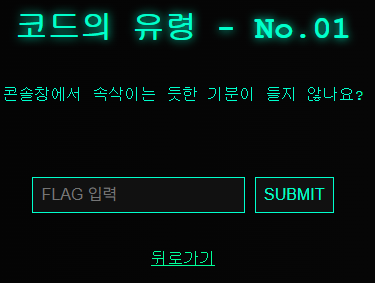
유령의집 메인 문제 목록

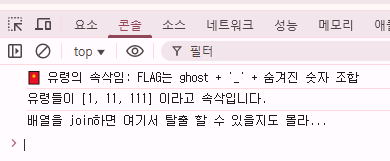


No.01



콘솔창에 뭔가가 있다는 힌트가 있는듯하다.

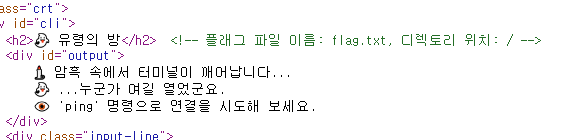
* F12 -> Console 창 확인

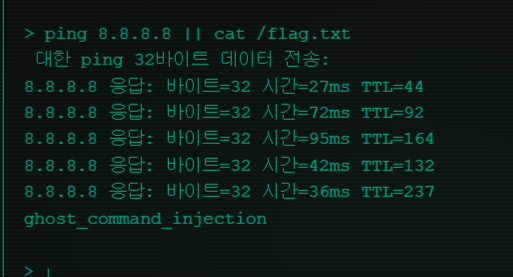


* FLAG는 ghost + \_ + 숫자 조합 확인
* Join 하라고 하였으니 플래그는 ghost\_1\_11\_111

No.02  
  
메인화면

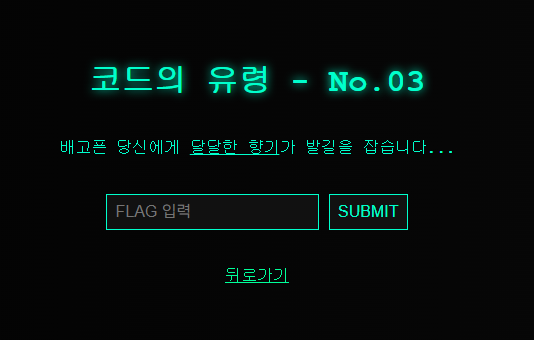
소스보기





Command injection 기법 사용으로 flag 추출완료

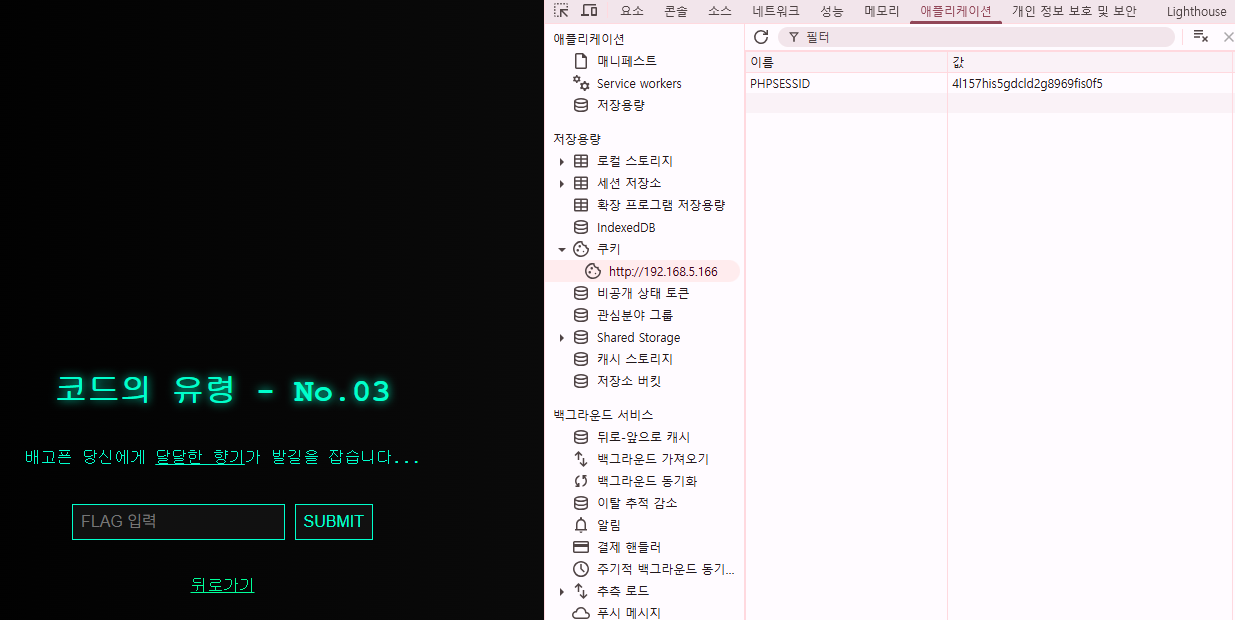
No.03

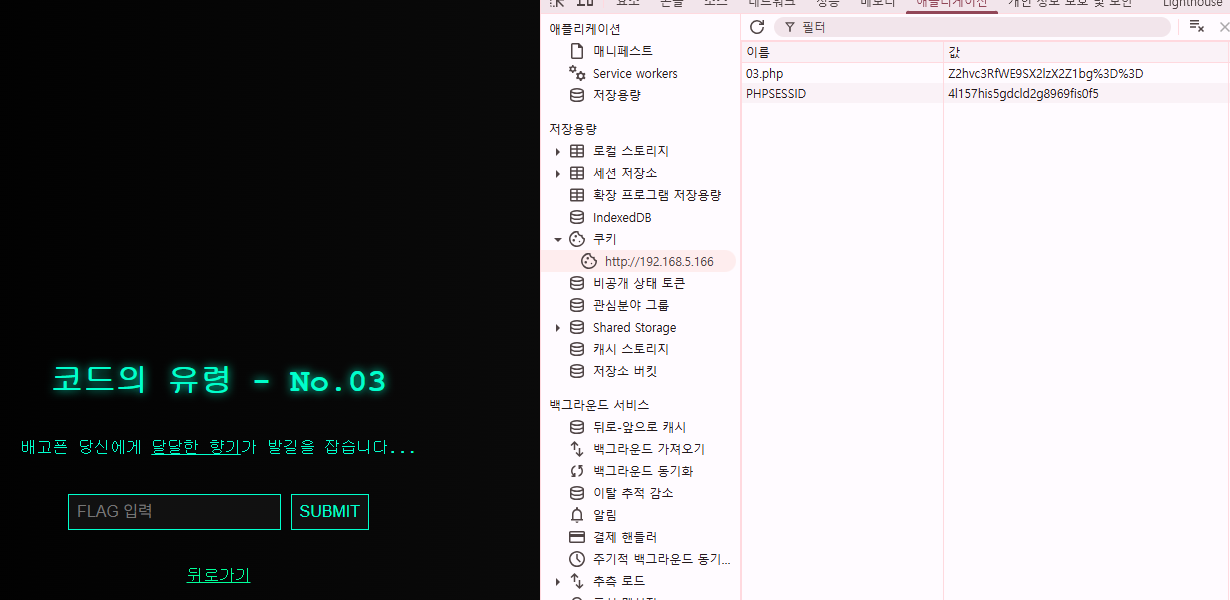


힌트를 얻기위해 소스보기 해보자.



소스를 보니 쿠키와 관련 있는 문제이며 03번 문제를 위한 cookie\_generator가 하이퍼링크가 걸려있는 것을 확인. 달달한 향기를 클릭해보자.

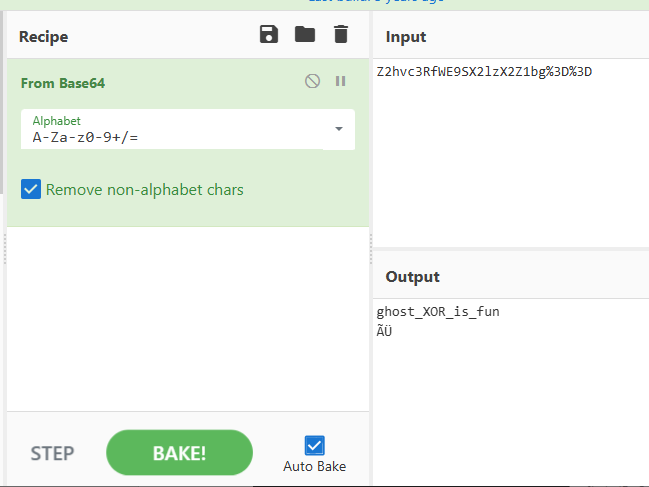




달달한 향기를 클릭 시 03.php 쿠키가 생성된 것을 확인

소스 및 콘솔창에서 힌트로 bake 하라고 되어있다.

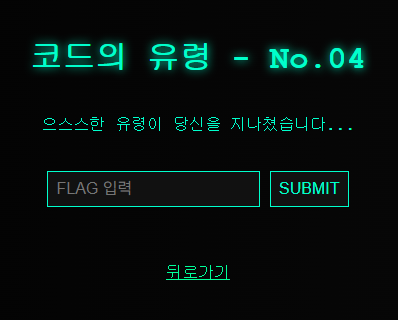
Bake 는 cyberchef와 연관되어있는거 같으니 이동해서 디코딩해보자



정상적으로 디코딩 되어 출력 되는 것으로 확인

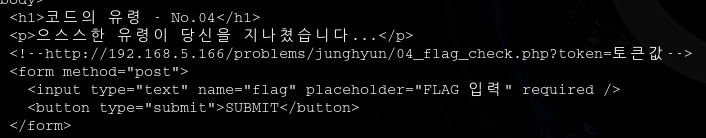
플래그는 ghost\_XOR\_is\_fun 으로 제출

No.04

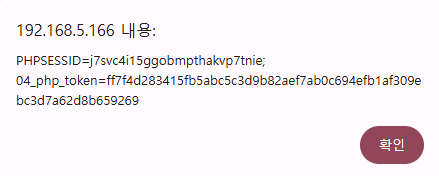


소스보기

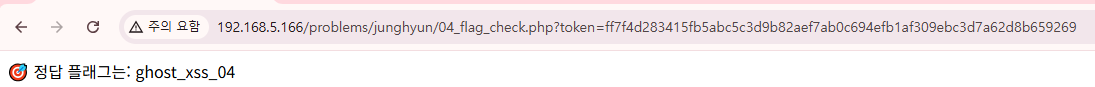




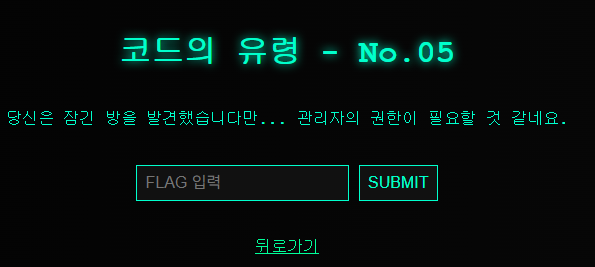
<http://192.168.5.166/problems/junghyun/04_flag_check.php?token=>토큰값이라는 힌트 발견

XSS 기법 시도  
<script>alert(document.cookie)</script>   


스크립트가 작동되며 토큰값이 보이는걸 확인 힌트대로 브라우저창에 입력해보자.



플래그 값을 얻을 수 있게 된다.

No.05  


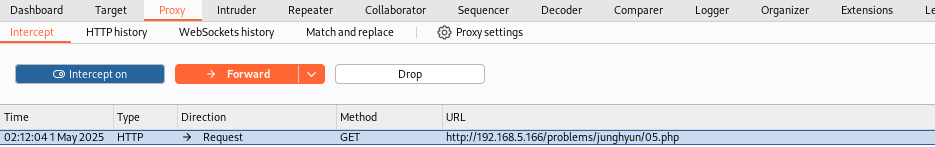
이 페이지에선 관리자의 권한이 필요하다고 한다..

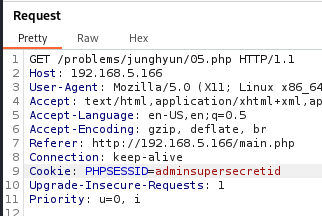
Session\_Hijacking 문제로 추측됨으로 관리자의 세션을 찾아보자.



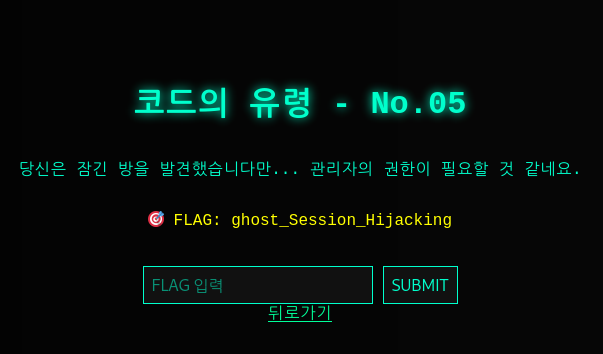
소스보기로 확인해보니 관리자가 남겨 놓은 주석에서 세션으로 추정되는 코드 발견

BurpSuite로 잡고 세션을 수정해서 관리자 권한으로 페이지를 확인해보자



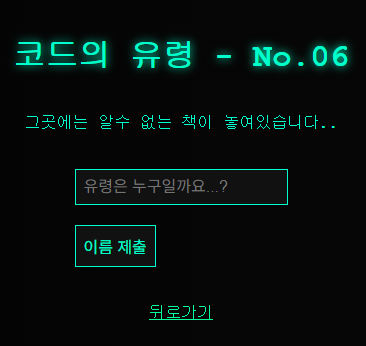


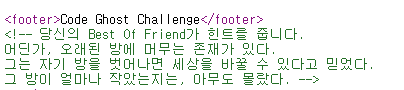
* 관리자 세션 수정 후 포워드



관리자의 권한을 획득하여 플래그를 발견

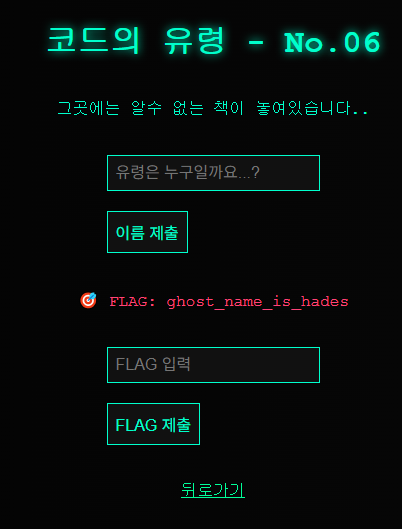
No.06



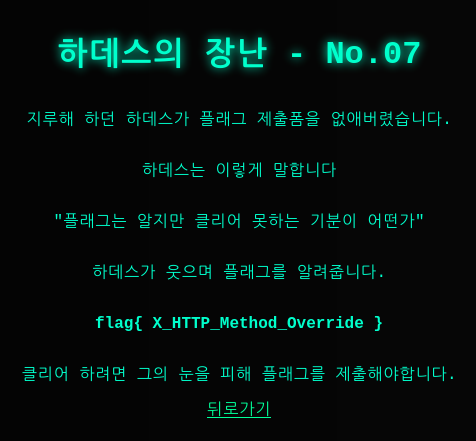


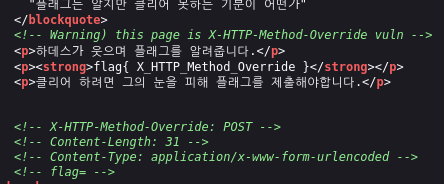
소스보기로 단서를 찾아보니 Best Of Friend(BOF) 가 힌트를 준다고 하며 방이 작고 벗어난다는 이야기를 강조하고있다. 이 단서로 BOF(버퍼오버플로우) 라는걸 추론

이름 제출칸에 아무값이나 계속 넣어서 버퍼오버플로우를 유도해보자.



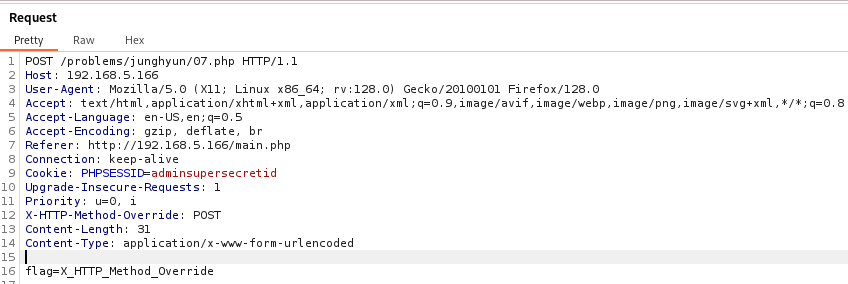
No.07





소스보기로 확인하니 X-HTTP-Method-Override 취약점이 있으며 헤더값에 어떻게 넣으면 취약점이 발생하는지 주석으로 적혀있는 것을 확인

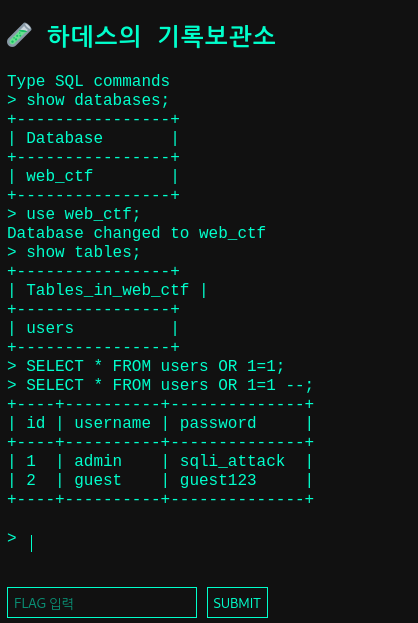




Burp suite 로 해당 페이지를 잡고 리퀘스트 주석 양식대로 수정 후 포워드해준다.

인터셉터를 종료하고 새로고침을 하면 메인화면으로 나온 걸 확인 할 수 있는데 문제를 클릭해보면 문제가 풀린것으로 확인 할 수 있다. (정상적으로 플래그값이 등록됨)

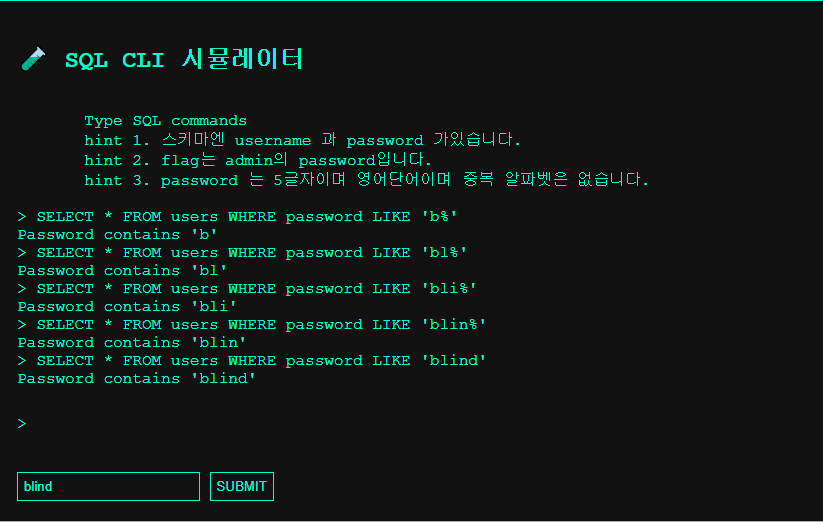
No.08



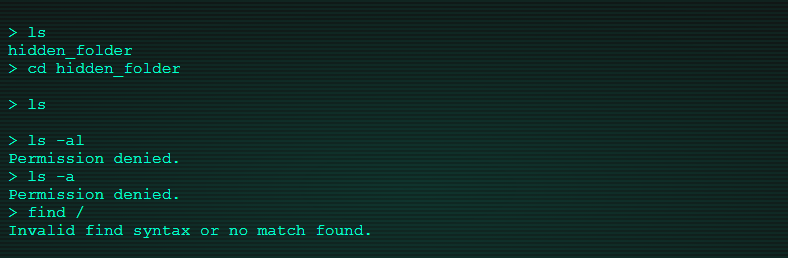
OR 1=1 – 로 SQLI 통해 비밀번호가 유출되는 것을 확인

FLAG 값에 비밀번호 입력

No.09



SQLI Blind 기법으로 비밀번호를 하나씩 추측하여 해킹한다.

No.10  


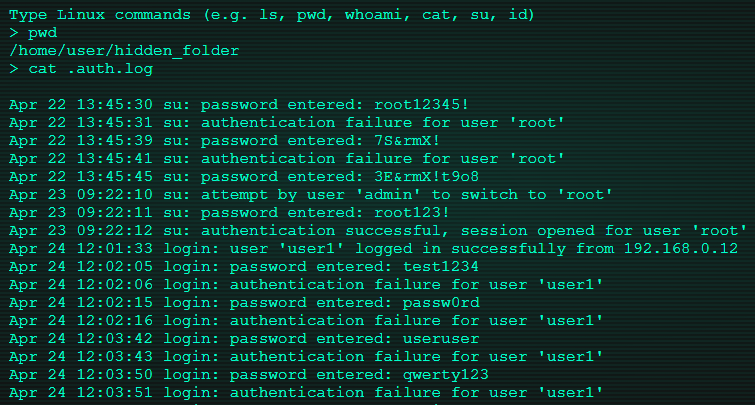
히든폴더에는 아무것도 보여지지않는다 숨김파일로는 뭔가가있는거같음.

find 명령어로 권한상승 방법을 찾아보자.

find 신텍스 가 맞지않다고 뜬다.. 문제가 로그 기록소니 허용되는 find 명령어를찾아보자

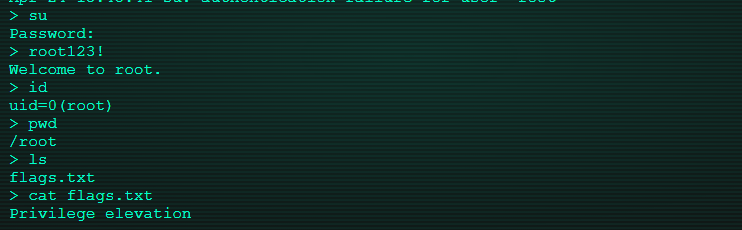
Find / -name \*.log  


로그로 끝나는 로그파일을 찾아보니 히든폴더에 .auth.log 가 숨겨져 있다는걸 확인



Cat 으로 확인해보니 로그 파일을 확인 할 수 있었다.

로그중 successful 떠있는 거 보니 위에 password로 입력한 root123!이 비밀번호인걸로 확인됨



루트권한을 얻으며 플레그를 획득할 수 있음.