

# Week 31\_ 각종 취약점 조사(2)

---

Refactoring Study

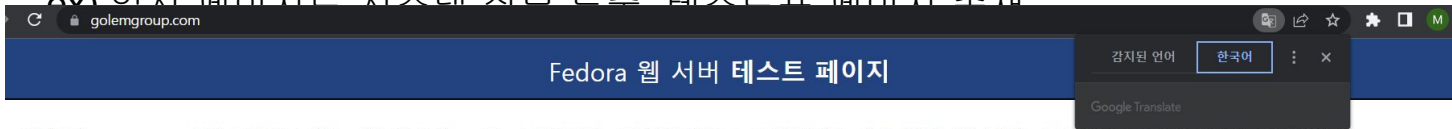
2022.10.22 Kwon Moonjeong

# 취약한 파일 존재 취약점

- 취약한 파일 존재 취약점이란?

- 웹 루트 하위에 내부 문서나 백업파일, 로그파일, 압축파일과 같은 파일이 존재할 경우 파일명을 유추하여 파일명을 알아내고, 직접 요청하여 해킹에 필요한 서비스 정보를 획득할 수 있는 취약점

- **예) 임시 페이지로 시스템 정보 노출 테스트용 페이지 존재**



이 페이지는 Fedora HTTP 서버가 설치된 후 제대로 작동하는지 테스트하는 데 사용됩니다. 이 페이지를 읽을 수 있다면 이 사이트에 설치된 웹 서버가 제대로 작동하지만 아직 구성되지 않았음을 의미합니다.

## 일반 대중의 구성원인 경우:

당신이 이 페이지를 보고 있다는 사실은 당신이 방문한 웹사이트에 문제가 있거나 일상적인 유지보수가 진행 중임을 나타냅니다.

이 웹사이트의 관리자에게 당신이 예상했던 페이지가 아닌 이 페이지를 보았다는 것을 알고 싶다면 이메일을 보내야 합니다. 일반적으로 "webmaster"라는 이름으로 보내지고 웹사이트의 도메인으로 전달되는 메일은 적절한 사람에게 도달해야 합니다.

예를 들어, `www.example.com`을 방문하는 동안 문제가 발생했다면 `webmaster@example.com`으로 이메일을 보내야 합니다.

Fedora는 널리 사용되는 컴퓨터 운영 체제인 Linux의 배포판입니다. 무료이며 무료 웹 서버 소프트웨어가 포함되어 있기 때문에 호스팅 회사에서 일반적으로 사용됩니다. 많은 경우 웹 서버를 올바르게 설정하지 않고 예상 웹 사이트 대신 이 "테스트 페이지"를 표시합니다.

따라서 다음 사실을 염두에 두십시오.

- Fedora Project 또는 Red Hat은 이 서버에서 호스팅되는 웹사이트 또는 콘텐츠와 아무런 관련이 없습니다(달리 명시적으로 언급되지 않는 한).
- Fedora Project나 Red Hat은 이 웹 서버를 "해킹"하지 않았습니다. 이 테스트 페이지는 Fedora 웹 서버 소프트웨어에 포함된 구성 요소입니다.

Fedora에 대한 자세한 내용은 [Fedora 프로젝트 웹사이트](#)를 참조하십시오.

## 웹사이트 관리자인 경우:

이제 webroot 디렉토리에 콘텐츠를 추가할 수 있습니다. 그렇게 하기 전까지는 귀하의 웹사이트를 방문하는 사람들에게 귀하의 콘텐츠가 아닌 이 페이지가 표시됩니다.

**Apache Webserver**를 사용하는 시스템의 경우: 이제 디렉토리에 콘텐츠를 추가할 수 있습니다. 그렇게 하기 전까지는 귀하의 웹사이트를 방문하는 사람들에게 귀하의 콘텐츠가 아닌 이 페이지가 표시됩니다. 이 페이지가 사용되지 않도록 하려면 파일의 지칭을 따르세요.

```
/var/www/html/etc/httpd/conf.d/welcome.conf
```

**Nginx**를 사용하는 시스템의 경우: 이제 콘텐츠를 원하는 위치에 놓고 **nginx** 구성 파일 `root`에서 구성 지시문을 편집해야 합니다 `/etc/nginx/nginx.conf`



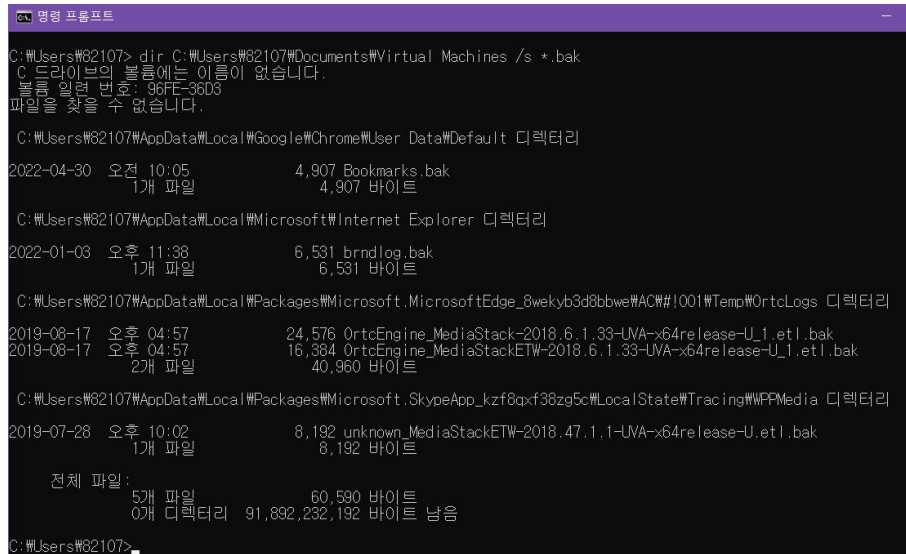
# 취약한 파일 존재 취약점

- 취약한 파일 점검 방법
    - 웹서버의 가상 디렉터리로 이동하여 다음에 제시되는 확장자의 파일을 찾아 불필요한 정보가 포함되었는지 여부를 판단
- ※ 문서파일일 경우 내용에 개인정보 등의 주요정보 존재여부 확인 필요

구 분	검색할 파일의 형식(확장자)
압축파일	.zip, .rar, .alz, .tar, .gz, .gzip 등의 압축파일
백업파일	.bak, .org 등
로그파일	.log, .txt 등
설정파일	.sql, .ini, .bat 등
문서파일	.hwp, .doc, .xls, .ppt, .pdf 등
기타	test.*, imsi.*, .tmp 등

# 취약한 파일 존재 취약점

- 웹 서버 디렉토리에서 .bak 확장자로 끝나는 백업 파일을 모두 찾는 경우의 예시
  - Unix / Linux의 검색 예시 : **find [웹 서버 디렉토리] - name "\*.bak"**  
\* find 명령어 : 리눅스 파일 시스템에서 파일을 검색하는 데 사용되는 명령어로, 다양한 표현식을 사용하여 원하는 파일의 목록을 추출할 수 있음
  - Windows의 검색 예시 : **dir [웹 서버 디렉토리] /s \*.bak**  
\* dir은 디렉토리 명령어로, 파일들을 보여줌.  
dir 뒤에 /s는 하위 경로를 포함하는 명령어로, 해당위치에 또 다른 디렉토리도 보여줌.



```
C:\Users\82107> dir C:\Users\82107\Documents\Virtual Machines /s *.bak
C 드라이브의 볼륨에는 이름이 없습니다.
볼륨 일련 번호: 96FE-36D6
파일을 찾을 수 없습니다.

C:\Users\82107\AppData\Local\Google\Chrome\User Data\Default 디렉터리
2022-04-30 오전 10:05 4,907 Bookmarks.bak
1개 파일 4,907 바이트

C:\Users\82107\AppData\Local\Microsoft\Internet Explorer 디렉터리
2022-01-03 오후 11:38 6,531 brndlog.bak
1개 파일 6,531 바이트

C:\Users\82107\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC#\1001\Temp\OrcLogs 디렉터리
2019-08-17 오후 04:57 24,576 OrcEngine_MediaStack-2018.6.1.33-UVA-x64release-U_1.etl.bak
2019-08-17 오후 04:57 16,384 OrcEngine_MediaStackETW-2018.6.1.33-UVA-x64release-U_1.etl.bak
2개 파일 40,960 바이트

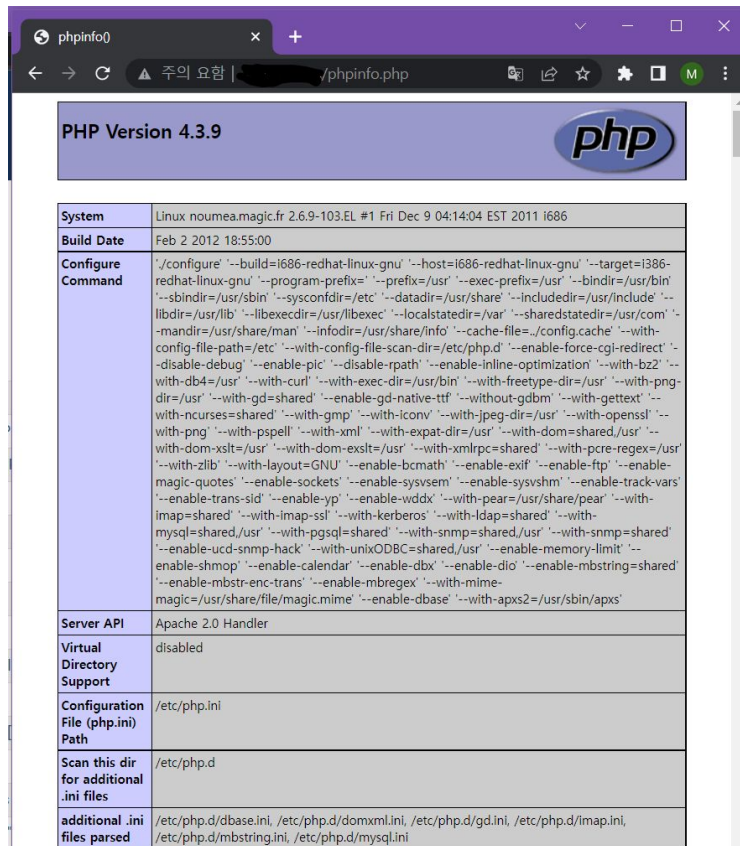
C:\Users\82107\AppData\Local\Packages\Microsoft.SkypeApp_kzf8qxf38zg5c\LocalState\Tracing\WPPMedia 디렉터리
2019-07-28 오후 10:02 8,192 unknown_MediaStackETW-2018.47.1.1-UVA-x64release-U.etl.bak
1개 파일 8,192 바이트

전체 파일:
52개 파일 60,590 바이트
0개 디렉터리 91,892,232 바이트 남음

C:\Users\82107>
```

# 취약한 파일 존재 취약점

- PHP 언어로 개발한 웹서버의 경우 PHP의 정보를 나타내는 기본 페이지(`phpinfo.php`)가 외부로 노출되었는지 점검 필요
  - 검색 방법(리눅스/유닉스) : `find [웹 서버 디렉터리] -name "phpinfo.php"`
  - 또는 모든 PHP 파일에 “`phpinfo()`” 문자열이 포함되어있는 파일을 조회 : `grep "phpinfo()" *php`
  - \* 파일내의 문자열 검색 시 시스템에 과부하가 발생할 수 있음



System	Linux noumea.magic.fr 2.6.9-103.EL #1 Fri Dec 9 04:14:04 EST 2011 i686
Build Date	Feb 2 2012 18:55:00
Configure Command	./configure '--build=i686-redhat-linux-gnu' '--host=i686-redhat-linux-gnu' '--target=i686-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib' '--libexecdir=/usr/libexec' '--localstatedir=/var' '--sharedstatedir=/usr/com' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--cache-file=../config.cache' '--with-config-file-path=/etc' '--with-config-file-scan-dir=/etc/php.d' '--enable-force-cgi-redirect' '--disable-debug' '--enable-pic' '--disable-rpath' '--enable-inline-optimization' '--with-bz2' '--with-db4=/usr' '--with-curl' '--with-exec-dir=/usr/bin' '--with-freetype-dir=/usr' '--with-png-dir=/usr' '--with-gd=shared' '--enable-gd-native-ttf' '--without-gdcm' '--with-gettext' '--with-ncurses=shared' '--with-gmp' '--with-iconv' '--with-jpeg-dir=/usr' '--with-openssl' '--with-png' '--with-pspell' '--with-xml' '--with-xmlrpc=shared' '--with-dom=shared' '--with-dom-xslt=/usr' '--with-dom-exslt=/usr' '--with-xmlrpc=shared' '--with-pcre-regex=/usr' '--with-zlib' '--with-layout=GNU' '--enable-bcmath' '--enable-exif' '--enable-ftp' '--enable-magic-quotes' '--enable-sockets' '--enable-sysvshm' '--enable-track-vars' '--enable-trans-sid' '--enable-yp' '--enable-wddx' '--with-pear=/usr/share/pear' '--with-imap=shared' '--with-imap-ssl' '--with-kerberos' '--with-ldap=shared' '--with-mysql=shared' '--with-pgsql=shared' '--with-snmp=shared' '--with-snmpp=shared' '--enable-ucd-snmpp-hack' '--with-unixODBC=shared' '--enable-memory-limit' '--enable-shmop' '--enable-calendar' '--enable-dbx' '--enable-did' '--enable-mbstring=shared' '--enable-mbstr-enc-trans' '--enable-mbregex' '--with-mime-magic=/usr/share/file/magic.mime' '--enable-dbase' '--with-apxs2=/usr/sbin/apxs'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
additional .ini files parsed	/etc/php.d/dbase.ini, /etc/php.d/domxml.ini, /etc/php.d/gd.ini, /etc/php.d/imap.ini, /etc/php.d/mstring.ini, /etc/php.d/mysql.ini

# 취약한 파일 존재 취약점

- 대응 방안
  - 웹 서버는 개발과 운영 환경을 분리하여 운영 환경에서 소스 코드 수정 또는 테스트 목적의 임시 파일을 생성하지 않도록 함
  - 웹 서버의 디렉터리에 존재하는 기본 설치 파일, 임시 및 백업 파일을 조사하여 웹 사용자가 접근하지 못하도록 조치, 장기적으로 불필요 파일을 검색하여 제거

구 분	설치 시 생성되는 기본 파일 위치
아파치(Apache)	ServerRoot/cgi-bin/
톰캣(Tomcat)	TOMCAT_HOME/examples
웹토비(WebToB)	ServerRoot/cgi-bin/

- 일반적으로 존재하는 백업파일 유형 : .bak, ws\_ftp.log, tar.gz, zip, .html.old, 파일명.날짜

# 계정 관리 취약점

- 계정 관리 취약점이란?

- 회원가입 시에 안전한 패스워드 규칙이 적용되지 않아서 취약한 패스워드로 회원 가입이 가능할 경우 무차별 대입공격 및 추측을 통해 패스워드가 누출될 수 있는 취약점  
ex) master, webmaster, admin, administrator, root, manager, test, masterweb

- 대응 방법

- 사용자가 취약한 패스워드를 사용할 수 없도록 패스워드 생성규칙을 강제 할 수 있는 로직을 적용

구분	내 용
패스워드 생성규칙	<ul style="list-style-type: none"><li>- 세가지 종류 이상의 문자구성으로 8자리 이상의 길이</li><li>- 두가지 종류 이상의 문자구성으로 10자리 이상의 길이</li></ul>
패스워드 생성 금지규칙	<ul style="list-style-type: none"><li>- 간단한 문자(영어단어 포함)나 숫자의 연속사용은 금지</li><li>- 키보드 상에서 일련화 된 배열을 따르는 패스워드 선택 금지</li><li>- 사전에 있는 단어, 이를 거꾸로 철자화한 단어 사용 금지</li><li>- 생일, 전화번호, 개인정보 및 아이디와 비슷한 추측하기 쉬운 비밀번호 사용 금지</li><li>- 이전에 사용한 패스워드는 재사용 금지</li><li>- 계정 잠금 정책 설정 예) 로그인 5회 실패 시 30분 동안 사용중지</li></ul>

# 실명인증 취약점

- 실명인증 취약점이란?
  - 사용자 본인 확인(실명인증) 과정을 정상적으로 마친 후, 웹 프록시 툴을 이용하여 사용자 정보를 변조할 수 있는 취약점
  - 실명인증 취약점을 통해 관리자로 위장하여 개인정보를 수집하거나, 홈페이지 가입 시 제공하는 포인트 등을 악용하는 등의 공격 가능

\* 프록시란? 서버와 클라이언트 사이에서 대리로 통신을 수행해주는 것.

웹 프록시 툴을 사용하여 웹 프록시 서버의 주소와 포트를 설정 해주면, 브라우저에서 보낸 웹 요청이 프록시 서버를 경유하게 되기 때문에 중간에 패킷을 가로챌 수 있음.

## 수동 프록시 설정

이더넷 또는 Wi-Fi 연결에 프록시 서버를 사용합니다. 이 설정은 VPN 연결에 적용되지 않습니다.

프록시 서버 사용

☒ 컴

주소

127.0.0.1

포트

8080

## Proxy Listeners



Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use

Add	Running	Interface	Invisible	Redirect	Certificate
Edit	<input checked="" type="checkbox"/>	127.0.0.1:8080			Per-host
Remove					



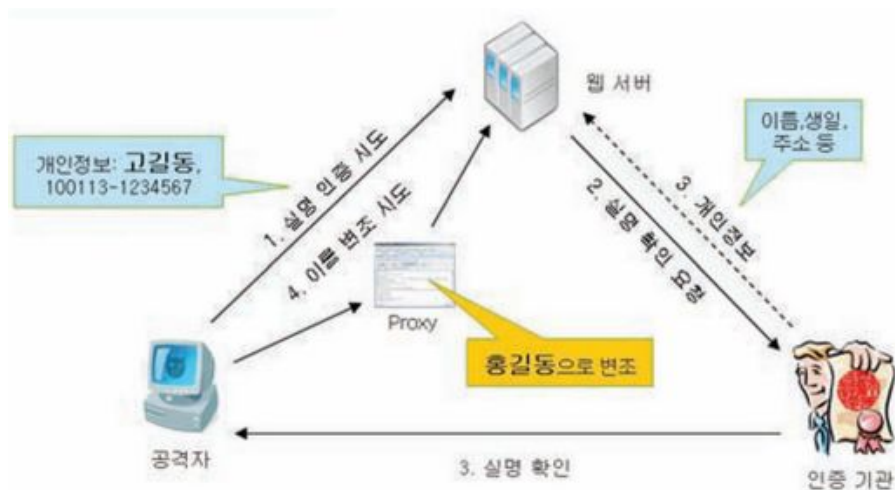
# 실명인증 취약점

---

- 점검 방법
  - 웹서버 내의 실명인증 페이지로 이동 후, 웹 프록시 프로그램을 이용하여 실명인증 과정 중에 발생하는 네트워크 트래픽을 모니터링함
  - 사용 가능한 웹 프록시 도구 : Paros, Burp Suite, Fiddler
  - 실명인증 우회 과정
    - ㉠ 공격자는 취약점이 존재하는 웹서버에 정상적인 사용자의 개인정보로 접속하여 실명인증 수행
    - ㉡ 웹서버(또는 개인)는 인증기관으로 실명정보 확인을 요청
    - ㉢ 실명정보를 확인한 인증기관은 웹서버에 사용자의 나이, 성별, 연락처 등의 개인정보를 전달하며 사용자에게는 "실명인증 성공" 메시지를 전달
    - ㉣ 공격자는 수신한 실명인증 결과를 웹 프록시 툴을 이용하여 임의의 사용자로 변조 후 가입 또는 글 작성을 완료
    - ㉤ 취약점이 존재하는 웹서버는 사용자가 요청한 정보를 검증과정 없이 신뢰하여 변조된 사용자의 가입(또는 글 작성)을 허용

# 실명인증 취약점

- 1~3. : “고길동” 이라는 진짜 정보로 실명 인증
- 4. : 웹 프록시 툴을 이용하여 임의의 사용자로 변조 후 홈페이지를 이용
- 실명인증은 정상적으로 수행했기에 사이트에 정상적으로 가입했으나, 이후에 개인 정보를 변조하여 악용 가능



- 대응 방안

- 중요한 정보가 있는 홈페이지(실명 등)은 재 인증 적용
- 안전하다고 확인된 라이브러리나 프레임워크(OpenSSL이나 ESAPI의 보안기능 등)를 사용

\* OpenSSL : 데이터통신을 위한 TLS, SSL 프로토콜을 이용할 수 있는 오픈소스 라이브러리

\* ESAPI(Enterprise Security API) : 웹 애플리케이션 개발 과정에서 발생하는 다양한 보안 침해사고를 해결하기 위해 OWASP에서 OWASP TOP10과 함께 해당 문제점을 개선하기 위해 제작, 배포되는 보안 라이브러리

# 전송 시 주요 정보 노출 취약점

- 전송 시 주요 정보 노출 취약점이란?
  - 프로그램이 보안과 관련된 민감한 데이터를 통신채널을 통해서 평문으로 송수신 할 경우, 통신채널 스니핑을 통해 인가되지 않은 사용자에게 민감한 데이터가 노출될 수 있는 취약점
- 점검 방법
  - 1) 점검 대상 웹서버의 로그인 페이지로 이동
  - 2) 네트워크 패킷 모니터링 프로그램 (ex. Wireshark)을 이용하여 로그인 과정상에서 발생하는 네트워크 트래픽을 저장
  - 3) 로그인 후 네트워크 패킷 모니터링 프로그램을 통해 로그인 시 저장된 인증 정보를 찾아 암호화 여부를 확인

\* 로그인 과정상에서 I-PIN, 전자서명인증서를 사용할 경우 취약점이 존재하지 하지 않음 (ID와 비밀번호를 병행할 경우 취약할 수 있음)

# 전송 시 주요 정보 노출 취약점

---

- 대응방안
  - 웹 서버 내에서의 조치
    - 전자서명인증서, **SSL(Secure Socket Layer)**을 이용하여 사용자 식별 및 **DATA** 전송 시 암호화 통신으로 데이터 전송의 안전성을 확보
    - 조치 완료 후 인증과정 등의 주요 정보 노출 여부를 재점검
  - 홈페이지 개발 보안 조치
    - 중요정보와 관련된 민감한 데이터(개인정보, 비밀번호 등) 전송 시 통신채널 (또는 전송데이터) 암호화 적용