Content Discovery TryHackme

Mukilan Baskaran · Follow
Published in InfoSec Write-ups
3 min read · Oct 7, 2021

Listen Share More

Hi, amazing fellow hackers, I produced an interesting topic web content discovery. It is useful in bug bounty and the most important thing during recon.

Content can be different types such as images, files, videos, and so on.

There are 3 main ways to discover content on web pages which are:

Manually, Automated, Osint(Open-Source Intelligence) methods.

> ***What is the Content Discovery method that begins with M?***

Ans: Manually

> ***What is the Content Discovery method that begins with A?***

Ans: Automated

> ***What is the Content Discovery method that begins with O?***

Ans: OSINT

Let us investigate manual discovery, there are so many ways lookup for manual discovery, and one thing for it is *robots.txt. Robots.txt document provides which page should not be allowed to show or crawl webpages.*

> ***What is the directory in the robots.txt that isn't allowed to be viewed by web crawlers?***

Ans: /staff-portal

Next, we move on to manual discovery by sitemap.xml which provides the page's owner like to list out on the website.

> ***What is the path of the secret area that can be found in the sitemap.xml file?***

Ans: /s3cr3t-area

The next step is the manual discovery by HTTP headers. HTTP Headers sometimes for use command ***curl http://machine-ip -v.***

> ***What is the flag value from the X-FLAG header?***

Ans: THM{HEADER_FLAG}

The next one is the manual discovery by framework stack. For detailed versions and more important details we can see the documentation part

> ***What is the flag from the framework's administration portal?***

Ans: THM{CHANGE_DEFAULT_CREDENTIALS}

follow instructions on the documentation you would get the flag.

Next Osint — Google hacking/dorks

Google dorks are used to getting customized content from google search engines. From you could get exposed passwords or hidden stuff from websites.

> *It can be filtered by* **site, inurl, filetype, intitle**
>
> ***What Google dork operator can be used to only show results from a particular site?***

Ans: site:

Wappalyzer is an online tool and extension is used to locate web technologies and version numbers.

> ***What online tool can be used to identify what technologies a website is running?***

Ans: Wappalyzer

Waybackmachine is a historical archive used for finding any previous web content which is now alive or not.

> ***What is the website address for the Wayback Machine?***

Ans: https://archive.org/web/

Github is another important website in which we can look up sensitive files such as config files, passwords, auth files, and so on. Git is a version control system that makes keeping track of files in a project.

> ***What is Git?***

Ans: version control system

Content discovery by Osint — S3 Buckets, S3 buckets are storage services provided by AWS. In this, some files are allocated by the public and some of them are private. In case it is incorrectly set which may lead to vulnerability.

> *The format of s3 buckets is http(s)://**{name}.s3.amazonaws.com***

One similar automation method is by using the company name followed by common terms {**name**}-assets, {**name**}-www, {**name**}-public, {**name**}-private, etc.

> ***What URL format do Amazon S3 buckets end in?***

Ans: .s3.amazonaws.com

Finally, we gonna see Automated discovery, which is simple, easy, and time-consuming compared to manual discovery. For this, we could use ***ffuf, dirb*** and ***gobuster*** so on.

> *Ex for **ffuf***

```
user@machine$ ffuf -w /usr/share/wordlists/SecLists/Discovery/Web-
Content/common.txt -u http://MACHINE_IP/FUZZ
```

> *Ex for **dirb***

```
user@machine$ dirb http://MACHINE_IP/
/usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt
```

> *Ex for* **gobuster**

```
user@machine$ gobuster dir --url http://MACHINE_IP/ -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt
```

> ***What is the name of the directory beginning "/mo…." that was discovered?***

Ans: /monthly

> ***What is the name of the log file that was discovered?***

Ans: /development.log

Tryhackme Tryhackme Walkthrough Tryhackme Writeup Bug Bounty

Content Discovery

Follow

Published in InfoSec Write-ups

49K Followers · Last published 9 hours ago

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. Subscribe to our weekly newsletter for the coolest infosec updates: https://weekly.infosecwriteups.com/

Follow

Written by Mukilan Baskaran

619 Followers · 917 Following

CTF player | Cyber Security Enthusiast

No responses yet

What are your thoughts?

Respond

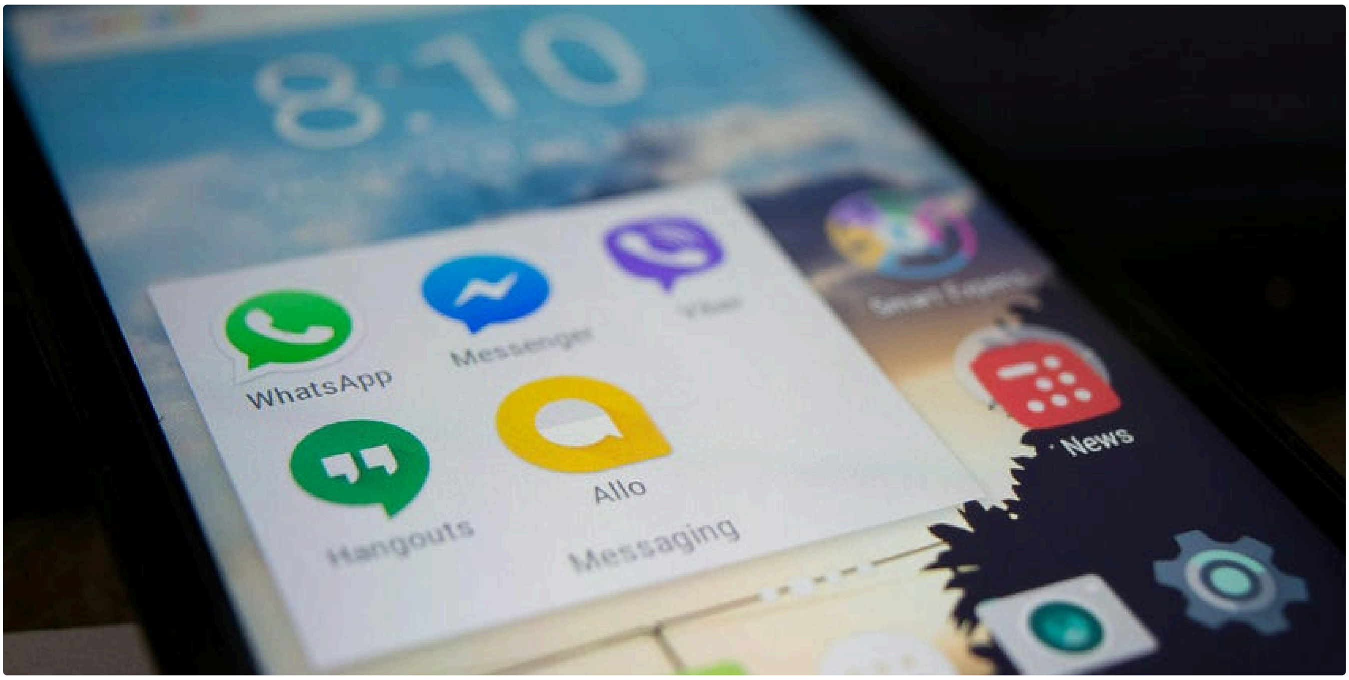
More from Mukilan Baskaran and InfoSec Write-ups

In System Weakness by Mukilan Baskaran

TryHackMe: Advent of Cyber 2024 Day 1 Solutions Guide

Day 1: Maybe SOC-mas music, he thought, doesn't come from a store?

Dec 12, 2024 50 1

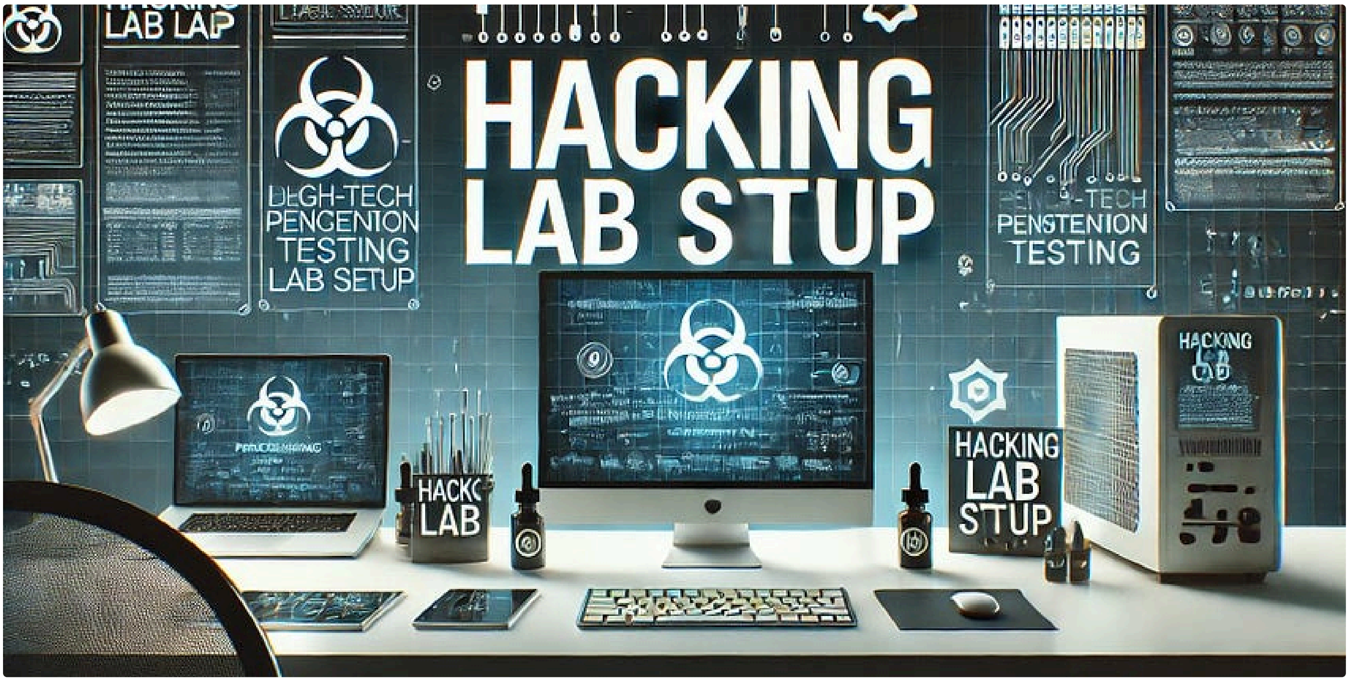


In InfoSec Write-ups by Visir

Could You Be the Next Victim? How to Protect Your Google Account Now

Today, nearly everyone is connected to the internet, and this dependency grew exponentially during the COVID-19 pandemic. With more people…

✦ 5d ago 15

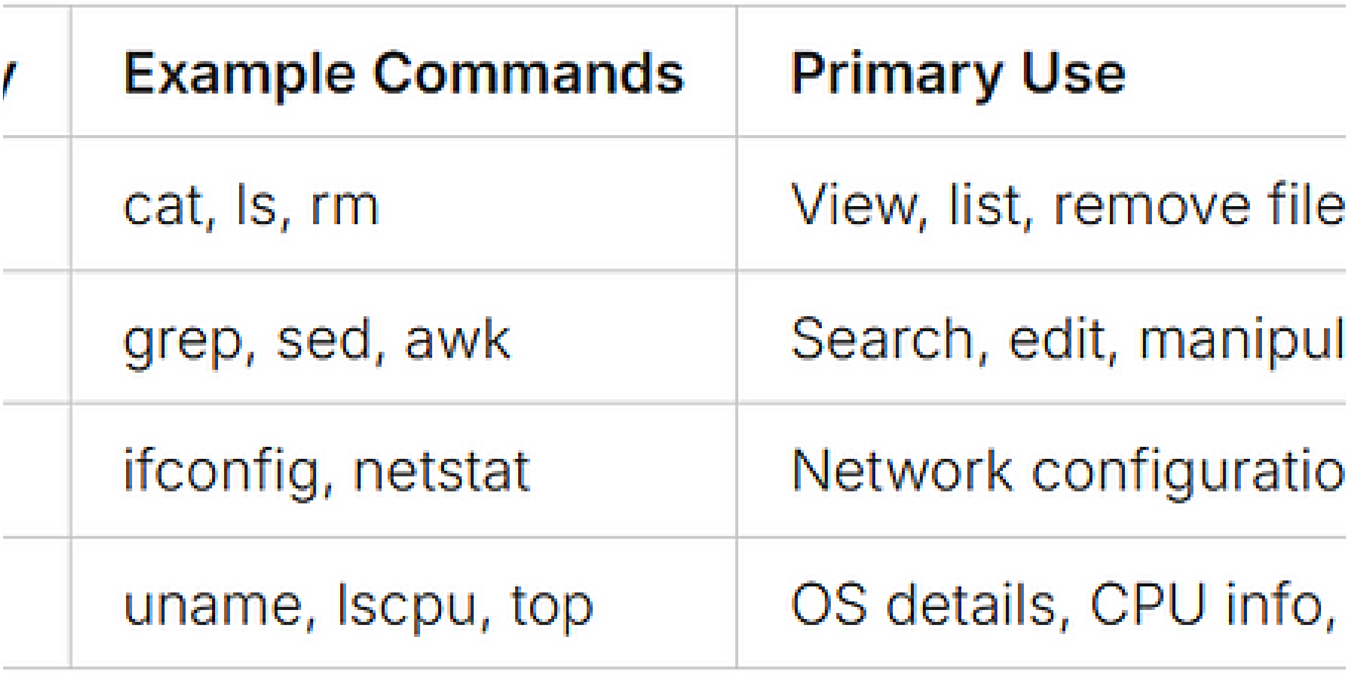


In InfoSec Write-ups by Shanzah Shahid

Hack Like a Pro: Mastering Penetration Testing with Virtual vs Physical Lab Setups

Learn how to build a powerful, cost-effective testing environment to sharpen your ethical hacking skills.

✦ 2d ago 44 2



/	Example Commands	Primary Use
	cat, ls, rm	View, list, remove file
	grep, sed, awk	Search, edit, manipul
	ifconfig, netstat	Network configuratio
	uname, lscpu, top	OS details, CPU info,

In InfoSec Write-ups by Mukilan Baskaran

Bash Scripting: Guide for Security & Bug Bounty Hunters

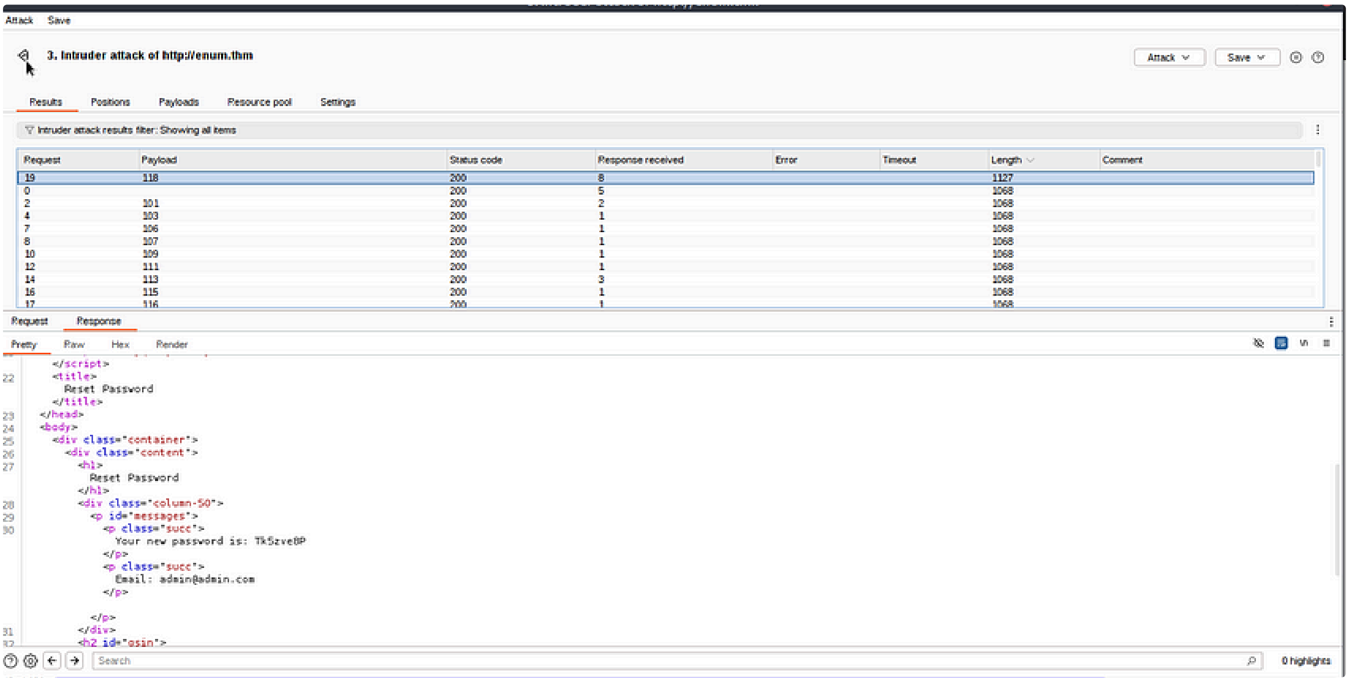
Have you ever wondered how top hackers automate their work? The secret is Bash scripting.

Dec 23, 2024 12

See all from Mukilan Baskaran

See all from InfoSec Write-ups

Recommended from Medium



3. Intruder attack of http://enum.thm

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
19	118	200	8			1127	
0		200	5			1068	
2	101	200	2			1068	
4	103	200	1			1068	
7	106	200	1			1068	
8	107	200	1			1068	
10	109	200	1			1068	
12	111	200	1			1068	
14	113	200	3			1068	
16	115	200	1			1068	
17	116	200	1			1068	

```
    </script>
    <title>
      Reset Password
    </title>
  </head>
  <body>
    <div class="container">
      <div class="content">
        <h1>
          Reset Password
        </h1>
        <div class="column-50">
          <p id="messages">
            <p class="succ">
              Your new password is: TkSzve8P
            </p>
            <p class="succ">
              Email: admin@admin.com
            </p>

          </p>
        </div>
        <h2 id="osin">
```

embossdotar

TryHackMe — Enumeration & Brute Force — Writeup

Key points: Enumeration | Brute Force | Exploring Authentication Mechanisms | Common Places to Enumerate | Verbose Errors | Password Reset…

Jul 31, 2024 26

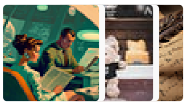
In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

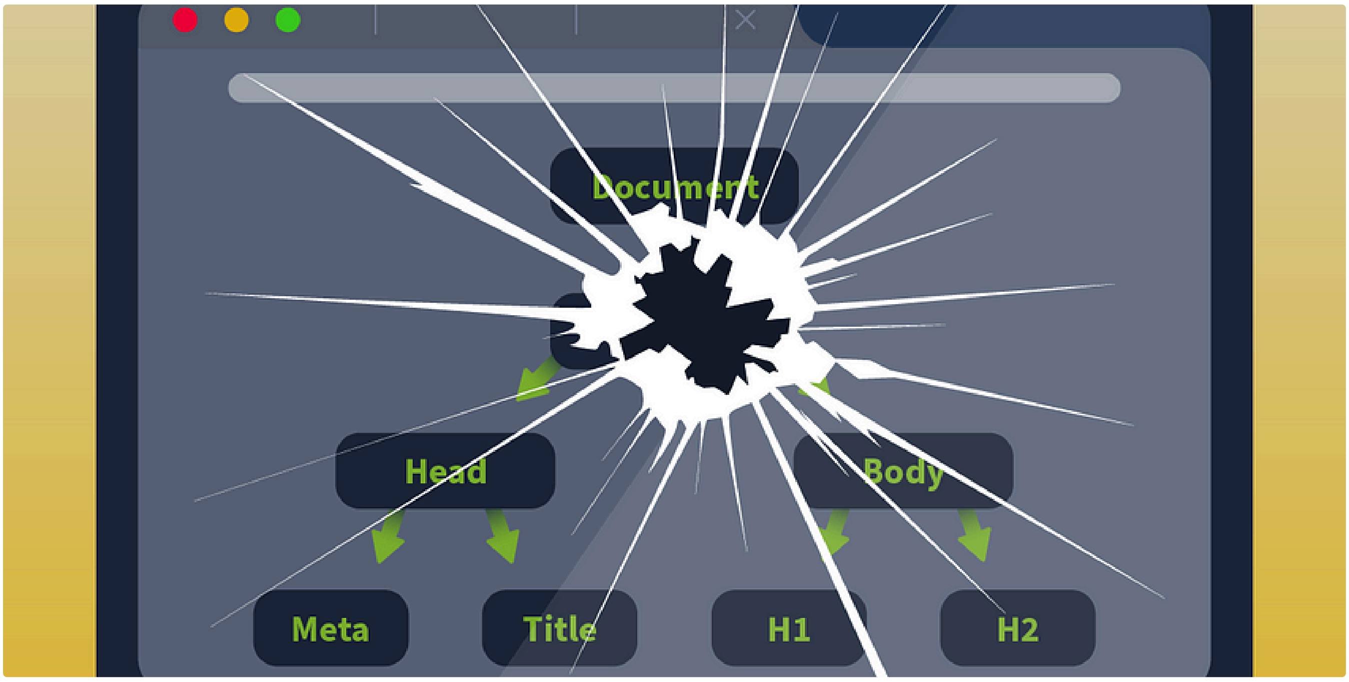
Nov 5, 2024 60

Lists



Medium's Huge List of Publications Accepting Submissions

377 stories · 4308 saves

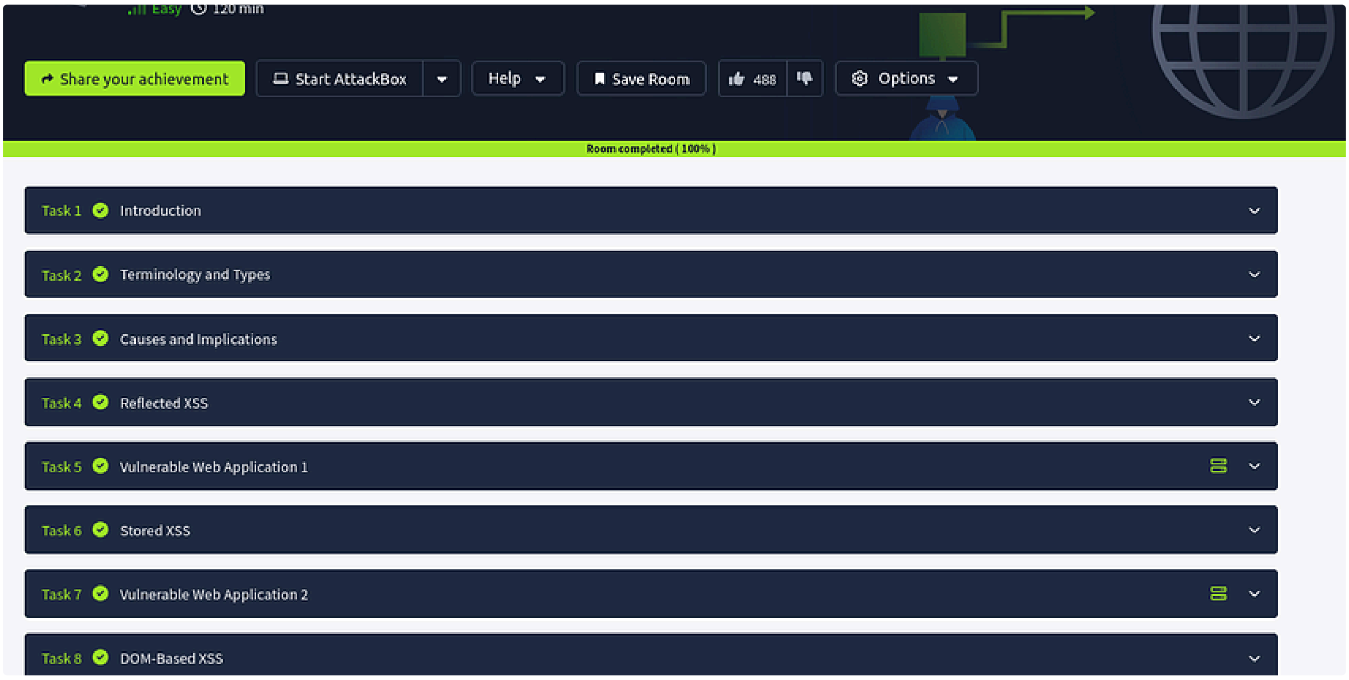


Jawstar

DOM-Based Attacks Tryhackme Write-up

Task 1 : Introduction

Nov 20, 2024



Room completed (100%)

Task 1 Introduction

Task 2 Terminology and Types

Task 3 Causes and Implications

Task 4 Reflected XSS

Task 5 Vulnerable Web Application 1

Task 6 Stored XSS

Task 7 Vulnerable Web Application 2

Task 8 DOM-Based XSS

Jawstar

XSS Tryhackme Walkthrough Write up

Overview:

Nov 20, 2024 4

In System Weakness by Sunny Singh Verma [SuNnY]

The Sticker Shop Motion Graphics TryHackMe Writeup | Beginner Friendly | Detailed Walkthrough |…

Motions graphics writeup for TryHackme Room → [The Sticker Shop]

Dec 22, 2024 👏 55

Jawstar

Advent of Cyber 2024 {Day - 23} Tryhackme Answers

The Story

✦ Dec 24, 2024

See more recommendations