

## HW8-DevSecOps-CI-CD

- Name: Tran Duc Tuan - VDT 2024
- Start dockers command: ``sudo docker compose up --build``
- URL access: `http://localhost:4000/`

## Vulnerability Analysis

### Unrestricted File Upload (/edit.php)

```

12
13 if ($_SERVER['REQUEST_METHOD'] == 'POST' && isset($_POST['id'])) {
14     $id = intval($_POST['id']);
15     if (isset($_FILES['file']) && $_FILES['file']['error'] == 0) {
16         $fileTempName = $_FILES['file']['tmp_name'];
17         $fileName = $_FILES['file']['name'];
18         $fileSize = $_FILES['file']['size'];
19         $fileType = $_FILES['file']['type'];
20
21         $maxsize = 100 * 1024 * 1024;
22         if ($fileSize > $maxsize) {
23             header("Location: /edit.php?id=$id&error=invalid_file_size");
24             exit;
25         }
26         // You, yesterday - initial web app
27         $uploadPath = './upload/' . $fileName;
28
29         if (move_uploaded_file($fileTempName, $uploadPath)) {
30             $conn = createConnection();
31
32             $update_query = "UPDATE jaegers SET image_path = ? WHERE id = ?";
33             $prepare_update = $conn->prepare($update_query);
34             $new_image_path = $uploadPath;
35             $prepare_update->bind_param("si", $new_image_path, $id);
36             $prepare_update->execute();
37
38             header("Location: /edit.php?id=$id&upload=done");
39             exit;
40         } else {
41             header("Location: /edit.php?id=$id&error=upload_error");
42             exit;
43         }
44     } else {
45         header("Location: /edit.php?id=$id&error=file_error");
46         exit;
47     }
48 }
49 ?>
50
51

```

- In server side, it just check file's size to attacker and easy upload a php shell to server

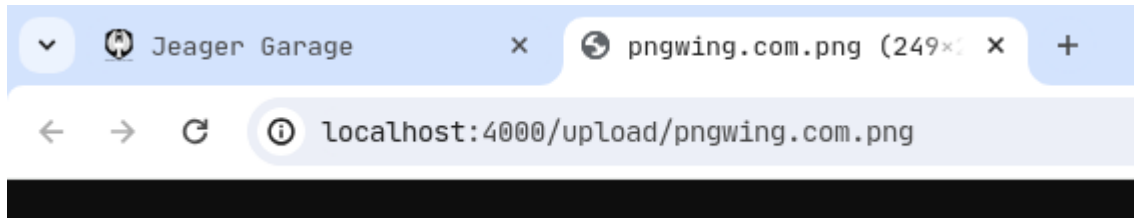
```
<?php phpinfo(); ?>
```

- Success upload shell

Choose file to upload:
No file chosen

Upload Success!

- While user experience the web site, they can realize that user can access images which are rendered in client by access image in `/upload/`



- Access `shell.php` in web server to confirm the vulnerability

Jeager Garage
PHP 8.0.30 - phpinfo()

localhost:4000/upload/shell.php

PHP Version 8.0.30

System	Linux 5d8977401d08 5.15.0-106-generic #116-Ubuntu SMP Wed Apr 17 09:17:56 UTC 2024 x86_64
Build Date	Nov 21 2023 16:12:52
Build System	Linux d6883f8a70f 5.10.0-13-cloud-amd64 #1 SMP Debian 5.10.106-1 (2022-03-17) x86_64 GNU/Linux
Configure Command	'./configure' '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--with-pic' '--enable-ftp' '--enable-mbstring' '--enable-mysqld' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-iconv' '--with-openssl' '--with-readline' '--with-zlib' '--disable-phpdbg' '--with-pear' '--with-libdir=lib/x86_64-linux-gnu' '--disable-cgi' '--with-apxs2' 'build_alias=x86_64-linux-gnu'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-mysql.ini, /usr/local/etc/php/conf.d/docker-php-ext-pdo_mysql.ini, /usr/local/etc/php/conf.d/docker-php-ext-sodium.ini
PHP API	20200930
PHP Extension	20200930
Zend Extension	420200930
Zend Extension Build	API420200930.NTS
PHP Extension Build	API20200930.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, convert.*, consumed, dechunk

This program makes use of the Zend Scripting Language Engine:  
Zend Engine v4.0.30, Copyright (c) Zend Technologies

- To fix this vulnerability, i recommend a snippet of code to filter some params of file upload

```

$allowed = [ 'jpg' => 'image/jpeg', 'jpeg' => 'image/jpeg', 'png' =>
'image/png', 'gif' => 'image/gif' ];

// Validate file name
if (!preg_match('/^[a-zA-Z0-9_-]+\.(jpg|jpeg|png|gif)$/', $fileName)) {
    header("Location: /edit.php?id=$id&error=invalid_file");
    exit;
}

// Validate file extension
$ext = strtolower(pathinfo($fileName, PATHINFO_EXTENSION));
if (!array_key_exists($ext, $allowed)) {
    header("Location: /edit.php?id=$id&error=invalid_file");
    exit;
}

// Validate Content-Type type provided by the browser
if ($fileType !== $allowed[$ext]) {
    header("Location: /edit.php?id=$id&error=invalid_file");
    exit;
}

// Validate MIME type using finfo
$finfo = finfo_open(FILEINFO_MIME_TYPE);
$realMimeType = finfo_file($finfo, $fileTempName);
finfo_close($finfo);

if ($realMimeType !== $allowed[$ext]) {
    header("Location: /edit.php?id=$id&error=invalid_file");
    exit;
}

```

## Insecure Direct Object Reference (/edit.php)

```

106
107 <div class="w3-row-padding w3-padding-16 w3-center">
108
109 <?php
110 $conn = createConnection();
111
112 $jaeger = "SELECT * FROM jaegers WHERE id = ?";
113 $jaeger_query = $conn->prepare($jaeger);
114 $jaeger_query->bind_param("ss", $_GET['id'], $_row['id']);
115 $jaeger_query->execute();
116 $jaeger_result = $jaeger_query->get_result();
117 $jaeger = $jaeger_result->fetch_assoc();
118 if ($jaeger) {
119     ?> You, 2 days ago • initial web app
120
121 <div class="imgcontainer">

```

- Server will get the data of jaeger to edit by if while dont check that user own it or not. In database design, jaeger 1, 2 and 3 belong to admin

```

INSERT INTO users (username, email, user_password, isAdmin) VALUES ('adminUser', 'admin@master.com', MD5('wakanda-forever'), TRUE);

SET @adminUserId = LAST_INSERT_ID();
INSERT INTO jaegers (user_id, jaeger_name, image_path, model, jaeger_status) VALUES (@adminUserId, 'Gipsy Danger', './upload/gipsy_danger.jpg', 'Mark-3', 'Active, Nuclear core, Plasma cannon');
INSERT INTO jaegers (user_id, jaeger_name, image_path, model, jaeger_status) VALUES (@adminUserId, 'Gipsy Danger', './upload/pngwing.com.png', 'Mark-3', 'Active, Nuclear core, Plasma cannon');
INSERT INTO jaegers (user_id, jaeger_name, image_path, model, jaeger_status) VALUES (@adminUserId, 'Striker Eureka', './upload/striker_eureka.png', 'Mark-5', 'Active, Missile full loaded, Big boom');

```

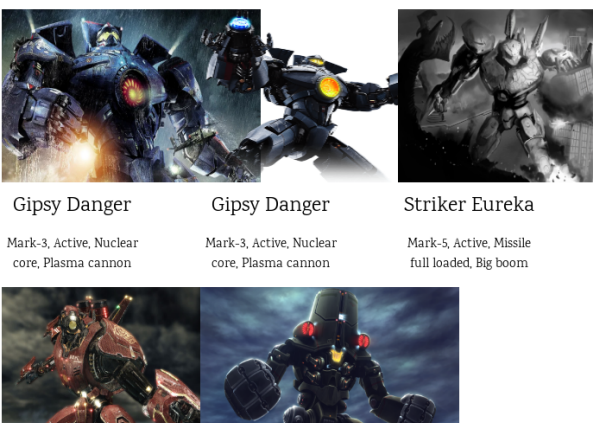
- Login with user1 credential

**Request**  
 Pretty Raw Hex  

```

1 GET / HTTP/1.1
2 Host: localhost:4000
3 sec-ch-ua: "Not-A.Brand";v="99", "Chromium";v="124"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Linux"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-US,en;q=0.9
15 Cookie: auth=dXNlcjE6MjRjOWUxNWU1MmFmYzQ3YzIyMTI3NTdLN2JlZTFlOWQwQ3Q3
16 Connection: close
17
18

```

**Response**  
 Pretty Raw Hex Render  


- Go to Provide, with user1's credential we can only get data of jaeger 4 & 5

Request
Pretty Raw Hex



```

1 GET /profile.php HTTP/1.1
2 Host: localhost:4000
3 sec-ch-ua: "Not-A.Brand";v="99", "Chromium";v="124"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Linux"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Referer: http://localhost:4000/
14 Accept-Encoding: gzip, deflate, br
15 Accept-Language: en-US,en;q=0.9
16 Cookie: auth=dXNlcjE6MjRjOWUxNWU1MmFmYzQ3YzIyNW13NTdlN2JlZTFmOWQwQ3D
17 Connection: close
18
19

```

Response
Pretty Raw Hex Render

## JEAGER GARAGE

Crimson Typhoon

Cherno Alpha

Mark-4, Repairing, Head missing, useless

Mark-1, Destroyed, Head blow, Crashed into trash

- Try to edit Jaeger 5


Request
Pretty Raw Hex

```

1 GET /edit.php?id=5 HTTP/1.1
2 Host: localhost:4000
3 Cache-Control: max-age=0
4 sec-ch-ua: "Not-A.Brand";v="99", "Chromium";v="124"
5 sec-ch-ua-mobile: ?0
6 sec-ch-ua-platform: "Linux"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: http://localhost:4000/profile.php
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-US,en;q=0.9
17 Cookie: auth=dXNlcjE6MjRjOWUxNWU1MmFmYzQ3YzIyNW13NTdlN2JlZTFmOWQwQ3D
18 Connection: close
19
20

```

Response
Pretty Raw Hex Render



Choose file to upload:  No file chosen

Jaeger Name

- Change param id to 1, we can access admin's jaeger


Request
Pretty Raw Hex

```

1 GET /edit.php?id=1 HTTP/1.1
2 Host: localhost:4000
3 sec-ch-ua: "Not-A.Brand";v="99", "Chromium";v="124"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Linux"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: none
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-US,en;q=0.9
15 Cookie: auth=dXNlcjE6MjRjOWUxNWU1MmFmYzQ3YzIyNW13NTdlN2JlZTFmOWQwQ3D
16 Connection: close
17
18

```

Response
Pretty Raw Hex Render



Choose file to upload:  No file chosen

Inspector
Request attributes
Request query parameters
Request cookies
Request headers
Response headers

- To fix this vulnerability, i recommend a snippet of code to check user of jaeger id

```
$cookieValue = base64_decode($_COOKIE['auth']);  
list($username, $password) = explode(':', $cookieValue);  
  
$query = "SELECT id FROM users WHERE username = ? AND user_password = ?";  
$prepare_query = $conn->prepare($query);  
$prepare_query->bind_param("ss", $username, $password);  
$prepare_query->execute();  
$result = $prepare_query->get_result();  
$row = $result->fetch_assoc();  
  
$jaeger = "SELECT * FROM jaegers WHERE id = ? AND user_id = ?";
```