

技术与经验分享研讨会 第三场（上）

CTF-Web 与代码审计(续)

东北大学 NEX 信息安全创新团队
2024年8月26日

漏洞类型与分类

Vulnerability classifications

- 信息泄露 (.git / .svn / .bak.zip / HTTP Header (PHP-Version)
- 逻辑漏洞 (鉴权绕过、越权、错误的参数校验)
- 条件竞争
- 文件上传、下载、解压
- SSRF
- 反序列化
- 动态代码/字节码执行
- SSTI
- 系统命令执行
- SQL 注入/执行
- CSRF/XSS

文件上传

File upload

Safe?

```
1  ' '
2  $target_dir = "uploads/";
3  $target_file = $target_dir . basename($_FILES["fileToUpload"]["name"]);
4  $uploadOk = 1;
5  $imageFileType = strtolower(pathinfo($target_file,PATHINFO_EXTENSION));
6
7  // Check if image file is a actual image or fake image
8  if(isset($_POST["submit"])) {
9      $check = getimagesize($_FILES["fileToUpload"]["tmp_name"]);
10     $uploadOk = ($check !== false) ? 1 : 0;
11 }
12
13 // Allow certain file formats
14 if($imageFileType != "jpg" && $imageFileType != "png" && $imageFileType != "jpeg"
15 && $imageFileType != "gif" ) {
16     echo "Sorry, only JPG, JPEG, PNG & GIF files are allowed.";
17     $uploadOk = 0;
18 }
19
20 // Check if $uploadOk is set to 0 by an error
21 if ($uploadOk == 0) {
22     echo "Sorry, your file was not uploaded.";
23 // if everything is ok, try to upload file
24 } else {
25     if (move_uploaded_file($_FILES["fileToUpload"]["tmp_name"], $target_file)) {
26         echo "The file ". htmlspecialchars( basename( $_FILES["fileToUpload"]["name"])) .
27         " was uploaded successfully";
28     } else {
29         echo "Sorry, there was an error uploading your file.";
30     }
31 }
```

文件上传

File upload

Safe?

```
2 $target_dir = "uploads/";
3 $target_file = $target_dir . basename($_FILES["fileToUpload"]["name"]);
4 $uploadOk = 1;
5 $imageFileType = strtolower(pathinfo($target_file,PATHINFO_EXTENSION));
6
7 // Check if image file is a actual image or fake image
8 if(isset($_POST["submit"])) {
9     $check = getimagesize($_FILES["fileToUpload"]["tmp_name"]);
10    $uploadOk = ($check !== false) ? 1 : 0;
11 }
12
13 // Allow certain file formats
14 if(preg_match('/^ph.*$/i', $imageFileType)) {
15     ✨echo "Sorry, PHs are forbidden.";
16     $uploadOk = 0;
17 }
18
19 // Check if $uploadOk is set to 0 by an error
20 if ($uploadOk == 0) {
21     echo "Sorry, your file was not uploaded.";
22     // if everything is ok, try to upload file
23 } else {
24     if (move_uploaded_file($_FILES["fileToUpload"]["tmp_name"], $target_file)) {
25         echo "The file ". htmlspecialchars( basename( $_FILES["fileToUpload"]["nam
26     ) else {
27         echo "Sorry, there was an error uploading your file.";
28     }
29 }
```

文件上传

File upload

Safe?

```
2  $target_dir = "uploads/";
3  $target_file = $target_dir . $_POST['name'];
4  $uploadOk = 1;
5  $imageFileType = strtolower(pathinfo($target_file,PATHINFO_EXTENSION));
6
7  // Check if image file is a actual image or fake image
8  if(isset($_POST["submit"])) {
9      $check = getimagesize($_FILES["fileToUpload"]["tmp_name"]);
10     $uploadOk = ($check !== false) ? 1 : 0;
11 }
12
13 // Allow certain file formats
14 if(preg_match('/^ph.*$/i', $imageFileType)) {
15     echo "Sorry, PHs are forbidden.";
16     $uploadOk = 0;
17 }
18
19 // Check if $uploadOk is set to 0 by an error
20 if ($uploadOk == 0) {
21     echo "Sorry, your file was not uploaded.";
22 // if everything is ok, try to upload file
23 } else {
24     if (move_uploaded_file($_FILES["fileToUpload"]["tmp_name"], $target_file)
25         echo "The file ". htmlspecialchars( basename( $_FILES["fileToUpload"]['
26     } else {
27         echo "Sorry, there was an error uploading your file.";
28     }
29 }
```

文件上传

File upload

Safe?

```
2  $target_dir = "uploads/";
3  $target_file = $target_dir . $_POST['name'];
4  $uploadOk = 1;
5  $imageFileType = strtolower(pathinfo($target_file,PATHINFO_EXTENSION));
6
7  // Check if image file is a actual image or fake image
8  if(isset($_POST["submit"])) {
9      $check = getimagesize($_FILES["fileToUpload"]["tmp_name"]);
10     $uploadOk = ($check !== false) ? 1 : 0;
11 }
12
13 // Allow certain file formats
14 if(preg_match('/^ph.*$/i', $imageFileType)) {
15     echo "Sorry, PHs are forbidden.";
16     $uploadOk = 0;
17 }
18
19 // try to upload the file
20 if (!move_uploaded_file($_FILES["fileToUpload"]["tmp_name"], $target_file)) {
21     $uploadOk = 0;
22 }
23
24 // Check if $uploadOk is set to 0 by an error
25 if ($uploadOk == 0) {
26     echo "Sorry, there was an error uploading your file.";
27     ✨ @unlink($target_file);
28 } else {
29     echo "The file ". htmlspecialchars( basename( $_FILES["fileToUpload"]["name"]
30 }
```

文件上传

File upload

Safe?

```
2  $target_dir = "uploads/";
3  $target_file = $target_dir . $_POST['name'];
4  $uploadOk = 1;
5  $imageFileType = strtolower(pathinfo($target_file,PATHINFO_EXTENSION));
6
7  // Check if image file is a actual image or fake image
8  if(isset($_POST["submit"])) {
9      $check = imagecreatefromjpeg($_FILES["fileToUpload"]["tmp_name"]);
10     ✦$uploadOk = ($check !== false) ? 1 : 0;
11
12     // Allow certain file formats
13     if(preg_match('/^ph.*$/ ', $imageFileType)) {
14         echo "Sorry, PHs are forbidden.";
15         $uploadOk = 0;
16     }
17
18     // try to upload the image
19     if (!imagejpeg($check, $target_file)) {
20         $uploadOk = 0;
21     }
22
23     // Check if $uploadOk is set to 0 by an error
24     if ($uploadOk == 0) {
25         echo "Sorry, there was an error uploading your file.";
26         @unlink($target_file);
27     } else {
28         echo "The file ". htmlspecialchars( basename( $_FILES["fileToUpload"][''
29     }
30
31 }
```

文件上传

File upload

Safe?

```
2  $target_dir = "uploads/";
3  $target_file = $target_dir . $_POST['name'];
4  $uploadOk = 1;
5  $imageFileType = strtolower(pathinfo($target_file,PATHINFO_EXTENSION));
6
7  // Check if image file is a actual image or fake image
8  if(isset($_POST["submit"])) {
9      $check = imagecreatefromjpeg($_FILES["fileToUpload"]["tmp_name"]);
10     $uploadOk = ($check !== false) ? 1 : 0;
11
12     // Allow certain file formats
13     if(preg_match('/^ph.*$/i', $imageFileType)) {
14         echo "Sorry, PHs are forbidden.";
15         $uploadOk = 0;
16     }
17
18     srand(time());
19     $target_file = $target_dir . strval(rand()) . '.' . $imageFileType;
20     // try to upload the image
21     if (!imagejpeg($check, $target_file)) {
22         $uploadOk = 0;
23     }
24
25     // Check if $uploadOk is set to 0 by an error
26     if ($uploadOk == 0) {
27         echo "Sorry, there was an error uploading your file.";
28         @unlink($target_file);
29     } else {
30         echo "The file " . htmlspecialchars( basename( $_FILES["fileToUpload"]['
31     ]
32
33 }
```


Safe?

```
3  $file = $_GET['file'];  
4  chdir('/var/www/html/images/');  
5  copy($file, '/var/www/html/backup/' . $file);  
6
```

```
.  
├── backup  
│   └── 1c  
├── images  
│   ├── 1c  
│   │   └── 1c2d.gif  
│   └── test.jpg
```

文件解压

File unzipping

Safe?

```
1  try (java.util.zip.ZipFile zipFile = new ZipFile(file)) {
2      Enumeration<? extends ZipEntry> entries = zipFile.entries();
3      while (entries.hasMoreElements()) {
4          ZipEntry entry = entries.nextElement();
5          File entryDestination = new File(outputDir, entry.getName());
6          if (entry.isDirectory()) {
7              entryDestination.mkdirs();
8          } else {
9              entryDestination.getParentFile().mkdirs();
10             try (InputStream in = zipFile.getInputStream(entry);
11                 OutputStream out = new FileOutputStream(entryDestination)) {
12                 IOUtils.copy(in, out);
13             }
14         }
15     }
16 }
```

文件解压

File unzipping

Safe?

```
1  @app.route('/unzip'):
2  def unzip():
3      id = request.args.get('id')
4      if id is None or not id.isalnum():
5          return 'id is required', 400
6      os.system(f'rm -rf /tmp/{id}')
7      os.system(f'mkdir /tmp/{id}')
8      with open(f'/tmp/{id}.zip', 'wb') as f:
9          f.write(request.data)
10     os.system(f'unzip /tmp/{id}.zip -d /tmp/{id}')
```

- <https://github.com/cookieY/Yearning>
- <https://github.com/vivo/MoonBox/blob/main/docker/docker-compose.yml>
- easyjava
- ezblog
- thinkshop
- thinkshopping
- goblog

感谢您的聆听

Thank you for your listening
