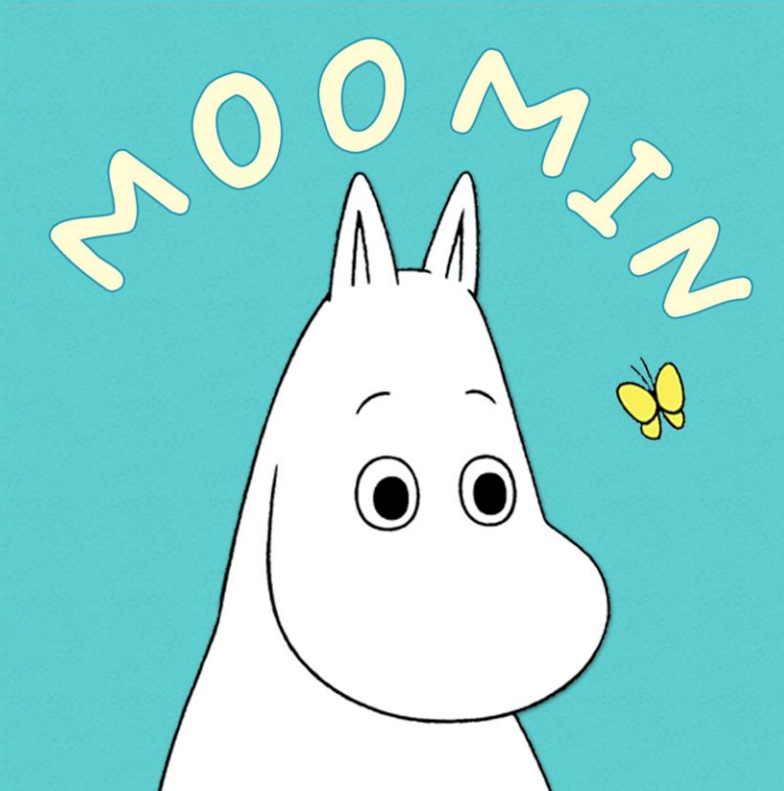


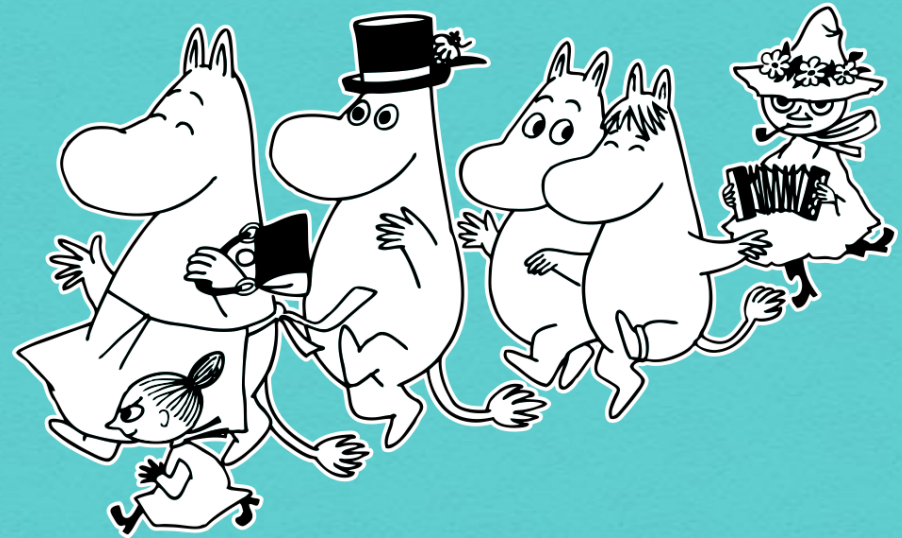
File download 추억점

2019.07.18 HACKDUN



Index

- 1 파일 다운로드 취약점이란 ?
- 2 웹 개발 - 파일 다운로드 구현
- 3 파일 다운로드 취약점 공격 실습
- 4 방어 방법 ?



1

파일 다운로드 취약점이란 ?



허용된 파일 외의 허용되지 않은 파일을 다운로드 하는 것
웹 서버의 소스 및 기밀 문서도 이에 해당되며
이는 웹 애플리케이션에서 **파일명을 필터링 하지 못했을 때** 발생함

파일 다운로드 취약점 공격 예시 (보통 ../ 7~10)

평문 - download.php?file=../ ../ ../ ../ ../ ../ ../ etc/passwd

URL인코딩 - download.php?file=../%2F../%2F../%2F../%2F../%2F../%2F../%2Fetc%2Fpasswd

BASE64인코딩 -download.php?file=Li4vLi4vLi4vLi4vLi4vLi4vZXRjL3Bhc3N3ZA==

2

웹 개발 - 파일 다운로드 구현



```
<?php
$file_name = "msg.txt";
$file = '/msg.txt';
header('Content-type: application/octet-stream');
header('Content-Disposition: attachment; filename="' . $file_name . '"');
header('Content-Transfer-Encoding: binary');

$fp = fopen($file, 'rb');
fpassthru($fp);
fclose($fp);
?>
```

다운 받을 파일 명 : msg.txt

Content-type : 파일 형태

Content-Disposition : attachment - 강제로 가져옴

Content-Transfer-Encoding : binary - 인코딩 하지 않음

파일 다운로드는 Content-Disposition : attachment,

Content-Transfer-Encoding : binary

두개만 있으면 할 수 있음

수정할 내용을 작성해주세요

닉네임 root

제목 파일 다운로드 실습

내용

```
<a href="download.php">file download</a>
```



EDIT

BOARD LIST

그리고 a 태그로 file download를 누르면
download.php가 실행되게 해줌

글을 확인해보세요

글 번호 :30

작성자 :root

파일 다운로드 실습

file download



[목록보기] [글쓰기] [수정] [삭제]

글을 확인해보세요

글 번호 :30

작성자 :root

파일 다운로드 실습

file download



[목록보기] [글쓰기] [수정] [삭제]

msg (1).txt

전체 보기





그런데!!!

실습을 하려는데 취약점이 없다...ㅎ



```
<?php

$file_name = $_GET['path'];
// $file = './';
$file = $file_name;

header('Content-type: application/octet-stream');
header('Content-Disposition: attachment; filename="' . $file_name . '"');
header('Content-Transfer-Encoding: binary');

$fp = fopen($file, 'rb');
fpassthru($fp);
fclose($fp);

?>
```

다운 받을 파일명을 GET방식으로 받아주도록 함


수정할 내용을 작성해주세요

닉네임

제목

내용

msg.txt 다운



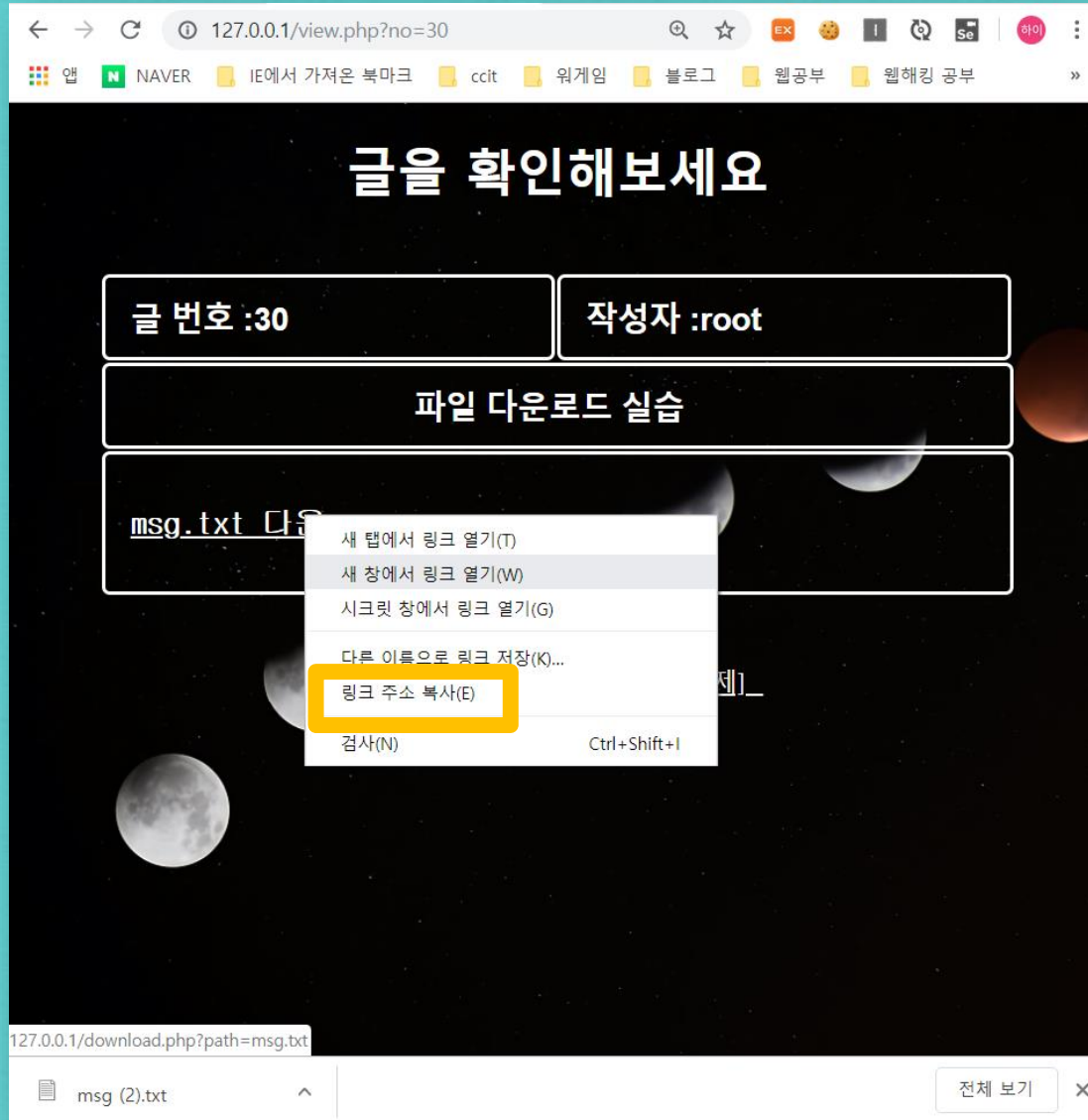
웹 페이지에 msg.txt파일을
다운로드 할 수 있는 버튼 생성



생성된 msg.txt 다운 버튼을 누르면 정상적으로 msg.txt가 다운로드 됨

3

파일 다운로드 취약점 공격 실습



마우스 오른쪽쪽을 눌러서 링크 주소를 복사하면

127.0.0.1/download.php?path=msg.txt

라는 링크 주소가 복사됨

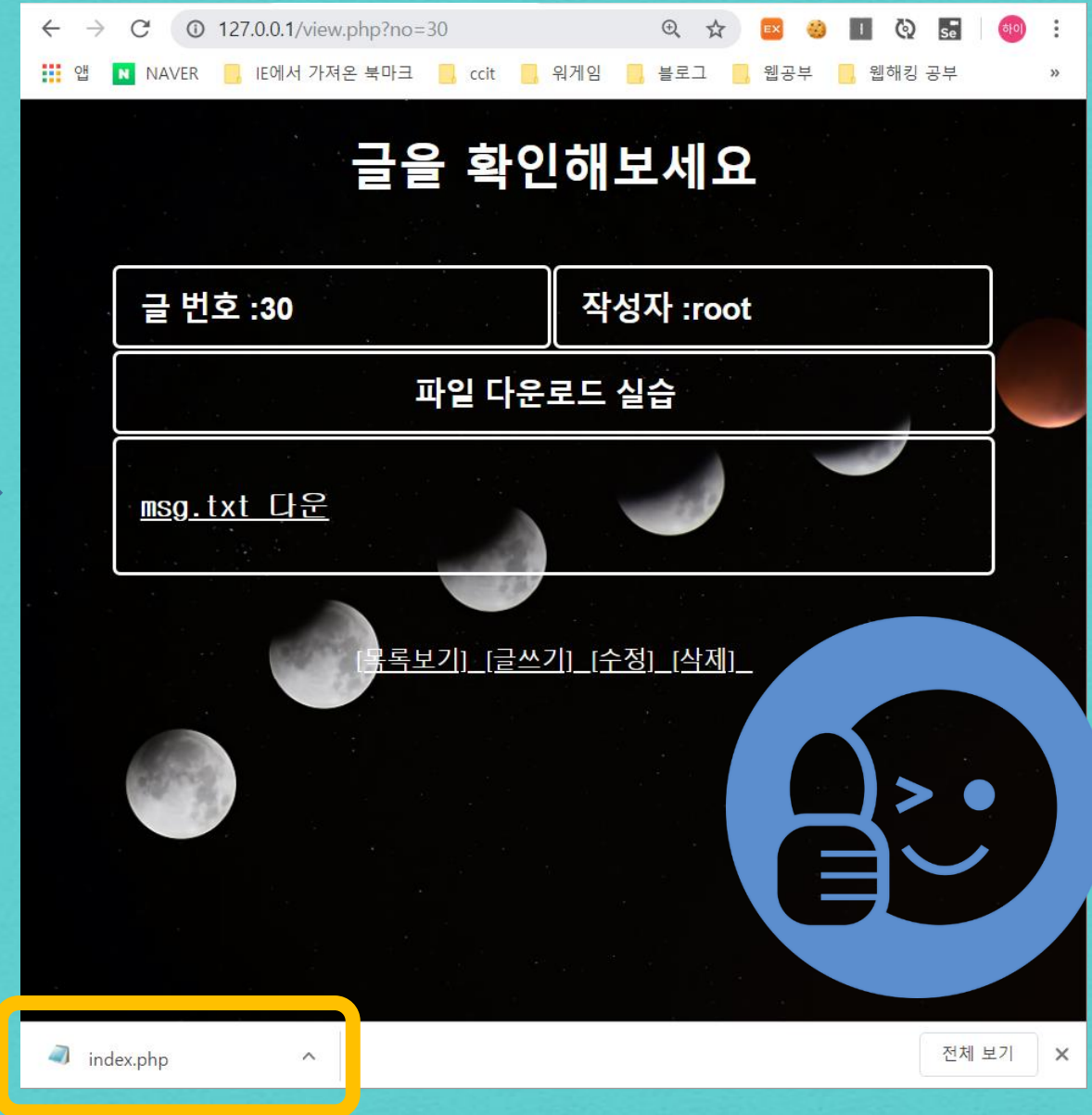
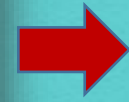
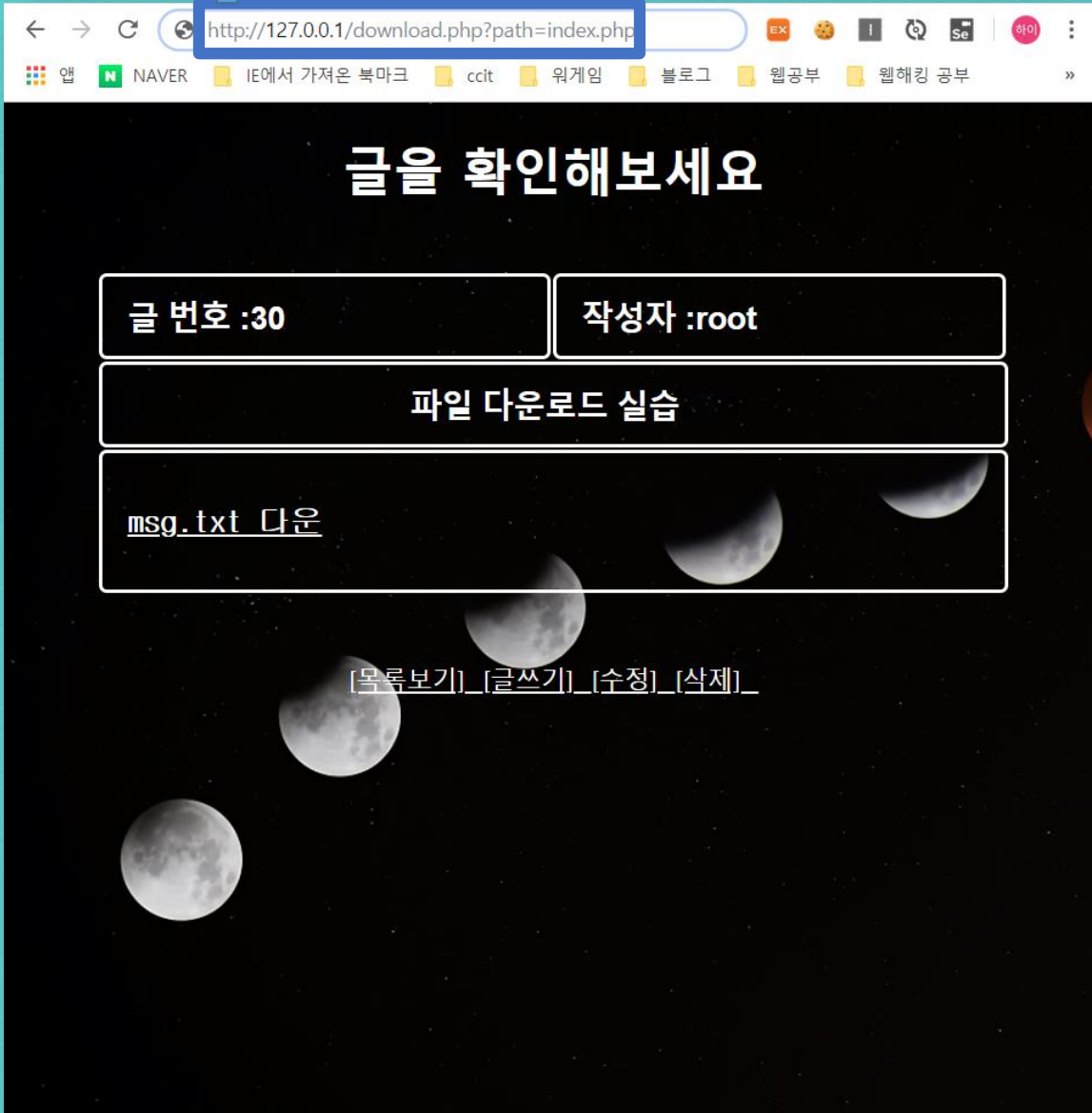
취약점 발견 !

GET 방식으로 path=msg.txt라는 값을 넘겨주고 있는데

여기서 msg.txt라는 파일명을 내가 원하는 파일명으로 바꿔준다면..?



→ http://127.0.0.1/download.php?path=index.php



127.0.0.1/view.php?no=30

앱 NAVER IE에서 가져온 북마크 ccit 워게임 블로그 웹공부 웹해킹 공부 Dun0107 ppt 공부 기획팀 ppt wallsofsheep

글을 확인해보세요

글 번호 :30

msg.txt 다운

index (2).php - 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```

<?php
session_start();
include "dbConnect.php";
?>

<html lang="en">
<center>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
<link rel="stylesheet" type="text/css" href="/main.css">
<body>
  <h1>Account Login</h1>
  <?php
  if(!isset($_COOKIE['session_Id']) && !isset($_COOKIE['logIn_time']) && !isset($_COOKIE['session_Pw'])
    echo "<script>alert('로그인해주세요'); location.href='login.php';</script>";
  } else {
    echo "<script>alert('이미 로그인 되어있습니다.');"
    echo "<a href=main.php>Home</a>";
  }
  ?>

</body>
</center>

```

공격자가 PHP파일의 소스 코드 모두 읽을 수 있게 됨

이렇듯 파일 다운로드 취약점을 공격한다면 파일명을 아는

모든 파일을 다운로드 할 수 있음

개발자만 볼 수 있는 PHP파일과 DB계정 정보가 담긴

중요한 문서들을 모두 다운로드 할 수 있음



상위 디렉토리에 있는 파일도
다운로드 할 수 있나요 ?

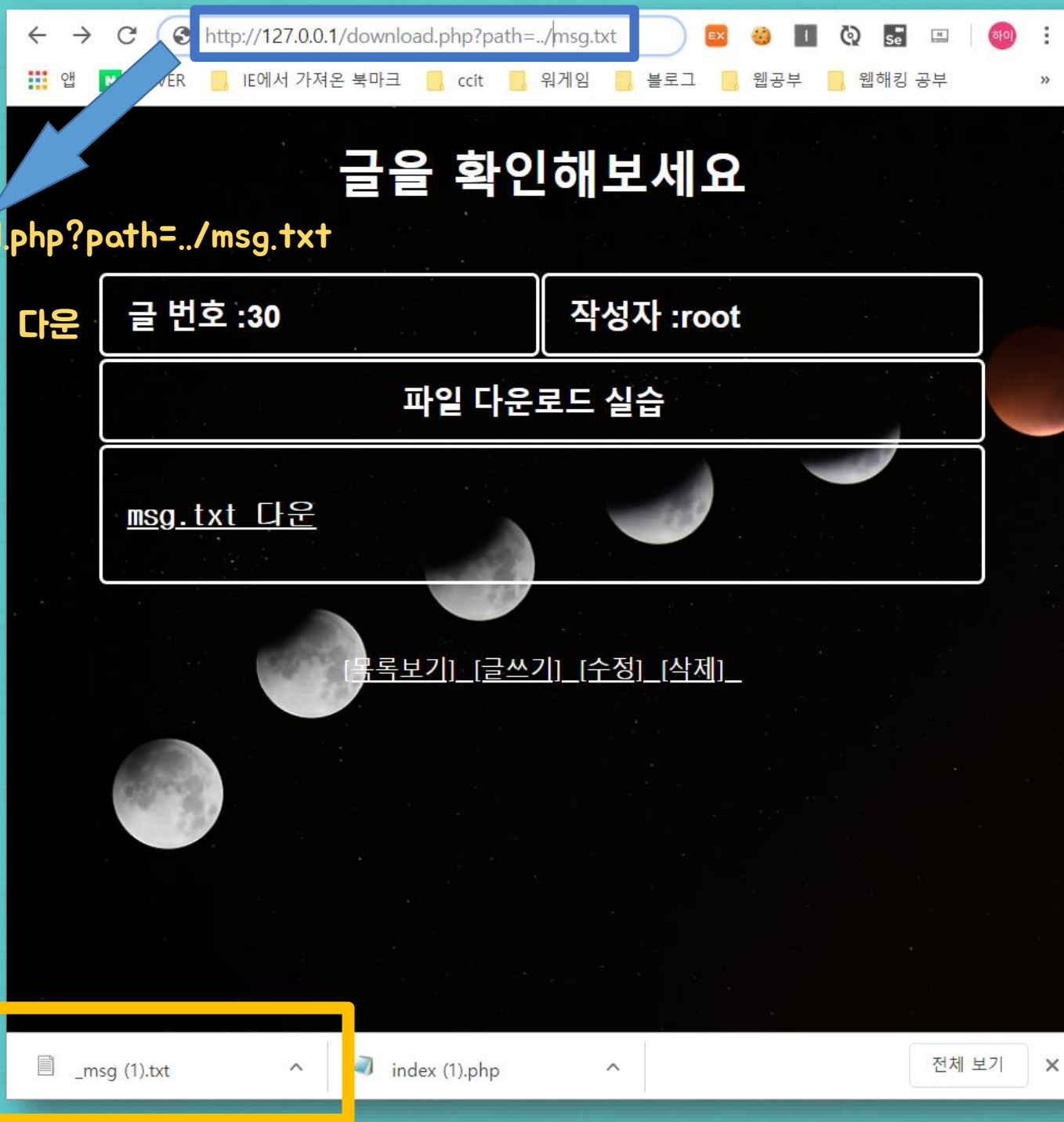
경로 설정 ?



상위 디렉토리에 있는 파일을 다운로드 하고싶으면

경로를 설정해주면 됨

➡ ../



http://127.0.0.1/download.php?path=../msg.txt

상위 디렉토리에 있는 msg.txt 다운

글 번호 :30

작성자 :root

파일 다운로드 실습

msg.txt 다운

[목록보기] [글쓰기] [수정] [삭제]

_msg (1).txt

index (1).php

전체 보기



성공~!

4

방어 방법 ?

1. 데이터 처리 방식을 Dynamic 방식이 아닌 Static 방식으로 함

- Dynamic 방식 `http://127.0.0.1/download.php?path=msg.txt`
- Static 방식 `msg.txt download`
 ➡ `/msg.txt`

2. 특수문자 필터링

ex) = , ../ 등

다음 주 예고

파일 다운로드 취약점을 공격해
원하는 파일을 다운로드하려면
파일명을 알아야하잖아.
파일명... 어떻게 얻어요?



다음 주 이 시간에....

리
글

MOOMIN

