

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Site map Scope

Filter: Showing all items

http://www.google.com

- /
- ▶ advanced\_search
- ▶ client\_204
- ▶ history
- ▶ images
- ▶ imghp
- ▶ intl
- ▶ language\_tools
- ▶ preferences
- ▼ search

- hl=en&gbv=1&ie=UTF-8&q=bipolar+test&
- hl=en&gbv=1&ie=UTF-8&q=burp+suite&s
- hl=en&gbv=1&ie=UTF-8&q=depression+t
- hl=en&gbv=1&ie=UTF-8&q=fun+test&sa=
- hl=en&gbv=1&ie=UTF-8&q=internet+spee
- hl=en&gbv=1&ie=UTF-8&q=kali+linux+tu
- hl=en&gbv=1&ie=UTF-8&q=learn+pentest
- hl=en&gbv=1&ie=UTF-8&q=metasploit&s
- hl=en&gbv=1&ie=UTF-8&q=pen+testing&
- hl=en&gbv=1&ie=UTF-8&q=personality+t
- hl=en&gbv=1&ie=UTF-8&q=phishing+fre
- hl=en&gbv=1&ie=UTF-8&q=related:https:
- hl=en&gbv=1&ie=UTF-8&q=related:https:
- hl=en&gbv=1&ie=UTF-8&q=related:https:

Contents Issues

Host	Method	URL	Params	Status
http://www.google.c...	GET	/search?ie=ISO-8859-1&hl=en&source=hp&biw=&bih=...	✓	200
http://www.google.c...	GET	/search?q=pentestgeek&hl=en&gbv=1&oq=pentestgee...	✓	200
http://www.google.c...	GET	/js/_/rsrc=xjs.hp.en_US.JrX4RoZae8k.O/m=sb_he,d/r...		200
http://www.google.c...	GET	/client_204?atyp=i&biw=1649&bih=742&ei=nzvhV9iy...	✓	204
http://www.google.c...	GET	/advanced_search		
http://www.google.c...	GET	/advanced_search?hl=en&authuser=0	✓	
http://www.google.c...	GET	/advanced_search?q=pentestgeek&hl=en&gbv=1&ie=U...	✓	

Request Response

Raw Params Headers Hex

GET  
/search?q=pentestgeek&hl=en&gbv=1&oq=pentestgeek&gs\_l=heirloom-serp.3..0j0i30.56132.572  
heirloom-serp..1.10.373.28pXsfQweKk HTTP/1.1  
Host: www.google.com  
User-Agent: SNCAppSec2016  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
DNT: 1  
Referer:  
http://www.google.com/search?ie=ISO-8859-1&hl=en&source=hp&biw=&bih=&q=test&gbv=1&oq=te  
.26166.0.26302.4.4.0.0.0.127.253.2j1.3.0....0...lac.1.34.heirloom-hp..2.2.126.3rCfcgk  
Cookie:

The screenshot displays the Burp Suite interface. On the left, a list of HTTP requests is shown in a table with columns: Host, Method, URL, Params, and Status. The second request is highlighted, showing a GET request to a Google search URL with parameters like 'ie=ISO-8859-1', 'hl=en', 'source=hp', 'biw=', 'bih=', 'q=pentestgeek', 'gbv=1', and 'oq=pentestgee...'. Below this table, the 'Request' tab is active, showing the raw HTTP request details. The request is a GET to 'http://www.google.com/search?q=pentestgeek&hl=en&gbv=1&oq=pentestgee...'. The 'Host' is 'www.google.com', 'User-Agent' is 'SNCAppSec2016', 'Accept' is 'text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8', 'Accept-Language' is 'en-US,en;q=0.5', 'Accept-Encoding' is 'gzip, deflate', 'DNT' is '1', and 'Referer' is 'http://www.google.com/search?ie=ISO-8859-1&hl=en&source=hp&biw=&bih=&q=test&gbv=1&oq=test&...'. The 'Cookie' field is also visible.

The image is a screenshot of the Burp Suite web proxy tool. The top section, titled 'Contents', displays a list of HTTP requests. The second request is highlighted, showing a GET request to 'http://www.google.com/search?q=pentestgeek&hl=en&gbv=1&oq=pentestgee...'. Below this, the 'Request' tab is active, showing the raw HTTP request details. The request is a GET to 'http://www.google.com/search?q=pentestgeek&hl=en&gbv=1&oq=pentestgee...'. The 'Host' is 'www.google.com', and the 'User-Agent' is 'SNCAppSec2016'. The 'Accept' header is 'text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8'. The 'Accept-Language' is 'en-US,en;q=0.5'. The 'Accept-Encoding' is 'gzip, deflate'. The 'DNT' is '1'. The 'Referer' is 'http://www.google.com/search?ie=ISO-8859-1&hl=en&source=hp&biw=&bih=&q=test&gbv=1&oq=te...'. The 'Cookie' is partially visible. The background of the image is dark with a grid pattern.

The image shows a screenshot of the Burp Suite web proxy tool. The top panel displays a list of HTTP requests. The second request is selected, which is a GET request to a Google search page with the query 'pentestgeek'. The bottom panel shows the details of this request, including the raw HTTP text. The 'Request' tab is active, showing the raw data. The 'Params' tab is also visible. The 'Host' is 'www.google.com' and the 'User-Agent' is 'SNCAppSec2016'. The 'Accept' header is 'text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8'. The 'Referer' is 'http://www.google.com/search?ie=ISO-8859-1&hl=en&source=hp&biw=&bih=...'. The 'Cookie' is also visible.

Host	Method	URL	Params	Status
http://www.google.c...	GET	/search?ie=ISO-8859-1&hl=en&source=hp&biw=&bih=...	✓	200
http://www.google.c...	GET	/search?q=pentestgeek&hl=en&gbv=1&oq=pentestgee...	✓	200
http://www.google.c...	GET	/xjs/_/js/k=xjs.hp.en_US.JrX4RoZaeBk.O/m=sb_he,d/r...	✗	200
http://www.google.c...	GET	/client_204741v19&bih=742&ei=nzvhV9iy...	✓	204
http://www.google.c...	GET	/advanced_search	✗	
http://www.google.c...	GET	/advanced_search?hl=en&authuser=0	✓	
http://www.google.c...	GET	/advanced_search?q=pentestgeek&hl=en&gbv=1&ie=U...	✓	

Request Response

Raw Params Headers Hex

GET  
/search?q=pentestgeek&hl=en&gbv=1&oq=pentestgeek...  
Host: www.google.com  
User-Agent: SNCAppSec2016  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
DNT: 1  
Referer: http://www.google.com/search?ie=ISO-8859-1&hl=en&source=hp&biw=&bih=...&q=test&gbv=1&oq=test...  
Cookie:

The image shows a screenshot of the Burp Suite web proxy tool. The top panel displays a list of HTTP requests. The second request is selected, which is a GET request to a Google search page with the query 'pentestgeek'. The bottom panel shows the details of this request, including the raw HTTP text. The 'Request' tab is active, showing the raw data. The 'Params' tab is also visible. The 'Host' is 'www.google.com' and the 'User-Agent' is 'SNCAppSec2016'. The 'Accept' header is 'text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8'. The 'Referer' is 'http://www.google.com/search?ie=ISO-8859-1&hl=en&source=hp&biw=&bih=...'. The 'Cookie' is also visible.

Host	Method	URL	Params	Status
http://www.google.c...	GET	/search?ie=ISO-8859-1&hl=en&source=hp&biw=&bih=...	✓	200
http://www.google.c...	GET	/search?q=pentestgeek&hl=en&gbv=1&oq=pentestgee...	✓	200
http://www.google.c...	GET	/xjs/_/js/k=xjs.hp.en_US.JrX4RoZaeBk.O/m=sb_he,d/r...	✗	200
http://www.google.c...	GET	/client_204741v19&bih=742&ei=nzvhV9iy...	✓	204
http://www.google.c...	GET	/advanced_search	✗	
http://www.google.c...	GET	/advanced_search?hl=en&authuser=0	✓	
http://www.google.c...	GET	/advanced_search?q=pentestgeek&hl=en&gbv=1&ie=U...	✓	

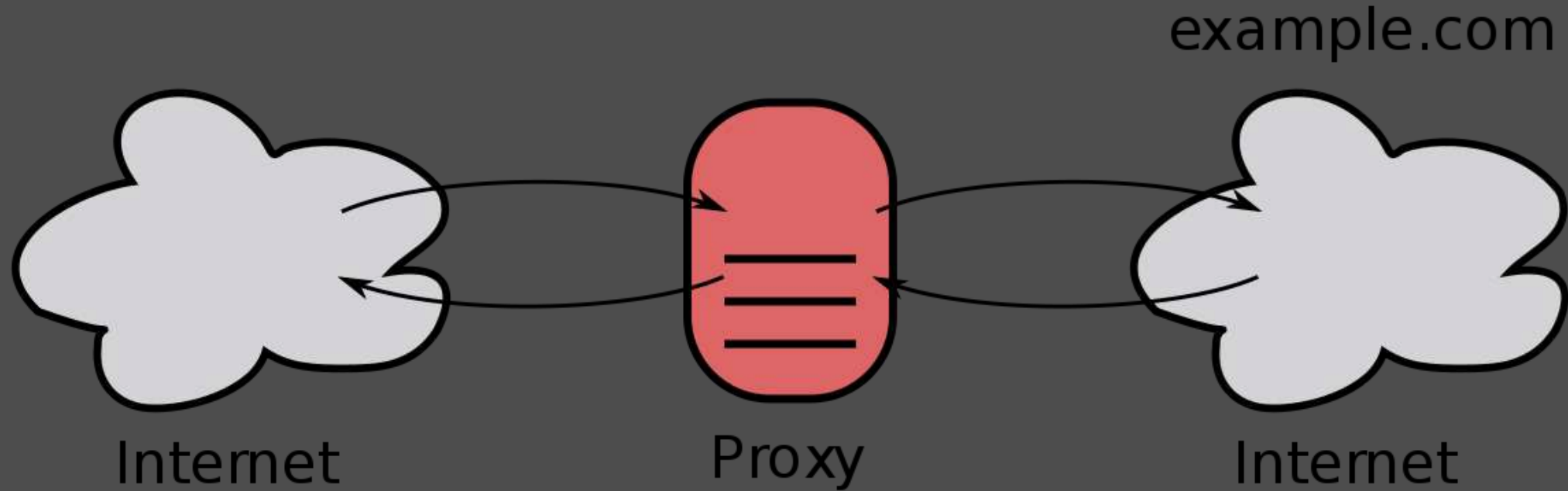
Request Response

Raw Params Headers Hex

GET  
/search?q=pentestgeek&hl=en&gbv=1&oq=pentestgeek...  
Host: www.google.com  
User-Agent: SNCAppSec2016  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
DNT: 1  
Referer: http://www.google.com/search?ie=ISO-8859-1&hl=en&source=hp&biw=&bih=...&q=test&gbv=1&oq=test...  
Cookie:

# 1. 버프스위트란

## 1. 버프스위트란



프록시 서버: 클라이언트와 서버 사이 간접적 접속

버프스위트의 경우 웹 프록시

# 1. 버프스위트란



네트워크 통신 패킷을 가로채 분석, 조작 가능

취약점 찾는 용도로 사용 가능

## 2. 버프스위트 활용

## 2. 버프스위트 활용

Burp Suite Community Edition v2023.3.2

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

*Note: Disk-based projects are only supported on Burp Suite Professional.*

☒ Temporary project

☐ New project on disk

Name:

File:

☐ Open existing project

Name	File
------	------

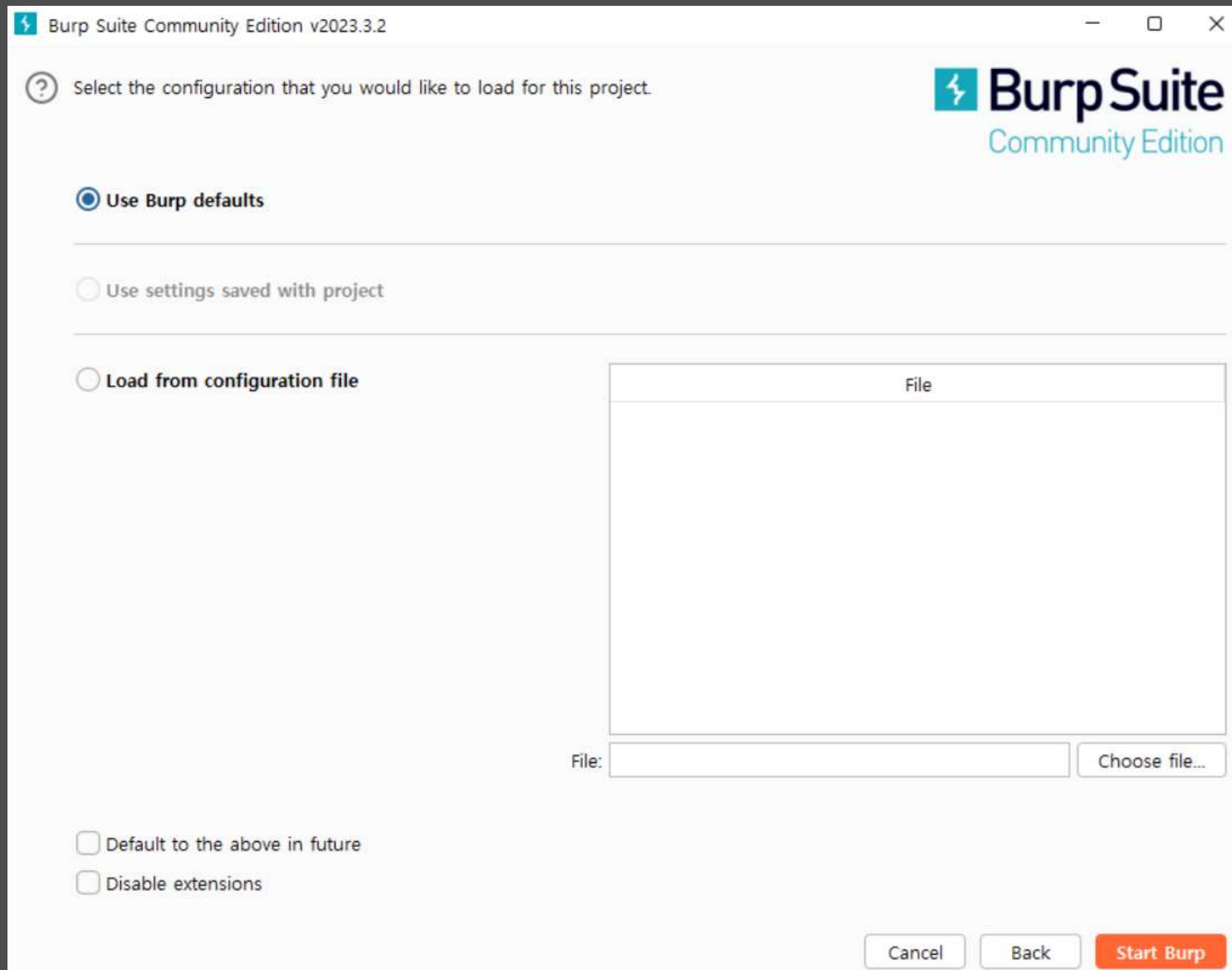
File:

☒ Pause Automated Tasks

프로젝트 저장 기능은  
어차피 유료 버전에만 !!



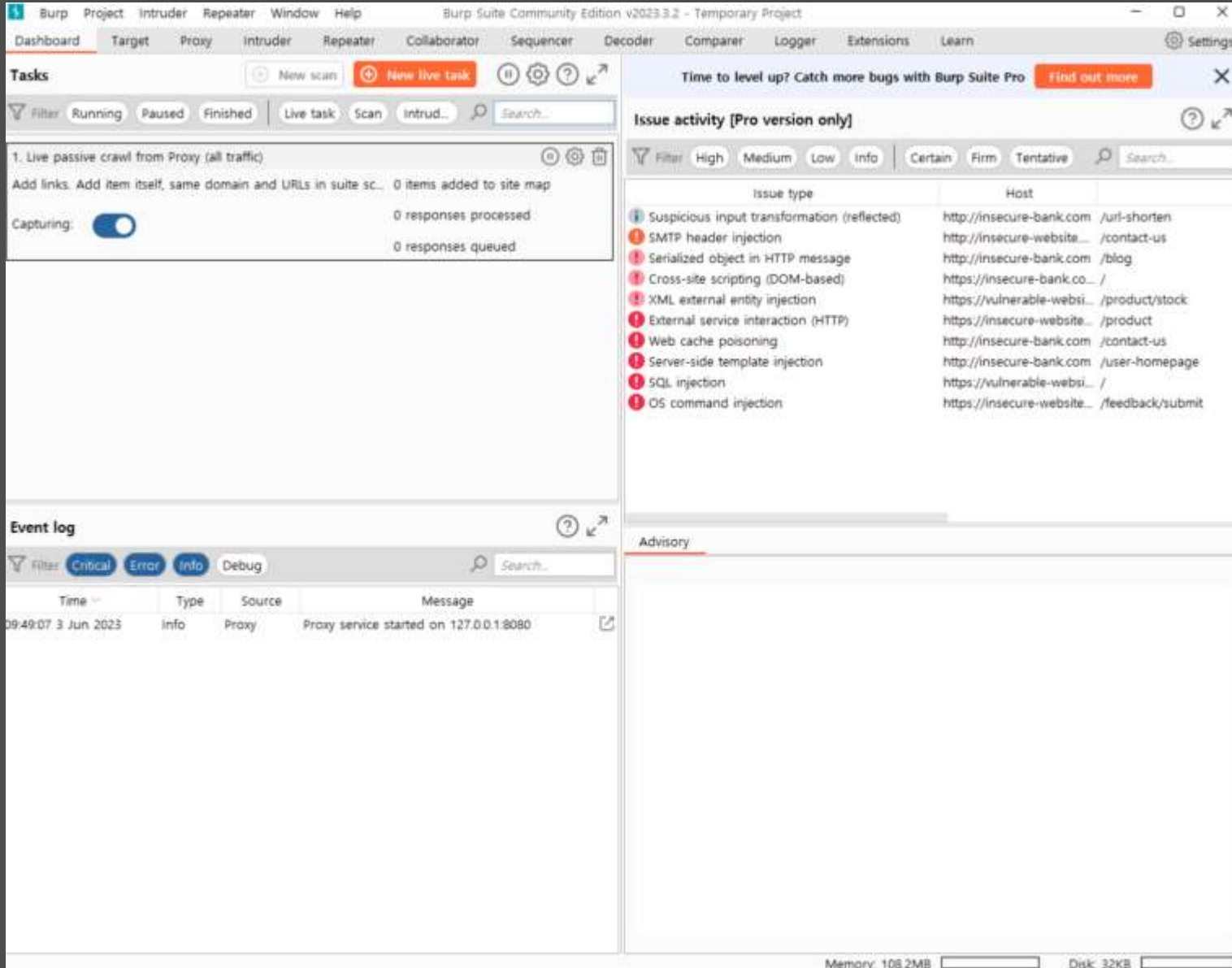
## 2. 버프스위트 활용



기본값 사용 후 NEXT

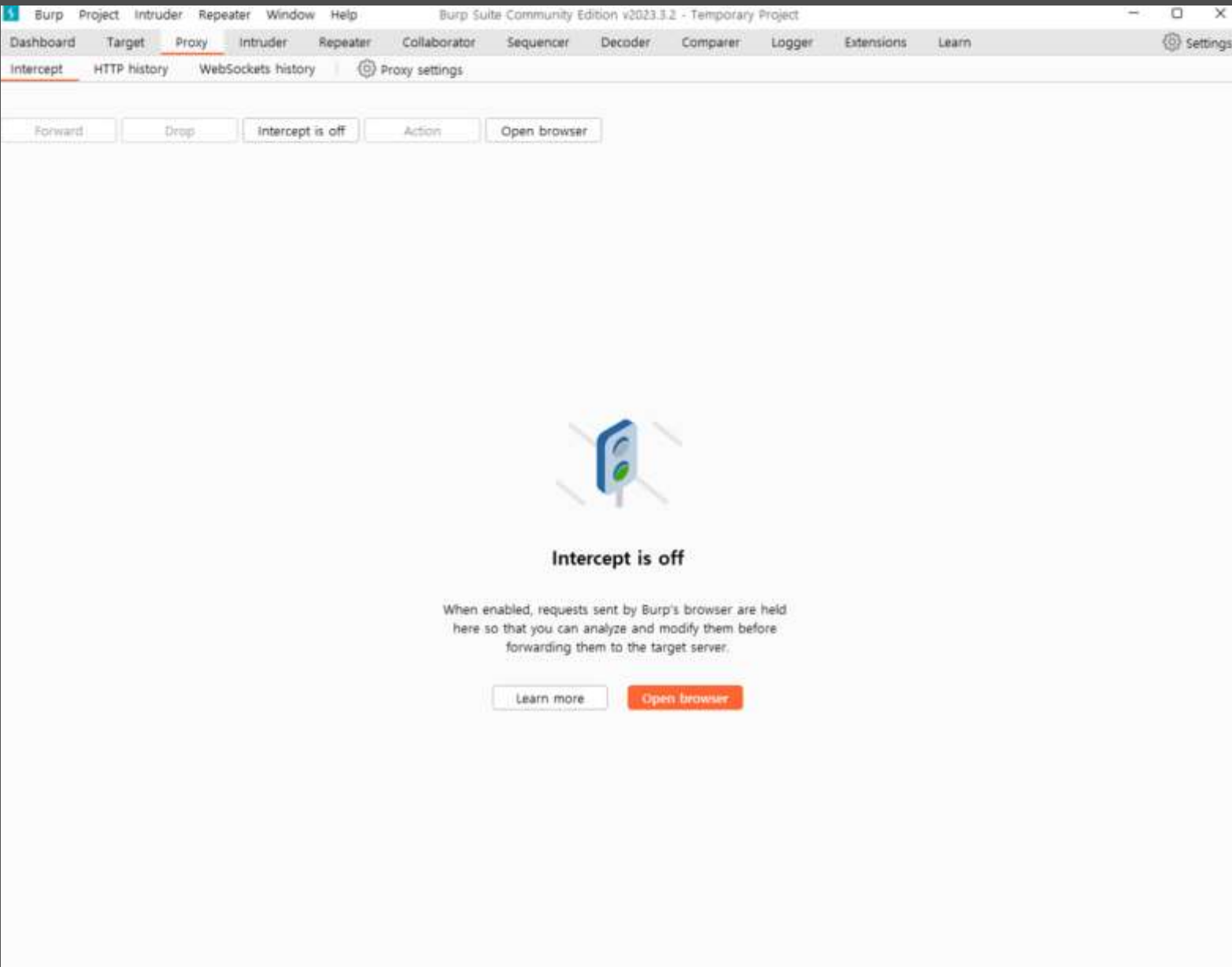


## 2. 버프스위트 활용



이 화면이 보일 시  
Proxy 로 들어가준다

## 2. 버프스위트 활용

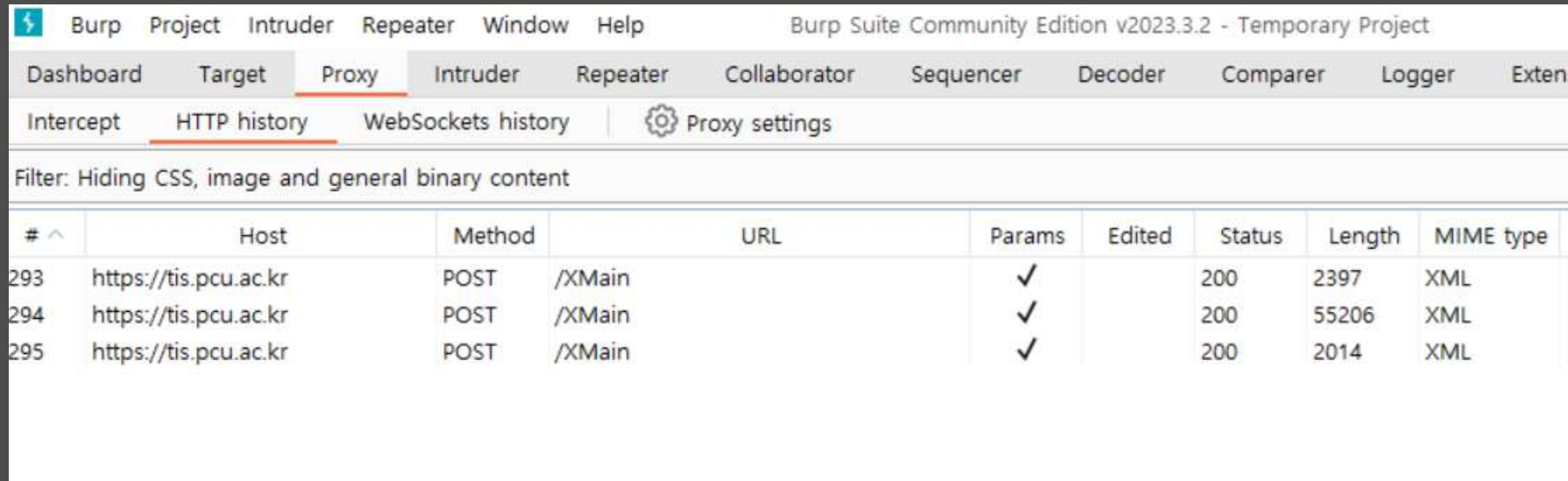


Open browser 클릭시  
브라우저가 팝업,

웹 서핑 후 HTTP history  
를 보면 HTTP, XML 등  
GET/POST된 내역을  
볼 수 있다.

## 2. 버프스위트 활용

배재대학교 통합정보 시스템에 들어간 후 history clear을  
시키고 “조회” 버튼을 누를 시



The screenshot shows the Burp Suite interface with the 'HTTP history' tab selected. The table below lists the captured HTTP requests.

#	Host	Method	URL	Params	Edited	Status	Length	MIME type
293	https://tis.pcu.ac.kr	POST	/XMain	✓		200	2397	XML
294	https://tis.pcu.ac.kr	POST	/XMain	✓		200	55206	XML
295	https://tis.pcu.ac.kr	POST	/XMain	✓		200	2014	XML

다음과 같이 3가지의 POST 방식 XML이 나온다. 딱 봐도 저기  
중 가장 길이가 긴 곳에 정보들이 저장 되어 있을 것 같다.

## 2. 버프스위트 활용

The screenshot displays the Burp Suite interface. At the top, the 'Proxy' tab is active, showing a list of intercepted requests. The table below shows three requests to 'https://tis.pcu.ac.kr' with status 200 and MIME type XML.

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment
293	https://tis.pcu.ac.kr	POST	/XMain	✓		200	2397	XML			
294	https://tis.pcu.ac.kr	POST	/XMain	✓		200	55206	XML			
295	https://tis.pcu.ac.kr	POST	/XMain	✓		200	2014	XML			

The 'Request' tab is selected, showing the details of the selected POST request. The request is a POST to '/XMain' with a 'Host' of 'tis.pcu.ac.kr'. The 'Request' tab is selected, showing the details of the selected POST request. The request is a POST to '/XMain' with a 'Host' of 'tis.pcu.ac.kr'. The 'Request' tab is selected, showing the details of the selected POST request. The request is a POST to '/XMain' with a 'Host' of 'tis.pcu.ac.kr'.

The 'Response' tab is selected, showing the details of the selected POST response. The response is an XML document with a root element 'Column' and several child elements. The 'Response' tab is selected, showing the details of the selected POST response. The response is an XML document with a root element 'Column' and several child elements. The 'Response' tab is selected, showing the details of the selected POST response. The response is an XML document with a root element 'Column' and several child elements.

The 'Inspector' tab is selected, showing the details of the selected POST response. The inspector shows the request attributes, request cookies, request headers, and response headers. The 'Inspector' tab is selected, showing the details of the selected POST response. The inspector shows the request attributes, request cookies, request headers, and response headers. The 'Inspector' tab is selected, showing the details of the selected POST response. The inspector shows the request attributes, request cookies, request headers, and response headers.

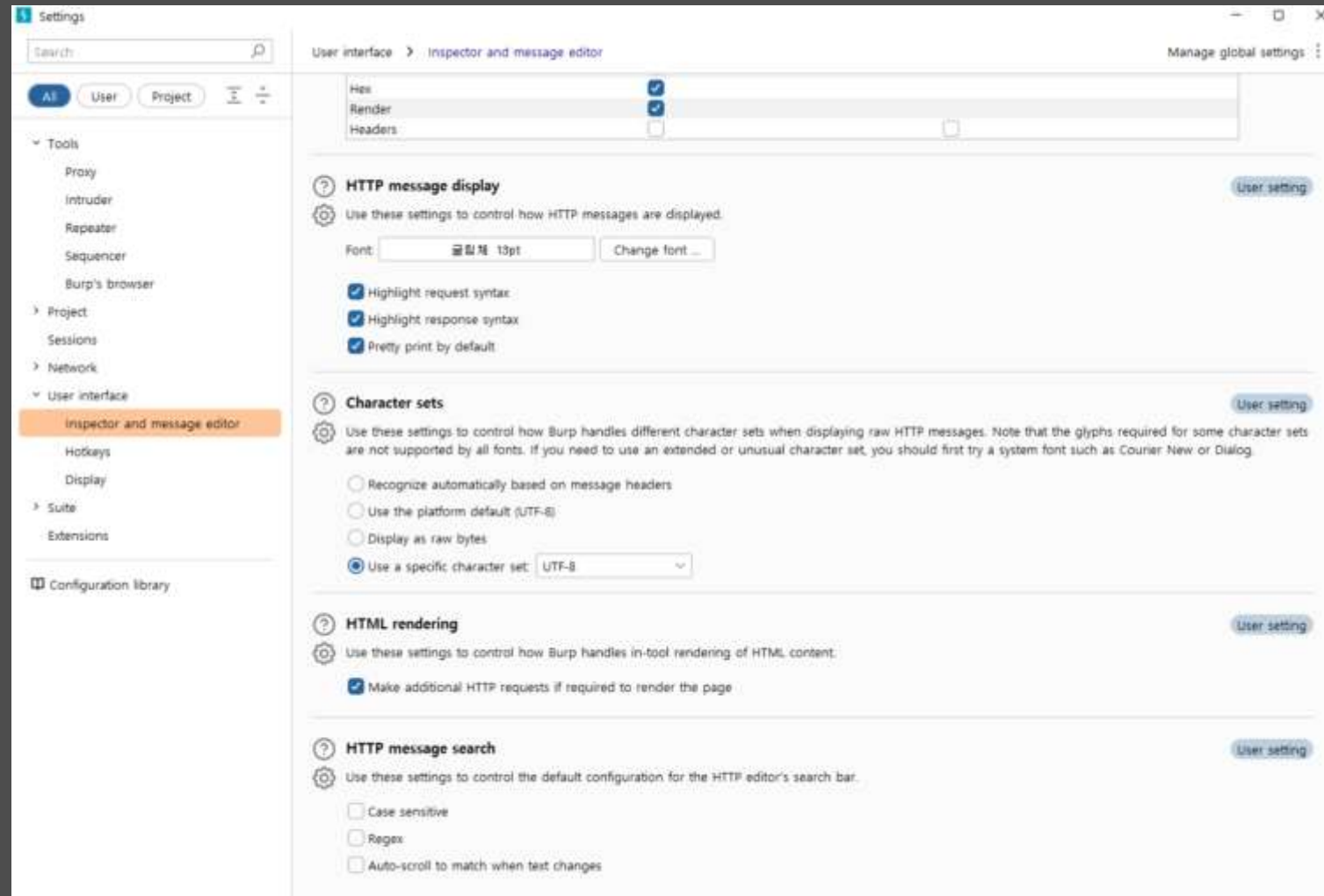
왼쪽 Request의 내용  
요청 시 오른쪽과 같이  
응답이 오는 형태이다.

이를 우리가 위/변조해서  
요청하고 싶다면 주황색  
라인을 우클릭 후  
Repeater로 보내주자

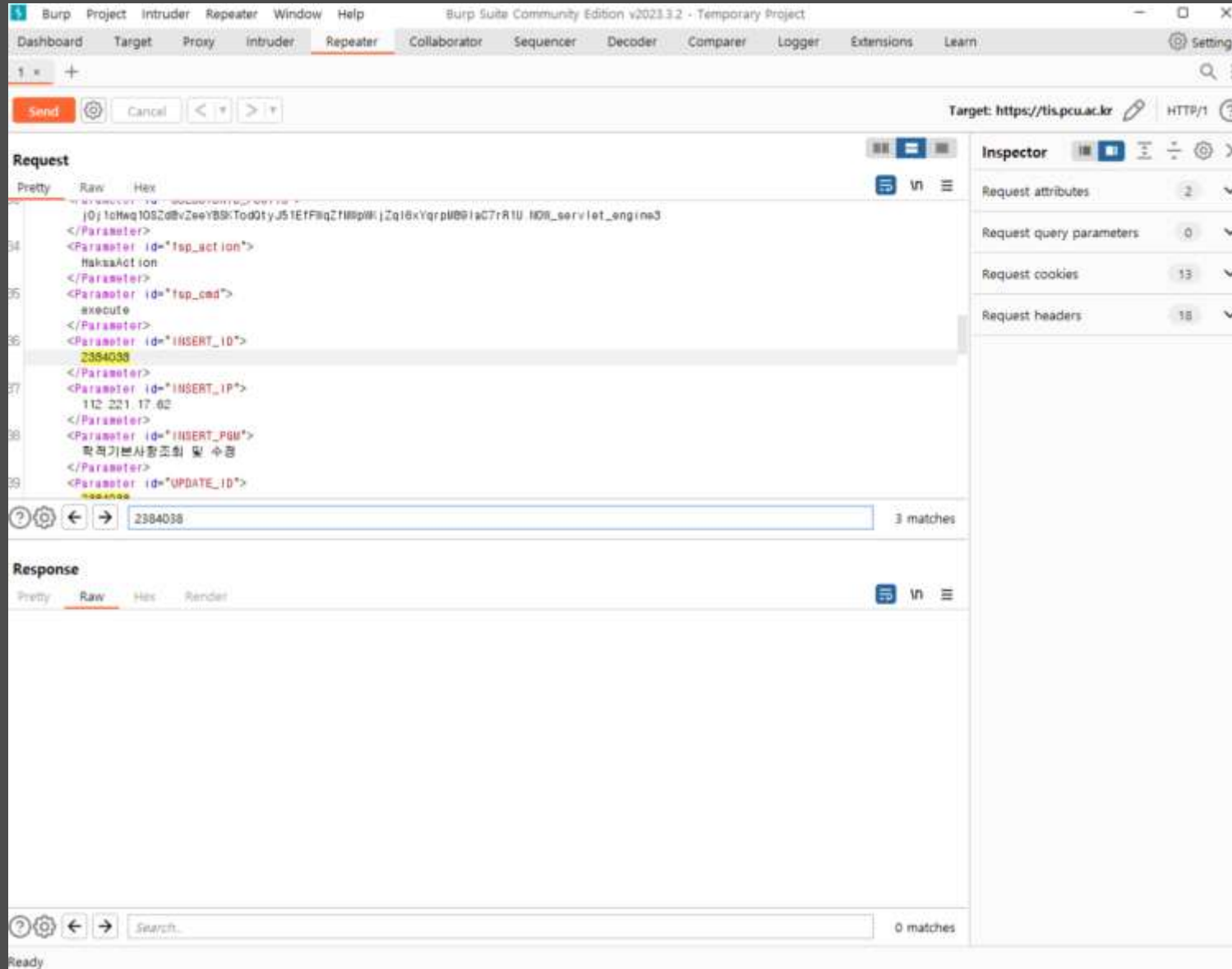
## 2. 버프스위트 활용

그 전에 한글이 깨질 경우  
인코딩과 폰트를 설정 해 주면  
된다.

이 곳에서 설정 가능 ->

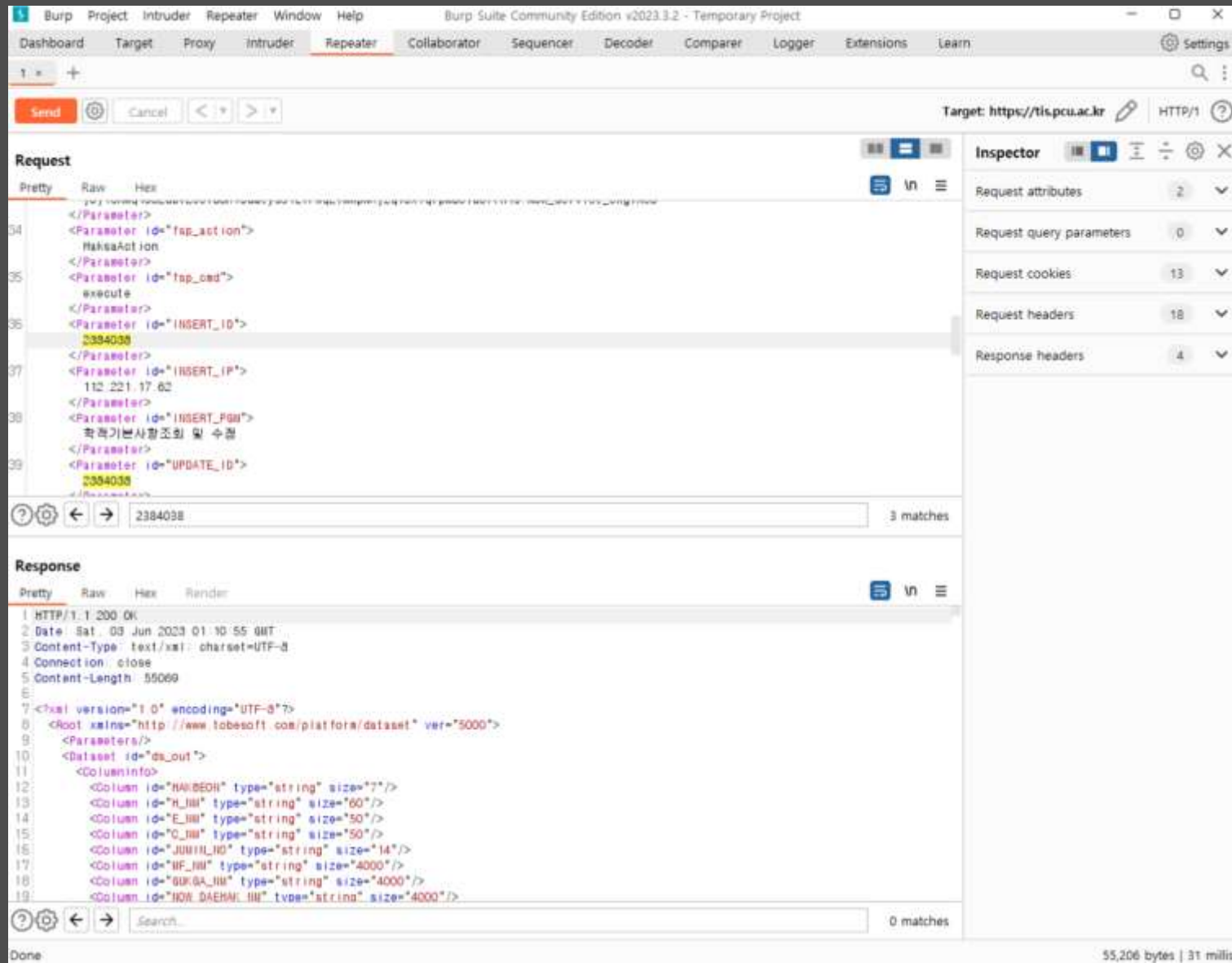


## 2. 버프스위트 활용



본론으로 넘어가 repeater  
로 넘긴 후 search 에서  
본인의 학번을 원하는 학번  
으로 변경 후 왼쪽 위 Send  
를 누른다면,

## 2. 버프스위트 활용



본론으로 넘어가 repeater로 넘긴 후 search에서 본인의 학번을 원하는 학번으로 변경 후 왼쪽 위 Send를 누른다면,

아래 Response에 변경된 정보가 나타날 것이다



## 2. 버프스위트 활용

이로서 배재대학교 통합정보  
시스템에서 정보 조회 시 패킷을  
가로채 학번 변경 만으로도 정보를  
얻을 수 있다는 취약점을 발견 한  
것이다.