모바일 웹 2.0 환경의 보안취약점 및 대응방안에 관한 연구

김완주° 문영주 이수진
국방대학교
sizipus1@gmail.com, ans74@naver.com, cyberkma@kndu.ac.kr

A Study on the Security Vulnerability and Countermeasure in the Mobile Web 2.0 Environments

Wanju Kim° Youngju Moon Soojin Lee
Korea National Defense University

1. 서 론

웹 기술은 그 특유의 단순함과 폭넓은 확장성으로 다양한 이기종 환경에 널리 적용되어 왔고, 인터넷 상의 다양한 자원들을 사용자가 손쉽게 접근하여 사용할 수 있도록 함으로써 이제는 단순한 검색환경 제공수준을 넘어 생활도구로서의 역할을 수행하고 있다. 그리고, 최근 와이브로(WiBro), HSDPA 등 이동통신 기술의 발달과 모바일 기기의 성능 향상으로 인해 웹 기술은 유선망 환경을 벗어나 모바일 환경으로 진화하고 있다. 또한 모바일 단말기술 및 무선네트워크 기반구조, 웹 기술의 융합은 '모바일 웹 2.0' 이라는 새로운 환경을 탄생하게 하였으며 기존의 웹 환경을 뛰어넘는 획기적인 모바일 플랫폼으로 주목받고 있다[1][2].

이러한 모바일 웹 2.0 환경은 기술의 발전과 더불어 사용자의 요구사항을 구현하는 도구로서 우리사회 전반에 깊숙이 관여하게 되었다. 특히 이동성(Mobility)과 개인화(Personalization)를 통해 모바일 전자결재, 위치기반 서비스, 전자투표, 이동형 멀티미디어기기 등의 서비스로 활용되어 지고 있다. 하지만 모바일 환경이 확대되면서 개인정보 유출, 개인 프라이버시 침해, 해킹, 바이러스 등 역기능적 피해 또한 증가되고 있다. 실제로 유선환경에서의 악의적인 보안위협들이 모바일 환경에서도 나타나고 있으며, 앞으로 더욱 확대될 것으로 전망된다.

2. 모바일 웹 2.0 환경과 보안 취약점

최근 웹 2.0의 특징으로 거론되는 '플랫폼으로서의 웹'을 기반으로 하여 모바일 환경에서도 기존의 모바일 웹으로부터 '모바일 웹 2.0'에 대한 다양한 노력들이 시작되었다. 다양한 XML 어플리케이션, 웹서비스, 시맨틱 웹 어플리케이션 등과 같은 차세대 웹 기술과 특징들을 수용하면서 새로운 변화를 시도하고 있다. 이러한 모바일 웹 2.0 환경의 진화와 표준화는 기존의 웹 환경을 모바일 환경에서 모두 수용할 수 있는 방향으로 진행되고 있다. 이는 기존의 웹 환경의 보안취약점이 모바일 환경으로 전이 되고 있음을 의미하며, 또한 다양한 디바이스와 접속 환경의 표준화는 악성 프로그램의 활동속도 증가와 파급효과에 큰 영향을 줄 것으로 예상된다.

기존 웹 어플리케이션 보안 취약점은 모바일 웹 2.0 환경에서도 대부분은 적용되며 실제로 모바일 단말기를 대상으로 하는 악성코드들은 2004년 Cabir를 시작으로 하여 2007년 4월까지 350개 이상이 발견되어 모바일 웹 환경이 해커들에게 주요 공격 대상이 되고 있음을 알 수 있다[3].

2007년 OWASP(The Open Web Application Security Project) 에서 발표한 웹 어플리케이션 프로그램 10대 취약점[4] 중 모바일 웹 환경에서도 핵심적인 위협요소로 작용 될 수 있을 것으로 예상되는 취약점은 XSS(Cross Site Scripting), Injection Flaws, Malicious File Execution이 있다.

3. 실험 및 결과

본 논문에서는 기존의 유선망 웹 환경의 보안취약 요인이 모바일 웹 2.0 환경에서도 동일하게 적용될 수 있음을 에뮬레이터 기반과 실장비 기반의 실험을 통해 확인한다. 실험의 진행은 SQL Injection 공격을 통해 모바일 웹 2.0 환경에서 모바일 단말기가 취약점 공격도구로서의 역할을 수행할 수 있는지를 확인하고 XSS 공격을 통해 공격대상이 될 수 있음을 확인한다.

실험 환경은 서버는 가상머신(VMware)상에서 동작하도록 구축하였으며 IIS, MS SQL, ASP를 이용하여 제작된 웹게시판을 대상으로 SQL Injection 취약점 및 XSS 취약점을 가지도록 제작하였다. 클라이언트 환경의 구성은 마이크로소프트사의 모바일운영체제 3종과 Symbian사의 Symbian S60 3.0, ACCESS사의 팜OS 5.4버전의 에뮬레이터를 이용하였으며 실 장비 기반의 테스트는 삼성에서 제작한 스마트폰 SCH-M620 (Samsung Blackjack)을 이용하였다. 실험 결과는 <표 1>과 같다.

<표 1> 모바일 웹 2.0 환경의 보안취약점 실험 결과

구 분		SQL Injection	XSS	Malicious File Execution
에뮬레이터	Windows CE 5.0	○	×	○
	WM5.0 PPC	○	×	○
	WM5.0 SP	○	×	○
	Symbian S60	○	×	○
	Palm OS 5.4 (NetFront Browser)	○ (○)	× (○)	○ (○)
실장비 (SCH-M620)	Mobile IE	○	○	○
	Opera	○	×	○

4. 대응방안

모바일 웹 어플리케이션의 보안 취약점은 기존의 웹 어플리케이션이 가지는 취약요소를 계승한다. 따라서 기존 웹 어플리케이션에서 적용하였던 보안 고려요소를 모바일 웹 어플리케이션에서도 반드시 적용하여야 하며 모바일 환경의 특성에 적합하도록 수정 · 보완되어야 한다.

모바일 웹 어플리케이션 설계시 다음 사항을 고려하여야 한다. 첫째 사용자의 입력 값과 출력 값을 검증하는 것이다. 시스템의 사용자 입력 값과 출력 값에는 제한된 범위내의 문자들만 허용하고 다른 데이터는 차단시켜야 한다. 둘째 오류 발생시 안전하게 처리를 수행하여야 한다. 버퍼 오버플로우 공격과 같이 메모리 영역의 한계를 초과 한 경우에도 안전하게 처리된다면 공격자로부터 안전할 것이다. 셋째 보안시스템을 사용자가 활용할 수 있도록 간결하게 유지하여야 한다. 넷째 개발시 신뢰할 수 있는 타인의 라이브러리나 컴포넌트를 활용하여야 하며 마지막으로 시스템은 작업 수행에 필요한 최소한의 권한을 가지도록 설계되어야 한다. 또한, 웹 서버 관리자는 주기적으로 취약점 스캐너와 수작업에 의한 취약점 점검방법을 이용해서 웹 서비스의 취약점을 점검하고 발견된 취약점은 제거해야 한다. 또한 제조사에서 제공하는 보안취약점에 대한 패치를 즉시 적용한다. 사용자는 모바일 웹 사이트 방문시 메일이나 웹 문서에 포함된 링크를 클릭하지 말고, 직접 브라우저 주소창에 URL을 입력하고, 브라우저의 최신 보안패치를 적용하도록 해야 한다.

5. 결 론

국내에는 아직까지 모바일 환경을 통한 공격 사례가 발견되고 있지는 않지만, 본 논문에서는 기존의 웹 어플리케이션 보안 취약점을 분석하여 모바일 환경에서도 중대한 위협요소로 작용할 수 있는 취약점과 공격 시나리오를 제시하였다. 또한 제시된 취약점을 에뮬레이터와 실 장비 기반의 실험을 통해 SQL Injection 이나 XSS 등 유선망 환경의 웹 공격기법이 모바일 환경에 적용될 수 있음을 확인 하였으며, 특히 SQL Injection 공격 실험을 통해 모바일 웹 2.0 환경이 공격도구가 XSS 공격 실험을 통해서 공격의 대상이 될 수 있음을 확인하였다. 이는 모바일 웹 2.0 환경으로의 변화에 따라 보안취약점도 함께 변화할 수 있다는 것을 증명하였고 이러한 연구결과는 모바일 웹 2.0 환경이 우리 생활에 적용 되었을때 발생될 수 있는 보안문제를 해결하는 중요한 기초자료가 될 것이다.

향후에는 모바일 웹 브라우저의 성능차이에 따른 보안 취약요인의 차이를 분석하고 다양한 공격 시나리오에 대한 분석을 통해 모바일 웹 2.0 환경에 최적화된 대응방안에 대한 연구가 추가적으로 이루어져야 할 것이다.

참고문헌

[1] O'Reilly, T."What is Web 2.0?", http://www.oreillynet.com, 2005.
[2] Robert M, Katarina S. "Mobile Web 2.0", 20thBledeConference eMergence:METPI, 2007. 6
[3] http://www.f-secure.com
[4] OWASP, "THE TEN MOST CRITICAL WEB APPLICATION SECURITY VULNERABILITIES", http://www. owasp.org, pp. 4, 2007.