|  |
| --- |
| 『WhiteHat School 1기』  **취약점 보고서**  (자체 제작 웹 서비스: OVERLOAD) |

2023.12.31

Team: 과부화

1) 파일 경로 조작

|  |  |  |  |
| --- | --- | --- | --- |
| **구분** | **상세 내용** | | |
| **취약점 명** | · Path Manipulatinon / Path Traversal Vulnerability | **위험도** | **상** |
| **취약점 내용** | · 이 취약점은 제품 상세 페이지에 존재하는 리뷰 기능에 이미지를 업로드 했을 시, 업로드한 이미지 파일 명이 그대로 올라가는 것을 통해 업로드 파일의 경로를 조작할 수 있습니다. | | |
| **발생가능 위험정보** | · 파일 경로를 조작하여 허가되지 않은 디렉터리나 파일에 액세스하여 중요한 정보를 읽거나 수정할 수 있습니다.  · 실행 가능한 파일을 삽입하여 시스템 명령을 실행할 수 있습니다.  · 시스템의 안정성과 무결성이 손상될 수 있습니다. | | |
| **검증관련**  **상세정보** | · 이하는 업로드가 된 이미지의 파일 명이 그대로 보이는 모습입니다.    *프록시를 통해 파일 경로를 직접 지정하는 모습 [1-1]*      *이미지 파일의 경로가 기존 경로의 상위 폴더에 업로드 되어 있는 모습 [1-2]* | | |
| **조치방안** | · 파일이 저장되는 경로를 절대 경로가 아닌 상대 경로를 사용하는 것을 추천합니다.  · 외부이 입력이 파일명인 경우에는 경로순회 공격의 위험이 있는 문자(/, ＼, ..) 등을 제거할 수 있는 필터를 사용하는 것을 추천합니다. | | |