□ **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>

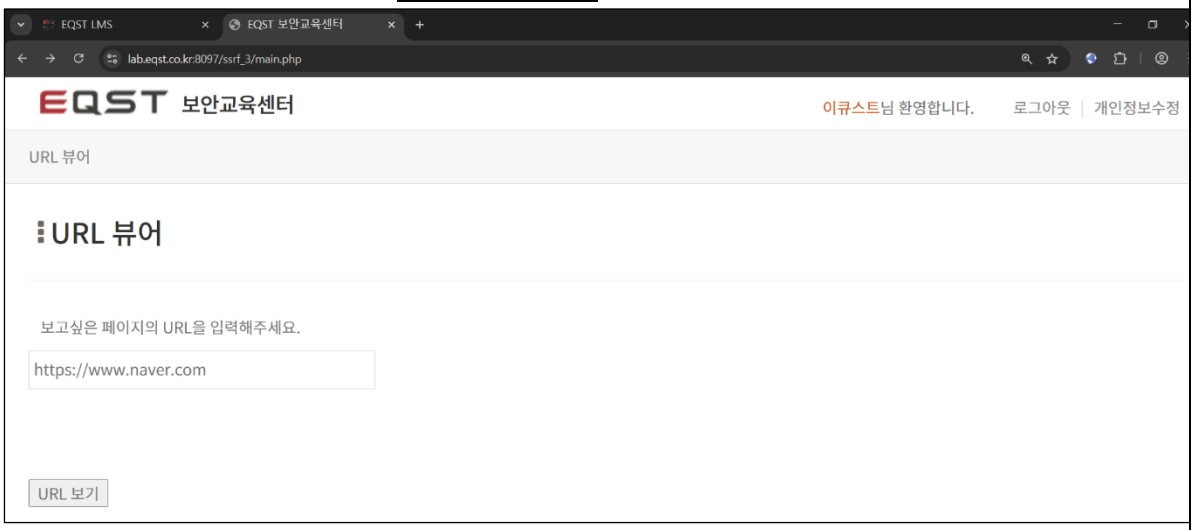
SSRF(Server-Side Request Forgery, 서버 측 요청 위조)는 공격자가 서버에서 이루어지는 요청을 변조하는 웹 취약점 공격이다. CSRF(Client-Side Request Forgery)가 '클라이언트의 권한을 이용해' 악의적인 요청을 전송하는 것과 달리, SSRF 는 '서버의 권한을 이용해' 악의적인 요청을 전송한다. 즉, 서버로부터 공격이 시작되기 때문에 외부에서 직접 접근이 불가한 내부 서버 및 시스템에 접근할 수 있으며, 내부 네트워크 내에서 악의적인 행위를 수행할 수 있다.

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.

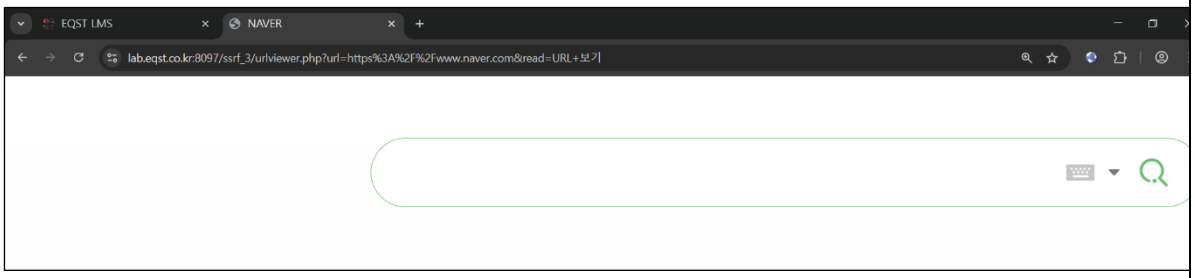
Step 1. 관리자 페이지 접근

Step 1-1. 페이지 작동 방식 확인

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

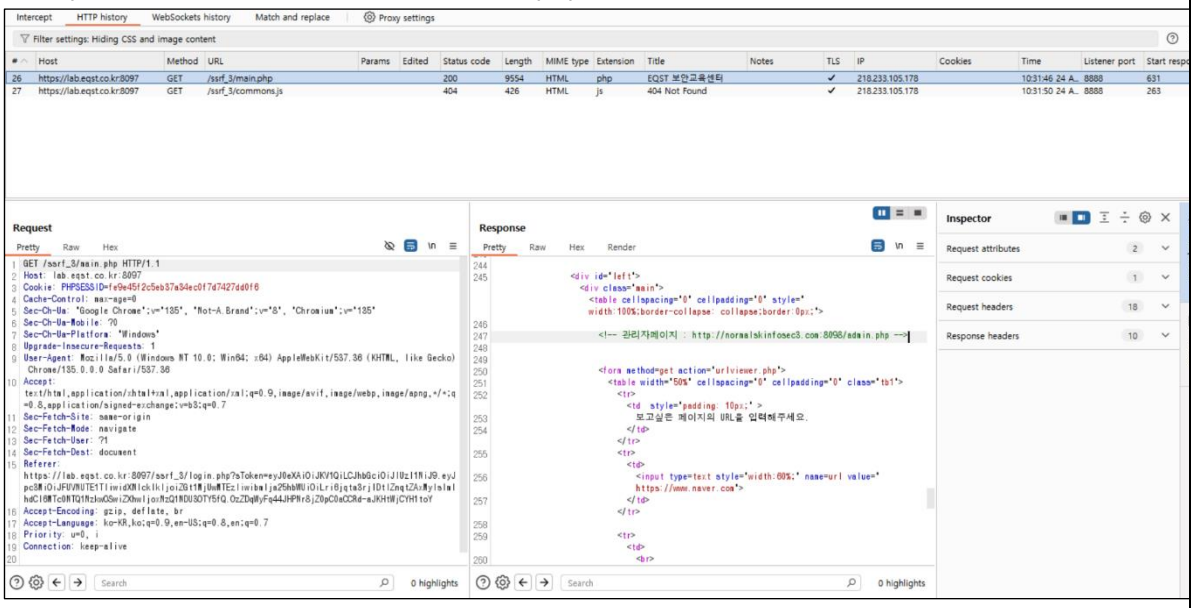


(네이버 사이트로 연결되는 것 확인)

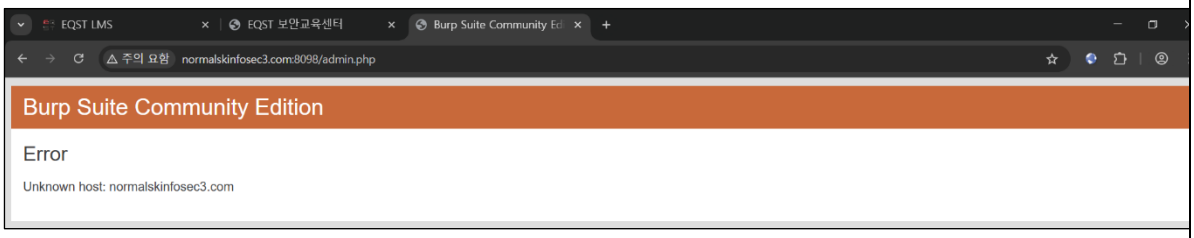


Step 1-2. 관리자 페이지 접속

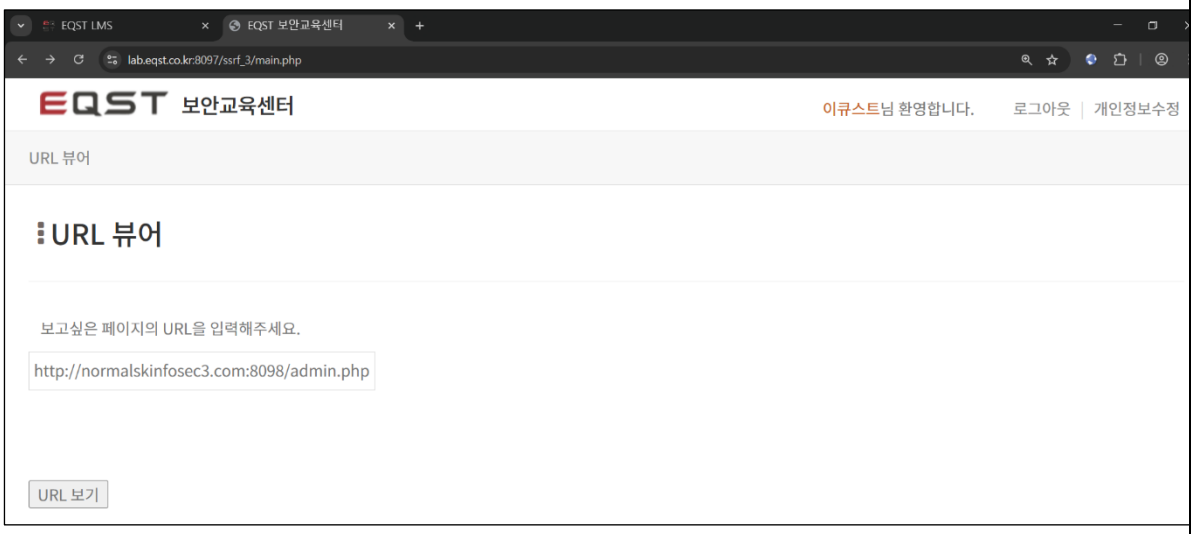
: Burp 로 응답을 확인해보면 코드 내 주석에서 관리자 페이지의 주소를 확인할 수 있다.
(http://normalskinfosec3.com:8098/admin.php)



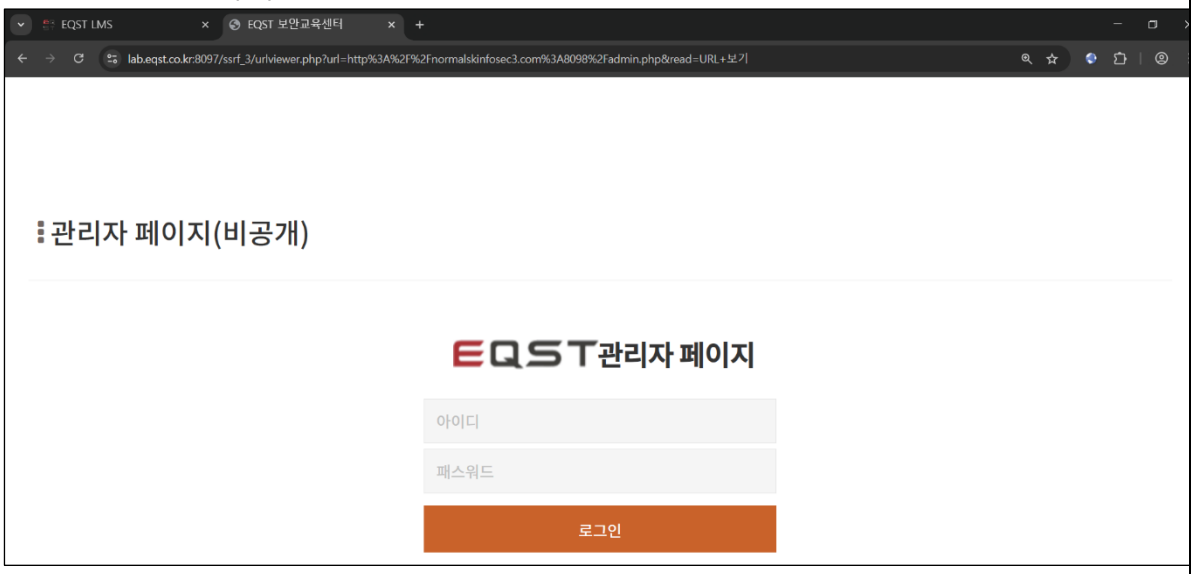
(URL 창에 관리자 페이지 주소를 직접 입력해서는 접속할 수 없음)



: URL 뷰어 페이지의 검색창에 관리자 페이지 주소를 입력하여 접속한다.



(접속 성공, URL 변경됨 (http://normalskinfosec3.com:8098/admin.php → https://lab.eqst.co.kr:8097/ssrf_3/urlviewer.php?url=http%3A%2F%2Fnormalskinfosec3.com%3A8098%2Fadmin.php&read=URL+보기))

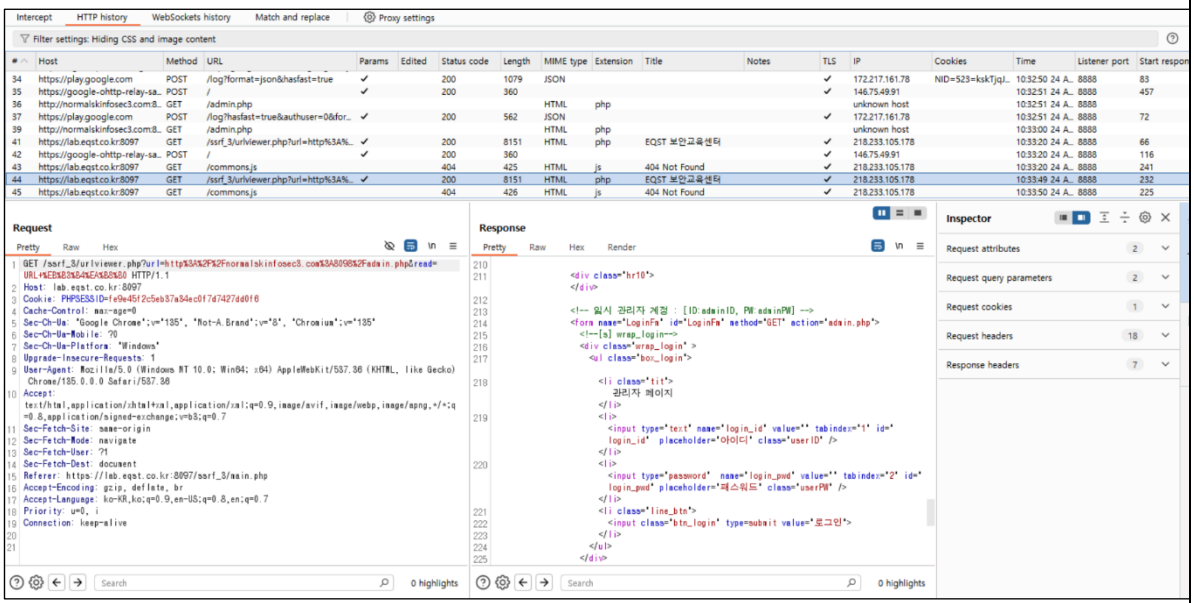


Step 2. 관리자 페이지 로그인

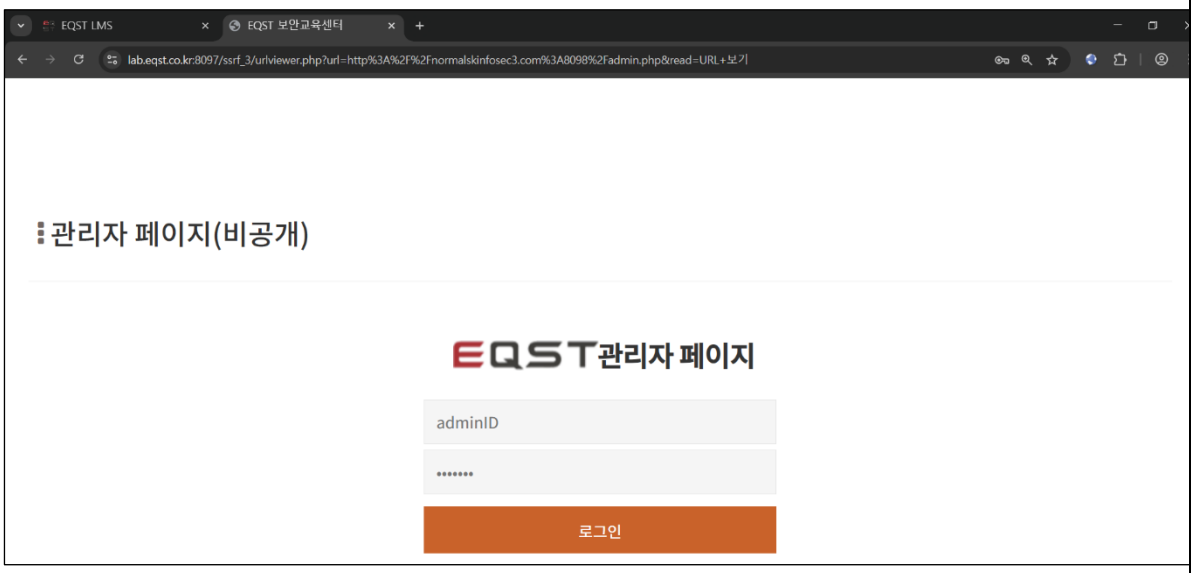
Step 2-1. 직접 로그인 시도

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

(ID: adminID, PW: adminPW)



: 관리자 페이지에 직접 로그인을 시도한다.

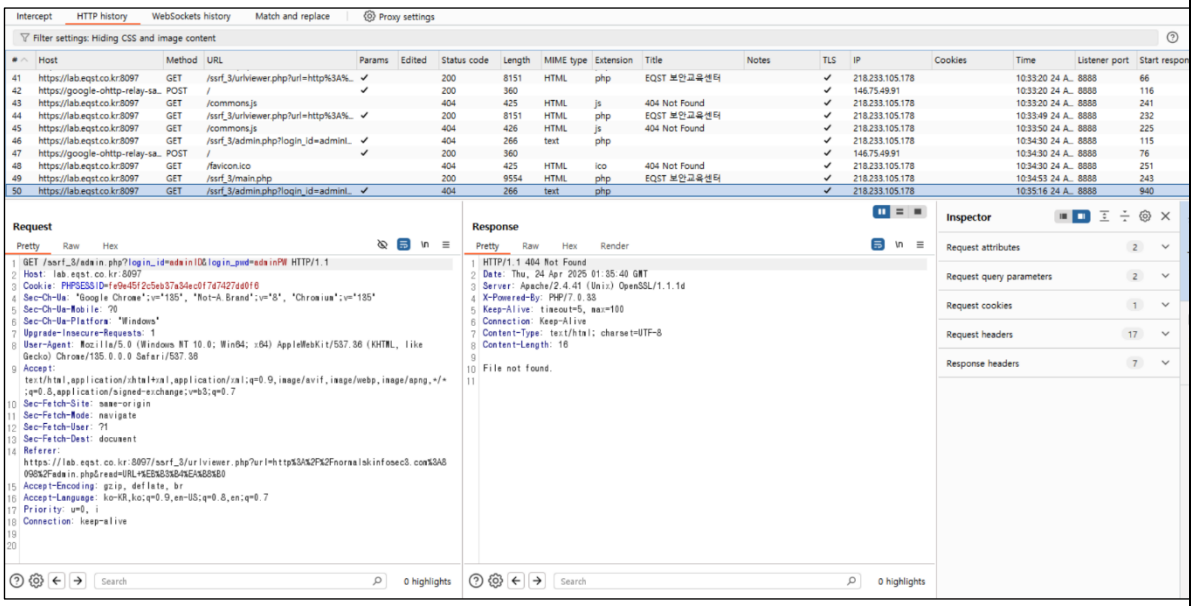


(로그인 창에 ID 와 PW 를 직접 입력해서는 접속할 수 없음)

Step 2-2. 다른 방법으로 로그인 시도

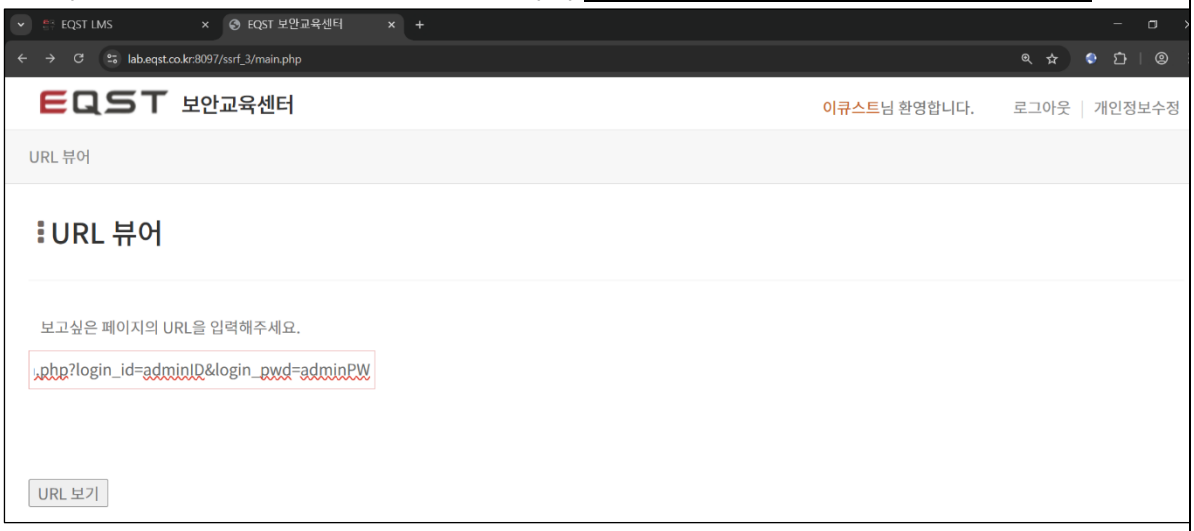
: Burp 를 통해 ID, PW 파라미터 및 값이 URL 에 어떻게 전달되는지 참고한다.

(?login_id=adminID&login_pwd=adminPW)

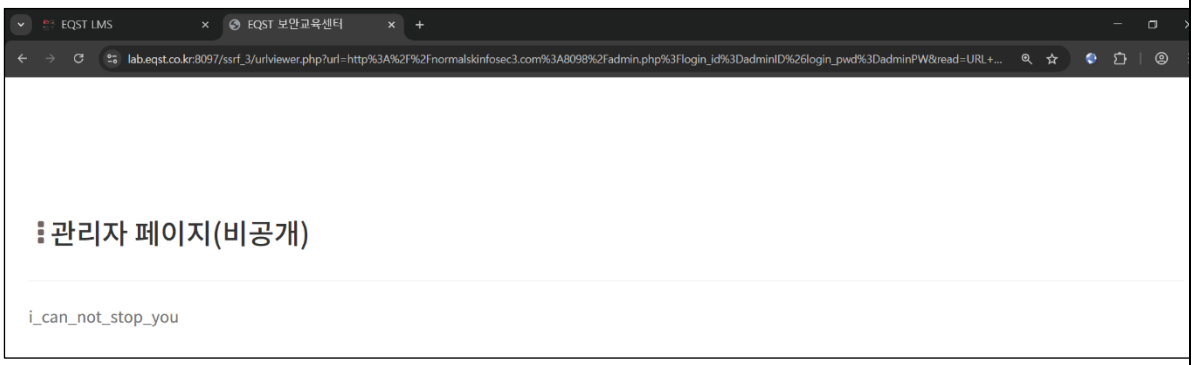


: 접속 시 URL 이 변경되지 않도록, 직접 관리자 페이지 주소에 파라미터와 값을 붙여 URL 뷰어에 입력한다.

(http://normalskinfosec3.com:8098/admin.php?login_id=adminID&login_pwd=adminPW)



: 로그인 성공



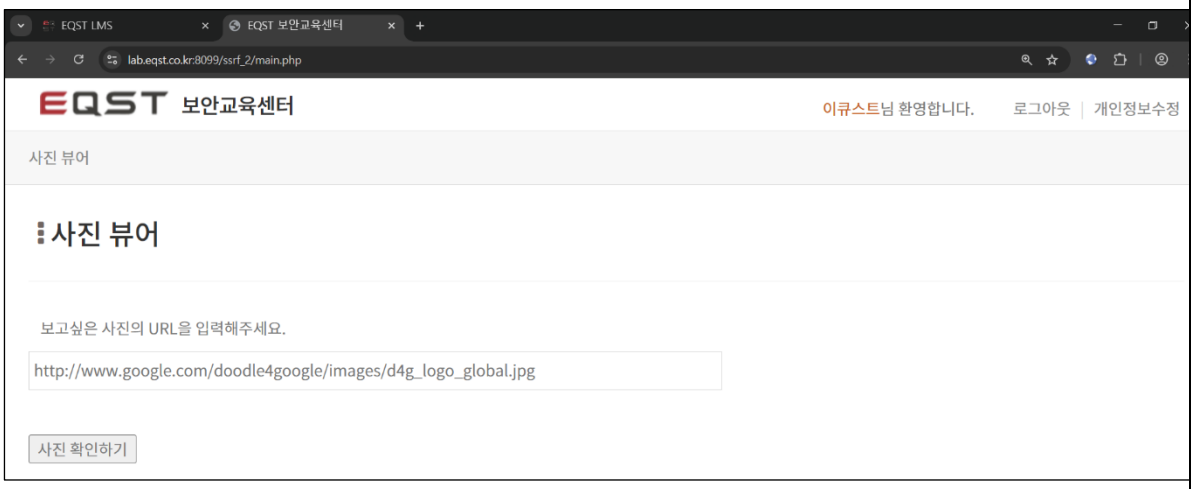
* SK 쉴더스 '[Special Report] 웹 취약점과 해킹 매커니즘#10 SSRF(Server-Side Request Forgery)' 참고 (https://blog.naver.com/PostView.naver?blogId=sk_shieldus&logNo=223013833037&parentCategoryNo=&categoryNo=&viewDate=&isShowPopularPosts=false&from=postView)

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

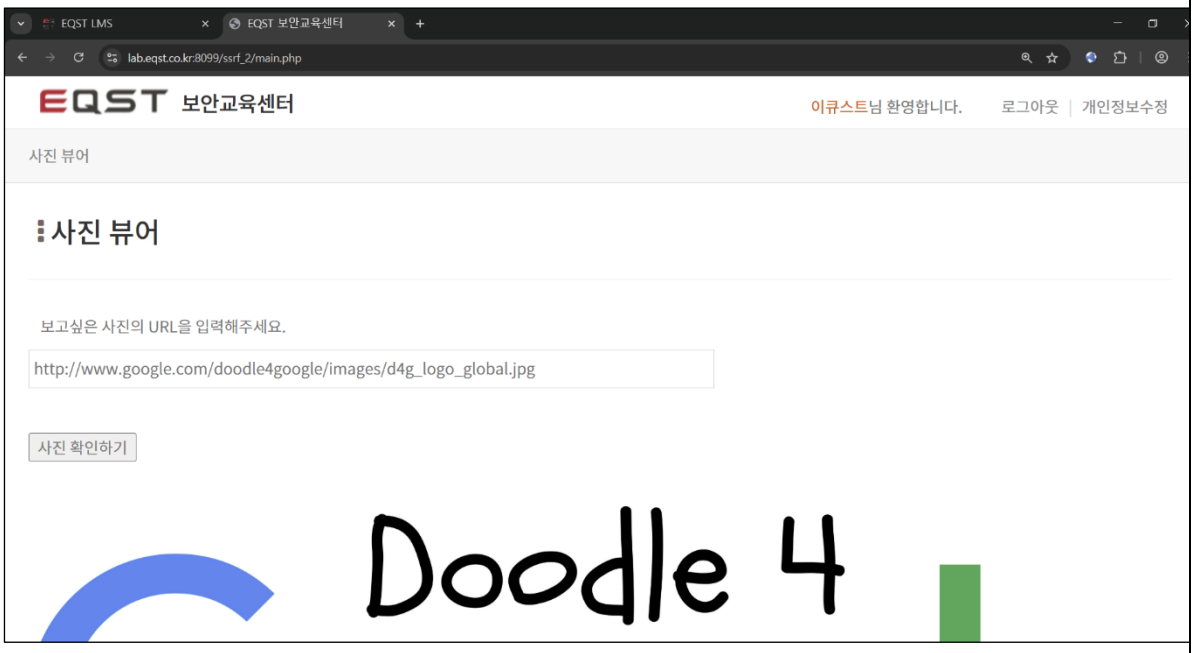
<과정 설명>

Step 1. 페이지 작동 방식 확인

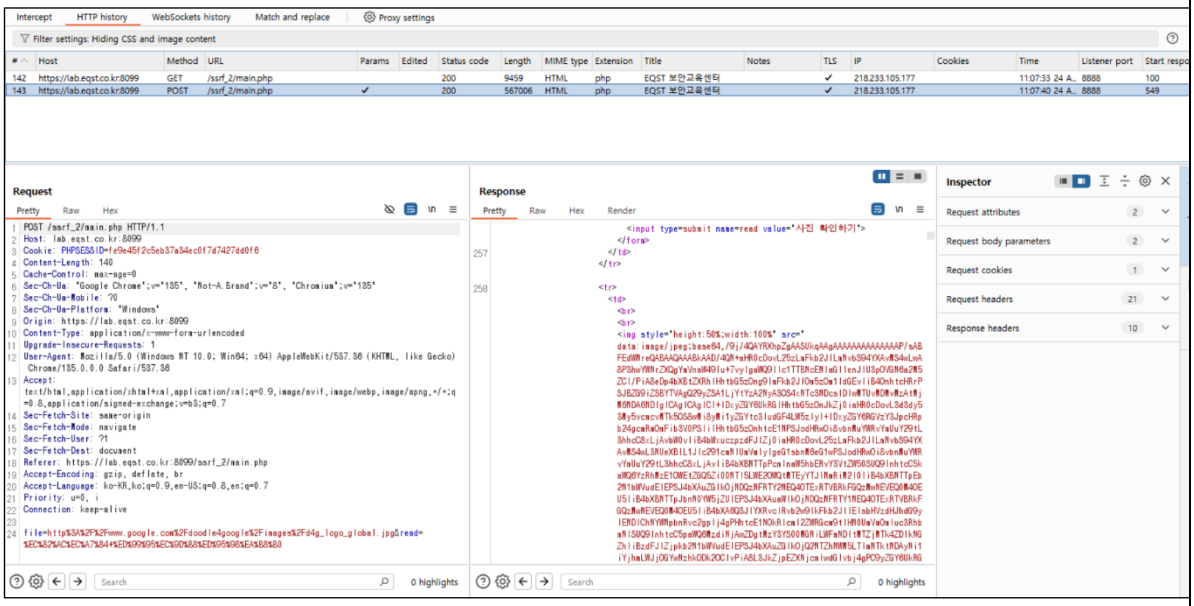
Step 1-1. 페이지 작동 방식 확인
: 사진 확인하기 버튼을 눌러 사진 뷰어 페이지의 기능을 확인한다.



(입력한 URL 의 사진을 가져와 보여줌)



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

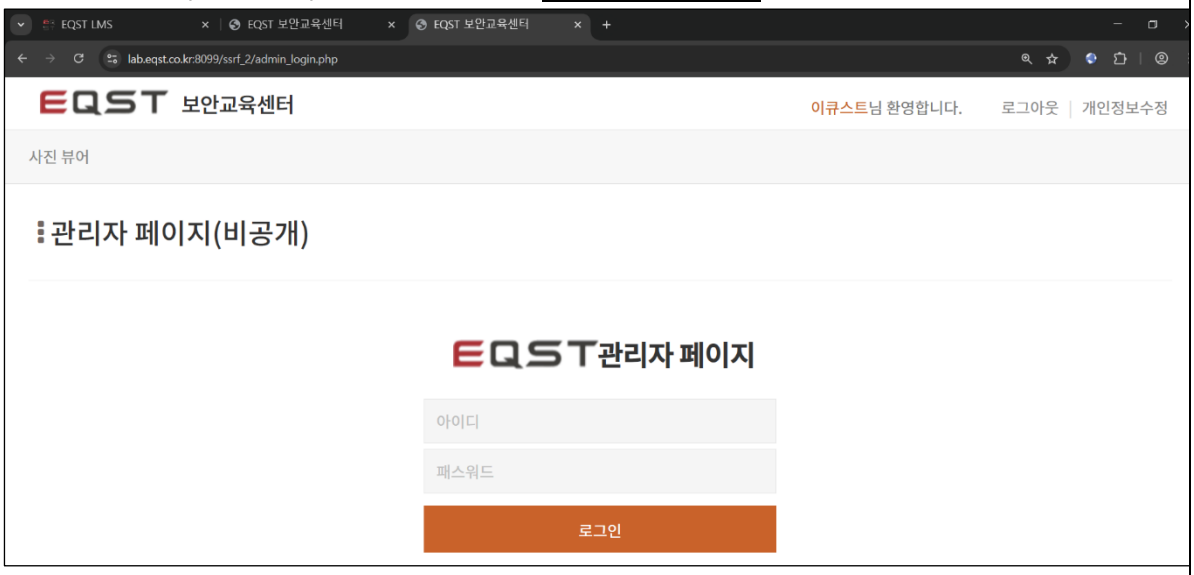


Step 2. admin.php 확인

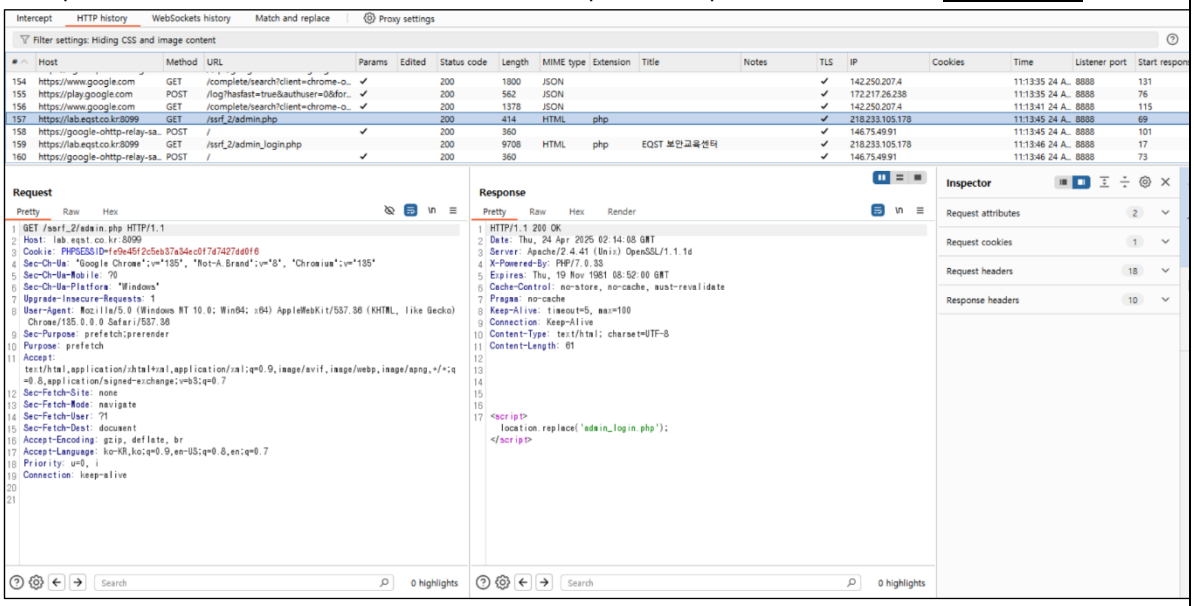
Step 2-1. https://lab.eqst.co.kr:8099/ssrf_2/admin.php 확인

: URL 창에 https://lab.eqst.co.kr:8099/ssrf_2/admin.php 를 입력하여 직접 접속을 시도해본다.

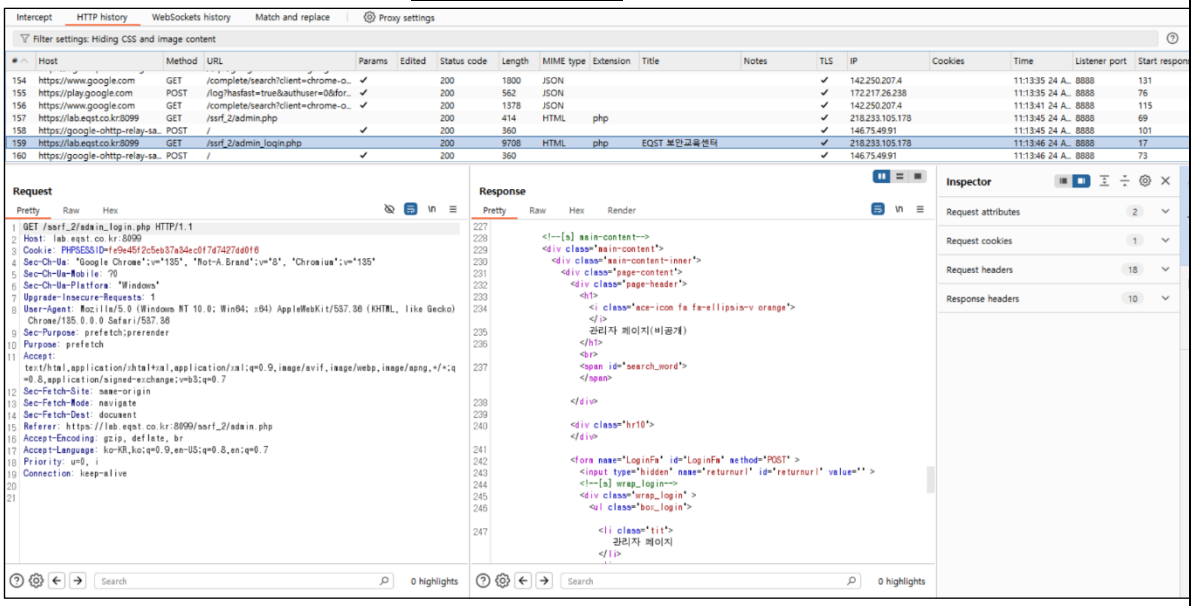
: 자동으로 https://lab.eqst.co.kr:8099/ssrf_2/admin_login.php 로 이동한다.



(Burp 를 통해 관련 코드를 확인할 수 있음, https://lab.eqst.co.kr:8099/ssrf_2/admin.php)



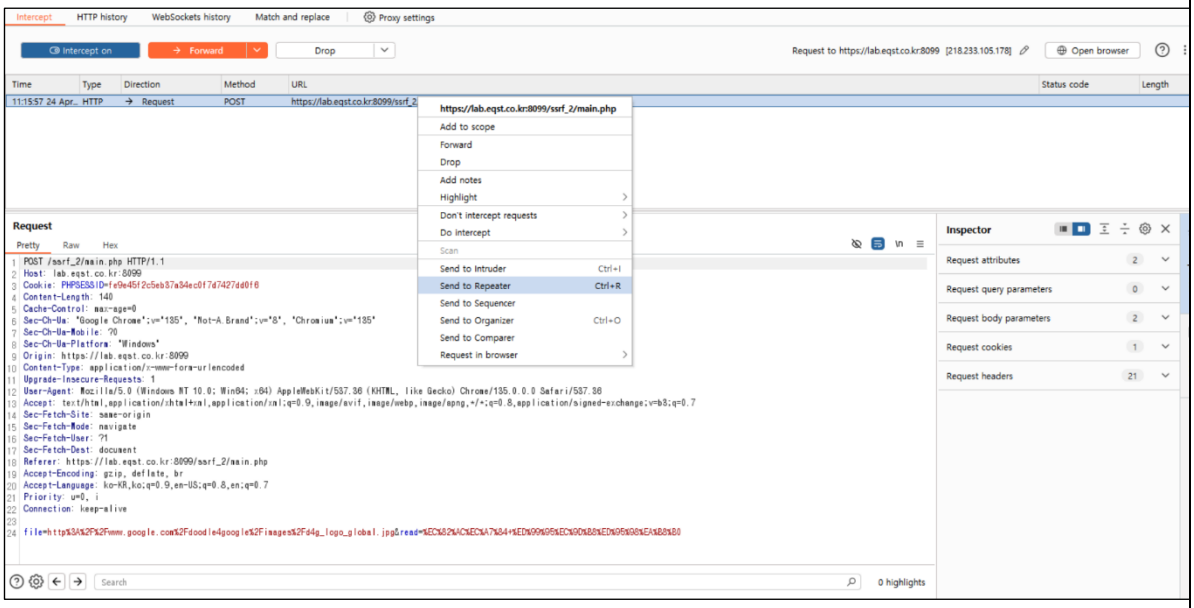
(https://lab.eqst.co.kr:8099/ssrf_2/admin_login.php)



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

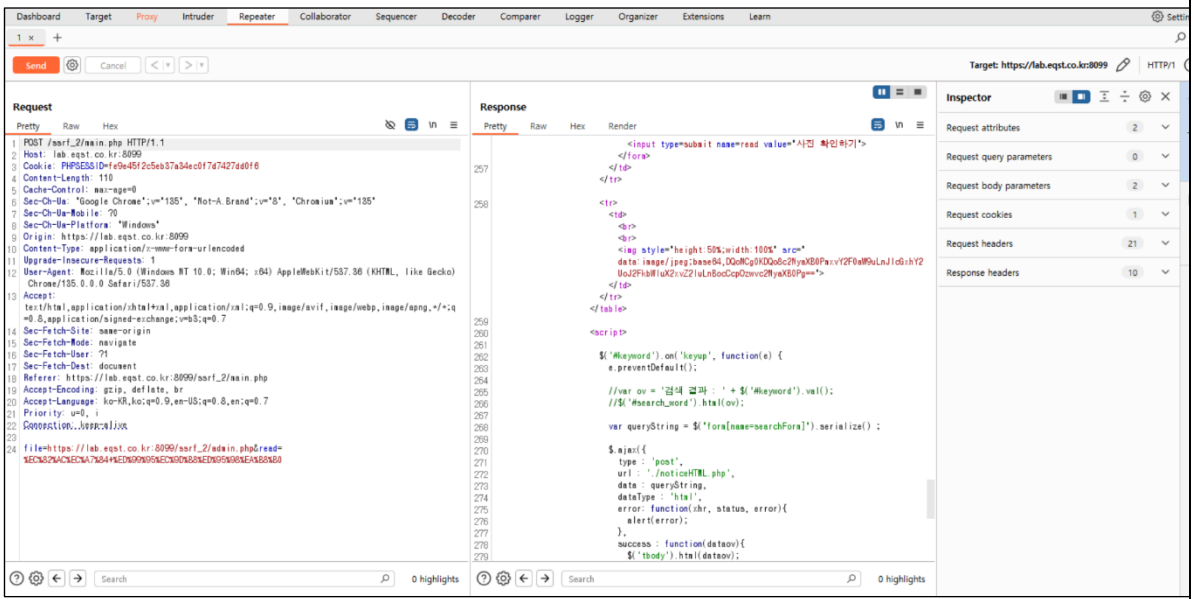
Step 3-1. repeater 로 이동

: 사진 뷰어 페이지에서의 요청을 intercept 하여 repeater 로 보낸다.

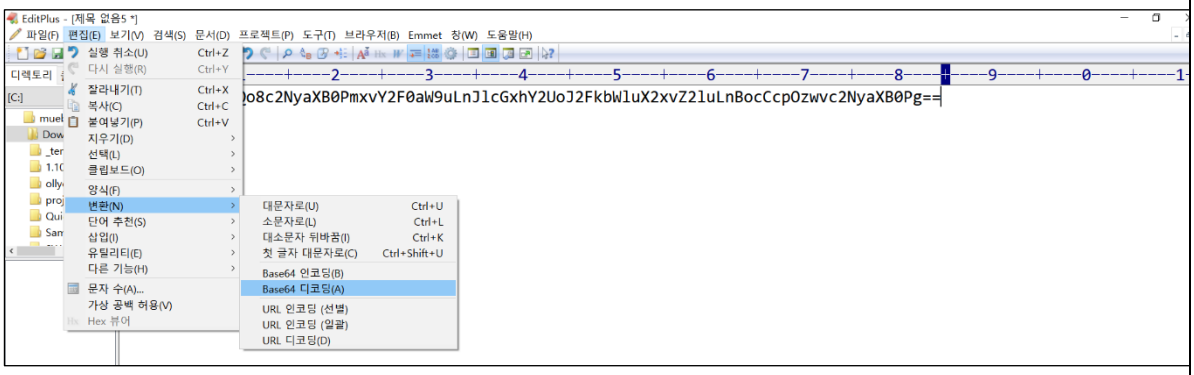


Step 3-2. file 파라미터에 https://lab.eqst.co.kr:8099/ssrf_2/admin.php 삽입 후 요청 전송

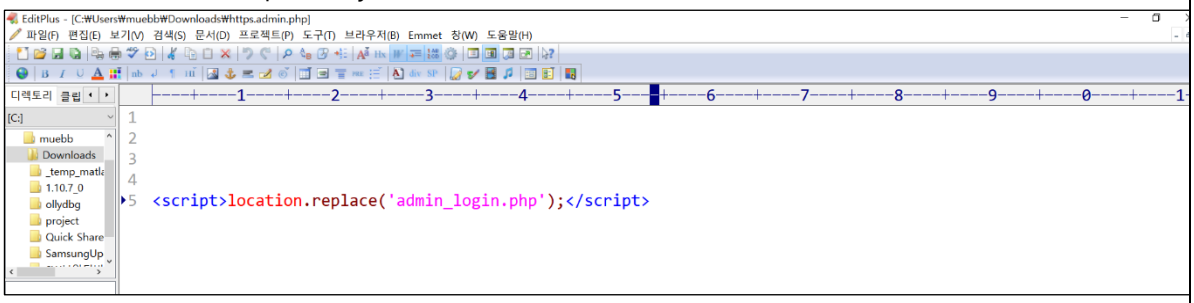
: img 태그에 어떤 데이터가 들어있음을 확인할 수 있다.



: 텍스트 편집기를 이용하여 Base64 디코딩을 수행한다.

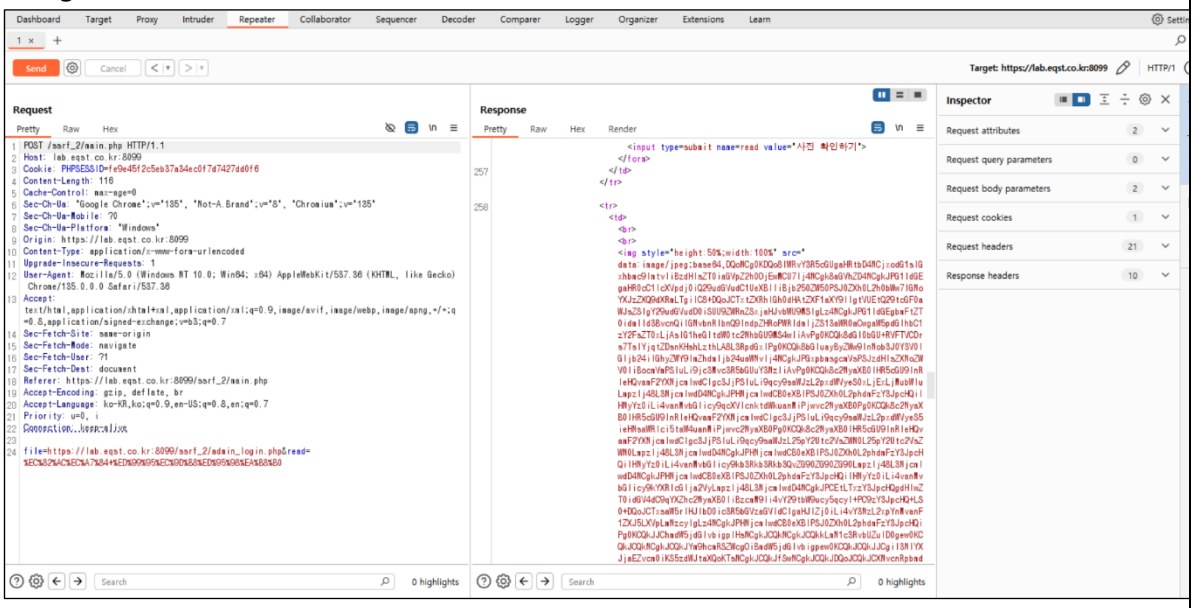


(코드 확인 가능, Burp history 에서 확인했던 내용과 동일)

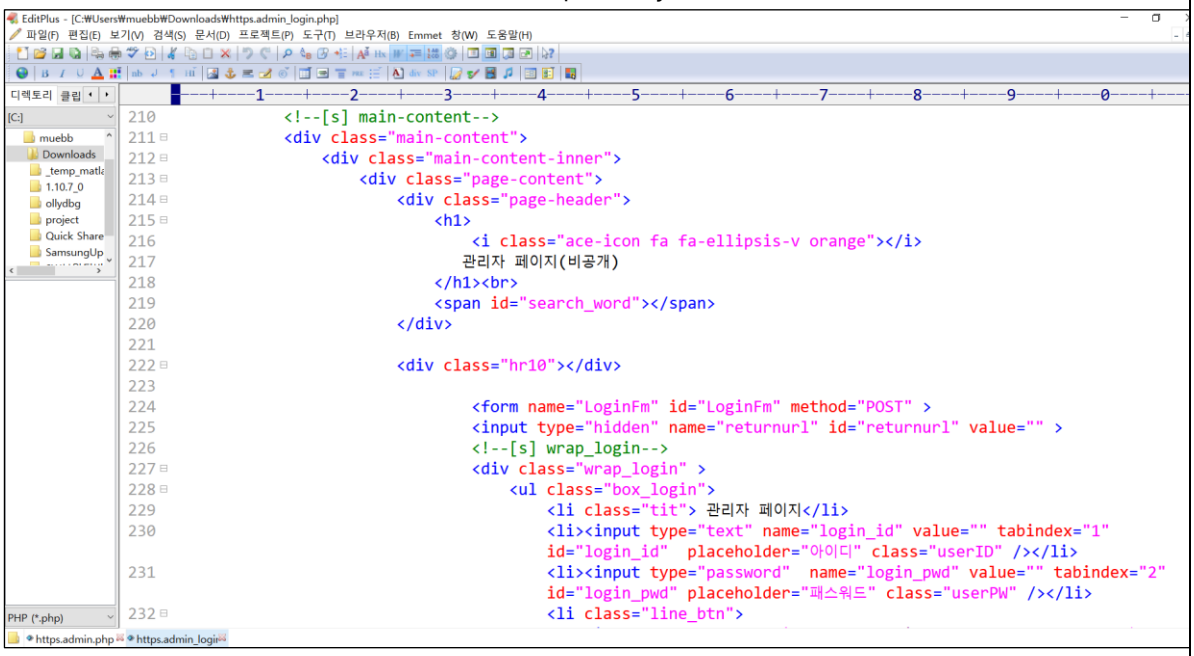


Step 3-3. file 파라미터에 https://lab.eqst.co.kr:8099/ssrf_2/admin_login.php 삽입 후 요청 전송

: img 태그에 어떤 데이터가 들어있음을 확인할 수 있다.

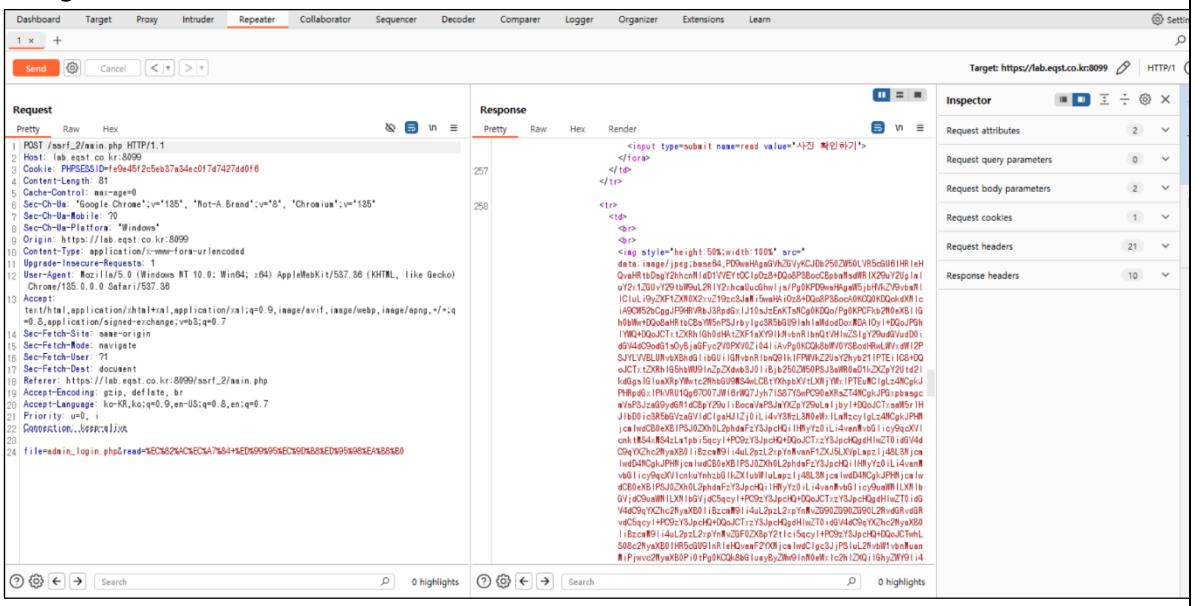


(base64 디코딩 수행 후 코드 확인 가능, Burp history 에서 확인했던 내용과 동일)

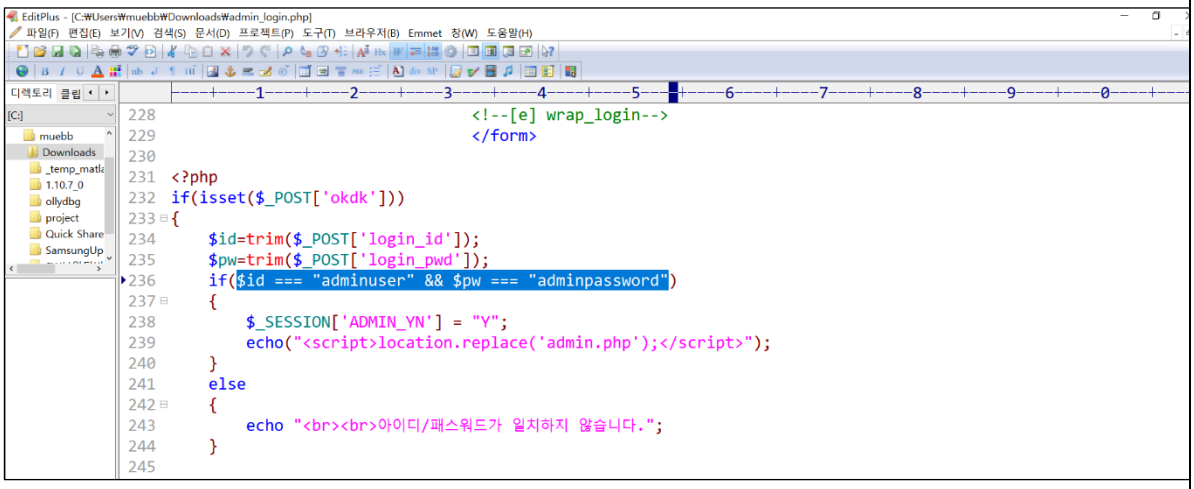


Step 3-4. file 파라미터에 admin_login.php 삽입 후 요청 전송

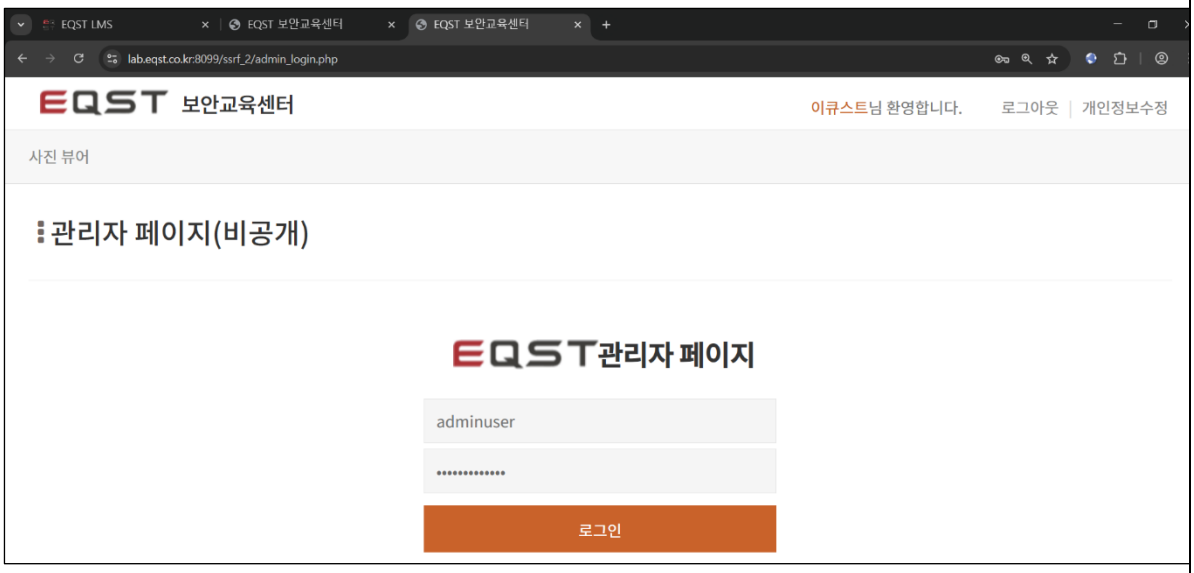
: img 태그에 어떤 데이터가 들어있음을 확인할 수 있다.



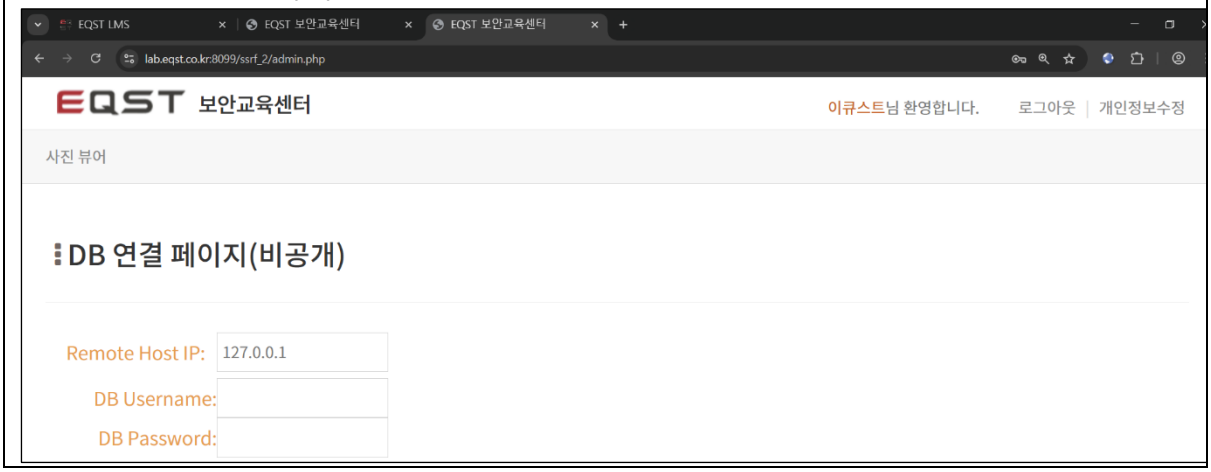
: Base64 디코딩 수행 후, 코드에서 관리자 페이지(admin_login.php)의 ID 와 PW 를 확인할 수 있다. (id: adminuser, pw: adminpassword)



: 관리자 페이지(admin_login)에 ID 와 PW 를 입력하여 로그인을 시도한다.



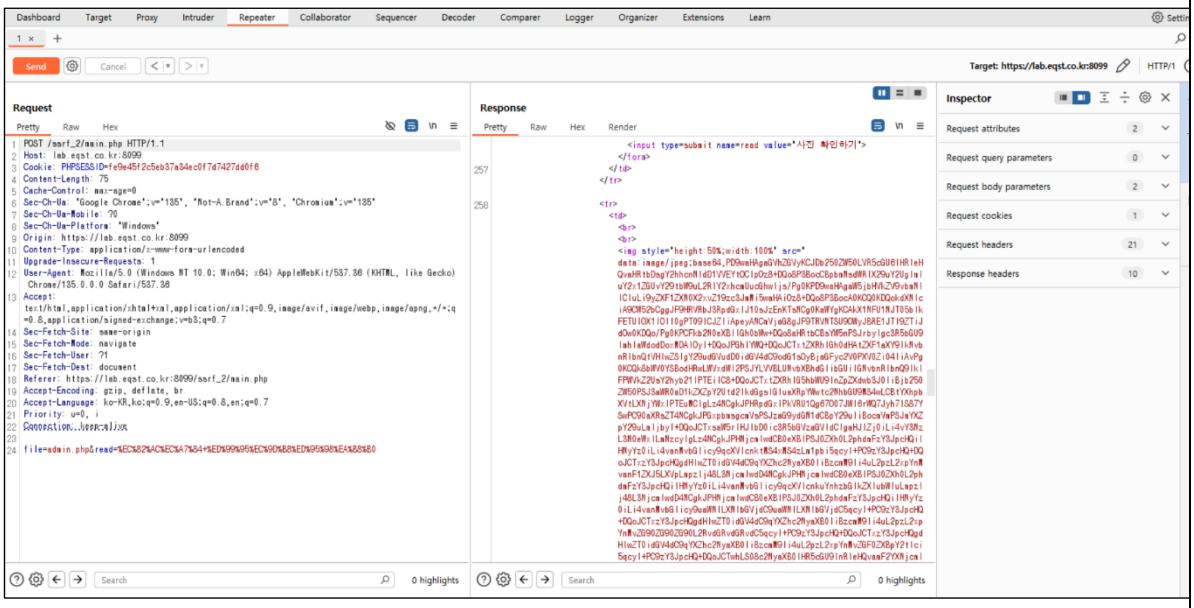
: 로그인 성공, admin.php 접속 성공



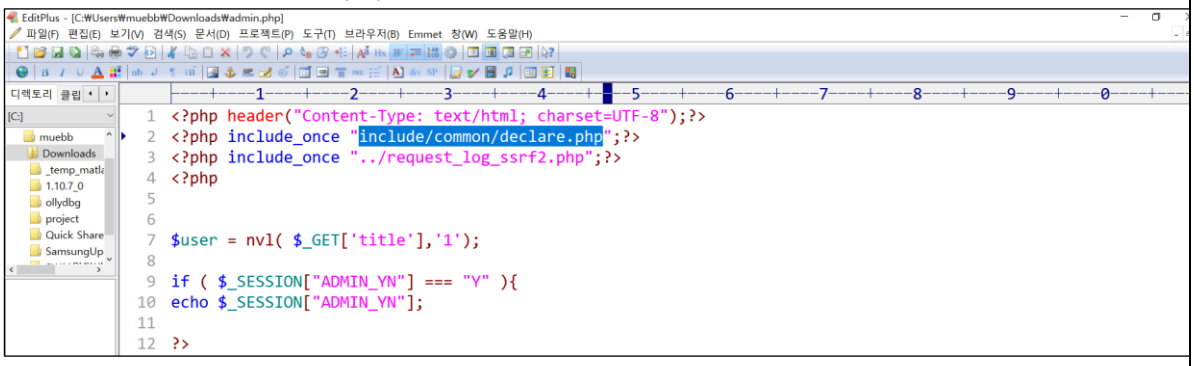
Step 4. DB 연결 페이지를 통한 내부 DB 서버 접속

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

: img 태그에 어떤 데이터가 들어있음을 확인할 수 있다.

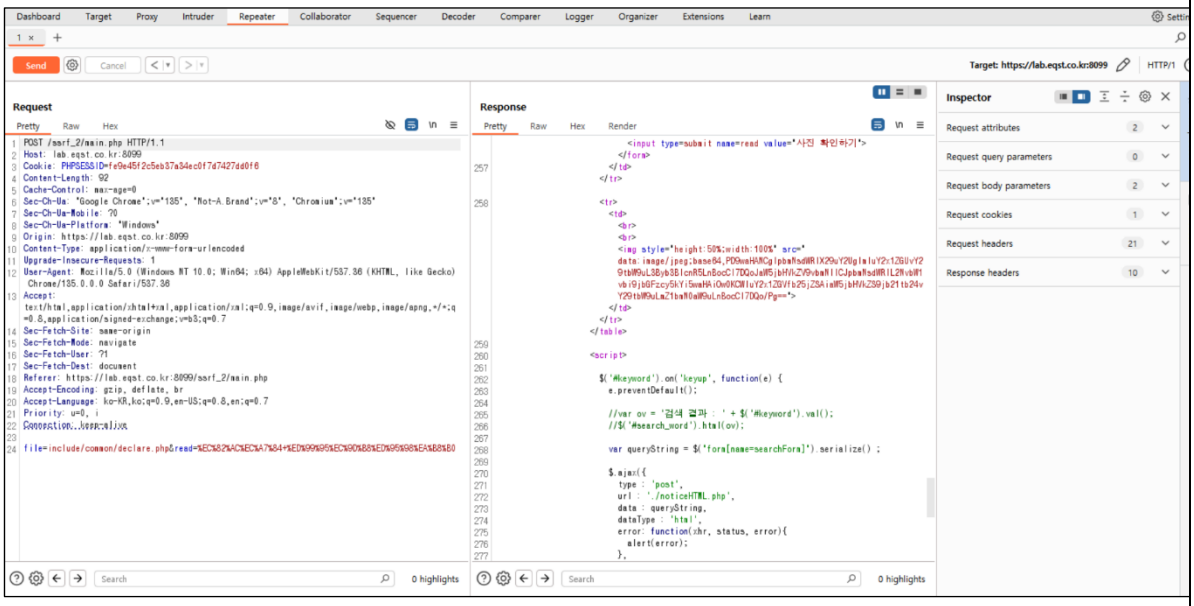


: Base64 디코딩 수행 후, 코드에서 admin.php 에 include 된 declare.php 를 확인할 수 있다. (include/common/declere.php)

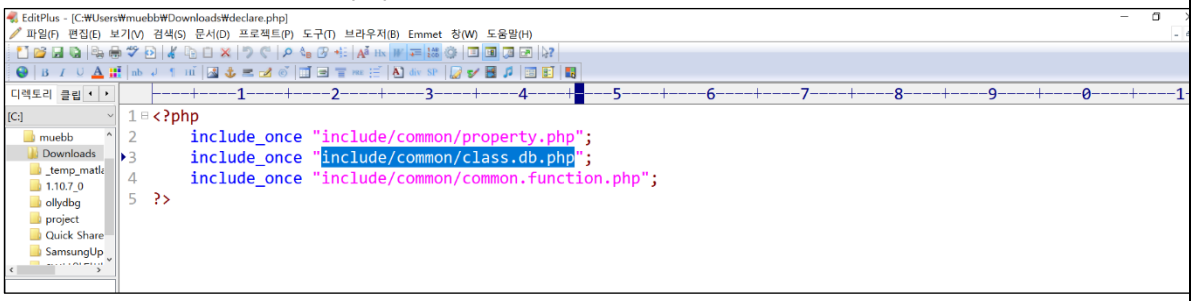


Step 4-2. file 파라미터에 include/common/declere.php 삽입 후 요청 전송

: img 태그에 어떤 데이터가 들어있음을 확인할 수 있다.

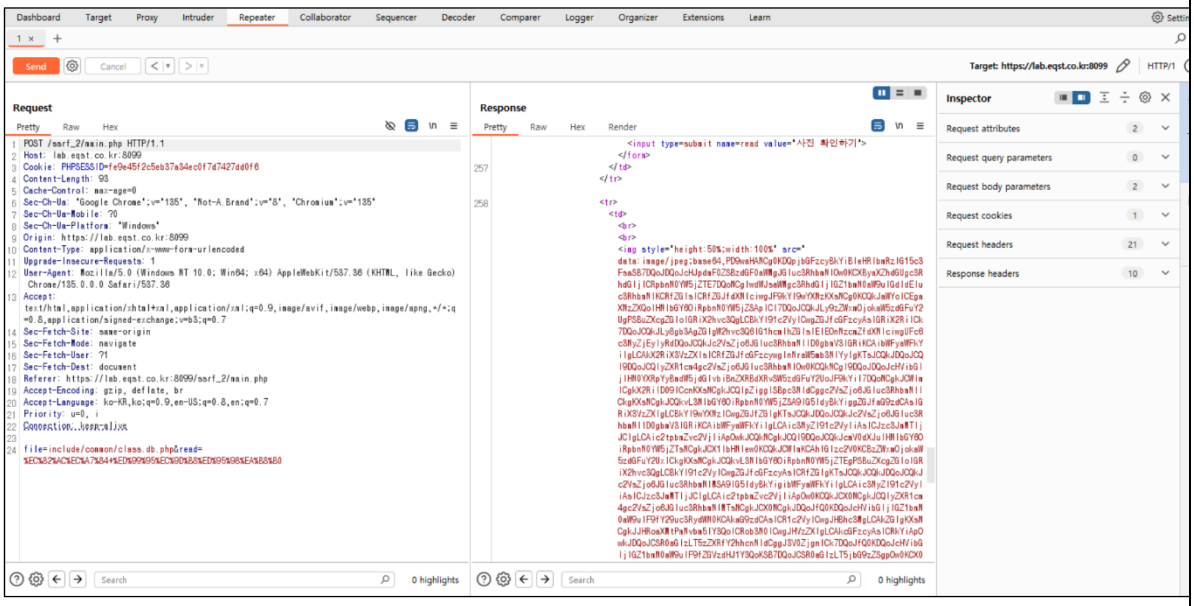


: Base64 디코딩 수행 후, 코드에서 declare.php 에 include 된 class.db.php 를 확인할 수 있다. (include/common/class.db.php)

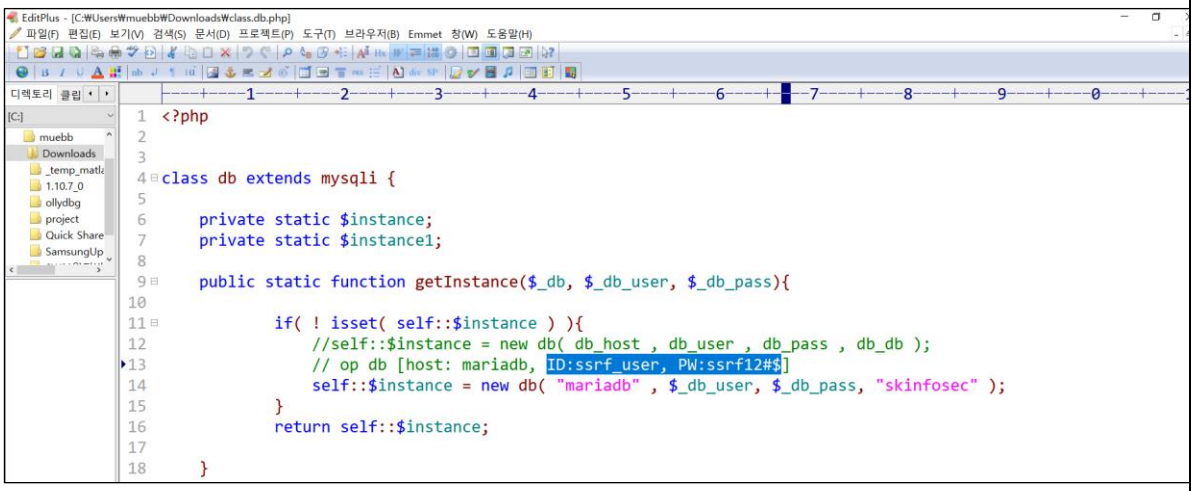


Step 4-3. file 파라미터에 include/common/class.db.php 삽입 후 요청 전송

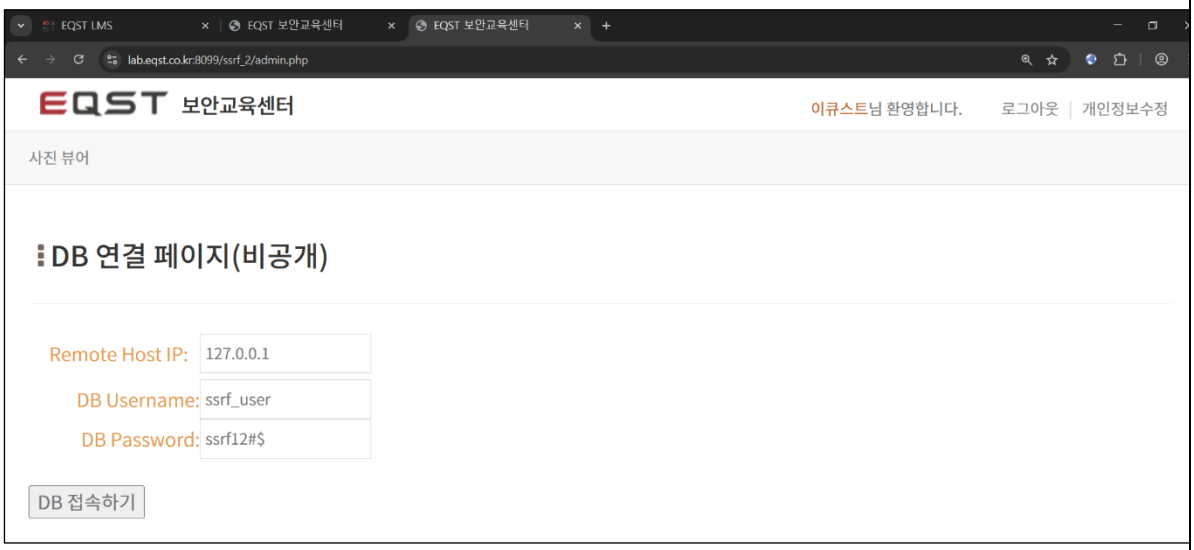
: img 태그에 어떤 데이터가 들어있음을 확인할 수 있다.



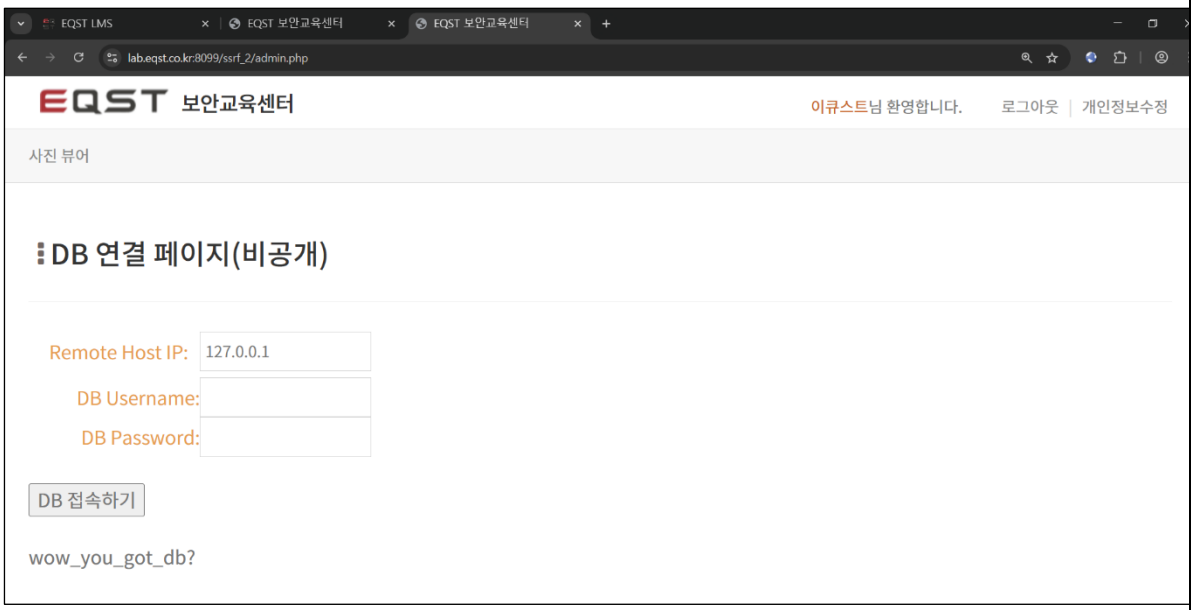
: Base64 디코딩 수행 후, 코드에서 DB 연결 페이지(admin.php)의 ID 와 PW 를 확인할 수 있다. (ID: ssrf_user, PW: ssrf12#$)



: 획득한 ID 와 PW 를 입력한다.



: 로그인 성공



* 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)

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.