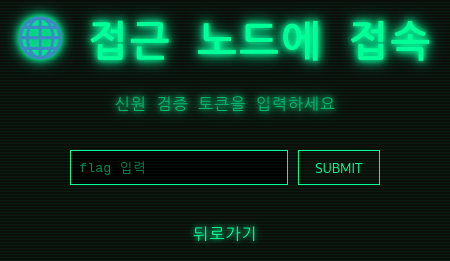
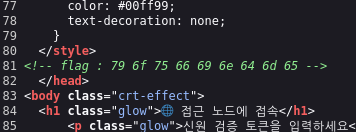
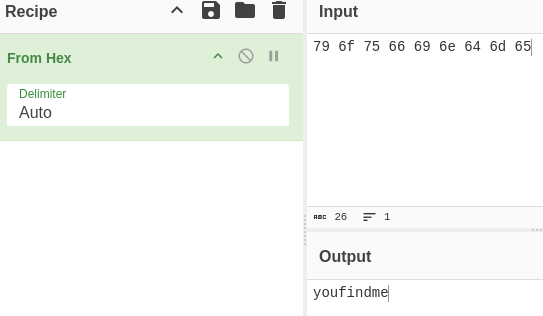
**ESG Walkthrough – 조범근**

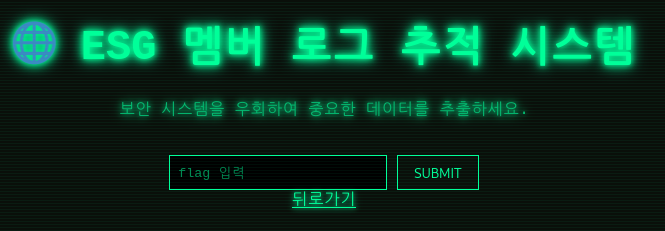
**◎ 1번 문제 - 접근 노드에 접속** (페이지 소스 확인) ****

1) 페이지 소스 보기

2) 하단 주석 확인 <!-- flag : 79 6f 75 66 69 6e 64 6d 65 -->  
****

3) CyberChef 에서 From Hex로 디코딩  


**[ FLAG ] youfindme**

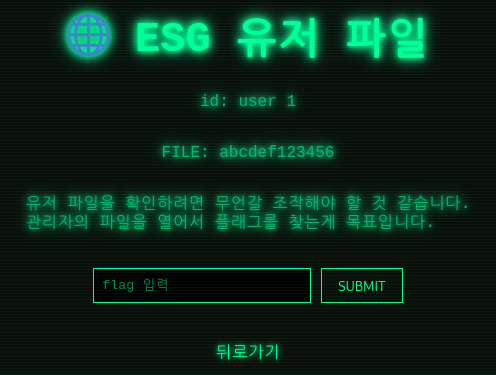
**◎ 2번 문제 - ESG 멤버 로그 추적 시스템** (파라미터 조작) ****

1) 상단 URL 확인  


2) 파라미터값 admin=0이 되어있는것을 1로 고친다  

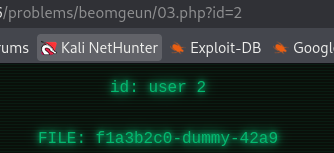

3) 플래그가 출력된 것을 확인

**[ FLAG ] intothedeep**

**◎ 3번 문제 - ESG 인증 포털** (IDOR) ****

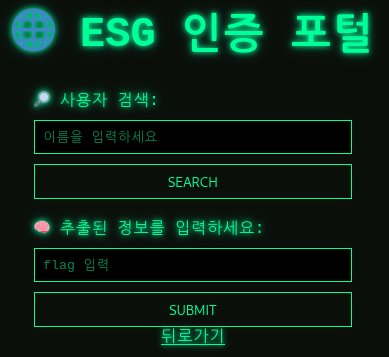
1) 무언갈 조작해야한다고 하니 파라미터 등을 조작해야 하는 문제인것을 확인

2) id: user 1 인것을 보니 2, 3 등 여러 유저가 있는것을 확인

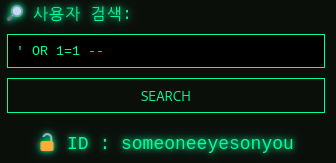
3) URL뒤에 ?id=2 를 입력, user 2의 파일이 출력된다  


4) 관리자의 파일을 열라고 했으니 URL뒤에 ?id=admin 을 입력하면 플래그 출력

**[ FLAG ] entertheesg**

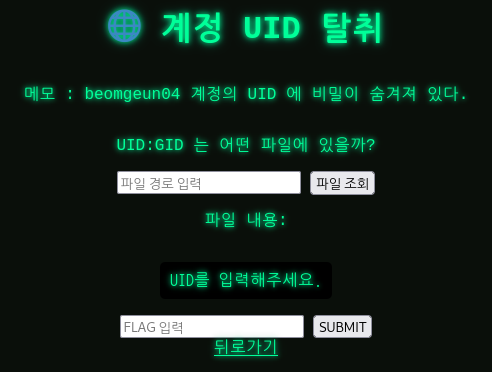
**◎ 4번 문제 - ESG 인증 포털** (SQL Injection) ****

1) DB의 사용자를 검색하는 문제이니 대표적인 SQL Injection 문구를 입력해본다

2) ' OR 1=1 -- 입력 후 SEARCH  


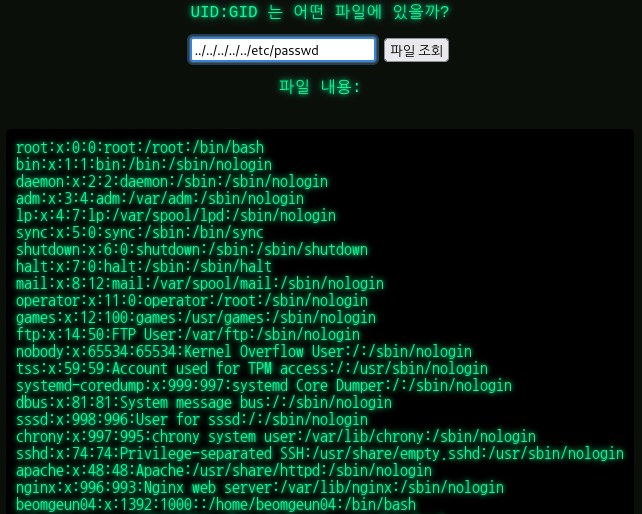
3) ID 확인

**[ FLAG ] someoneeyesonyou**

**◎ 5번 문제 - 계정 UID 탈취** (디렉토리 트래버설) ****

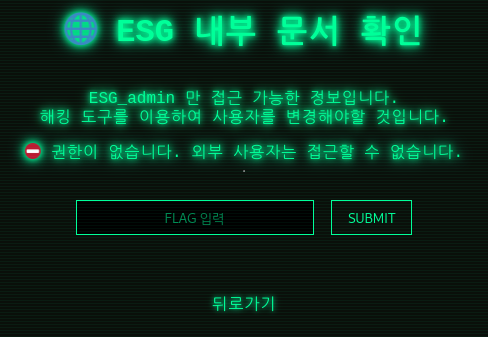
1) UID:GID 는 /etc/passwd 파일에 저장되어 있다

2) 디렉토리 트래버설을 이용해 ../ 를 하나씩 추가하여 찾아본다

3) ../../../../../etc/passwd 입력  


4) UID를 찾았으면 입력

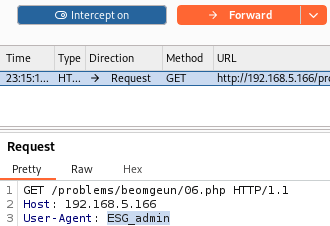
**[ FLAG ] 1392**

**◎ 6번 문제 - ESG 내부 문서 확인** (User-Agent 기반 인증 우회) ****

1) ESG\_admin만 접속 가능하다는것을 확인

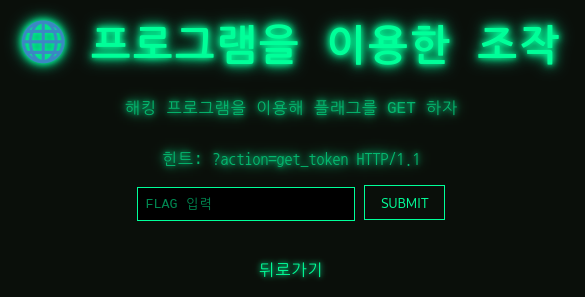
2) 해킹 도구를 이용해야 한다고 했으니 burpsuite를 준비한다

3) burpsuite로 Intercept 후 새로고침

4) User-Agent: 란을 지우고 ESG\_admin으로 수정 후 Forward  


5) FLAG 확인

**[ FLAG ] youresharp**

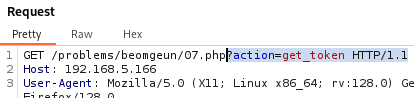
**◎ 7번 문제 - 프로그램을 이용한 조작** (HTTP Method Manipulation) ****

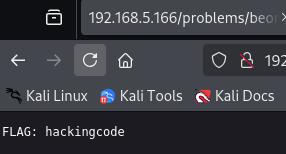
1) 해킹 프로그램을 이용하랬으니 burpsuite를 준비한다

2) GET 하자고 했으니 POST/GET 방식을 이용한 문제로 확인

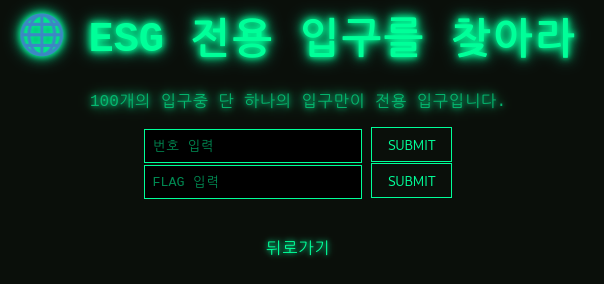
3) 힌트 ?action=get\_token HTTP/1.1 확인

4) FLAG 입력칸에 아무 값이나 입력 후 SUBMIT을 burpsuite로 잡는다

5) POST를 GET으로 바꾸고 주소 뒤에 이전의 힌트 파라미터를 추가한다  


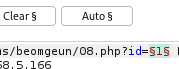
6) Forward 후 플래그 확인  


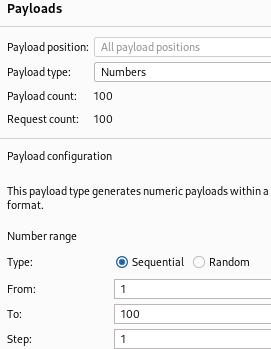
**[ FLAG ] hackingcode**

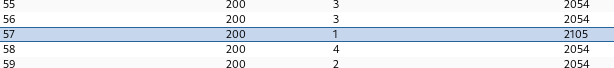
**◎ 8번 문제 - ESG 전용 입구를 찾아라** (Burte Force Attack) ****

1) 100개의 입구 중 전용 입구를 찾는 것이니 burpsuite를 이용한다

2) 입력칸에 아무 값이나 넣고 SUBMIT을 Intercept 후 Intruder로 넘긴다  

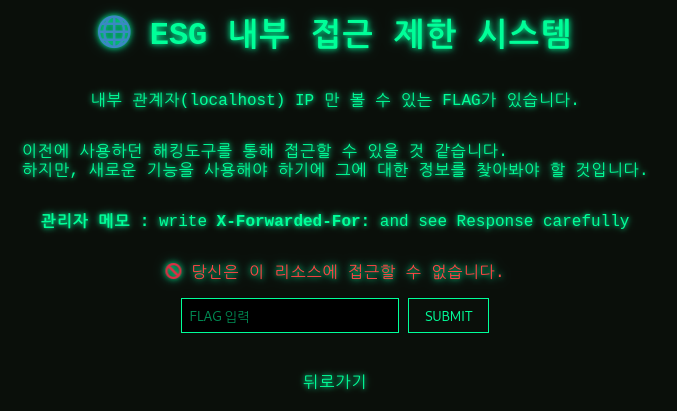

3) id= 에 나온 할당값을 페이로드로 지정한다  


4) 페이로드 타입을 Numbers로 수정하고 시작을 1, 끝을 100으로 지정한 후 Attack  


5) 57번 응답의 길이가 다른 응답과는 다른것을 확인  


6) 페이지에서 57번을 입력하면 플래그를 확인 가능

**[ FLAG ] stopdiggingin**

**◎ 9번 문제 - 내부 접근 제한 시스템** (HTTP 헤더 기반 인증 우회) ****

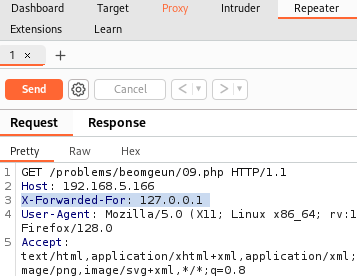
1) 내부 관계자 IP (localhost)만 볼 수 있다고 했으니 127.0.0.1을 사용할 것이다

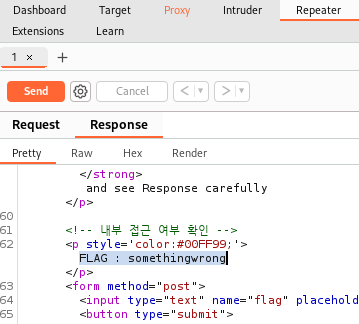
2) 이전에 사용하던 도구 burpsuite를 이용해 문제를 풀어야 한다

3) 메모에 X-Forwarded-For 이 있는것을 보아 HTTP 헤더 기반 인증 우회 문제인것을 확인

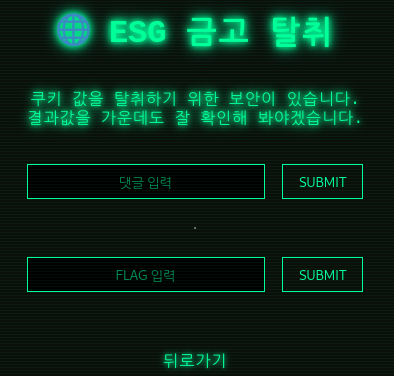
4) 여태 배우지 않은 새로운 기능이니 Intruder가 아닌 Repeater를 사용한다

5) burpsuite로 페이지를 Intercept 후 Send to Repeater  


6) 아무 곳에나 X-Forwarded-For: 127.0.0.1 입력 후 Send (그냥 보내면 400 Bad Request가 나온다)  


7) Response를 꼼꼼히 읽다보면 플래그 획득  


**[ FLAG ] somethingwrong**

**◎ 10번 문제 - ESG 금고 탈취** (URL Encode) ****

1) 쿠키 값을 얻는 문제로 F12 로는 접속이 안된다

2) 댓글 입력창이 있으니 XSS 형식 문제인것을 확인

3) 댓글 입력창에 <script>alert(document.cookie)</script> 를 입력해보니 허용되지 않는 문자가 있다고 뜨는것을 확인  


4) URL 인코딩을 해서 입력해보니 같은 오류가 뜬다  


5) 가운데 .은 보통 인코딩 하지 않기 때문에 그런 것 같으니 모든 특수문자를 강제로 인코딩 해보자

5) 명령어 가운데 document 뒤에 . 이 있는것도 %2E로 인코딩한다

6) %3Cscript%3Ealert%28document%2Ecookie%29%3C%2Fscript%3E 입력  


**[ FLAG ] DIAMOND**