|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 팀 명 | 어니언-조각치킨 | | | | | |
| 소 속 | 방공관제사령부 32전대 |  | |  | |  |
| 팀 원 | 정성조 |  | |  | |  |
| 접속 IP | 222.103.0.150 |  | |  | |  |
| 팀장  E-mail | cpstd\_hs@naver.com | | 팀장 전화번호 | | 010-7906-7715 | |

문 제 풀 이 보 고 서

**\* 핵심 풀이과정 및 플래그 획득 화면 캡처가 포함되어야 합니다.**

|  |  |  |  |
| --- | --- | --- | --- |
| 문 제 | | 분 야 | 점 수 |
| 1.1 Hidden Command | | Web | 미기입 |
| 첩보 활동 중 적국의 간부들이 사용하는 게시판을 발견했다.  해당 게시판에서 적국의 기밀 정보를 찾아내라.  - http://x.x.x.x  - front.py | | | |
| 풀이 절차 | 비밀번호 찾기 기능의 취약점을 이용하여  admin 권한을 획득해 비밀 게시물 내의 플래그를 획득함. | | |
| 정 답 | FLAG{N0t\_s3cur3\_4t\_411} | | |
| 풀 이 과 정 | | | |
| 문제에서 주어진 웹 페이지에 접속하면 다음과 같은 화면을 확인할 수  있습니다.    상단의 메뉴 중 Sign Up 메뉴를 통해 회원가입 후 로그인을 할 수  있습니다.  로그인 후 Board 메뉴에 접속해 게시판을 확인하면 아래와 같은 화면을 볼 수 있고, Admin이 작성한 Secret Document라는 제목의 게시물을  확인할 수 있습니다.    문제의 목표는 적국의 기밀 정보를 찾아내는 것이므로, Admin 권한을  획득해 Secret Document 게시물을 읽는 것이 문제의 목표로 보입니다.  주어진 front.py 소스코드를 분석해보면,    게시물을 읽을 때 게시물의 작성자의 username인 b.username과  현재 로그인한 사용자의 ID인 current\_user.username을 비교해  서로 같은 경우에만 게시물을 읽을 수 있습니다.  Admin이 작성한 Secret Document 게시물을 읽기 위해  current\_user.username을 조작할 수 있는 방법을 찾아야 합니다.  front.py에서 비밀번호 찾기 기능과 관련된 부분을 보면,    같은 username, email과 새로운 password로 새로운 계정을 DB에 추가하고, 기존 계정은 clear\_user 함수를 통해 삭제하는 것을 확인할 수 있습니다.  clear\_user 함수를 보면,    계정을 DB에서 삭제하는 것이 아니고, username, password, email을 모두 Admin 계정의 것으로 바꿔서 더 이상 해당 계정으로 접속이 불가능하도록 막는 것을 확인할 수 있습니다.  만약 이미 user라는 계정으로 로그인을 한 상태에서 user 계정의 비밀번호 찾기 기능을 수행하면 user 계정의 username, password, email이  Admin 계정의 것으로 바뀌게 됩니다.  이후 Secret Document 게시물을 읽으면 current\_user.username 이 Admin이므로 게시물을 읽을 수 있습니다.  <공격 과정>   1. hyomin 계정으로 로그인      1. /forget 페이지에 접속해 hyomin 계정의 비밀번호 찾기 기능 수행 (clear\_user 함수에 의해 current\_user.username이 Admin으로 변경)      1. /board 페이지에 접속해 Secret Document 게시물 확인   위와 같은 과정을 통해 Admin 권한을 획득하고,  아래와 같이 Secret Document 게시물을 확인할 수 있습니다.    플래그는 FLAG{N0t\_s3cur3\_4t\_411}입니다. | | | |