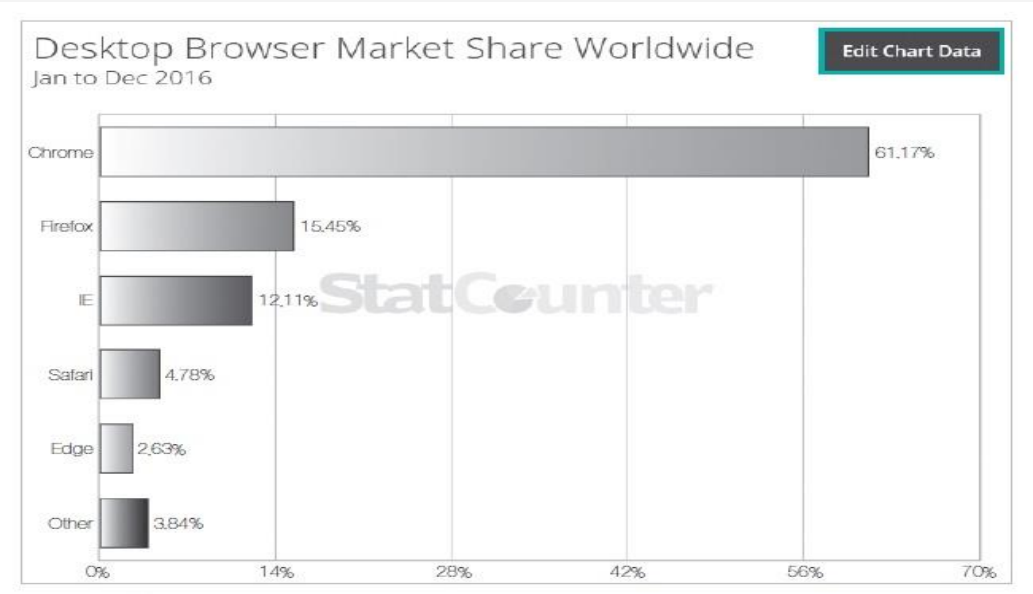
1 웹 브라우저의 종류와 기능

1 웹 브라우저

- 인터넷 세상을 탐험(브라우징)할 때 사용하는 필수적인 도구(웹 서버 ↔ 웹 브라우저)
- 웹 브라우저의 종류
  - 마이크로소프트의 인터넷 익스플로러, 구글의 크롬, 모질라의 파이어폭스 등(익스플로러 vs. 크롬)

1 웹 브라우저

[웹 브라우저 사용 통계(2016년 , 데스크톱 기준)]



※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 인터넷 익스플로러

- 마이크로소프트에서 개발한 웹 브라우저 프로그램
- 1995년 8월 16일에 버전 1.0이 첫 선을 보인 후 지속적으로 발전하여 2017년 현재 버전 11까지 나옴 (운영체제에 포함시킴)

3 인터넷 익스플로러의 개발자 도구

- 버전 6 이상부터 '개발자 도구' 기능 내장
- 인터넷 익스플로러를 실행하고 [F12]를 누르거나
  오른쪽 상단의 설정 메뉴에서 [F12 개발자 도구] 클릭
- 가장 많이 사용하는 기능은 요소 찾기와 특정 값 찾기
  (소스 보기)

3 인터넷 익스플로러의 개발자 도구

[인터넷 익스플로러의 개발자 도구 실행 화면]

※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

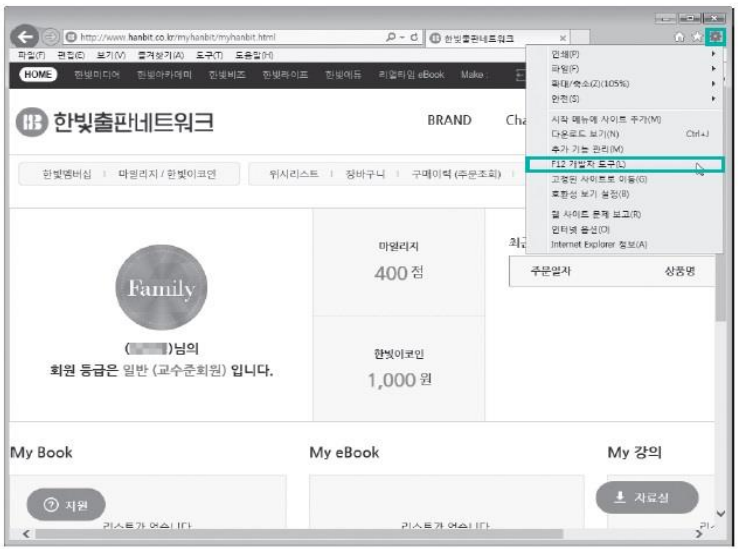
4 인터넷 익스플로러의 개발자 도구 실습하기

1 인터넷 익스플로러의 개발자 도구 실행

- 인터넷 익스플로러 실행 후 단축키 [F12]를 누르거나 브라우저 화면 오른쪽 상단에 있는 설정 메뉴에서 [F12 개발자 도구] 클릭

4 인터넷 익스플로러의 개발자 도구 실습하기

[인터넷 익스플로러의 개발자 도구 선택 화면]

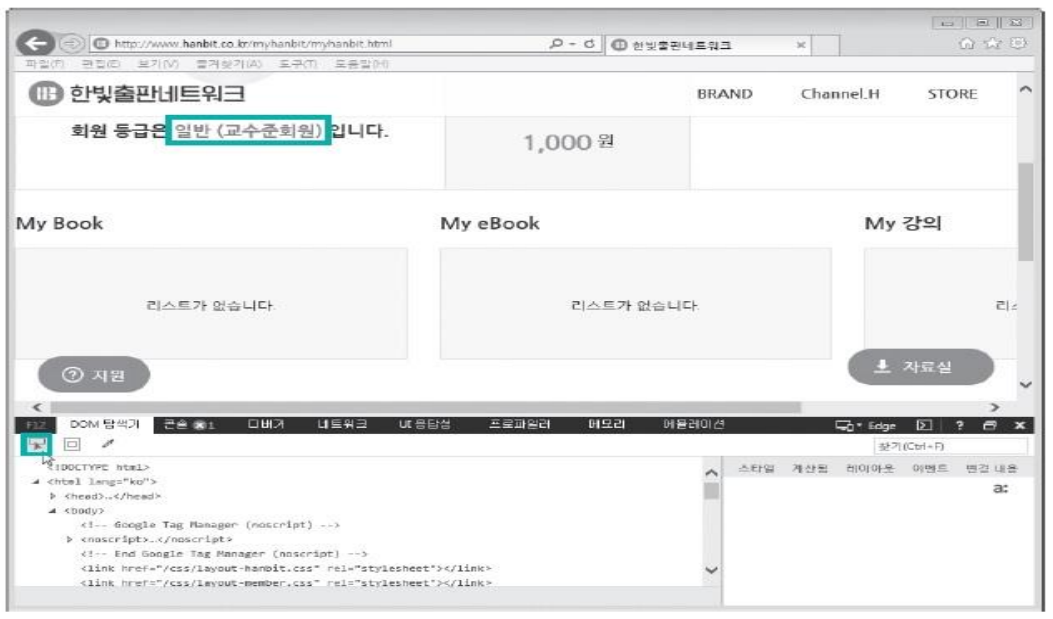


※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 인터넷 익스플로러의 개발자 도구 실습하기

2 웹 페이지의 특정 요소 식별

- 개발자 도구 화면에서 [DOM 탐색기] 메뉴의 〈요소 선택〉 아이콘 클릭



[인터넷 익스플로러의 [요소 선택] 메뉴 클릭]

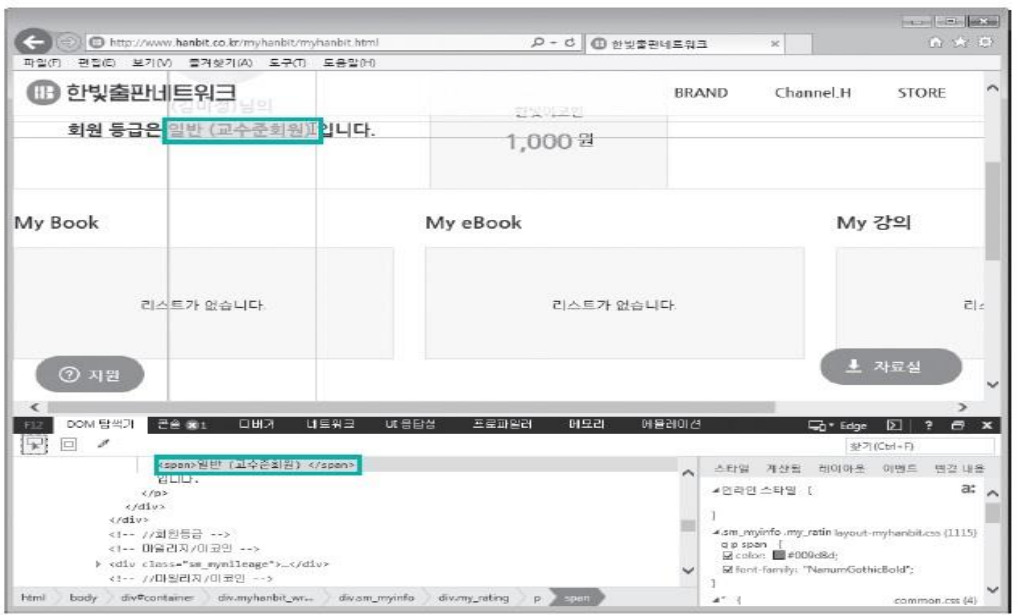
※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 인터넷 익스플로러의 개발자 도구 실습하기

2 웹 페이지의 특정 요소 식별

- 웹 페이지에서 '일반(교수준회원)' 부분에 마우스 포인터를 갖다 댄 후 박스가 생기면 클릭

[인터넷 익스플로러에서 특정 영역 선택]



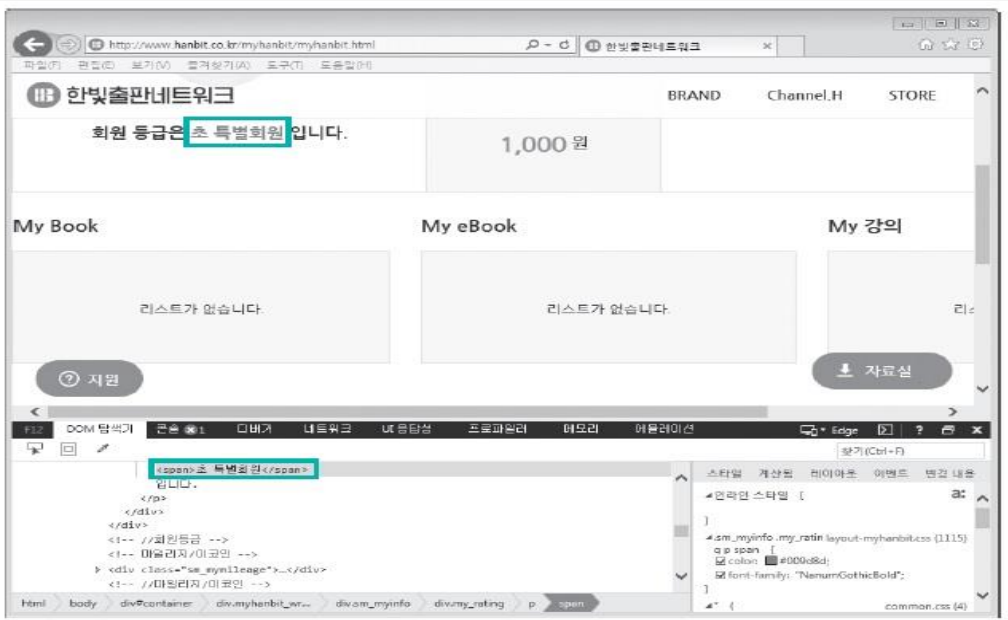
※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 인터넷 익스플로러의 개발자 도구 실습하기

3 웹 페이지의 데이터 변조

- 개발자 도구 화면에서 '일반(교수준회원)'을 '초 특별회원'으로 변경
- (실제 변경 아님)

[인터넷 익스플로러에서 특정 영역에서 데이터 수정]



※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

5 크롬

- 2008년 9월 2일에 공개된 구글에서 개발한 웹 브라우저
- 가장 많은 사용자를 보유한 웹 브라우저
  (메모리를 많이 먹지만 빠름)
- 2013년에는 버전 25, 2017년에는 버전 58 출시

5 크롬

크롬의 개발자 도구

- 브라우저 화면 오른쪽 상단의 설정 아이콘 클릭 후
  [도구 더보기]-[개발자 도구] 메뉴 선택

- 개발자 도구 화면의 왼쪽 상단에 있는
  〈Select an element in the page to inspect it〉
  아이콘을 클릭하고 웹 사이트의 특정 영역을 클릭하면
  해당 코드가 개발자 도구 화면에 나타남

5 크롬

크롬의 개발자 도구

[크롬의 [개발자 도구] 메뉴 클릭]

※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

6 파이어 폭스

- 모질라에서 개발한 웹 브라우저

6 파이어 폭스

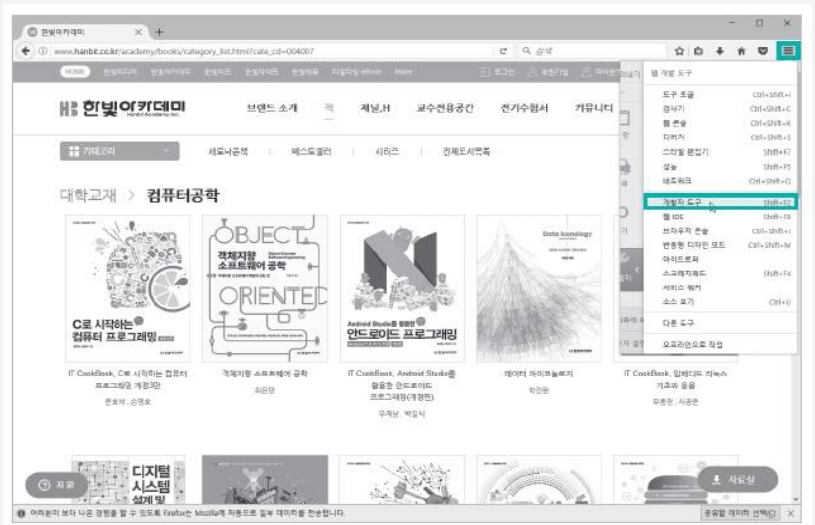
파이어 폭스의 개발자 도구

- 왼쪽 상단의 <메뉴 열기> 아이콘을 클릭 후 [개발자]-[개발자 도구] 메뉴 선택
- 개발자 도구 화면 왼쪽 상단의 <페이지에서 요소 고르기> 아이콘을 클릭하고 웹 페이지의 특정 영역을 선택하면 해당 영역에 대한 소스코드를 볼 수 있음

6 파이어 폭스

파이어 폭스의 개발자 도구

[파이어 폭스의
[개발자 도구] 메뉴 클릭]

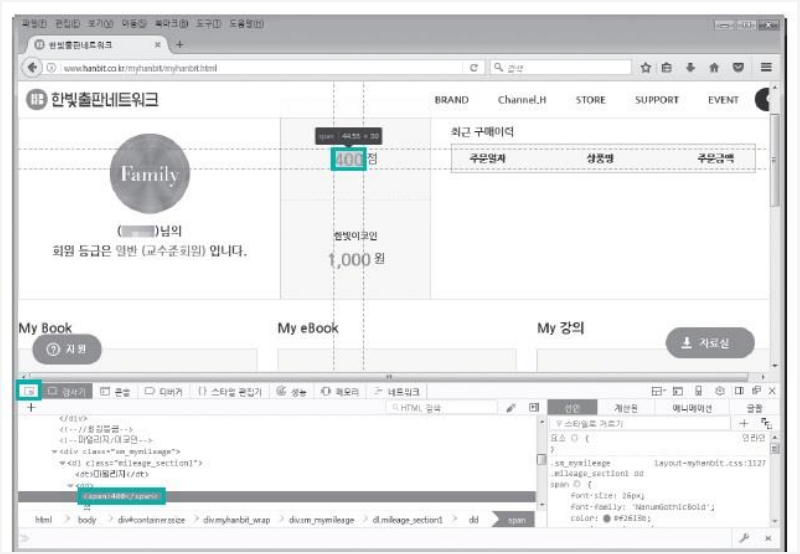


※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

6 파이어 폭스

파이어 폭스의 개발자 도구

[파이어 폭스에서
특정 영역의 데이터 수정]

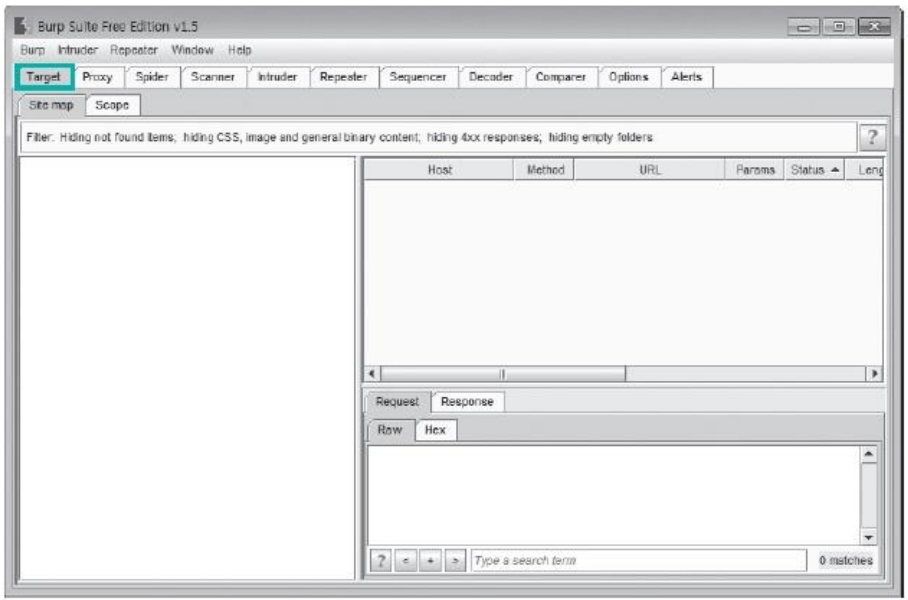


※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 웹 애플리케이션 프록시 프로그램

1 Target 기능

- [Target] 탭을 선택하면
  Burp Suite로 탐색한 사이트에
  대한 정보를 확인할 수 있음
  (웹 사이트의 구조를 분석할 때 유용)
  (탐색 정보)



[Burp Suite의 [Target] 탭]

※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 Burp Suite의 Target 기능 연습하기

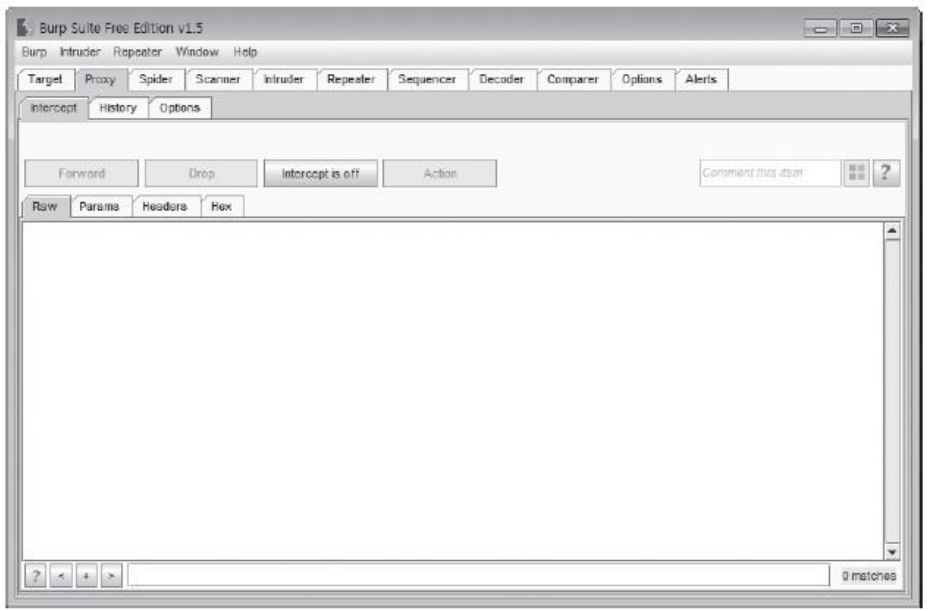
1 Burp Suite 실행

- Burp Suite를 실행하고 브라우저의 프록시 기능을 활성화

2 Burp Suite의 Target 기능 연습하기

2 프록시 기능 비활성화

- 구조를 분석하고 싶은 웹 사이트 접속
- Burp Suite의 [Proxy] 탭에서 <Intercept is on>을 클릭하여 <Intercept is off>로 변경



[프록시 기능 비활성화]

※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 Burp Suite의 Target 기능 연습하기

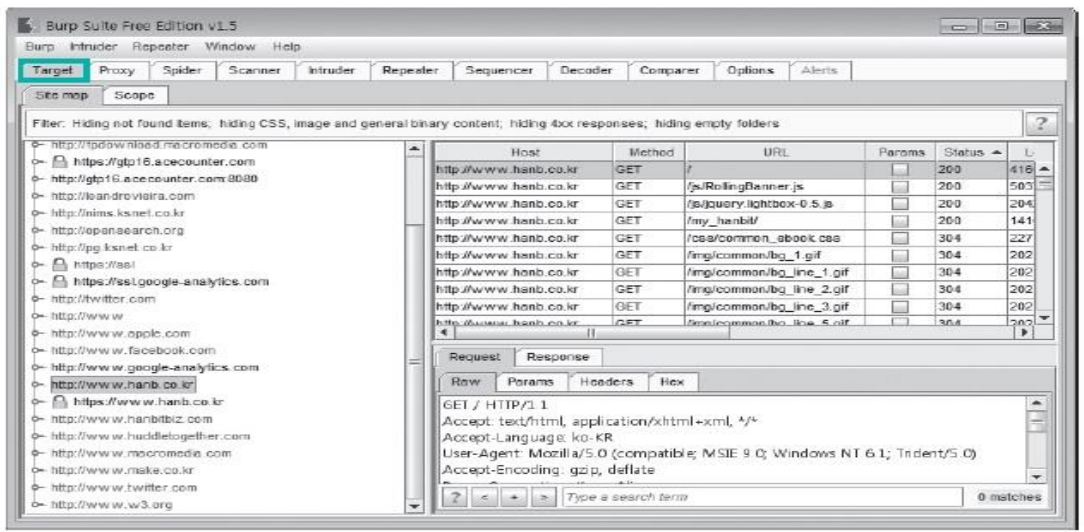
3 웹 사이트 탐색

- 웹 사이트의 메뉴를 가급적 모두 클릭해보고, 로그인도 시도

2 Burp Suite의 Target 기능 연습하기

4 [Target] 탭 확인

- [Target] 탭을 클릭하면 많은 웹 사이트가 목록화되어 있음 (탐색 정보)



[웹 사이트 탐색 후 [Target] 탭 화면]

※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 Burp Suite의 Target 기능 연습하기

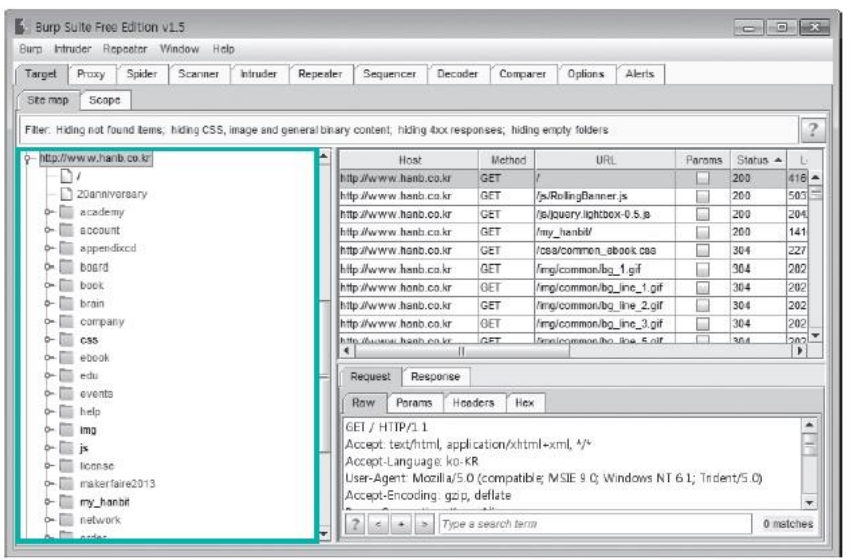
5 웹 사이트의 구조 확인

- [Target] 탭에서 분석을 원하는 웹 사이트를 선택하고 더블클릭이나 ▶ 클릭
- 특정 페이지를 클릭하면 오른쪽 화면에서 해당 페이지에 대한 HTTP 헤더와 Request, Response 정보를 상세히 확인할 수 있음

2 Burp Suite의 Target 기능 연습하기

5 웹 사이트의 구조 확인

[특정 웹 사이트의 디렉터리 구조 확인]

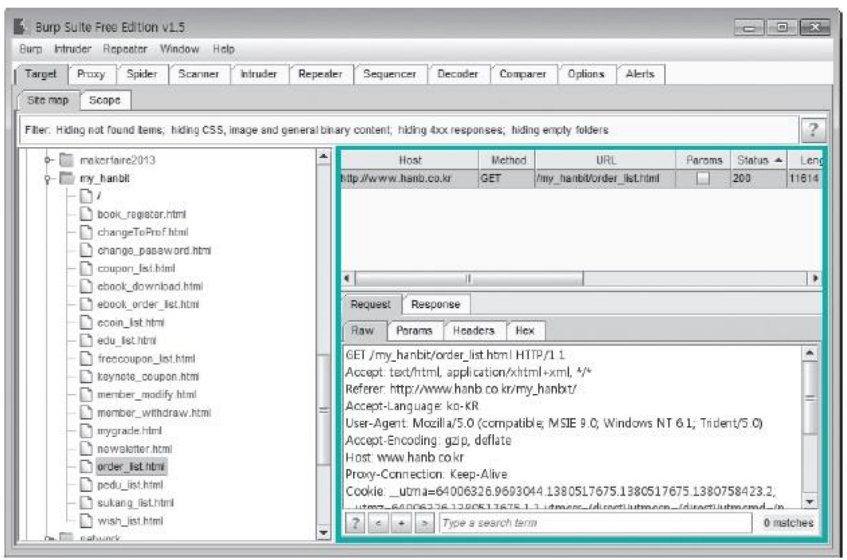


※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

2 Burp Suite의 Target 기능 연습하기

5 웹 사이트의 구조 확인

[특정 페이지의 정보 확인]



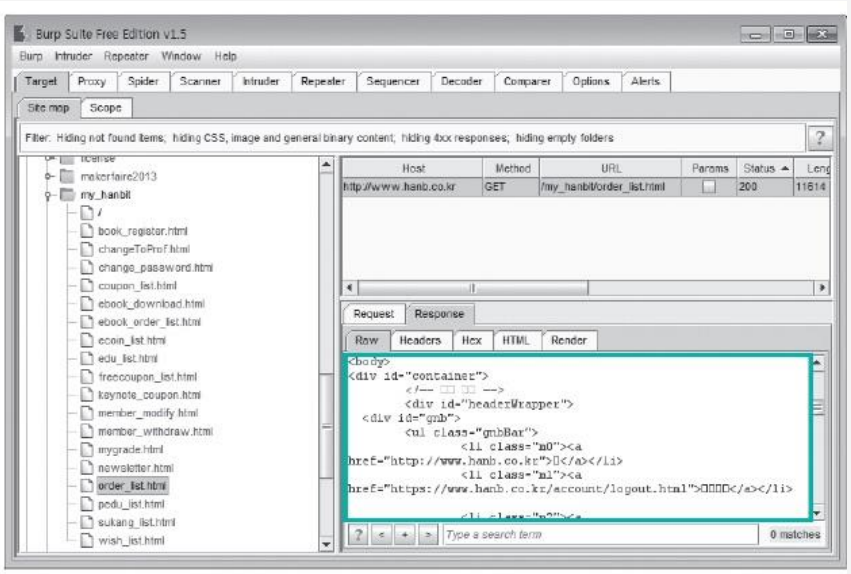
※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 Burp Suite의 Response에서 한글이 깨지는 문제 해결하기

- [Response] 탭을 보면 한글이 모두 '□'로 표시되어 있음
- [Options]-[Display] 탭 클릭 후
  HTTP Message Display 항목을 보면
  현재 사용 중인 폰트 정보를 확인할 수 있음

3 Burp Suite의 Response에서 한글이 깨지는 문제 해결하기

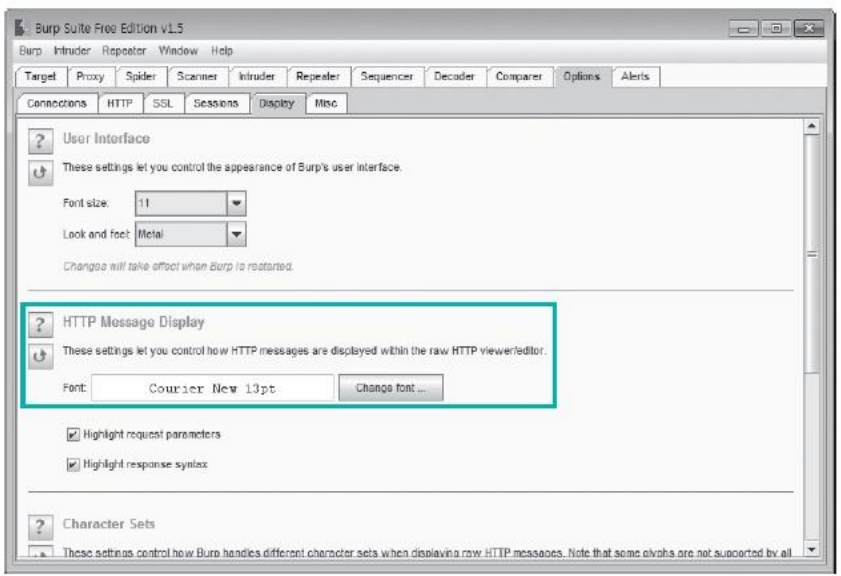
[Burp Suite에서 폰트 문제로 한글이 깨지는 현상]



※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 Burp Suite의 Response에서 한글이 깨지는 문제 해결하기

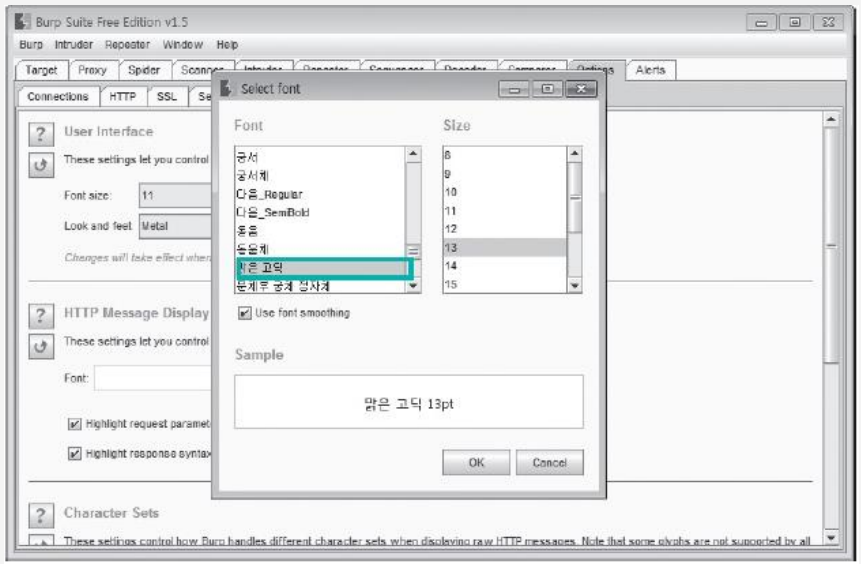
[Burp Suite에서 사용 중인 폰트 정보 확인]



※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 Burp Suite의 Response에서 한글이 깨지는 문제 해결하기

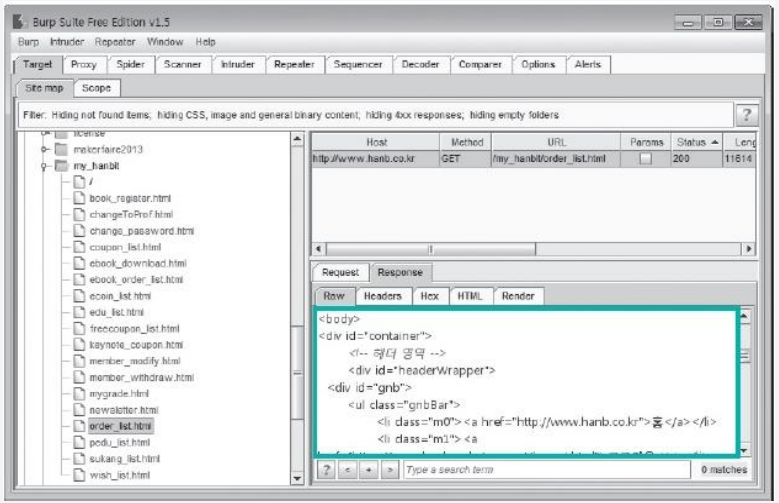
- 〈Change font〉를 클릭하여 한글 표시가 가능한 폰트 선택



※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

3 Burp Suite의 Response에서 한글이 깨지는 문제 해결하기

- 한글 폰트를 선택한 후 다시 [Target]-[Response] 탭을 보면 한글이 정상적으로 나타남



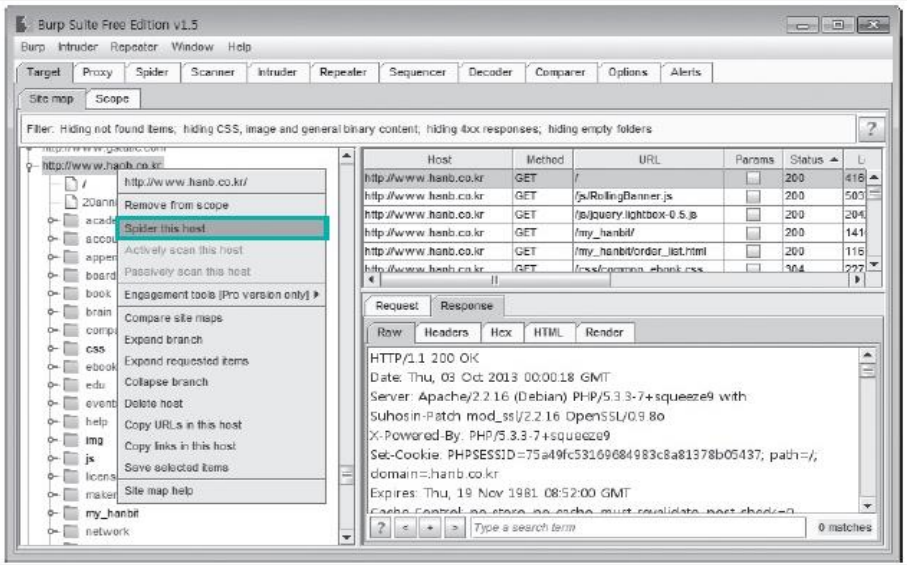
※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 Spider 기능

- 해당 사이트에서 수작업으로 확인되지 않는 페이지까지 자동으로 접속하는 기능(수동 기능)
- 짧은 시간에 매우 많은 사이트에 접속하여 정보를 수집하기 때문에 금융권과 같이 모니터링하는 사이트의 경우는 주의가 필요함
- Spider 기능을 실행하려면 [Target] 탭에서 원하는 호스트를 선택 후 마우스 오른쪽 버튼을 눌러 나타나는 메뉴에서 [Spider this host] 클릭

4 Spider 기능

[Spider 기능 실행]



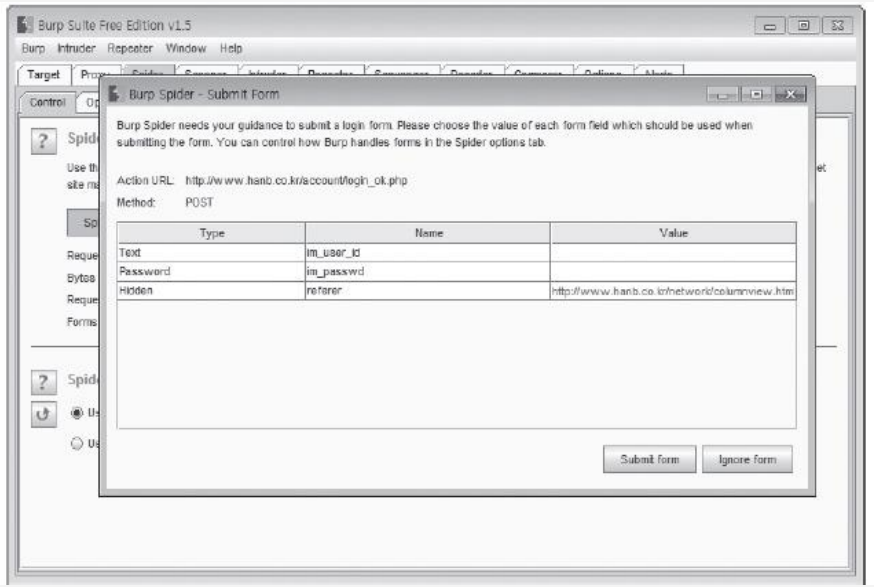
※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 Spider 기능

- 사용자의 입력값을 받아서 처리하는 페이지를 조사할 때는 해당 변숫값을 입력하는 창이 뜸
- 중간에 기능을 멈추려면 [Spider] 탭의 <Spider is running>을 클릭하여<Spider is paused>로 변경

4 Spider 기능

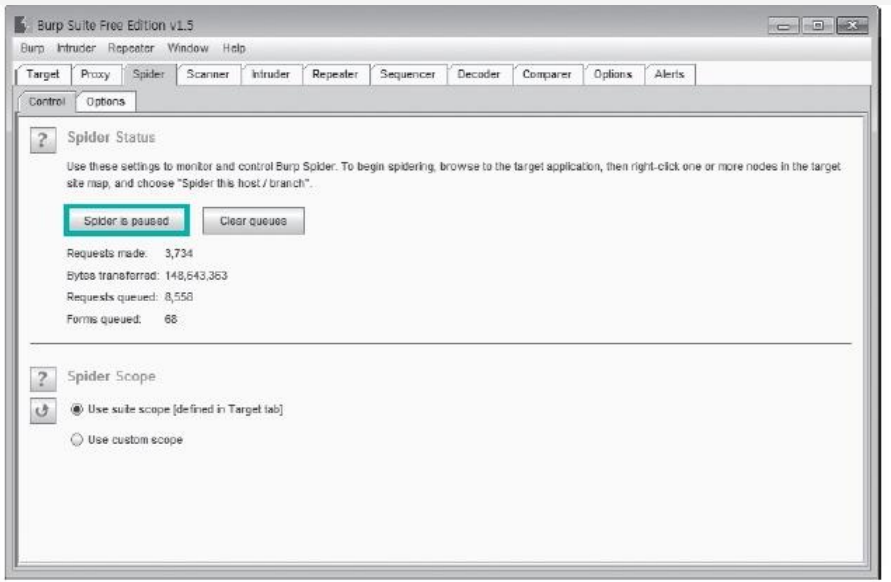
[Spider 기능 실행 시 전송 폼]



※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

4 Spider 기능

[Spider 기능 일시 중지]



※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

5 Intruder 기능

- 공격자가 수작업으로 접속하여 일일이 확인하지 않아도 해당 웹 페이지에 전달되는 변숫값을 자동으로 생성하여 전달하도록 규칙을 만들어서 해당 페이지를 계속 탐색하는 기능(자동 기능)
- [Target] 탭에서 해당 URL을 클릭하여 Intruder 기능으로 보내서 이용

5 Intruder 기능

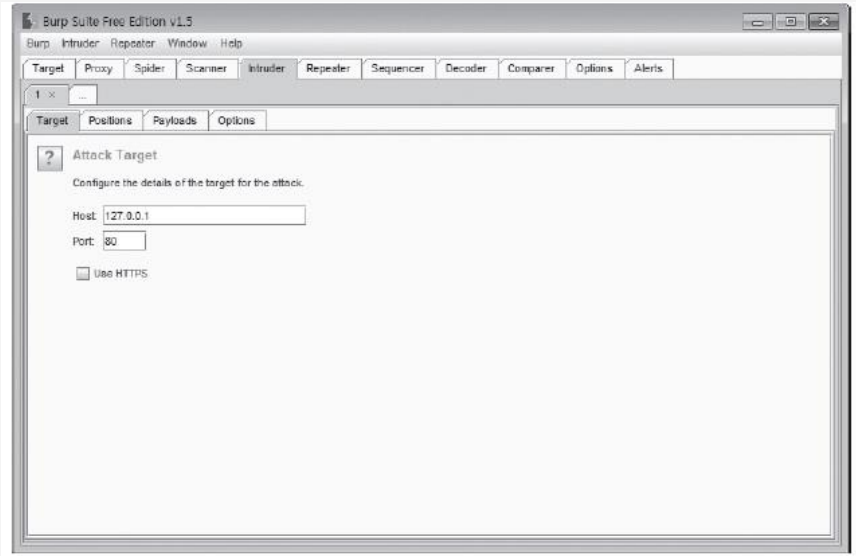
- [Target]
  : 공격 대상을 정하는 화면

- [Positions]
  : 어떤 변숫값을 조작할 것인지 정하는 화면

- [Payloads]
  : 변숫값의 종류와 범위를 선택할 수 있는 화면

5 Intruder 기능

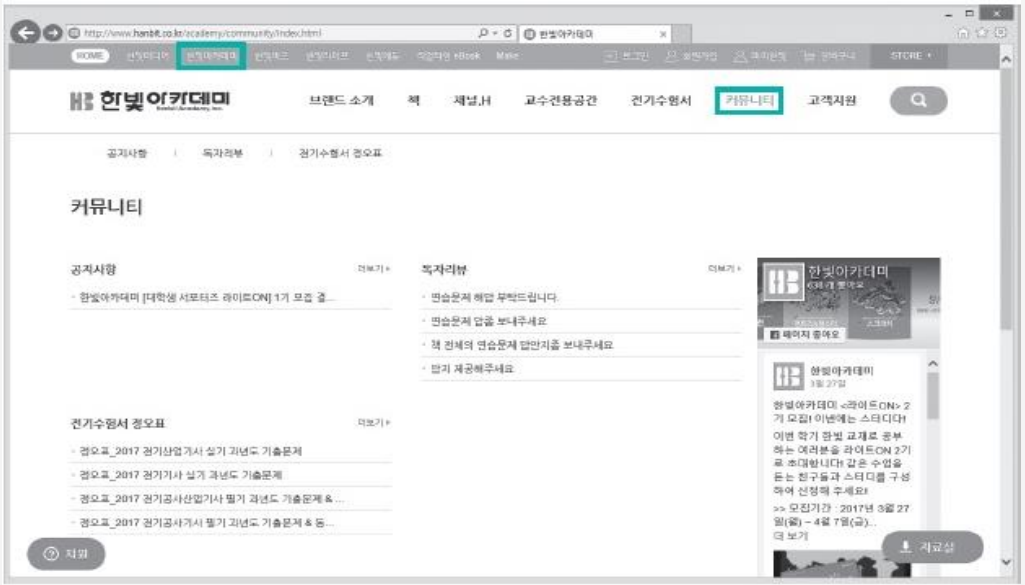
[Intruder 탭 화면]



※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

6 Burp Suite의 Intruder 기능 연습하기

1. Send to Intruder 클릭
   - 한빛미디어 홈페이지의 상위 메뉴에서 [한빛아카데미]-[커뮤니티]를 눌러 [독자리뷰] 화면 확인



[한빛아카데미의 독자리뷰 화면]

※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

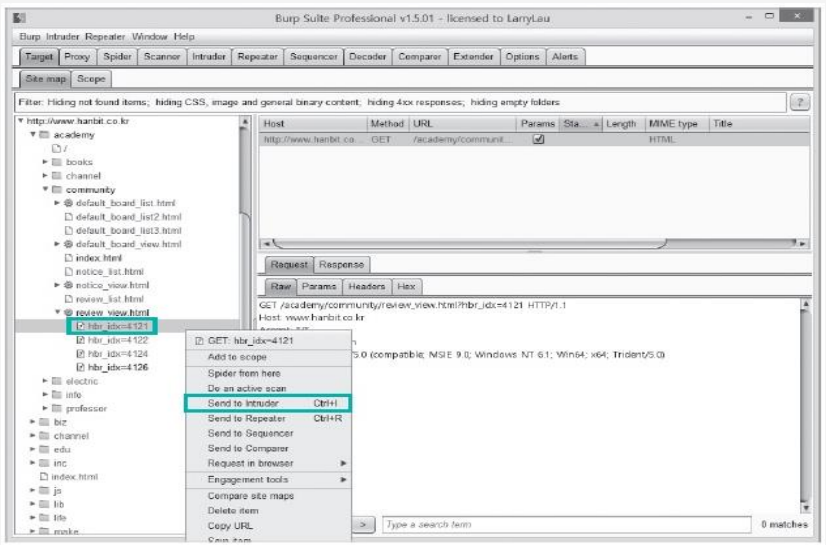
6 Burp Suite의 Intruder 기능 연습하기

1. Send to Intruder 클릭
   - [Target] 탭에서 'http://www.hanbit.co.kr-academy-communityreview_view.html-hbr_idx=4121 (번호는 매번 바뀌므로 맨 위에 있는 것 선택)'을 클릭하고, 마우스 오른쪽 버튼을 눌러 <Send to Intruder> 를 선택(4121을 바꿔가면서 보고 싶음)

6 Burp Suite의 Intruder 기능 연습하기

1 Send to Intruder 클릭

[Intruder 기능 선택 화면]



※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

6 Burp Suite의 Intruder 기능 연습하기

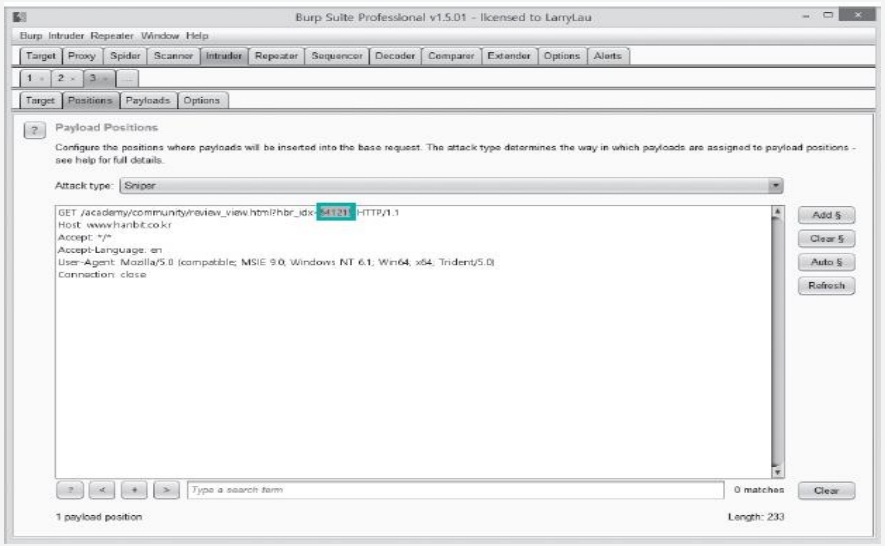
2 Intruder 기능의 Positions 부분 살펴보기

- [Intruder]-[Positions] 탭을 클릭하면 해당 요청 내용이 자동으로 입력되어 있음
- 변숫값 '4121'이 '4121'로 강조 표시된 부분은 공격자가 규칙에 의해 자동으로 해당 값 조절 가능(어디를 변경할 것인가?)

6 Burp Suite의 Intruder 기능 연습하기

2 Intruder 기능의 Positions 부분 살펴보기

[Intruder의 Positions 부분 화면]



※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

6 Burp Suite의 Intruder 기능 연습하기

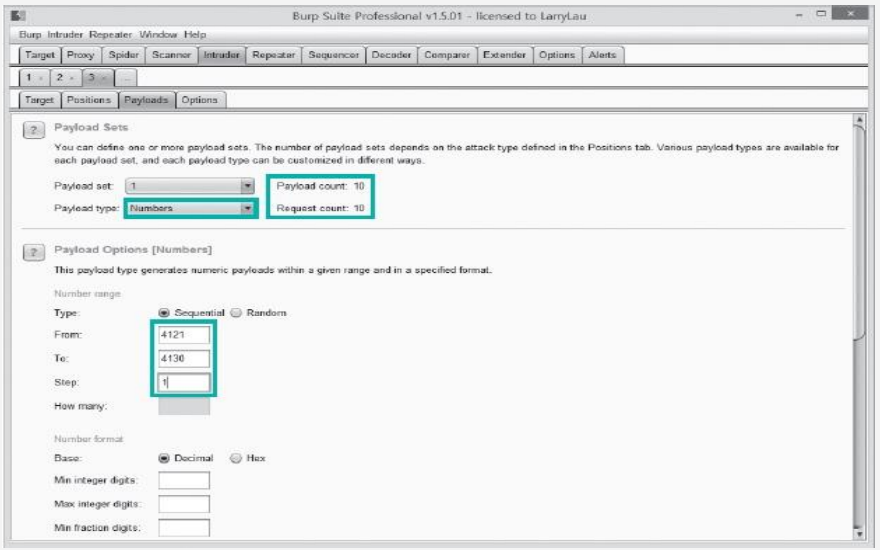
3 Payloads 수정

- 변숫값을 4121에서 4130까지 자동으로 증가시키면서 해당 페이지의 내용을 가져오는 실습
- [Payloads] 탭 상단의 Payloads Sets 항목에서 다양한 페이로드 설정

6 Burp Suite의 Intruder 기능 연습하기

3 Payloads 수정

[Intruder의 Positions 화면]



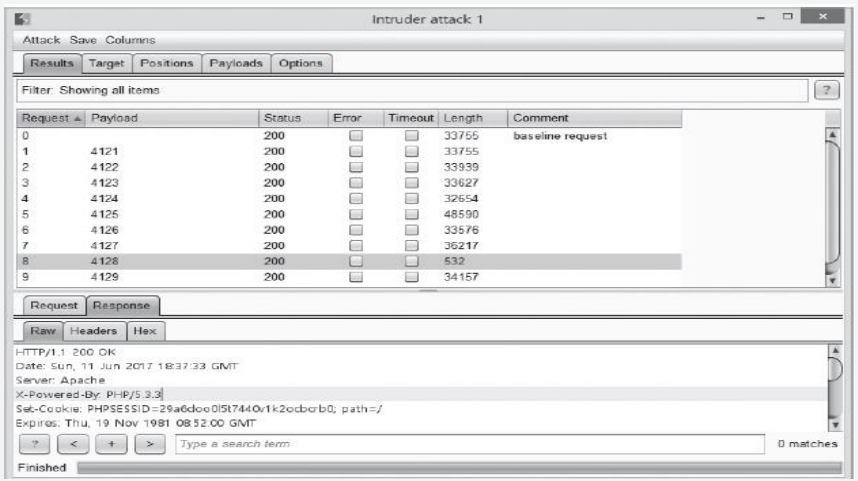
※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

6 Burp Suite의 Intruder 기능 연습하기

4 Intruder 실행

- [Intruder]-[Start attack] 메뉴를 선택 후 실행 결과 확인

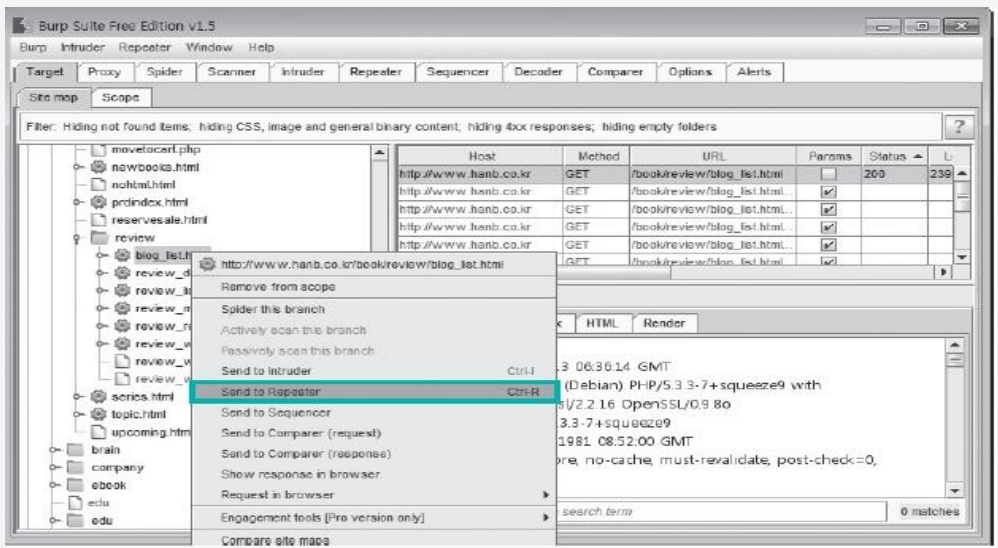
[Intruder 실행 결과]



※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

7 Repeater 기능

- [Target] 탭에서 특정 페이지를 클릭 후 마우스 오른쪽 버튼을 눌러 <Send to Repeater>를 선택하면 해당 요청을 [Repeater]로 전달(반복 기능)



[Repeater로 해당 패킷 전달]

※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

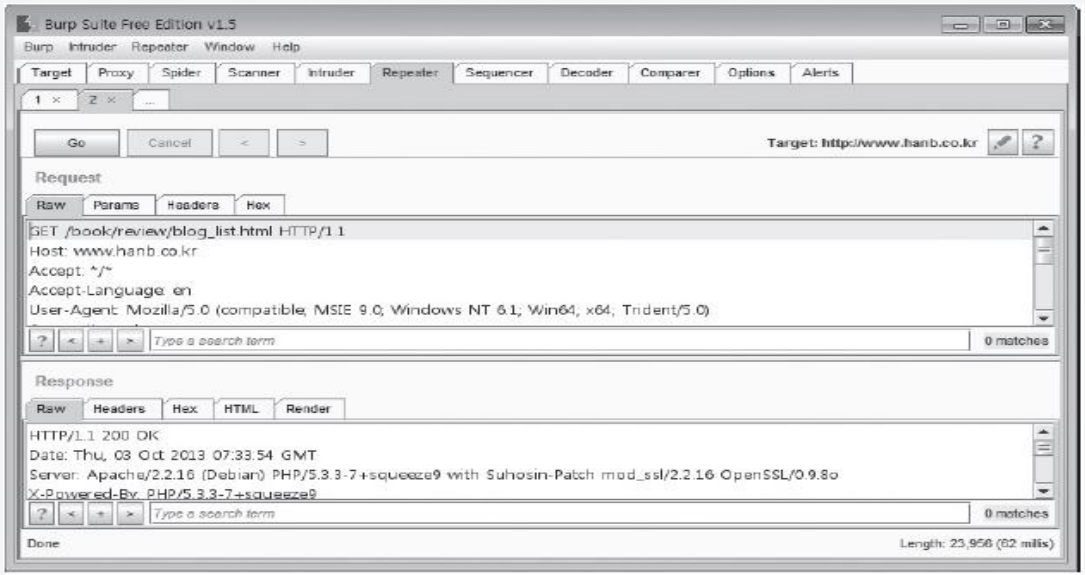
7 Repeater 기능

- [Repeater] 탭의 Request 항목을 보면
  [Target] 탭에서 전달한 요청이 있음

- 해당 요청을 다시 전달하기 위해 <Go>를 클릭하면
  Response 항목에서 결과를 볼 수 있음

7 Repeater 기능

[Repeater 기능 실행]



※출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017