

비박스 환경을 활용한 웹 모의해킹 완벽 실습

보안프로젝트 조정원, 이승준, 김영선, 최일선, 이선경, 이해인 지음





보안프로젝트 조정원, 이승준, 김영선, 최일선, 이선경, 이해인 지음

비박스 환경을 활용한 웹 모의해킹 완벽 실습





표지 사진 **김은진** 이 책의 표지는 김은진님이 보내 주신 풍경사진을 담았습니다. 리얼타임은 독자의 시선을 담은 풍경사진을 책 표지로 보여주고자 합니다. 사진 보내기 ebookwriter@hanbit.co.kr

비박스 환경을 활용한 웹 모의해킹 완벽 실습

초판발행 2016년 9월 9일

지은이 조정원, 이승준, 김영선, 최일선, 이선경, 이해인 / 펴낸이 김태현 펴낸곳 한빛미디어(주) / 주소 서울시 마포구 양화로7길 83 한빛미디어(주) IT출판부 전화 02-325-5544 / 팩스 02-336-7124 등록 1999년 6월 24일 제10-1779호 ISBN 978-89-6848-841-2 95000 / 정가 18,000원

총괄 전태호 / 책임편집 김창수 / 기획·편집 정지연 디자인 표지 강은영 내지 여동일, 조판 최송실 마케팅 박상용, 송경석, 변지영 / 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 Copyright © 2016 조정원, 이승준, 김영선, 최일선, 이선경, 이해인 & HANBIT Media, Inc. 이 책의 저작권은 조정원, 이승준, 김영선, 최일선, 이선경, 이해인과 한빛미디어(주)에 있습니다. 저작권법에 의해 보호를 받는 저작물이므로 무단 복제 및 무단 전재를 금합니다.

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. 지은이_ 조정원(chogar@naver.com)

KB투자증권에서 보안 업무를 담당하며, 보안프로젝트(www.boanproject.com) 운영 자로 활동하고 있다. 에이쓰리시큐리티에서 5년 동안 모의해킹 컨설턴트를 하였고, 모 의해킹 프로젝트 매니저, 웹 애플리케이션, 소스 코드 진단 등 다양한 영역에서 취약점 진단을 수행하였다. 이후 KTH 보안팀에서 모바일 서비스, 클라우드 서비스 보안, 침 해사고 대응업무를 하였다.

주요 저서로는 『버프스위트 활용과 웹 모의해킹』 『워드프레스 플러그인 취약점 분석 과 모의해킹』(이상 한빛미디어, 2015), 『IT엔지니어의 투잡, 책내기』 『IT엔지니어로 사 는 법 1』(이상 비팬북스, 2015), 『안드로이드 모바일 악성코드와 모의해킹 진단』 『칼리 리눅스를 활용한 모의해킹』(이상 에이콘출판사, 2014), 『모의해킹이란 무엇인가』(위키북 스, 2014), 『디지털 포렌식의 세계』(인포더북스, 2014), 『크래커 잡는 명탐정 해커』(성안 당, 2010) 등이 있으며, 보안프로젝트 멤버들과 함께 다양한 영역에서 활동하고 있다.

지은이_ 이승준

NSHC 싱가포르 지사 소속으로 국내외 보안 트레이닝을 총괄하며, 보안프로젝트에서 활동하고 있다. 미국에서 컴퓨터공학을 공부하다 배울 만한 수업 내용이 없어 3학년을 마친 후 자퇴하고 프리랜서로 3년 동안 소프트웨어 개발을 하였다. 개발하면서 보안에 관심이 많아 침투 테스트 관련 연구 및 공부를 하고 4년 동안 모의해킹 컨설팅을 하였 다. 이후 국내에서 트레이닝하며 홍콩 경찰청을 시작으로 이란 경찰청, 르완다, 콜롬비 아, 싱가포르 등 여러 나라에서 침투 테스트, 악성코드 분석, 침해대응, 스카다 등에 대 한 보안 트레이닝을 하고 있다. 보안 외에도 인공지능, 게임 개발에도 관심이 많아 연 구와 공부를 병행하고 있다.

지은이_ 김영선

서울여자대학교에서 정보보안과 멀티미디어를 전공하였으며 NXT 개발 및 비컨^{Beacon} 을 이용한 IoT 앱 개발 프로젝트 등을 진행하였다. 보안에 관심이 많아 보안에 대한 특강을 접한 것을 시작으로 보안프로젝트 멤버로 활동하고 있다. 오픈소스 도구 분석 및 웹 취약점 진단에 대한 연구를 하였으며, 최근 모의해킹에 대해 공부하고 있다. 현 재는 NSHC 보안교육팀 소속 연구원으로 콘텐츠 개발 및 트레이너로 활동 중이다.

지은이_ 최일선

비전공자로 뒤늦게 IT 공부를 시작하였으며 현재 보안프로젝트 연구원으로 활동 중이 다. 윈도우 플랫폼 악성코드 취약점 진단 온·오프라인 장기 과정을 맡고 있다. 윈도우 애플리케이션 취약점, 악성코드 분석을 위한 메모리 포렌식 등 전문 강의를 맡고 있다. 보안뿐 아니라 프로그래밍, 데이터 과학, 알고리즘, IoT 등에도 관심이 많다.

지은이_ 이선경

정보보호학을 전공하였으며, 현재 보안프로젝트 멤버로 활동 중이다. 모의 환경에 서 OWASP Top 10을 기준으로 웹 취약점 진단을 공부하였으며 하둡을 이용한 SIEM^{Security Identity and Event Management} 파일럿 제작 프로젝트에도 참여하였다. IoT 환경 에서 발생 가능한 보안 사고에 대한 대비책을 연구 목적으로 삼고 있으며 파이썬을 활 용한 취약점 진단 도구 제작과 머신러닝에도 관심이 많다. 지은이_ **이해인**

서울여자대학교에서 정보보호를 전공하였다. 보안프로젝트 오프라인 스터디 멤버로 1년간 활동하면서 웹 애플리케이션 취약점 진단, 윈도우 악성코드 분석, 네트워크 해 킹 방어 등 다양한 프로젝트를 수행하였다. 현재는 ICS/SCADA 해킹과 램넉스 도구 분석에 관심이 있어 이를 연구 중이다. 웹 애플리케이션 취약점은 나날이 증가하고 있다. 모바일 기기를 사용하더라도 연결 은 웹을 통한다. 웹과 통신하는 방식은 달라지지 않으니 외부에 노출되는 서버가 오히 려 많아지고 있다. 여전히 모의해킹 실무에서 웹 애플리케이션 취약점을 진단하는 프 로젝트가 대부분인 것도 이 때문이다. 웹 애플리케이션 취약점은 앞으로도 줄어들지 않을 것이다. 웹 환경은 더 다양해질 것이므로 웹에 대한 보안이 더 중요해질 것이다.

또한, 웹 서비스를 구성하는 데 사용하는 모듈과 라이브러리들도 다양해지고 오픈소 스 플랫폼의 사용도 증가하고 있다. 이 서비스들이 보안 관리가 잘되면 좋겠지만, 보안 을 담당하는 인력에 제한이 있고 솔루션으로 방어하는 데도 한계가 있다. 이 책에서 강 조하는 시큐어 코딩뿐만 아니라 서버 보안 설정, 보안 프로세스 강화까지 많은 것을 고 려해야 한다.

보안 교육은 책이나 강의를 통하여 꾸준히 진행되고 있지만, 실습 환경이 단일화되어 있지 않고 책 한 권에서도 여러 환경을 설치하는 경우가 많다. 그래서 한 환경에서 다 양한 공격기법을 실습하고 대응방안을 고려할 수 없을까 고민하다가 비박스^{bee-box}를 선택하게 되었다.

비박스는 최신 시스템 공격 기법을 포함하고 있으며 항목별로 난이도가 조정되어 단 계별로 실습해 나가면서 웹 애플리케이션 취약점의 공격 기법을 이해할 수 있다. 이 책 에서 모든 항목을 다루지는 못하지만, 주요 항목에 대한 실습 가이드를 제시하므로 나 머지는 공부하면서 스스로 해결해 보자. 대상 독자

이 책은 모의해킹 업무 및 웹 애플리케이션 취약점에 대한 궁금증이 있는 입문자부터 실무자까지를 대상으로 쓴 책으로, 다음과 같은 독자에게 이 책을 추천한다.

- 웹 애플리케이션 취약점을 포함한 최신 공격 기법 실습
- 실습 환경에 맞춰 다양한 공격 기법 사례 및 대응방안 제시
- 공격을 진행하기 위한 도구(버프스위트, 메타스플로잇 등)의 활용 방법 제시

주의할 점

이 책은 모의해킹 진단에 입문하는 독자도 대상으로 하고 있어서 로컬 PC에서 테스트 할 수 있는 환경을 구성하는 부분까지 자세히 설명하고 있다. 이 책에 사용한 도구로 허용받지 않은 서비스 대상에 해킹을 시도하는 행위는 절대 금지한다. 해킹을 시도할 때 발생하는 법적인 책임은 이를 행한 사용자에게 있다는 것을 항상 명심하기 바란다.



chapter **1 개요** _____ 017 1.1 비박스란 _____ 017 1.2 취약점 분류 _____ 018

1.3 점검 환경 구성 ----- 023

Part 1 A1 - 인젝션 ---- 039

 chapter 2
 HTML 인젝션 — 041

 2.1
 반사(GET) _ 042

 2.2
 반사(POST) _ 048

 2.3
 저장(Blog) _ 054

 chapter 3
 기타 인젝션 공격 _ 059

 3.1
 iframe 인젝션 _ 059

 3.2
 OS 커맨드 인젝션 _ 068

 3.3
 PHP 코드 인젝션 _ 072

 3.4
 SSI 인젝션 _ 084

- 4.1 GET/Search _____ 084
- 4.2 POST/Search _____ 095
- 4.3 GET/Select _____ 104
- 4.4 POST/Select ----- 108

- 4.5 AJAX/JSON/jQuery _____ 120
- 4.6 Login Form/Hero _____ 126
- 4.7 저장(Blog) ----- 129

chapter 5	Blind SQL 인젝션 —— 13		- 133	
	5.1	Boolean Based —		— 134
	5.2	Time Based —		142
	5.3	웹 서비스/SOAP —		— 150
chapter 6	XML	_/Xpath 인젝션 —	161	

- 6.1 Login Form 162
- 6.2 Search 171

Part 2 A2 - 인증 결함과 세션 관리 ---- 177

chapter **7** 인증 결함 — 179

- 7.1 안전하지 않은 로그인 형식 _____ 179
- 7.2 비밀번호 무차별 대입 공격 _____ 185
- 7.3 비밀번호 사전 대입 공격 _____ 189

chapter **8 세션 관리** — 195

8.1 관리자 페이지 접근 _____ 195

8.2 URL 주소 조작을 통한 세션 우회 _____ 199

Part 3 A3 - 크로스 사이트 스크립팅 ---- 203

chapter 9 저장된 XSS 취약점 _____ 205

- 9.1 Blog 206
- 9.2 Change Secret _____ 209
- 9.3 User-Agent ----- 214

chapter 10 반사된 XSS 취약점 ----- 219

- 10.1 GET 219
- 10.2 POST _____ 222
- 10.3 JSON _____ 229
- 10.4 AJAX/JSON _____ 231
- 10.5 eval 238
- 10.6 HREF _____ 240
- 10.7 phpMyAdmin _____ 245
- 10.8 PHP_SELF _____ 249

Part 4 A4 - 취약한 직접 객체 참조 ---- 255

chapter 11 중요 정보 변경 ----- 257

11.1 난이도 하 _____ 257

11.2 대응방안 _____ 258

chapter 12 중요 정보 초기화 ----- 260

12.1 난이도 하 _____ 260

12.2 대응방안 _____ 263

chapter **13 상품 주문 가격 조작** <u>265</u> 13.1 난이도 하 <u>265</u>

13.2	대응빙	안	266

Part 5 A5 - 보안 설정 오류 ____ 267

chapter 14 Robots 파일 내 중요한 정보 노출 ----- 269

14.1 난이도 하 _____ 269

chapter 15 안전하지 않은 WebDAV 설정 ----- 273

15.1 난이도 하 _____ 273

15.2 대응방안 _____ 277

Part 6 A6 - 민감 데이터 노출 ---- 279

chapter 16 Base64 인코딩 복호화 281 16.1 난이도 하 281 16.2 대응방안 283

chapter 17 HTTP 페이지 내 평문 데이터 — 284

17.1 난이도 하	284
17.2 대응방안	291

chapter 18 HTML5 웹 저장소 _____ 292

18.1 난이도 하 ——	292
18.2 대응방안	295

chapter 19 중요 정보 텍스트 파일 저장 ----- 296

19.1 난이도 하	296
19.2 난이도 중	298
19.3 대응방안	299

 chapter 20 하트블리드 취약점
 301

 20.1 난이도 하
 301

 20.2 대응방안
 306

Part 7 A7 - 기능 수준의 접근 통제 누락 ---- 307

chapter 21	디렉터리	리스팅	취약점	309
------------	------	-----	-----	-----

21.1 디렉터리	- 309
-----------	-------

21.2 파일 312	312
-------------	-----

chapter **22 파일삽입** 316 22.1 난이도 하 316

		-	
22.2	대응병	방안	320

chapter 23 디바이스 접근 제한 ----- 322

23.1	난이도 하	322

23.2 대응방안 _____ 326

chapter 24 서버 측 요청 변조 ----- 327

24.1 난이도 하	327
24.2 대응방안	334

Part 8 A8 - 크로스 사이트 요청 변조 ---- 335

- chapter 25 XML 외부 엔티티 공격 ------ 337
 - 25.1 난이도 하 _____ 337
 - 25.2 대응방안 ----- **341**

chapter **26 비밀번호 변경 ----- 343** 26.1 난이도 하 ------ **343**

26.2 대응방안	345
2012 1002	• • •

chapter 27 비밀번호 힌트 변경 ----- 347

27.1 난이도 하 ——	347
27.2 대응방안	349

chapter 28 계좌 이체 ----- 352

28.1 난이도 하	352
28.2 대응방안	354

Part 9 A9 - 알려진 취약점이 있는 컴포넌트 사용 ---- 357

chapter 29 PHP CGI 원격 실행 공격 ----- 359

29.1 난이도 하 _____ 359

chapter 30 셸쇼크 취약점 ----- 365

Part 10 A10 - 검증되지 않은 리다이렉트와 포워드 _____ 369

chapter 31 검증되지 않은 리다이렉트와 포워드 (1) ----- 371

31.1 난이도 하 _____ 371

31.2 대응방안 _____ 372

chapter 32 검증되지 않은 리다이렉트와 포워드 (2) ----- 374

32.1 난이도 하 _____ 374

32.2 대응방안 _____ 375

마무리하며 _____ 376

chapter **1** 개요

1.1 비박스란

비박스^{bee-box01}는 웹 취약점을 공격할 수 있는 오픈소스 웹 애플리케이션인 bWAPP^{buggy Web Application}이 설치된 가상환경으로, 웹 취약점 공격을 공부하기 위 하여 만들어졌으며 100여 개가 넘는 웹 취약점이 존재한다. 취약점은 OWASP Top 10을 기준으로 분류되었으며 각 항목은 '1.2 취약점 분류'에서 소개하다.

비박스는 웹 애플리케이션 취약점의 기본인 인젝션과 XSS 취약점부터 최근에 발 견된 셸쇼크^{ShellShock} 취약점, 하트블리드^{Heartbleed} 취약점 등 웹 애플리케이션뿐만 아니라 웹 서버, 네트워크 기반의 취약점까지 포함되어 있어서 다양한 취약점을 연구하고 실습할 수 있다.

하지만 힌트를 제공하지 않기 때문에 처음 공부를 시작하는 사람들은 어떤 공격 방법을 사용할지 알 수 없다. 또한, 취약점 종류가 많고, 하^{Low} 단계의 난도가 상당 히 높아서 중^{Medium}이나 상^{High} 단계까지 살펴보는 데 시간이 오래 걸리며 중과 상 의 경계가 불분명하다는 단점이 있다.

비박스를 사용할 때는 웹 애플리케이션인 bWAPP을 해당 호스트에 설치하는 방 법과 비박스를 가상환경에 설치하여 미리 설치된 bWAPP을 사용하는 방법이 있 는데, 이 책에서는 두 번째 방법을 사용한다.

⁰¹ 비박스 공식 홈페이지: http://www.itsecgames.com/

먼저 비박스 다운로드 페이지⁰²에 접속하여 상단에 있는 압축 파일(bee-box_ v1.6.7z)을 다운로드한다. 그다음 가상머신에 비박스 환경을 만들기 위하여 하드웨 어 가상머신 소프트웨어인 VM웨어^{VMware}나 버추얼박스^{VirtualBox}로 비박스를 설치 한다.

그림 1-1 비박스 가상 이미지 다운로드

an extremely but Brought to you by: n	iggy web a nmesellem	рр!				
Summary Files	Reviews	Support Wiki	Code Tickets	Discussion I	Blog	
Looking for the late Home / bee-box	est version? E	Oownload bWAPP_la	test.zip (15.1 M	B) Downloads /	Week	لا
Name +		Modified †	Size 🕈	Downloads	÷	
↑ Parent folder						
bee-box_v1.6.7z		2014-11-02	1.2 GB	226	0	
release_notes.txt		2014-11-02	1.9 kB	11	0	,
README.txt		2014-09-27	832 Bytes	15	_ 0	
INSTALL.txt		2014-09-27	2.4 kB	22	_ 0	

1.2 취약점 분류

비박스는 3단계로 구성되는데, 하 단계만 포함된 취약점 항목도 있다. 취약점은 'OWASP Top 10 - 2013 가장 심각한 웹 애플리케이션 보안 위험 10가지'를 기준으로 분류하였고, 그 외 취약점은 '기타(Other bugs)' 항목에 포함한다. 이 책 에서는 모든 취약점을 다루지는 않고 항목당 중요 순위대로 뽑아서 다루겠다.

⁰² 비박스 이미지 다운로드 페이지: http://sourceforge.net/projects/bwapp/files/bee-box/

분류	취약점
A1 인젝션(Injection)	HTML Injection - Reflected (GET)
	HTML Injection - Reflected (POST)
	HTML Injection - Reflected (URL)
	HTML Injection - Stored (Blog)
	iframe Injection
	LDAP Connection Settings
	Mail Header Injection (SMTP)
·	OS Command Injection
	OS Command Injection – Blind
	PHP Code Injection
	Server-Side Includes (SSI) Injection
	SQL Injection (GET/Search)
	SQL Injection (GET/Select)
	SQL Injection (POST/Search)
	SQL Injection (POST/Select)
	SQL Injection (AJAX/JSON/jQuery)
	SQL Injection (CAPTCHA)
	SQL Injection (Login Form/Hero)
	SQL Injection (Login Form/User)
	SQL Injection (SQLite)
	SQL Injection (Drupal)
	SQL Injection - Stored (Blog)
	SQL Injection - Stored (SQLite)
	SQL Injection - Stored (User-Agent)
	SQL Injection - Stored (XML)
	SQL Injection - Blind - Boolean-Based
	SQL Injection - Blind - Time-Based
	SQL Injection - Blind (SQLite)
	SQL Injection - Blind (Web Services/SOAP)

분류	취약점
A1 인젝션(Injection)	XML/XPath Injection (Login Form)
	XML/XPath Injection (Search)
	SQL Injection (Drupal)
	SQLInjection - Stored (XML)
	XML/XPath Injection (Search)
A2 인증 결함과 세션 관리	Broken Authentication – CAPTCHA Bypassing
(Broken Authentication & Session Management)	Broken Authentication - Forgotten Function
Managementy	Broken Authentication – Insecure Login Forms
	Broken Authentication – Logout Management
	Broken Authentication – Password Attacks
	Broken Authentication – Weak Passwords
	Session Management – Administrative Portals
	Session Management – Cookies (HTTPOnly)
	Session Management – Cookies (Secure)
	Session Management – Session ID in URL
	Session Management – Strong Sessions
A3 크로스 사이트 스크립팅	Cross-Site Scripting - Reflected (GET)
(XSS, Cross-Site Scripting)	Cross-Site Scripting - Reflected (POST)
	Cross-Site Scripting - Reflected (JSON)
	Cross-Site Scripting - Reflected (AJAX/JSON)
	Cross-Site Scripting - Reflected (AJAX/XML)
	Cross-Site Scripting - Reflected (Back Button)
	Cross-Site Scripting - Reflected (Custom Header)
	Cross-Site Scripting - Reflected (Eval)
	Cross-Site Scripting - Reflected (HREF)
	Cross-Site Scripting - Reflected (Login Form)
	Cross-Site Scripting - Reflected (phpMyAdmin)
	Cross-Site Scripting - Reflected (PHP_SELF)
	Cross-Site Scripting - Reflected (Referer)

분류	취약점		
A3 크로스 사이트 스크립팅 (XSS, Cross-Site Scripting)	Cross-Site Scripting - Reflected (User-Agent)		
	Cross-Site Scripting - Stored (Blog)		
	Cross-Site Scripting - Stored (Change Secret)		
	Cross-Site Scripting - Stored (Cookies)		
	Cross-Site Scripting - Stored (SQLiteManager)		
	Cross-Site Scripting - Stored (User-Agent)		
A4 취약한 직접 객체 참조	Insecure DOR (Change Secret)		
(Insecure Direct Object References)	Insecure DOR (Reset Secret)		
	Insecure DOR (Order Tickets)		
A5 보안 설정 오류	Arbitrary File Access (Samba)		
(Security Misconfiguration)	Cross-Domain Policy File (Flash)		
	Cross-Origin Resource Sharing (AJAX)		
	Cross-Site Tracing (XST)		
	Denial-of-Service (Large Chunk Size)		
	Denial-of-Service (S난이도 하 HTTP DoS)		
	Denial-of-Service (SSL-Exhaustion)		
	Denial-of-Service (XML Bomb)		
	Insecure DistCC Configuration		
	Insecure FTP Configuration		
	Insecure NTP Configuration		
	Insecure SNMP Configuration		
	Insecure VNC Configuration		
	Insecure WebDAV Configuration		
	Local Privilege Escalation (sendpage)		
	Local Privilege Escalation (udev)		
	Man-in-the-Middle Attack (HTTP)		
	Man-in-the-Middle Attack (SMTP)		
	Old/Backup & Unreferenced Files		
	Robots File (Disclosure)		

A6 민감 데이터 노출 (Sensitive Data Exposure) BEAST/CRIME/BREATCH Attacks Clear Text HTTP (Credentials) Heartbleed Vulnerability Host Header Attack (Reset Poisoning) HTML5 Web Storage (Secret) POODLE Vulnerability SSL 2.0 Deprecated Protocol1-9 Text Files (Accounts)
(Sensitive Data Exposure) BEAST/CRIME/BREATCH Attacks Clear Text HTTP (Credentials) Heartbleed Vulnerability Host Header Attack (Reset Poisoning) HTML5 Web Storage (Secret) POODLE Vulnerability SSL 2.0 Deprecated Protocol1–9 Text Files (Accounts)
Clear Text HTTP (Credentials) Heartbleed Vulnerability Host Header Attack (Reset Poisoning) HTML5 Web Storage (Secret) POODLE Vulnerability SSL 2.0 Deprecated Protocol1–9 Text Files (Accounts)
Heartbleed Vulnerability Host Header Attack (Reset Poisoning) HTML5 Web Storage (Secret) POODLE Vulnerability SSL 2.0 Deprecated Protocol1–9 Text Files (Accounts)
Host Header Attack (Reset Poisoning) HTML5 Web Storage (Secret) POODLE Vulnerability SSL 2.0 Deprecated Protocol1-9 Text Files (Accounts)
HTML5 Web Storage (Secret) POODLE Vulnerability SSL 2.0 Deprecated Protocol1-9 Text Files (Accounts)
POODLE Vulnerability SSL 2.0 Deprecated Protocol1-9 Text Files (Accounts)
SSL 2.0 Deprecated Protocol1-9 Text Files (Accounts)
A7 기능 수준의 접근통제 누락 Directory Traversal - Directories
(Missing Function Level Access Control) Directory Traversal – Files
Host Header Attack (Cache Poisoning)
Host Header Attack (Reset Poisoning)
Local File Inclusion (SQLiteManager)
Remote & Local File Inclusion (RFI/LFI)
Restrict Device Access
Restrict Folder Access
Server Side Request Forgery (SSRF)
XML External Entity Attacks (XXE)
A8 크로스 사이트 요청 변조 Cross-Site Request Forgery (Change Password)
(CSRF, Cross-Site Request Forgery) Cross-Site Request Forgery (Change Secret)
Cross-Site Request Forgery (Transfer Amount)
A9 알려진 취약점이 있는 컴포넌트 사용 Buffer Overflow (Local)
(Using Components with Known Vulnerabilities) Buffer Overflow (Remote)
Drupal SQL 인젝션 (Drupageddon)
Heartbleed Vulnerability
PHP CGI Remote Code Execution
PHP Eval Function
phpMyAdmin BBCode Tag XSS
Shellshock Vulnerability (CGI)

분류	취약점	
A9 알려진 취약점이 있는 컴포넌트 사용 (Using Components with Known Vulnerabilities)	SQLiteManager Local File Inclusion	
	SQLiteManager PHP Code Injection	
	SQLiteManager XSS	
A10 검증되지 않은 리다이렉트 및 포워드	Unvalidated Redirects & Forwards (1)	
(Unvalidated Redirects & Forwards)	Unvalidated Redirects & Forwards (2)	
기타(Other bugs)	ClickJacking (Movie Tickets)	
	Client-Side Validation (Password)	
	HTTP Parameter Pollution	
	HTTP Response Splitting	
	HTTP Verb Tampering	
	Information Disclosure – Favicon	
	Information Disclosure - Headers	
	Information Disclosure – PHP version	
	Information Disclosure - Robots File	
	Insecure iFrame (Login Form)	
	Unrestricted File Upload	

1.3 점검 환경 구성

이 책에서는 공격자 단말에서 칼리 리눅스^{Kali Linux}와 윈도우 환경을 이용하고 대 상 가상환경으로 비박스를 선택하였다. 개인 사용자가 많이 사용하는 가상머신은 VM웨어와 버추얼박스인데, 여기서는 무료로 이용할 수 있는 버추얼박스를 선택 하였다. 버추얼박스에 두 개의 이미지로 공격자와 대상자를 구성해 보자.

1.3.1 버추얼박스에 비박스 설치하기

버추얼박스는 공식 홈페이지⁰³에서 다운로드하여 설치한다. 설치할 때 컴퓨터 사

⁰³ 버추얼박스 홈페이지: https://www.virtualbox.org/

용자 이름을 영문으로 하는 것만 주의하면 나머지는 간단하므로 설치 과정은 생략 하겠다. 설치한 버추얼박스를 실행한 후 메뉴에서 [새로 만들기]를 클릭한다. '이 름 및 운영 체제' 설정 화면에서 종류는 'Linux', 버전은 'Ubuntu (32-bit)'로 설 정한다. 다른 환경으로 설정할 경우 설치되지 않는다.

그림 1-2 가상머신 새로만들기

파일(F) 머신(M) 도움말(H)	
값 % %	
5 ×	반
> 가상 머신 만들기	meta 제: Debian (32-bit)
이름 및 운영 체제	스템
새 가상 머신을 나타내는 이름을 입력하고 설치할 운영 체제를 선택하십시 오. 입력한 이름은 VirtualBox에서 가상 머신을 식별하는 데 사용됩니다.	모리: 768 MB 서: 플로피 디스크, VT-X/AMD-V, 반가상화
이름(N): bee-box	
종류(T): Linux 🔹 👽	스플레이
버젼(V): Ubuntu (32-bit)	메모리: 12 MB
	스크톱 서버: 사용 안할 캡처: 사용 안할
	장소
	H: IDE 컨더리 마스터: [광학 H: SATA
전문가 모드(E) 다음(N) 취소) 포트 0: Metas
	U 2

참고로, VM웨어에서 비박스를 사용하려면 다운로드한 파일의 압축을 해제한 후 'bee-box'라는 디렉터리가 나올 때까지 클릭해서 들어간다. 'bee-box' 디렉터 리에서 'bee-box'라는 이름의 '.vmx' 확장자 파일을 VM웨어에서 실행한다. 운영체제를 선택한 후 [그림 1-3]과 같이 원하는 크기의 메모리를 설정한다.

그림 1-3 가상머신 메모리 크기 할당

<u> १</u> ×
🚱 가상 머신 만들기
메모리 크기
가상 머신에 할당할 메모리(RAM) 크기를 메가바이트 단위로 입력하십시오.
추천 메모리 크기는 768 MB입니다.
4 MB 16384 MB
다음(N) 취소

그다음 '기존 가상 하드 디스크 파일 사용'을 선택하고, 경로명 옆에 있는 [디렉터 리 열기] 버튼을 선택하여 압축 파일을 해제한 디렉터리로 이동한다.

그림 1-4 기존 가상 하드 디스크 파일 사용 선택

2 ×
ⓒ 가상 머신 만들기
하드디스크
필요하다면 새 가상 머신에 가상 하드 디스크를 추가할 수 있습니다. 새 하 드 디스크 파일을 만들거나, 목록에서 선택하거나, 폴더 아이콘을 통하며 다 른 위치에 있는 가상 하드 디스크 파일을 선택할 수 있습니다.
더 자세한 구성미 필요하다면 이 단계를 건너뛰고 가상 머신을 만든 다음 설 정을 진행하십시오.
추천하는 하드 디스크 크기는 8,00 GB입니다.
◎ 가상 하드 디스크를 추가하지 않음(D)
◎ 기존 가상 하드 디스크 파일 사용(U)
bee-box, vmdk (일반, 20,00 GB) 🔹 🗸
만들기 취소

[그림 1-5]와 같이 'bee-box' 디렉터리에서 'bee-box.vmdk' 파일을 선택 한다. 그림 1-5 가상 하드 디스크 파일 선택

▶ 새 볼륨 (F:) ▶ vmware_원	본들 🕨 bee-box_v1.6	6 ► bee-box		
이름		수정한 날짜	유형	크기
😻 bee-box.vmdk		2014-11-03 오전	Virtual Machine	1KB
🗣 bee-box-s001.vmdk		2014-11-03 오전	Virtual Machine	137,536KB
bee-box-s002.vmdk		2014-11-03 오전	Virtual Machine	1,225,536

이미지를 불러왔다면 [그림 1-6]과 같이 네트워크를 설정한다. 이 책에서는 '호스 트 전용 어댑터'로 설정하는데, 설정한 뒤에 IP가 제대로 할당되지 않으면 'MAC 주소' 옆에 있는 [새로고침] 버튼을 클릭하면 된다.

그림 1-6 가상머신 네트워크 설정

🕑 bee	e-box - 설정	<u>8 x</u>
	일반	네트워크
	시스템	어댑터 1 이댑터 2 어댑터 3 어댑터 4
	디스플레이	☑ 네트워크 어댑터 사용하기(E)
\square	저장소	다음에 연결됨(A): 호스트 전용 어댑터 💌
	오디오	이름(N): VirtualBox Host-Only Ethernet Adapter
P	네트워크	어댑터 종류(T): Intel PRO/1000 MT Desktop (82540EM)
	직렬 포트	무작위 모드(P): 모두 허용
	USB	MAC 주소(M): 080027633347 (중)
	공유 폴더	☑ 케이블 연결될(C) 포트 포워딩(P)
	사용자 인터페이스	
		확인 취소 도움말(H)

모든 설정이 완료되면 [그림 1-7]과 같이 [시작] 버튼을 클릭하여 비박스 가상머 신을 실행한다. 우분투 화면에서 비박스 메인 페이지가 나오면 정상적으로 동작하 는 것이다. 가상머신 내에서 마우스 커서가 제멋대로 동작하는 경우 왼쪽 마우스 로 전체화면을 몇 번 드래그하면 커서가 정상적으로 작동한다. 이는 가상머신 이 미지를 변환하는 과정에서 발생하는 버그 중에 하나로 생각한다.

그림 1-7 가상머신 시작 및 동작 확인



그다음 비박스 가상머신 콘솔을 클릭해서 연다. ifconfig 명령어를 입력하여 IP 주소를 확인하고, 호스트에서 해당 IP로 접근하였을 때 테스트 환경이 정상적으 로 동작하는지 확인한다. 테스트 환경이 동작하지 않으면 네트워크 설정이 잘못된 것이므로 다시 확인하기 바란다.

그림 1-8 비박스 IP 확인



IP 주소를 확인했으면 호스트의 웹 브라우저에 IP 주소를 입력한다. 그러면 웹 애 플리케이션을 실행할 수 있는 페이지가 보인다. 만약 콘솔에서 영문 입력이 되지 않는다면 키보드 입력을 추가해야 한다. [그림 1-9]와 같이 화면 상단 메뉴에 마우스 오른쪽을 클릭한 후 메뉴에서 '키보드 기본 설정'을 클릭한다.

그림 1-9 키보드 기본 설정

	벨기에 4월 5일(화)오	후 12:14	16	📃 bee	С
bWAPP	그룹(<u>G</u>)				ı X
	키보드 기본 설정(<u>P</u>)				
26 255 Mask:255.2	현재 배치 표시(L) 7 도움말(<u>H</u>) 7 정보(<u>A</u>)				
etric:1 :0 frame:0 :0 carrier:0	 패널에서 지우기(<u>R</u>) 옮기기(<u>M</u>) 				
	패널에 잠그기(<u>K</u>)				

키보드 설정 화면이 나오면 '키 배치' 탭의 '키 배치' 항목에서 대한민국을 선택한 다. 또는 영어를 선택하여도 된다.

그림 1-10 키 배치 추가하기

	키보드 설정		x	
일반 키 배치 접근성 기	등 마우스 키 타이핑 휴식 시간			a x
키보드 모델(M):	일반 105키 (국제 버전	PC	:26 .255 Misk:255.255.255.0	(A)
선택한 키 배치(<u>S</u>):			ppe:Link	
ヲ 出版大		기본값	:0 frame:0	
벨기에		0	s:0 carrier:0	
대한민국 101/104 key	Compatible	۲	56 (1.7 MB)	
	6	a	까지 바이지 않는 아이지?	404
에 각 참아다 별도 키네: 	хіц) , ^{glai(P)} 	변종(V): 기본값 미리 보기:	:	
보드 설정 시험 하기(<u>]</u>):				
0 289(F)				

설정을 완료한 후 상단에 언어를 클릭하면 추가된 언어로 전환된다. 콘솔을 실행 하고 키를 입력하면 정상적으로 ifconfig가 입력될 것이다.

그림 1-11 키 배치 입력



주소 확인까지 끝나면 호스트 운영체제에서 웹으로 접근하여 테스트를 진행한다.

1.3.2 웹 애플리케이션 접속하기

비박스로 웹 애플리케이션을 실행하는 방법은 두 가지가 있는데, 첫 번째는 비박 스가 설치된 가상환경 안에서 'bWAPP-Start'를 눌러서 시작하는 방법이다.

그림 1-12 bWAPP-Start를 클릭하여 bWAPP 실행



가상머신에서 테스트하기 불편하면 호스트에서 직접 URL 주소를 입력하여 웹 애 플리케이션을 실행한다. [그림 1-13]과 같이 메인 페이지 화면이 나오면 정상적 으로 동작하는 것이다. 이 책에서 실습할 'bWAPP'이 상단에 보이고 그외 취약점 실습을 할 수 있는 환경 링크들이 있다.

그림 1-13 bWAPP 메인 페이지

← → C 🗋 192.168.56.101



'bWAPP'을 클릭하면 로그인 페이지가 나오는데, 기본 설정된 아이디는 'bee', 비밀번호는 'bug'다. 비밀번호 아래 'Set the security level'이라는 드롭다운 메뉴로 난이도 조절이 가능하다. 난이도는 하^{Low}, 중^{Medium}, 상^{High} 순이고, 마지막 단계가 가장 어렵다. 상 단계에서는 취약점을 막는 대응방안을 참고할 수 있다. 로 그인 후에는 실습할 항목을 선택하고 [Hack] 버튼을 클릭하면 해당 항목 페이지 가 열린다. 그림 1-14 bWAPP 로그인과 공격 실행

ogin New User Info Ta	/ Portal /
/ Login /	bWAPP, or a buggy web application, is a free and open s It helps security enthusiasts, developers and students to bWAPP covers all major known web vulnerabilities, inclu It is for security-testing and educational purposes only.
Login:	Which bug do you want to hack today? :)
bee	SQL Injection (POST/Search)
Password:	SQL Injection (AJAX/JSON/jQuery) SQL Injection (CAPTCHA)
Set the security level:	SQL Injection (Login Form/Hero) SQL Injection (Login Form/User) SQL Injection (SQLite)
low V	SQL Injection (Drupal) SQL Injection - Stored (Blog)
Login	Hack

1.3.3 버추얼박스에 칼리 리눅스 환경 설치하기

이번에는 버추얼박스에 칼리 리눅스 환경을 설치해 보자. 칼리 리눅스 다운로드 페이지⁰⁴에 가면 [그림 1-15]와 같이 버추얼박스 이미지 다운로드 버튼이 있다. 이중에서 [KALI VIRTUAL IMAGES]를 클릭한다.

그림 1-15 버추얼박스 이미지 다운로드

Download Kali Linux VMware, VirtualBox and ARM images

Are you looking for **Kali Linux VMWare**, **VirtualBox** or **ARM** images? The good folks at Offensive Security (who are also the funders, founders, and developers of Kali Linux) have generated alternate flavours of Kali using the same build infrastructure as the official Kali releases. **VMWare**, **VirtualBox** and **ARM architecture** Kali images produced by Offensive Security can be found on the Official <u>Offensive Security Kali Linux Virtual Images</u> and Offensive Security Kali Linux ARM Images pages respectively.

KALI VIRTUAL IMAGES

KALI ARM IMAGES

KALI ARM BUILD SCRIPTS

⁰⁴ 칼리 리눅스 다운로드 페이지: https://www.kali.org/downloads/

그러면 페이지 중간쯤에 [그림 1-16]과 같은 화면이 나오는데, 이 중에서 버추얼 박스 이미지 다운로드 링크 탭(Prebuilt Kali Linux VirtualBox Images)을 클릭한 다. 이 책에서는 32비트 환경을 선택하며, 파일은 .ova 형태로 다운로드된다.

그림 1-16 칼리 리눅스 가상머신 이미지 다운로드

Prebuilt Kali Linux VMw	are Imag	es	Prebuilt Kali Linux VirtualBox Images				
Image Name Torrent Size			Version	SHA1Sum			
Kali Linux 64 bit VBox	Torrent	3.0G	2016.1	f1f59b09b97903f5d4a3f47fa2e13896daf3c2ef			
Kali Linux 32 bit VBox PAE Torrent 3.0G		2016.1	987f2c04a4d595b1716ecfe61ce4074d1adac303				

그다음 버추얼박스 메뉴에서 [파일 → 가상 시스템 가져오기]를 클릭하고, 디렉터 리 열기로 [그림 1-17]과 같이 다운로드한 .ova 가상 이미지를 가져온다.

그림 1-17 가상 시스템 가져오기(1)



[다음]을 클릭하면 [그림 1-18]과 같이 가져오기가 진행되며 이 단계가 지나면 버 추얼박스에 칼리 리눅스가 추가된다. 이후에는 비박스를 설치할 때와 마찬가지로 네트워크를 설정(호스트 전용 어댑티)하고 네트워크 IP가 비박스와 동일한 네트워크 대역인지 확인하면 된다. ping 명령어로 통신이 원활한지도 체크해 보자. 그림 1-18 가상 시스템 가져오기(2)



1.3.4 윈도우 환경에 버프스위트 설치하기

버프스위트^{Burp Suite}는 로컬 프락시 서버로, 클라이언트와 서버 사이의 요청과 응답 을 수정, 생성, 재사용하는 등의 기능이 있다. HTTP 요청과 응답을 수정하여 서 비스 절차를 우회하거나 권한을 상승하여 공격에 주로 활용한다. 버프스위트는 칼 리 리눅스에 포함되어 있지만, 윈도우 환경에서 많이 사용하므로 윈도우 환경에서 실행 방법을 설명하겠다. 칼리 리눅스에서는 burpsuite 명령어를 입력하면 바로 실행된다.

버프스위트는 자바를 기반으로 동작하는 프로그램이어서 설치 전에 자바 JDK⁰⁵ 를 설치해야 한다. 버프스위트는 다운로드 페이지⁰⁶에서 무료 버전(Free Edition) 을 다운로드하고, 다운로드한 JAR 파일로 버프스위트를 실행한다.

⁰⁵ 자바 JDK 다운로드: http://www.oracle.com/technetwork/java/javase/downloads/index.html

⁰⁶ 버프스위트 다운로드: https://portswigger.net/burp/download.html

	Free Edition	Professional Edition \$299 per user per year
Burp Proxy	2	2
Burp Spider	2	
Burp Repeater	2	0
Burp Sequencer	2	<u> </u>
Burp Decoder	~	 Ø
Burp Comparer	2	· · · · · · · · · · · · · · · · · · ·
Burp Intruder	Time-throttled demo	Ø
Burp Scanner		2
Save and Restore		2
Search		2
Target Analyzer		2
Content Discovery		2
Task Scheduler		 Ø
Release Schedule	Major point releases	Frequent updates, earlier releases, beta versions

여러 기능을 제공하고 있지만 가장 기본 기능인 프락시를 사용하려면 웹 브라우저 의 인터넷 설정에서 연결 탭에 있는 LAN 설정을 수정해야 한다. 프락시 서버 설 정 칸에서 IP는 '127.0.0.1', 포트 번호는 '8080'에 맞춘다. 프락시 기능을 사용 하려면 실제 요청이 들어오는 포트와 다른 포트 번호를 사용하여야 버프스위트에 서 확인할 수 있다. [그림 1-20]은 인터넷 익스플로러의 프락시 설정 화면이다. 그림 1-20 웹 브라우저 프락시 설정

E LAN 설정									
자동 구성 자동 구성은 수동 설정보다 우선합니다. 수동 설정을 사용하려면 자동 구 성을 사용하지 마십시오.									
🔲 자동으로 설정 검색(A)									
🔲 자동 구성 스크립트 사용(S)									
주소(R):									
프록시 서버									
☑ 사용자 LAN에 프록시 서버 사용(이 설정은 전화 연결이나 VPN 연결 에는 적용되지 않음)(X)									
주소(E): 127.0.0.1 포트(T): 8080 고급(C)									
확인 취소									

버프스위트의 Proxy 탭에서 [intercept is on] 버튼이 활성화되어 있으면 인터 넷 연결 시 주고받는 HTTP 요청, 응답 세션을 모두 버프스위트로 가로챈다. 이 때 가로챈 요청을 전송하려면 [Forward] 버튼을 클릭하고, 전송하지 않으려면 [Drop] 버튼을 클릭한다. 요청이나 응답을 전송하지 않으면 버프스위트에서 웹 브라우저에 자체적으로 오류 메시지를 출력한다.

Surp Suite Fr	ee Edition v1.6	-									
Burp Intruder R	Burp Intruder Repeater Window Help										
Repeater	Sequencer	Decoder	Comparer	Extender	Options	Alerts					
Target	Proxy	Spie	der	Scanner	Intru	der					
Intercept HTT	TP history WebS	ockets history	Options								
Forward Raw Hex	Drop	Intercept	Action	Comment this	; item						
? <	+ > Type	a search term	1			0 matches					

그림 1-21 버프스위트에서 요청이나 응답 가로채기 설정

프락시 사용을 중지하고 싶을 때는 [intercept is on] 버튼을 한 번 클릭하면 [intercept is off]가 되어 버프스위트가 요청과 응답 값을 가로채지 못한다.

버프스위트에서 주로 사용하는 탭은 Proxy와 Intruder, Repeater다. 그러나 Proxy 탭에서 가로챈 세션을 Intruder나 Repeater에서 사용하게 보내는 기능 이 있으므로 Proxy 탭만 사용하여도 된다. 세션을 가로챈 다음 [Action] 버튼을 클릭하거나 Proxy의 하위 탭인 'Intercept'의 세션 내용에 마우스를 대고 오른 쪽 버튼을 클릭하면 세션을 여러 탭으로 보내는 팝업 메뉴가 나타난다. 여기서 보 내고 싶은 탭을 선택하면 된다.

그림 1-22 가로챈 세션을 다른 탭에 보내기

5 Burp Suite Fre	e Edition v1.6	_	-					x		
Burp Intruder Re	epeater Window H	elp						_		
Repeater	Repeater Sequencer Decoder Comparer Extender Options Alerts									
Target	Proxy	Sp	ider	ſ	Scanner	Inti	ruder			
Intercept HTTP history WebSockets history Options										
Request to h	10111111111111111111111111111111111111	:80		Send t	o Spider]		
Forward	Drop	Intercept is		Do an	active scan			?		
				Send t Send t	o Intruder o Repeater		Ctrl+I Ctrl+R	2		
Raw Params	Headers Hex			Send t	o Sequencer					
GET /bWAPP/1 Host: 192 16	ogin.php HTT. 8 74 140	P/1.1		Send t	o Comparer					
User-Agent:	Mozilla/5.0	(Windows N	т в.	Send t	o Decoder					
Gecko/201001	.01 Firefox/3	9.0		Reque	st in browser		►			
Accept: text/html.an	plication/xh	tml+xml.an	nlie	Engag	ement tools [Pro v	ersion only]	•			
Accept-Langu	age: ko-KR,k	o;q=0.8,en	-US;	Chang	e request method					
Accept-Encod	ling: gzip, d	eflate		Chang	e body encoding					
Connection:	keep-alive	; PHPSESSI	D=a4	Сору І	JRL					
	·····			Сору а	as curl command					
				Copy t	o file					
				Paste	from file					
				Save it	tem					
? < +	> Type a	search term		Don't ir	ntercept requests		•	hes		

Intercept 하위의 'Raw' 탭에서는 요청 세션의 내용을 보여주고, 'Params' 탭 에서는 세션에서 사용하는 변수와 그 값을 테이블 형태로 보여준다. 'Headers' 탭에서는 세션을 헤더별로 분류하여 보여주며, 'Hex' 탭에서는 요청 값을 16진 수로 보여준다. 모든 탭에서 세션 내용을 수정할 수 있지만, 정상적인 값이 아닐 경우 요청에 대한 응답이 오지 않는다.

그림 1-23 Intercept 탭의 하위 탭

Surp Suite Fre	e Edition v1.6		-	-						
Burp Intruder Re	epeater Window	Help								
Repeater Sequencer Decoder Comparer Extender Options										
Target	Target Proxy Spider Scanner Intru									
Intercept HTT	P history Webs	Sockets history	Options							
Request to h	Request to http://192.168.74.140:80 Forward Drop Intercept is on Action Raw Params Headers Hex									
GET request to /bW	/APP/login.php									
Type Name		Value				Add				
Cookie security	level	0								
Cookie PHPSES	Cookie PHPSESSID a422920431f38135409f8d4a6f2977d1									
Body encoding:										

버프스위트의 프락시 기능은 기본 설정으로 요청 세션만 가로챈다. 응답 세션도 가로채려면 Proxy 하위 탭인 'Options'에서 'Intercept Server Responses' 옵션을 수정한다. 그러면 요청과 함께 응답도 버프스위트에서 확인할 수 있다. 요 청과 마찬가지로 웹 브라우저에서 응답을 확인하려면 [Forward] 버튼을 클릭하 여 가로챈 세션을 전송한다.

그림 1-24 응답 세션 가로채기 설정

5 Burp Suite	Free Edition v1	.6					• ×		
Burp Intruder	Repeater Wind	low Help							
Intruder	Repeater	Sequence	r Decode	comparer	Extender	Options	Alerts		
Та	rget	Pro	xy	Spider	ſ	Scanner			
Intercept	ITTP history W	/ebSockets his	tory Options						
 Intercept Server Responses Use these settings to control which responses are stalled for viewing and editing in the Intercept tab. Intercept responses based on the following rules: 									
		operator	Content type	Matches	text				
E	dit 🗌	Or	Request	Was modified					
Ren	love	Or	Request	Was intercepted					
		And	Status code	Does not match	^304\$				
U	p U	And	URL	is in target scope					
Do	wn								
Automatically update Content-Length header when the response is edited									
•									

이 책에서는 버프스위트로 진단하는 데 필요한 기능만 다루었다. 버프스위트를 제대로 활용하고 싶다면 『버프스위트의 활용과 웹 모의해킹』(한빛미디어, 2015) (http://www.hanbit.co.kr/store/books/look.php?p_code=E5762585261)을 참고하 기 바란다.

이제 모든 환경 구성이 끝났다. 다음 장부터는 비박스에서 웹 해킹 항목을 하나씩 살펴보면서 이론 설명과 실습을 진행하겠다.