1-day 취약점 분석 문제

Target : CVE-2023-30145

1. 해당 취약점이 발생한 프로그램과 취약 버전(범위), 패치버전을 서술하시오

Camaleon CMS

v2.7.0 이전, v2.7.4 에서 해결됨

1. RCE란 무엇이고, SSTI 취약점이 RCE로 이어질 수 있는 이유를 서술하시오

rce란 원격에서 임의 코드를 실행할 수 있는 취약점

템플릿 엔진 특성상 조건문, 반복문 구현에 code evaluate 함수를 사용하는 경우가 많기 때문이다

1. CVE-2023-30145 관련 공개된 poc와 정보들을 바탕으로, /home/flag 파일의 내용을 읽어오는 페이로드를 작성하시오( 파라메터 고려없이, 취약한 인자에 전달할 페이로드만 포함하여 작성하면, 어떤 형태이던 정답처리 ex: {{7\*7}} )

<%= File.open('/home/flag').read %>

1. CVE-2023-30145의 CVSS 점수를 서술하고, 해당 점수의 근거를 바탕으로 취약점 파급력을 설명하여라

9.8

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

위 내용 포함 시 정답