

□ 단국대학교 > 사이버보안 학과 > 인터넷 보안 > 보고서 템플릿

25년 1학기 인터넷 보안 수업

File Upload

2025년 5월 13일

학번 : 32231594
이름 : 박기쁨

1. 워게임 5 번 문항

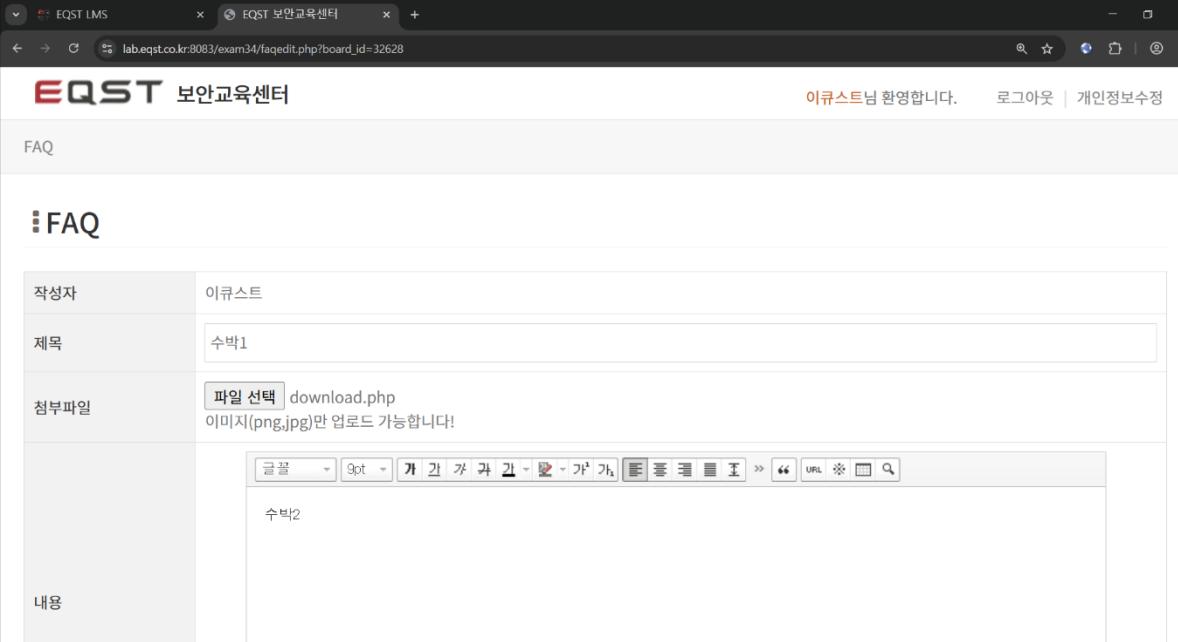
<과정 설명>

File Upload 취약점 공격은 파일을 업로드하는 과정에서의 취약점을 이용하여 원하는 정보를 탈취하는 행위를 말한다. 본 실습에서는 File Upload 취약점을 이용해 .php 확장자의 파일을 업로드 해보고자 한다.

Step 1. php 파일 업로드

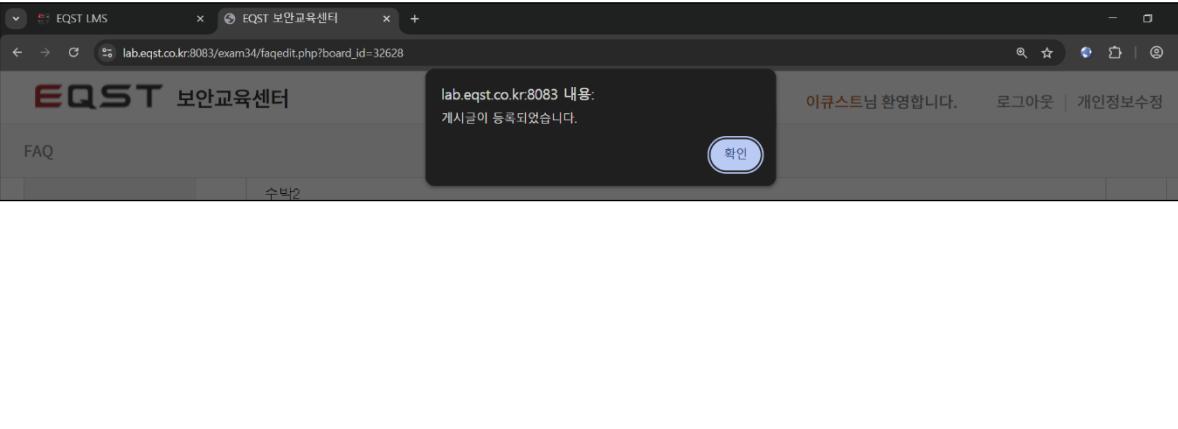
Step 1-1. php 파일 업로드

: 목표 페이지의 게시판에 php 파일을 업로드 한다.



The screenshot shows a web browser displaying the 'FAQ' section of the 'EQST 보안교육센터' website. The URL in the address bar is `lab.eqst.co.kr:8083/exam34/faqedit.php?board_id=32628`. The page contains fields for '작성자' (Writer) set to '이큐스트', '제목' (Title) set to '수박1', and '첨부파일' (Attachment) with a file input field containing 'download.php'. Below these fields is a rich text editor toolbar and a text area labeled '수박2'. A large gray box covers the bottom portion of the page, obscuring the footer and some content. The status bar at the bottom of the browser window shows the URL again: `lab.eqst.co.kr:8083/exam34/faqedit.php?board_id=32628`.

(게시물이 정상적으로 업로드 된다.)



The screenshot shows the same web browser after the file upload. A dark gray modal dialog box is centered on the screen, displaying the message 'lab.eqst.co.kr:8083 내용: 게시글이 등록되었습니다.' (Content: The post has been registered successfully.) and a blue '확인' (Confirm) button. The rest of the page content is visible behind the dialog.

: 게시물은 정상적으로 업로드 되었지만, php 파일은 삭제된 것을 알 수 있다.

The screenshot shows a web browser displaying the EQST LMS platform. The URL in the address bar is `lab.eqst.co.kr:8083/exam34/faqview.php?pageIndex=1&board_id=32628&sorting=&sotingAd=DESC&startDt=&endDt=&searchType=all&keyword=`. The page title is "FAQ". The main content area displays a table with the following data:

제목	수박1
작성일	2025-05-19 02:19:22
첨부파일	
내용	수박2

At the bottom right of the content area, there are two buttons: "수정" (Edit) and "삭제" (Delete). The "삭제" button is highlighted with a red background.

Step 2. png 파일 업로드

Step 2-1. png 파일 업로드

: 목표 페이지의 게시판 파일 업로드 방식 등을 확인하기 위하여 png 파일을 업로드 해본다.

The screenshot shows a web browser displaying the EQST LMS platform. The URL in the address bar is `lab.eqst.co.kr:8083/exam34/faqwrite.php`. The page title is "FAQ". The main content area displays a form with the following data:

작성자	이큐스트
제목	수박1
첨부파일	<input type="file" value="파일 선택"/> 수박.png 이미지(png,jpg)만 업로드 가능합니다!
내용	<p>수박2</p>

The "첨부파일" field contains a file input field with the placeholder "파일 선택" and the file name "수박.png". A note below it says "이미지(png,jpg)만 업로드 가능합니다!". The "내용" field contains the text "수박2". At the bottom right of the content area, there are two buttons: "수정" (Edit) and "삭제" (Delete).

Step 2-2. intercept 및 content-Type 확인

: 게시물을 저장 과정을 intercept 하여 패킷의 Content-Type 을 확인한다.

: 수박.png 파일의 Content-Type 은 image/png 이다.

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A request is being viewed for the URL <https://lab.eqt.co.kr:8083/exam34/process/faqProcess.php>. The request is a POST method with the following payload:

```
-----WebKitFormBoundaryF0etMSJGBUopv1g
Content-Disposition: form-data; name="fileuploaded"; filename="100%20.png"
Content-Type: image/png
100%20.png
-----
```

The response pane shows a status code of 200 OK and a length of 1000 bytes. The 'Inspector' pane on the right shows the selected text as "image/png".

Step 3. php 파일 업로드 (재시도)

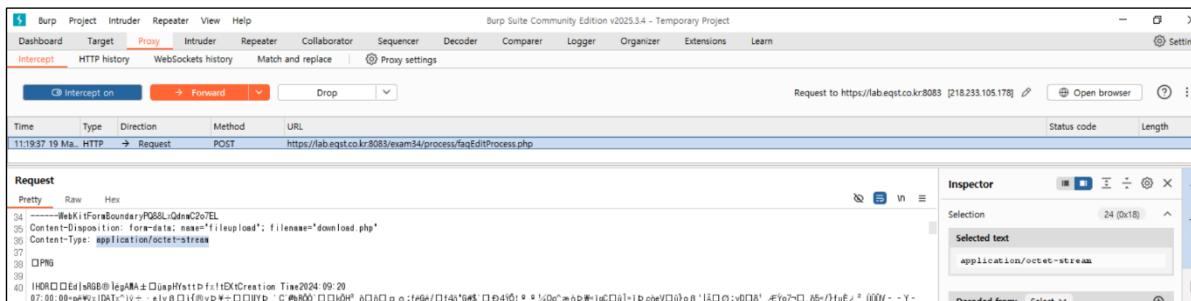
Step 3-1. php 파일 업로드 (재시도)

: 목표 페이지의 게시판에 php 파일을 업로드 한다.

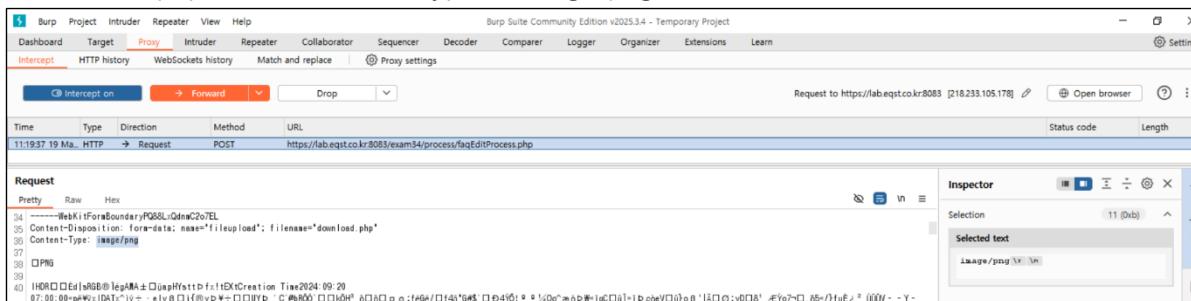
작성자	이큐스트
제목	수박1
첨부파일	<input type="button" value="파일 선택"/> download.php 이미지(png,jpg)만 업로드 가능합니다!
내용	<p>수박2</p>

Step 3-2. intercept 및 content-Type 확인

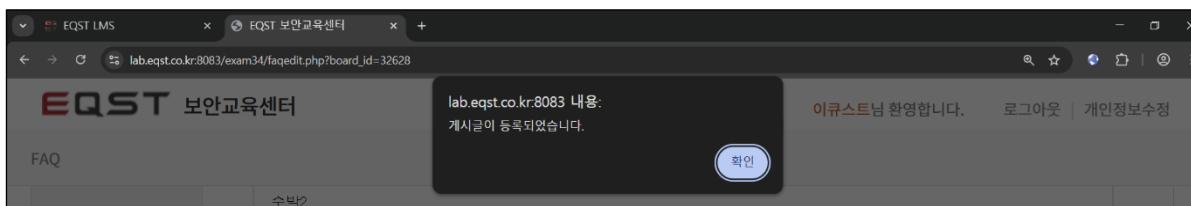
- : 게시물을 저장 과정을 intercept 하여 패킷의 Content-Type 을 확인한다.
- : download.php 파일의 Content-Type 은 application/octet-stream 이다.



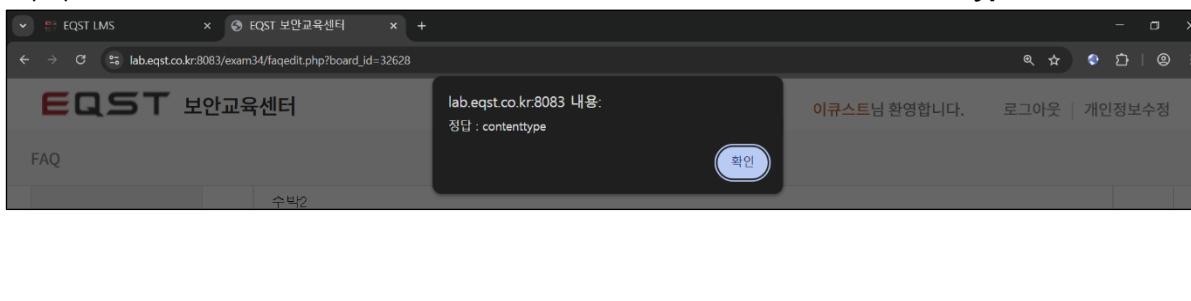
: download.php 파일의 Content-Type 을 image/png 로 변경한다.



(게시물이 정상적으로 업로드 된다.)



: php 파일이 성공적으로 업로드 되어 정답을 획득할 수 있다. (정답: contenttype)



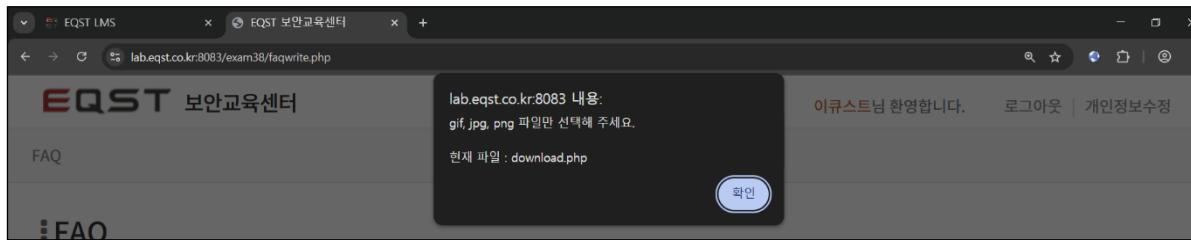
2. 워게임 6 번 문항

<과정 설명>

Step 1. php 파일 업로드

Step 1-1. php 파일 업로드

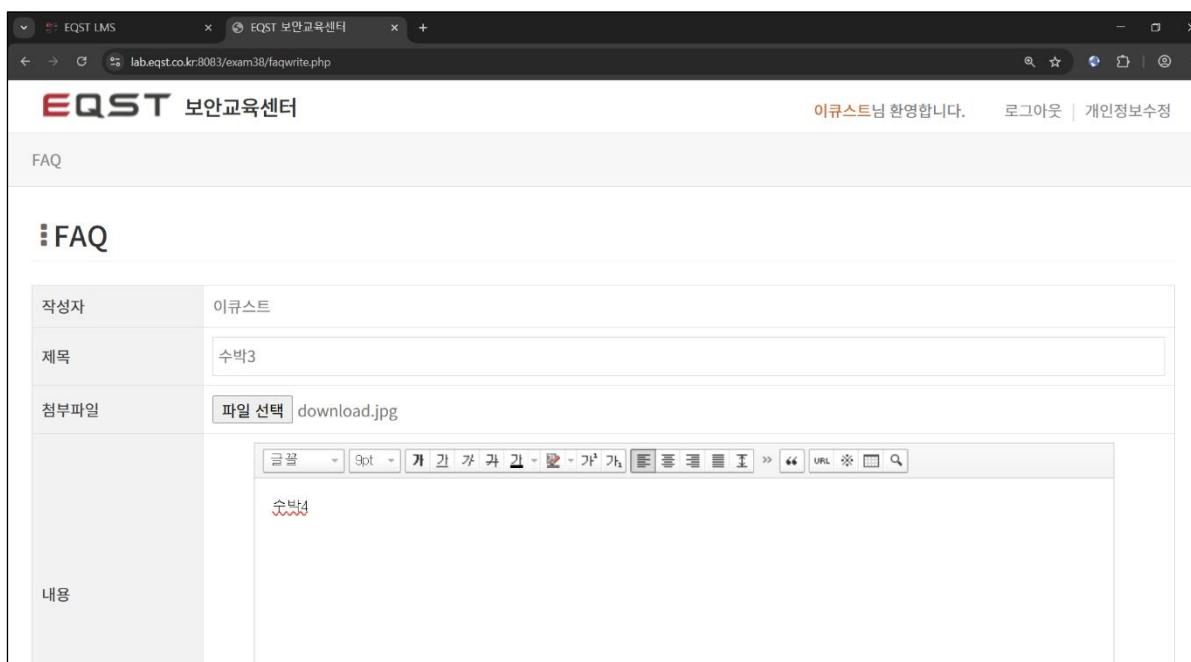
- : 목표 페이지의 게시판에 php 파일을 업로드 한다.
- : 첨부파일 선택 과정에서 .php 확장자 파일 업로드가 필터링 되는 것을 알 수 있다.



Step 2. php 파일 확장자 변경

Step 2-1. php 파일 확장자 변경

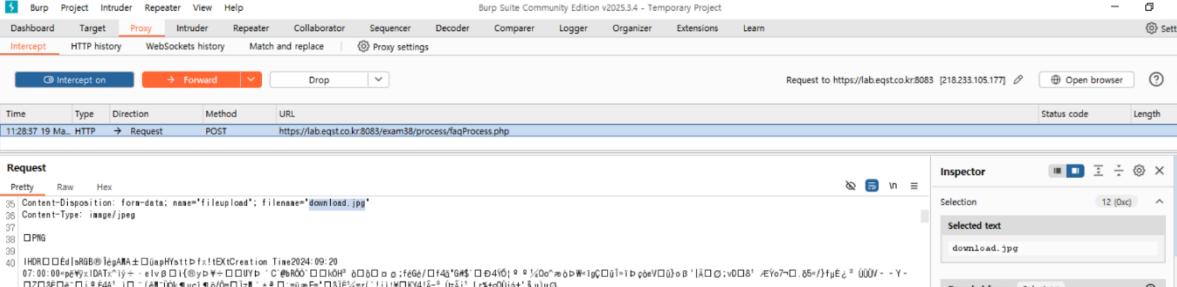
- : 첨부파일 선택 과정에서의 확장자 필터링을 우회하기 위해, php 파일의 확장자를 jpg 로 변경하여 업로드한다.
- : 첨부파일 선택 과정에서 필터링 되지 않는다.



Step 3. php 파일 확장자 원상복구 (재시도)

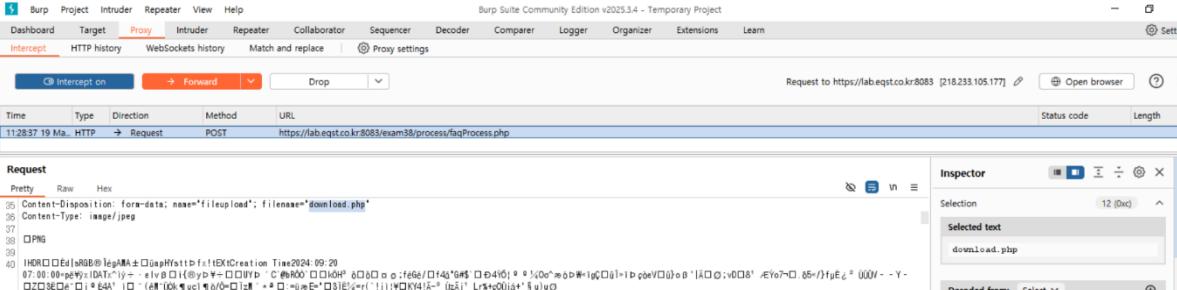
Step 3-1. php 파일 확장자 원상복구

: 게시물을 저장 과정을 intercept 하여 확장자를 php로 원상복구한다.



The screenshot shows the Burp Suite interface in 'Proxy' mode. A POST request is selected. In the 'Request' tab, the 'Content-Disposition' header is set to 'form-data; name="fileupload"; filename="download.jpg"'. The 'Selected text' in the 'Inspector' panel is 'download.jpg'. The URL is https://lab.eqst.co.kr:8083/exam38/process/faqProcess.php.

(.jpg 를 .php 로 변경한다.)



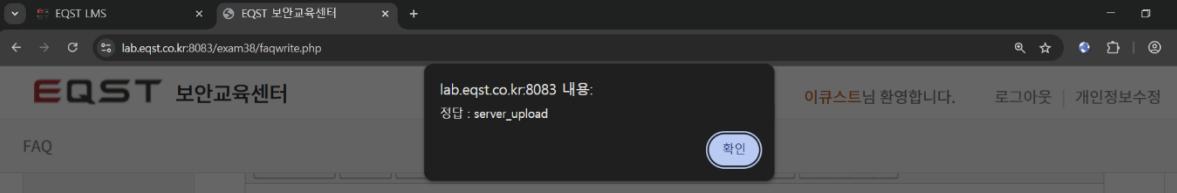
The screenshot shows the Burp Suite interface in 'Proxy' mode. A POST request is selected. In the 'Request' tab, the 'Content-Disposition' header is set to 'form-data; name="fileupload"; filename="download.php"'. The 'Selected text' in the 'Inspector' panel is 'download.php'. The URL is https://lab.eqst.co.kr:8083/exam38/process/faqProcess.php.

(게시물이 정상적으로 업로드 된다.)



The screenshot shows a browser window for 'EQST LMS'. The URL is lab.eqst.co.kr:8083/exam38/faqwrite.php. The page displays a success message: 'lab.eqst.co.kr:8083 내용: 게시글이 등록되었습니다.' (Content: Article registered successfully). There is a blue '확인' (Confirm) button at the bottom right.

: php 파일이 성공적으로 업로드 되어 정답을 획득할 수 있다. (정답: server_upload)



The screenshot shows a browser window for 'EQST LMS'. The URL is lab.eqst.co.kr:8083/exam38/faqwrite.php. The page displays a success message: 'lab.eqst.co.kr:8083 내용: 정답 : server_upload' (Content: Answer: server_upload). There is a blue '확인' (Confirm) button at the bottom right.

3. 워게임 7 번 문항

<과정 설명>

Step 1. php 파일 업로드

Step 1-1. php 파일 업로드

- : 목표 페이지의 게시판에 php 파일을 업로드 한다.
- : 첨부파일 선택 과정에서 .php 확장자 파일 업로드가 필터링 되는 것을 알 수 있다.

The screenshot shows a web browser window with the URL `lab.eqst.co.kr:8083/exam33/faqwrite.php`. The page title is "FAQ". There is a form for creating a new FAQ entry. In the "첨부파일" (Attachment) field, the user has selected a file named "download.php". A preview area shows the file content as "수박5". Below the form is a rich text editor toolbar.

작성자	이큐스트
제목	수박5
첨부파일	파일 선택 download.php 수박5
내용	

- : 게시물은 정상적으로 업로드 되었지만, php 파일은 삭제된 것을 알 수 있다.

The screenshot shows a web browser window with the URL `lab.eqst.co.kr:8083/exam33/faqview.php?pageIndex=1&board_id=32631&sorting=&sotingAd=DESC&startDt=&endDt=&searchType=all&keyword=`. The page title is "FAQ". It displays a list of FAQ entries. The first entry has the same details as the one in the previous screenshot: title "수박5", created by "이큐스트" on "2025-05-19 02:30:54", and 1 reply. The content of the entry is "수박6".

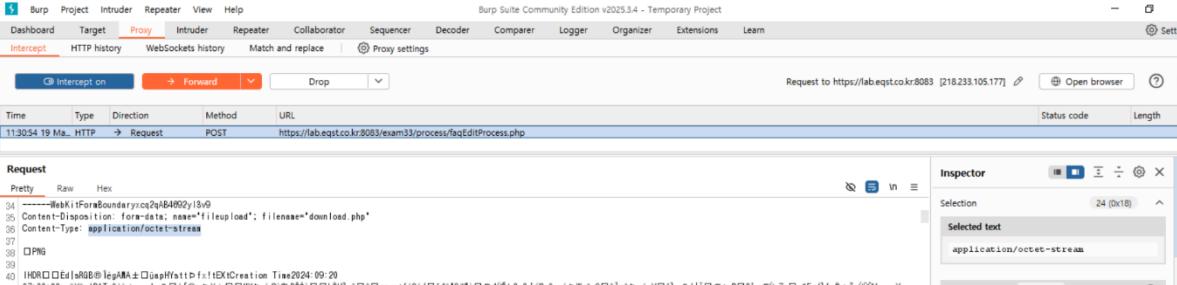
제목	수박5		
작성일	2025-05-19 02:30:54	조회	1
첨부파일		작성자	이큐스트
내용	수박6		

Step 2. php 파일 업로드 및 Content-Type 변경

Step 2-1. intercept 및 content-Type 확인

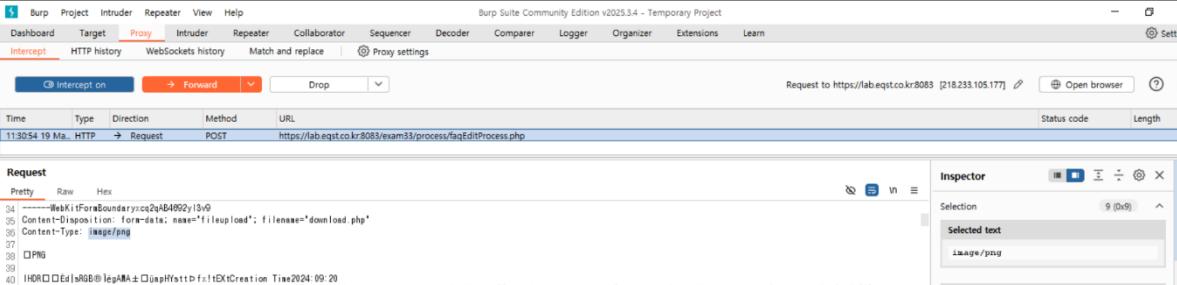
: 게시물을 저장 과정을 intercept 하여 패킷의 Content-Type 을 확인한다.

: download.php 파일의 Content-Type 은 application/octet-stream 이다.



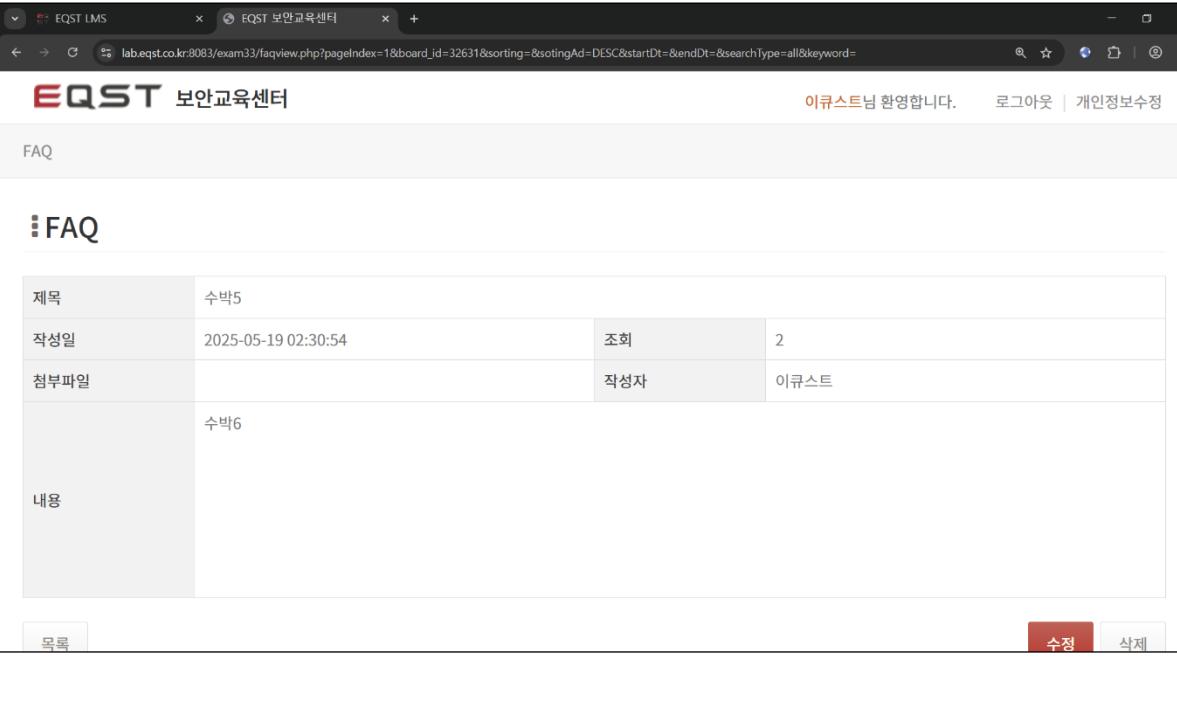
The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A single request is captured for the URL <https://lab.eqst.co.kr:8083/exam33/process/faqEditProcess.php>. In the 'Request' pane, the Content-Type field is highlighted and shows the value 'application/octet-stream'. This indicates that the file was uploaded as a binary stream rather than an image.

: download.php 파일의 Content-Type 을 image/png 로 변경한다.



This screenshot shows the same captured request as the previous one, but with the Content-Type value changed in the Inspector panel from 'application/octet-stream' to 'image/png'. This change is intended to bypass content-type checks that might prevent file uploads.

: 여전히 게시물은 정상적으로 업로드 되었지만, php 파일은 삭제된 것을 알 수 있다.



The screenshot shows a web browser displaying the EQST FAQ page. A file named '수박5' (Watermelon 5) is listed in the table. At the bottom right of the table, there is a red '삭제' (Delete) button. This visual cue suggests that the file has been successfully deleted despite the Content-Type being changed.

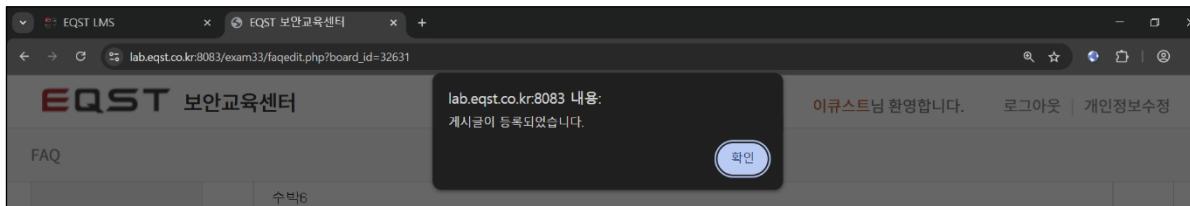
Step 3. php 파일 확장자 PhP 로 변경

Step 3-1. php 파일 확장자 PhP 로 변경

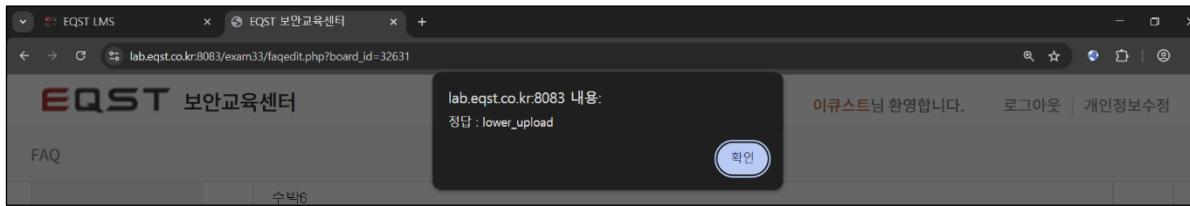
: .php 확장자 필터링을 우회하기 위해 php 파일의 확장자에 대문자를 섞어 PhP로 변경한다.

The screenshot shows the 'FAQ' section of the EQST LMS. A file named 'download.PhP' is selected for upload. The content area contains the text '수박6'. The browser address bar shows 'lab.eqst.co.kr:8083/exam33/faqedit.php?board_id=32631'.

(게시물이 정상적으로 업로드 된다.)



: php 파일이 성공적으로 업로드 되어 정답을 획득할 수 있다. (정답: lower_upload)



4. 워게임 9 번 문항

<과정 설명>

Step 1. 웹쉘 업로드

Step 1-1. 웹쉘 업로드

: 목표 페이지의 게시판에 웹쉘을 업로드 한다.

The screenshot shows a web browser window for the EQST LMS system. The URL is `lab.eqst.co.kr:8083/exam31/faqwrite.php`. The page title is "FAQ". There is a table for entering post information:

작성자	이큐스트
제목	웹쉘1
첨부파일	<input type="button" value="파일 선택"/> php_lms_webshell.php

In the "첨부파일" field, there is a file selection button labeled "파일 선택" and the file name "php_lms_webshell.php". Below the table is a rich text editor toolbar. The content area contains the text "웹쉘2".

(게시물이 정상적으로 업로드 된다.)

The screenshot shows a web browser window for the EQST LMS system. The URL is `lab.eqst.co.kr:8083/exam31/faqview.php?pageIndex=1&board_id=32632&sorting=&sotingAd=DESC&startDt=&endDt=&searchType=all&keyword=`. The page title is "FAQ". There is a table for viewing post details:

제목	웹쉘1		
작성일	2025-05-19 02:35:40	조회	1
첨부파일	php_lms_webshell.php	작성자	이큐스트

In the "내용" (Content) section, the text "웹쉘2" is visible. At the bottom right of the page, there are "수정" (Edit) and "삭제" (Delete) buttons.

Step 2. 웹쉘 경로 찾기 및 실행하기

Step 2-1. 웹쉘 경로 찾기

: 개발자도구를 사용하여 첨부파일 관련 코드를 확인한다.

: 목표 페이지의 주소는 8083 이지만, 첨부파일의 주소는 8085 인 것을 확인할 수 있다.

(https://lab.eqst.co.kr:8085/exam31/lib/download.php?file_path=/file/faq/&file_name=php_lms_webshell.php)

The screenshot shows a browser window with the title 'EQST LMS' and the URL 'lab.eqst.co.kr:8083/exam31/faqview.php?pageIndex=1&board_id=32632&sorting=&soringAd=DESC&startDt=&endDt=&searchType=all&keyword='.

The main content is the 'FAQ' section of the 'EQST 보안교육센터' website. It displays a table with two rows:

제목	웹쉘1
작성일	2025-05-19 02:35:40
첨부파일	php_lms_webshell.php
	웹쉘2

The DevTools sidebar is open, specifically the 'Elements' tab. A table row is selected, and the code pane shows the following snippet:

```
<tr>
  <td>첨부파일</td>
  <td><a href="#" class="txt_lft">
    <!--a href="#" class="txt_lft">파일선택 .php</a-->
    <a href="https://lab.eqst.co.kr:8085/exam31/lib/downl...<!--a href="#" class="txt_lft"> 파일선택 .php</a-->
    <td>작성자</td>
    <td class="txt_lft"> 이류스</td>
  </tr>
```

: 첨부파일의 주소를 참고하여 경로를 수정한 후 접속해본다.

(https://lab.eqst.co.kr:8085/exam31/lib/file/faq/php_lms_webshell.php)

The screenshot shows a browser window with the title 'EQST LMS' and the URL 'https://lab.eqst.co.kr:8085/exam31/lib/file/faq/php_lms_webshell.php' in the address bar.

: 웹쉘 실행에 성공한다.

The screenshot shows a browser window with the title 'EQST LMS' and the URL 'lab.eqst.co.kr:8085/exam31/lib/file/faq/php_lms_webshell.php' in the address bar.

The main content area contains a form with a single input field and a 'Execute' button:

Input field: _____

Execute

Step 3. DB 설정 파일 내 DB 계정 비밀번호 탈취

Step 3-1. 웹쉘 파악

- : 실행된 웹쉘의 검색창에 ls -la 를 입력해본다.
- : 입력한 ls -la 가 정상적으로 작동하므로 웹쉘이 리눅스 기반임을 알 수 있다.

```
ls -la
total 22604
drwxrwxrwx 3 nobody nobody 32768 May 18 15:53 .
drwxrwxrwx 3 nobody nobody 4096 Apr  7 09:27 ..
drwxrwxrwx 3 nobody nobody 326 May 13 01:38 "php_lms_webshell.php"
drwxrwxrwx 3 nobody nobody 326 May 13 01:38 $php_lms_webshell.php
drwxrwxrwx 1 nobody nobody 19 Apr  7 09:27 .htaccess
drwxrwxrwx 1 www-data www-data 326 May 13 01:31 .jpg
drwxrwxrwx 1 nobody nobody 326 May 13 01:31 .php
drwxrwxrwx 1 nobody nobody 45 Apr  7 09:27 02.php
drwxrwxrwx 1 nobody nobody 45 Apr  7 09:27 03.php
drwxrwxrwx 1 nobody nobody 326 Apr  7 09:27 0319-1325.php
drwxrwxrwx 1 nobody nobody 326 Apr  7 09:27 0319-1326.php
drwxrwxrwx 1 nobody nobody 1139 Apr  7 09:27 0618.txt
```

Step 3-2. DB 설정 파일 탐색

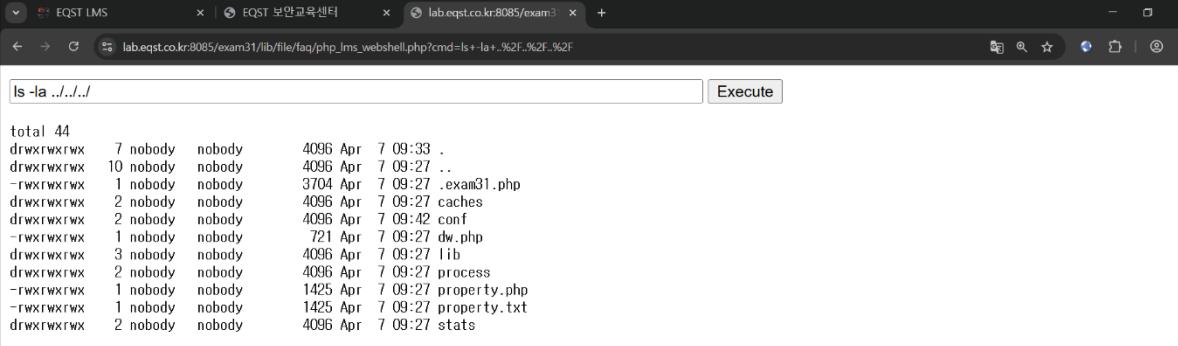
- : ls -la 에 ../../를 하나씩 붙여가며 상위 디렉토리를 탐색해본다.

```
ls -la ..
total 48
drwxrwxrwx 3 nobody nobody 4096 Apr  7 09:27 .
drwxrwxrwx 3 nobody nobody 4096 Apr  7 09:27 ..
drwxrwxrwx 1 nobody nobody 481 Apr  7 09:27 attack.php
drwxrwxrwx 3 nobody nobody 32768 May 20 00:20 faq
```

(../../ 탐색)

```
ls -la ../../
total 20
drwxrwxrwx 3 nobody nobody 4096 Apr  7 09:27 .
drwxrwxrwx 7 nobody nobody 4096 Apr  7 09:33 ..
drwxrwxrwx 1 nobody nobody 3704 Apr  7 09:27 .lib.php
drwxrwxrwx 1 nobody nobody 0 Apr  7 09:27 127.0.0.1
drwxrwxrwx 1 nobody nobody 721 Apr  7 09:27 download.php
drwxrwxrwx 3 nobody nobody 4096 Apr  7 09:27 file
drwxrwxrwx 1 nobody nobody 21 Apr  7 09:27 test.php
drwxrwxrwx 1 nobody nobody 21 Apr  7 09:27 test.txt
```

: ../../ 디렉토리에서 DB 설정 파일로 추정되는 property.php 파일을 발견할 수 있다.

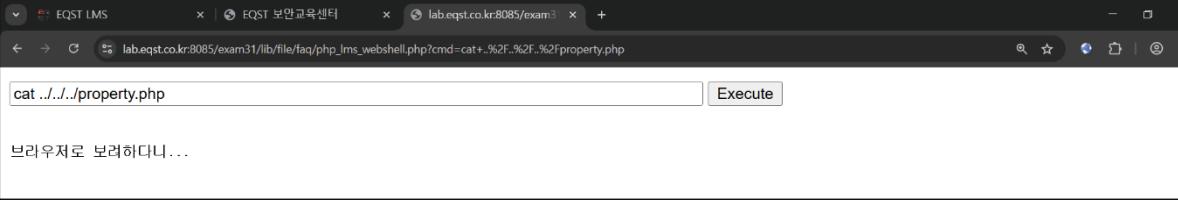


```
ls -la ../../
total 44
drwxrwxrwx 7 nobody nobody 4096 Apr  7 09:33 .
drwxrwxrwx 10 nobody nobody 4096 Apr  7 09:27 ..
-rwxrwxrwx 1 nobody nobody 3704 Apr  7 09:27 .exam31.php
drwxrwxrwx 2 nobody nobody 4096 Apr  7 09:27 caches
drwxrwxrwx 2 nobody nobody 4096 Apr  7 09:42 conf
-rwxrwxrwx 1 nobody nobody 721 Apr  7 09:27 dw.php
drwxrwxrwx 3 nobody nobody 4096 Apr  7 09:27 lib
drwxrwxrwx 2 nobody nobody 4096 Apr  7 09:27 process
-rwxrwxrwx 1 nobody nobody 1425 Apr  7 09:27 property.php
-rwxrwxrwx 1 nobody nobody 1425 Apr  7 09:27 property.txt
drwxrwxrwx 2 nobody nobody 4096 Apr  7 09:27 stats
```

Step 3-3. DB 설정 파일 확인

: 발견한 property.php 파일을 cat 명령어로 출력해본다.

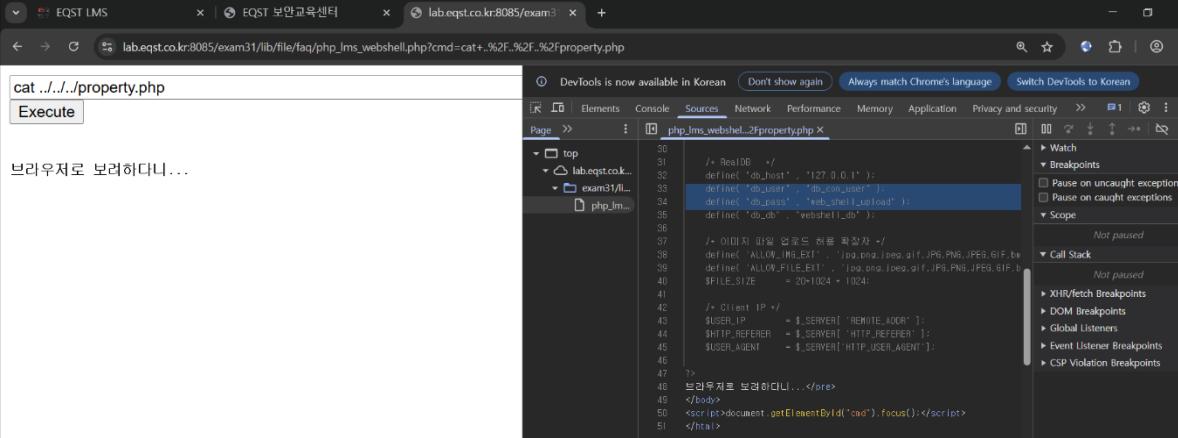
: 브라우저로 내용을 확인할 수 없게 설정되어 있음을 알 수 있다.



```
cat ../../property.php
브라우저로 보려하디니...
```

: 개발자도구를 이용하여 코드를 확인한다.

: 주석 처리된 DB User 명과 DB 계정 비밀번호를 획득할 수 있다. (정답: web_shell_upload)



```
cat ../../property.php
Execute

브라우저로 보려하디니...

// RealDB
// db.host = '127.0.0.1';
define('db_user', 'db_com_user');
define('db_pass', 'web_shell_upload');
define('db_db', 'webshell_db');

// 이미지 파일 업로드 허용 확장자
define(ALLOW_IMG_EXT, ['jpg.png.jpeg.gif.JPG.PNG.JPGE.JPGE']);
define(ALLOW_FILE_EXT, ['rar.zip.tar.gz.tgz']);
$FILE_SIZE = 20*1024 * 1024;

// Client IP
$_USER_IP = $_SERVER['REMOTE_ADDR'];
$_HTTP_REFERER = $_SERVER['HTTP_REFERER'];
$_USER_AGENT = $_SERVER['HTTP_USER_AGENT'];

?>
// 브라우저로 보려하디니...
</body>
<script>document.getElementById('cat').focus();</script>
</html>
```

성명	프로젝트 후 소감
박기쁨	<p>File Upload 취약점에 대해 실습하며, 다양한 방식으로 파일 업로드 필터링을 우회할 수 있음을 배웠다. 수많은 필터링 속에서도, 공격자의 입장에서는 우회 방법을 단 한 가지라도 발견한다면, 방어자의 입장에서는 취약점이 단 한 가지라도 존재한다면, 결국 해킹이 이루어지게 되고 정보가 누출된다는 점이 참 어렵고도 잔인하다고 느껴졌다.</p> <p>또, 파일 업로드 우회에 이어 실제로 웹쉘을 이용하여 DB 정보를 탈취하는 실습을 통해, 실제 해킹 시 사용될 법한 방법과 과정을 직접 경험해볼 수 있어 매우 흥미로웠다.</p>