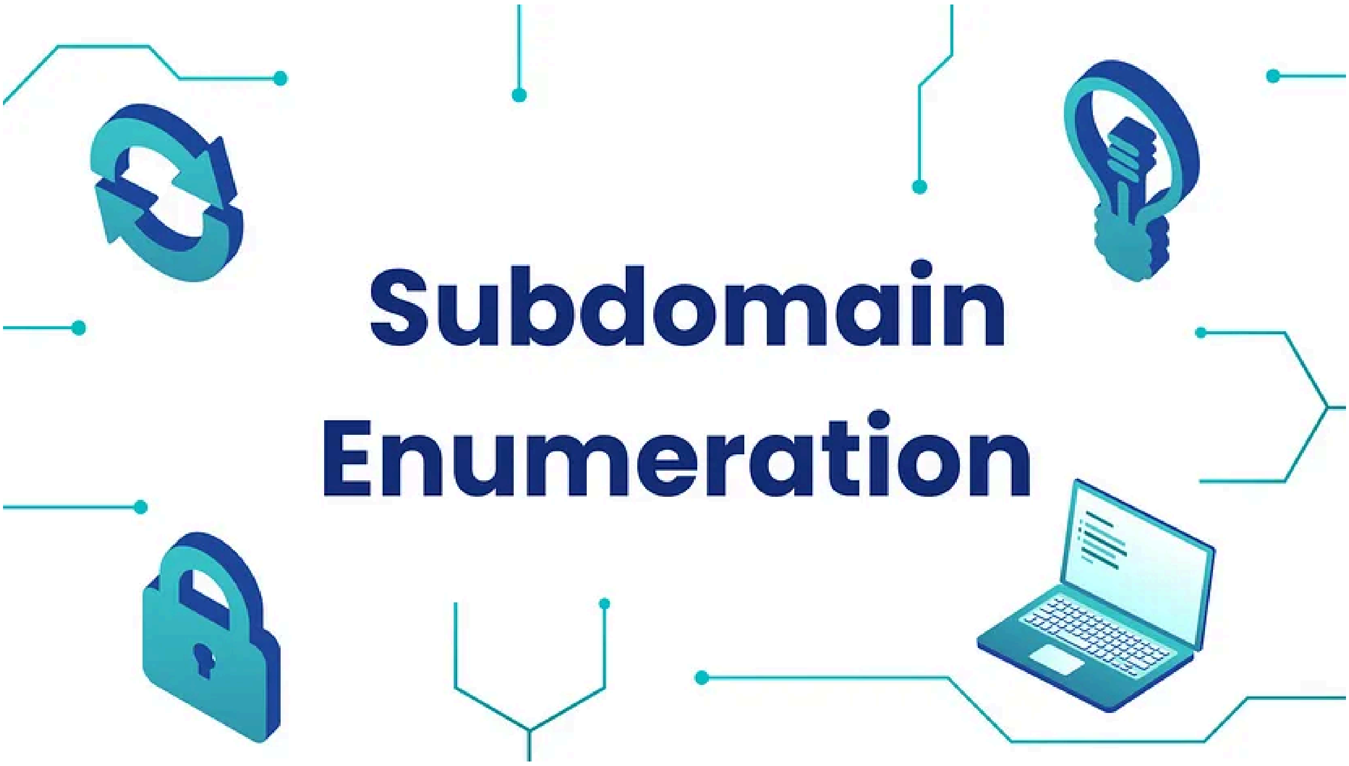
Subdomain Enumeration | Tryhackme Walkthrough

Rahul Kumar · Follow
4 min read · Jul 21, 2023

Listen Share ••• More

> *Learn the various ways of discovering subdomains to expand your attack surface of a target.*



B *reif:*

Subdomain enumeration is the process of finding valid subdomains for a domain, but why do we do this? We do this to expand our attack surface to try and discover more *potential points of vulnerability.*

We will explore three different subdomain enumeration methods: ***Brute Force, OSINT (Open-Source Intelligence) and Virtual Host.***

Start the machine and then move onto the next task.

Ques 1: What is a subdomain enumeration method beginning with B?
Ans 1: Brute Force

Ques 2: What is a subdomain enumeration method beginning with O?
Ans 2: OSINT

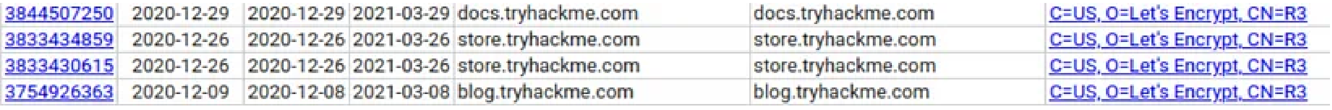
Ques 3: What is a subdomain enumeration method beginning with V?
Ans 3: Virtual Host

OSINT — SSL/TLS Certificates:

When an SSL/TLS (Secure Sockets Layer/Transport Layer Security) certificate is created for a domain by a CA (Certificate Authority), CA's take part in what's called "Certificate Transparency (CT) logs". These are publicly accessible logs of every SSL/TLS certificate created for a domain name. The purpose of Certificate Transparency logs is to stop malicious and accidentally made certificates from being used. We can use this service to our advantage to discover subdomains belonging to a domain, sites like https://crt.sh and https://ui.ctsearch.entrust.com/ui/ctsearchui offer a searchable database of certificates that shows current and historical results.

Go to crt.sh and search for the domain name ***tryhackme.com****, find the entry that was logged at* ***2020–12–26*** *and enter the domain below to answer the question.*

Ques 1: What domain was logged on crt.sh at 2020–12–26?
Ans 1: store.tryhackme.com



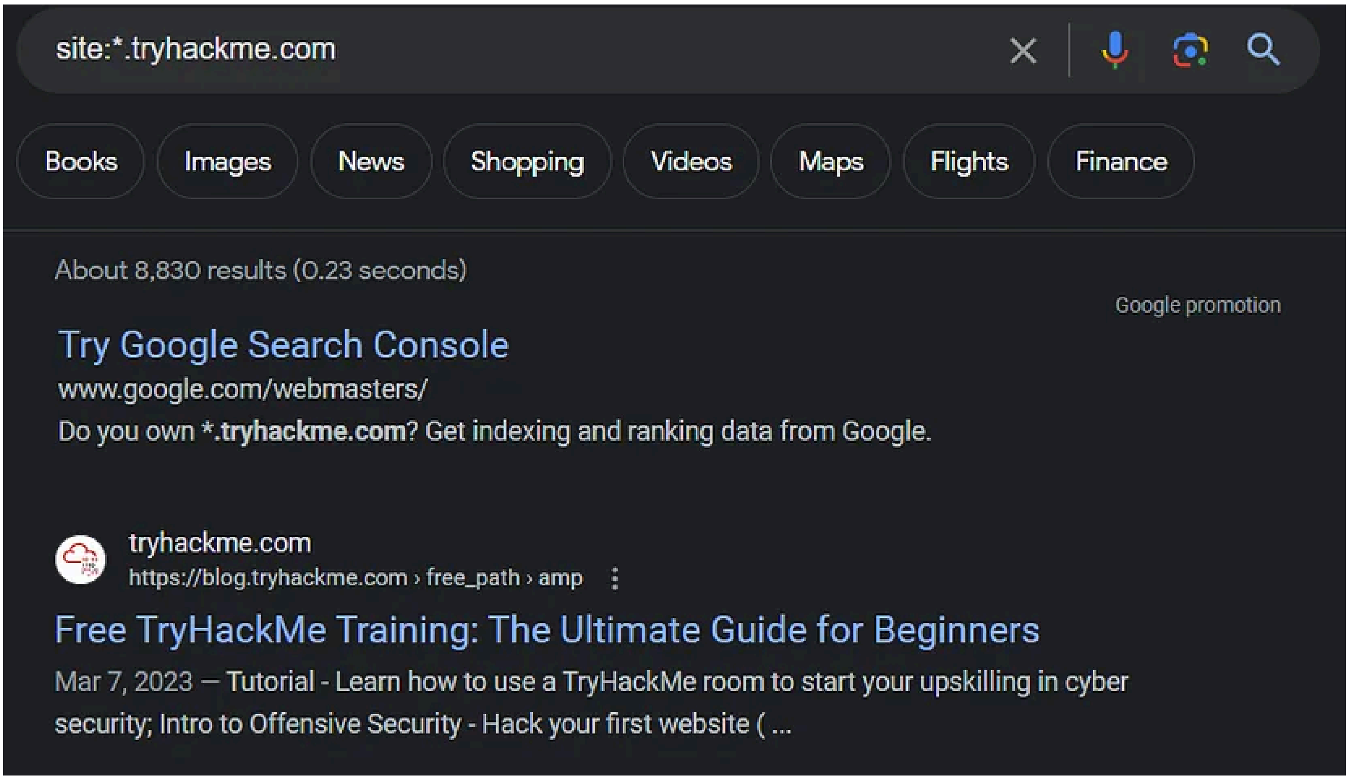
3844507250	2020-12-29	2020-12-29	2021-03-29	docs.tryhackme.com	docs.tryhackme.com	C=US, O=Let's Encrypt, CN=R3
3833434859	2020-12-26	2020-12-26	2021-03-26	store.tryhackme.com	store.tryhackme.com	C=US, O=Let's Encrypt, CN=R3
3833430615	2020-12-26	2020-12-26	2021-03-26	store.tryhackme.com	store.tryhackme.com	C=US, O=Let's Encrypt, CN=R3
3754926363	2020-12-09	2020-12-08	2021-03-08	blog.tryhackme.com	blog.tryhackme.com	C=US, O=Let's Encrypt, CN=R3

OSINT — Search Engines:

Search engines contain trillions of links to more than a billion websites, which can be an excellent resource for finding new subdomains. Using advanced search methods on websites like Google, such as the site: filter, can narrow the search results. For example, “-site:www.domain.com site:.domain.com” would only contain results leading to the domain name domain.com but exclude any links to www.domain.com; therefore, it shows us only subdomain names belonging to domain.com.*

Go to Google and use the search term ***-site:www.tryhackme.com site:*.tryhackme.com****, which should reveal a subdomain for tryhackme.com; use that subdomain to answer the question below.*

Ques 1: What is the TryHackMe subdomain beginning with **B** discovered using the above Google search?
Ans 1: blog.tryhackme.com



About 8,830 results (0.23 seconds)

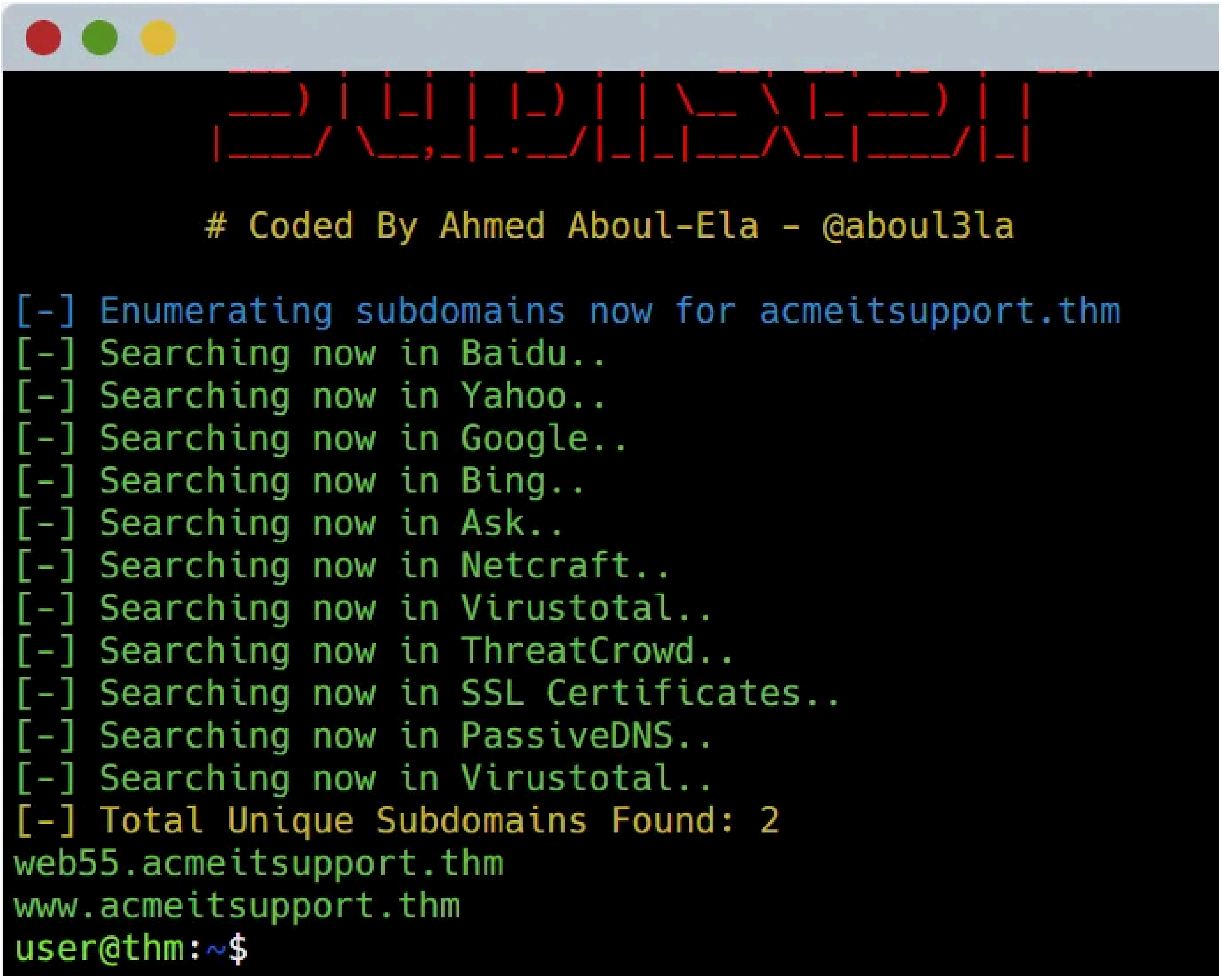
Try Google Search Console
www.google.com/webmasters/
Do you own ***.tryhackme.com**? Get indexing and ranking data from Google.

tryhackme.com
https://blog.tryhackme.com › free_path › amp
Free TryHackMe Training: The Ultimate Guide for Beginners
Mar 7, 2023 — Tutorial - Learn how to use a TryHackMe room to start your upskilling in cyber security; Intro to Offensive Security - Hack your first website (...

DNS Bruteforce:

Bruteforce DNS (Domain Name System) enumeration is the method of trying tens, hundreds, thousands or even millions of different possible subdomains from a pre-defined list of commonly used subdomains. Because this method requires many requests, we automate it with tools to make the process quicker. In this instance, we are using a tool called dnsrecon to perform this. Click the "View Site" button to open the static site, press the "Run DNSrecon Request" button to start the simulation, and then answer the question below.

Ques 1: To speed up the process of OSINT subdomain discovery, we can automate the above methods with the help of tools like Sublist3r, click the "View Site" button to open up the static site and run the sublist3r simulation to discover a new subdomain that will help answer the question below.
Ans 1: web55.acmeitsupport.thm



```
 ___) | |_| | |_) | | \__ \ |_ ___) | |
|____/ \__,_|_.__/|_|_|___/\__|____/|_|

        # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for acmeitsupport.thm
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Searching now in Virustotal..
[-] Total Unique Subdomains Found: 2
web55.acmeitsupport.thm
www.acmeitsupport.thm
user@thm:~$
```

Virtual Hosts:

Some subdomains aren't always hosted in publically accessible DNS results, such as development versions of a web application or administration portals. Instead, the DNS record could be kept on a private DNS server or recorded on the developer's machines in their /etc/hosts file (or c:\windows\system32\drivers\etc\hosts file for Windows users) which maps domain names to IP addresses.

Because web servers can host multiple websites from one server when a website is requested from a client, the server knows which website the client wants from the ***Host*** *header. We can utilise this host header by making changes to it and monitoring the response to see if we've discovered a new website.*

Like with DNS Bruteforce, we can automate this process by using a wordlist of commonly used subdomains.

Start an AttackBox and then try the following command against the Acme IT Support machine to try and discover a new subdomain.

The above command uses the ***-w*** *switch to specify the wordlist we are going to use. The* ***-H*** *switch adds/edits a header (in this instance, the Host header), we have the* ***FUZZ*** *keyword in the space where a subdomain would normally go, and this is where we will try all the options from the wordlist.*

Because the above command will always produce a valid result, we need to filter the output. We can do this by using the page size result with the ***-fs*** *switch. Edit the below command replacing {size} with the most occurring size value from the previous result and try it on the AttackBox.*

> *user@machine$ ffuf -w /usr/share/wordlists/SecLists/Discovery/DNS/namelist.txt -H “Host: FUZZ.acmeitsupport.thm” -u http://MACHINE_IP -fs {size}*

This command has a similar syntax to the first apart from the ***-fs*** *switch, which tells ffuf to ignore any results that are of the specified size.*

The above command should have revealed two positive results that we haven’t come across before.

Ques 1: What is the first subdomain discovered?
Ans 1 : delta

Ques 2: What is the second subdomain discovered?
Ans 2: yellow

References: https://tryhackme.com/room/subdomainenumeration

Tryhackme Tryhackme Walkthrough Cybersecurity Subdomains Enumeration

Subdomain Takeover

Follow

Written by Rahul Kumar

150 Followers · 6 Following

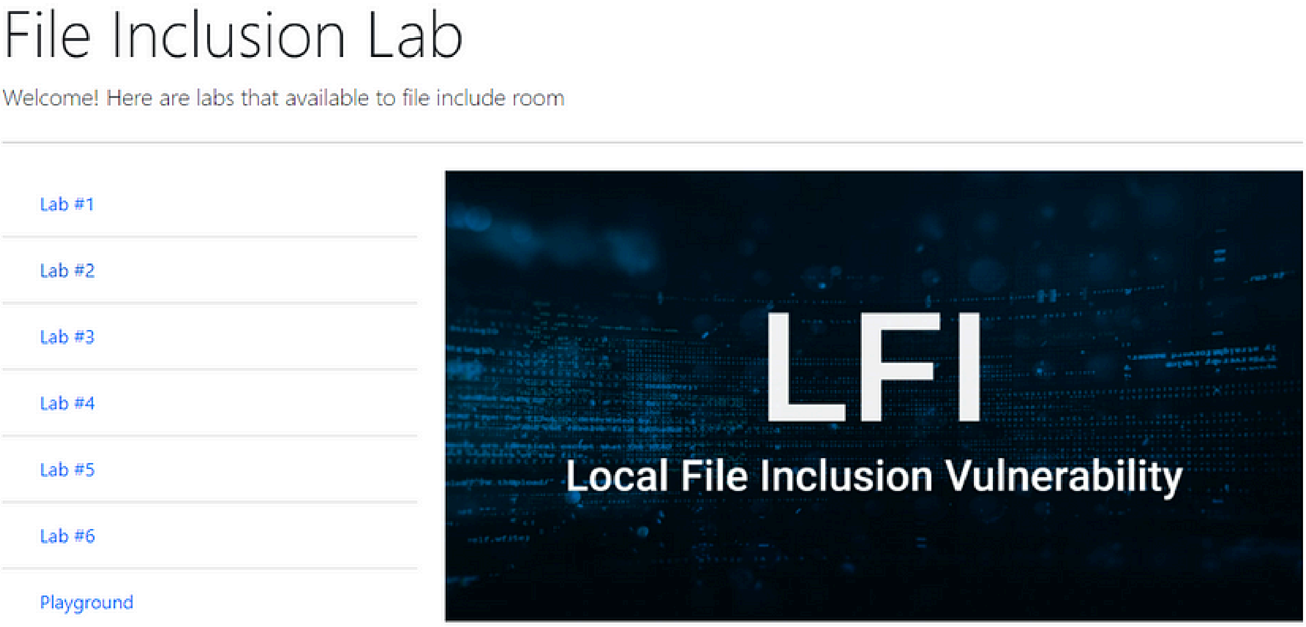
Cybersecurity Enthusiast!! | COMPTIA SEC+ | CCSK | CEH | MTA S&N | Cybersecurity Analyst | Web Application Security

No responses yet

What are your thoughts?

Respond

More from Rahul Kumar



File Inclusion Lab

Welcome! Here are labs that available to file include room

Rahul Kumar

File Inclusion | Tryhackme Walkthrough

This room introduces file inclusion vulnerabilities, including Local File Inclusion (LFI), Remote File Inclusion (RFI), and directory…

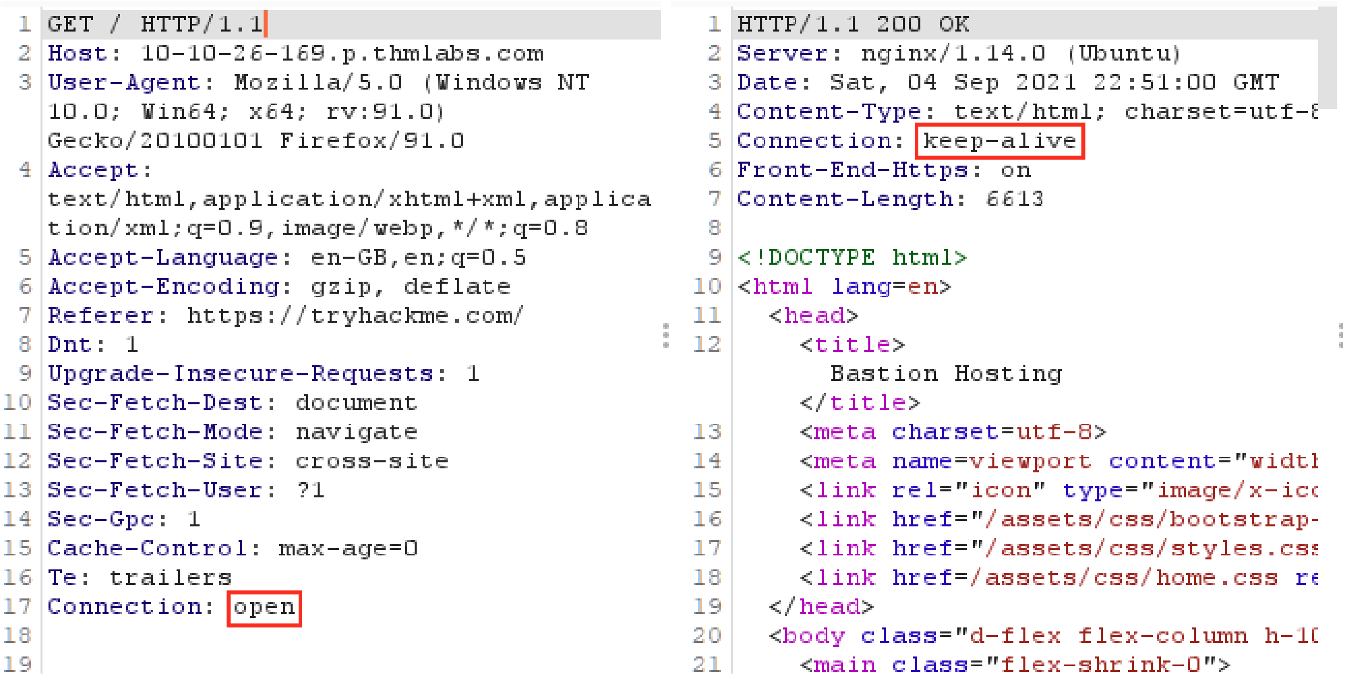
Jul 25, 2023 74 2

Rahul Kumar

Burp Suite : Other Module

Take a dive into some of Burp Suite’s lesser known modules

Aug 4, 2023 52 1



```
GET / HTTP/1.1
Host: 10-10-26-169.p.thmlabs.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://tryhackme.com/
Dnt: 1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
Sec-Gpc: 1
Cache-Control: max-age=0
Te: trailers
Connection: open
```

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Sat, 04 Sep 2021 22:51:00 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Front-End-Https: on
Content-Length: 6613

<!DOCTYPE html>
<html lang=en>
  <head>
    <title>
      Bastion Hosting
    </title>
    <meta charset=utf-8>
    <meta name=viewport content="widt
    <link rel="icon" type="image/x-ico
    <link href="/assets/css/bootstrap-
    <link href="/assets/css/styles.css
    <link href=/assets/css/home.css re
  </head>
  <body class="d-flex flex-column h-10
    <main class="flex-shrink-0">
```

Rahul Kumar

Burp Suite: Repeater | Tryhackme Walkthrough

Learn how to use Repeater to duplicate requests in Burp Suite

Jul 28, 2023 7

Rahul Kumar

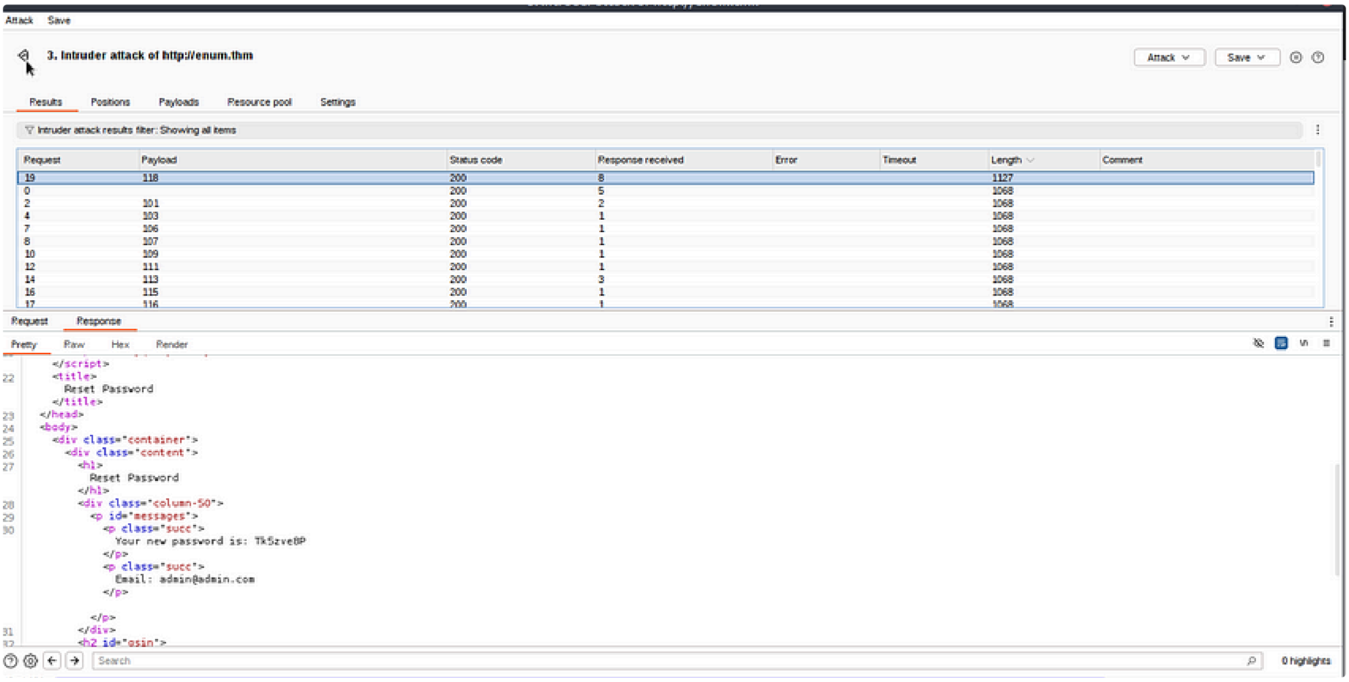
Command Injection | Tryhackme Walkthrough

Learn about a vulnerability allowing you to execute commands through a vulnerable app, and its remediations.

Jul 27, 2023 6

See all from Rahul Kumar

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	

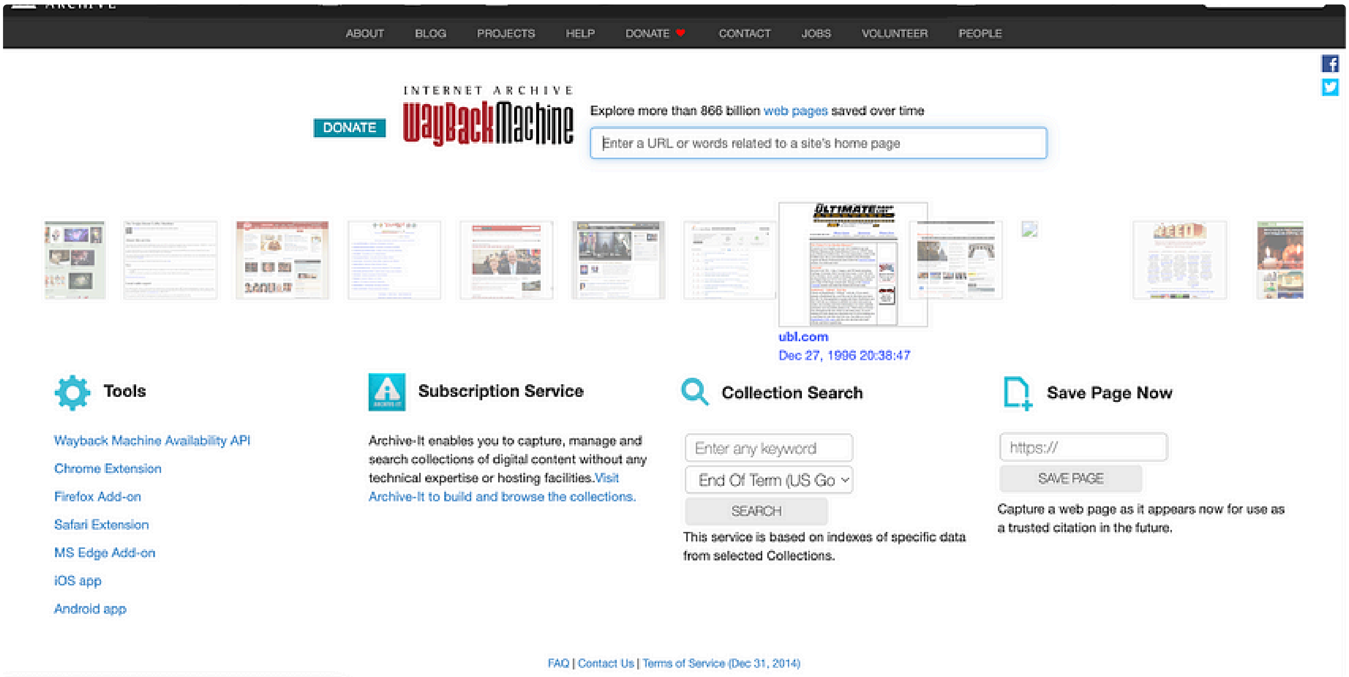
```
    </script>
    <title>
      Reset Password
    </title>
  </head>
  <body>
    <div class="container">
      <div class="content">
        <h1>
          Reset Password
        </h1>
        <div class="column-50">
          <p id="messages">
            <p class="succ">
              Your new password is: Tk5zve8P
            </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



Explore more than 866 billion web pages saved over time

Enter a URL or words related to a site's home page

ubl.com
Dec 27, 1996 20:38:47

Tools

Wayback Machine Availability API
Chrome Extension
Firefox Add-on
Safari Extension
MS Edge Add-on
iOS app
Android app

Subscription Service

Archive-It enables you to capture, manage and search collections of digital content without any technical expertise or hosting facilities. Visit Archive-It to build and browse the collections.

Collection Search

Enter any keyword
End Of Term (US Go
SEARCH

This service is based on indexes of specific data from selected Collections.

Save Page Now

https://
SAVE PAGE

Capture a web page as it appears now for use as a trusted citation in the future.

FAQ | Contact Us | Terms of Service (Dec 31, 2014)

S3N5E

Web Archives: A Journey Through Digital History

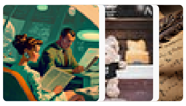
In the fast-paced digital world, websites come and go, leaving only fleeting traces of their existence behind. However, thanks to the…

Jul 17, 2024 · 31 · 1

Lists

Tech & Tools

22 stories · 377 saves

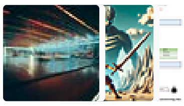


Medium's Huge List of Publications Accepting Submissions

377 stories · 4308 saves

Staff picks

791 stories · 1544 saves



Natural Language Processing

1882 stories · 1519 saves

Abhijeet kumawat

Day 5 of 30 Days — 30 Vulnerabilities | Open Redirects

Day 5: Mastering Open Redirects — Essential Tricks & Techniques Based on Personal Experience and Valuable POCs

✦ Aug 7, 2024 116

Advent of Cyber 2024
Dive into the wonderful world of cyber security by engaging in festive beginner-friendly exercises every day in the lead-up to Christmas!
I'm all atomic inside!
Day 4
Answers
cyberw1ng.medium.com

In InfoSec Write-ups by Karthikeyan Nagaraj

Advent of Cyber 2024 [Day 4] Writeup with Answers | TryHackMe Walkthrough

I'm all atomic inside!

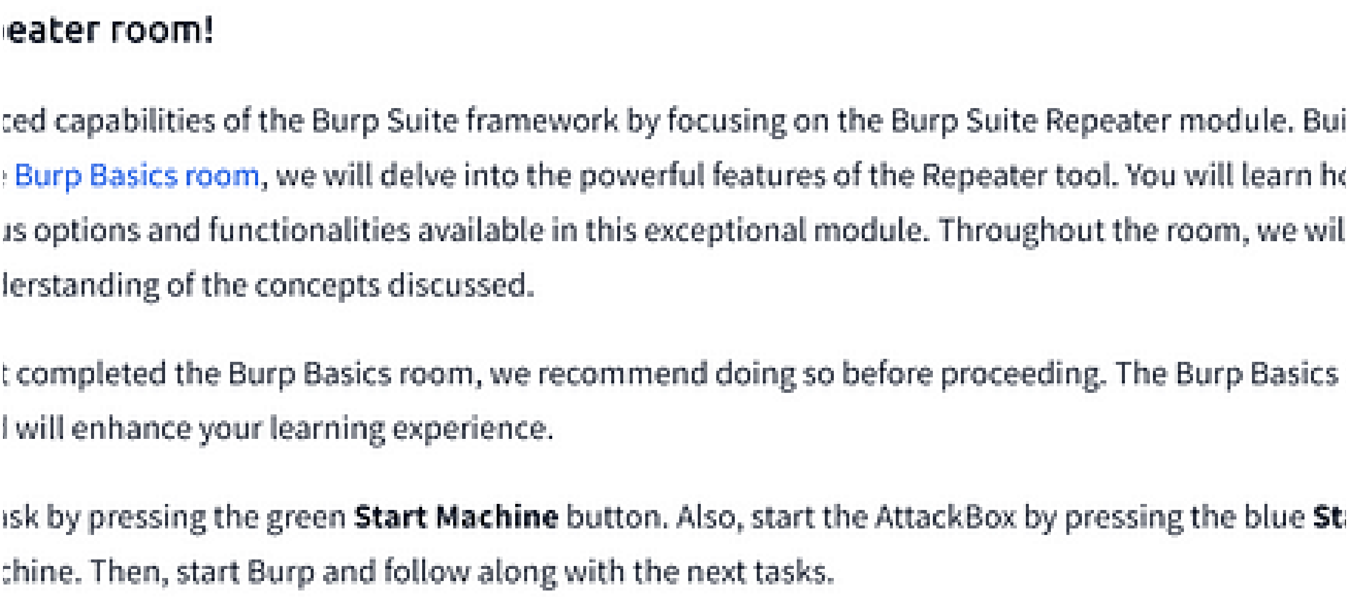
Dec 4, 2024 882 1

IritT

Intro to Cross-site Scripting — TryHackMe Walkthrough

Learn how to detect and exploit XSS vulnerabilities, giving you control of other visitor's browsers.

Sep 10, 2024



eater room!

ced capabilities of the Burp Suite framework by focusing on the Burp Suite Repeater module. Bui Burp Basics room, we will delve into the powerful features of the Repeater tool. You will learn hc is options and functionalities available in this exceptional module. Throughout the room, we wil lerstanding of the concepts discussed.

t completed the Burp Basics room, we recommend doing so before proceeding. The Burp Basics l will enhance your learning experience.

isk by pressing the green **Start Machine** button. Also, start the AttackBox by pressing the blue **St** chine. Then, start Burp and follow along with the next tasks.

Daniel Schwarzentraub

Tryhackme Free Walk-through Room: Burp Suite: Repeater (Updated room)

Tryhackme Free Walk-through Room: Burp Suite: Repeater (Updated room)

Aug 27, 2024

See more recommendations