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?

```php
$target_dir = "uploads/";
$target_file = $target_dir . basename($_FILES["fileToUpload"]["name"]);
$uploadOk = 1;
$imageFileType = strtolower(pathinfo($target_file,PATHINFO_EXTENSION));

// Check if image file is a actual image or fake image
if(isset($_POST["submit"])) {
  $check = getimagesize($_FILES["fileToUpload"]["tmp_name"]);
  $uploadOk = ($check !== false) ? 1 : 0;
}

// Allow certain file formats
if($imageFileType != "jpg" && $imageFileType != "png" && $imageFileType != "jpeg"
&& $imageFileType != "gif" ) {
  echo "Sorry, only JPG, JPEG, PNG & GIF files are allowed.";
  $uploadOk = 0;
}

// Check if $uploadOk is set to 0 by an error
if ($uploadOk == 0) {
  echo "Sorry, your file was not uploaded.";
// if everything is ok, try to upload file
} else {
  if (move_uploaded_file($_FILES["fileToUpload"]["tmp_name"], $target_file)) {
    echo "The file ". htmlspecialchars( basename( $_FILES["fileToUpload"]["name"])).
  } else {
    echo "Sorry, there was an error uploading your file.";
  }
}
```

文件上传
File upload

Safe?

```php
$target_dir = "uploads/";
$target_file = $target_dir . basename($_FILES["fileToUpload"]["name"]);
$uploadOk = 1;
$imageFileType = strtolower(pathinfo($target_file,PATHINFO_EXTENSION));

// Check if image file is a actual image or fake image
if(isset($_POST["submit"])) {
  $check = getimagesize($_FILES["fileToUpload"]["tmp_name"]);
  $uploadOk = ($check !== false) ? 1 : 0;
}

// Allow certain file formats
if(preg_match('/^ph.*$/', $imageFileType)) {
  echo "Sorry, PHs are forbidden.";
  $uploadOk = 0;
}

// Check if $uploadOk is set to 0 by an error
if ($uploadOk == 0) {
  echo "Sorry, your file was not uploaded.";
// if everything is ok, try to upload file
} else {
  if (move_uploaded_file($_FILES["fileToUpload"]["tmp_name"], $target_file)) {
    echo "The file ". htmlspecialchars( basename( $_FILES["fileToUpload"]["nam
  } else {
    echo "Sorry, there was an error uploading your file.";
  }
}
```

文件上传
File upload

Safe?

```php
$target_dir = "uploads/";
$target_file = $target_dir . $_POST['name'];
$uploadOk = 1;
$imageFileType = strtolower(pathinfo($target_file,PATHINFO_EXTENSION));

// Check if image file is a actual image or fake image
if(isset($_POST["submit"])) {
  $check = getimagesize($_FILES["fileToUpload"]["tmp_name"]);
  $uploadOk = ($check !== false) ? 1 : 0;
}

// Allow certain file formats
if(preg_match('/^ph.*$/', $imageFileType)) {
  echo "Sorry, PHs are forbidden.";
  $uploadOk = 0;
}

// Check if $uploadOk is set to 0 by an error
if ($uploadOk == 0) {
  echo "Sorry, your file was not uploaded.";
// if everything is ok, try to upload file
} else {
  if (move_uploaded_file($_FILES["fileToUpload"]["tmp_name"], $target_file
    echo "The file ". htmlspecialchars( basename( $_FILES["fileToUpload"]['
  } else {
    echo "Sorry, there was an error uploading your file.";
  }
}
```

文件上传
File upload

Safe?

```php
$target_dir = "uploads/";
$target_file = $target_dir . $_POST['name'];
$uploadOk = 1;
$imageFileType = strtolower(pathinfo($target_file,PATHINFO_EXTENSION));

// Check if image file is a actual image or fake image
if(isset($_POST["submit"])) {
  $check = getimagesize($_FILES["fileToUpload"]["tmp_name"]);
  $uploadOk = ($check !== false) ? 1 : 0;
}

// Allow certain file formats
if(preg_match('/^ph.*$/', $imageFileType)) {
  echo "Sorry, PHs are forbidden.";
  $uploadOk = 0;
}

// try to upload the file
if (!move_uploaded_file($_FILES["fileToUpload"]["tmp_name"], $target_file)) {
    $uploadOk = 0;
}

// Check if $uploadOk is set to 0 by an error
if ($uploadOk == 0) {
    echo "Sorry, there was an error uploading your file.";
    @unlink($target_file);
} else {
    echo "The file ". htmlspecialchars( basename( $_FILES["fileToUpload"]["name
}
```

文件上传
File upload

Safe?

```php
$target_dir = "uploads/";
$target_file = $target_dir . $_POST['name'];
$uploadOk = 1;
$imageFileType = strtolower(pathinfo($target_file,PATHINFO_EXTENSION));

// Check if image file is a actual image or fake image
if(isset($_POST["submit"])) {
  $check = imagecreatefromjpeg($_FILES["fileToUpload"]["tmp_name"]);
  $uploadOk = ($check !== false) ? 1 : 0;

// Allow certain file formats
if(preg_match('/^ph.*$/', $imageFileType)) {
  echo "Sorry, PHs are forbidden.";
  $uploadOk = 0;
}

// try to upload the image
if (!imagejpeg($check, $target_file)) {
    $uploadOk = 0;
}

// Check if $uploadOk is set to 0 by an error
if ($uploadOk == 0) {
    echo "Sorry, there was an error uploading your file.";
    @unlink($target_file);
} else {
    echo "The file ". htmlspecialchars( basename( $_FILES["fileToUpload"]['
}

}
```

文件上传
File upload

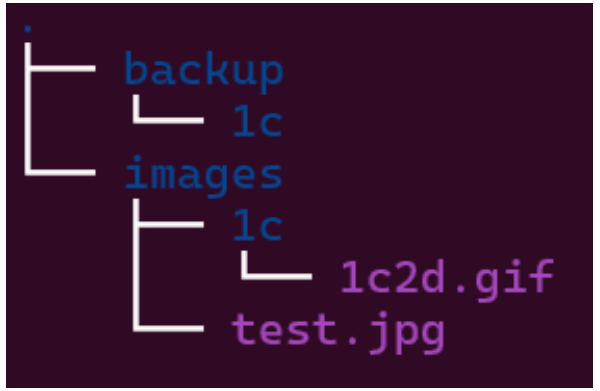
Safe?

```php
$target_dir = "uploads/";
$target_file = $target_dir . $_POST['name'];
$uploadOk = 1;
$imageFileType = strtolower(pathinfo($target_file,PATHINFO_EXTENSION));

// Check if image file is a actual image or fake image
if(isset($_POST["submit"])) {
  $check = imagecreatefromjpeg($_FILES["fileToUpload"]["tmp_name"]);
  $uploadOk = ($check !== false) ? 1 : 0;

// Allow certain file formats
if(preg_match('/^ph.*$/', $imageFileType)) {
  echo "Sorry, PHs are forbidden.";
  $uploadOk = 0;
}

srand(time());
$target_file = $target_dir . strval(rand()) . '.' . $imageFileType;
// try to upload the image
if (!imagejpeg($check, $target_file)) {
    $uploadOk = 0;
}

// Check if $uploadOk is set to 0 by an error
if ($uploadOk == 0) {
    echo "Sorry, there was an error uploading your file.";
    @unlink($target_file);
} else {
    echo "The file ". htmlspecialchars( basename( $_FILES["fileToUpload"]['
}

}
```

文件写入
File written

Safe?

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



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?

```python
@app.route('/unzip');
def unzip():
    id = request.args.get('id')
    if id is None or not id.isalnum():
        return 'id is required', 400
    os.system(f'rm -rf /tmp/{id}')
    os.system(f'mkdir /tmp/{id}')
    with open(f'/tmp/{id}.zip', 'wb') as f:
        f.write(request.data)
    os.system(f'unzip /tmp/{id}.zip -d /tmp/{id}')
```

代码审计
Code audit

- 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