개요

Burp Suite 는 웹 애플리케이션 분석에 사용할 수 있는 도구 입니다. HTTP Request 가로채기 및 수정, 로그인 창에 Brute Force (무차별 대입) 공격 등 다양한 업무를 수행할 수 있습니다. 본 문서에서는 Burp Suite 의 주요기능에 대해 설명합니다.

다운로드

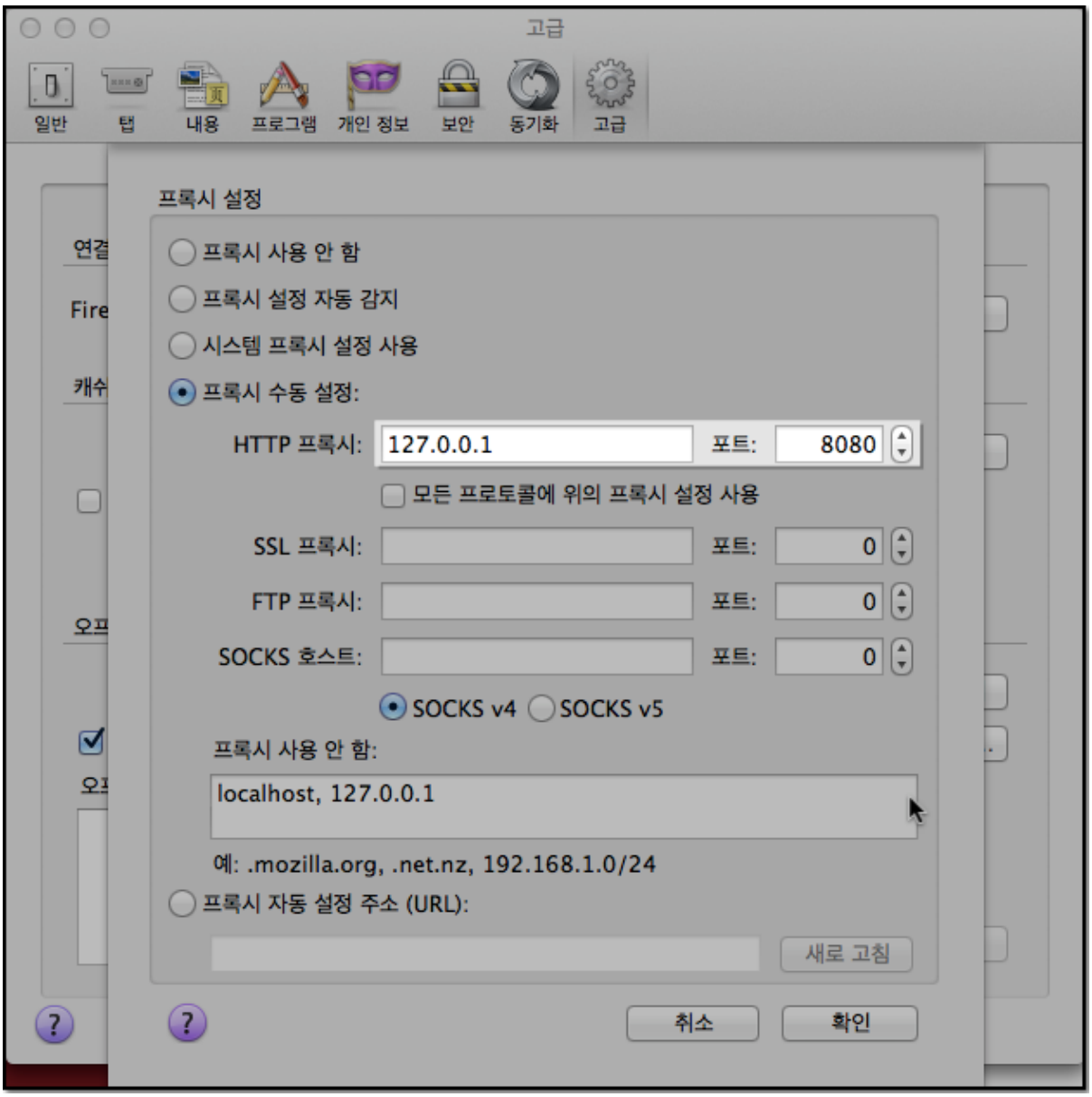
http://portswigger.net/burp/download.html

Burp Suite는 무료 버전과 유료 버전이 있으며, 무료 버전에서 지원하는 기능은 일부 Intruder 기능 및 Scanner 기능, 대상 분석기, 작업 스케줄러 등이 있습니다.

기능

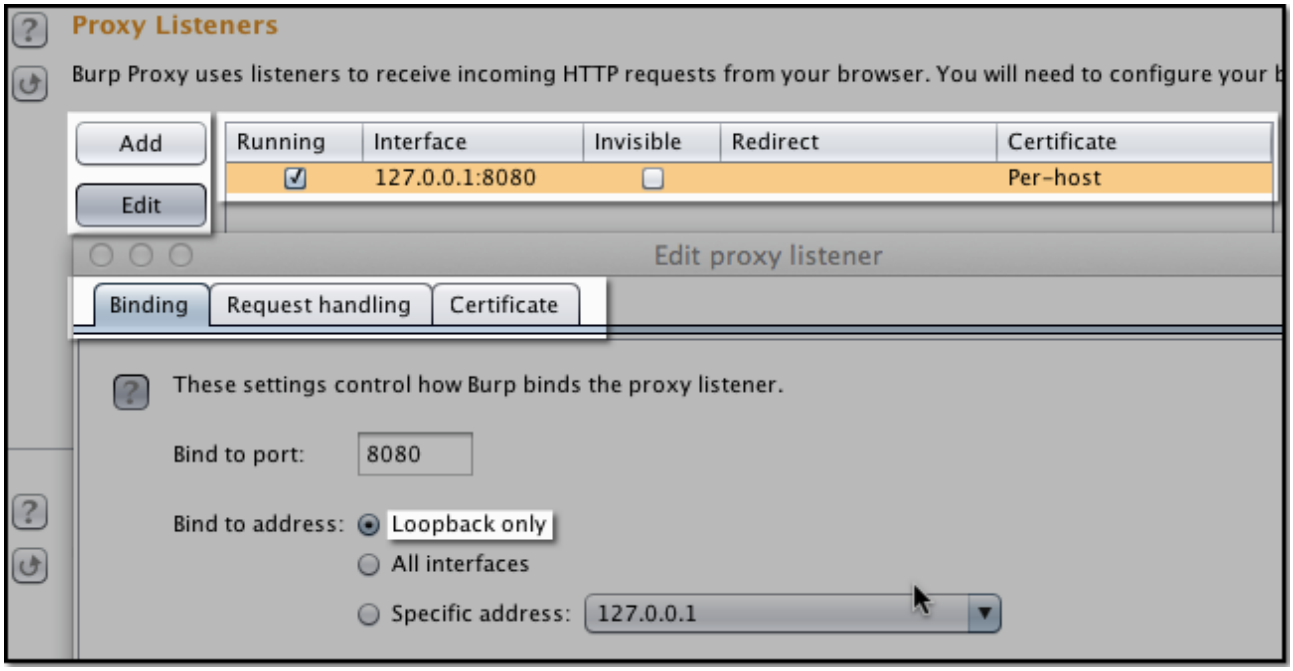
1) Proxy

Proxy 기능은 Request를 가로채고 수정하는데 사용합니다. 해당 기능을 사용하기 위해 웹 트래픽이 Proxy 를 향하도록 구성해야 하며, 설정 기본 값은 127.0.0.1:8080 입니다.

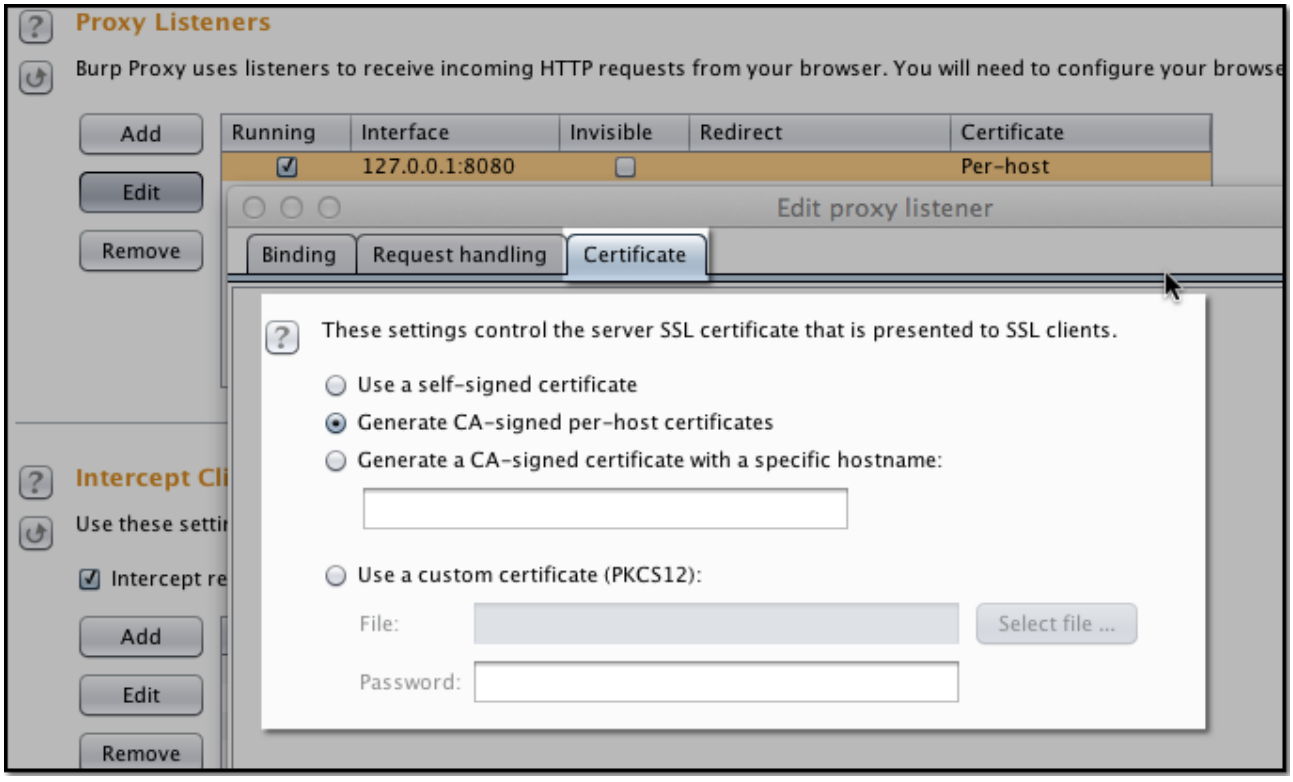


브라우저에서 설정이 끝나면, Burp Suite 를 열고 [Proxy]에서 [Intercept is on]으로 되어있는지 확인합니다.

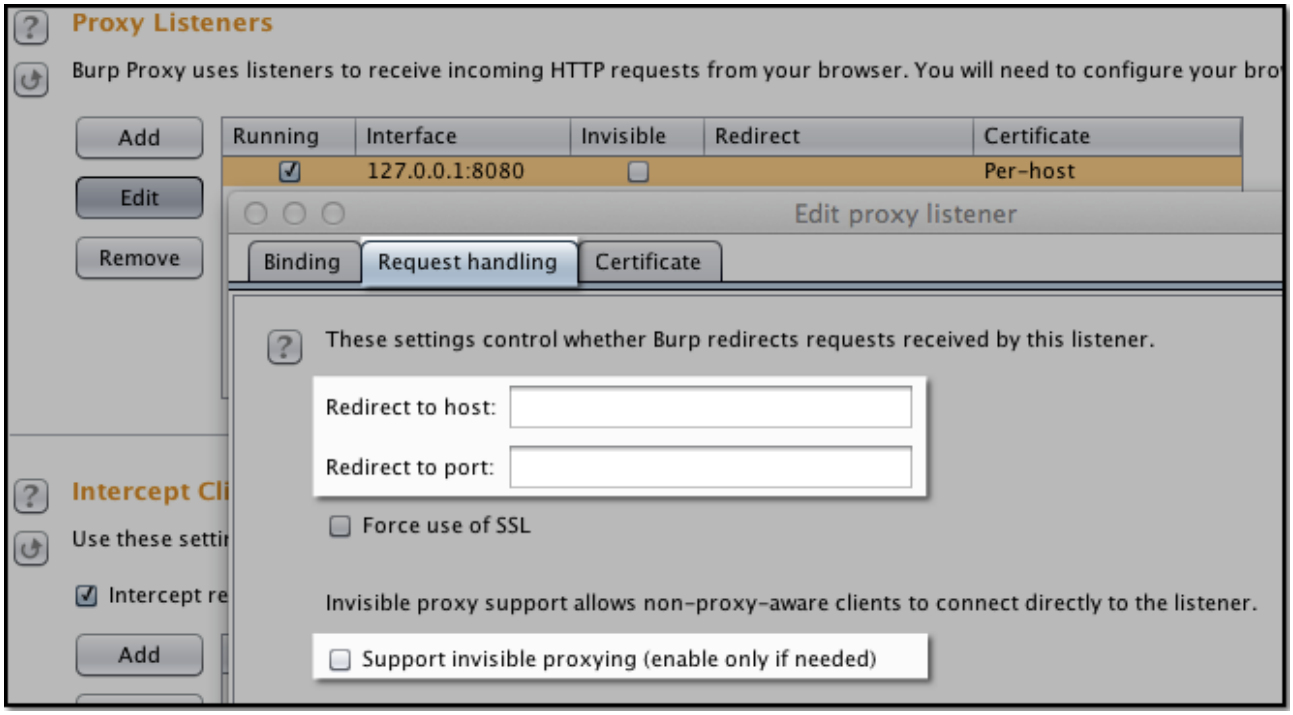
[Alerts] 탭으로 가면 8080 포트로 proxy 기능이 작동하고 있는지 확인할 수 있으며, [Proxy] 아래 [Options] 탭에서 기본 설정에 대한 구성을 변경할 수 있습니다.



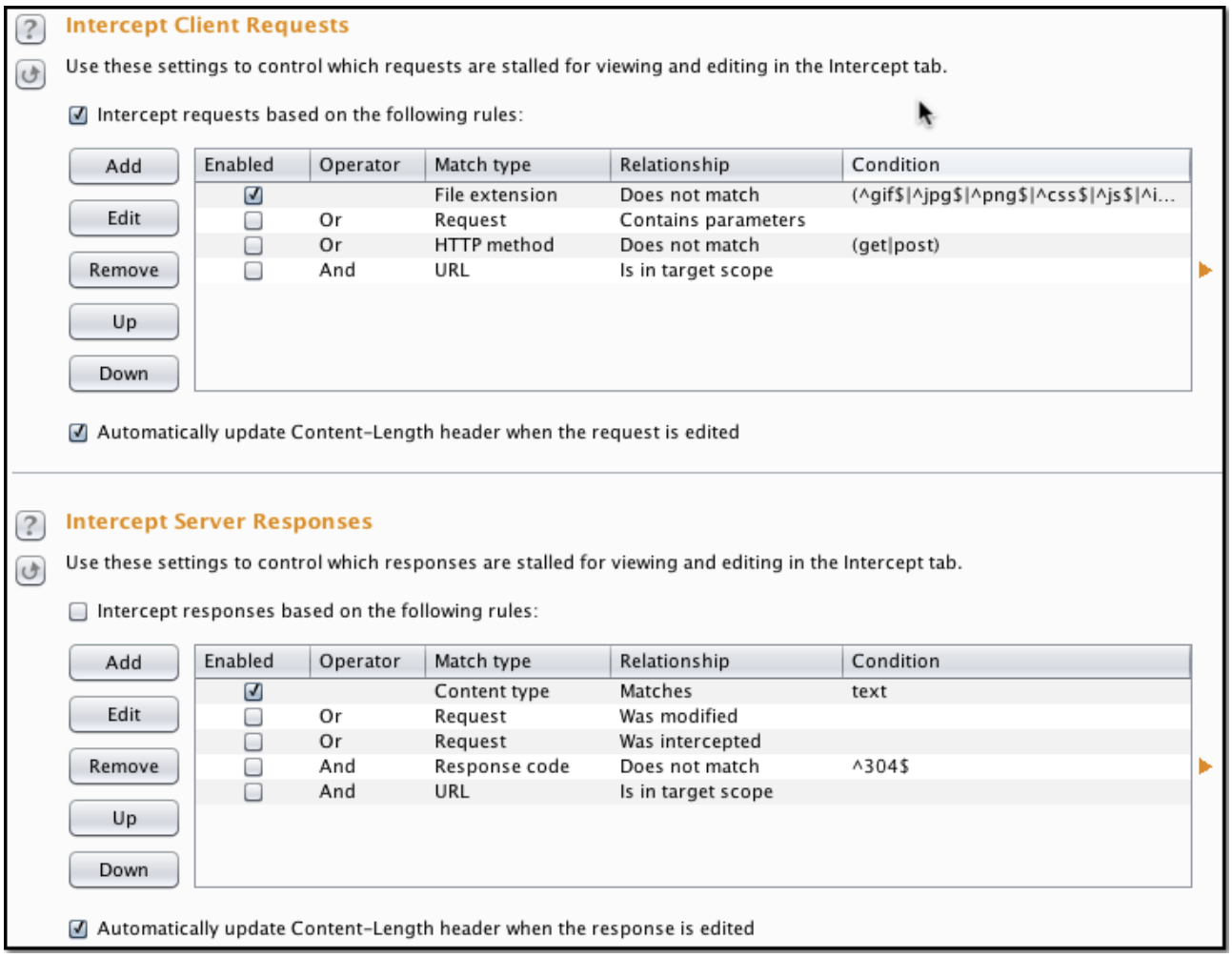
해당 탭에서 Edit 를 클릭해 수신하는 Proxy 포트를 수정할 수 있으며, Add 를 클릭해 새 Proxy Listener 를 추가로 구성할 수 있습니다. Edit - [Binding] 탭 에서 Bind to address - Loopback only 대신 다른 옵션을 사용해 네트워크 상의 또 다른 시스템의 Proxy 로 사용할 수 있습니다. 즉, 동일한 네트워크 상의 모든 호스트는 Burp Proxy 기능을 사용할 수 있으며, Proxy 를 통해 트래픽을 릴레이할 수 있습니다.



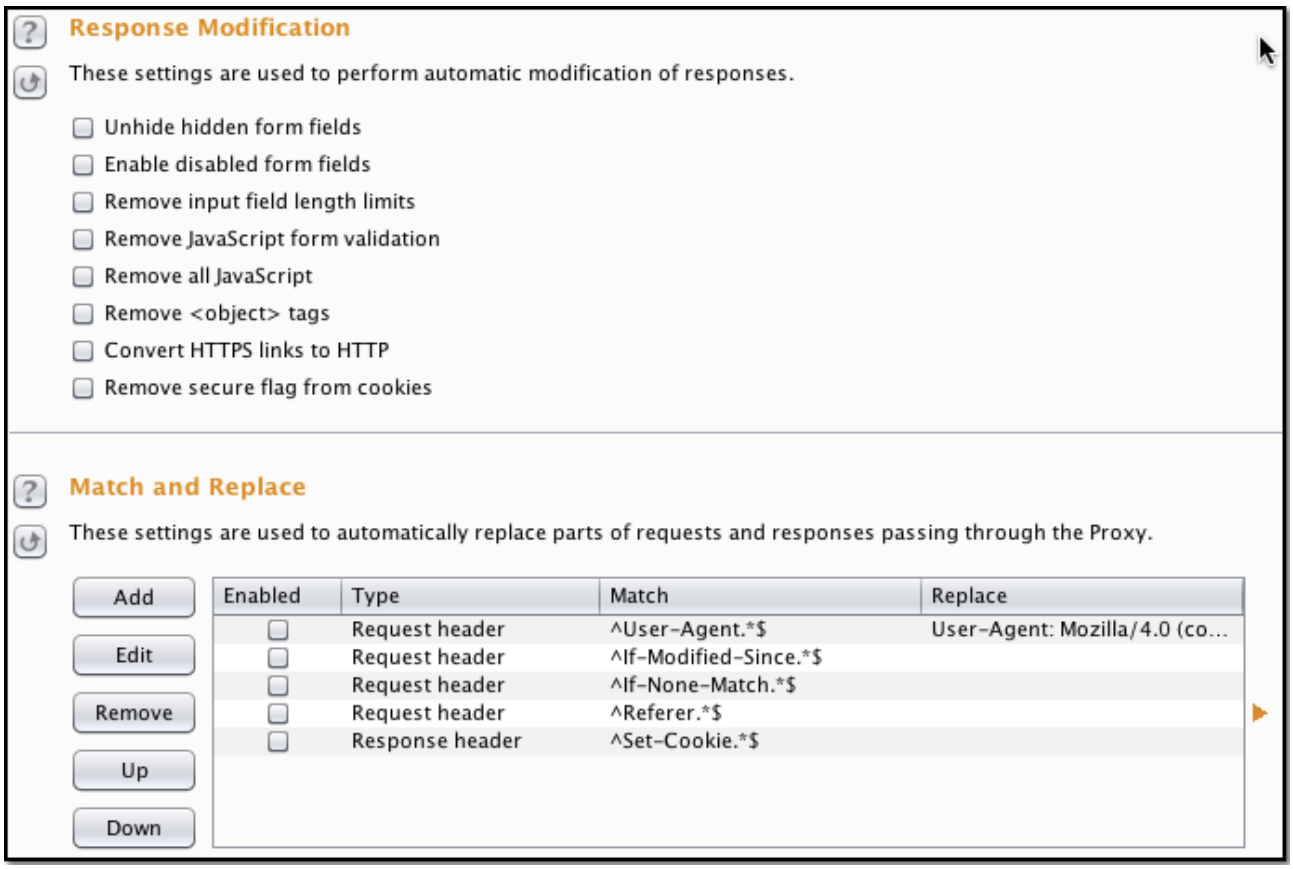
Burp 는 SSL 보호 웹 사이트에 인증서를 제공할 수 있는 옵션도 있습니다. 기본적으로 Burp 는 자체 서명된 CA 인증서를 생성합니다. 현재 선택된 옵션 즉, Generate CA-signed per-host certificates는 클라이언트에서 연결하려는 특정 호스트에 대해 Burp의 CA인증서로 서명한 인증서를 생성합니다. 웹 애플리케이션 분석 시 우려할 유일한 일은 SSL(TLS)로 보호된 웹 사이트에 연결할 때 인증서 오류의 경고 수를 줄이는 것입니다.



Support invisible proxying (enable only if needed) 옵션은 Proxy 를 사용하고 있는지 모르는 클라이언트에서 사용합니다. 이는 Proxy 설정이 브라우저의 옵션이 아닌 다른 위치 (예: hosts) 에 있는 경우를 말합니다. 이 경우의 Request 는 브라우저에서 설정한 경우의 Request 와 약간 다르기 때문에 해당 옵션을 사용함으로써 Burp 에 알려주는 역활을 . Redirect to host, Redirect to port 는 옵션 이름과 같이 호스트와 포트를 설정 값으로 Redirect 합니다.



“Intercept Client Requests”, “Intercept Server Responses” 옵션 항목에서 지정하는 규칙에 따라 Request 와 Response 를 가로챌 수 있습니다. 트래픽이 많을 경우 우리가 원하는 일부 Request 만 가로채도록 설정할 수 있습니다.

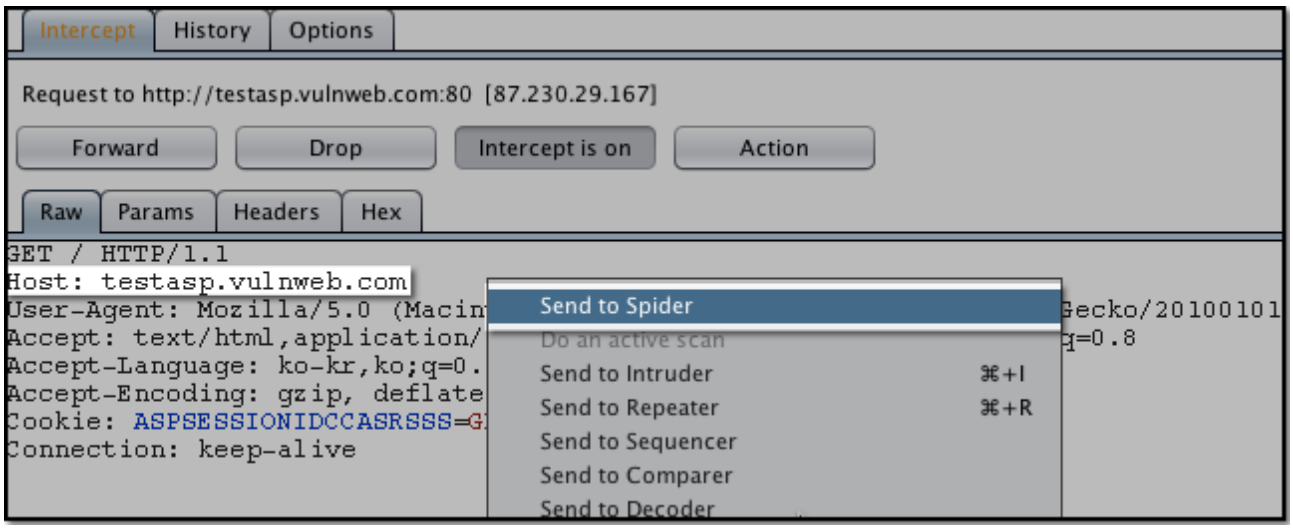


“Response Modification”, “Match and Replace” 옵션 항목에서 서버로부터 받은 Response 를 수정할 수 있습니다. 숨겨진 폼 필드를 표시(Unhide hidden from fields)하거나, 모든 자바 스크립트를 제거(Remove all JavaScript) 할 수 있습니다. 또한, 특정 패턴에 대해 사용자 지정 문자열로 있습니다. “Match and Replace” 옵션 항목 작성 시 정규 표현식(RegEx)을 지정할 수 있습니다. Burp는 특정 패턴을 찾아서 지정 문자열로 대체하기 위해, 자동으로 Request 또는 Response 분석할 것입니다.

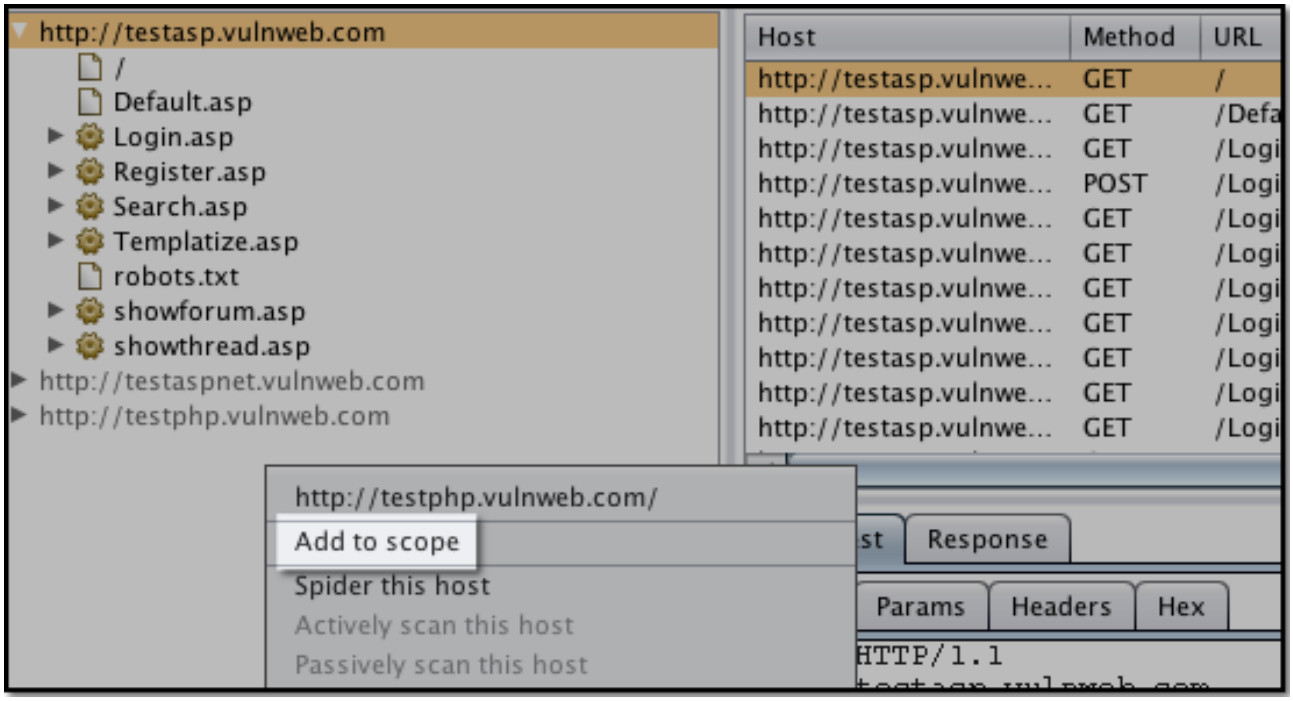
여기까지 Proxy 기능에 대한 설정을 완료했다면, Request 및 Response 를 가로챌 수 있습니다. Request 를 보낼 때나 Response 를 받을 때 마다 Burp 에 의해 가로채어지므로, 일일이 수작업으로 해당 패킷들을 Forward 시켜야 합니다. 따라서 패킷의 내용을 수정해야 할 때만 [Intercept is on] 옵션을 유지 하는 것이 좋습니다.

2) Spider

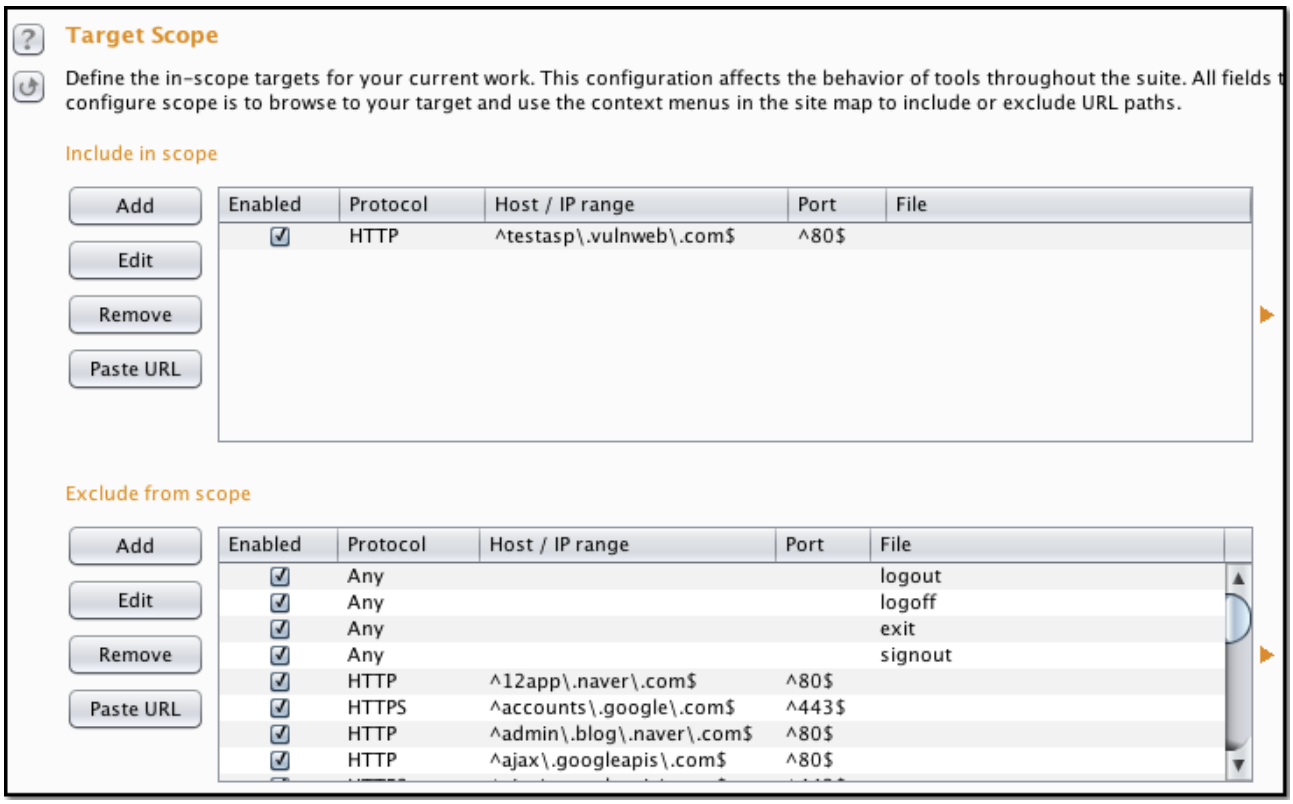
Burp Spider 는 웹 애플리케이션의 지도를 만들 때 사용합니다. 전체 웹 애플리케이션에 대한 상세 분석을 하기 위해 웹 애플리케이션을 자동으로 크롤링해서, 링크 및 모든 로그인 폼을 알려줄 것입니다. 이렇게 찾은 링크들은 세부 검색을 위해 Scanner 로 보내지게 됩니다. Spider 기능을 간단히 사용하기 위해 브라우저에서 취약한 웹 애플리케이션의 주소로 이동하여 Burp 가 가로챈 Request 에서 마우스 오른쪽 버튼 클릭 후 “Send to Spider” 항목을 선택합니다.



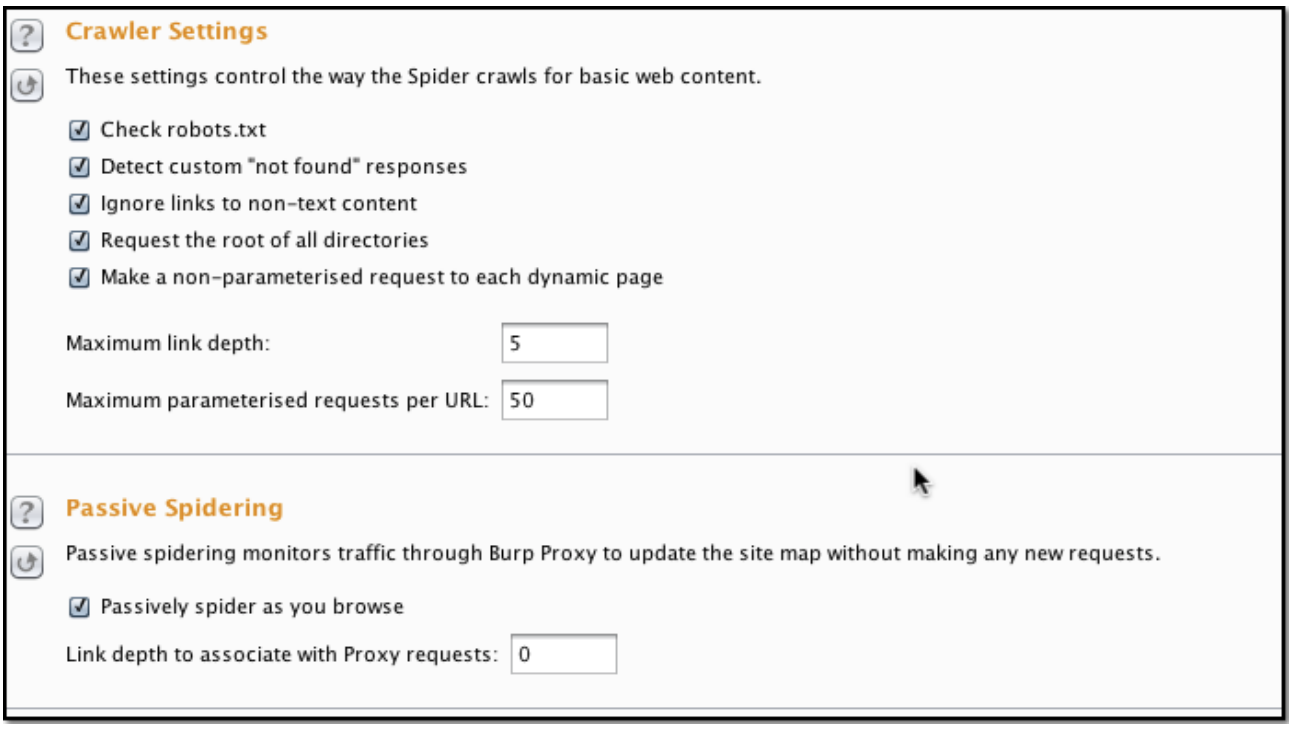
이렇게 하면 경고 창이 팝업 되면서 Scope(범위)에 대상을 추가할 것인지 물어보는데 [Yes] 를 선택합니다. 여기에서 Scope(범위)는 테스트를 실행 하고자 하는 대상 영역을 정의 합니다.



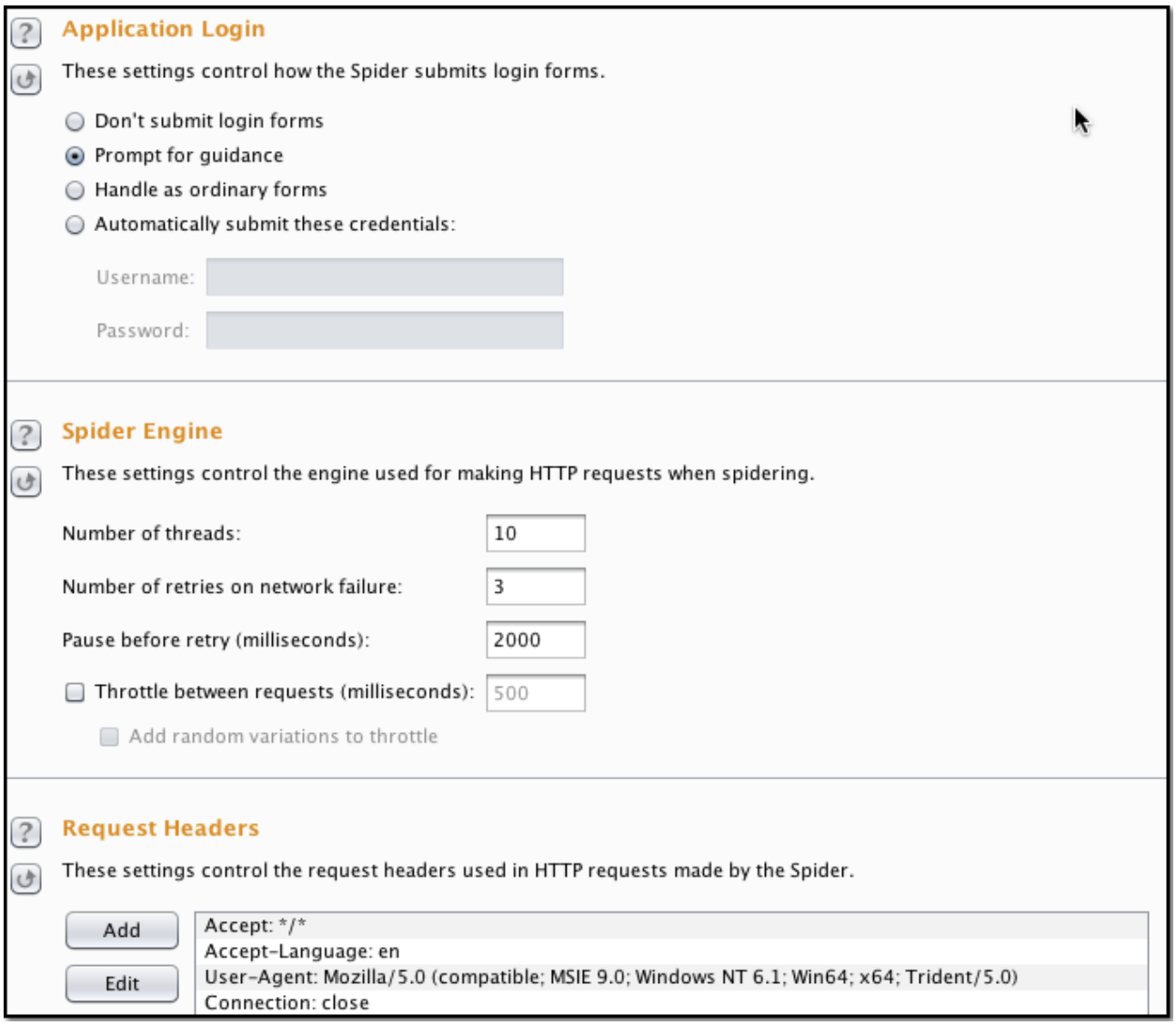
[Target] 의 [Site map] 탭으로 이동하면, Target에 웹 애플리케이션 URL이 추가되어 있는 것을 볼 수 있습니다. 또한, http://google.com 같은 다른 대상까지 목록에 추가 된 것을 볼 수 있을 것입니다. Burp 는 Proxy 기능을 사용 하는 동안, 사용자가 탐색하는 웹 애플리케이션을 자동으로 Target 의 대상 목록에 추가합니다. 어떤 대상이든지 마우스 오른쪽 버튼을 클릭하고 “Add item to scope” 항목을 선택해 [Scope]에 추가할 수 있습니다.



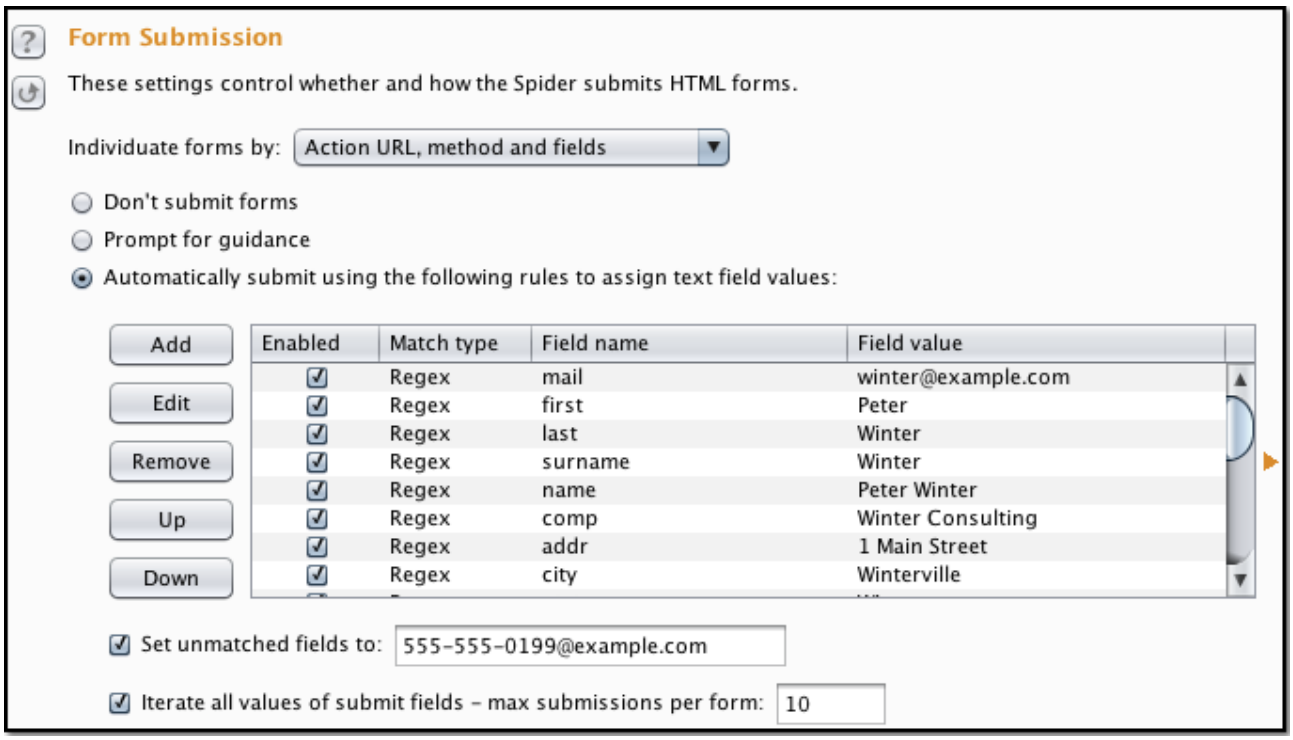
[Scope] 탭으로 이동하면 취약한 웹 애플리케이션의 URL이 추가되었음을 확인할 수 있습니다.



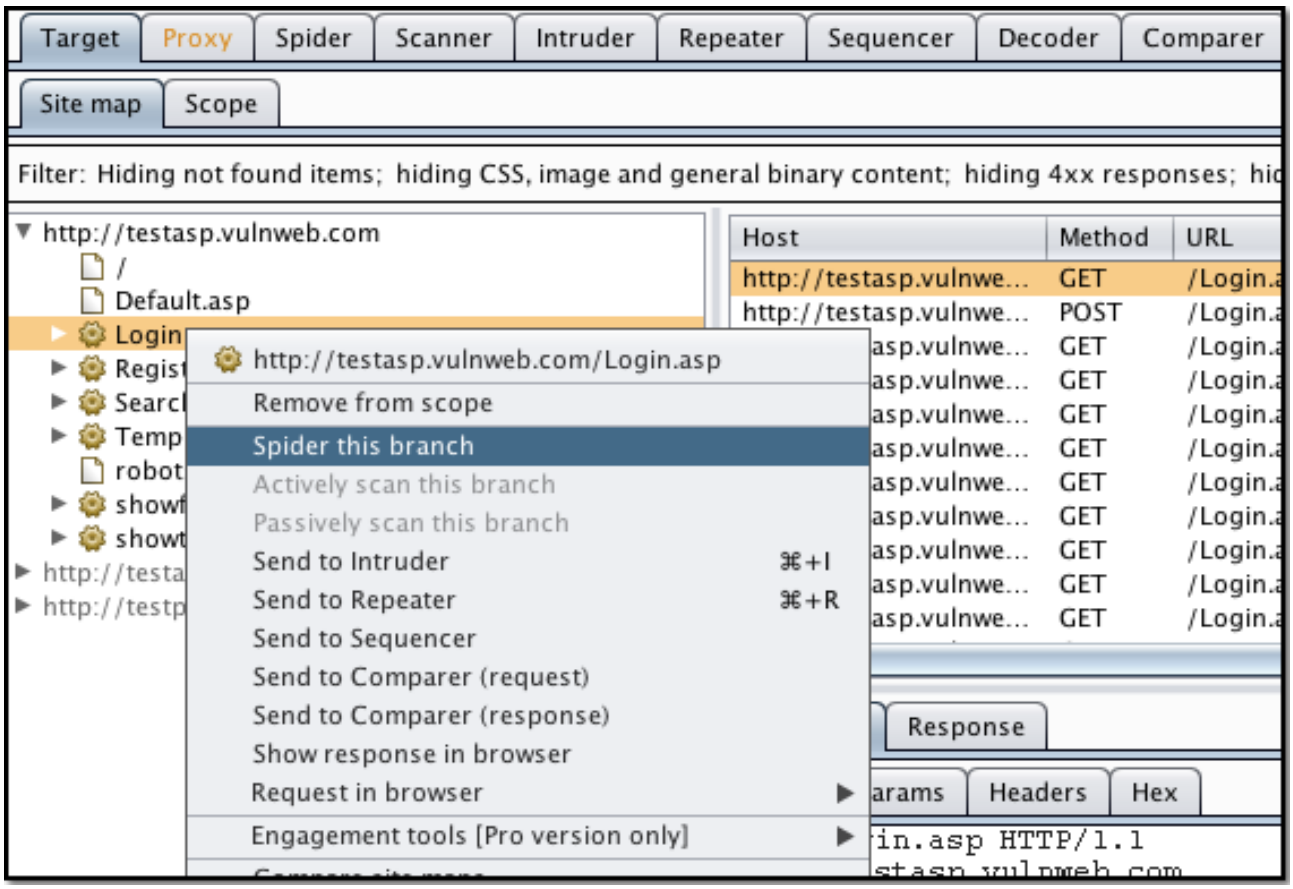
이제 [Spider] 탭에 가서 [Option] 탭을 선택합니다. 해당 탭에서 Burp Spider 가 작동 방식에 대한 다양한 옵션을 설정할 수 있습니다. 웹 사이트 관리자가 검색 엔진에 인덱싱 되지 않도록 robots.txt 설정한 경우 파일 존재 여부에 대한 확인을 요청할 수 있습니다. 다른 중요 옵션은 [Passively spider as you browse] 입니다. 기본적으로 Burp Spider는 Passive 와 Active 모드 모두에서 실행할 수 있습니다. Active 모드의 경우 Burp의 Proxy 기능을 사용하여 웹 애플리케이션 분석하는 동안, 새로운 링크와 콘텐트에 대한 Scanning 을 유지할 것인지 묻습니다. Passive 모드의 경우 묻지 않고 유지합니다.



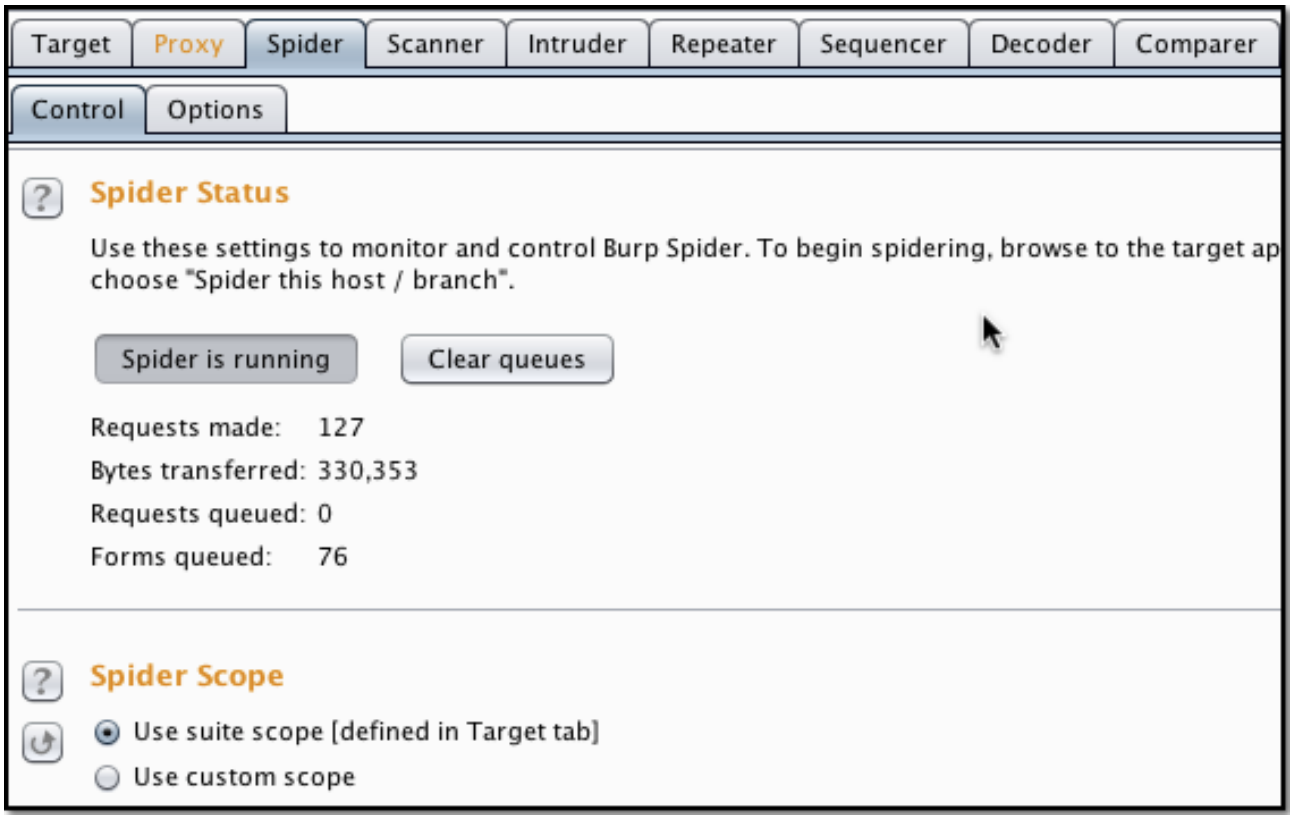
또 다른 중요 옵션은 [Application Login] 입니다. “Automactically submit these credentials” 항목을 선택해 Burp Spider 가 로그인 폼을 만날 때마다 자동으로 [admin/password] 같은 자격증명을 제출하도록 설정할 수 있습니다. Burp Spider 는 자동으로 이 자격증명을 제출하고 추가 정보를 찾기 위해 크롤링을 계속 할 것입니다. [Spider Engine] 옵션에서 사용자가 원하는 경우 쓰레드 수를 변경할 수도 있습니다.



마지막으로 [Form Submission] 옵션에서 웹 페이지 폼의 사용자 입력 부에 대한 값을 자동으로 제출하도록 설정할 수 있습니다. Proxy 기능의 [Match and Replace] 옵션과 같이 옵션 항목 작성 시 정규 표현식(RegEx)을 지정할 수 있습니다. Burp는 폼 필드 이름의 특정 패턴을 찾아서 지정 문자열을 자동으로 제출하기 위해, 웹 페이지를 분석할 것입니다.



[Target] 의 [Site map] 탭에서 Spider 를 시작하려면, 웹 애플리케이션 URL을 선택하고 마우스 오른쪽 버튼을 클릭하여 “Spider this branch” 항목을 선택합니다.

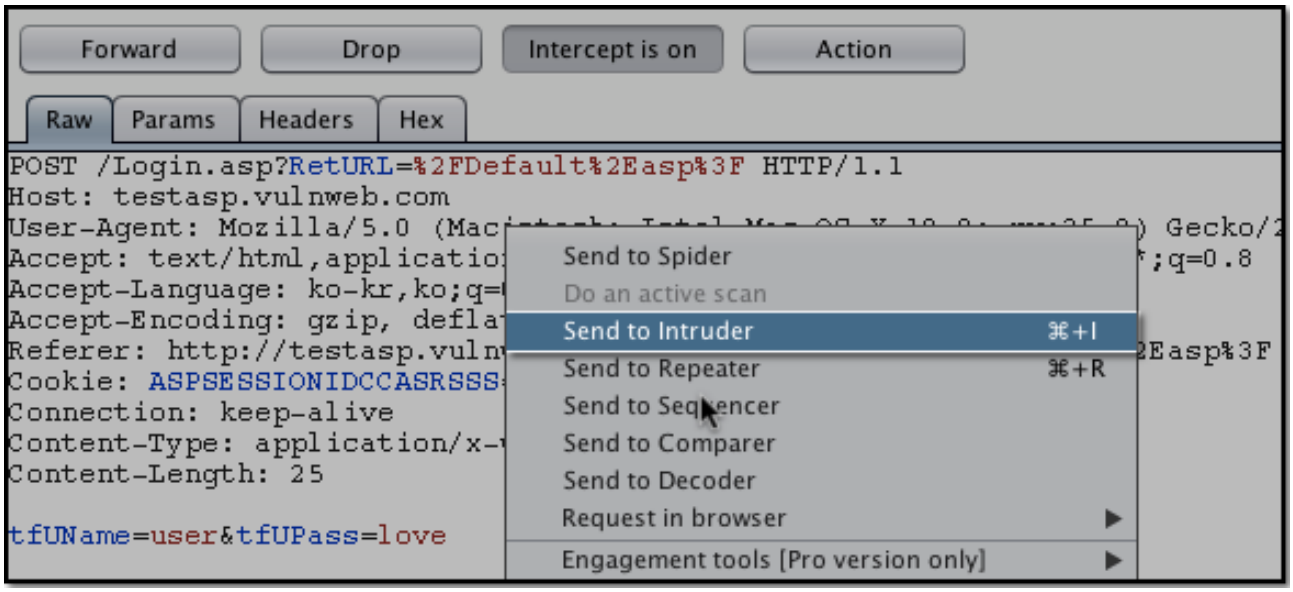


이렇게 하면 Burp Spider 가 시작되고 [Spider] 의 [Control] 탭에서 Spider 가 자동으로 생성하고있는 Request 를 볼 수 있습니다. 또한, Burp Spider 에 대한 사용자 정의 Scope 를 지정할 수도 있습니다.

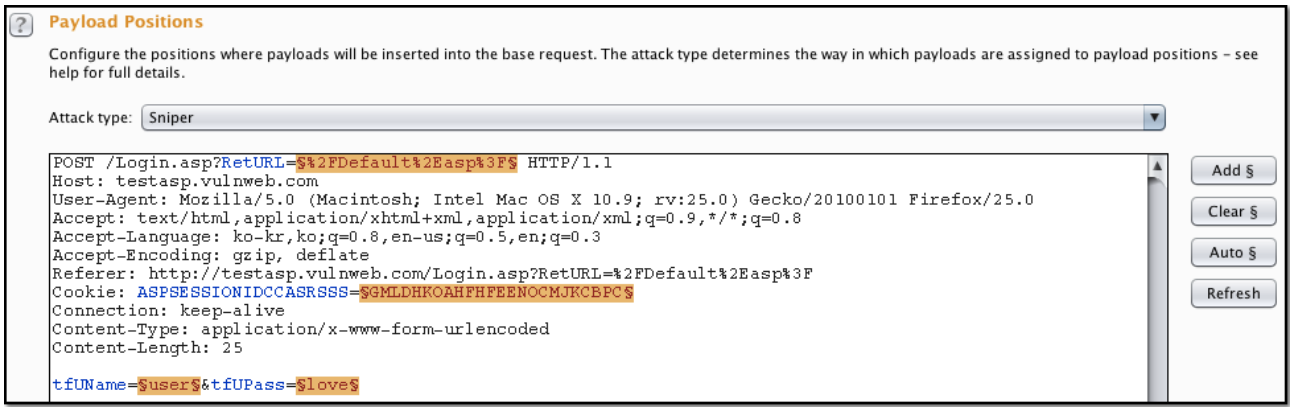
Spidering 이 완료되면, 웹 애플리케이션에 대한 새로 발견된 URL 들이 표시 됩니다. 이 URL 들은 매우 유용한 정보를 제공하며, Burp Scanner 와 같은 다른 Burp 기능에 보내어 취약점 탐색을 할 수 있습니다.

3) Intruder

Burp Intruder 는 Fuzzing, Brute Force(무차별 대입) 공격에 이용할 수 있습니다. 이번 예제에서는 Brute Force(무차별 대입) 공격 기능을 사용할 것입니다. Burp Suite에서 [Intercept is on] 으로 되어있는지 확인하고 웹 페이지에서 로그인 합니다.

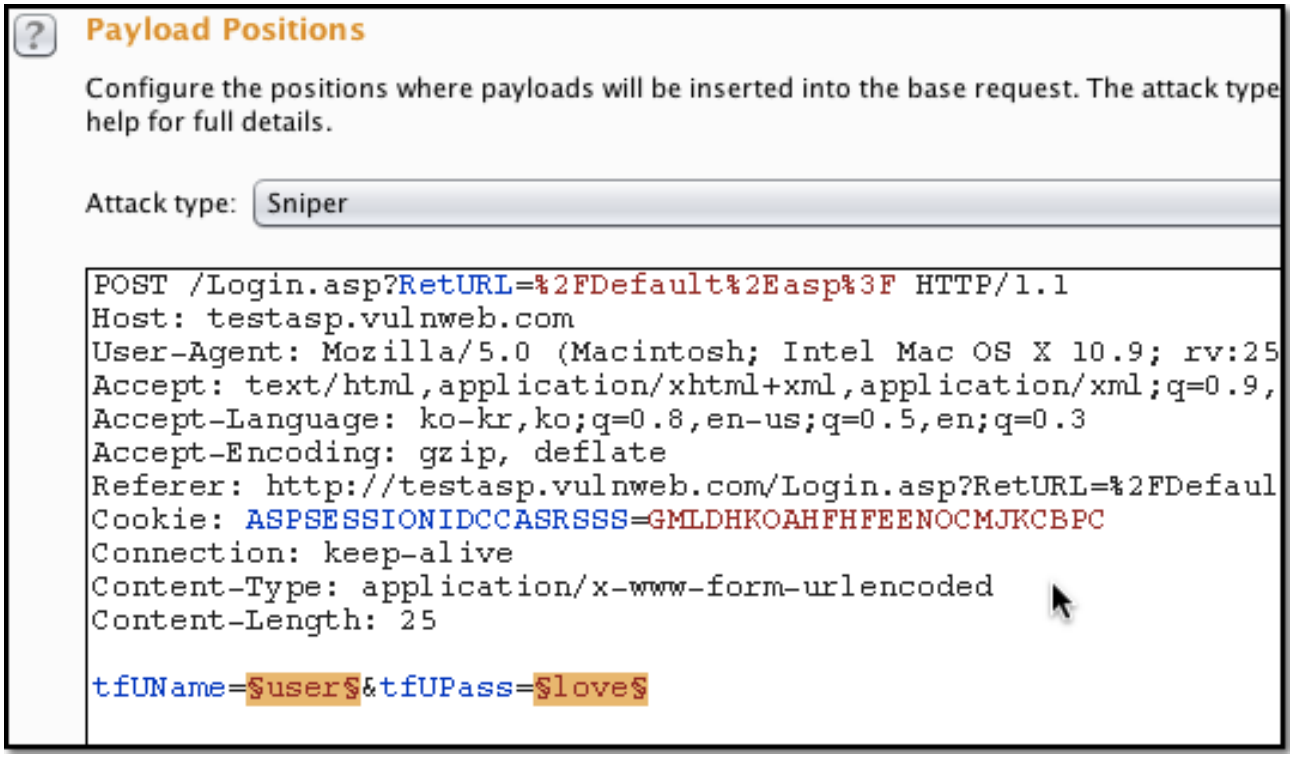


가로챈 사용자 Request 에서 마우스 오른쪽 클릭 후 “Send to Intruder” 항목을 선택하여 [Intruder] 로 Request 정보를 보냅니다.



[Intruder] 탭으로 이동하여 Attack Target 을 확인합니다. [Positions] 탭을 선택하면 사용자가 Intruder 로 보낸 Request 를 볼 수 있으며, 일부 강조 표시가 되어있습니다. 강조 표시는 기본적으로 Brute Force(무차별 대입) 공격 시 변경 되어질 부분을 Burp 에서 추측한 것입니다. 예제에서는 단지 사용자 이름 및 암호가 변경될 것이므로, Burp 의 강조 표시를 적절하게 수정합니다.

오른쪽에 [Clear] 버튼을 클릭하면. 강조 표시된 텍스트가 모두 제거됩니다. 공격에 대한 매개변수로 사용자 이름 및 암호만을 설정해야 합니다. 이 Request에서 tfUName(예제의 경우 "user")을 드래그하고 [Add] 버튼을 클릭합니다. 마찬가지로 password인 “love”를 드래그하고 [Add] 버튼을 클릭합니다. 이렇게 하면 tfUName 과 tfUPass 가 첫 번째 및 두 번째 변수로 추가되어 다음과 같이 보일 것입니다.



다음으로 Request 윗 부분에 있는 공격에 대한 유형 [Attack type]을 설정합니다. 기본 값으로 “Sniper” 가 설정되어 있으나 예제의 경우에는 “Cluster bomb” 항목을 사용해야 합니다.

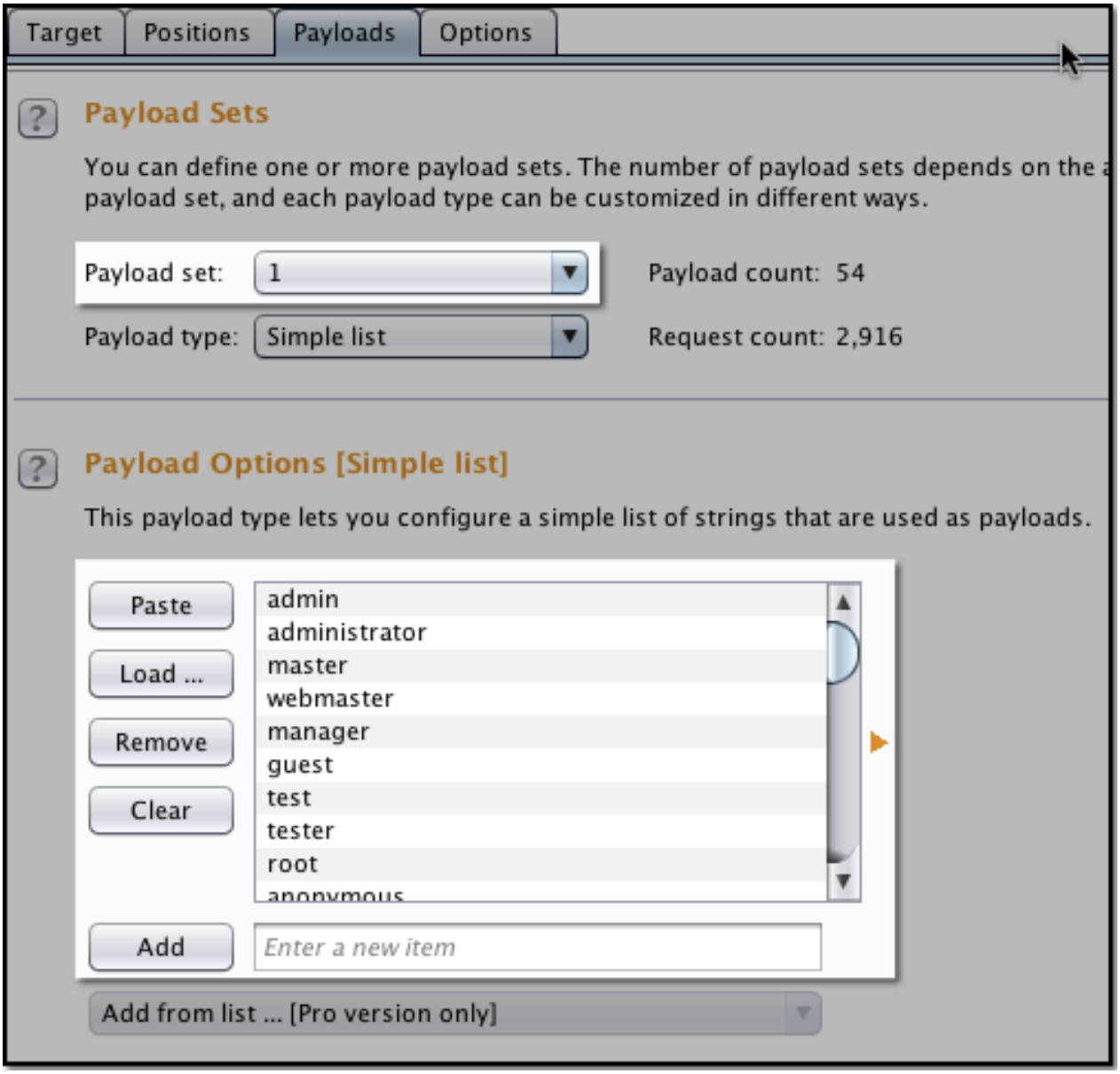
아래는 Portswigger.net 에서 설명하는 공격의 종류 및 차이입니다.

Intruder 공격 유형	
Sniper	단일 Payload Set 을 사용하며, 사용자 정의 매개변수 순서대로 Payload 를 입력합니다. 주어진 Request 를 처리하는 동안 지정한 변수를 제외하고는 영향을 받지 않습니다. 이 공격 형식은 XSS 처럼 공통적이고 개별적인 다수의 필드를 테스트 하는 데 유용 합니다. 위와 같이 tfUName 과 tfUPass 두 필드를 변수로 지정한 경우 tfUName 에 Payload 를 순서대로 입력하는동안 tfUPass 에는 Payload 를 입력하지 않습니다. tfUName 에 Payload Set 의 모든 요소가 입력되면 그 다음으로 tfUName 에는 기본 값 (user)을 유지하며, tfUPass 에 Payload 를 순서대로 입력합니다.
Battering ram	단일 Payload Set 을 사용하며, 사용자 정의 매개변수에 동일한 Payload Set 을 한꺼번에 입력합니다. 즉, tfUName 과 tfUPass 에 같은 Payload 값이 입력됩니다. 이 공격 유형은 HTTP 요청 내 여러 위치에 같은 입력 값을 삽입할 경우에 유용합니다.
Pitchfork	여러 Payload Set 을 사용하며, 사용자 정의 매개변수에 다른 Payload Set(최대 8개)을 입력합니다. 예를 들어, 첫 번째 Request 는 변수 1에 Payload Set 1 의 첫 번째 값을 입력하고, 변수 2에 Payload Set 2 의 첫 번째 값을 입력합니다. 두 번째 Request에서는 Payload Set 1 의 두 번째 값을 변수 1에 입력하고, Payload Set 2의 두 번째 값을 변수 2 에 입력합니다. 이 공격 유형은 서로 다르지만 관련된 입력을 다수의 위치에 적용해야 할 경우(예를 들어, 사용자 이름과 사용자 번호 등)에 유용합니다.

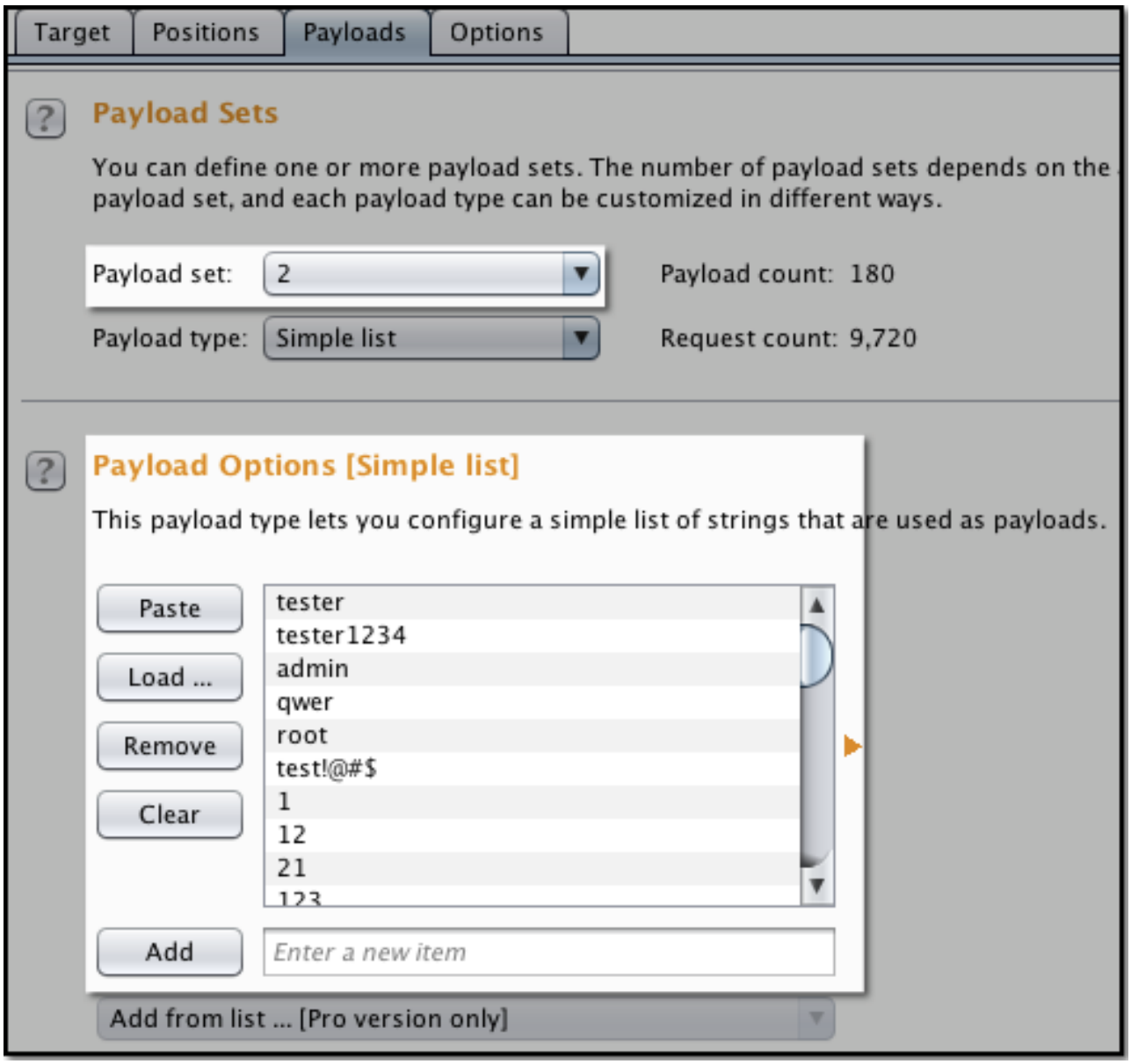
Intruder 공격 유형	
Cluster bomb	여러 Payload Set 을 사용하며, 사용자 정의 매개변수에 다른 Payload Set(최대 8개)을 입력합니다. Pitchfork 유형과 다른점은 각 Payload Set 을 순서대로 반복해 모든 Payload 의 조합을 테스트한다는 것입니다. 예를 들어, 사용자 정의한 변수가 두 개 있는 경우, Payload Set 1 에서 첫 번째 값을 변수 1에 입력하고, Payload Set 2 의 모든 값을 변수 2에서 반복 입력한 다음, Payload Set 1 의 두 번째 값을 변수 1에 입력하고, Payload Set 2 의 모든 값을 변수 2에 반복 입력합니다. 이 공격 유형은 서로 다르고 관련이 없는 변수가 다수 위치에 있는 경우 (예를 들어, 사용자 이름과 패스워드)에 유용합니다.

예제에서는 공격 유형을 "Cluster bomb"으로 설정합니다.

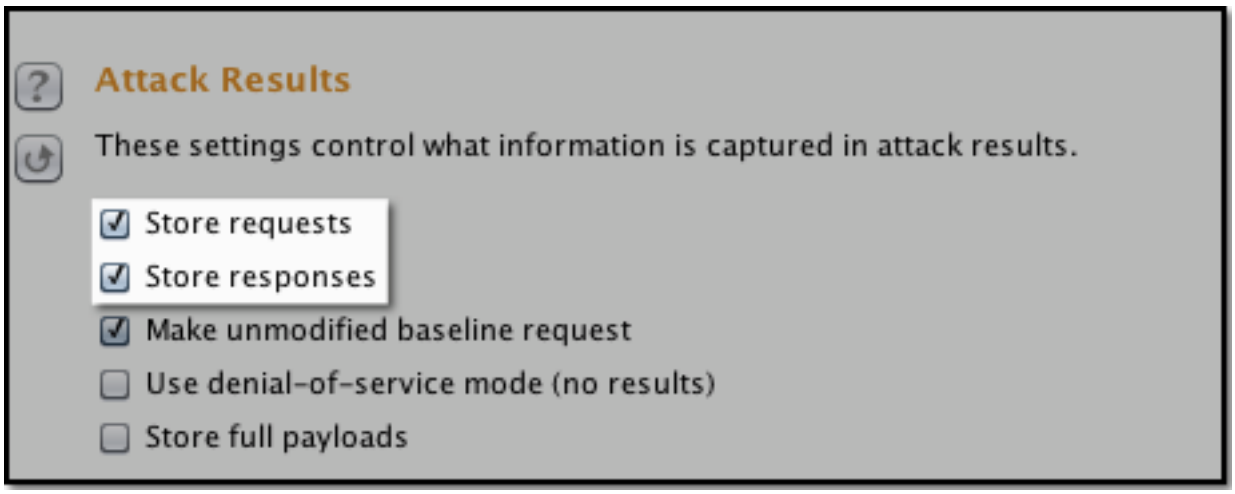
[Payload] 탭으로 가서, Payload Sets 옵션에서 “Payload set: 1” 을 선택하고 있는지 확인하고, [Load ···] 버튼을 클릭하고 사용자 이름 목록이 들어 있는 파일을 선택합니다. 사용자 이름 목록이 있는 파일을 불러오면 모든 사용자 이름이 아래 그림처럼 보여집니다.



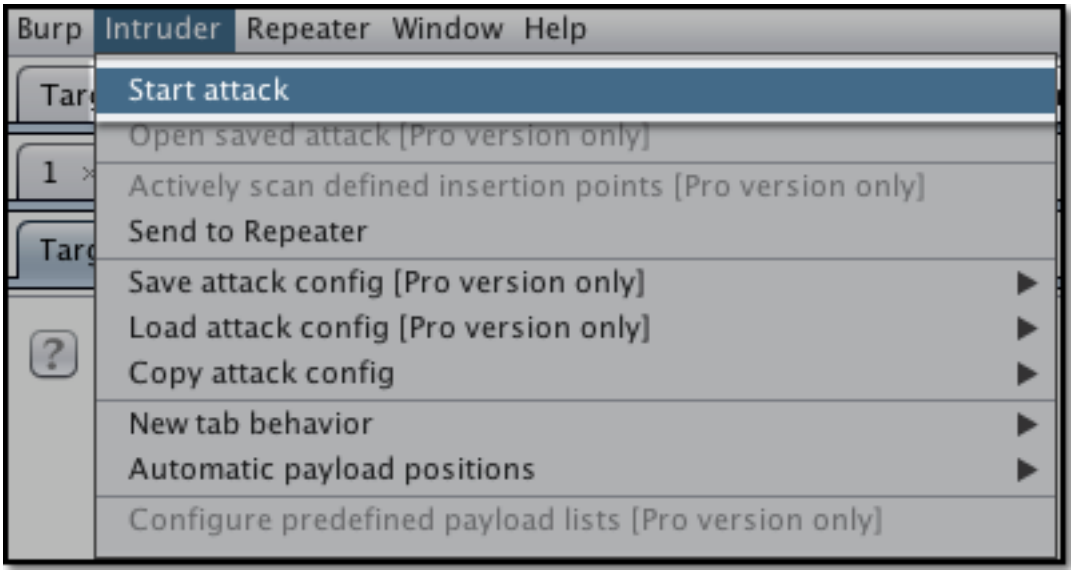
마찬가지로 “Payload set: 2” 를 선택하고 [Load ···] 버튼을 클릭해 암호 목록이 들어 있는 파일을 선택합니다.



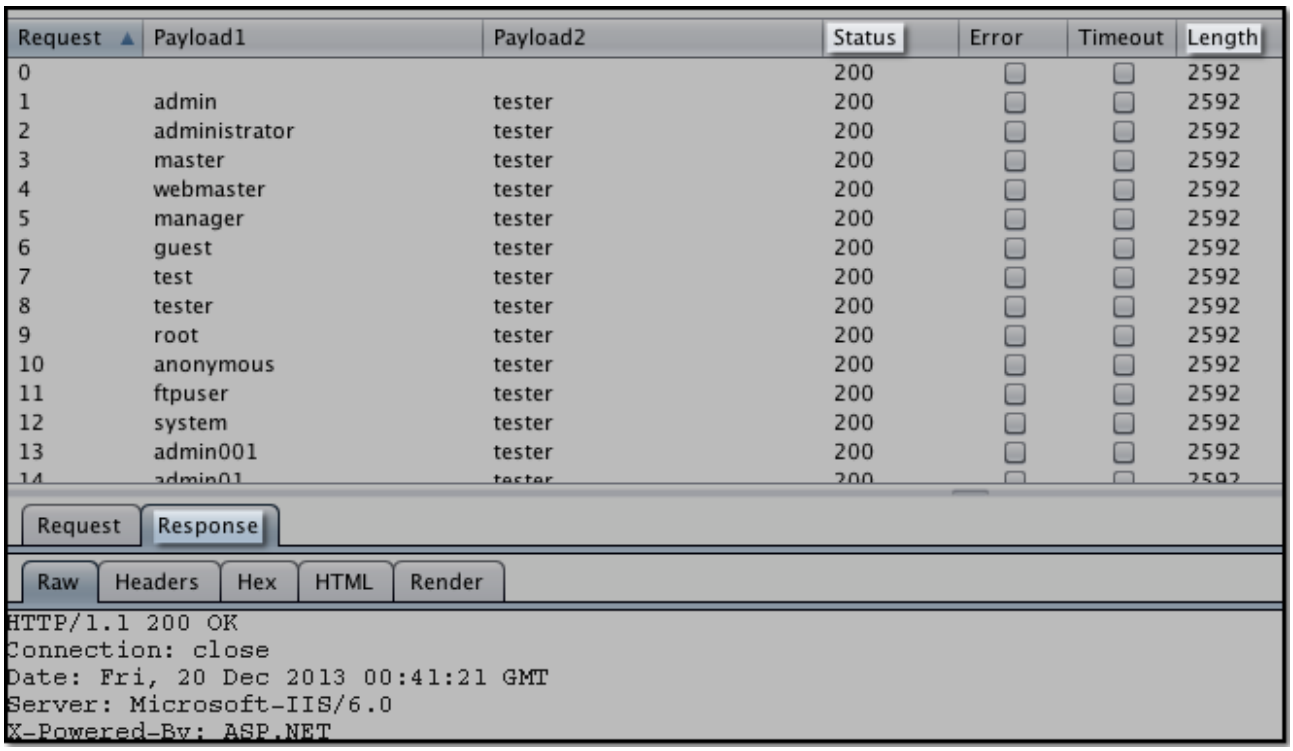
[Options] 탭으로 가서 Attack Results 옵션 아래에 "Store requests" 및 "Store responses" 항목이 설정 되어 있는지 확인합니다.



공격을 하기 위한 설정이 다 되었습니다. 왼쪽 상단 메뉴바에서 [Intruder] 를 클릭하고 “Start attack” 항목을 선택합니다. 새 창이 팝업 되고 결과가 만들어지는 것을 확인할 수 있습니다.

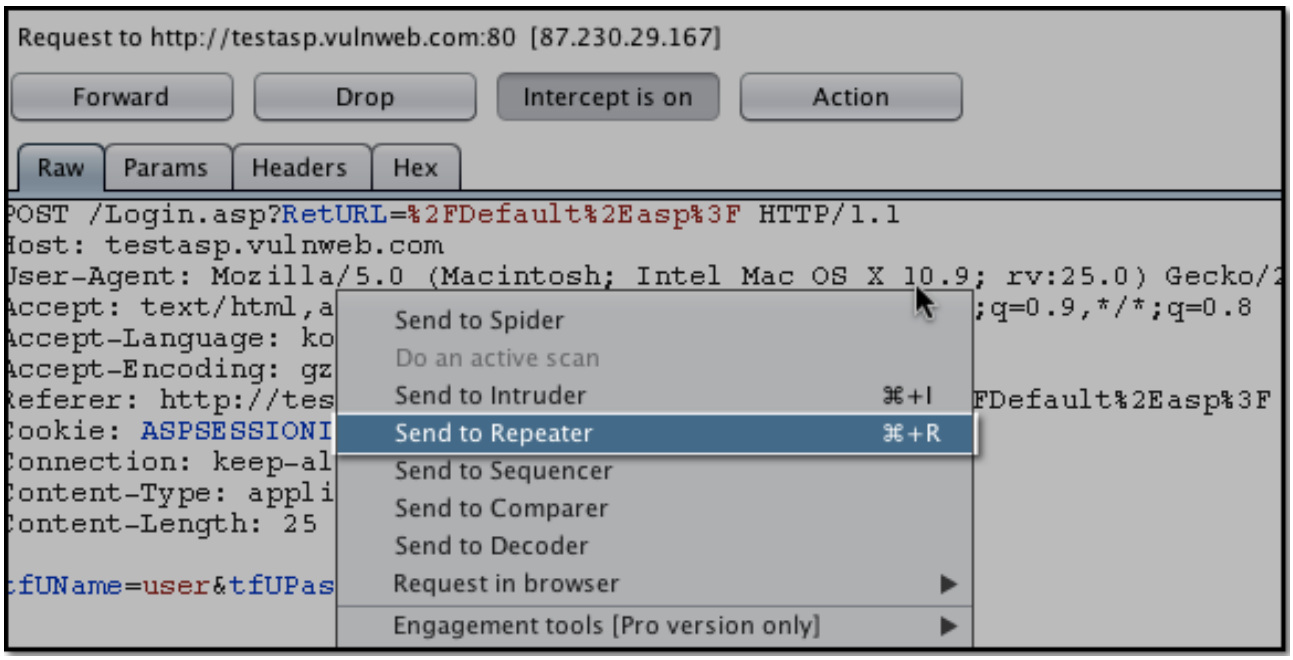


그럼 Intruder 의 Request 가 성공한 것을 어떻게 알 수 있을까요? 일반적으로 성공한 Request는 실패한 Request 와 다른 Response 또는 다른 상태의 Response 를 반환할 것입니다. “Status” 와 “Length” 를 확인하고 다른 상태 또는 길이를 가진 Response 의 Request 를 선택해 확인합니다.

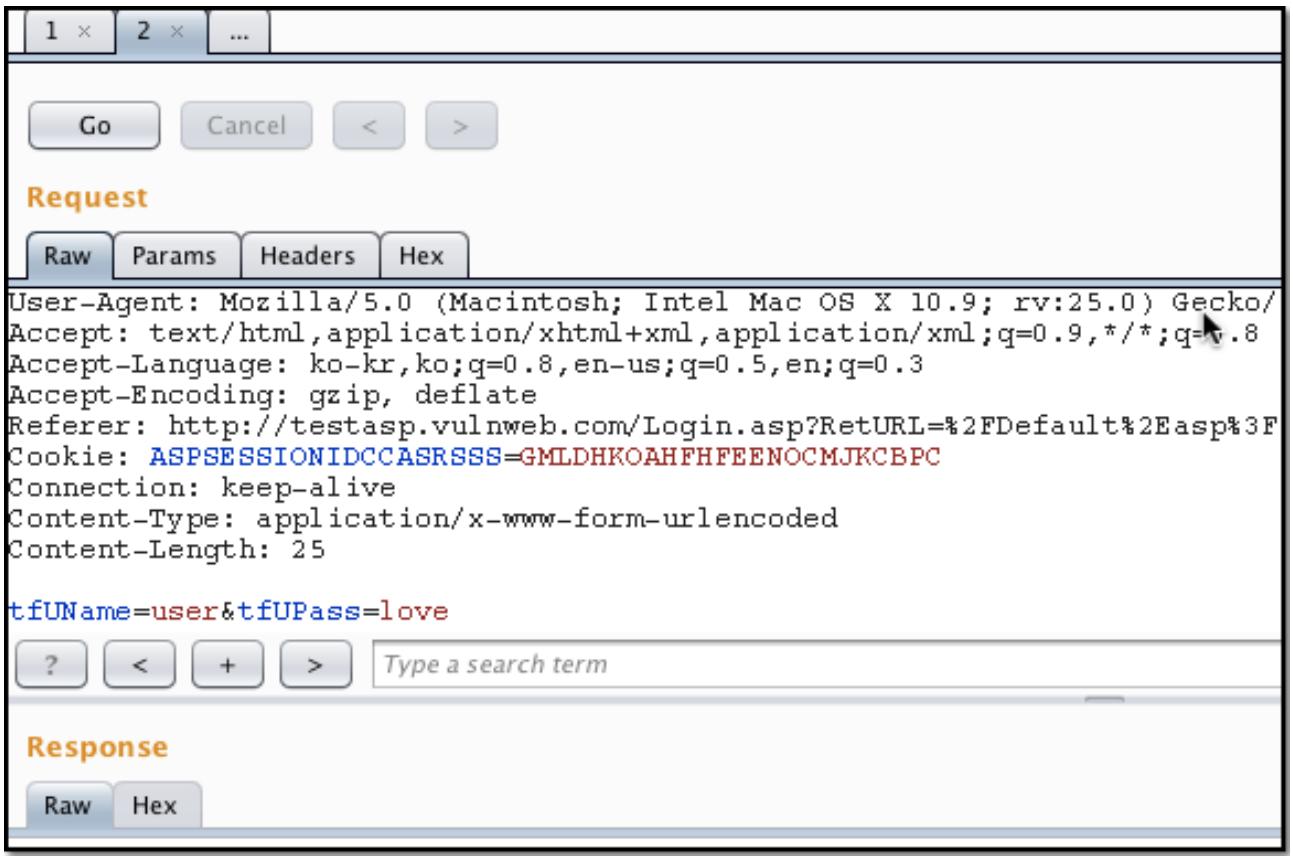


4) Repeater

Burp Repeater 를 사용해서 수동으로 Request 를 수정하고 Response 를 분석하기 위한 재전송 작업을 할 수 있습니다. [Intruder] 와 마찬가지로 사용자 Request 에서 마우스 오른쪽 클릭 후 “Send to Repeater” 항목을 선택하여 [Repeater] 로 Request 정보를 보냅니다. Intruder, Proxy 등 다양한 탭에서 Request 를 [Repeater] 로 보낼 수 있습니다.



[Repeater] 탭으로 이동하여 방금 보낸 Request 를 볼 수 있습니다. Repeater 상단에 1, 2 로 되어있는 두 개의 탭을 볼 수 있습니다. 각 Request 당 한 개의 탭을 사용합니다.



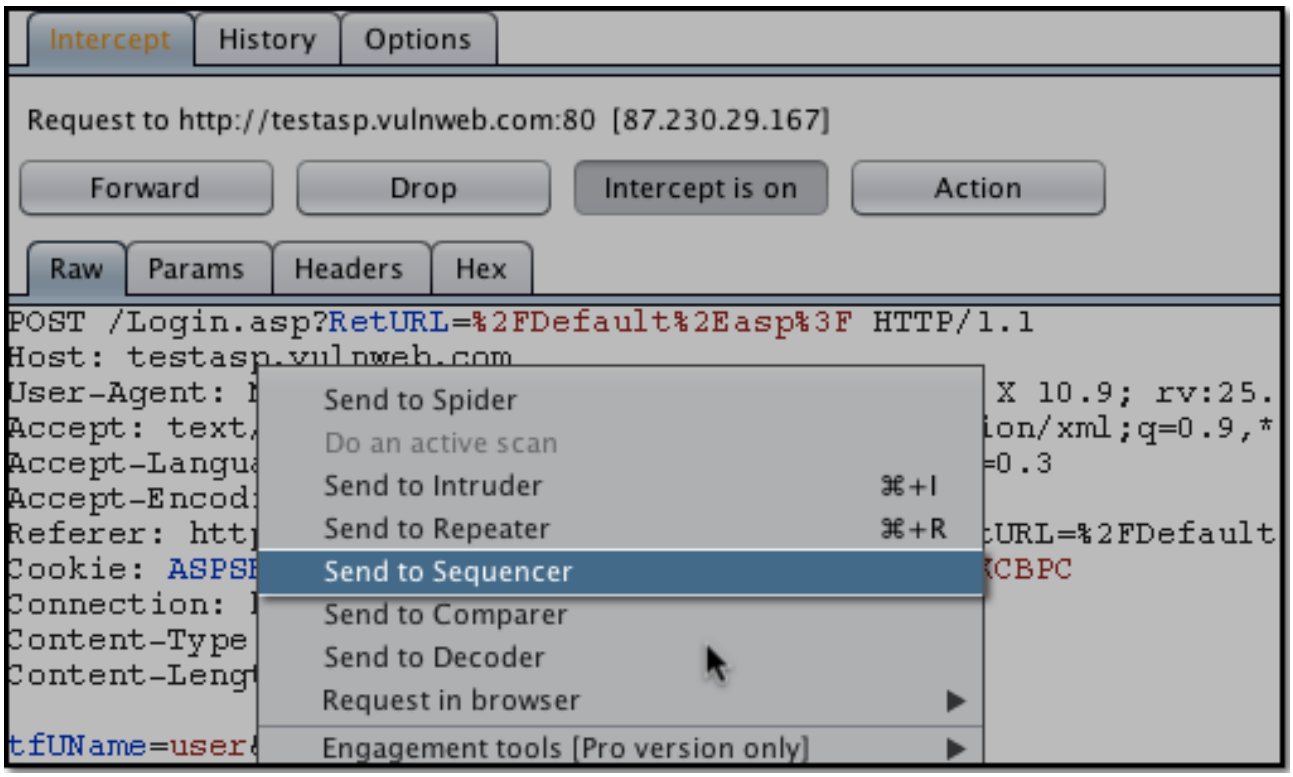
Request 를 [Raw], [Params], [Headers], [Hex] 형식으로 출력할 수 있습니다.

Request 를 수정한 후 그리고 [Go] 버튼을 눌러 해당 Request 를 서버로 보냅니다. 그리고 Response 섹션에서 Response 를 분석합니다.

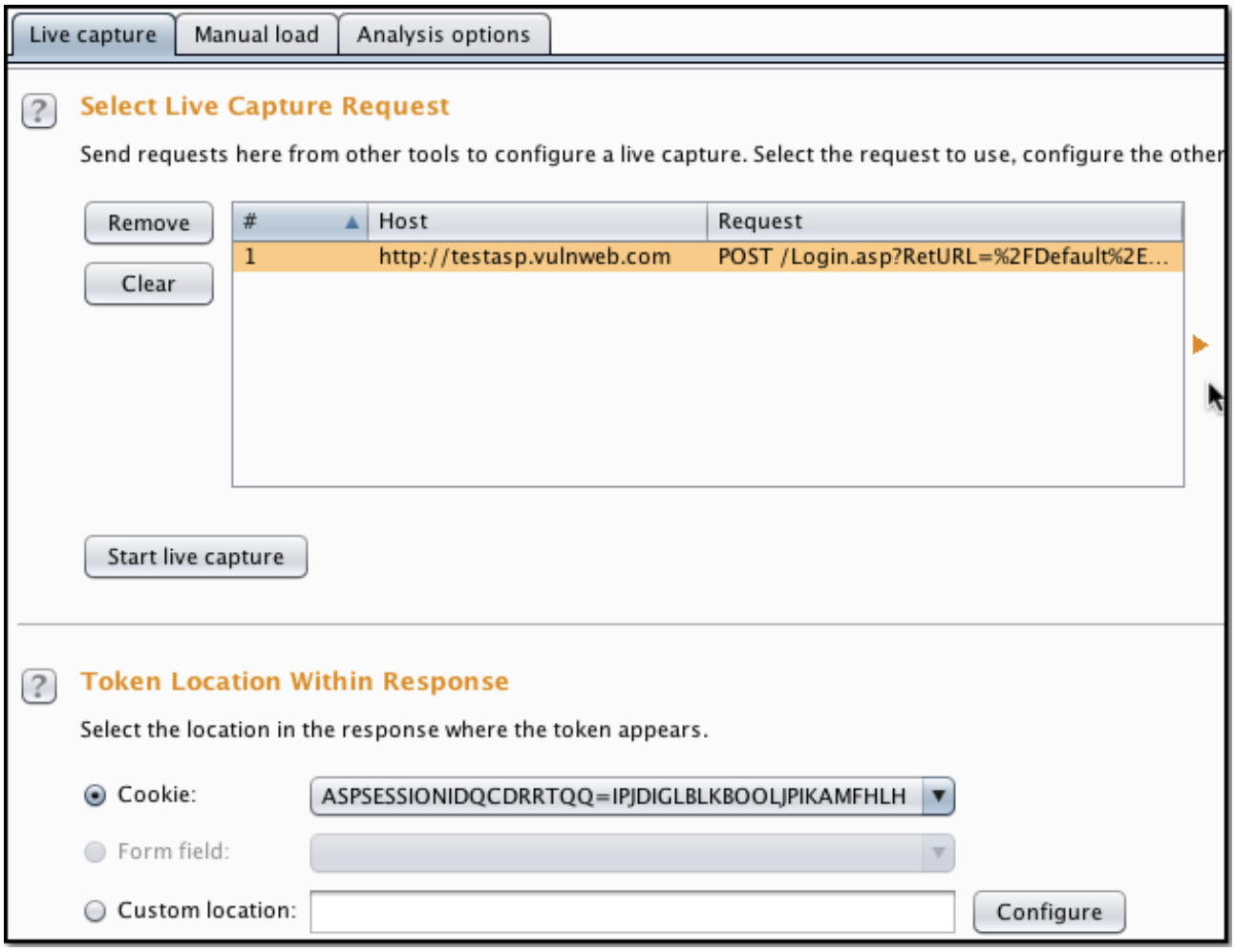
5) Sequencer

일반적으로 사용자 인증에 관련이 있기 때문에 웹 애플리케이션 보안 상 세션 토큰은 높은 임의성을 가지는 것이 중요합니다. Burp Sequencer 는 웹 애플리케이션이 자동으로 생성한 이러한 세션 토큰의 임의성을 파악하는 데 사용합니다.

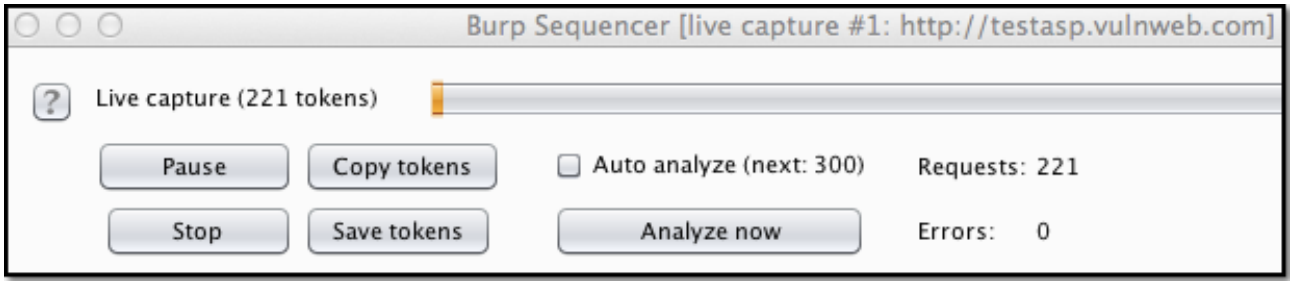
세션 토큰을 반환하는 Request 를 보내 봅니다. 다른 기능과 마찬가지로 사용자 Request 에서 마우스 오른쪽 클릭하여 “Send to Sequencer” 항목을 선택하여 [Sequencer] 로 Request 정보를 보냅니다.



[Sequencer] 탭으로 이동하면 자동으로 ID 매개 변수를 식별한 것을 볼 수 있으며, 사용자 정의 설정을 위해 [Manual load] 를 사용할 수 있습니다.

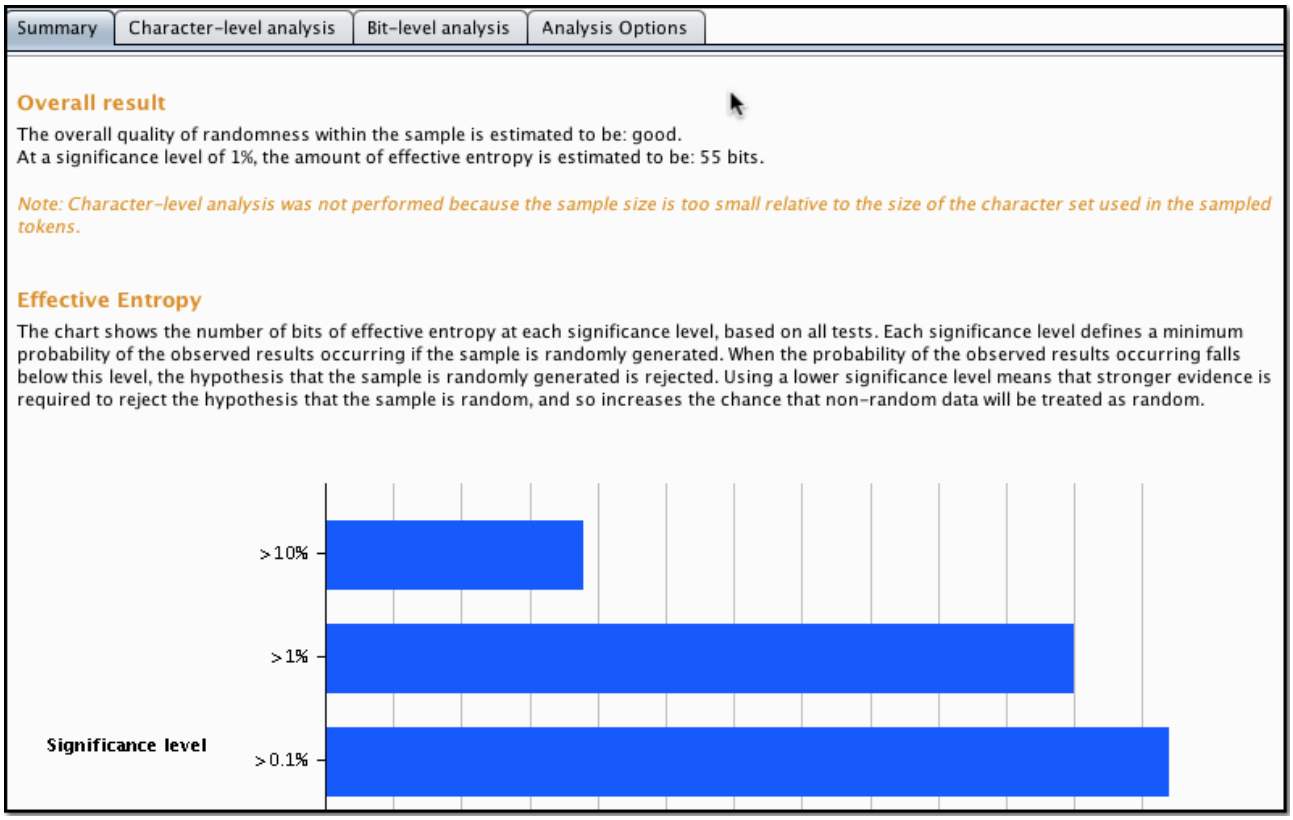


작업을 시작 하려면 [Start live capture]를 클릭 합니다.



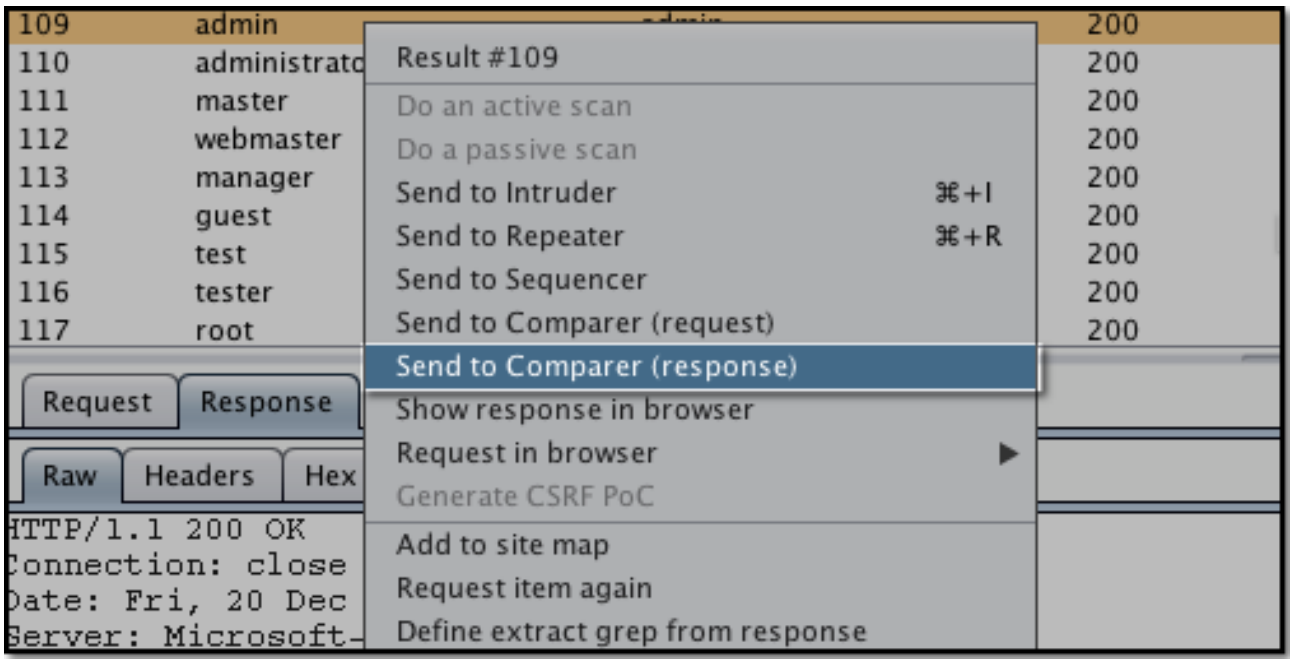
자동으로 생성하는 Request 수 및 수신하는 토큰 수를 볼 수 있습니다. 분석은 적어도 100~200 개의 토큰을 캡처하고 시작하는 것이 좋습니다. 더 많은 토큰이 더 나은 테스트 결과를 보여줄 수 있습니다. 충분한 토큰을 캡처 했다면, [Analyse now] 버튼을 클릭합니다.

결과는 아래 그림과 같이 표시 됩니다. 보이는 것처럼, 샘플의 전반적인 임의성은 우수한 것으로 추정합니다. 다양한 유형의 분석의 결과를 보기 위하여 상단의 탭을 선택하여 다양한 유형의 분석 결과를 볼 수 있습니다.

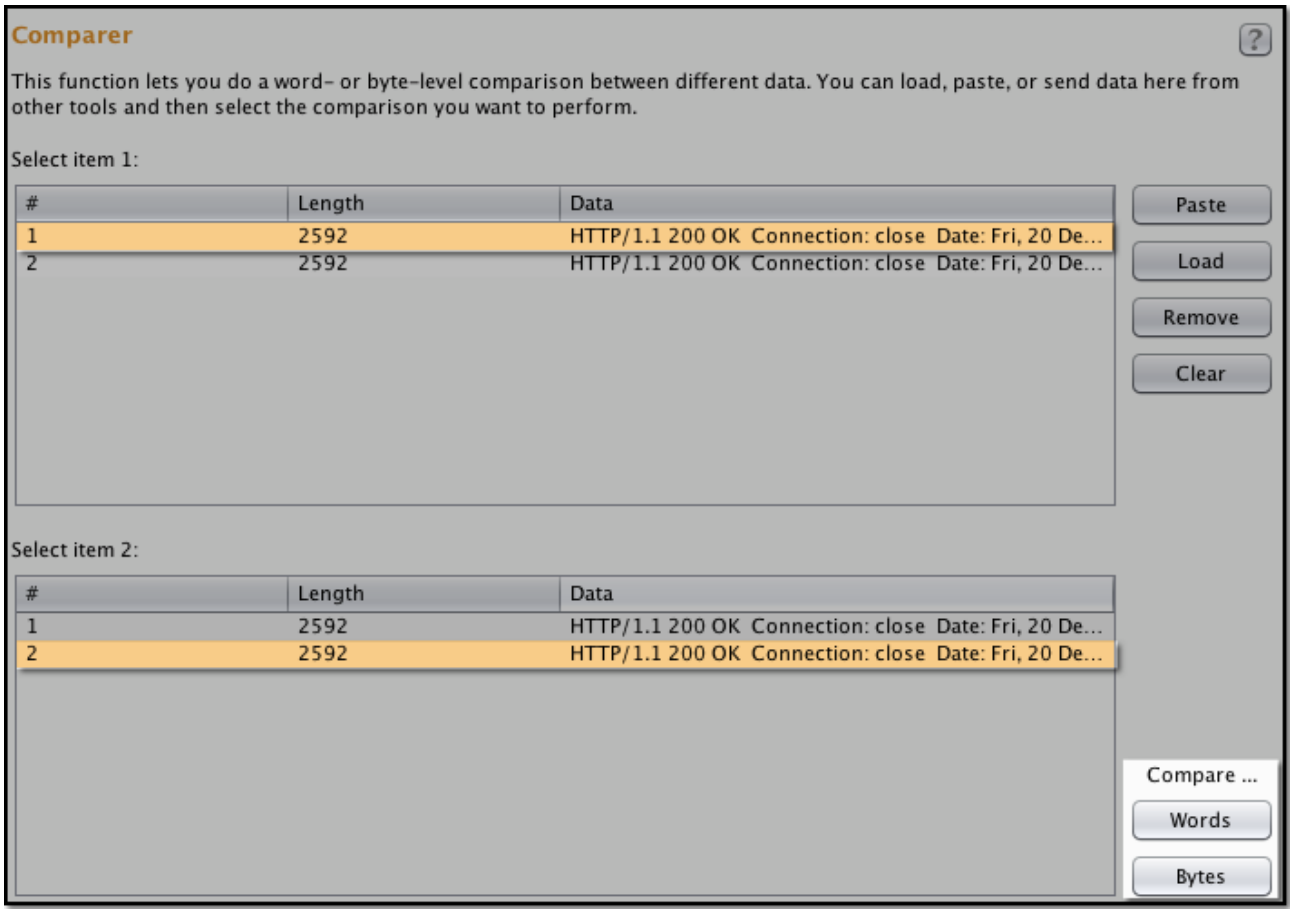


6) Comparer

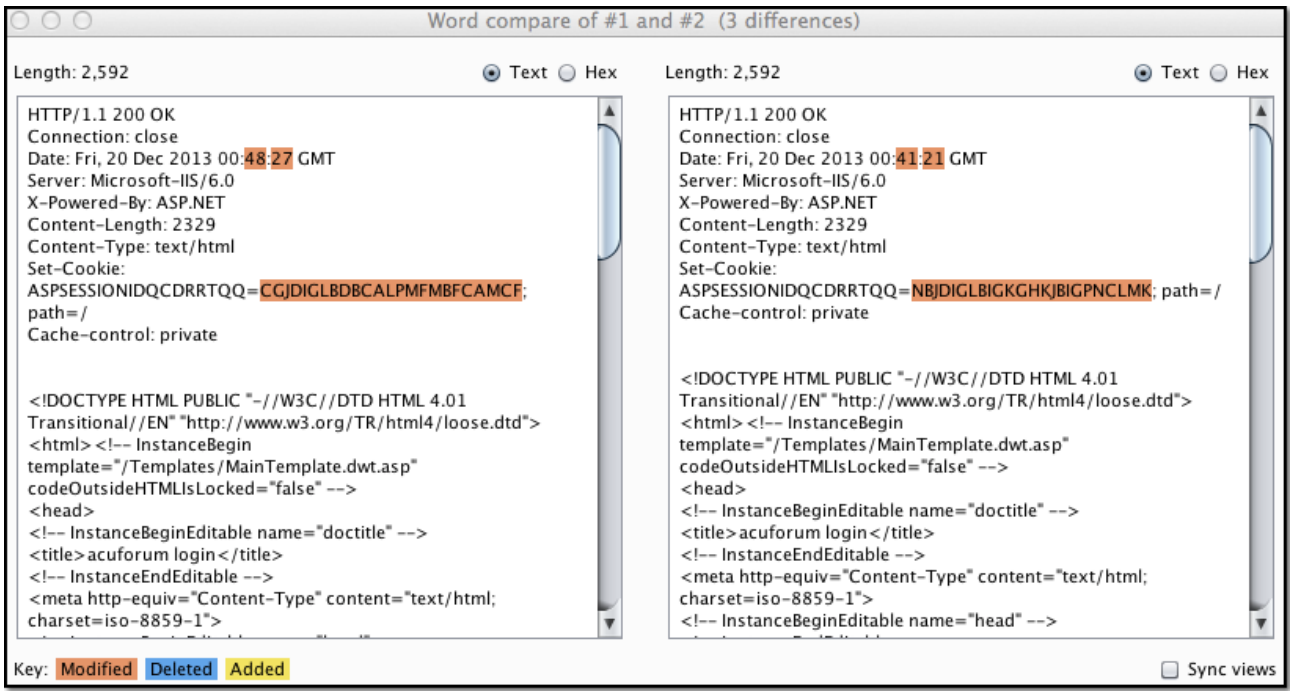
Burp Comparer 는 Request, Response 등과 같은 데이터를 비교하는데 사용합니다. 예제에서는 위에서 Brute Force(무차별 대입) 공격 시 받은 Response 두 개를 비교해 보겠습니다. [Intruder] 의 [Result] 탭에서 각각 Request 에 마우스 오른쪽 클릭 후 “Send to Comparer (response) 항목을 선택합니다.



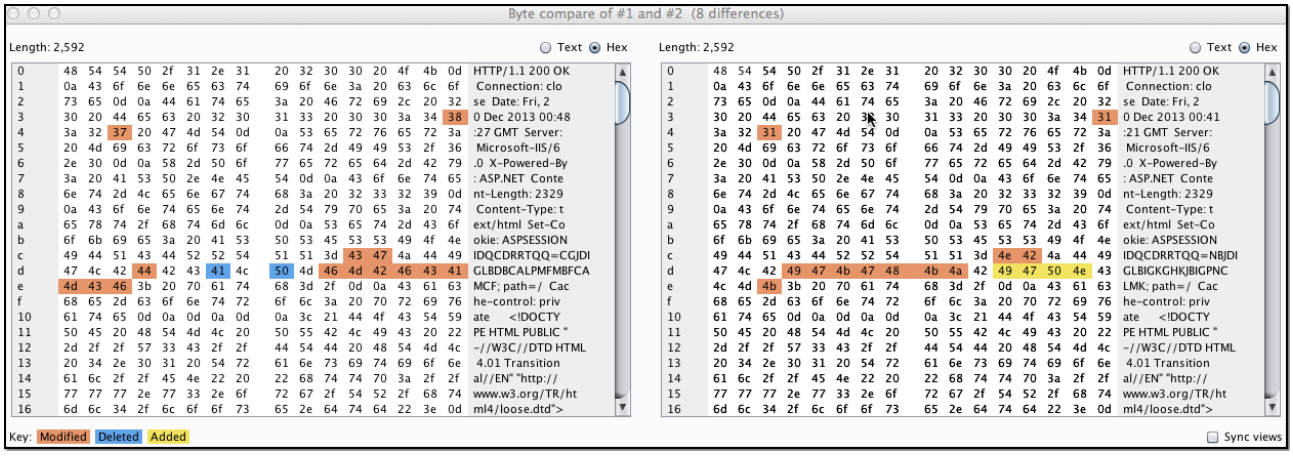
[Comparer] 탭으로 이동합니다. 사용자가 보낸 두 개의 Response 를 볼 수 있습니다. 윗 부분(item 1) 첫 번째 Response (#1)와 아래 부분(item 2) 두 번째 Response (#2) 를 클릭합니다.



Comparer 에서는 Words 또는 Bytes 2가지 유형으로 선택한 아이템을 비교를 할 수 있습니다. [Words] 버튼을 클릭하면 단어로 비교합니다. 결과는 아주 분명합니다. 두 응답의 세션 토큰이 다른 것을 확인할 수 있습니다.

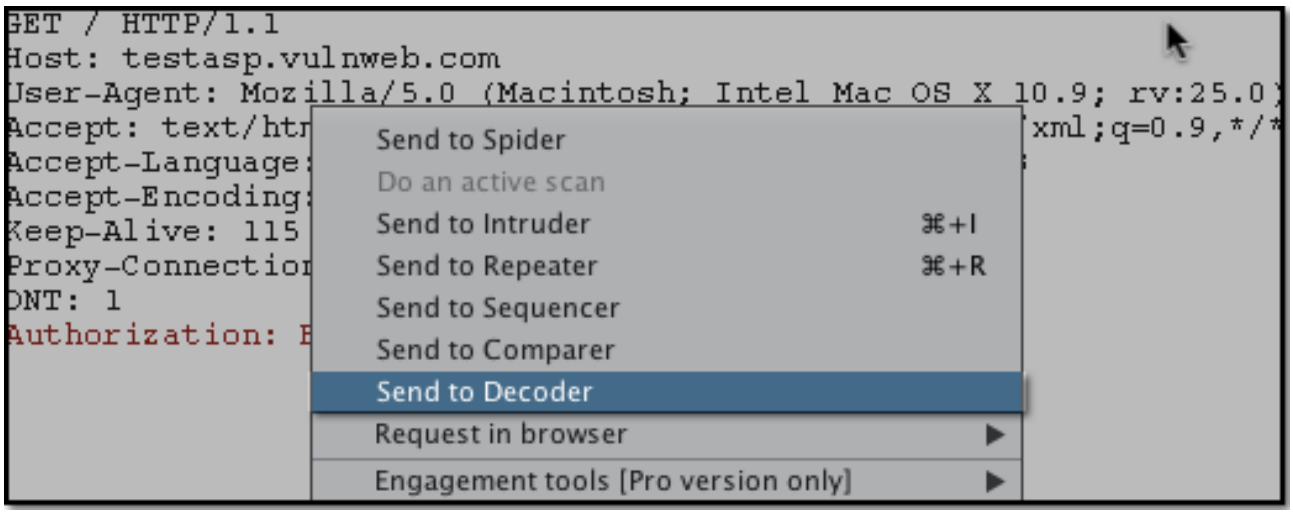


마찬가지로, 바이트를 사용하여 비교하면 다음과 같은 출력을 볼 수 있습니다.



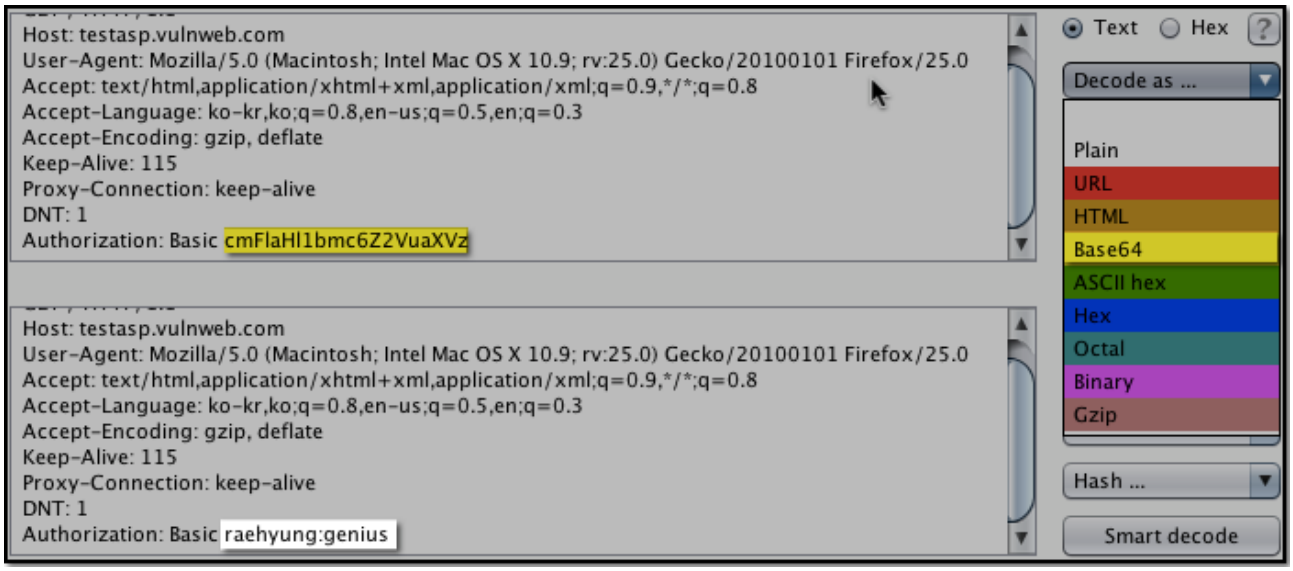
7) Decoder

Burp Decoder는 암호화 된 데이터를 해독하거나 데이터를 암호화하는데 사용합니다. 수동으로 [Decoder] 에 데이터를 붙여 넣거나 인코딩 된 Request 를 Decoder 에 보낼 수 있습니다. 이 경우 base64 인코딩 형식으로 암호화된 사용자 이름 및 암호를 포함하는 HTML Basic 인증 Request 를 [Decoder] 로 보낼 것입니다. 다른 기능과 마찬가지로 사용자 Request 에서 마우스 오른쪽 클릭 후 “Send to Decoder” 항목을 선택하여 [Decoder] 로 Request 정보를 보냅니다.



암호화된 부분을 드래그하고 [Decode as ⋯] 버튼을 클릭하고 “Base64” 항목을 선택합니다.

Burp Decoder 가 base64로 암호화된 문자열을 해독하여 사용자 이름/암호를 평문으로 제공합니다.



8) Scanner

Burp Scanner 는 가장 강력한 웹 애플리케이션 취약점 탐색 도구 중 하나입니다. 하지만, 다른 도구들처럼 완벽하지 않으며, False Positive 가 발생할 수 있습니다. Burp Scanner 는 무료 버전에서는 사용할 수 없습니다.

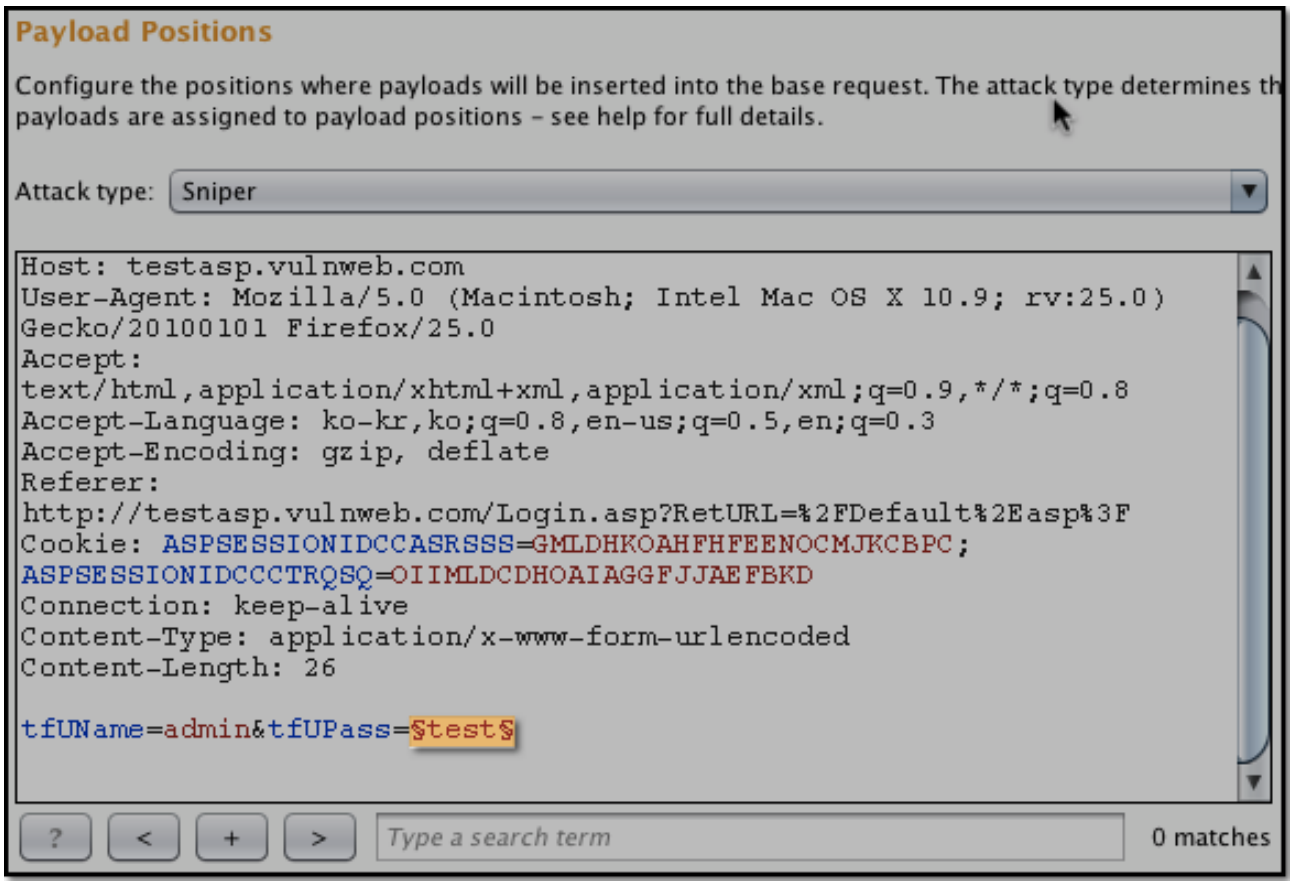
응용: Burp Intruder via SQL Injection

Blind 방식이나 Error 기반의 취약점으로 작동할 수 있는 SQL Injection 도구들은 많이 존재하며, Kali 리눅스 같은 배포판 OS 에 미리 설치되어 실행할 준비가 되어 있습니다. SQLMap 은 그 좋은 예입니다. 이런 도구들은 데이터베이스에서 데이터를 추출하는 것 외 루트 권한을 획득하는 등 다른 많은 일을 할 수 있습니다. 하지만 이 문서에서는 Burp Intruder 를 통해 구현할 수 있는 (단지 데이터 추출만을 위한) SQL 인젝션 기술을 설명하고자 합니다.

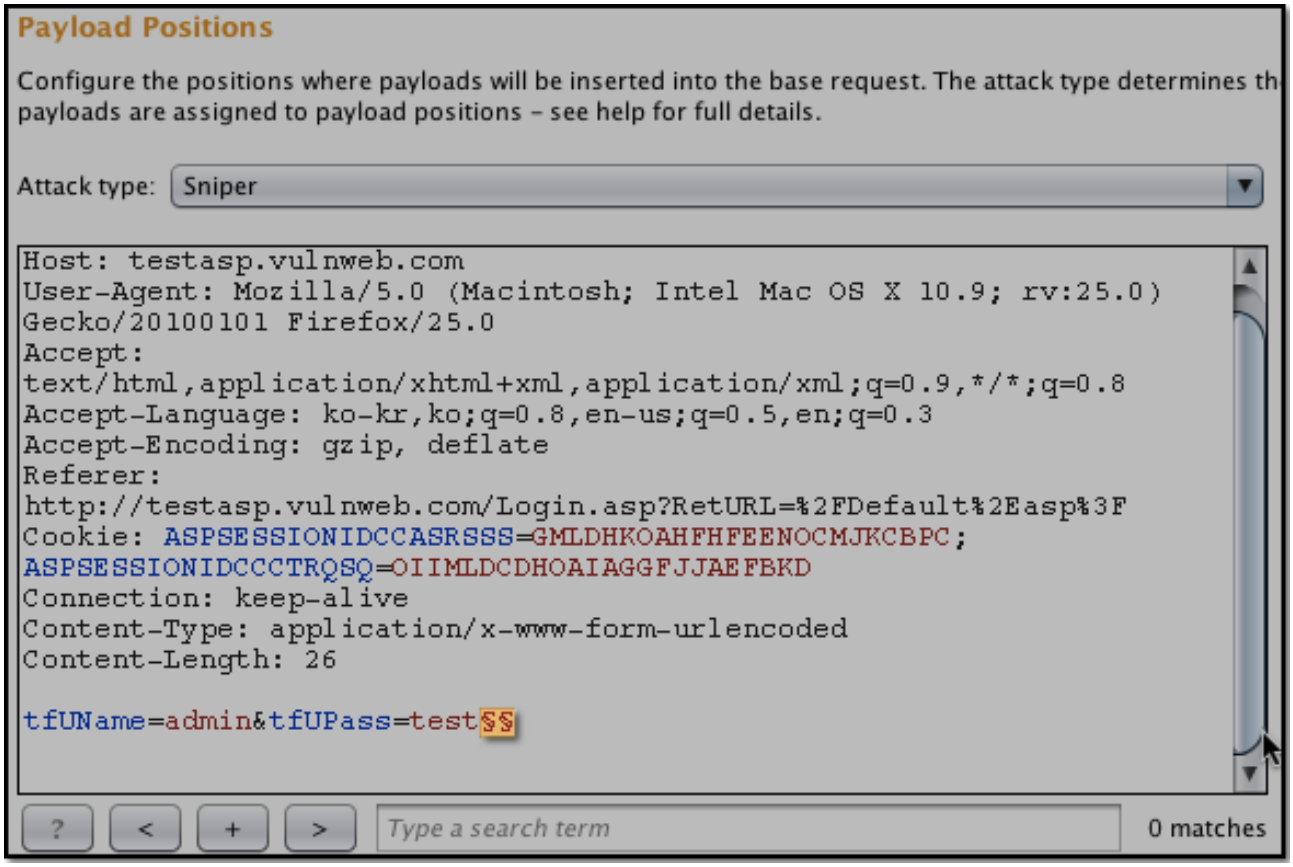
제일 먼저 해야할 일은 Request 를 확인을 통해 SQL Injection 에 취약한 부분을 발견하는 것입니다:

SQL Injection 공격이 가능해 보이는 Request 를 마우스 오른쪽 클릭 후 “Send to Intruder” 항목을 선택합니다.

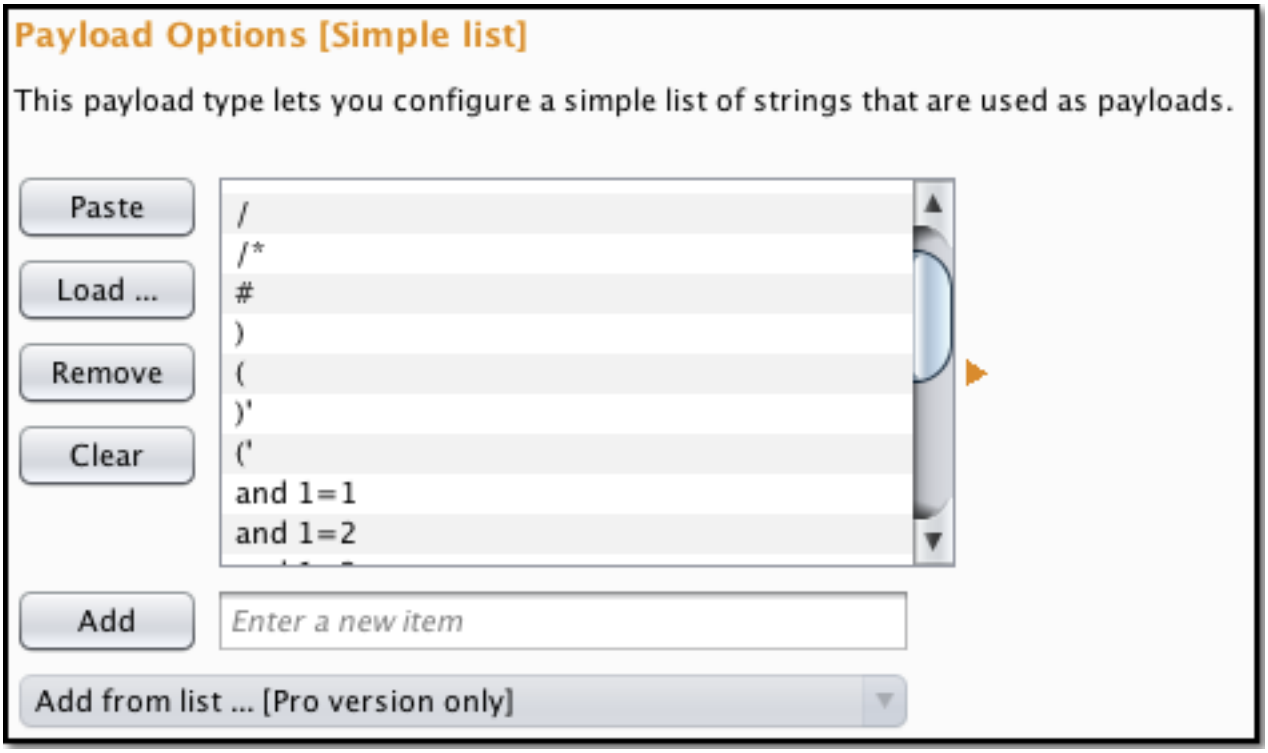
다음과 같이 SQL 인젝션이 가능한 파라미터의 값을 Intruder 의 변수로 지정하며 단일 Payload Set 을 사용할 것이므로 공격 유형을 “Sniper” 로 지정합니다.



Intruder 의 변수는 파라미터 값 다음에 올 수도 있습니다.



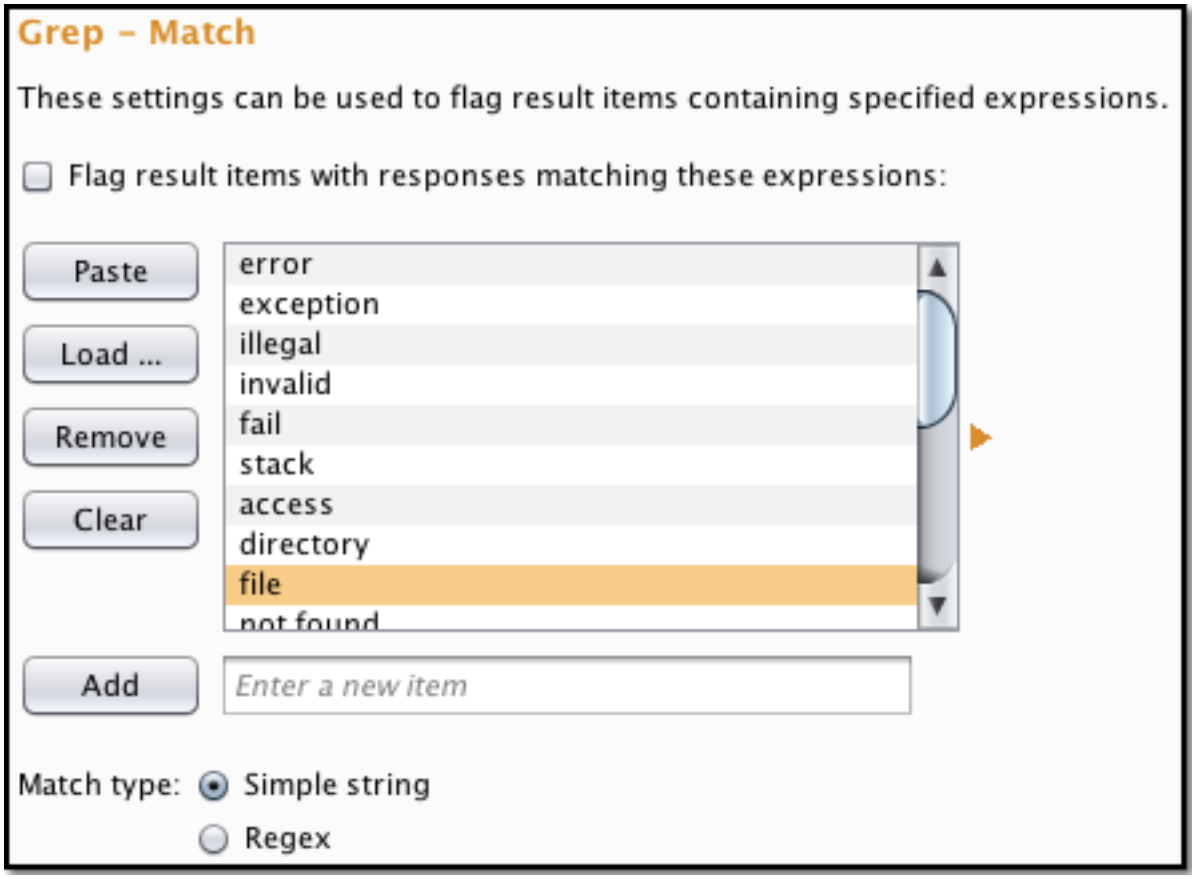
다음으로 Payload Set 을 지정합니다.



SQL Injection 가능 여부 확인을 위한 Payload Set 으로 다음과 같은 목록을 사용할 수 있습니다.

SQLi Test
'
"
/
/*
#
)
(
)'
('
and 1=1
and 1=2
and 1>2
and 1<=2
+and+1=1
+and+1=2
+and+1>2
+and+1<=2
/**/and/**/1=1
/**/and/**/1=2
/**/and/**/1>2
/**/and/**/1<=2

마지막으로 [Intruder]의 [Options] 탭에서 Grep 항목을 설정합니다. 여기서는 Intruder 프로세스 후 얻는 결과 페이지 목록을 설정할 수 있습니다. 예를 들어 Grep 에서 “Cookie” 를 추가하면, 결과 페이지 중 “Cookie” 라는 단어가 존재하는 페이지만 결과 목록에 나타납니다.



Grep 에 설정할 Payload Set 으로 다음과 같은 목록(SQL Error 메시지)을 사용할 수 있습니다.

SQL Error Message
unknown column
unknown
no record found
mysql_num_rows()
mysql_fetch_array()
Error Occurred While Processing Request
Server Error in '/' Application
Microsoft OLE DB Provider for ODBC Drivers error
error in your SQL syntax
Invalid Querystring
OLE DB Provider for ODBC
VBScript Runtime

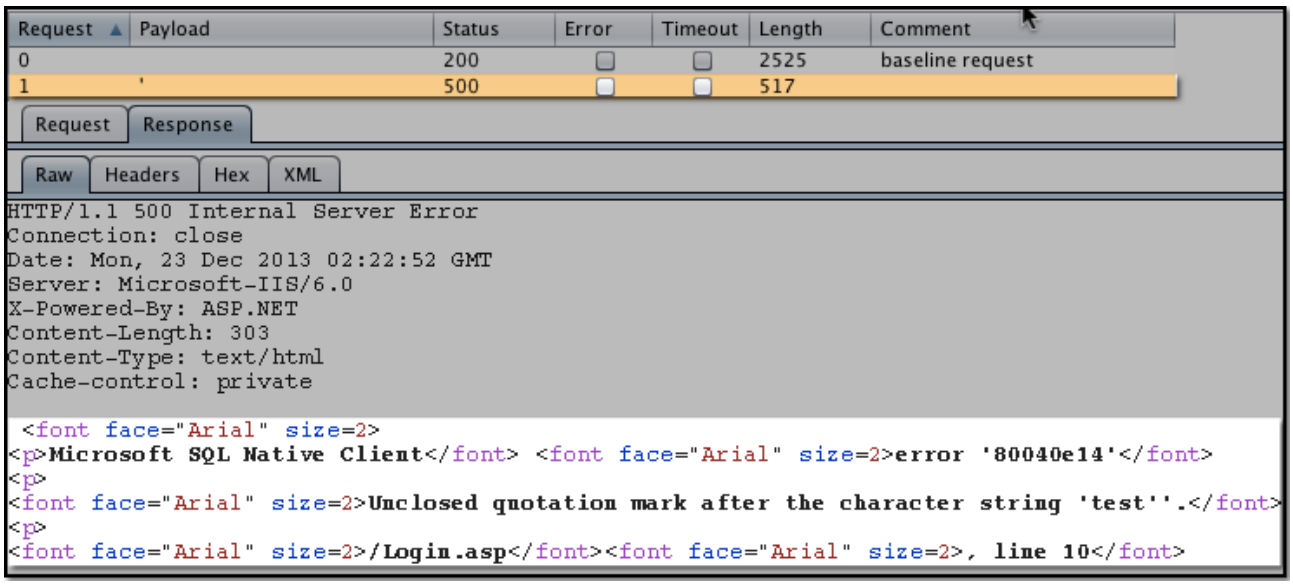
SQL Error Message
ADODB.Field
BOF or EOF
ADODB.Command
JET Database
mysql_fetch_row()
include()
mysql_fetch_assoc()
mysql_fetch_object()
mysql_numrows()
GetArray()
FetchRow()
Input string was not in a correct format
Microsoft VBScript
A syntax error has occurred
ADODB.Field error
ASP.NET is configured to show verbose error messages
ASP.NET_SessionId
Active Server Pages error
An illegal character has been found in the statement
An unexpected token "END-OF-STATEMENT" was found
CLI Driver
Can't connect to local
Custom Error Message
DB2 Driver
DB2 Error
DB2 ODBC
Died at
Disallowed Parent Path
Error Diagnostic Information
Error Message : Error loading required libraries.
Error Report
Error converting data type varchar to numeric

SQL Error Message
Fatal error
Incorrect syntax near
Index of
Internal Server Error
Invalid Path Character
Invalid procedure call or argument
Invision Power Board Database Error
JDBC Driver
JDBC Error
JDBC MySQL
JDBC Oracle
JDBC SQL
Microsoft OLE DB Provider for ODBC Drivers
Microsoft VBScript compilation error
Microsoft VBScript error
MySQL Driver
MySQL Error
MySQL ODBC
ODBC DB2
ODBC Driver
ODBC Error
ODBC Microsoft Access
ODBC Oracle
ODBC SQL
ODBC SQL Server
OLE/DB provider returned message
ORA-0
ORA-1
Oracle DB2
Oracle Driver
Oracle Error
Oracle ODBC

SQL Error Message
PHP Error
PHP Parse error
PHP Warning
Parent Directory
Permission denied: 'GetObject'
PostgreSQL query failed: ERROR: parser: parse error
SQL Server Driver][SQL Server
SQL command not properly ended
SQLException
Supplied argument is not a valid PostgreSQL result
Syntax error in query expression
The error occurred in
The script whose uid is
Type mismatch
Unable to jump to row
Unclosed quotation mark before the character string
Unterminated string constant
Warning: Cannot modify header information - headers already sent
Warning: Supplied argument is not a valid File-Handle resource in
Warning: mysql_query()
Warning: pg_connect(): Unable to connect to PostgreSQL server: FATAL
You have an error in your SQL syntax near
detected an internal error [IBM][CLI Driver][DB2/6000]
error
include_path
invalid query
is not allowed to access
missing expression
mySQL error with query
mysql error
on MySQL result index
on line

SQL Error Message
server at
server object error
supplied argument is not a valid MySQL result resource
unexpected end of SQL command

이제 Burp Intruder 를 실행하고 취약한 Request 를 확인합니다.



같은 방법으로 발견한 Request 에 대해 Payload Set 을 변경하여 Intruder 를 다시 실행합니다. Payload Set 으로 알려진 SQL Injection 구문을 목록화하여 사용할 수 있습니다.

참고 문서

http://resources.infosecinstitute.com/burp-suite-walkthrough/
http://resources.infosecinstitute.com/fuzzing-sql-injection-burp-suite-intruder/