Hanbit RealTime 109

버프스위트 활용과 웹 모의해킹

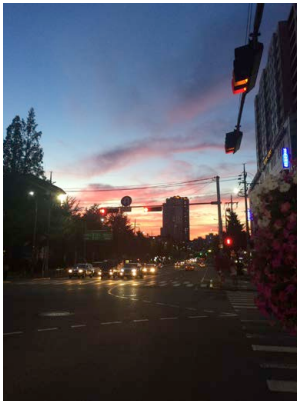
조정원, 김명근, 조승현 지음

한빛미디어 Hanbit Media, Inc.

버프스위트 활용과 웹 모의해킹

조정원, 김명근, 조승현 지음

한빛미디어 Hanbit Media, Inc.



표지 사진 **김제민**

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

사진 보내기 **ebookwriter@hanbit.co.kr**

버프스위트 활용과 웹 모의해킹

초판발행 2015년 9월 24일

지은이 조정원, 김명근, 조승현 / **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 978-89-6848-770-5 15000 / **정가** 15,000원

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

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 『워드프레스 플러그인 취약점 분석과 모의해킹』(한빛미디어, 2015, 유희만 공저), 『파이썬 오픈소스 도구를 활용한 악성코드 분석』(에이콘출판사, 2015, 최우석 외 공저), 『IT 엔지니어로 사는 법 1』(비팬북스, 2015, 권순용 외 공저), 『안드로이드 모바일 악성코드와 모의 해킹 진단』(에이콘출판사, 2014, 박병욱 외 공저), 『모의해킹이란 무엇인가』(위키북스, 2014), 『칼리 리눅스와 백트랙을 활용한 모의해킹』(에이콘출판사, 2013, 박병욱 외 공저), 『디지털 포렌식의 세계』(인포더북스, 2013, 이준형 공저), 『크래커 잡는 명탐정 해커』(성안당, 2010) 등이 있으며, 보안프로젝트 멤버들과 함께 다양한 영역에서 활동하고 있다.

김명근(xitcsk@naver.com)

한국정보기술연구원에서 모의해킹 6기 과정을 수료하고 현재 동국대학교 정보보호 석사 과정에 재학하고 있다. 보안프로젝트(www.boanproject.com) 스태프 및 연구원으로 활동하고 있다. 주요 연구 분야로는 웹 애플리케이션 및 모바일 애플리케이션 취약점 진단, 소스 코드 진단, 소프트웨어 엔지니어링, 퍼징 테스트 등이 있다.

조승현(huk2da@naver.com)

에스알센터 선임 연구원이며 KUCIS 정보보호교육, 한전KDN 웹 보안 실무 과정 등 전문강사로 활동하고 있다. 보안프로젝트(www.boanproject.com) 스태프로 활동하며 웹 애플리케이션 취약점 진단과 모바일 악성코드 분석 중심으로 연구를 진행하고 있다.

저자 서문

지은이_ **조정원**

모의해킹 업무를 하다 보면 항상 실행하고 있는 것이 있다. 바로 클라이언트 프락시 도구다. 실무에서는 버프스위트BurpSuite와 피들러Fiddler를 많이 사용한다. 나도 버프스위트 도구를 사용하면서 항상 '이렇게 많은 메뉴가 있는데, 활용하는 것은 극히 일부분이네? 다른 기능들은 어떻게 활용될까?'라는 고민만 했다. 그러던 중 다시 버프스위트를 연구할 기회가 생겼고 메뉴 하나씩 모의해킹 진단 항목들과 연관하여 살펴보니 좋은 기능이 무척 많았다. 웹 애플리케이션 주요 항목을 모두 점검하는 데 큰 문제가 없을 정도의 종합 진단 프레임워크라는 생각이 들 정도다.

이 책을 집필하는 데 시간이 많이 들었으며 노력도 많이 하였다. 같이 집필한 팀원들이 없었다면 절대로 마무리되지 않았을 것이다. 목표를 향해 열심히 해 준 보안프로젝트의 모든 멤버들에게도 항상 감사하다. 이 책을 쓰는 동안 옆에서 항상 응원해 준 아내 김혜진과 아들 호영, 딸 희영에게 사랑한다고 전하고 싶다.

지은이_**김명근**

설렘과 두려움을 안고 시작했던 역곡 프로젝트를 시작으로 보안프로젝트에서 활동을 시작한 후, 이제야 비로소 작지만 소중한 나의 첫 출판이 결실을 보게 되었다. 처음에는 저자로서 독자에게 어떤 내용을 전달할지, 독자가 아닌 저자로 책을 읽고 글을 쓴다는 것에 고민이 많았으며 불안감도 들었다. 내가 공부하고 생각한 것을 정리하여 누군가에게 전달한다는 것, 그리고 내 이름으로 책을 낸다는 것이 책을 읽고 생각의 정리만 해 왔던 나에게 어려운 일이었다. 그러나 그런 나를 믿어주고 할 수 있다는 용기와 기회를 주신 조정원 선배님께 감사의 인사를 드린다. 또한, 이 책은 오로지 나만의 힘으로 완성된 것이 아니다. 함께 연구와 집필을 한 조정원 선배님과 승현이 형 그리고 한국 정보기술연구원에서부터 지금까지 옆에서 같이 응원해 주고 도움을 준 광수 형과 재형이 형에게 감사의 인사를 전한다. 마지막으로 지난 시간을 돌이켜 보며 이 책을 준비하는 데 도움을 준 모든 보안프로젝트 멤버들에게 고마움을 전한다.

지은이_**조승현**

보안을 공부하는 학생들에게 어떤 도구를 이용하는지 물어본 적이 있다. 대부분 버프스위트와 기타 잘 알려진 도구들을 사용한다고 답변했지만 버프스위트를 단순 프락시 도구로만 알고 있거나 함께 포함된 다른 도구들을 제대로 활용하지 못하고 있었다. 학생들이 이러한 답변을 할 수밖에 없는 이유는 국내에서 버프스위트에 대한 자료가 많지 않은 것도 있지만, 한국어로 된 대부분 자료는 프락시 도구를 주 내용으로 장식하고 있고 나머지 도구는 기본적인 개념으로만 채워 놓고 있어서 제대로 활용하기에 어려움이 있다는 것이다.

이 책을 통해 누군가와 나의 작은 지식을 나눌 수 있다는 것에 감사하고 참 기쁘다. 혼자가 아닌 좋은 사람들과 같이 완성했다는 것도 나에게는 큰 의미가 있었다. 또한, 많은 분께 감사하다. 먼저 나를 이끌어주고 집필의 방향을 제시해준 조정원 형님께 감사드린다. 항상 많은 조언을 해주시고 지켜봐 주시는 덕에 많은 것들을 할 수 있었던 것 같다. 그리고 함께 집필에 참여하고, 꼼꼼하게 챙겨준 명근이에게도 고마운 마음뿐이다. 부족한 나를 옆에서 지켜봐 주시고 항상 지원해주신 전영재 대표님께도 감사하다.

이 책이 나오기까지 항상 챙겨주시고 지켜봐 주신 부모님께 감사드린다. 또한, 같이 공부하면서 좋은 일, 불편한 일 등을 함께 봐온 광수, 재형이에게도 고마운 마음을 전하고 싶다.

사람들은 실생활에서 대부분 정보를 웹을 통해 얻는다. 이동 중에는 모바일 단말을 이용하여 정보를 보고 있지만, 그 안에서는 웹 애플리케이션이나 관련 서버들을 통해 데이터를 받아온다.

모의해킹 업무에서 웹 애플리케이션 취약점 진단 비중이 제일 높고, 가장 많이 사용하는 도구는 클라이언트 프락시 도구다. 개인 단말에서 서버에 전달하는 요청값과 서버에서 개인 단말로 전달하는 값을 분석하는 것은 매우 중요하다. 거대한 사막에서 동전을 찾아내듯이 파라미터 값 하나에 의해 어떻게 서버가 반응하는지 분석해야 한다. 중간에 데이터를 수정하고 반복되는 작업을 자동으로 한다거나 응답 값을 항목별로 상세히 분석하기 위한 모든 기능이 버프스위트라는 도구에 포함되어 있다.

이 책에서는 크게 매뉴얼과 활용법을 다루고 있다. Part 2에서는 매뉴얼 관점에서 각 옵션의 기능들을 살펴봄으로써 상황에 따라 어떻게 사용하는지를 살펴본다. 실습 환경에서 각 메뉴를 클릭하면서 반응을 살펴보면 재미있게 따라갈 수 있다. Part 3에서는 웹 애플리케이션 환경에서 어떻게 진단할 수 있는지 단계적으로 살펴본다. 많은 강의 경험을 토대로 입문자들도 충분히 따라올 수 있게 설명하였다.

이 책은 최대한 실무적인 관점에서 살펴보려고 노력하였다. 기능만 살피는 것이 아니라 쉽게 구축할 수 있는 테스트 환경에서 어떻게 활용할 수 있는지 자세히 알아보고, 조금이라도 업무를 빠르고 정확하게 할 수 있는 것이라면 옵션 하나라도 놓치지 않고 모두 다루었다. 또한, 버프스위트에서 활용할 수 있는 몇 가지 플러그인 기능을 설명하였다. 이 책을 읽고 플러그인 활용에 관심이 많다면 플러그인 개발도 추가로 연구하길 추천한다.

버프스위트에 숨겨진 기능들을 하나씩 살펴보면서 앞으로 모의해킹 실무를 할 때도 유용하게 활용할 수 있기를 바란다. 책에서는 앞에서 제시했던 문제들을 해결하기 위해 도구마다 어떻게 사용할 것인지 설명하고 이를 업무에 어떻게 적용할 것인지에 대

한 내용을 담고 있다. 버프스위트가 비록 무료 버전과 유료 버전으로 구분되어 기능 제한을 두긴 했지만 무료 버전만으로도 많은 테스트를 수행할 수 있다는 점에서 공부하는 학생이나 담당자들도 요긴하게 활용할 수 있으리라 생각한다.

이 책의 구성

이 책은 모의해킹 분야에 관심이 있는 입문자를 대상으로 구성하였다.

Part 1 '버프스위트 알아보기'에서는 버프스위트를 설치하고 테스트 환경을 구축한다.

Part 2 '버프스위트 기본 기능 활용'에서는 버프스위트의 사용법을 자세히 설명하고 버프스위트 플러그인을 활용하여 다양한 취약점을 분석할 수 있는 환경을 소개한다.

Part 3장 '버프스위트를 활용한 웹 모의해킹'에서는 웹 애플리케이션 취약점 진단에 대한 실질적인 이론과 취약점의 원리를 파악하고 직접 실습함으로써 해당 취약점에 대한 공격 방법과 대응 방안을 수립할 수 있는 능력을 길러 준다.

이 책의 대상 독자

이 책은 버프스위트 매뉴얼과 활용법, 항목별 취약점, 대응 방안에 대해 다룬 책이다. 다음 독자에게 이 책을 추천한다.

- 모의해킹 컨설턴트 진로를 선택한 독자
- 웹 애플리케이션 취약점 분석에 대해 궁금한 독자
- 버프스위트의 자세한 활용법에 대해 궁금한 독자

이 책의 특징

모의해킹 컨설턴트로 진로를 잡고 공부하는 학생이라면 이 책을 통하여 웹 애플리케이션 취약점 진단과 그 대응법 등 실무를 간접적으로 경험하고 알아볼 수 있으며 모의

해킹 컨설턴트로서의 기초 능력을 기를 수 있다. 모의해킹 실무자라면 미처 알지 못했던 버프스위트의 다양한 활용법을 습득하여 기술적인 능력에 도움을 줄 뿐 아니라 취약점에 대한 원리 파악을 통하여 모의해킹 시나리오를 수립하는 데 도움을 줄 수 있다. 이외에 서비스 관리자에게는 보안 사고를 예방할 수 있는 능력을 길러 주며 사고 발생 시 대응 방안을 수립하는 데 도움을 줄 것이다.

주의할 점

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

한빛 리얼타임

한빛 리얼타임은 IT 개발자를 위한 전자책입니다.

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 나가겠습니다.

차례

Part 1

버프스위트 알아보기

Part 1에서는 버프스위트Burp Suite의 상세한 기능을 다루기에 앞서 버프스위트가 무엇이고, 어떤 기능이 있는지, 버프스위트를 효과적으로 활용하는 데 필요한 환경은 무엇인지를 설명하겠다. Part 1은 Part 2부터 소개할 버프스위트의 기본 기능과 Part 3의 웹 모의해킹 실습을 위해서 꼭 필요한 내용이므로 이를 바탕으로 환경을 잘 구축하여 실습에 어려움이 없길 바란다.

chapter 1

버프스위트 개요

버프스위트는 PortSwigger[01]사에서 만든 웹 애플리케이션의 취약점 진단(테스트)을 수행하기 위한 통합 플랫폼이다. 버프스위트는 웹 애플리케이션, 모바일 서비스 등을 대상으로 진단 중간에 만날 수 있는 모든 환경 작업을 수행하기 위한 여러 가지 도구를 포함한다. 사용자는 자동화된 기술과 수동적인 방법을 결합하여 진단을 더 빠르고 효율적으로 진행할 수 있다. 또한, 사용자가 명확하게 알 수 있는 결과물을 제공한다.

버프스위트는 실제적인 웹 테스트를 수행하기 위한 Web Proxy Server, Web Spider, Intruder, Repeater 등으로 구성되어 있고, 실무 모의해킹 진단에서도 버프스위트의 기능을 활용하여 많은 작업을 수행한다.

하지만 모의해킹(Penetration Test)를 수행할 때 환경에 따라 수동으로 진단해야 하는 상황이 많기 때문에 프락시 도구만 사용하는 경우가 있다. 이 책을 통하여 다른 도구도 접해 보고 해당 도구가 어떤 영향을 주는지 충분히 테스트한 후에 업무에 활용하기 바란다.

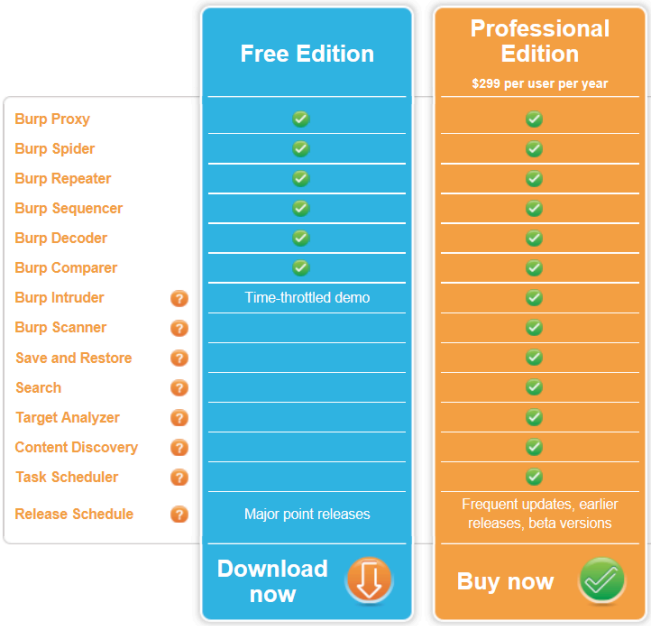
버프스위트에는 진단 대상 시스템에 영향을 주는 기능이 포함되어 있어서 실 서비스에 자동 프로세스를 적용할 때 주의해야 한다. 기능을 활용하기 전에 테스트를 충분히 한 뒤 적용하기 바란다(이는 다른 자동 진단 도구를 활용할 때도 마찬가지다).

01 http://portswigger.net/

1.1 버프스위트 설치

버프스위트는 PostSwigger 홈페이지[02]에서 다운로드하는데, 무료 버전Free Edition과 유료 버전Professional Edition, 전문가 버전으로 나누어져 있다. 무료 버전과 유료 버전은 몇 가지 기능의 차이를 제외하고 동일하다. 이 책에서는 무료 버전을 기준으로 작성하였으며 스캐너Scanner 기능을 포함한 일부 내용만 유료 버전을 기준으로 작성하였다. 유료 버전을 기준으로 작성한 것은 별도로 표기하겠다.

그림 1-1 버프스위트 다운로드



유료 버전에서 추가로 사용할 수 있는 기능은 다음과 같으며 각 기능 상세 설명은 'Part 2 버프스위트 기본 기능 활용'에서 설명한다.

02 http://portswigger.net/burp/download.html

표 1-1 버프스위트 무료 버전과 유료 버전 비교

기능	내용
Burp Intruder	무료 버전에서는 기본으로 Intruder 도구가 활성화되어 있지만 일부 기능은 제한되어 있다. 유료 버전에서는 공격 수행 때 사용자 임의대로 옵션을 설정하여 수행할 수 있다.
Burp Scanner	무료 버전에서 Scanner는 비활성화되어 있다. 유료 버전에서는 이 기능을 이용하여 웹 애플리케이션에 다량의 패턴을 삽입하여 자동으로 취약점 검색을 수행할 수 있다.
Save and Restore	수행했던 항목을 저장하고 다시 복구하여 이용할 수 있다. 대표적으로 프락시 기록, Target 탭의 Site map 등을 저장하고 복구 마법사를 이용하여 상태를 복구시켜 사용할 수 있다.
Search	검색(Search) 기능을 이용하여 버프스위트에서 나온 결과물을 검색할 수 있다. 간단한 텍스트부터 주석, 스크립트, URL 등을 검색할 수 있으며 세부적인 옵션도 제공한다.
Target Analyzer	대상 웹 애플리케이션 분석을 진행하고 결과를 출력한다. 동적 URL, 정적 URL을 구분하여 리스트가 형성되고 URL에 포함된 매개변수 사용 횟수 등을 분석한다.
Content Discovery	콘텐츠를 브라우징하거나 Spider 기능을 통하여 보이는 콘텐츠 이외에 연결되지 않은 콘텐츠의 상관관계를 출력한다.
Task Scheduler	자동으로 테스트를 수행하는 작업 스케줄을 설정할 수 있다. 이 기능을 이용하여 원하는 시간대에 원하는 작업을 자동으로 수행하거나 중단하도록 예약할 수 있다.
Release Schedule	지속적인 업데이트를 수행한다.

1.2 버프스위트 실행

버프스위트는 독립적인 자바 실행 파일로 배포된 자바 응용프로그램으로서 확장자는 JAR이다. 버프스위트의 JAR 파일은 JRE[Java Runtime Environment]에서 실행되기 때문에 자바가 설치되어야 한다. 자바의 설치 여부는 각 운영체제 터미널(cmd.exe)에서 '`java  - version`' 명령으로 확인할 수 있다.

[그림 1-2]는 윈도우의 명령 프롬프트에서 자바 버전 정보를 출력한 모습이다. 자바가 설치되어 있지 않다면 오라클 홈페이지에서 JRE를 다운로드한 후 설치하

고,[03] 자바 1.6 버전 이상을 설치해야 한다.

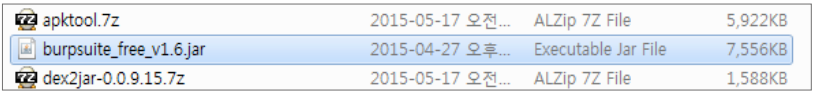
그림 1-2 자바 버전 확인

```
C:₩>java -version
java version "1.8.0_40"
Java(TM) SE Runtime Environment (build 1.8.0_40-b25)
Java HotSpot(TM) Client VM (build 25.40-b25, mixed mode)

C:₩>_
```

자바 설치 확인이 끝났으면 다운로드한 JAR 파일을 더블 클릭하여 버프스위트를 실행한다. 명령어 라인Command Line에서 실행하는 경우 버프스위트를 실행하는 시스템에 적합한 메모리를 할당하도록 제어할 수 있다. 해당 명령은 '`java -jar -Xmx1024m /path/burp.jar`'와 같다. 이 명령은 메모리를 1024MB만큼 할당하고 해당 파일의 위치는 /path/burp.jar라는 의미다. 메모리 할당은 개인 시스템에 맞추어 변경한다.

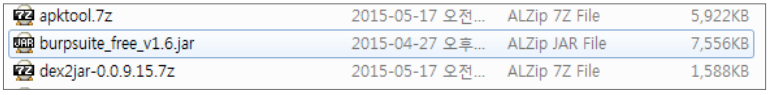
그림 1-3 .jar 파일을 더블 클릭하여 실행



NOTE .jar 파일이 다른 프로그램과 연결되어 있다면?

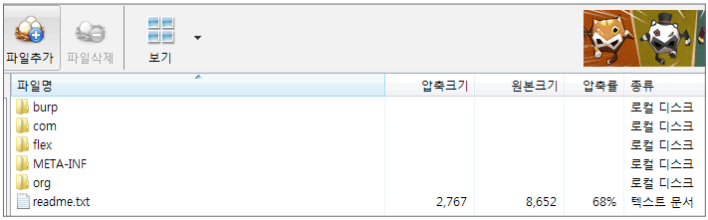
.jar 파일은 압축 형태의 파일이다 보니 압축 프로그램을 업데이트하거나 새로 설치하면 확장자를 기준으로 [그림 1-4]와 같이 압축 프로그램에 연결한다. .jar 파일을 클릭하면 [그림 1-5]와 같이 압축 해제 화면으로 넘어간다.

그림 1-4 jar 파일이 압축 프로그램과 연결



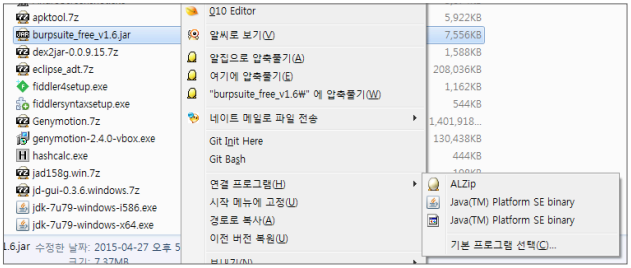
03 자바 다운로드 : http://www.oracle.com/technetwork/java/javase/downloads/index.html

그림 1-5 .jar 파일이 압축 프로그램에서 해제될 때



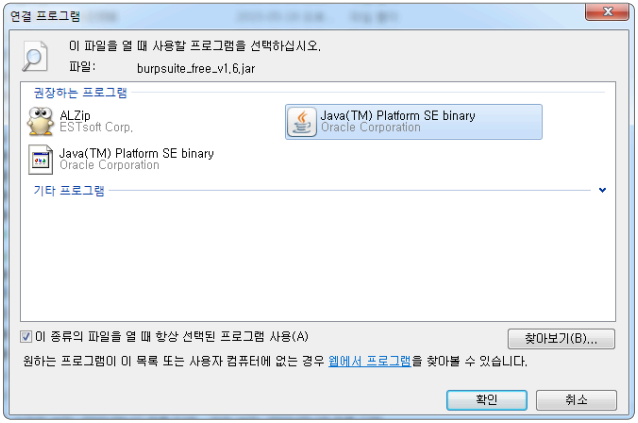
이 경우에는 콘솔에서 명령어로 실행할 수 있지만 연결 프로그램을 바꿔 놓으면 더블 클릭으로 간편하게 실행할 수 있다. .jar 파일에 커서를 두고 Shift 키를 누른 상태에서 마우스 오른쪽 버튼을 클릭하면 메뉴가 나온다. 이 메뉴에서 [그림 1-6]과 같이 [연결 프로그램 → 기본 프로그램 선택]을 클릭한다.

그림 1-6 .jar 파일 연결 프로그램



[그림 1-7]과 같이 '이 종류의 파일을 열 때 항상 선택된 프로그램 사용'을 체크하고 'Java(TM) Platform SE binary' 프로그램을 선택한 뒤 [확인] 버튼을 클릭한다.

그림 1-7 .jar 파일을 JSE에 연결

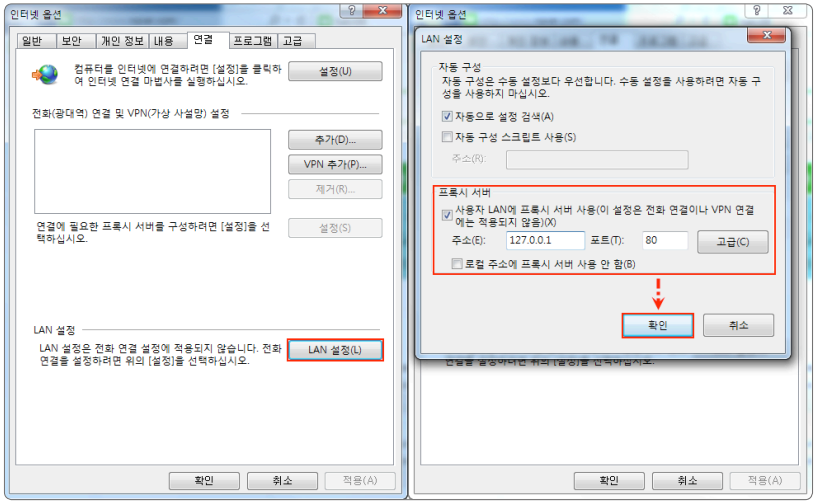


1.3 프락시 서버 설정

버프스위트의 기능을 사용하려면 우선 브라우저의 프락시 기능을 설정해야 한다. 사용자가 많은 브라우저로는 인터넷 익스플로러Internet Explorer, 크롬Chrome, 파이어폭스Firefox가 있다. 각 브라우저의 서버 설정은 각각 다음에 명시한 인터넷 옵션 경로를 따라 하면 된다.

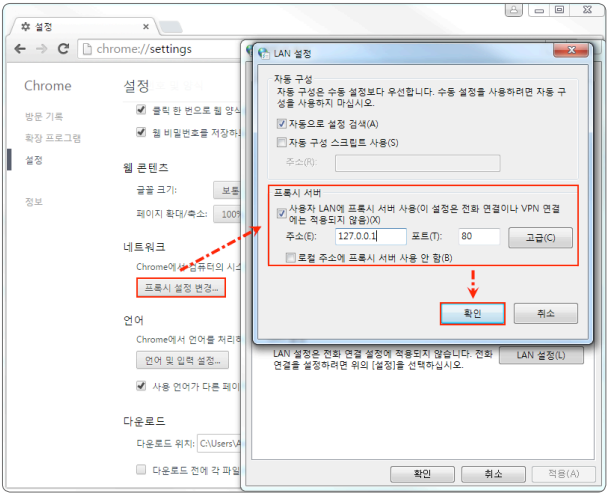
인터넷 익스플로러는 [도구 → 인터넷 옵션 → LAN 설정 → 프락시 서버]에서 설정한다.

그림 1-8 인터넷 익스플로러 프락시 서버 설정



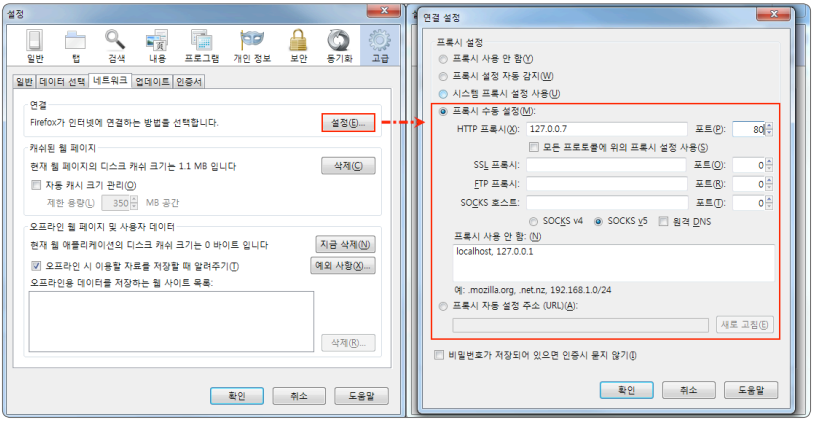
크롬은 [설정 → 고급 설정 표시 → 프락시 설정 변경 → 연결 → LAN 설정 → 프락시 서버]에서 설정한다.

그림 1-9 크롬 브라우저 프락시 서버 설정



파이어폭스는 [옵션 → 네트워크 → 설정 → 프락시 수동 설정]에서 설정한다.

그림 1-10 파이어폭스 브라우저 프락시 서버 설정

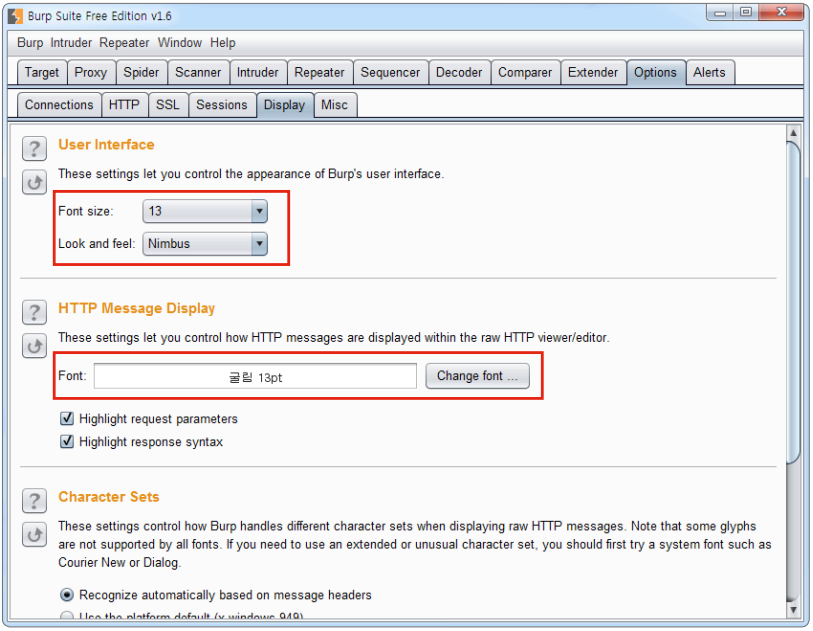


1.4 버프스위트 디스플레이 설정

버프스위트는 기본으로 단말과 서버 간의 데이터를 영문으로만 지원하므로 HTML 내에 한글로 작성한 내용은 모두 깨진다. 또한, 버프스위트 사용자 화면이

해상도에 따라 너무 작게 보이기도 한다. 이러한 경우에 [Options → Display]에서 [그림 1-11]처럼 설정한다. [User Interface사용자 인터페이스]의 크기와 형태를 수정하고 [HTTP Message DisplayHTTP 메시지 화면]은 [Chage font...]를 클릭한 뒤 지원되는 한글 폰트를 선택한다. 사용자 화면은 버프스위트를 종료한 뒤에 다시 실행해야 설정한 부분이 적용된다.

그림 1-12 버프스위트 디스플레이 설정



chapter 3

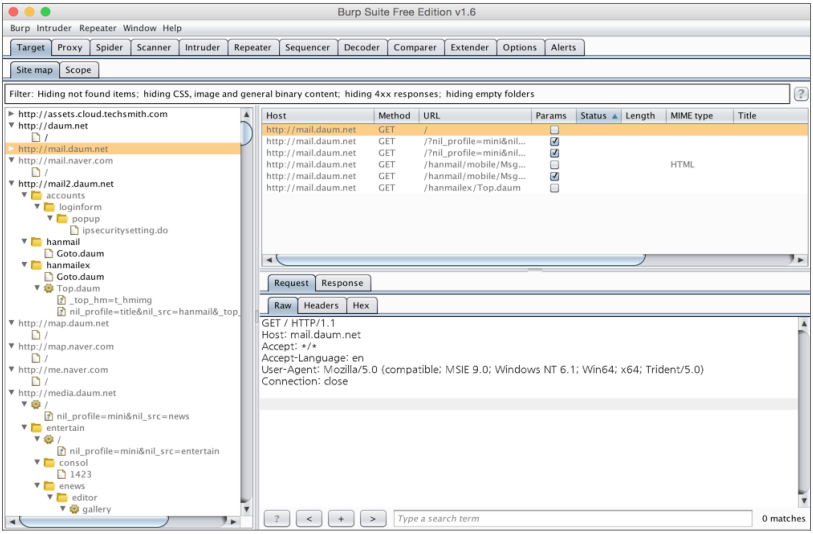
Target

버프스위트의 Target을 통하여 대상 애플리케이션이 제공하는 콘텐츠와 기능을 살펴볼 수 있는데, 이 기능은 애플리케이션 진단 과정에서 중요한 역할을 한다. Target에서는 다음과 같은 방법을 이용하여 효율적인 테스트를 진행할 수 있다. '1.3 프락시 서버 설정'에서 설명했듯이 브라우저에서 프락시 설정을 해야 방문한 사이트가 Target에 등록된다.

애플리케이션 수동 매핑

프락시를 통하여 요청한 항목과 애플리케이션의 응답으로부터 추측할 수 있는 콘텐츠는 Target의 Site map 항목에 추가된다. 기본적으로 눈에 보이는 모든 콘텐츠가 완벽히 기록되기 때문에 대상 애플리케이션 구조를 파악할 수 있다. 대상 애플리케이션을 직접 요청하여 수동으로 매핑하는 방법은 진단 범위 이외의 대상을 만나는 경우 회피를 하거나 임의로 제거할 수 있어서 자동으로 매핑하는 방법보다 안전하고 효과적이다.

그림 3-1 애플리케이션 매핑 화면



대상 범위 지정

애플리케이션 매핑이 완료되면 Site map에 기록된 항목 중 원하는 항목만 표시하도록 설정하고 추가로 테스트를 진행할 수 있다.

요청하지 않은 항목 처리

수동 매핑을 진행하면 원하지 않는 항목도 Site map 리스트에 추가된다. 직접 사이트를 방문하여 추가로 생성되는 항목은 회색으로 표시되며 이러한 항목을 필터링으로 숨길 수 있다.

숨겨진 콘텐츠 확인

수동 매핑으로 알려진 콘텐츠에 대한 매핑을 완료했다면 자동화된 작업을 통하여 사용자의 눈에 보이지 않는 콘텐츠도 항목에 추가할 수 있다.

공격 대상 분석

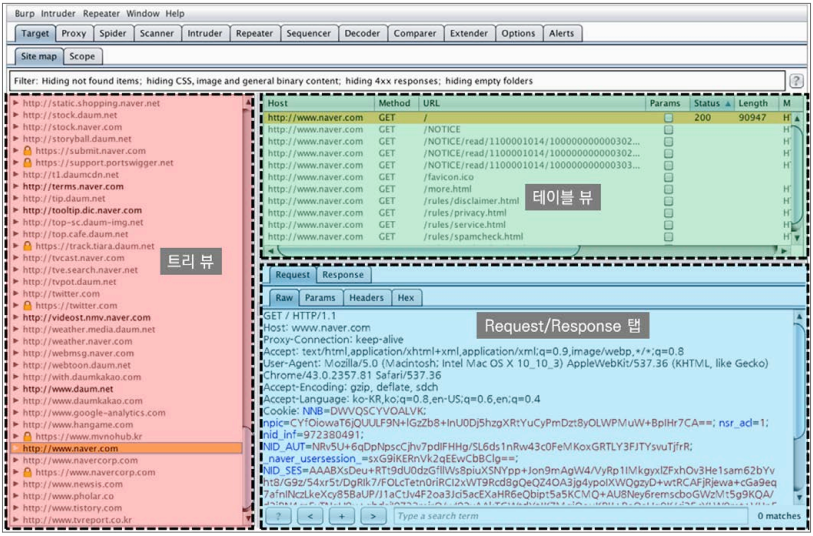
분석 도구를 이용하면 대상이 매핑되어 Site map에 표시되는 애플리케이션 항

목 중 공격에 취약한 부분을 찾아낼 수 있다. 분석 도구는 기본으로 Site map을 통하여 지원한다. Target의 Site map에 표시되는 항목을 바탕으로 대상 애플리케이션 정보를 수집하고 앞에서 제시한 기능을 수행할 수 있다. 또한, Site map에 표시되는 항목을 선택하여 버프스위트에서 제공하는 도구와 연계하여 테스트를 진행할 수 있으며 외부 도구와 연계하여 공격을 수행하는 확장 기능을 사용할 수 있다.

Site map

Site map은 Target에서 가장 핵심적인 부분으로 대상 애플리케이션의 정보를 보여 주고 개별적인 항목 요청과 응답을 출력한다. 또한, 대상 애플리케이션뿐만 아니라 프락시를 설정한 후 사용자가 이용하는 모든 항목의 정보를 기록하고 출력한다.

그림 3-2 Site map 기능



Site map은 크게 트리 뷰(Tree View), 테이블 뷰(Table View), Request/Response 탭 세 부분으로 나뉘는데, 각 영역의 기능은 다음과 같다.

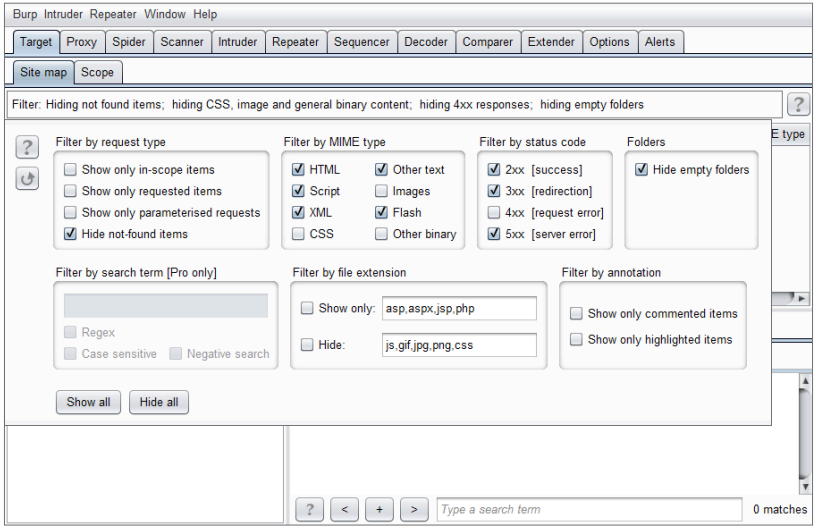
- **트리 뷰** URL을 트리 형태로 표현한다. URL은 도메인, 디렉터리, 파일과 매개변수 요청을 포함하여 세분화되어 있다.
- **테이블 뷰** 트리 뷰에서 선택한 항목의 세부적인 내용을 출력한다. Host, Method, URL, 상태 코드 등으로 구성되어 있다.
- **Request/Response 탭** 테이블 뷰에서 선택한 항목의 요청과 응답 결과를 출력한다. 탭에 표시되는 내용은 편집할 수 있는 형태로 제공된다.

버프스위트로 수집한 정보는 Site map에 기록한다. 즉, 모든 작업은 Site map에서 시작하므로 Site map을 잘 활용하면 효율적인 진단을 시작할 수 있다.

Site map → Display Filter

애플리케이션 정보를 수집하다 보면 진단 대상과 관련한 항목이 많이 추가되고 그 중에서는 관련 없는 항목도 쌓인다. Target에서는 [그림 3-3]과 같이 쌓인 항목을 필터링하여 작업에 필요한 항목만 표시하게 하는 Display Filter를 제공한다.

그림 3-3 Display Filter의 세부 항목

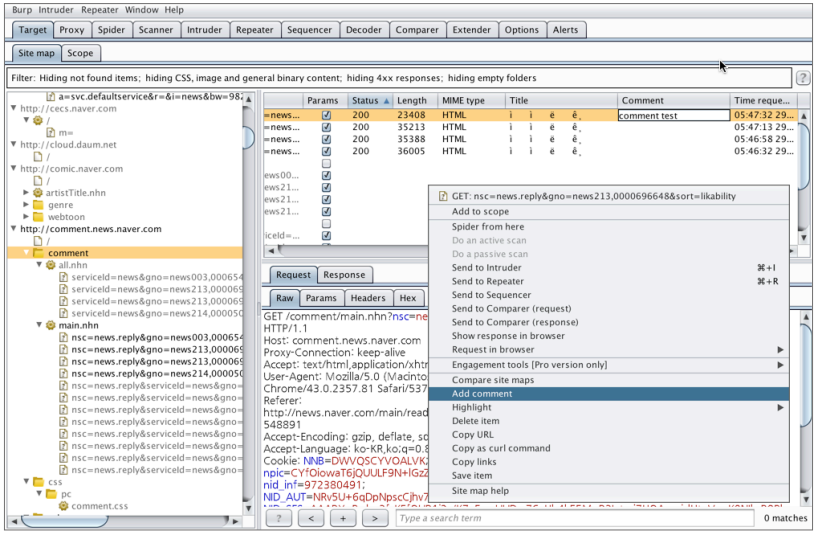


Display Filter는 Site map 상단에 있으며 Filter 바를 클릭하면 세부 항목을 편집할 수 있는 옵션 창이 나타난다. 세부 항목에서는 요청 타입(Request Type),

MIME 타입(MIME Type), 상태 코드(Status Code), 폴더 옵션(Folders), 검색어 지정(Search Term), 파일 확장자 지정(File Extension), Comment와 Highlight 옵션(Annotation)으로 일치하거나 일치하지 않는 항목만 구분하여 내용을 표시할 수 있다. 이 기능은 복잡하거나 큰 규모의 애플리케이션을 대상으로 테스트를 진행할 때 유용하다. Display Filter를 이용하여 숨긴 항목은 삭제한 것이 아니라 일시적으로 숨긴 것이므로 설정을 해제하면 숨겼던 항목이 모두 표시된다.

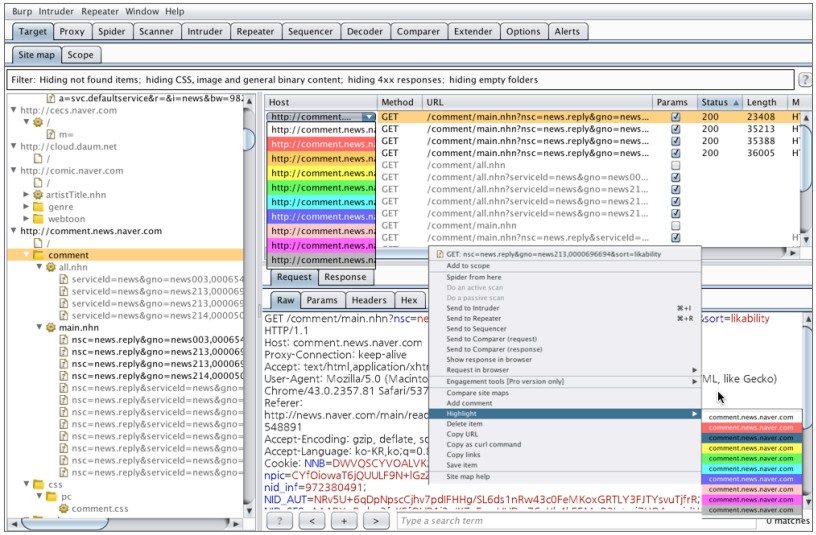
앞에서 Comment와 Highlight 옵션으로도 필터링할 수 있다고 했는데, 해당 옵션을 적용하려면 사용자가 Comment나 Highlight를 추가해야 한다. 방법은 다음과 같다. Comment는 [그림 3-4]와 같이 테이블 뷰에서 보이는 항목을 선택하여 Comment 칼럼에서 추가하거나 Context 메뉴의 'Add comment'를 선택하여 추가할 수 있다.

그림 3-4 Comment 추가



Highlight는 [그림 3-5]와 같이 Comment와 마찬가지로 테이블 뷰의 항목에서 Host 칼럼의 드롭다운 메뉴로 추가하거나 Context 메뉴의 'Highlight'를 선택하여 추가할 수 있다.

그림 3-5 Highlight 추가



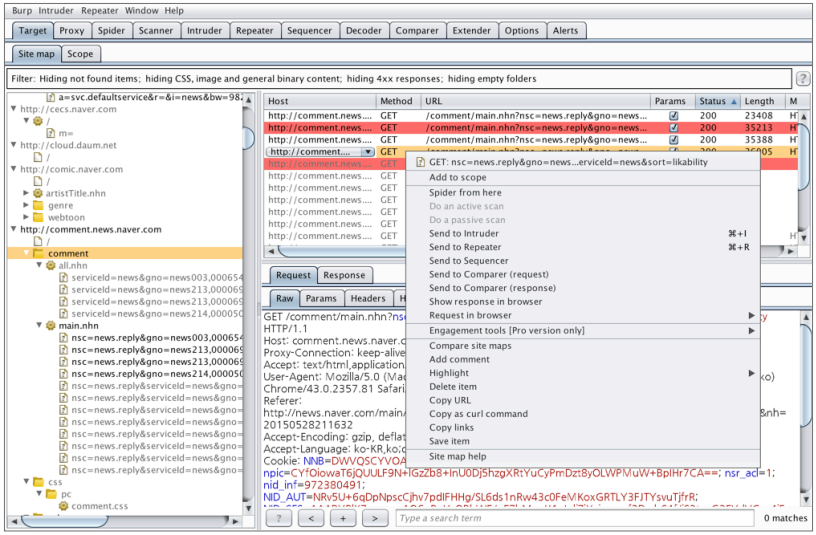
이와 같이 필요한 항목을 구분하여 테스트를 진행하고 필요하지 않은 항목을 숨기면 작업을 더 효율적으로 진행할 수 있다.

Context 메뉴

지금까지 Target의 Site map에 수집된 정보를 설명하고 필터링하는 방법을 설명했다. Site map에서는 앞에서 설명한 기능 외에도 다른 도구와의 연계 기능을 이용할 수 있다. 각 항목에서 마우스 오른쪽 버튼을 클릭하면 Context 메뉴가 나오는데, 이를 통하여 연계 기능을 이용할 수 있다.

Context 메뉴를 통하여 선택된 대상으로 특정 공격을 하거나 추가적인 정보를 수집하는 등의 제어가 가능하다. 이때 사용할 수 있는 옵션은 Context 메뉴가 호출된 위치나 선택된 항목의 형태에 따라 달라진다. [그림 3-6]은 Site map의 테이블 뷰에서 Context 메뉴를 호출한 화면이다.

그림 3-6 Target의 Context 메뉴



Context 메뉴의 기본 기능은 [표 3-1]과 같다.

표 3-1 Context 메뉴의 기능

종류	설명
Add to scope/ Remove from scope	선택한 항목을 필터링을 위한 목록에 추가하거나 삭제한다. 추가한 항목은 Target의 Scope 탭에서 설정할 수 있으며 필터링을 이용하는 경우 적용된다.
Scan/Spider/Send to	선택한 항목을 대상으로 추가적인 공격을 시도하거나 분석하기 위해 다른 버프스위트에 정보를 전달하여 작업을 수행할 수 있다.
Show request/response in browser	버프스위트에서 제공하는 Burp renderer를 사용하여 표시하지 못 하는 항목이 있을 경우 해당 항목을 브라우저에서 렌더링하도록 한다.
Engagement tools	선택한 항목과 관련하여 검색, 분석, 코드 생성, 트래픽 유발 등의 기능을 사용할 수 있다. 이 기능은 유료 버전에서만 가능하다.

Target은 버프스위트를 이용할 때 가장 많이 사용한다. 대상 애플리케이션 정보가 모두 기록되기 때문에 취약한 부분을 찾아 공격을 수행하기 전에 반드시 정리가 잘 되어 있어야 한다. 앞에서 소개한 Target의 기능을 잘 활용하면 정보 수집과 추가 공격을 수행하기 좋은 환경으로 만들 수 있다.