웹 취약점 (2)

Burp Suite 사용하기

Burp Suite란?

- 전 세계 보안 전문가들이 가장 많이 쓰는 웹 보안 테스트 툴
- 웹 브라우저와 서버 사이의 트래픽을 가로채고, 수정하고, 재전송할 수 있는 프록시(Proxy) 역할
- 브라우저 ↔ 서버 사이에 중간자(Man-in-the-Middle, MITM) 프록시처럼 동작
- 내가 접속하는 웹사이트의 요청/응답을 가로채서 보고, 수정할 수 있음
- 보안 취약점(예: XSS, SQL Injection, CSRF 등)을 찾거나 재현하는 데 활용

Burp Suite의 주요 기능

Proxy

- 브라우저 트래픽을 가로채서 헤더/본문 확인, 수정, 차단 가능
- 예: 로그인 요청을 가로채서 비밀번호를 바꿔보거나, 쿠키 값을 수정해봄

Repeater

- 특정 요청을 반복적으로 보내면서 파라미터 값을 조금씩 바꿔 테스트
- 예: 로그인 시도 시 id=admin pw=1234, pw=12345 ... 반복 테스트

Intruder (자동화 공격 도구)

- 여러 입력값을 자동으로 대입(브루트포스, 파라미터 조합 등)
- 예: 취약한 로그인 폼에서 비밀번호 대입 공격

Scanner (Pro 버전)

- 자동으로 웹 취약점 스캔 (SQLi, XSS 등)
- 취약한 파라미터나 입력창을 자동 탐지

Decoder/Comparer

- 인코딩된 값(Base64, URL encoding 등)을 쉽게 해석
- 응답 비교 기능 제공

Burp Suite 버전

Community Edition (무료판)

- Proxy, Repeater 등 핵심 기능은 제공
- Intruder 자동화 제한, Scanner 없음

Professional (유료판)

- 자동화 스캐너, Intruder 무제한, CI/CD 연동 등 지원

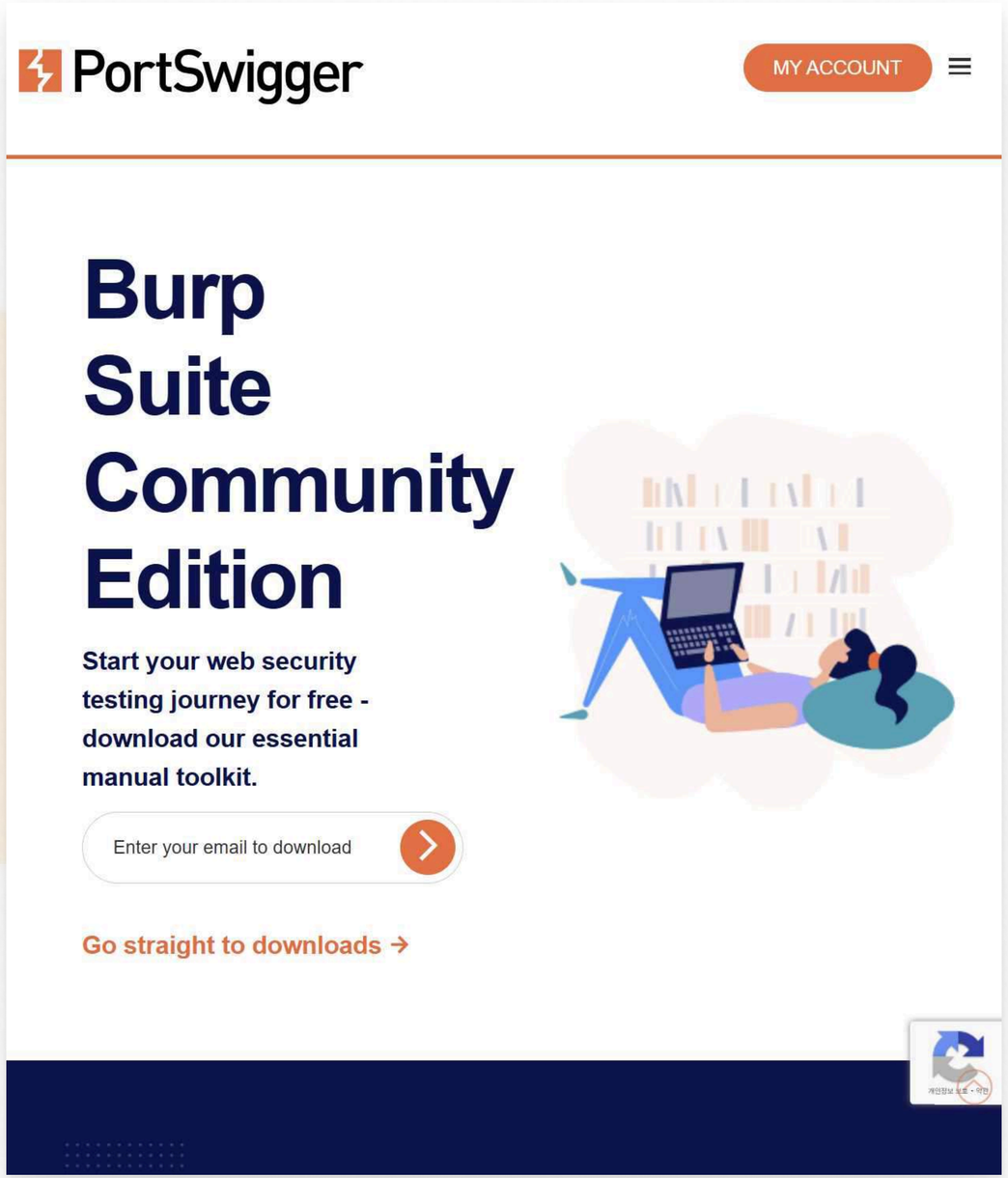
Enterprise

- 대규모 조직에서 자동화 스캔, 보고서 기능 강화

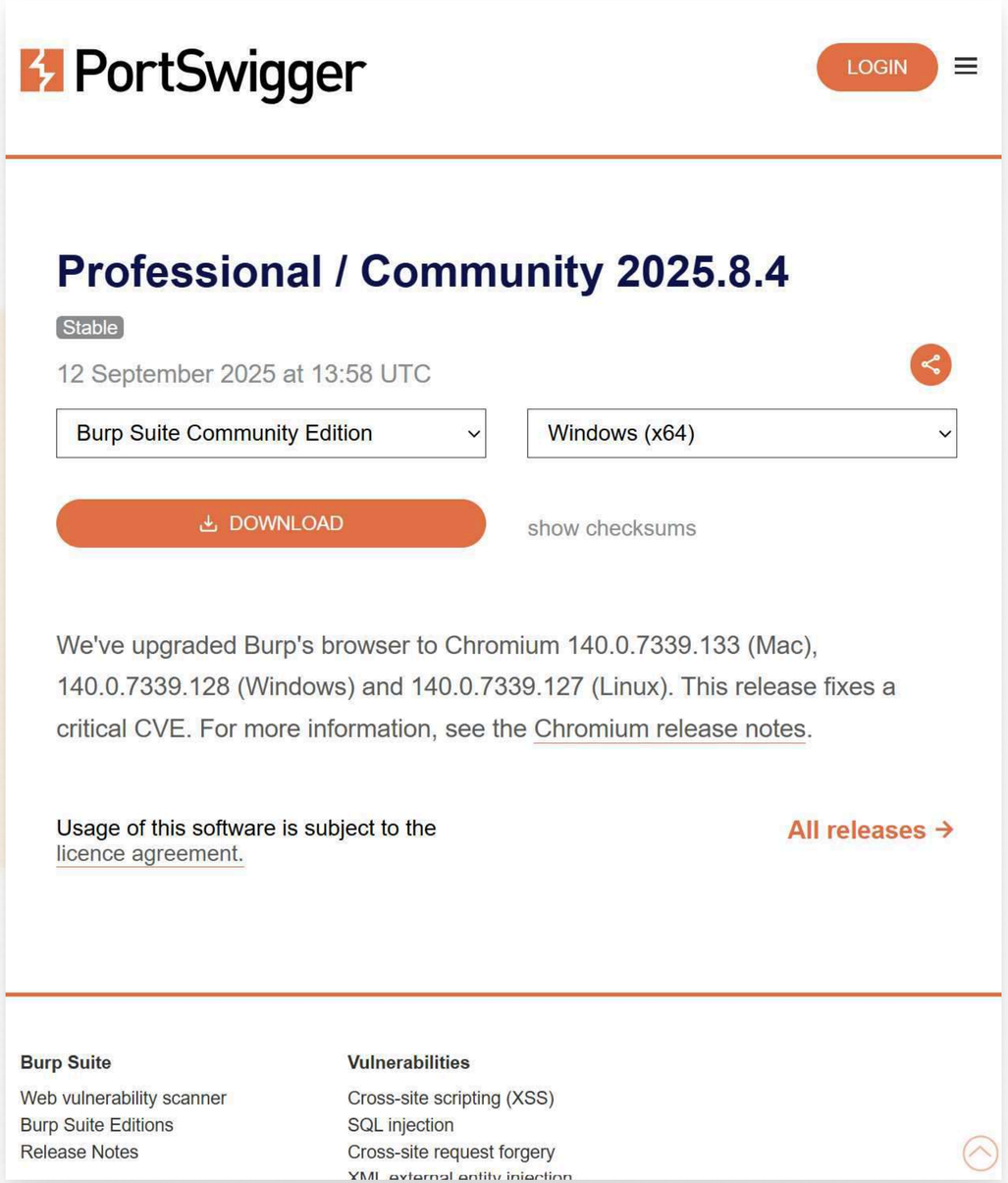
주의

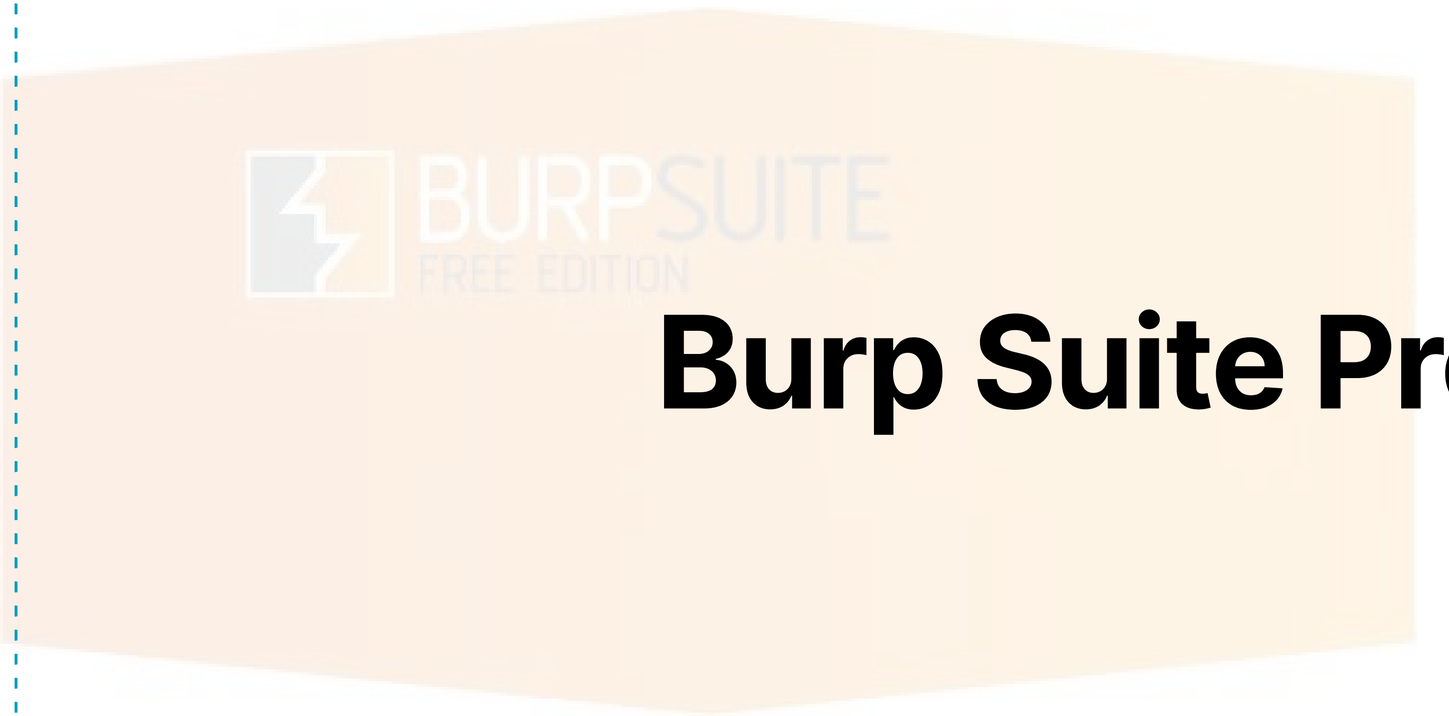
- Burp Suite는 강력한 해킹 도구에 해당합니다.
- 본인 소유의 웹사이트나, 허가받은 실습용 환경(CTF, DVWA, Juice Shop 등)에서만 사용해야 합니다.
- 허가 없이 남의 웹사이트에 Burp Suite로 테스트하는 건 불법입니ㅏ.

Burp Suite 다운로드



Burp Suite 다운로드

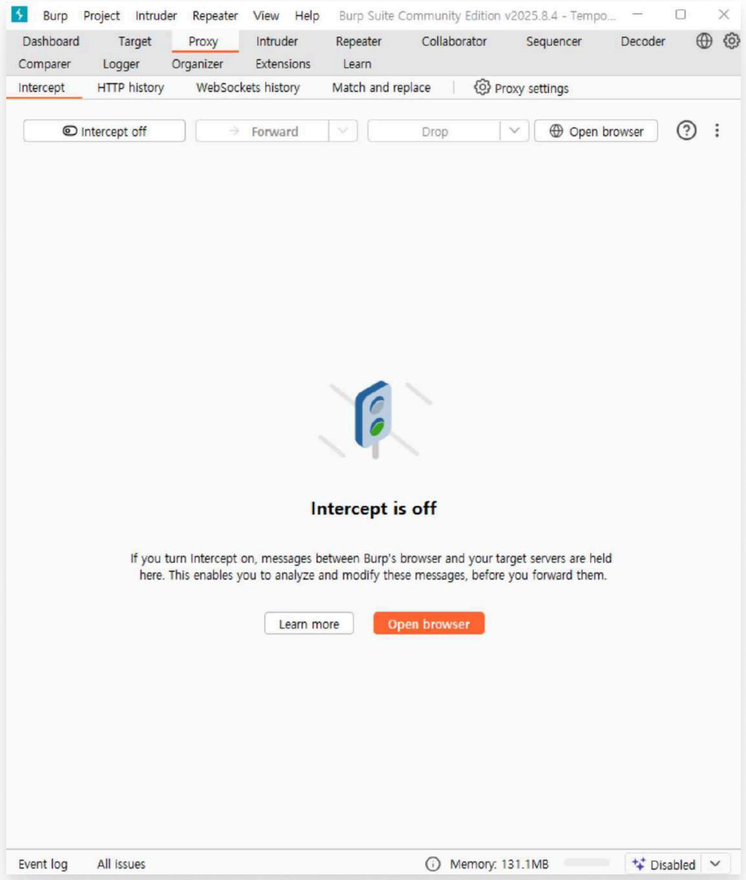




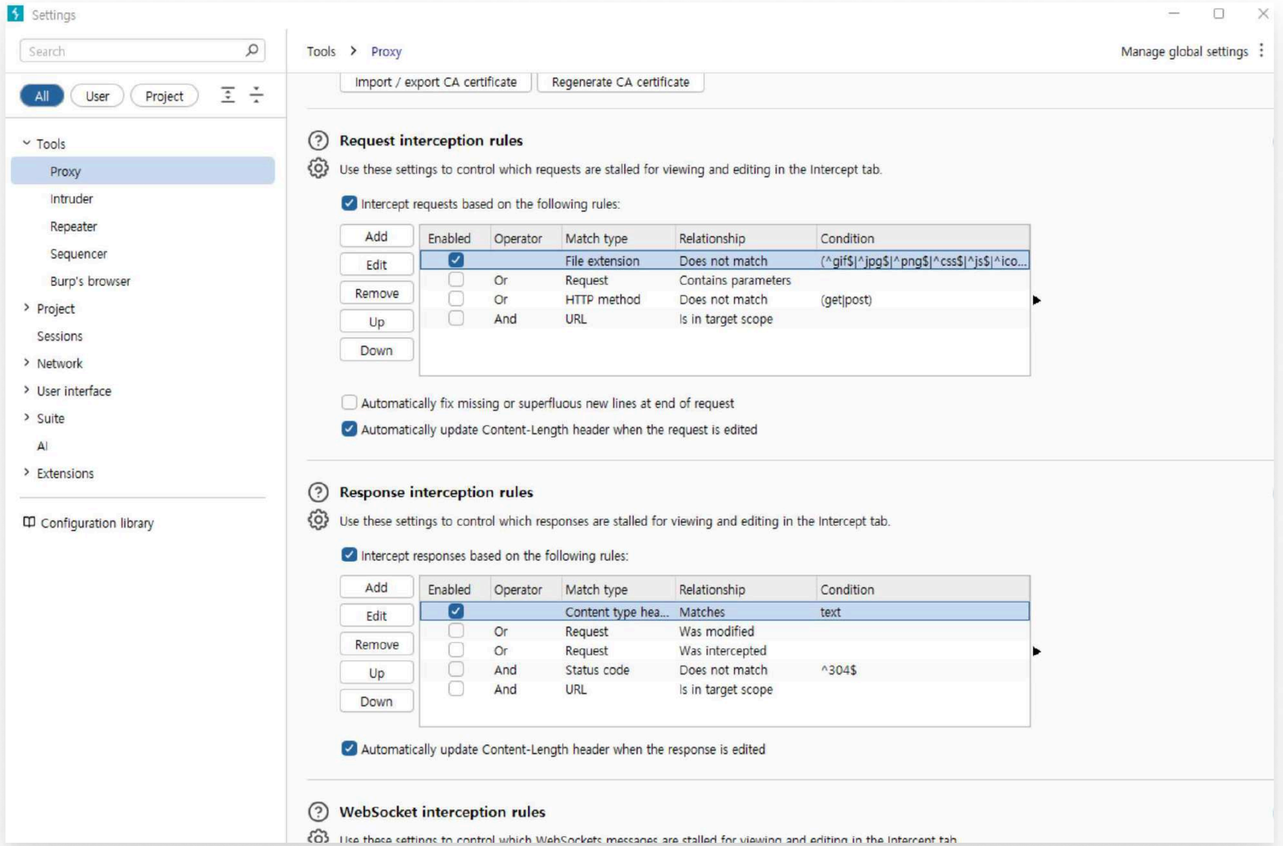
Burp Suite Proxy 실습

Proxy란?

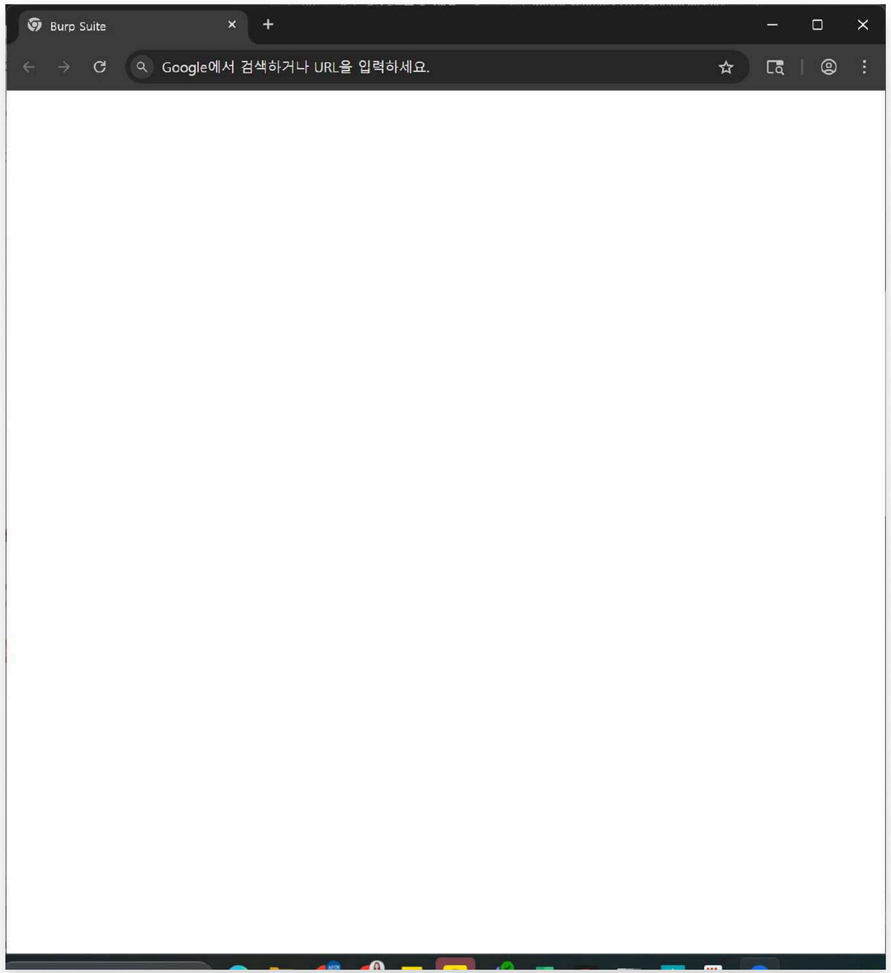
Proxy 접속



Proxy Setting > Reqest, Response 체크

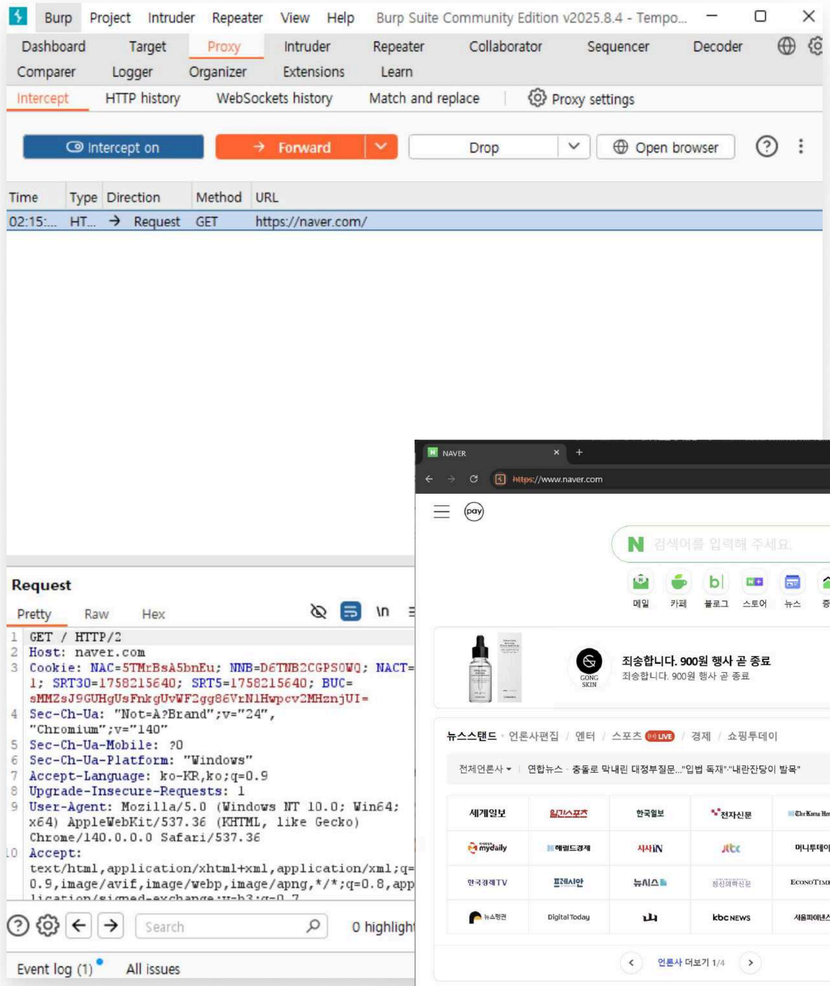


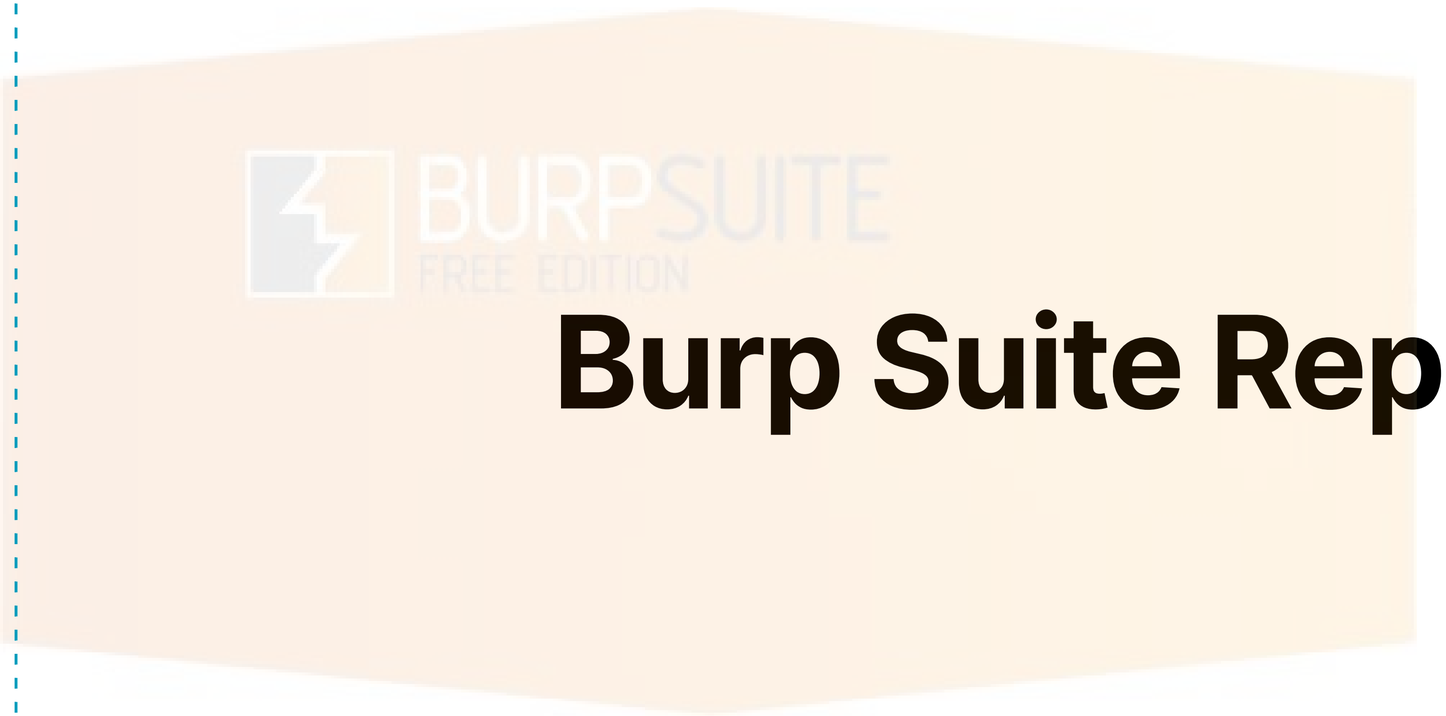
Proxy > Open browser



Proxy >Intercept on

다음 단계로 넘어가고 싶을 때마다 Ctrl + F 또는 Forward 버튼을 눌러주세요.

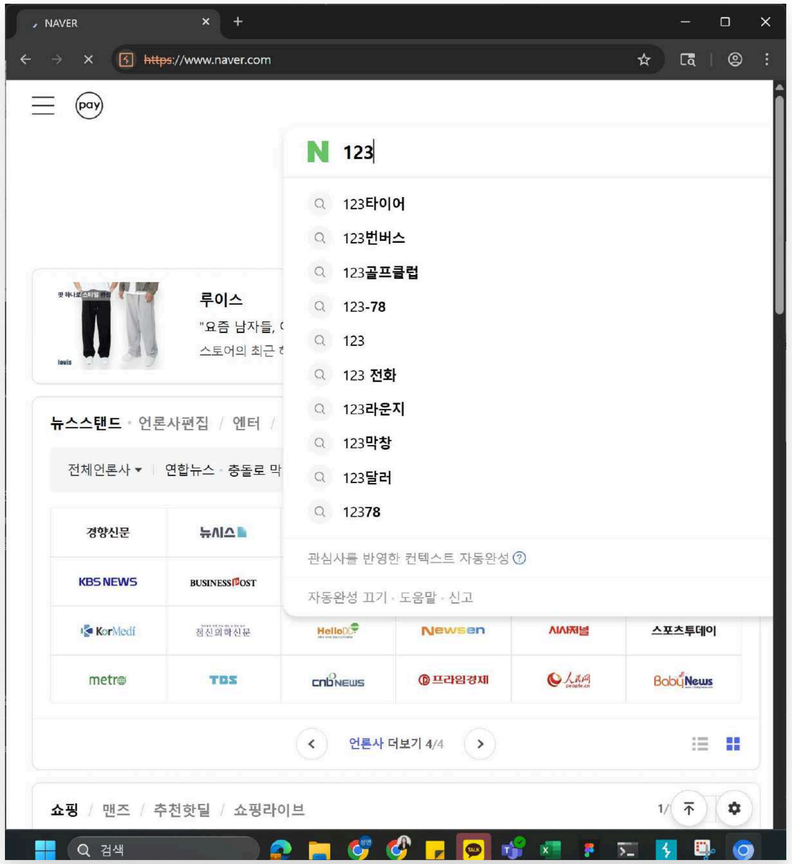




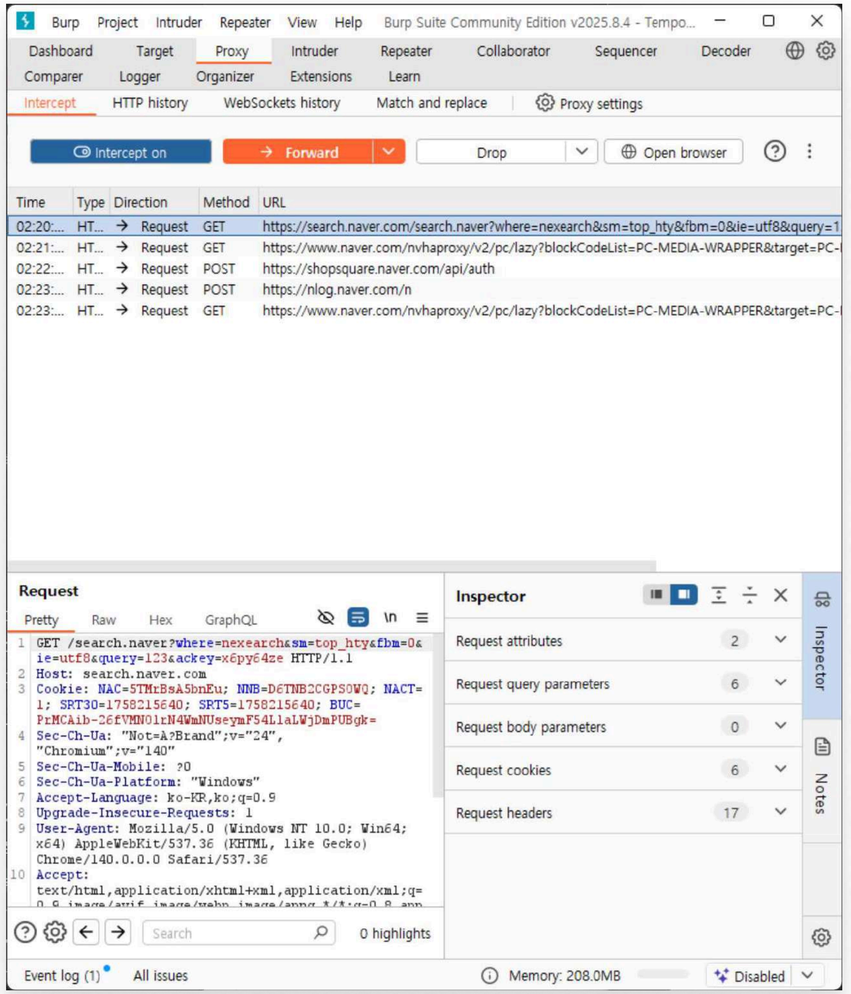
Burp Suite Repeater 실습

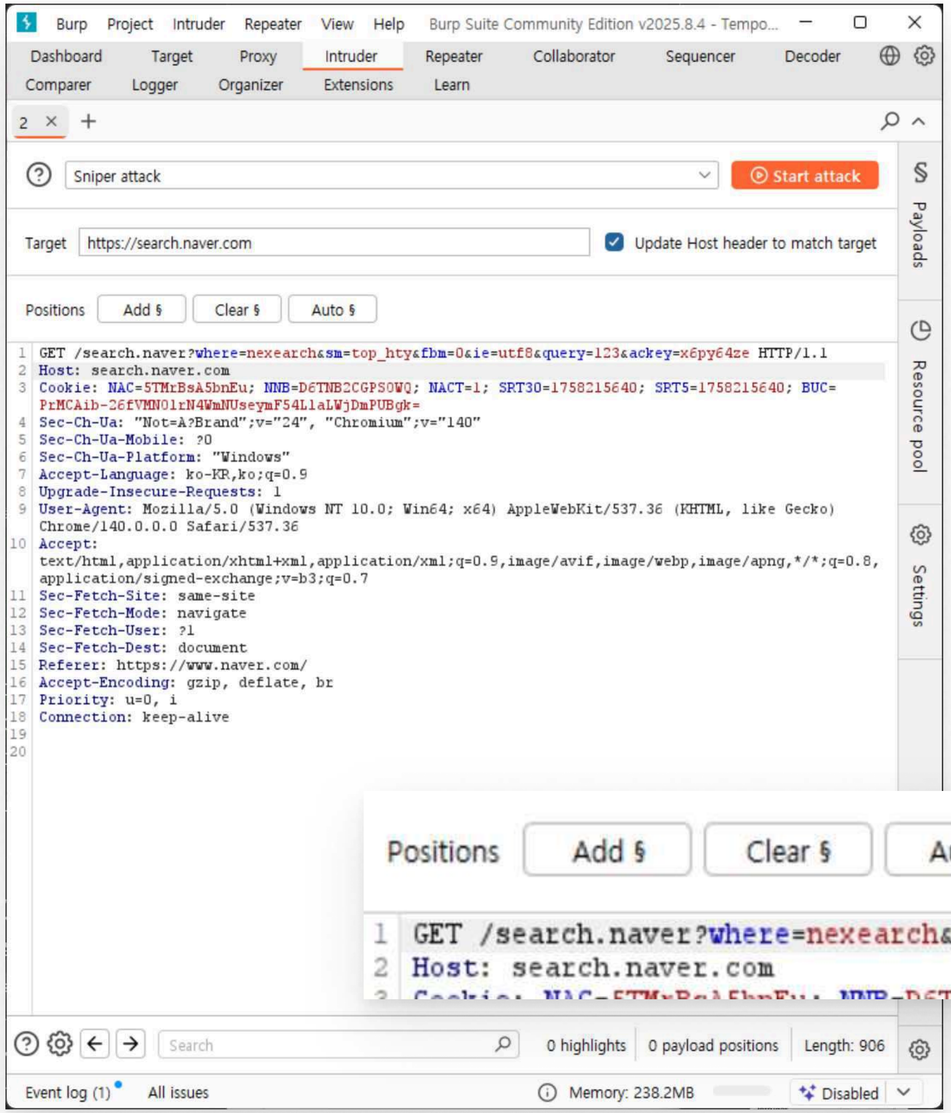
Burp Suite Intruder 실습

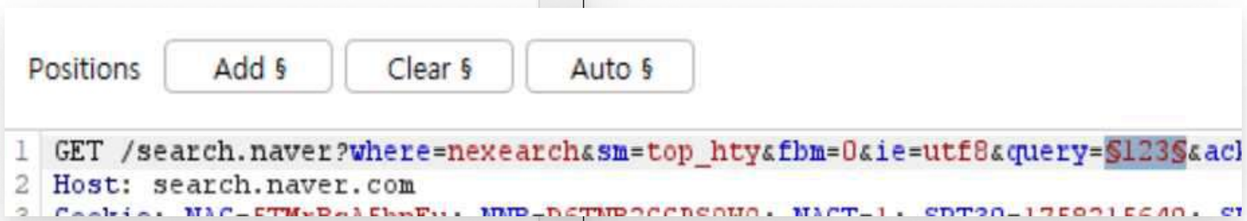
네이버에서 아무거나 검색



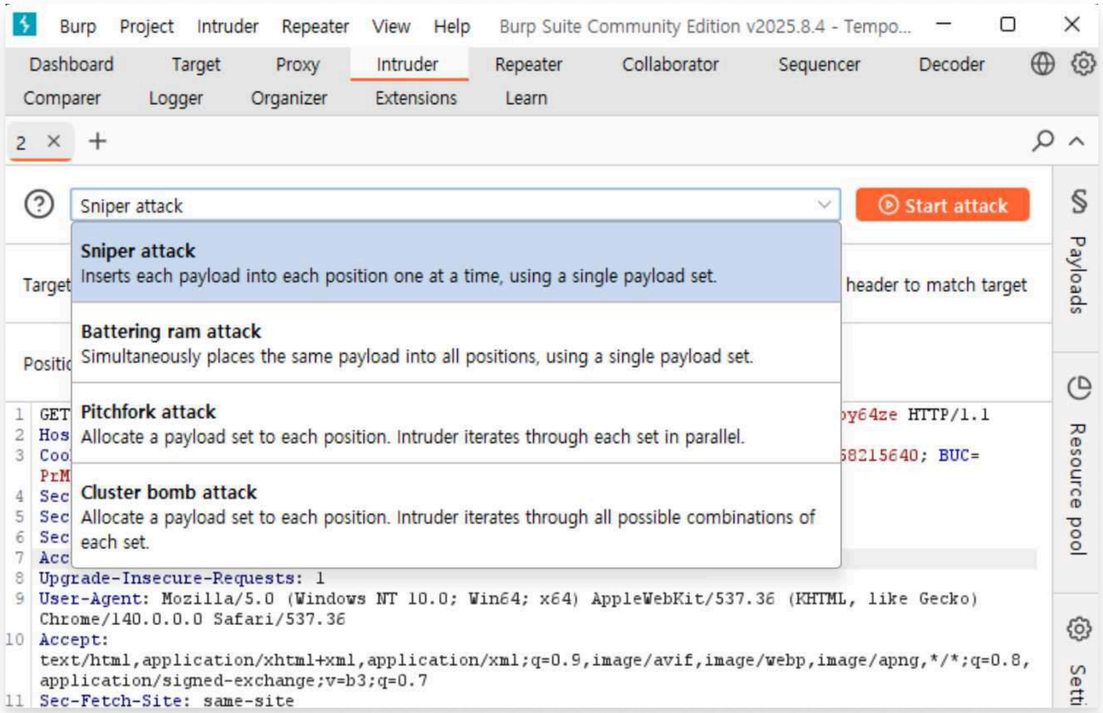
Proxy에서 search 부분이 잡히면 멈추기
마우스 우클릭 → Send to Intruder



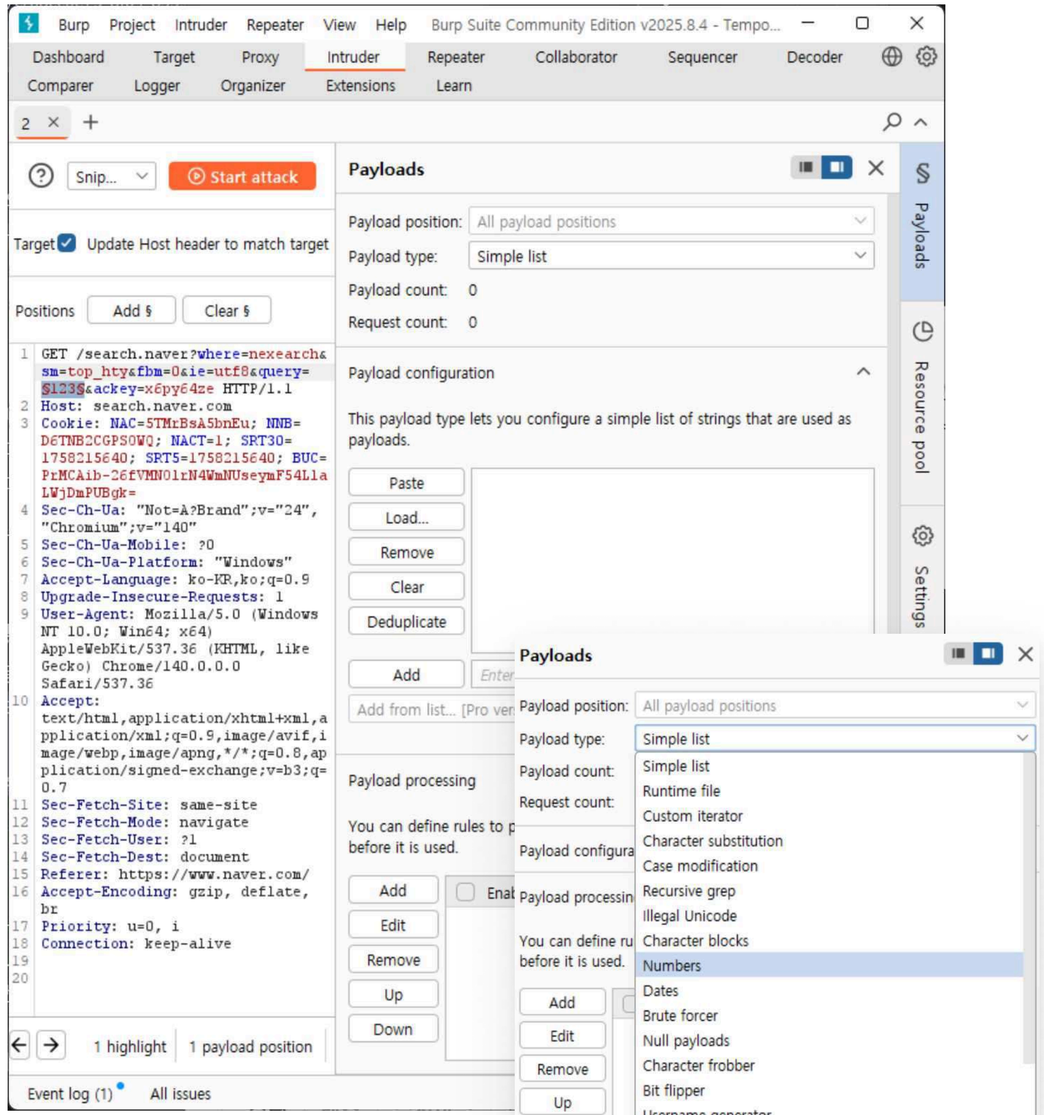




Intruder 탭 접속 후 search 내용을 바꿔볼거에요.
내 검색어(123)은 query 파라미터에 있습니다.
query 파라미터의 값 부분에 $$ 기호를 Add 해줍니다.



상단에서 Sniper Attack 선택
Sniper: 하나의 파라미터에 여러 값(비밀번호 리스트) 시도
Cluster Bomb: 여러 파라미터(예: username, password) 조합 시도
Pitchfork: 여러 파라미터에 각각 리스트를 순차적으로 매칭



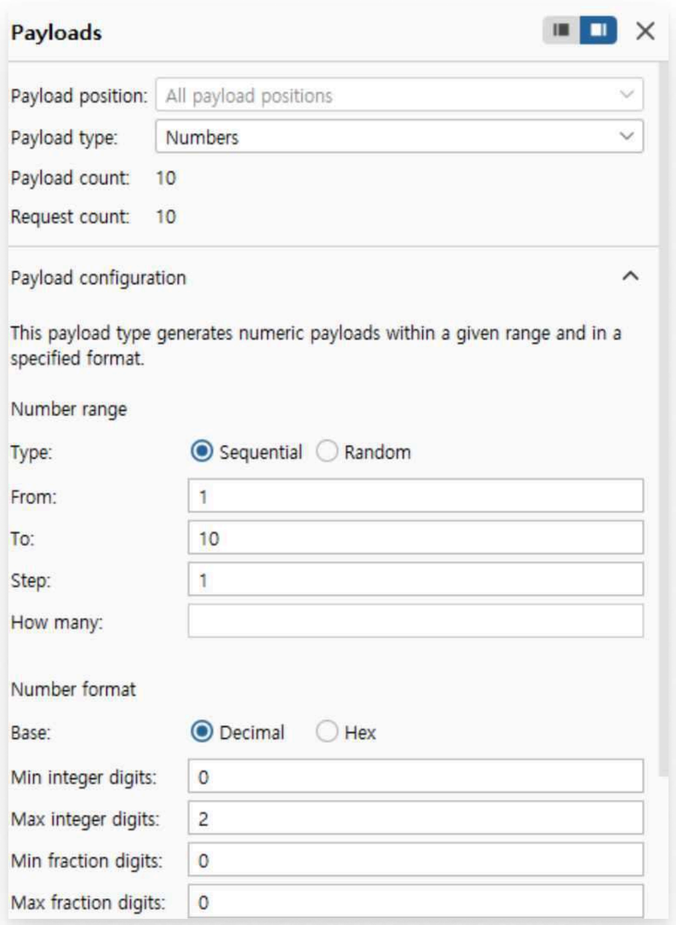
우측 탭에 Payloads 탭으로 이동

Payload Options에 테스트할 비밀번호 후보들 입력

- 직접 입력하거나
- 사전 파일(wordlist, 예: rockyou.txt) 불러오기 가능

payload type → Numbers 선택

- 검색어에 1~10까지 넣어볼거기 때문에 Numbers 선택

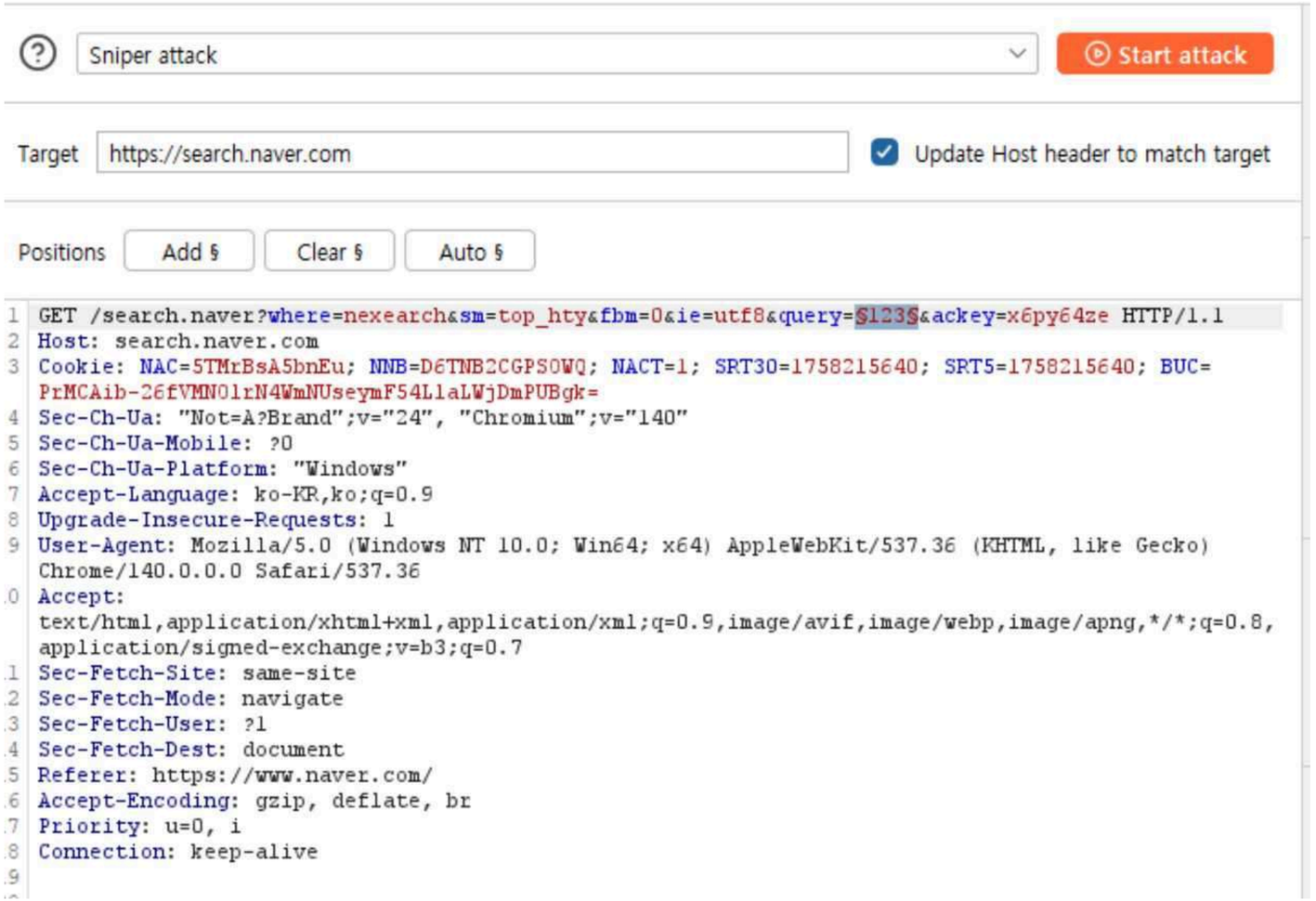


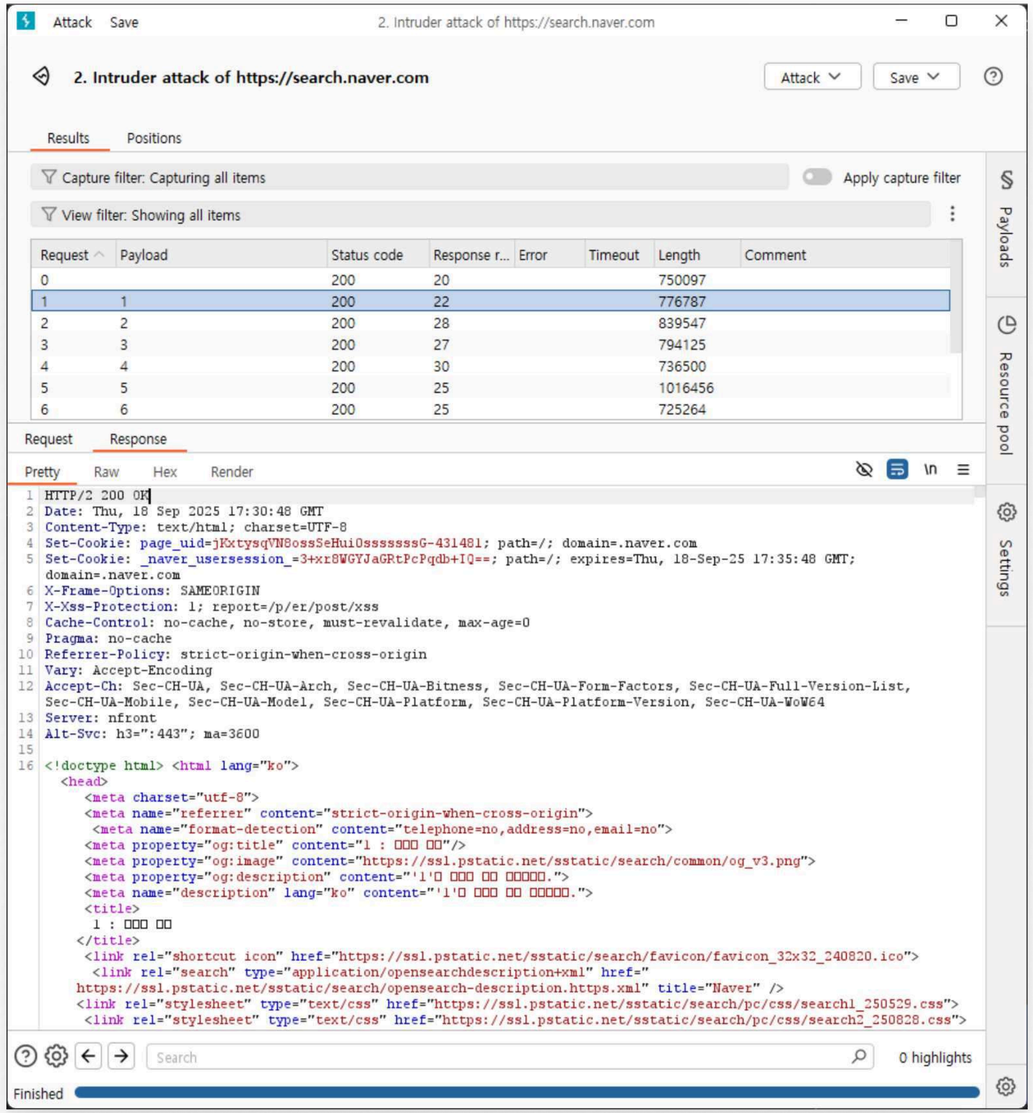
Options 설정:

- From: 1
- To: 10
- Step: 1

⇒ 1부터 10까지 1씩 올리면서 대입

Start Attack !!!!!!!!





1부터 10까지 넣은 결과 값에 대한 결과창을 볼 수 있음

- Request에서는 내가 요청한 내용을
- Response에서는 내가 받은 결과값을 확인할 수 있음

Burp Suite를 사용해 계정 탈취 실습