CTF Season 5 Round #10 Write up

Pharmacy (web)

32기 유연서

uploads	2024-05-20 오후 4:45	파일 폴더	
index.php	2024-05-20 오후 4:45	PHP 파일	2KB
style	2024-05-20 오후 4:45	Cascading Style S...	1KB
supermarket.php	2024-05-20 오후 4:45	PHP 파일	1KB

src폴더를 보면 두 개의 php파일이 있다. 위의 index.php를 먼저 확인해보자

```php
<?php
require("supermarket.php");
?>
```

index.php는 처음 부분에서 supermarket.php를 호출한다.

```php
<!DOCTYPE html>
<html>
<head>
    <link rel="stylesheet" type="text/css" href="style.css">
    <title>Pharmacy</title>
</head>
<body>
    <h1>Pharmacy💊</h1>
    <h2>Upload your prescription in gif format...</h2>
    <form action="index.php" method="post" enctype="multipart/form-data" class="file-upload-form">
        <input type="file" name="fileToUpload" id="fileToUpload" class="file-upload-input">
        <input type="submit" value="upload" name="submit" class="file-upload-button">
    </form>
    <br>
```

이후 구조를 살펴보자. 이 부분은 뒷부분에서 활용할 것들을 미리 만들어둔 것 같다.

```php
<?php
$targetDirectory = "uploads/";
$uploadOK = 1;

if( isset($_POST["submit"])) {
    echo '<pre class="file-upload-form">';
    $tmpFile = $_FILES["fileToUpload"]["tmp_name"];
    $currentFile = $_FILES["fileToUpload"]["name"];
    $fileExtension = strtolower(pathinfo($currentFile, PATHINFO_EXTENSION));

    if (mime_content_type($tmpFile) !== "image/gif" || $fileExtension !== "gif") {
        echo "Prescription not gif!₩n";
        $uploadOK = 0;
    }
```

먼저 이 프로그램은 업로드하려는 파일이 gif인지 확인하려는 것 같아 보인다.

```
    if ($uploadOK == 0) {
        echo "Prescription upload failed.₩n";
    } else {
        $randomFileName = bin2hex(random_bytes(16));
        $targetFile = $targetDirectory . $randomFileName . "." . $fileExtension;
        if (move_uploaded_file($tmpFile, $targetFile)) {
            if (isset($_POST['emergent']))
                $targetFile = 'phar://' . $targetFile;
            else
                $targetFile = $targetFile;

            if (file_exists($targetFile)) {
                echo "Prescription submitted!₩n";
            }
        } else {
            echo "Prescription upload failed.₩n";
        }
    }
    echo '</pre>';
```

이후로는 file_exists() 함수를 사용해 파일이 실제로 존재하는지를 확인하는 것 같다.

결론적으로 이 PHP코드와 HTML은 Pharmacy 라는 웹 페이지를 생성하며, 사용자가 GIF를 업로드하도록 하는 것 같다. 더 이상의 해석은 불가능했다.

```
<?php
function goodbye($customer) {
    echo "Good bye, $customer!₩n";
}

class Supermarket {
    public $greet = 'goodbye';
    public $customer = 'dream';
    function __destruct() {
        call_user_func($this->greet, $this->customer);
    }
}
?>
```

한편 위의 index.php 앞부분에서 호출했던 supermarket.php 파일을 확인해보았는데, 그저 인사말을 출력할 수 있도록 한 코드인 것 같았다.

이 문제를 해결하기 위해선 내가 위에서 진행한 웹 코드 분석을 통해 취약점을 유추할 수 있어야 할 텐데.. 그러지 못해 속상했다. 하지만 생각해보면 코드 분석마저도 제대로 하지 못했다고 느낀다. 앞으로의 웹 ctf 문제 풀이를 위해서는 php프로그램 코드에 대한 공부가 필수적일 것 같다 느낀다.