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

2023.12.28

Team: 과부화

1) 스크립트 삽입을 통한 XSS

|  |  |  |  |
| --- | --- | --- | --- |
| **구분** | **상세 내용** | | |
| **취약점 명** | · XSS(Cross-Site Scripting) | **위험도** | **상** |
| **취약점 내용** | · 이 취약점은 문의하기 게시판에 스크립트를 삽입해 공격자의 악의적인 스크립트가 실행될 수 있습니다. 악성 스크립트를 통해서 토큰의 정보를 탈취하거나 사용자의 개인정보를 탈취할 수 있습니다. 또한 스크립트를 통해 사이트의 UI를 바꿀 수 있습니다. | | |
| **발생가능 위험정보** | · 문의하기 내용에 포함되는 스크립트 및 HTML 태그가 그대로 실행되기 때문에 이로 인한 개인정보 유출의 위험이 있습니다.  · 악성 스크립트를 통해 피싱사이트의 연결 등 2차 피해가 생길 위험이 있습니다.  · 스크립트를 통해 UI를 임의로 조작함으로써, 사용자가 부주의하게 오인하거나 실수할 수 있는 상황을 유도할 수 있습니다. | | |
| **검증관련**  **상세정보** | · 이하는 삽입된 스크립트와 해당 스크립트가 실행되는 모습입니다.  스크립트에 대한 필터링이 없어 임의의 스크립트가 실행됩니다.    *삽입된 스크립트 [1-1]*    *스크립트 실행 화면 [1-2]*  · 이하는 스크립트 삽입을 통해 UI를 조작한 모습입니다.  사용자가 조작된 UI를 오인하여 해당 버튼을 클릭 시, 피싱사이트로 연결이 됩니다.   |  |  | | --- | --- | | **변경 전** | **변경 후 후** | |  |  |   *UI 변경 전/후 [2-1]*    *삽입된 스크립트 [2-2]*    *버튼 클릭 후, 스크립트가 실행된 화면 [2-3]* | | |
| **조치방안** | · 특수문자의 치환이나 측정 단어의 필터 등, 사용자로부터 받는 문자에 대한 이스케이핑을 하는 것을 추천합니다.  · CSP를 설정하여 허용된 리소스만을 로드되게 하는 것을 추천합니다.. | | |