File Upload Vulnerable

<?php

if( isset( $\_POST[ 'Upload' ] ) ) {

// Where are we going to be writing to?

$target\_path = DVWA\_WEB\_PAGE\_TO\_ROOT . "hackable/uploads/";

$target\_path .= basename( $\_FILES[ 'uploaded' ][ 'name' ] );

// Can we move the file to the upload folder?

if( !move\_uploaded\_file( $\_FILES[ 'uploaded' ][ 'tmp\_name' ], $target\_path ) ) {

// No

$html .= '<pre>Your image was not uploaded.</pre>';

}

else {

// Yes!

$html .= "<pre>{$target\_path} succesfully uploaded!</pre>";

}

}

?>

위 코드는 업로드 파일에 대한 검증이 없는 매우 취약한 코드 입니다.

스크린샷, 조류이(가) 표시된 사진

자동 생성된 설명

<hack.php>

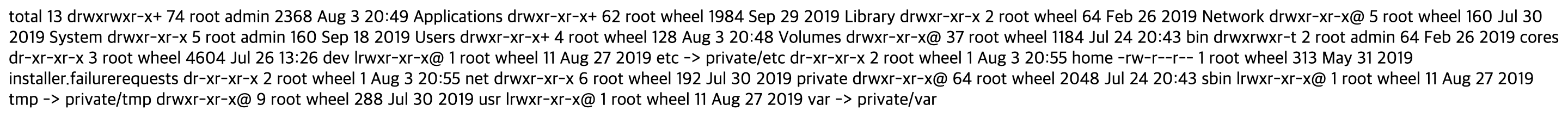
플레이어이(가) 표시된 사진

자동 생성된 설명

Hack.php는 이와 같은 코드 내용을 담고 있습니다.

이 파일을 업로드할 경우 upload 되는 경로에서 이 파일을 확인하게 될 경우 아래와 같이 쉘 코드가 실행된 것을 볼 수 있습니다.

<실행 결과>

이러한 점을 활용하여 악성 코드를 삽입하거나 cat /etc/passwd 명령을 입력하거나 하여 데이터를 가져갈 수 있으므로 파일 형식을 체크해주는 것은 매우 중요합니다.