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

2023.12.31

Team: 과부화

1) Session 값을 이용한 로그인

|  |  |  |  |
| --- | --- | --- | --- |
| **구분** | **상세 내용** | | |
| **취약점 명** | · Session Hijacking | **위험도** | **상** |
| **취약점 내용** | · 이 취약점은 로그인 상태에서 남아있는 세션 값을 로그아웃인 상태에서 직접 Session 값을 만들어 대입하였을 때 로그인 과정 없이 계정에 접근할 수 있습니다. 동일한 계정으로 다시 로그인을 할 때마다 세션 값이 바뀌게 되는데 로그아웃을 했을 시 세션 값이 무효화가 되지 않아 바뀐 세션 값이 아닌 이전의 세션 값을 이용해도 로그인이 되는 것을 확인하였습니다. | | |
| **발생가능 위험정보** | · 로그인 상태에서 쉽게 세션 값이 확인할 수 있기에, 네트워크를 감시하는 공격자가 세션 값을 가로채서 회원 권한을 얻고 회원 정보를 쉽게 탈취할 수 있습니다. | | |
| **검증관련**  **상세정보** | · 이하는 개발자 도구(F12)에서 세션 값을 획득한 모습입니다.  획득한 세션 값을 로그아웃 상태에서 재사용했을 시, 세션 값을 획득한 계정으로  다시 로그인이 되는 모습입니다.    *세션 값 획득 [1-1]*    *세션 값 재사용 [1-2]* | | |
| **조치방안** | · 세션 ID를 안전하게 저장하고 전송하기 위해 암호화 기술을 사용하는 것을 추천합니다.  · 사용자가 로그아웃을 할 때마다 서버에서 기존의 세션 정보를 삭제하는 기능을 구현하는 것을 추천합니다. | | |