

Vulnerability Discovery_11

Target

: <http://124.60.4.10:6662/download.php>

Payload

: 버퍼 스위트를 사용, 리피터를 통해 파일 경로를 ../../../../etc/passwd로 수정하여 Request 후 etc/passwd 파일 다운로드

Impact

: 서버 내 파일을 강제 다운로드 하여 계정 정보 및 DB 정보를 담은 민감한 파일 다운로드 가능

