

★ Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



# Putting it all together | Tryhackme Writeup/Walkthrough | By Md Amiruddin



Md Amiruddin · Follow

Published in InfoSec Write-ups

7 min read · Mar 5, 2023



Listen



Share

... More

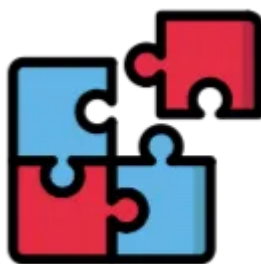
Learn how all the individual components of the web work together to bring you access to your favourite web sites.



Room Link : <https://tryhackme.com/room/puttingitaltogether>

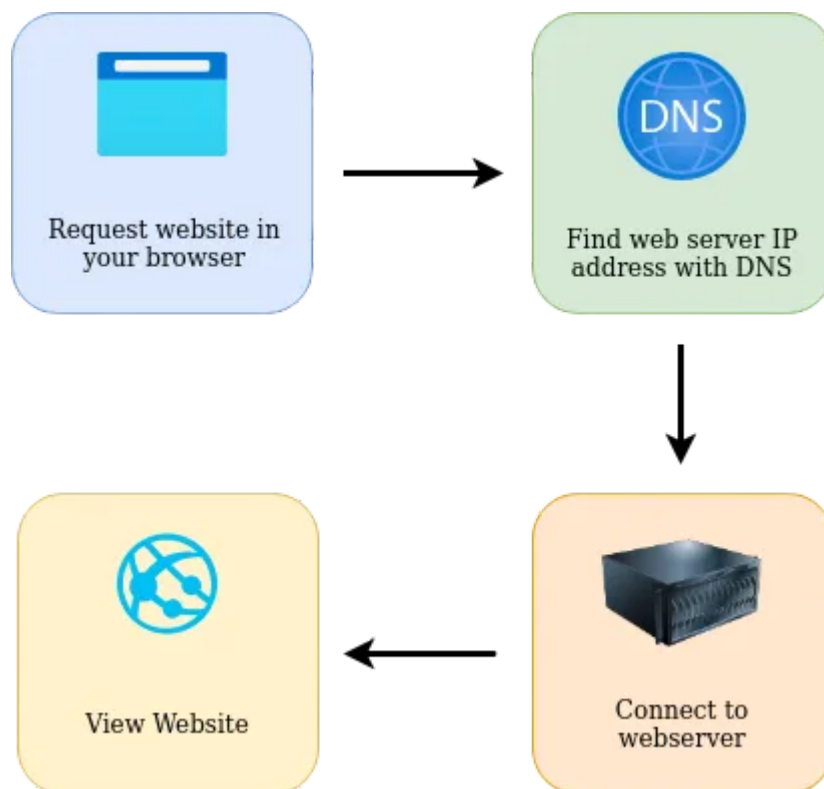
## Task 1: Putting It All Together

### Putting It All Together



From the previous modules, you'll have learned that quite a lot of things go on behind the scenes when you request a webpage in your browser.

To summarise, when you request a website, your computer needs to know the server's IP address it needs to talk to; for this, it uses DNS. Your computer then talks to the web server using a special set of commands called the HTTP protocol; the webserver then returns HTML, JavaScript, CSS, Images, etc., which your browser then uses to correctly format and display the website to you.



There are also a few other components that help the web run more efficiently and provide extra features.

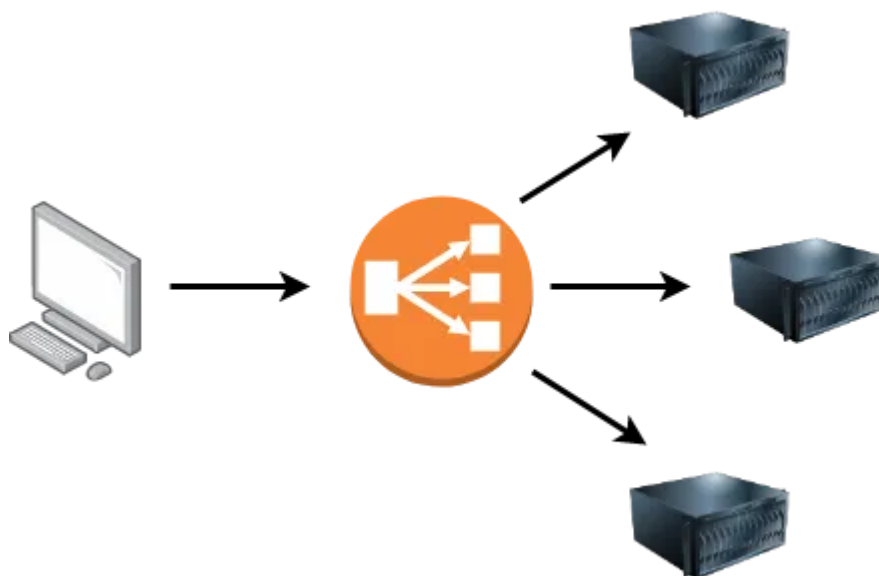
## Task 2 : Other Components

### Load Balancers

When a website's traffic starts getting quite large or is running an application that needs to have high availability, one web server might no longer do the job. Load balancers provide two main features, ensuring high traffic websites can handle the load and providing a failover if a server becomes unresponsive.

When you request a website with a load balancer, the load balancer will receive your request first and then forward it to one of the multiple servers behind it. The load balancer uses different algorithms to help it decide which server is best to deal with the request. A couple of examples of these algorithms are **round-robin**, which sends it to each server in turn, or **weighted**, which checks how many requests a server is currently dealing with and sends it to the least busy server.

Load balancers also perform periodic checks with each server to ensure they are running correctly; this is called a **health check**. If a server doesn't respond appropriately or doesn't respond, the load balancer will stop sending traffic until it responds appropriately again.

[Open in app ↗](#)**Medium**

videos, and host them across thousands of servers all over the world. When a user requests one of the hosted files, the CDN works out where the nearest server is physically located and sends the request there instead of potentially the other side of the world.

## Databases

Often websites will need a way of storing information for their users. Webservers can communicate with databases to store and recall data from them. Databases can range from just a simple plain text file up to complex clusters of multiple servers providing speed and resilience. You'll come across some common databases: MySQL, MSSQL, MongoDB, GraphQL, Postgres, and more; each has its specific features.

## WAF (Web Application Firewall)

A WAF sits between your web request and the web server; its primary purpose is to protect the webserver from hacking or denial of service attacks. It analyses the web requests for common attack techniques, whether the request is from a real browser rather than a bot. It also checks if an excessive amount of web requests are being

sent by utilising something called rate limiting, which will only allow a certain amount of requests from an IP per second. If a request is deemed a potential attack, it will be dropped and never sent to the webserver.



**Answer the questions below :**

1. What can be used to host static files and speed up a clients visit to a website?  
A. CDN
2. What does a load balancer perform to make sure a host is still alive?  
A. health check
3. What can be used to help against the hacking of a website?  
A. WAF

## Task 3 : How Web Servers Work

### How Web servers work.

#### What is a Web Server?

A web server is a software that listens for incoming connections and then utilises the HTTP protocol to deliver web content to its clients. The most common web server software you'll come across is Apache, Nginx, IIS and NodeJS. A Web server delivers files from what's called its root directory, which is defined in the software settings. For example, Nginx and Apache share the same default location of `/var/www/html` in Linux operating systems, and IIS uses `C:\inetpub\wwwroot` for the Windows operating systems. So, for example, if you requested the file <http://www.example.com/picture.jpg>, it would send the file `/var/www/html/picture.jpg` from its local hard drive.

## Virtual Hosts

Web servers can host multiple websites with different domain names; to achieve this, they use virtual hosts. The web server software checks the hostname being requested from the HTTP headers and matches that against its virtual hosts (virtual hosts are just text-based configuration files). If it finds a match, the correct website will be provided. If no match is found, the default website will be provided instead.

Virtual Hosts can have their root directory mapped to different locations on the hard drive. For example, one.com being mapped to /var/www/website\_one, and two.com being mapped to /var/www/website\_two

There's no limit to the number of different websites you can host on a web server.

## Static Vs Dynamic Content

Static content, as the name suggests, is content that never changes. Common examples of this are pictures, javascript, CSS, etc., but can also include HTML that never changes. Furthermore, these are files that are directly served from the webserver with no changes made to them.

Dynamic content, on the other hand, is content that could change with different requests. Take, for example, a blog. On the homepage of the blog, it will show you the latest entries. If a new entry is created, the home page is then updated with the latest entry, or a second example might be a search page on a blog. Depending on what word you search, different results will be displayed.

These changes to what you end up seeing are done in what is called the **Backend** with the use of programming and scripting languages. It's called the Backend because what is being done is all done behind the scenes. You can't view the websites' HTML source and see what's happening in the Backend, while the HTML is the result of the processing from the Backend. Everything you see in your browser is called the **Frontend**.

## Scripting and Backend Languages

There's not much of a limit to what a backend language can achieve, and these are what make a website interactive to the user. Some examples of these languages (in no particular order :p) are PHP, Python, Ruby, NodeJS, Perl and many more. These languages can interact with databases, call external services, process data from the

user, and so much more. A very basic PHP example of this would be if you requested the website <http://example.com/index.php?name=adam>

If index.php was built like this:

```
<html><body>Hello <?php echo $_GET["name"]; ?></body></html>
```

It would output the following to the client:

```
<html><body>Hello adam</body></html>
```

You'll notice that the client doesn't see any PHP code because it's on the Backend. This interactivity opens up a lot more security issues for web applications that haven't been created securely, as you learn in further modules.

**Answer the questions below :**

1. What does web server software use to host multiple sites?  
A. Virtual Hosts
2. What is the name for the type of content that can change?  
A. Dynamic
3. Does the client see the backend code? Yay/Nay  
A. Nay

## Task 4 : Quiz

### The Quiz

Click the "View Site" button on the right. Using everything you've learnt from the other modules, drag and drop the tiles into the correct order of how a request to a website works to reveal the flag.

**Note:** When placing a tile in the correct position, it will highlight in green. When a tile is in the wrong spot, it will highlight in red. Make sure **not** to refresh the page, as it will reset the tiles all to blank again!



Request  
tryhackme.com in  
your browser.



Check Local Cache  
for IP Address



Check your  
recursive DNS  
Server for Address







**Answer the questions below :**

1. Flag

A. THM{YOU\_GOT\_THE\_ORDER}

**Thankyou For Reading.**

Tryhackme

Tryhackme Walkthrough

Tryhackme Writeup

Infosec

Web Server



Follow

## Published in InfoSec Write-ups

49K Followers · Last published 10 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 Md Amiruddin

155 Followers · 6 Following

This is a profile of a cybersecurity enthusiast and CTF writer. He is an experienced information security professional and highly motivated individual.

**No responses yet**



What are your thoughts?

Respond

## More from Md Amiruddin and InfoSec Write-ups



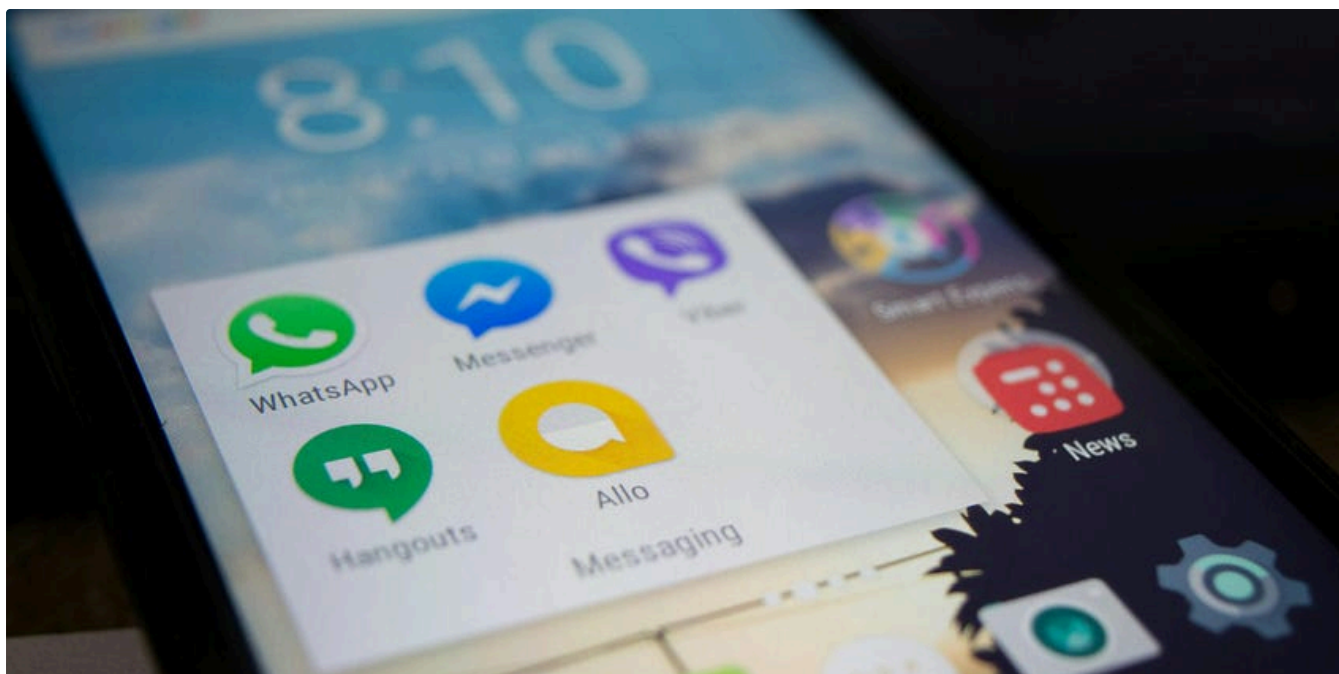
 In InfoSec Write-ups by Md Amiruddin

### Vulnhub Writeup/Walkthrough SickOS 1.1 | By Md Amiruddin

This CTF walkthrough is similar to the labs found in the OSCP exam course.

Dec 21, 2022



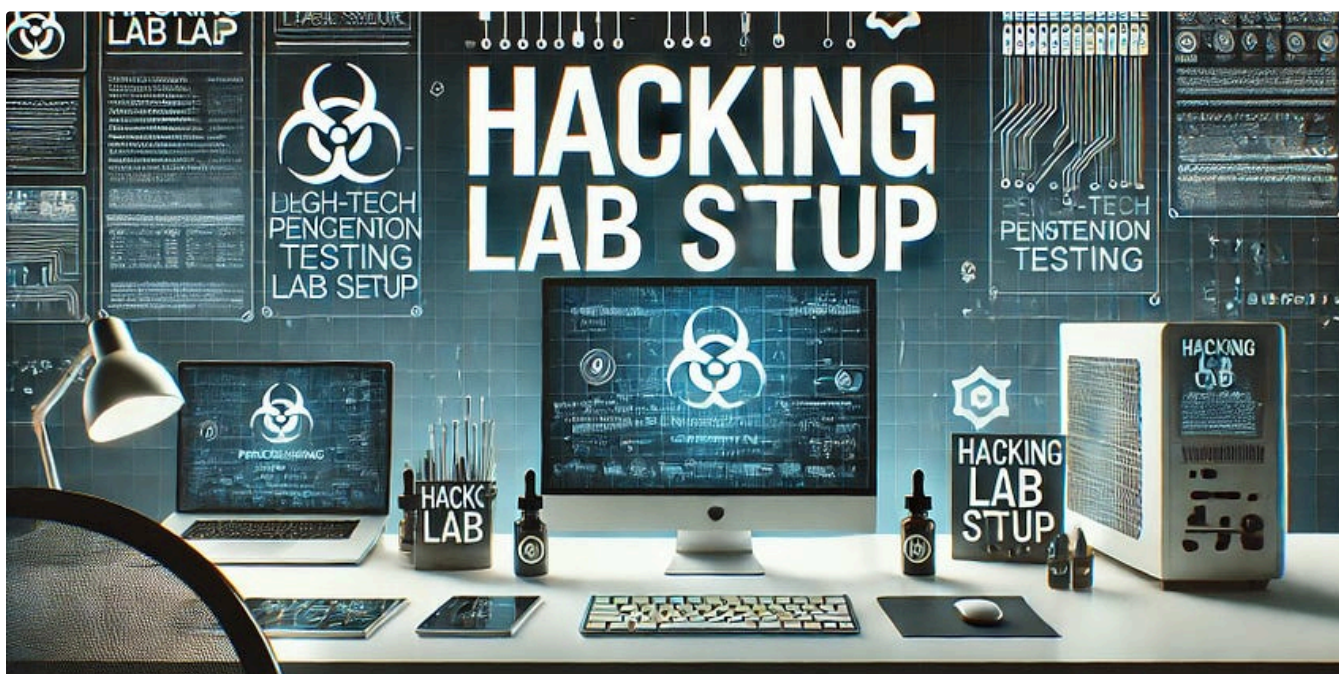


 In InfoSec Write-ups by Visir

## 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...

🌟 6d 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



 In InfoSec Write-ups by Md Amiruddin

## Intro to Docker | Tryhackme Writeup/Walkthrough | By Md Amiruddin

Learn to create, build and deploy Docker containers!

May 5, 2023 🖱️ 5



See all from Md Amiruddin

See all from InfoSec Write-ups

## Recommended from Medium



erative that we understand and can protect against common attacks.

mon techniques used by attackers to target people online. It will also teach some of the best wa



Daniel Schwarzentraub

## Tryhackme Free Walk-through Room: Common Attacks

Tryhackme Free Walk-through Room: Common Attacks

Sep 13, 2024



AttackSave

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

AttackSave

ResultsPositionsPayloadsResource poolSettings


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	

RequestResponse

RawHexRender

```
22 </script>
23 <title>
24   Reset Password
25 </title>
26 </head>
27 <body>
28   <div class="container">
29     <div class="content">
30       <div class="column-50">
31         <div id="messages">
32           <div class="succ">
33             Your new password is: Tk5zve0P
34           </div>
35           <div class="succ">
36             Email: admin@edwin.com
37           </div>
38         </div>
39       </div>
40     </div>
41   </div>
42   <div id="assin">
```



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



## Lists



### Staff picks

793 stories · 1548 saves



### Stories to Help You Level-Up at Work

19 stories · 909 saves



### Self-Improvement 101

20 stories · 3184 saves



### Productivity 101

20 stories · 2697 saves



Koro

## TryHackMe | Active Reconnaissance

After learning Passive Reconnaissance I can say that this type of reconnaissance is safe to do to collect as much information to the...

Aug 31, 2024 🖱 50





 In T3CH by Axoloth

## TryHackMe | Search Skills | WriteUp

Learn to efficiently search the Internet and use specialized search engines and technical docs

★ Oct 26, 2024 🖱 61



 CyferNest Sec

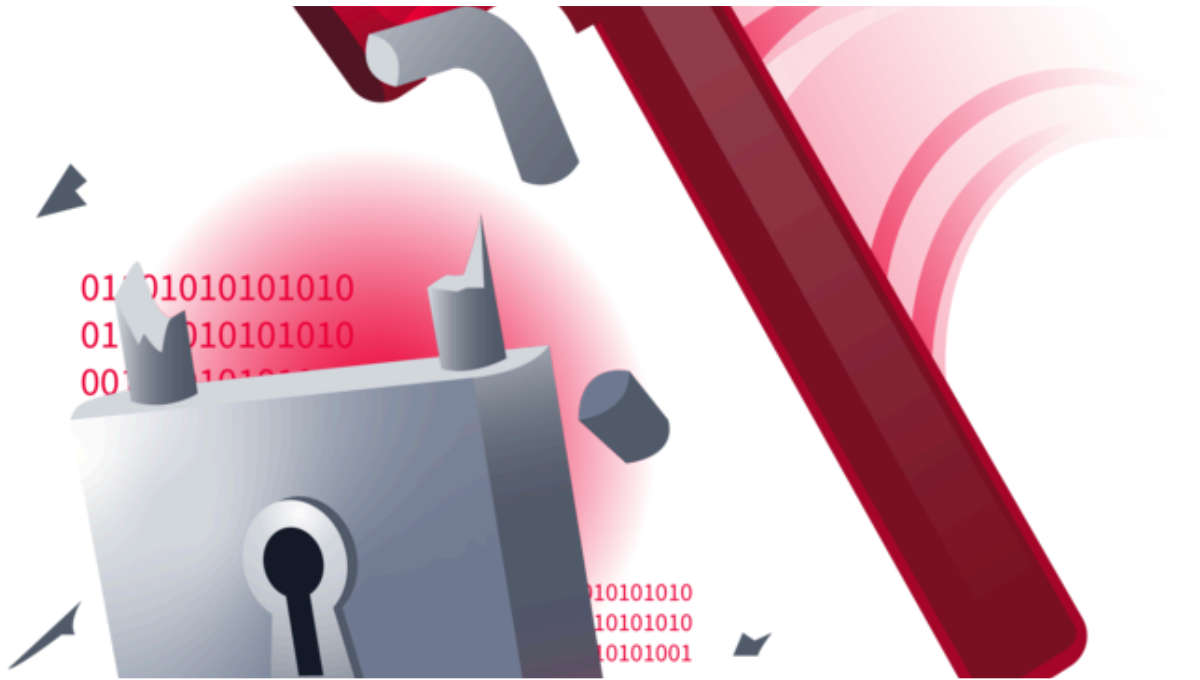
## JWT Security | TryHackMe Walkthrough

TASK 2: Token-Based Authentication

Nov 26, 2024







Berat Arslan

## TryHackMe—Hammer Writeup

'Hammer' is one of the 'Medium' difficulty rooms in THM.

Sep 1, 2024    69    1



See more recommendations