The Hacking Championship Junior 2020

Write-Up

|  |  |  |  |
| --- | --- | --- | --- |
| 팀 이름 | 구경만할게요 | 팀원 | 이경준, 최승혁, 황선우, 황영진 |
| 문제 | 시나리오 03 | 날짜 | 2020.11.25 |
| 정답 FLAG | HC{bb6a347659f4e6f8accf6ae29a171d44} | | |
| 풀이과정 | /notice/fileDownloadAction.jsp에서 LFI 취약점이 발생해서 소스코드를 릭 할 수 있었다.    파일 업로드가 가능한 지점은 세가지 포인트가 있었는데(notice, enquire, cloud) 이 중 cloud에 업로드하는 지점에서만 jsp 코드 업로드가 가능했다.    추가로, 코드에는 getRealPath 함수를 이용해 업로드 디렉토리를 찾는 코드가 있었다. JSP 애플리케이션의 실행주소는 `/yess`부터이니, `getRealPath(“/cloud/”)`가 가리키는 주소는 `/yess/cloud/`라고 예상했다. 따라서 jsp 웹쉘을 업로드할 수 있었고, 이를 `http://211.170.162.67/yess/cloud/파일명`으로 접속해서 실행할 수 있다.  웹쉘은 깃허브에 있는 한 코드를 이용했다. (<https://github.com/tennc/webshell/blob/master/fuzzdb-webshell/jsp/cmd.jsp>)    이렇게 jsp 웹쉘을 업로드했다.    웹쉘에 접속해서 플래그 파일을 읽을 수 있었다. | | |

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