

enumeration

nmap result

```
nmap -sC -sV -sT -oN /home/kali/machines/retired/tartarsauce/nmap.txt  
10.10.10.88
```

Starting Nmap 7.91 (<https://nmap.org>) at 2021-03-11 08:45 EST

Nmap scan report for 10.10.10.88

Host is up (0.18s latency).

Not shown: 999 closed ports

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

| http-robots.txt: 5 disallowed entries

| /webservices/tar/tar/source/

| /webservices/monstra-3.0.4/ /webservices/easy-file-uploader/

|_ /webservices/developmental/ /webservices/phpmyadmin/

|_ http-server-header: Apache/2.4.18 (Ubuntu)

|_ http-title: Landing Page

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 37.27 seconds

now running the full scan

full port scan confirms no more port is open

```
80/tcp open  http   Apache httpd 2.4.18 ((Ubuntu))
```

| http-robots.txt: 5 disallowed entries

| /webservices/tar/tar/source/

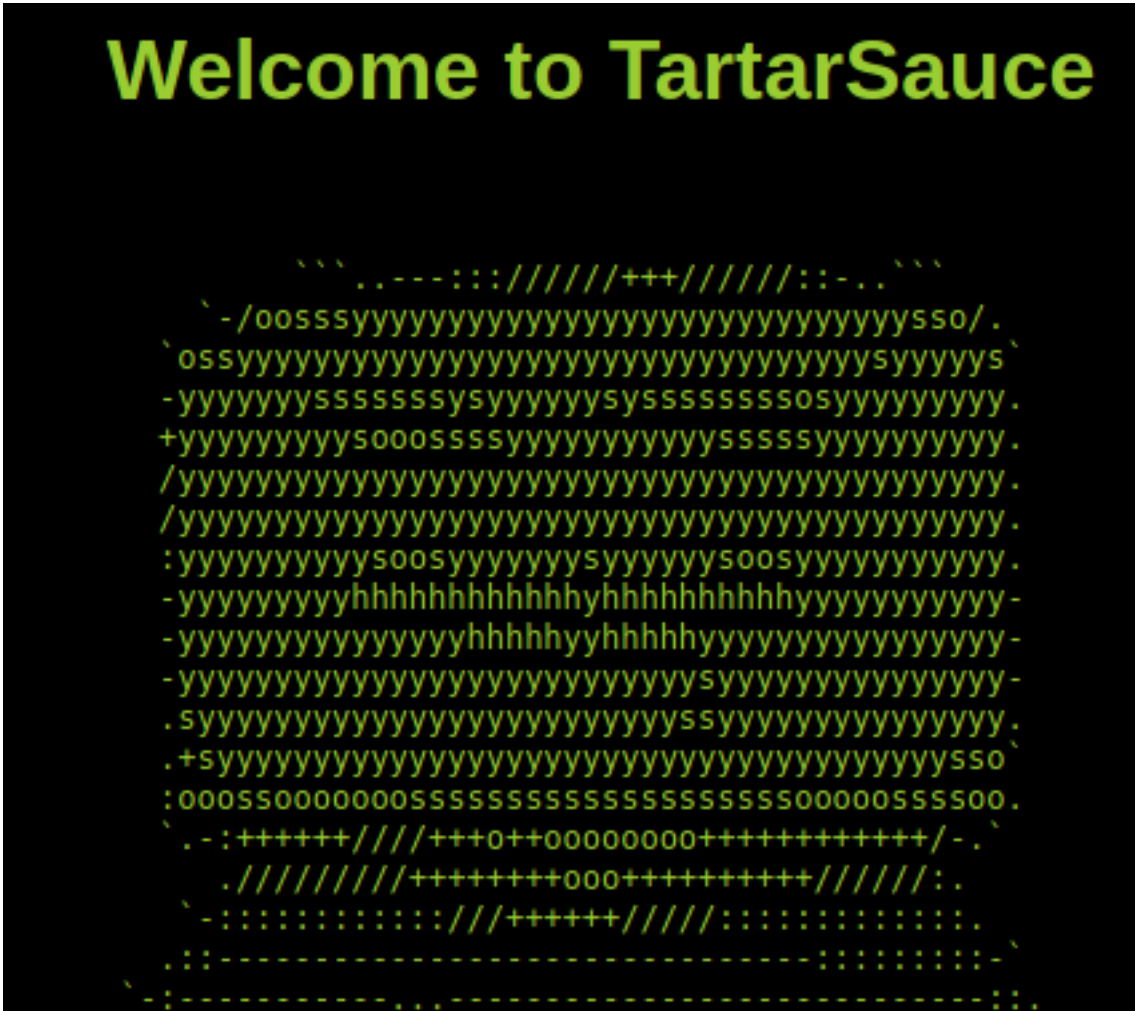
| /webservices/monstra-3.0.4/ /webservices/easy-file-uploader/

|_ /webservices/developmental/ /webservices/phpmyadmin/

|_ http-server-header: Apache/2.4.18 (Ubuntu)

|_ http-title: Landing Page

here we can see only port 80 is open with some directories



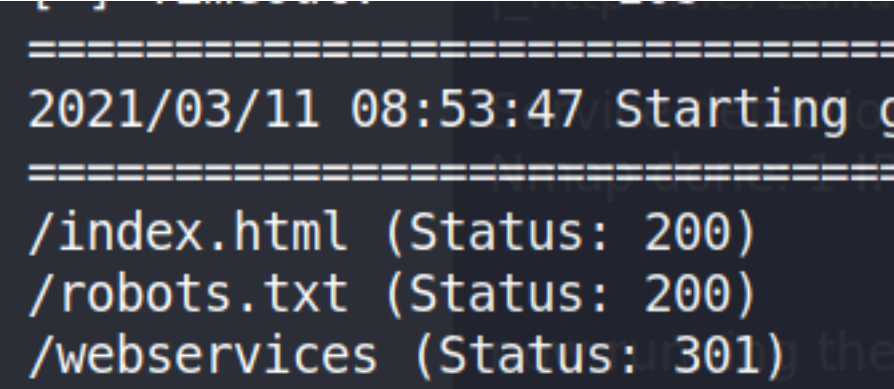
page looks like this

and nothing but a rabbithole at the end of page

```
561
562
563 <!--Carry on, nothing to see here :D-->
564
```

now lets run nikto gobuster

nothing on nikto running go buster



here is result of gobuster

going to robot.txt we see

```
User-agent: *
Disallow: /webservices/tar/tar/source/
Disallow: /webservices/monstra-3.0.4/
Disallow: /webservices/easy-file-uploader/
Disallow: /webservices/developmental/
Disallow: /webservices/phpmyadmin/
```

but /webservices is forbidden

trying all the paths in robot.txt we finally found a working path

/webservices/monstra-3.0.4/

TartarSauce

[Home](#) [Blog](#) [Users](#) [Log In](#) [Registration](#)

Home

Welcome!

Welcome to your new Monstra powered website.
Monstra is succesfully installed, you can start editing the content and customising your site.

Getting Started

This is a default home page of your website.
Here's a quick description of how to edit this page:

- First make sure you're [logged in](#).
- Go to the [Pages Manager](#) and click "Edit" button for this page.
- Make your changes, click "Save" and you're done!

Online Resources

- [Official Site](#)
- [Official Support Forum](#)
- [Documentation](#)

[Sitemap](#)

Powered by [Monstra](#) 3.0.4

lets see whats in this

clicking all the links we see nothing except the logged in button which takes us to the login page

MONSTRA

Username

Password

Log In

we tried admin admin and we successfully logged in

MONSTRA

Dashboard


Content ▾

Extends ▾

System ▾

Help ▾

View Site

admin 

Welcome back, **admin**

Create New ▾Upload File

Content	Extends	System	Help
Pages Blocks Files Menu	Plugins Themes Snippets	Settings Users Backups Emails Information	Documentation Official Support Forum

here is the login page

/admin/index.php?id=themes&action=edit_template&filename=index

we cannot upload file in the content/files though a exploit says we can

Files

Select file

Upload

Drop File Here

Maximum upload file size: 2 MB

Create New Directory

uploads

Name	Extension	Size
------	-----------	------

Monstra was made by Sergey Romanenko and is maintained by Monstra Community / © 2012 - 2016 Monstra – Version 3.0.4

so i think it is a rabbit hole and we have to look for other way we have a directory /webservices lets run gobuster on it and see result

```
[+] User Agent:      gobust
[+] Extensions:     txt,ht
[+] Timeout:        10s
=====
2021/03/12 09:03:06 Starti
=====
/wp (Status: 301)
```

we see we have a directory /wp lets open it and see the result

Toggle navigation

[Test blog](#)

- [Uncategorized](#) (1)

February 9, 2018

Hello world!

This blog site is under construction, stay tuned.

- [Sample Page](#)

© 2021 Test blog.

Voce theme by [limbenjamin](#). Powered by [WordPress](#).

we see a page

we found that it is written in wordpress so lets run wpscan

```
wpscan --url http://10.10.10.88/webservices/wp/ --enumerate
```

but we didnt got any result