모의해킹 보고서

1. 개요

https://demo.testfire.net 에 대한 모의해킹 결과 보고서이다.
해당 사이트는 IBM에서 제공하는 온라인 뱅킹 데모 사이트이다.
이 사이트가 중요하게 여기는 것은 기밀성이라고 생각한다. 고객의 계좌정보, 개인정보 등이 유출되지 않도록 하는 것이 중심이다.

2. 목표(공격 시나리오)

악성 스크립트를 실행시켜 접속한 사용자의 정보를 수집한다.

3. 사용 도구

OWASP-ZAP

4. 발견된 취약점

OWASP-ZAP의 spider 기능을 통해 모든 URL을 찾고, active scan을 한 결과
(1) Cross Site Scripting (Reflected) 2건
(2) Path Traversal 2건

5. 위험도/우선도

High - Cross Site Scripting, Path Traversal

6. 공격 활동

Cross Site Scripting 취약점 공격
(1) search.jsp - 매개변수 : query
(2) sendFeedback - 매개변수 : name
각 매개변수에 스크립트 삽입하여 공격 성공 여부 확인 (스크린샷 참조)

Path Traversal 취약점 공격
(1) https://demo.testfire.net/index.jsp?content=../WEB-INF/web.xml 입력 시
웹페이지에 파일 내용 출력됨. (스크린샷 참조)

7. 취약점 보완 방법

Cross Site Scripting 취약점 보완
(1) 악성 스크립트를 실행할 수 없도록 특수문자를 제한 (정규식)
(2) XssAttackFilter 클래스를 적용하여 특수문자를 치환하여 반환

Path Traversal 취약점 보완
(1) 상대 경로 (.., /, \\) 문자열을 검증하는 로직 추가
(2) 파라미터로 파일명을 넘기지 않고 임시 디렉터리를 활용하는 등 업로드 경로를 노출하지 않도록 한다.