The Hacking Championship Junior 2020

Write-Up

|  |  |  |  |
| --- | --- | --- | --- |
| 팀 이름 | 구경만할게요 | 팀원 | 이경준, 최승혁, 황선우, 황영진 |
| 문제 | 시나리오 02 | 날짜 | 2020.11.25 |
| 정답 FLAG | HC{a8767eea29a020502a8be802e7f57f46} | | |
| 풀이과정 | /notice/fileDownloadAction.jsp에서 LFI 취약점이 발생해서 소스코드를 릭 할 수 있었다.    코드를 보면, 쿼리 실행 후에 필터링이 이루어지고, 필터링이 이루어지더라도 클라이언트 측에서만 차단이 일어날 뿐 그대로 결과가 반환된다는 것을 알 수 있다.  따라서 일반적인 Blind SQL injection과 같은 방법으로 문제를 해결할 수 있는데…  직접 짠 스크립트도 사용할 수 없다는 조건 때문에 일일이 수작업으로 값을 얻어야 했다.    데이터 베이스 이름을 알아오는 페이로드. 500 일 때는 if문이 실패했을 때고, 200일때는 조건이 만족하는 것으로 결과를 구분했다. 알아낸 데이터베이스의 이름은 `hack` 이었다.    이렇게 500이 나오면 조건이 일치하지 않는다는 것을 알 수 있다. 위 페이로드는 테이블 이름을 알아내는 데 사용했다. 알아낸 테이블의 이름은,  `enquire`, `notice`, `user` 였다.  컬럼 이름은 게싱으로 풀었는데, 다행히 맞았다. `user` 테이블 아래에 `id`와 `pw`라는 컬럼이 있었다.    이렇게 한자리씩 구했다.  1~10  HC{a8767ee  11~19  a29a02050  20~36  2a8be802e7f57f46}  합치면 HC{a8767eea29a020502a8be802e7f57f46} | | |

지금까지 작성한 Write-Up의 모든 내용에 대한 책임은 참가자에게 있으며, 미제출 및 부정 행위에 대해 실격 또는 불이익이 있을 수 있습니다.