

# Vulnerabilities101 Lab

A screenshot of a web browser showing the completion screen for the 'Vulnerabilities 101' room on TryHackMe. The browser address bar shows 'tryhackme.com/room/vulnerabilities101'. The main content area features a large green and yellow bug icon with a checkmark. Below it, the text 'You did it! 🎉 Vulnerabilities 101 complete!' is displayed. A row of five blue boxes contains the following statistics: 'Points earned 72', 'Completed tasks 7', 'Room type Walkthrough', 'Difficulty Easy', and 'Streak 20'. Below these boxes, a message states '80,245 users are actively learning this week'. At the bottom, there are two buttons: 'Leave Feedback' and 'Continue'.

TryHackMe | Vulnerabilities 101

tryhackme.com/room/vulnerabilities101

Sign in

You did it! 🎉 Vulnerabilities 101 complete!

Points earned 72

Completed tasks 7

Room type Walkthrough

Difficulty Easy

Streak 20

80,245 users are actively learning this week

Leave Feedback

Continue

A screenshot of the 'Vulnerabilities 101' room page on TryHackMe. The browser address bar shows 'tryhackme.com/room/vulnerabilities101'. The page header includes the TryHackMe logo, navigation links (Dashboard, Learn, Practice, Compete), a search bar, a 'Go Premium' button, a '20' badge, and a user profile icon. The main content area features a large green and yellow bug icon, the title 'Vulnerabilities 101', and a description: 'Understand the flaws of an application and apply your researching skills on some vulnerability databases.' Below this, there are buttons for 'Share your achievement', 'Show Split View', 'Save Room', '2757 Recommend', and 'Options'. A green bar at the bottom indicates 'Room completed (100%)'. Below this bar, a list of tasks is shown: 'Task 1 Introduction', 'Task 2 Introduction to Vulnerabilities', and 'Task 3 Scoring Vulnerabilities (CVSS & VPR)'. Each task has a green checkmark and a dropdown arrow.

TryHackMe

Dashboard Learn Practice Compete

Go Premium 20

h

Learn > Vulnerabilities 101

Vulnerabilities 101

Understand the flaws of an application and apply your researching skills on some vulnerability databases.

20 min 1,54,861

Share your achievement

Show Split View

Save Room

2757 Recommend

Options

Room completed (100%)

Task 1 Introduction

Task 2 Introduction to Vulnerabilities

Task 3 Scoring Vulnerabilities (CVSS & VPR)

TryHackMe | Vulnerabilities 101

tryhackme.com/room/vulnerabilities101

Sign in

Room completed (100%)

Task 1 Introduction


Cybersecurity is big business in the modern-day world. The hacks that we hear about in newspapers are from exploiting vulnerabilities. In this room, we're going to explain exactly what a vulnerability is, the types of vulnerabilities and how we can exploit these for success in our penetration testing endeavours.

An enormous part of penetration testing is knowing the skills and resources for whatever situation you face. This room is going to introduce you to some resources that are essential when researching vulnerabilities, specifically, you are going to be introduced to:

- What vulnerabilities are
- Why they're worthy of learning about
- How are vulnerabilities rated
- Databases for vulnerability research
- A showcase of how vulnerability research is used on ACKme's engagement

Answer the questions below

Read this task!

No answer needed

✓ Correct Answer

TryHackMe | Vulnerabilities 101

tryhackme.com/room/vulnerabilities101

Sign in

Room completed (100%)

Credentials	dashboard may have the username and password of "admin". These are easy to guess by an attacker.
Application Logic	These vulnerabilities are a result of poorly designed applications. For example, poorly implemented authentication mechanisms that may result in an attacker being able to impersonate a user.
Human-Factor	Human-Factor vulnerabilities are vulnerabilities that leverage human behaviour. For example, phishing emails are designed to trick humans into believing they are legitimate.

As a cybersecurity researcher, you will be assessing applications and systems - using vulnerabilities against these targets in day-to-day life, so it is crucial to become familiar with this discovery and exploitation process.

Answer the questions below

An attacker has been able to upgrade the permissions of their system account from "user" to "administrator". What type of vulnerability is this?

Operating System

✓ Correct Answer

You manage to bypass a login panel using cookies to authenticate. What type of vulnerability is this?

Application Logic

✓ Correct Answer

Task 3 Scoring Vulnerabilities (CVSS & VPR)

TryHackMe | Vulnerabilities 101

tryhackme.com/room/vulnerabilities101

Room completed (100%)

Scorings are not final and are very dynamic, meaning the priority a vulnerability should be given can change as the vulnerability ages.

Intentionally left blank.

Answer the questions below

What year was the first iteration of CVSS published?

2005

✓ Correct Answer

If you wanted to assess vulnerability based on the risk it poses to an organisation, what framework would you use?

Note: We are looking for the acronym here.

VPR

✓ Correct Answer

If you wanted to use a framework that was free and open-source, what framework would that be?

Note: We are looking for the acronym here.

CVSS

✓ Correct Answer

Task 4 Vulnerability Databases

TryHackMe | Vulnerabilities 101

tryhackme.com/room/vulnerabilities101

Room completed (100%)

2021-08-02	✗	Online Hotel Reservation System 1.0 - Multiple Cross-site scripting (XSS)	WebApps	PHP	Mohammad Koochaki
2021-08-02	✗	Neo4j 3.4.18 - RMI based Remote Code Execution (RCE)	Remote	Java	Christopher Ellis
2021-08-02	✗	Men Salon Management System 1.0 - SQL Injection Authentication Bypass	WebApps	PHP	Akshay Khanna
2021-07-29	✗	Oracle FatWire 6.3 - Multiple Vulnerabilities	WebApps	Multiple	J. Francisco Bolivar
2021-07-29	✗	CloverDX 5.9.0 - Cross-Site Request Forgery (CSRF) to Remote Code Execution (RCE)	WebApps	Java	niebardzo
2021-07-29	✗	Care2x Integrated Hospital Info System 2.7 - Multiple SQL Injection	WebApps	PHP	securityforeveryone.com
2021-07-29	✗	IntelliChoice eFORCE Software Suite 2.5.9 - Username Enumeration	WebApps	ASPX	LiquidWorm
2021-07-29	✗	Longjing Technology BEMS API 1.21 - Remote Arbitrary File Download	WebApps	Hardware	LiquidWorm
2021-07-29	✗	Denver IP Camera SHO-110 - Unauthenticated Snapshot	WebApps	Hardware	Ivan Nikolsky

Answer the questions below

Using **NVD**, how many CVEs were published in July 2021?

1554

✓ Correct Answer

Hint

Who is the author of **Exploit-DB**?

OffSec

✓ Correct Answer

5 An Example of Finding a Vulnerability

TryHackMe | Vulnerabilities 101

tryhackme.com/room/vulnerabilities101

Room completed (100%)

Filters Reset All

Search: Tomcat 9.0

Date	D	A	V	Title	Type	Platform	Author
2021-07-13			X	Apache Tomcat 9.0.0.M1 - Cross-Site Scripting (XSS)	WebApps	Multiple	Central InfoSec
2021-07-13			X	Apache Tomcat 9.0.0.M1 - Open Redirect	WebApps	Multiple	Central InfoSec
2020-01-08			X	Tomcat proprietaryEvaluate 9.0.0.M1 - Sandbox Escape	WebApps	Java	hantwister
2017-10-09			✓	Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)	WebApps	JSP	intx0x80
2017-09-20			X	Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)	WebApps	Windows	x0legend

Showing 1 to 5 of 5 entries (filtered from 44,305 total entries)

FIRST PREVIOUS 1 NEXT LAST

Great! After searching Exploit-DB, there are a total of five exploits that may be useful to us for this specific version of the application.

Answer the questions below

What type of vulnerability did we use to find the name and version of the application in this example?

Version Disclosure

✓ Correct Answer

6 Showcase: Exploiting Ackme's Application

TryHackMe | Vulnerabilities 101

tryhackme.com/room/vulnerabilities101

Room completed (100%)

Task 4 ✓ Vulnerability Databases

Task 5 ✓ An Example of Finding a Vulnerability

Task 6 ✓ Showcase: Exploiting Ackme's Application

It is your first week on the job as Jr. Penetration tester at ThePentestingCo. For your first engagement, you are shadowing a Sr. Penetration Tester within the company.

Deploy the site attached to this task and follow the steps that the Sr. Penetration Tester took to exploit a vulnerability against ACKme IT Service's infrastructure.

Complete the engagement to retrieve a flag.

Answer the questions below

Follow along with the showcase of exploiting ACKme's application to the end to retrieve a flag. What is this flag?

THM{ACKME\_ENGAGEMENT}

✓ Correct Answer

7 Conclusion

TryHackMe | Vulnerabilities 101

tryhackme.com/room/vulnerabilities101

Room completed (100%)

Task 5 ✓ An Example of Finding a Vulnerability

Task 6 ✓ Showcase: Exploiting Ackme's Application

Task 7 ✓ Conclusion


Nice work! We've made it to the end. This room has served as an introductory to vulnerability research and some skills and resources this requires, where you have practically applied this knowledge.

Answer the questions below

Continue on your learning with the additional rooms in this [module](#).

No answer needed

✓ Correct Answer



Glad you're enjoying it! What did you love the most?

1

2

3

4

5

6

7

8

9

10

TryHackMe | Vulnerabilities 101

tryhackme.com/room/vulnerabilities101

Room completed (100%)

Task 6 ✓ Showcase: Exploiting Ackme's Application

Task 7 ✓ Conclusion


Nice work! We've made it to the end. This room has served as an introductory to vulnerability research and some skills and resources this requires, where you have practically applied this knowledge.

Answer the questions below

Continue on your learning with the additional rooms in this [module](#).

No answer needed

✓ Correct Answer



Thank you! 🎉

Your feedback helps us improve our content! We appreciate the time you took to share your thoughts!

✓ Close