최신 웹 사이트의 취약점 사례 탐구 및 웹 보안 사이트 설계

정유진*, 김재룡**, 이상무***, 한도현****, 박성환*****
*가천대학교 컴퓨터공학과
**인천대학교 컴퓨터공학부
***인천대학교 컴퓨터공학부
****인천대학교 컴퓨터공학부
*****DGIST 기초학부
e-mail : intjyj@naver.com

Exploring the latest web site vulnerability cases and Designing Web security site

You Jin Jung *, Jae Ryong Kim**, Sang Mu Lee***, Do Hyeon Han****, Seong hwan Park*****
*Dept. of Computer Engineering, Gachon University
**Dept. of Computer Engineering, Incheon national University
*** Dept. of Computer Engineering, Incheon national University
**** Dept. of Computer Engineering, Incheon national University
*****College of transdisciplinary studies, DGIST

요 약

세계적인 웹 어플리케이션 취약점을 다루는 OWASP(The Open Web Application Security Project) TOP 10 [1]에 따르면 빈도가 높고 영향이 큰 취약점들은 모두 철저한 웹 보안 코드를 작성하면 어느 정도 예방할 수 있다는 결론이 나왔다. 이에 따라 최근 국내에서 일어난 웹 사이트의 취약점 사례를 알아보고 그 대응법에 대하여 분석한 후, 직접 개발한 웹 사이트에 웹 보안 코드를 적용할 수 있도록 하였다. 또한, 소프트웨어 공학자를 위한 java 시큐어코딩 가이드를 숙지하여 웹 개발 시 보안 유지를 강화하였다.

1. 서론

2017 년도에 발표된 OWASP TOP 10 에서 인젝션(Injection), 인증 및 세션 관리 취약점(Broken Authentication and Session Management), 크로스 사이트 스크립팅(Cross-Site Scripting) 이 3 가지 분야를 포함한 여러 취약점은 지난 2013 년의 발표 결과와 다름없이 순위권에 안착하였다. 이처럼 웹 개발자들을 괴롭히는 고질적인 공격에 대비하여 웹 보안 전문가의 필요성이 절실하지만 무분별한 웹 사이트의 개발로 인해 보안 실정은 나아지지 않는 것이 현실이다.

본 연구는 최신 국내 웹 사이트의 해킹 사례 및 대응법을 알아보고, 실제 웹 개발 기간 동안 미리 숙지한 이전 사례들을 바탕으로 웹 해킹을 최소화 할 수 있는 개발을 진행하였다. 또한, 행정안전부에서 제공한 SW 개발 보안 시큐어코딩 가이드 [2]를 적극 활용하여 소프트웨어 보안 약점 기준에 어긋나지 않는 웹 사이트 개발을 목표로 하였다.

2. 최신 국내 웹 사이트의 해킹 사례 및 문제점

최근 국내 홈페이지의 해킹은 악성코드 유포 현황을 통하여 증가하고 있고, SQL injection 취약점 공격이 빈번하게 일어나고 있다. SQL injection 공격은 DB 를 공격하여 정보를 탈취하는 대표적인 웹 해킹 공격으로, 웹 내 사용자 입력 값에 필터링이 제대로 적용되어 있지 않을 때에 발생한다.

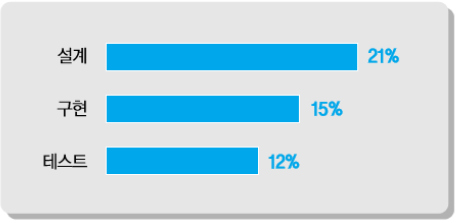
실제 우리가 뉴스에서 흔히 접할 수 있는 대기업의 고객 개인정보 유출 사례는 주로 서버 유지보수를 맡고 있는 직원의 노트북을 악성코드에 감염시킴으로써 일어나는 경우가 태반이다. 이러한 경우 전산망 마비가 오면서 서버가 파괴된다. 이 외에도, 해킹 파일 업로드 취약점을 이용해 고객의 비밀번호를 비암호화하는 등의 여러가지 수법이 있다. 몇 십 또는 몇 백만 명의 사용자가 개인정보 유출 위험에 무방비 상태로 노출되어 있는 지금, 웹 DB 관리를 용이하게 하기 위

해서는 개발 시점부터 개발자가 '내가 이 웹의 사용자다.'라는 마인드를 갖고 개발을 철저히 하는 것이 중요하다.

<표 1> 최근 개인 정보 유출 사례(2014)

날짜		사고내용
2014년	1월	국민/신한/하나/우리은행카드사 연계은행, 1,500만 명 개인정보 유출
	2월	대한의사협회/의사협회/한의사협회, 홈페이지 해킹, 중 15만명 개인정보 유출
	2월	KT홈페이지 해킹, 1,200만명 개인정보 유출
	3월	SKT/LG U+ 420만 건,금융기관 11곳 100만 건, 여행사/쇼핑몰 187만 건 등 1,230만 명의 정보 유출
	3월	국토교통부, 자동차민원 관리사업자 포털, 2,000만 명 개인정보 유출
	3월	티켓몬스터 등 225개 사이트 해킹, 1,700만 명 개인정보 유출
	3월	현대기아자동차, 홈페이지 해킹, 8만 명의 개인정보 유출
	3월	AK프라자, 내부직원에 의해 20만 명의 고객 정보 유출
	3월	파인리조트, 홈페이지 해킹, 19만 명 고객 정보 유출
	4월	KB국민/NH농협/롯데카드 3사 2차 유출, 총 17만명 개인정보 유출
	4월	포스단말기 해킹으로 광주은행/신한카드/농협카드/국민카드/IBK/씨티은행 등 10개 은행에서 20만 명의 금융정보 유출
	4월	KDB생명, 고객 상담 내용 1만 건의 녹취 파일이 웹사이트에 공개
	4월	천재교육, 350만 명의 개인정보유출, 서버해킹으로 추정
	5월	토니모리, 홈페이지를 통해 50만 명의 회원 개인정보 유출
	10월	판도라TV, 해커가 745만 명의 개인정보 유출, 11만 건의 개인정보 외부 유출
	10월	최근 3년간 공무원이 국가망으로 연예인 정보를 1,122회 엿봄

기존의 국내 웹 사이트는 시스템에 추가적으로 웹 방화벽, IDS/IPS 등의 보안장비를 도입하는 방식으로 웹을 관리하는 것이 보편적이다. 그러나 이러한 방식은 시스템 설계 및 개발 단계의 편의성에 치중한 나머지, 초기에 정보보호에 대하여 고려하지 않은 경우를 방지하는 차선책일 뿐이다. 이미 구축되어 있는 웹 서버의 취약점을 보완하는 것은 비용적인 면에서 큰 타격이 아닐 수 없다. 따라서, 웹 개발자들은 웹 설계 단계에서부터 시간을 들여 웹 보안을 고려해야 할 의무가 있는 것이다. 실제 개발 단계에서 정보보호 사항을 충분히 반영한다면 웹 유지보수 비용이 훨씬 절감된다는 결과가 있다. [3]



(그림 1) 개발 단계별 비용 절감 효과

3. 정보보호를 고려한 웹 사이트의 필요성 및 설계

본 연구는 일반 홈페이지도 웹 설계 단계에서 보안 취약점을 최소화할 수 있다는 사례를 보여주고자 '야구인들을 위한 승부예측 웹 사이트'를 제작하였다. 일반 홈페이지 구축 시 주로 사용되는 게시판 기능과 DB 를 활용하는 회원제 시스템을 설계하여 기본 구성을 충실히 하였다. 더욱이 사이트 관리자의 입장을 충분히 고려할 수 있도록 관리자 계정 보안 및 관리자 권한 명시에 유념하였다.

사이트 제작 전 XSS attack, CSRF(Cross Site Request Forgery) 등 웹 상에서 빈번히 발생하는 취약점의 원리와 그 사례에 대하여 찾아보았으며 java 시큐어코딩 가이드 내 점검 항목을 모두 숙지하였다.

'야구인들을 위한 승부예측 웹 사이트' 에는 현재까지 습득한 소프트웨어 개발 보안 점검 항목을 바탕으로 웹 보안 취약점을 최소화한 jsp 코드를 적용하였다. 개발 환경은 Cent OS 이며 웹 어플리케이션 서버(WAS)로 Tomcat 을 사용하였다. 야구 경기의 '승률 예측'을 위해 python 을 사용한 것을 제외하고, 이 외의 개발 언어를 java, jsp 로 통일하여 java 시큐어코딩 가이드를 적용하는 데에 어려움이 없도록 하였다. 또한, mysql 을 이용한 DBMS 에도 순차적으로 보안 설계를 적용하였다.

먼저, 웹 사이트의 관리자 계정 패스워드는 "영문 대소문자 + 숫자 + 특수문자"로 이루어진 9 글자 이상의 조합으로 하여 관리자 계정에 대한 임의의 유추가 불가능하도록 하였다. 이를 위해 password 복잡도 검증을 추가적으로 수행하였다. 또한, 로그인 시 get 방식이 아닌 post 방식으로 입력 값을 받아 post 방식으로 파라미터를 넘길 수 있도록 하였다.

```
<!-- Main -->
    <section class="wrapper style1">
    <form name= "form1" method="post" action="login2.jsp">
        <div class="container">
            <div id="content">

                <!-- Content -->

                <article>
                    <header>
                        <h2>로그인</h2>

                    </header>

                    <div id="contents">
                        <h3> 로그인(로그인 정보를 입력하세요.) </h3>
                        <br>
                        <br>

                        <label for="user_id">아이디</label>
                        <input type="text" id="id" name="id" required>
                        <br>
                        <br>

                        <label for="user_pwd">password</label>
                        <input type="password" id="pwd" name="pwd" required>
                        <br>
                        <br>
                        <br>
```

(그림 2) 로그인 시 POST 방식을 사용한 코드

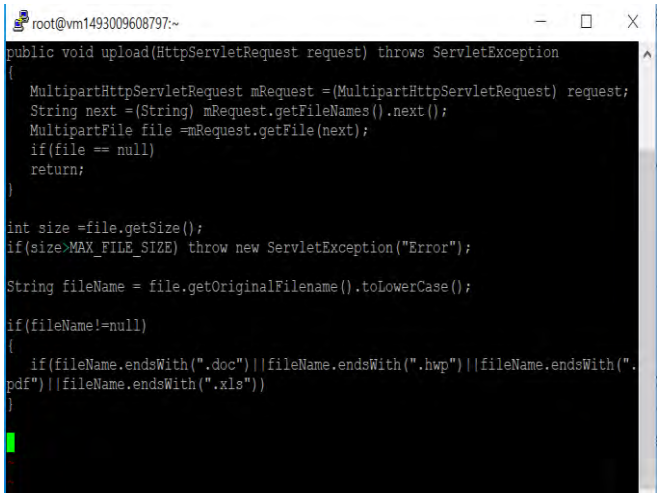
DB 를 구축하는 일반 사이트에서 방어하기 쉽지 않은 SQL injection 을 대비하기 위해서는 웹 소스 구현 시 아이디/비밀번호 인증을 통한 SQL 삽입 문제를 확인해 보았다. 검색어 필드에 로그인 ID 를 입력한 후, DB error 가 일어나는지 살펴 보았으며, 로그인 모듈 점검을 실행하였다. 또한, DBMS 에서 default 값을 갖는 DB 관리자 계정을 추측하기 어려운 이름 및 패스워드로 변경하였다.

(그림 3) 로그인 모듈 점검

웹 사용자들 간의 소통을 담당하는 '커뮤니티' 창의 게시판에는 첨부파일 업로드 기능의 제어를 강화하였다. 홈페이지 내에서 사용자의 접근이 용이한 첨부파일 업로드 기능은 반드시 검증이 필요한 항목이다. 이에 따라, 팀 내 개발자들은 3 가지의 게시판(구단 별 커뮤니티, 야구용품 중고거래, 구장 별 티켓거래) 구현 소스에 파일의 확장자에 대한 적합성 여부를 검증하는 루틴을 추가하였다.

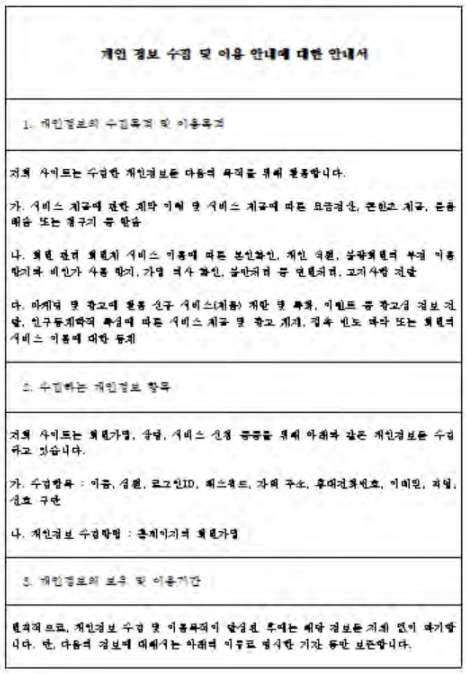
먼저, jsp, php 등의 확장자를 가진 파일을 업로드하여 실행 가능한 확장자의 업로드 가능 여부를 조사하였다. 그리고 jsp 코드를 적용하여 첨부 파일의 확장자를 필터링하였다. 일례로, 확장자가 대문자로 이루어져 있거나 확장자의 파일 크기가 지나치게 크다면 필터링 되는 방식이 그것이다. 이처럼 허용된 확장자만 파일 업로드가 가능하도록 설정하는 것을 whitelist 방식이라고 한다.

(그림 4) '커뮤니티' 게시판 생성



(그림 5) 확장자 파일 업로드 제어 코드

마지막으로 사이트를 이용하는 사용자들에게 보다 확실하고 편리한 정보를 제공하기 위하여 로그인 시 개인정보보호 동의서 및 이용약관 창을 적용하여 신뢰감을 높였다. [4] 이는 홈페이지 사용자들에게 보안에 대한 기본 지침서가 될 뿐 아니라 관리자의 권리를 사용자들에게 정확하게 명시함으로써 향후 보안 관련 문제 발생 시 후속 처리가 명확할 수 있도록 문서로 증명하는 기능을 한다.


개인 정보 수집 및 이용 안내에 대한 안내서

1. 개인정보의 수집목적 및 이용목적

귀하 사이트는 수집한 개인정보를 다음의 목적을 위해 활용합니다.

가. 서비스 제공에 관한 계약 이행 및 서비스 제공에 따른 요금정산, 콘텐츠 제공, 문의 사항 또는 불구기 등 발송

나. 회원 관리 회원제 서비스 이용에 따른 본인확인, 개인 식별, 불량회원의 부정 이용 방지와 비인가 사용 방지, 가입 의사 확인, 불만처리 등 민원처리, 고지사항 전달

다. 마케팅 및 광고에 활용 신규 서비스(제품) 개발 및 특화, 이벤트 등 광고성 정보 전달, 인구통계학적 특성에 따른 서비스 제공 및 광고 게재, 접속 빈도 파악 또는 회원의 서비스 이용에 대한 통계

2. 수집하는 개인정보 항목

귀하 사이트는 회원가입, 상담, 서비스 신청 등등을 위해 아래와 같은 개인정보를 수집하고 있습니다.

가. 수집항목 : 이름, 생년, 로그인ID, 패스워드, 자택 주소, 휴대전화번호, 이메일, 직업, 성호 구분

나. 개인정보 수집방법 : 홈페이지의 회원가입

3. 개인정보의 보유 및 이용기간

원칙적으로, 개인정보 수집 및 이용목적이 달성된 후에는 해당 정보를 지체 없이 파기합니다. 단, 다음의 정보에 대해서는 아래의 이유로 명시한 기간 동안 보존합니다.

(그림 6) 개인정보보호 동의서

4. 결론

최근 발발한 Ransomware 사고로 인하여 우리 사회의 보안에 대한 경각심은 최고조에 이르렀다. 본 논문은 이러한 사회 이슈를 조명하고, 웹 개발자들에게 웹 보안에 대한 생각의 전환점을 전달해주고자 제시되었다. 현재 대부분의 사이트는 웹 방화벽, IDS 등을 활용해 추가(Add-on) 방식으로 웹을 관리 중이다. 그러나 개발자들이 사전 설계 시 보안에 최적화된 코드를 작성하여 웹 취약점을 사전에 차단한다면 홈페이지 해킹의 위험은 훨씬 줄어들 것이다.

본 논문은 직접 제작한 사이트를 활용하여 일반 사이트에도 웹 보안을 충분히 설계 및 적용할 수 있다는 것을 보여주었다. 특히, 웹 서버 및 DB 관리자에게 강력한 관리자 계정의 생성에 대한 필요성을 일깨워주었다.

또한, 사용자들의 편의를 위해 만든 야구 승부예측 사이트에 개인정보보호 동의서와 같은 증명을 포함함으로써, 사용자들이 개인정보보호에 대하여 한 번 더

생각해보는 계기를 갖도록 하였다. 이와 같이, 웹을 만들고 사용하는 모든 사람들에게 웹 보안의 중요성을 알리는 본보기가 되고자 한다.

참고문헌

[1] OWASP, The Free and Open Software Security Community
https://www.owasp.org/index.php/Top_10_2017-Top_10
[2] Java Secure Coding Guide for Software Engineer
http://www.moi.go.kr/frt/bbs/type001/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000012&nttId=42152
[3] Homepage Development Security Guide
http://ois.khu.ac.kr/04/homepage_dev_guide.pdf
[4] Guidance on Personal Information Protection for Communication Service Providers
https://www.kisa.or.kr/public/laws/laws3_View.jsp?cPage=8&mode=view&p_No=259&b_No=259&d_No=7&ST=T&SV=

"본 논문은 2017 년 한이음 ICT 멘토링 프로젝트의 결과물입니다."