attacker could get any single frame from a YouTube video marked as private. The researcher who found the vulnerability showed that he could ask for several frames and somewhat reconstruct the video. Since the expectation from a user when marking a video as private would be that nobody had access to it, this was indeed accepted as a broken access control vulnerability.

Answer the questions below

Read and understand what broken access control is.
No answer needed ✓ Correct Answer

Task 4 Broken Access Control (IDOR Challenge)

Task 5 2. Cryptographic Failures

89°F Partly sunny

cs-sa07-24019

John_Mbithi_Mutave

The screenshot shows a web browser window with the URL tryhackme.com/r/room/owasptop102021. The page displays a challenge titled "OWASPTop102021".

Challenge Overview: Some tasks will have you learning by doing, often through hacking a virtual machine. First, let's start the Virtual Machine by pressing the Start Machine button at the top of this task.

To access these machines, you need to either:

- Connect using OpenVPN**: Follow the guide [here](#) to connect using OpenVPN.
- Use an in-browser Linux Machine**: If you're [subscribed](#), deploy the in-browser AttackBox!

Answer the questions below

Connect to our network or deploy the AttackBox.

No answer needed ✓ Correct Answer

Tasks:

- Task 3** 1. Broken Access Control
- Task 4** Broken Access Control (IDOR Challenge)
- Task 5** 2. Cryptographic Failures

Activate Windows
Go to Settings to activate Windows

8:35 AM 6/21/2024

The screenshot shows a web browser window with the URL tryhackme.com/r/room/owasptop102021. The page displays a challenge titled "OWASPTop102021".

Challenge Overview: The room has been designed for beginners and assumes no previous security knowledge.

Answer the questions below

Read the above.

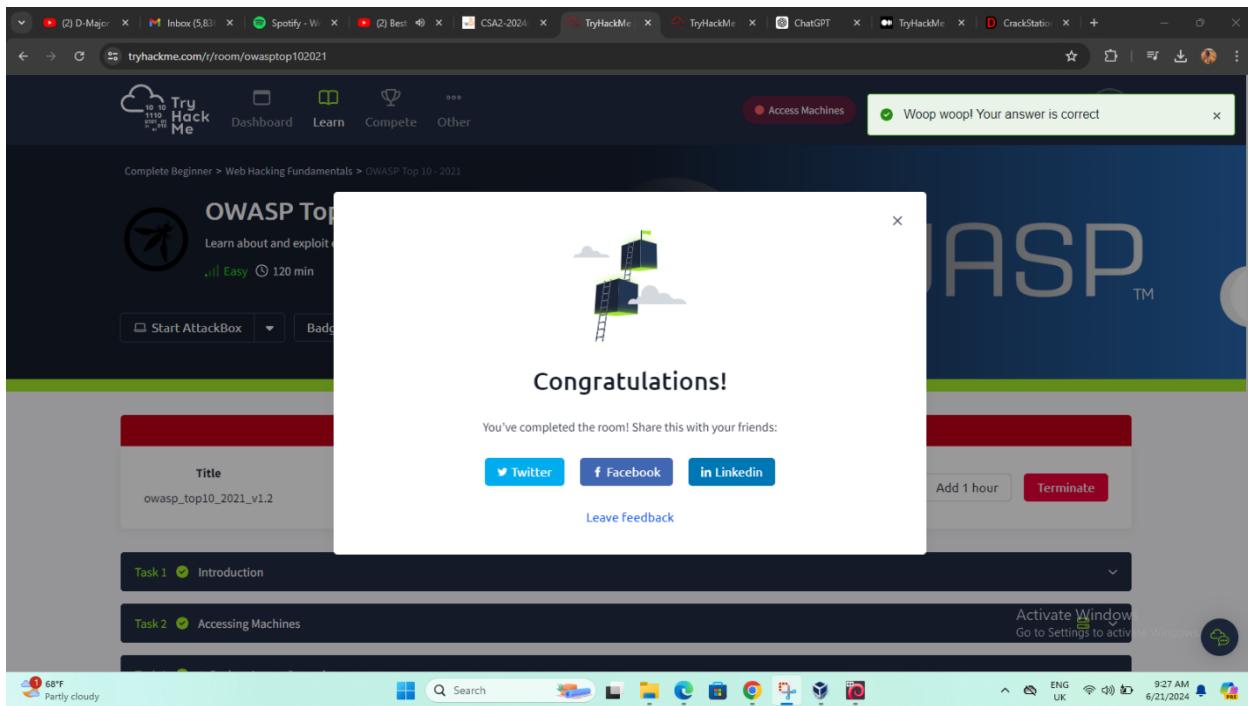
No answer needed ✓ Correct Answer

Tasks:

- Task 2** Accessing Machines
- Task 3** 1. Broken Access Control
- Task 4** Broken Access Control (IDOR Challenge)
- Task 5** 2. Cryptographic Failures

Activate Windows
Go to Settings to activate Windows

8:35 AM 6/21/2024



Shareable link - <http://www.tryhackme.com/r/room/owasptop102021>

Conclusion

Completing the OWASP Top 10 - 2021 course on TryHackMe provided a comprehensive understanding of the most critical web security risks. The combination of theoretical content and practical challenges allowed for the application of knowledge in real-world scenarios, enhancing both detection and mitigation skills. This training is crucial for staying current with web security practices and protecting applications from prevalent threats.

cs-sa07-24019

John_Mbiti_Mutave