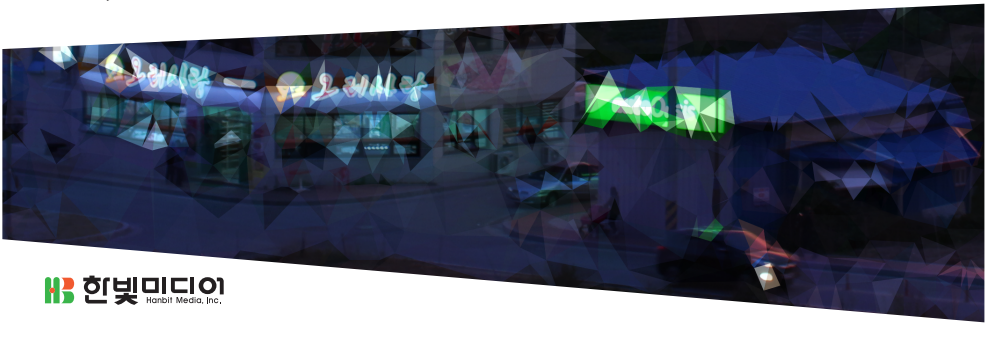
Hanbit RealTime 108

워드프레스 플러그인

취약점 진단과 모의해킹

조정원, 유희만 지음



한빛미디어 Hanbit Media, Inc.

워드프레스 플러그인
취약점 진단과 모의해킹

조정원, 유희만 지음

한빛미디어
Hanbit Media, Inc.

표지 사진 **김종욱**

이 책의 표지는 김종욱 님이 보내 주신 풍경사진을 담았습니다.
리얼타임은 독자의 시선을 담은 풍경사진을 책 표지로 보여주고자 합니다.

사진 보내기 **ebookwriter@hanbit.co.kr**

워드프레스 플러그인 취약점 진단과 모의해킹

초판발행 2015년 7월 10일

지은이 조정원, 유희만 / **펴낸이** 김태헌
펴낸곳 한빛미디어(주) / **주소** 서울시 마포구 양화로 7길 83 한빛미디어(주) IT출판부
전화 02-325-5544 / **팩스** 02-336-7124
등록 1999년 6월 24일 제10-1779호
ISBN 978-89-6848-769-9 15000 / **정가** 14,000원

총괄 배용석 / **책임편집** 김창수 / **기획·편집** 정지연 / **교정** 이미연
디자인 표지/내지 여동일, 조판 최송실
마케팅 박상용 / **영업** 김형진, 김진불, 조유미

이 책에 대한 의견이나 오탈자 및 잘못된 내용에 대한 수정 정보는 한빛미디어(주)의 홈페이지나 아래 이메일로 알려주십시오.
한빛미디어 홈페이지 www.hanbit.co.kr / **이메일** ask@hanbit.co.kr

Published by HANBIT Media, Inc. Printed in Korea

지금 하지 않으면 할 수 없는 일이 있습니다.
책으로 펴내고 싶은 아이디어나 원고를 메일(ebookwriter@hanbit.co.kr)로 보내주세요.
한빛미디어(주)는 여러분의 소중한 경험과 지식을 기다리고 있습니다.

저자 소개

지은이_ **조정원**

chogar@naver.com

KB투자증권에서 보안 업무를 담당하고 있으며, 보안프로젝트(www.boanproject.com) 운영자로 활동하고 있다. 에이쓰리시큐리티에서 5년 동안 모의해킹 컨설턴트를 하였으며, 모의해킹 프로젝트 매니저, 웹 애플리케이션, 소스 코드 진단 등 다양한 영역에서 취약점 진단을 수행하였다. 이후 KTH 보안팀에서 모바일 서비스, 클라우드 서비스 보안, 침해사고 대응업무를 하였다.

주요 저서로는 『IT엔지니어로 사는법 1』(비팬북스, 2015), 『안드로이드 모바일 악성코드와 모의 해킹 진단』(에이콘출판사, 2014), 『모의해킹이란 무엇인가』(위키북스, 2014), 『칼리 리눅스를 활용한 모의 해킹』(에이콘출판사, 2014), 『디지털 포렌식의 세계』(인포더북스, 2014), 『크래커 잡는 명탐정 해커』(성안당, 2010) 등이 있으며, 보안프로젝트 멤버들과 함께 다양한 영역에서 활동하고 있다.

지은이_**유희만**

god2zuzu@naver.com

SK인포섹에서 모의해킹 업무를 담당하고 있으며, 보안프로젝트(www.boanproject.com) 연구원으로 활동하고 있다. 수원대학교 보안동아리 FLAG 회장을 역임하였고, 아마추어 해킹그룹 JAC-LAB에서 활동하고 있다. 웹 애플리케이션, 모바일 애플리케이션, 소스 코드 진단 등 다양한 영역에서 취약점 진단을 수행하였으며, 워드프레스와 관련된 신규 취약점을 발견하여 Exploit-DB에 등록하였다.

감사의 말

지은이_ **조정원**

모의해킹 컨설팅 업체 생활을 마치고 관리실무를 하기 시작할 때가 생각난다. 공격자가 아닌 방어자의 입장이 되어 주 업무가 침해사고대응으로 바뀌었다. 모의해킹 업무를 해 왔기 때문에 필자가 소속된 서비스를 정기적으로 진단도 하였다. 그러자 컨설팅 할 때에는 보이지 않던 것이 보이기 시작했다. 세상에는 정말 많은 오픈소스 서비스가 있다는 것이다. 이 오픈소스를 기반으로 서비스를 개발하면 버전에 따라, 어떤 기능을 더하냐에 따라 취약점이 달리 나온다. 개발자가 제대로 관리하지 않으면 순식간에 공격자에게 당하고 만다. 아무리 사전대응한다고 하더라도 공개된 웹을 통해 들어오는 공격은 너무 다양하고, 하루하루 변형되는 공격 코드는 항상 방어체계보다 빠르다.

워드프레스는 세계에서 가장 많이 사용하는 CMS 오픈소스 서비스다. 국내에도 워드프레스를 활용하는 책이 많이 출간되며 대중에게 알려졌다. 호스팅 서비스(가비아 등)에 홈페이지를 제작할 때 워드프레스를 무료 설치로 선택할 수 있다. 추천 플러그인도 설치되어 있고, 유료 테마를 추천하여 구매하게 유도한다. 아무 생각 없이 설치한 서비스는 언젠가 공격자의 표적이 된다. 아무리 보안의식을 교육해도 임직원조차 보안의식이 쉽사리 바뀌지 않는데 대중에게 보안의식을 강화한다는 것은 오죽이나 어려울까. 이것은 끊임없는 과제일 것이다.

이 책을 읽는 독자는 모의해킹 진단이나 워드프레스로 서비스를 운영하는 회사의 보안담당자일 가능성이 크다. 이 책에서 모든 공격 유형을 다루지는 못하지만, 각 공격 유형에 대해 배워 보고, 우회기법은 어떤 것이 있는지, 워드프레스를 보안하기 위해서 어떤 노력이 필요한지 충분히 느낄 수 있을 것이다. 고객의 서비스를 진단하든 자사의 서비스를 진단하든 이 책이 좋은 참고 자료가 되었으면 하는 바람이다.

이 책을 집필하는 데 많은 시간을 쏟고 무척 노력하였다. 같이 집필한 팀원들이 없었다면 절대로 마무리되지 않았을 것이다. 목표를 향해 열심히 해 준 보안프로젝트의 모든

멤버에게 항상 감사하다. 이 책을 쓰는 동안 옆에서 항상 응원해 준 아내 김혜진과 아들 호영, 딸 희영에게 사랑한다고 전하고 싶다.

지은이_**유희만**

CMS 기반의 웹 서비스가 늘어나면서 이에 따라 보안 사고도 급증하고 있다. 이 책은 CMS 중 가장 많이 사용하는 워드프레스를 중심으로 관리적·기술적 취약점을 분석하고 이에 대한 대응 방안을 수립하는 데 길잡이가 되도록 작성하였다.

이 책에서는 기존의 웹 해킹 관련 도서와 달리 이론에 대한 부분을 많이 다루지 않았다. 오픈소스라는 이점을 살려 기존에 알던 이론을 이용하여 공격 방법을 직접 실습하고, 해당 공격에 대한 대응 방안을 수립할 수 있는 지식을 알려주며, 워드프레스 플러그인의 취약점 분석을 통해 워드프레스를 공부하는 학생이나 모의해킹 실무자에게 모의해킹 방법에 대한 이해를 도와준다. 또한, 워드프레스를 실습해 볼 수 있는 환경을 구성하는 방법을 쉽게 설명하고 있어 책으로 습득하는 이론적인 지식에 끝나지 않고 직접 실습해 볼 수 있다.

책에서 다룬 취약점 외에도 Exploit-DB(http://www.exploit-db.com)를 통해 더욱 다양한 취약점 분석을 경험할 수 있다. 워드프레스를 공부하는 학생은 이 책을 통해 실무에서 취약점을 어떻게 발견하며 어떻게 진단하는지 살펴볼 수 있다. 모의해킹 실무자에게는 취약점 분석을 통해 모의해킹 방법론에 대해 다시 한 번 정리해 줄 뿐만 아니라 취약점 대응 방안을 수립하는 데 도움을 줄 것이다. 또한, 워드프레스로 웹 서비스를 제공하는 관리자에게는 보안 플러그인을 통한 홈페이지의 보안성을 강화할 수 방법을 제공한다.

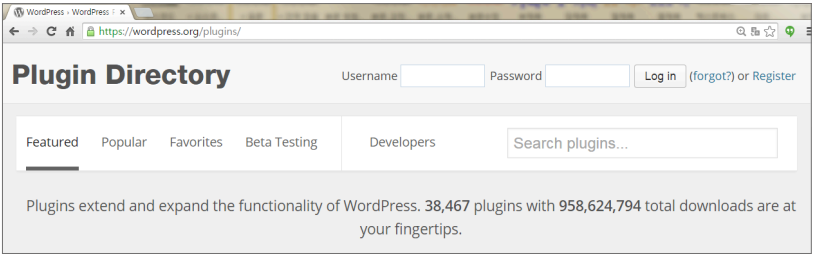
보안프로젝트에서 활동을 시작한 후, 워드프레스 연구 활동을 하며 조정원 선배님과 집필을 준비하는 데 1년에 가까운 시간이 소요되었다. 어떻게 보면 길고 어떻게 보면 짧은 시간이지만 이 책을 출판하기까지의 모든 시간이 무척이나 소중하다. 이 책을 준비하는 데 도움을 주신 보안프로젝트 집필 멤버들과 팀원들께 고마움을 전하고 싶다. 이분들의 열정이 있어 포기하지 않고 이 책을 출판할 수 있게 되었다. 첫 출판이라는 좋은 기회를 주신 보안프로젝트 운영자 조정원 선배님께 다시 한 번 감사의 인사를 드리고, 밤늦도록 주말까지 열심히 연구 활동을 하는 보안프로젝트의 모든 맴버에게 응원의 메시지를 보낸다.

이 책은 입문자가 웹 서비스 취약점 진단을 이해하도록 가이드하고 있다. 수많은 오픈소스 블로그 및 사이트, 쇼핑몰이 있음에도 워드프레스를 예제로 시나리오를 풀어간 이유는 다음과 같다.

워드프레스 사용 증가

워드프레스의 테마가 다양해지고 플러그인 수가 증가하여 개인 사용자에게 워드프레스에 대한 반응이 좋다. 국내 파워블로거도 광고수입, 테마 변화와 레이아웃 설정의 자유로운 적용 등의 이유로 워드프레스를 점점 많이 사용하고 있다. 대중적으로 사용이 증가하다 보면 보안도 같이 이슈가 될 수밖에 없다. 콘텐츠 관리 플랫폼에서는 그 안에 담긴 콘텐츠가 곧 자산이기 때문이다. 플러그인을 통해 확장성을 강화하여 서비스하는 만큼 플러그인의 위협에 대해 개인이 스스로 보안을 해야 할 시점이다.

그림 워드프레스 플러그인 개수(3만 8천여 개)



오픈소스를 이용한 포괄적 지식 습득 가능

워드프레스는 엔진/모듈을 포함해서 플러그인까지 모두 소스 코드를 열람할 수 있다. 오픈소스이기 때문에 사용자가 직접 플러그인 개발에 참여할 수 있으며, 기능적인 개선 의견에 참여할 수도 있다. 따라서 APM(Apache, PHP, MySQL)의 환경을 토대로 학습하는 사람에게 매우 좋은 예제다. 게다가 개인 사용자가 선호하는 환경과 동일하기 때문에 웹에서 발생할 수 있는 취약점이 모두 존재한다. 웹에서 많이 발생하는 파일 업로드 취약점, SQL 인젝션(Injection) 등 시스템에 큰 영향을 줄 수 있는 취약점과 단순 정보 노출

까지 발생한다. 그렇기 때문에 워드프레스를 연구하다 보면 웹 애플리케이션 취약점 연구를 다양하고 재미있게 할 수 있다. 또한, 보안 이슈가 발생할 때 대처를 빨리 할 수 있어서 PHP 시큐어코딩을 학습할 때에는 좋은 본보기가 된다.

국내에 워드프레스 취약점 가이드 미흡

소개글에서 말했듯이 국내에도 워드프레스 사용자가 증가하고 있다. 국내에는 개인 사용자가 사용하는 경향이 높기 때문에 개인 사용자에게 적합한 보안 가이드가 필요하다. 하지만 국내에서는 워드프레스 취약점에 대한 보안 위협을 쉽게 생각하고 있다. 앞으로 공격 코드 하나로 개인정보를 대량 유출할 수 있는 위협이 점점 많아질 것이다. 따라서 사용자에게 공격 측면에서의 워드프레스 위협을 알리고 적합한 보안 가이드를 제시하고자 하였다.

이 책에서는 워드프레스 취약점 중에서 높은 비율을 차지하고 있는 공격 기법을 우선으로 설명하였다. 각 공격 기법을 최대한 이해하기 쉽게 설명하였고, 워드프레스 환경을 구축하여 직접 테스트할 수 있도록 하였다. 또한, 연구하면서 발견한 신규 취약점은 어떤 방식으로 접근하였는지 어떤 절차를 통해 등록할 수 있는지 설명하였다. 이 책을 통해 워드프레스 취약점과 웹 애플리케이션 취약점을 같이 이해할 수 있는 기회가 되길 바란다.

이 책의 구성

이 책은 모의해킹 분야에 관심이 있는 입문자를 대상으로 구성하였다.

1장은 워드프레스의 위협과 이 책에서 실습할 환경을 설명한다. 취약점 진단에 칼리리눅스Kali Linux를 활용하였다. 취약점 사례를 다루며 사용할 도구를 모두 포함하기 때문에 반드시 익히고 가길 바란다.

2장은 워드프레스 플러그인과 테마 등에서 발생할 수 있는 취약점 사례와 진단 방법을

설명한다. 웹 애플리케이션 주요 항목 기준으로 워드프레스 프레임워크에서 발생할 수 있는 위협을 살펴본다. 각 취약점의 원리를 설명하고 어떤 취약점을 통해 공격할 수 있는지 단계별로 실습을 통해 알아본다.

3장은 워드프레스 신규 취약점 분석 방법을 설명한다. 이미 알려져 배포된 취약점을 우회하여 발생할 수 있는 신규 취약점(Zero-day vulnerability) 경험을 공개한다. 신규 취약점을 벤더사에 보고하고 취약점 공격 코드 정보사이트인 Exploit-DB 사이트에 등록하는 절차도 자세히 설명한다.

4장은 워드프레스 사용자 보안 가이드를 제시한다. 주요 항목의 공격 기법을 습득한 뒤에는 이에 대응하는 방안을 습득하는 것이 필수다. 워드프레스를 설치하여 운영하는 사용자와 기업이 기본적으로 설정해야 할 보안과 플러그인, 모니터링 방법 등을 설명한다.

이 책의 특징

이 책은 워드프레스에서 발생할 수 있는 주요 공격 기법 및 대응 방안을 자세히 다루었다. 국내에 워드프레스 사용자가 증가하고 있음에도 이에 대해 표준화된 보안 가이드가 제시되고 있지 않다. 지금도 워드프레스로 구성된 수많은 홈페이지가 보안 위협에 노출되고 있다. 이 책은 보안 가이드뿐만 아니라 주요 항목을 직접 테스트할 수 있도록 공격 기법도 포함하고 있다. 공격 기법을 잘 이해하고 대응하는 것과 이해하지 못하고 대응하는 것은 큰 차이가 있기 때문이다. 또한, 취약점 진단 전문가를 꿈꾸고 있는 독자에게는 신규 취약점 분석 방법론을 이해할 좋은 기회가 될 것이다.

이 책의 대상 독자

이 책은 워드프레스 취약점을 바탕으로 웹 애플리케이션 취약점 분석 방법 및 대응 방안에 대해 다룬 책으로, 다음 독자에게 이 책을 추천한다.

- 모의해킹 컨설턴트 진로를 선택한 독자
- 웹 애플리케이션 취약점 분석에 대해 궁금한 독자
- 워드프레스 취약점 사례 및 분석에 대해 궁금한 독자

주의할 점

이 책에서는 독자의 로컬 PC에서 테스트할 수 있도록 환경 구성 부분까지 최대한 자세히 설명하고 있다. **이 도구를 이용하여 허용받지 않은 서비스 대상에 해킹을 시도하는 행위는 절대 금지**한다. 해킹을 시도할 때에 발생하는 법적인 책임은 이를 행한 사용자에게 있다는 것을 항상 명심하기 바란다.

한빛 리얼타임

한빛 리얼타임은 IT 개발자를 위한 eBook입니다.

요즘 IT 업계에는 하루가 멀다 하고 수많은 기술이 나타나고 사라져 갑니다. 인터넷을 아무리 뒤져도 조금이나마 정리된 정보를 찾기도 쉽지 않습니다. 또한, 잘 정리되어 책으로 나오기까지는 오랜 시간이 걸립니다. 어떻게 하면 조금이라도 더 유용한 정보를 빠르게 얻을 수 있을까요? 어떻게 하면 남보다 조금 더 빨리 경험하고 습득한 지식을 공유하고 발전시켜 나갈 수 있을까요? 세상에는 수많은 종이책이 있습니다. 그리고 그 종이책을 그대로 옮긴 전자책도 많습니다. 전자책에는 전자책에 적합한 콘텐츠와 전자책의 특성을 살린 형식이 있다고 생각합니다.

한빛이 지금 생각하고 추구하는, 개발자를 위한 리얼타임 전자책은 이렇습니다.

1 eBook First – 빠르게 변화하는 IT 기술에 대해 핵심적인 정보를 신속하게 제공합니다

500페이지 가까운 분량의 잘 정리된 도서(종이책)가 아니라, 핵심적인 내용을 빠르게 전달하기 위해 조금은 거칠지만 100페이지 내외의 전자책 전용으로 개발한 서비스입니다. 독자에게는 새로운 정보를 빨리 얻을 기회가 되고, 자신이 먼저 경험한 지식과 정보를 책으로 펴내고 싶지만 너무 바빠서 엄두를 못 내는 선배, 전문가, 고수 분에게는 좀 더 쉽게 집필할 수 있는 기회가 될 수 있으리라 생각합니다. 또한, 새로운 정보와 지식을 빠르게 전달하기 위해 O'Reilly의 전자책 번역 서비스도 하고 있습니다.

2 무료로 업데이트되는 전자책 전용 서비스입니다

종이책으로는 기술의 변화 속도를 따라잡기가 쉽지 않습니다. 책이 일정 분량 이상으로 집필되고 정리되어 나오는 동안 기술은 이미 변해 있습니다. 전자책으로 출간된 이후에도 버전 업을 통해 중요한 기술적 변화가 있거나 저자(역자)와 독자가 소통하면서 보완하여 발전된 노하우가 정리되면 구매하신 분께 무료로 업데이트해 드립니다.

3 독자의 편의를 위해 DRM-Free로 제공합니다

구매한 전자책을 다양한 IT 기기에서 자유롭게 활용할 수 있도록 DRM-Free PDF 포맷으로 제공합니다. 이는 독자 여러분과 한빛이 생각하고 추구하는 전자책을 만들어 나가기 위해 독자 여러분이 언제 어디서 어떤 기기를 사용하더라도 편리하게 전자책을 볼 수 있도록 하기 위함입니다.

4 전자책 환경을 고려한 최적의 형태와 디자인에 담고자 노력했습니다

종이책을 그대로 옮겨 놓아 가독성이 떨어지고 읽기 어려운 전자책이 아니라, 전자책의 환경에 가능한 한 최적화하여 쾌적한 경험을 드리고자 합니다. 링크 등의 기능을 적극적으로 이용할 수 있음은 물론이고 글자 크기나 행간, 여백 등을 전자책에 가장 최적화된 형태로 새롭게 디자인하였습니다.

앞으로도 독자 여러분의 충고에 귀 기울이며 지속해서 발전시켜 나가도록 하겠습니다.

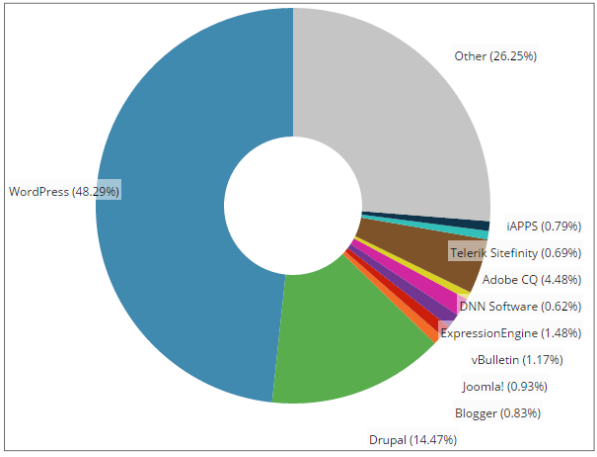
차례

chapter 1

워드프레스에 대해서

워드프레스는 PHP 기반의 공개 블로그 서비스다. 최근에 워드프레스 관련 도서가 많이 출간되는 것으로 보아, 이제는 국내 일반 사용자도 많이 사용하는 대표적인 오픈소스 CMS 플랫폼이라 할 수 있다. CMS는 'Content Management System'의 약자로 블로그와 이력 관리시스템 등에 활용한다. 대부분 공개되어 있는 플랫폼이어서 취약점에 대한 정기적인 진단이 필수로 이루어져야 한다.

그림 1-1 전 세계 CMS 사용 비율[01]



CMS 서비스를 사용하는 웹 사이트의 50% 가까이가 워드프레스를 사용하고 있다. 국내에서도 블로터[02]를 비롯하여 많은 개인 사용자와 기업에서 워드프레스를

01 출처: http://trends.builtwith.com/cms

02 http://www.bloter.net

사용하고 있다. 웹 호스팅 업체에서도 서비스를 원하는 사용자에게 워드프레스를 기본으로 설치하여 제공한다. 또한, 워드프레스를 국내 상황에 맞게 차별화한 플러그인과 테마를 적용하여 몇십만 원에 제공한다. 홈페이지 제작 비용에 비해 매우 저렴하게 때문에 워드프레스를 조금만 활용할 줄 안다면 개인 사업자에게 매우 좋은 서비스다.

그림 1-2 워드프레스 사용 예-블로터

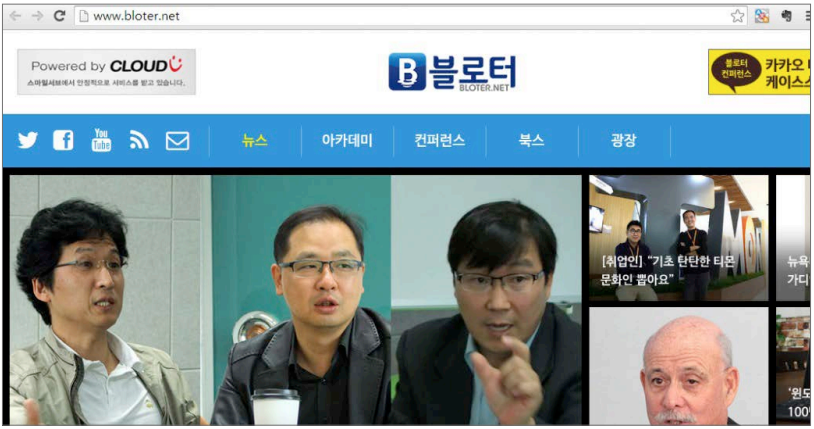
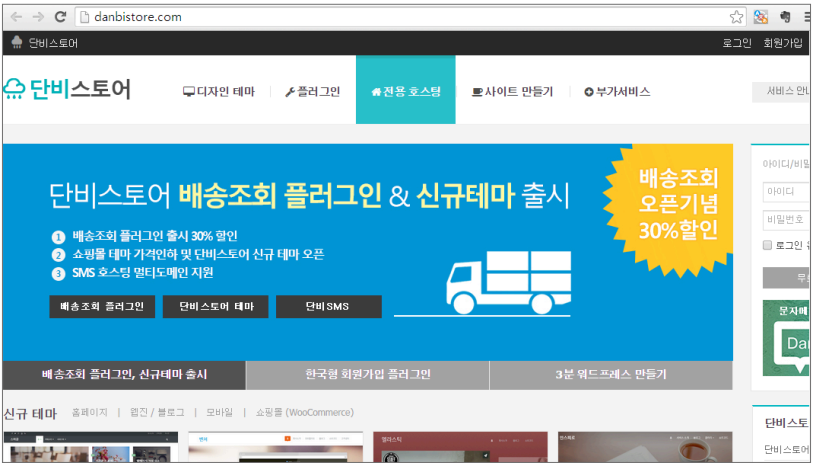


그림 1-3 워드프레스 사용 예-단비 스토어



워드프레스에는 수만 개의 무료 플러그인이 있다(2013년을 기준으로 25,700개, 4억 7천 5백만 번 다운로드함). 유료 테마와 플러그인도 존재하지만 무료만 잘 활용해도 자신이 원하는 페이지를 제작하는 데 무리가 없다.

자유롭게 수정할 수 있고 유연하게 사용할 수 있는 프레임워크지만, 소스가 공개되어 있기 때문에 하나의 취약점이 많은 서비스에 타격을 줄 수 있다. 악성코드가 업로드되는 공격(웹쉘 공격)에 노출된다면 중요한 정보가 노출되거나 서비스가 장애가 발생할 소지가 있기 때문에 워드프레스에 관심이 많아지는 만큼 워드프레스 보안에도 관심을 가져야 한다.

1.1 최신 취약점 미패치의 위협

웹 서비스가 공격을 당해 침투되는 것은 모두 '최신 취약점 미패치'부터 시작된다. 서비스에 다양한 플랫폼과 프로그래밍을 하였는데 이를 신속하게 패치하지 않으면 위협이 발생한다는 뜻이다. 외부에 노출된 서버군, WAS 등은 심각한 취약점 패치를 하나라도 하지 않는다면 공격 코드 한두 개로 인해서 시스템까지 바로 침투당할 가능성이 크다.

워드프레스 플러그인 취약점으로 인해서 피해가 발생한 경우도 많다. 기사(Slimstat 플러그인 취약점으로 인해서 130만사이트가 취약[03])를 보더라도 빠른 취약점 패치가 이루어지지 않는다면 사이트뿐만 아니라 해당 사이트에 접근하는 사용자 PC에 악성코드 감염 등의 큰 위협을 초래할 수 있다고 한다.

최근(2015년 4월 27일)에 발생한 크로스 사이트 스크립팅 취약점[04]도 최신 업데이트가 되지 않았다면 모두 공격대상에 포함된다.

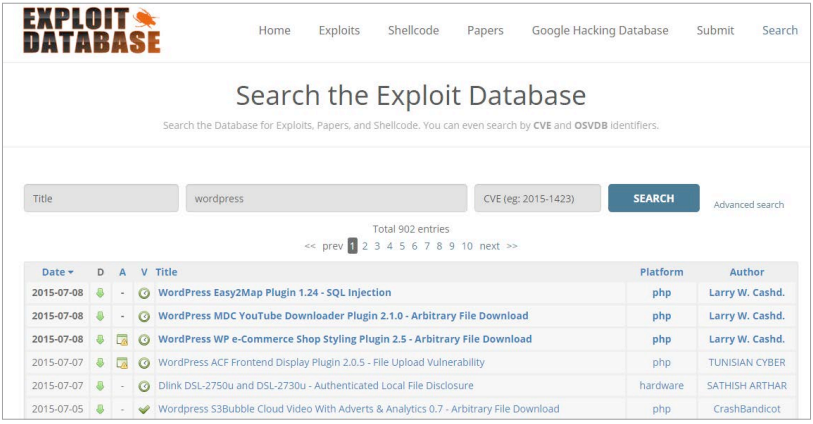
---

03 http://goo.gl/nCcYo4

04 http://goo.gl/gOUd1F

그렇다면 이런 취약점을 모니터링하기 위한 방법은 어떤 것이 있을까? 신규 취약점을 검색하기 위해서 많이 참고하는 사이트가 있다. 그중에서 신규 정보와 공격 코드를 같이 확인할 수 있는 것은 트위터와 페이스북 등의 소셜 네트워크 서비스에서 공유된 정보를 통해서다. 공격 코드는 대표적으로 Exploit-DB[05]에서 확인할 수 있다. 이 사이트에서 'wordpress'로 검색하면 [그림 1-4]와 같은 결과가 나온다. 결과를 확인해 보면 대부분 플러그인과 관련된 취약점이다. 매월 발표되는 개수가 증가하고 있으며 여기에 등록되지 않는 영향도가 낮은 취약점까지 포함하면 그 증가율은 더욱 높다. 이 책에서도 워드프레스의 플러그인을 대상으로 취약점 진단 방법을 설명하겠다.

그림 1-4 Exploit-DB에서 'wordpress' 검색 결과[06]



[그림 1-5]는 워드프레스에 많이 사용하는 플러그인의 다운로드 횟수와 취약점을 나타낸 자료다(플러그인의 이름은 악의적인 목적으로 이용될 수 있어 공개하지 않았다). 많은 사용자가 취약점이 있는 플러그인을 다운로드하여 사용하고 있는데, 이는 사용자가 플러그인 업데이트를 정기적으로 관리하지 않는다면 악성코드 배포 사이트로 이용될 수 있음을 의미한다.

05 http://www.exploit-db.com
06 https://goo.gl/emTQVC

그림 1-5 유명 플러그인을 대상으로 한 취약점 결과[07]

Plugin	LOC	# Downloads	SQLi	XSS	CSRF	PT
[redacted] Lists related entries	4,682	2,093,718	■			
[redacted] Tests the site for broken links and missing images	20,636	1,493,609			■	
[redacted] Add links to Facebook	8,857	1,029,626		■		
[redacted] A review system for comments	26,326	1,002,808	■	■	■	
[redacted] An RSS aggregator	15,481	622,894	■	■		
[redacted] Site backup	247,816	464,212		■		■
[redacted] Embeds Flash and HTML5 video	13,676	380,551		■		■
[redacted] Saves contact from data	22,591	372,150	■	■	■	
[redacted] An alternative WordPress editor	11,395	263,171		■		■
[redacted] Management of site statistics	3,593	152,467	■	■	■	■
[redacted] Transforms WordPress sites to mobile apps	3,820	84,863		■		

이외에도 취약점 정보를 획득하는 사이트는 다음과 같다. 취약점 정보의 데이터베이스를 활용하여 만든 도구를 보면 대부분 다음의 사이트를 참고하고 있다.

- ScipvulDB: http://www.scip.ch/en/?vuldb
- CVE: http://cve.mitre.org
- OsvDB: http://www.osvdb.org (outdated, 02/03/2011)
- SecurityFocus: http://www.securityfocus.com/bid/
- SecurityTracker: http://www.securitytracker.com

1.2 워드프레스 취약점 데이터베이스

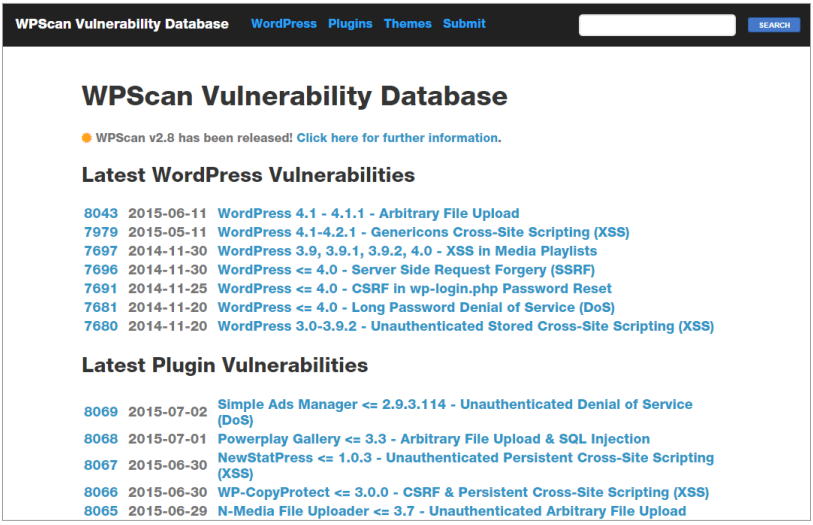
워드프레스는 전세계 CMS 사용 사이트 중 가장 많이 이용하고 있다. 국내 개인 사용자도 워드프레스 사용이 점차 증가하고 있으며, 기업에서도 워드프레스와 그 테마 및 플러그인을 활용하여 사이트를 바꿔 나가는 것을 볼 수 있다.

07 출처: http://securityaffairs.co/wordpress/15638/security/the-security-state-of-wordpress-top-50-plugins.html

워드프레스로 만든 사이트에서 플러그인을 기본으로 5개 이상, 많게는 10개 이상을 사용하는데, 문제는 이 플러그인 취약점에 대한 관리가 되고 있지 않다는 점이다. 사용자가 매번 관심을 가지고 플러그인을 최신 업데이트해야 하는데 일반 사용자가 이것을 수행하는 것은 당연히 어려울 수밖에 없다. 그러나 워드프레스 취약점을 통해서 시스템에 침투할 수 있고 악성코드 배포까지 가능하기 때문에 워드프레스를 사용하는 기업이나 사용자는 반드시 자신이 사용하는 플러그인 및 워드프레스 버전 취약점을 모니터링해야 한다.

워드프레스 취약점 스캔으로 가장 유명한 것은 WPScan이다. WPScan은 오픈소스로, 칼리리눅스Kali Linux에 기본으로 포함되어 있다. 프로그램은 WPScan의 공식 홈페이지[08]에서 다운로드할 수 있다. 이 WPScan에서 사용하는 데이터베이스를 이용해서 내부적으로 패치관리 이력을 만들어 보는 것도 좋다. 이 데이터베이스를 한곳에 모아 둔 서비스 페이지[09]가 이번에 공개되었다.

그림 1-6 WPScan의 워드프레스 취약점 목록

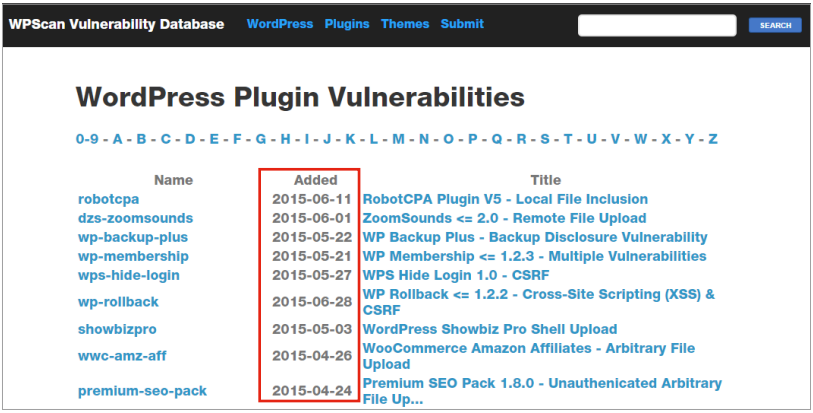


08 http://wpscan.org/

09 https://wpvulndb.com/

이중에서 플러그인 취약점은 하루가 멀다 하고 발표되고 있다. 발표된 것만 이 정도며 발표되지 않은 상태에서 사용되고 있는 취약점은 더 많다. 일반 사용자는 버전 관리도 힘들고 최신 패치를 모니터링하는 것도 어렵기 때문에 플러그인 취약점에 대한 보안 위협이 매우 크다고 할 수 있다.

그림 1-7 워드프레스 플러그인 취약점 목록[10]



1.3 워드프레스 진단 환경 설정

1.3.1 칼리리눅스 도구 설치 및 사용법

칼리리눅스는 모의해킹 진단을 포함하여 포렌식, 무선 네트워크 진단, 프로그램 개발 등에서 다양하게 활용할 수 있는 도구의 모음이다. 이 책은 칼리리눅스 매뉴얼이 아니므로 칼리리눅스에 대한 설명은 생략하겠다. 칼리리눅스에 대해 더 자세히 알고 싶다면 『칼리 리눅스와 백트랙을 활용한 모의 해킹』(에이콘출판사, 2014)를 추천한다.

10 참고자료: http://threatpost.com/wpscan-vulnerability-database-a-new-wordpress-security-resource/108607

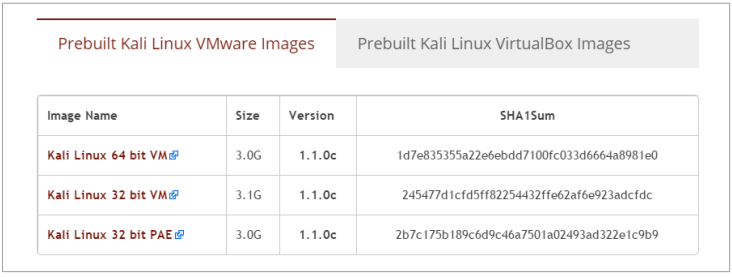
칼리리눅스 설치

칼리리눅스 환경을 구성하기 위해서 몇 가지 프로그램을 설치해야 한다. 진단을 위해 로컬 PC에 라이브 시디를 바로 설치하는 경우는 거의 없고, 가상 머신에 이미지를 설치하거나 가상 이미지 파일을 다운로드하여 압축을 푼 뒤 불러와 진단한다. 이 책에서는 VMware 워크스테이션(평가판)에 환경을 구성한다. 우선 VMware 홈페이지[11]에서 무료 평가판을 다운로드하여 설치한다. 설치 과정은 다음 버튼만 누르면 되므로 생략하겠다.

그림 1-8 VMware 워크스테이션 다운로드

두 번째는 칼리리눅스 이미지인데, ISO 이미지 파일을 다운로드하여 직접 설치해도 되지만 이 책에서는 https://www.offensive-security.com/kali-linux-vmware-arm-image-download/에서 VMware 이미지 파일을 다운로드하여 설치하겠다.

그림 1-9 칼리리눅스 다운로드



11 http://www.vmware.com/kr/products/workstation

다운로드한 압축 파일을 적당한 곳에 풀고, VMware 워크스테이션을 실행한 후 [그림 1-10]과 같이 [File → Open ...]을 선택하여 압축 해제한 파일을 불러온다.

그림 1-10 WMware 워크스테이션에서 불러오기

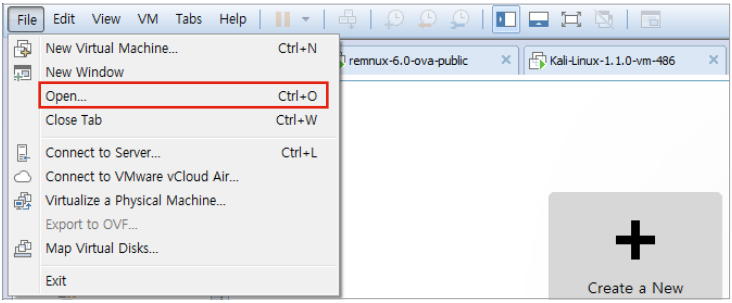
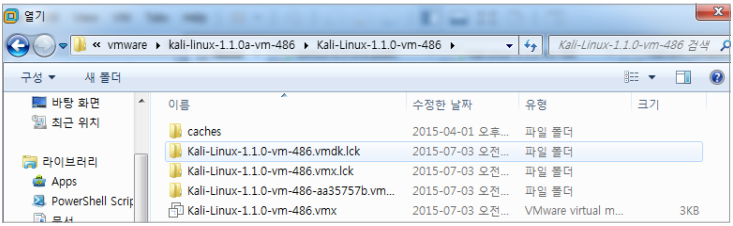


그림 1-11 칼리리눅스 이미지 선택



이미지를 불러오면 실행이 되면서 [그림 1-12]와 같은 화면이 나온다. 첫 번째 모드를 선택하고 계정 입력 화면에서 기본 계정이름은 'root', 패스워드는 'toor'을 입력하면 칼리리눅스가 실행된다.

그림 1-12 칼리리눅스 실행하기

WPScan 설치

워드프레스 진단에서 가장 많이 사용하는 도구는 WPScan[12]이다. WPScan은 워드프레스 최신 취약점 미패치, 플러그인, 테마 취약점 미패치를 데이터베이스화하여 보여 주는 도구로, 루비 언어로 되어 있어서 루비 환경이 구성되어 있다면 어디에서든 활용할 수 있다. [그림 1-13]과 같이 WPScan 공식 홈페이지 왼쪽 상단에서 소스 코드를 다운로드하여 실행한다.

그림 1-13 WPScan 다운로드

다음은 우분투 환경에서 WPScan을 설치하는 명령이다(윈도우 환경은 다양한 라이브러리를 구성하기 힘들어서 이 책에서는 제외하였다).

```
sudo apt-get install libcurl4-gnutls-dev libxml2 libxml2-dev libxslt1-dev
ruby-dev build-essential
git clone https://github.com/wpscanteam/wpscan.git
cd wpscan
sudo gem install bundler && bundle install —without test
```

칼리리눅스Kali Linux, 백박스 BackBox, 펜투Pentoo 등 모의해킹 진단 전용 라이브 시디에는 WPScan이 기본으로 설치되어 있다. 이 책에서 다루는 칼리리눅스에서도 [그림 1-14]의 메뉴에서 [Web Applications → CMS Identification → wpscan]을 선택하면 실행된다.

12 http://wpscan.org

그림 1-14 칼리리눅스 기반 WPScan

WPScan을 실행하기 전에 업데이트하길 추천한다. 엔진뿐만 아니라 플러그인과 테마 취약점이 포함된 시그니처 데이터베이스까지 업데이트해야 진단할 때 정확한 취약점 정보를 얻을 수 있다. 업데이트할 때 [그림 1-15]와 같은 오류가 발생하면 `apt-get install` 명령으로 WPScan을 업데이트한다.

그림 1-15 WPScan 업데이트 시 오류 발생

```
root@kali:~# wpscan --update
_____________________________________________________________

        __          _______     _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version v2.4.1
    Sponsored by the RandomStorm Open Source Initiative
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_____________________________________________________________

[i] Svn / Git not installed, or wpscan has not been installed with one of them.
[!] Update aborted
root@kali:~# apt-get install wpscan
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
```

정상적으로 업데이트가 완료되면 콘솔에서 wpscan 명령어로 간단하게 WPScan이 실행된다. WPScan으로 진단할 때는 [그림 1-16]과 같이 명령어를 입력한다. /wordpress는 /var/www/ 이하 디렉터리에 홈페이지 최상위 디렉터리명이다.

그림 1-16 WPScan 진단 실행

```
root@kali:~# wpscan --url http://192.168.10.137/wordpress
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.5.1
    Sponsored by the RandomStorm Open Source Initiative
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[+] URL: http://192.168.10.137/wordpress/
```

진단 서비스에 취약한 플러그인이 존재한다면 [그림 1-17]과 같이 버전 정보 및 취약한 정보 목록이 같이 출력된다. 여기서 OSVDB, Exploit-DB, WPScan Vulnerability Database 등은 취약 버전 정보를 검색할 때 많이 사용하는 서비스다.

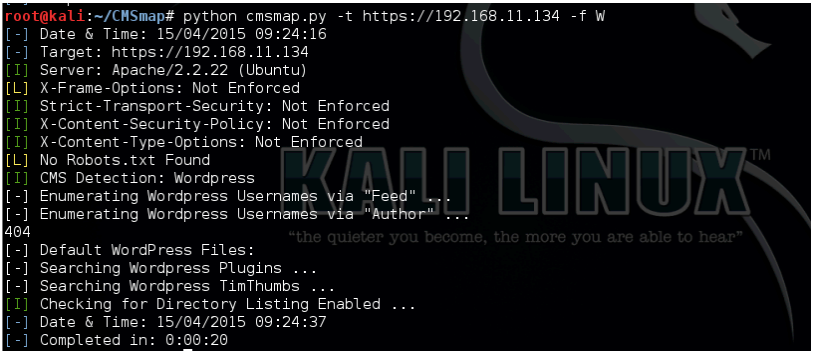
그림 1-17 취약한 플러그인 정보

```
[+] Name: like-dislike-counter-for-posts-pages-and-comments - v1.2.3
 |  Location: http://192.168.10.137/wordpress/wp-content/plugins/like-dislike-co
unter-for-posts-pages-and-comments/
 |  Readme: http://192.168.10.137/wordpress/wp-content/plugins/like-dislike-coun
ter-for-posts-pages-and-comments/readme.txt

[+] Name: paid-business-listings - v1.0.3
 |  Location: http://192.168.10.137/wordpress/wp-content/plugins/paid-business-l
istings/
 |  Readme: http://192.168.10.137/wordpress/wp-content/plugins/paid-business-lis
tings/readme.txt

[!] Title: Paid Business Listings 1.0.2 - Form Submission pbl_listing_pkg_id Par
ameter SQL Injection
    Reference: https://wpvulndb.com/vulnerabilities/6164
    Reference: http://osvdb.org/83768
    Reference: http://www.exploit-db.com/exploits/19481/

[+] Name: rocket-responsive-gallery - v1.0
 |  Location: http://192.168.10.137/wordpress/wp-content/plugins/rocket-responsi
ve-gallery/
```

WPScan은 기본으로 4만여 개(2.5.1 버전 기준)의 워드프레스 플러그인 목록을 가지고 있다. 칼리리눅스에는 /usr/share/wpscan/data/plugins_full.txt 파일에 포함되어 있다. 이 목록에 없다면 직접 추가해서 진단하면 취약한 서비스의 플러그인을 확인할 수 있다.

WPScan과 비슷한 기능을 가지고 있으면서 다른 CMS의 취약점 진단 항목까지 포함한 CMSmap[13]이라는 도구도 있다.

그림 1-18 CMSmap으로 진단한 결과



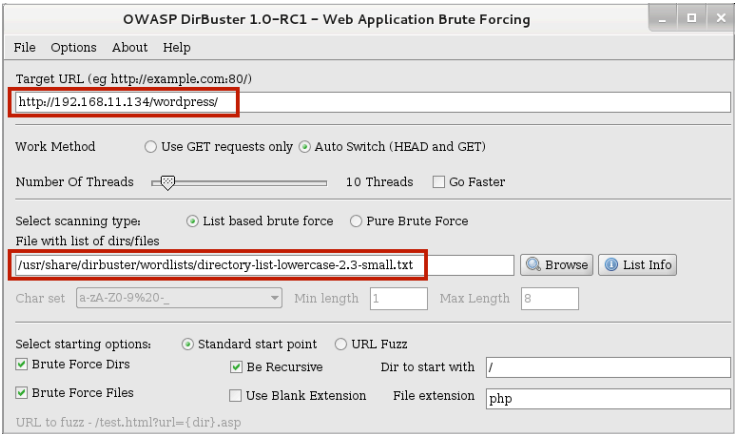
워드프레스 플러그인 목록 힌트 얻기

2.4 디렉터리 리스팅 취약점에서 상세히 다룰 도구를 이 절에서 잠깐 활용하겠다. 워드프레스 플러그인 목록은 배포된 플러그인에 비해 많이 부족하다. 플러그인 목록을 알고 있다면 등록하여 WPScan으로 검색하면 버전 정보를 확인할 수 있지만 등록이 안 된 플러그인은 검색되지 않아 그냥 지나칠 수 있다. 이때는 디렉터리를 검색하는 자동 도구를 활용하여 조금이나마 힌트를 얻을 수 있다.

칼리리눅스에서 dirbuster 명령어를 입력하면 [그림 1-19]의 초기 설정 창이 나온다. [Target URL] 항목에 워드프레스가 설치된 서버 주소를 입력하고, [File with list of dirs/files]에서 다음과 같은 리스트 파일 중 하나를 선택한다.

13 https://github.com/Dionach/CMSmap

그림 1-19 dirbuster를 활용한 디렉터리 구조 파악



파일 이름을 보면 알 수 있듯이 패턴 형태가 어떤 종류로 반영되었느냐에 따라 구분된다. directory-list-2.3-medium.txt 파일이 가장 많은 패턴이 포함되어 있지만, 이 책에서는 directory-list-2.3-small.txt를 선택하겠다.

```
/usr/share/dirbuster/wordlists/directory-list-1.0.txt
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
/usr/share/dirbuster/wordlists/directory-list-2.3-small.txt
/usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt
/usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt
```

스캔을 진행하면 잠시 후에 검색된 디렉터리와 파일 정보가 나타난다. 결과를 확인하면 접근할 수 있는 디렉터리 중 플러그인과 관련된 내용이 보인다.

그림 1-20 dirbuster를 활용한 디렉터리 구조 파악 중 플러그인 정보 획득