사이버보안연구실

작성 : 이예인

작성일자 : 2024/10/02

<table>
<tr><td colspan="4">Cross-site scripting (XSS) attacks and mitigation: A survey</td></tr>
<tr><td>저자</td><td>Germán E. Rodríguez</td><td>저널</td><td>Computer Networks</td></tr>
<tr><td colspan="4">리뷰</td></tr>
<tr><td>요약</td><td colspan="3">● 문제점
■ Cisco의 2018년 연례 보안 보고서에 따르면, 모든 분석된 웹 애플리케이션에는 최소 하나의 취약점이 존재한다.
■ XSS는 전체 공격 시도의 40%를 차지하는 가장 흔한 공격 기법이다.
■ 웹 공격은 점점 더 빈번하고 정교해져 사용자의 정보 유출 및 시스템 제어에 악용될 가능성이 있다.
● 해결하고자 하는 문제
■ XSS 공격을 탐지하고 완화하기 위해 사용된 다양한 방법과 도구를 연구하는 것을 목표로 함
■ 인공지능을 활용한 XSS 공격 탐지 연구를 보완하는데 기여하고자함
■ XSS 공격 탐지 및 완화에 대한 연구자들에게 유용한 가이드 제공</td></tr>
<tr><td>강점</td><td colspan="3">● Static, Dynamic, Hybrid로 XSS 방어기법문서 분석
● XSS 방어 Client, Server, Hybrid으로 방어 위치 분류</td></tr>
<tr><td>약점</td><td colspan="3">● 2020년 논문이다보니, 20년대 최신 논문에 대한 분석이 없고 19년까지의 문서를 분석함</td></tr>
<tr><td>아이디어</td><td colspan="3">● 이 논문을 기준으로는 인공지능을 통한 XSS 방어가 부족하다지만, 24년 현재를 기준으로 어떤지 알아볼 필요있음</td></tr>
<tr><td>배운점</td><td colspan="3">● Reflected, Persistent, DOM XSS별 공격방법 시나리오
● 쿠키의 사용목적과 XSS 공격에서 쿠키 악용되는 방법에 대해 알게 됨
● XSS는 잘못된 구현이나 다양한 입력 경로를 통한 공격 가능성 때문에 방어가 까다롭기 때문에, 38%의 낮은 취약점 해결비율(수정률)을 보임</td></tr>
</table>

용어 정리

Remediation rate : 발견된 특정 보안 취약점이나 문제에 대해 해결 조치가 완료된 비율