정보보호시스템 구축 및 모의해킹을 통한 정보보호이해

정상미*, 김창현**, 노현우***, 최진우****, 정유진*****, 문의성******
*안랩 소프트웨어 QA
**강릉원주대학 정보기술공학과
***서울시립대학 컴퓨터과학부
****한국외국어대학 정보통신공학과
*****가천대학 컴퓨터공학과
******광운대학 전자공학과
e-mail: moon7392@naver.com

Building protection system and Understanding information protection through simulation hacking

Sang-Mi Jung*, Chang-Hyeon Kim**, Hyeon-Woo Noh***, Jin-Woo Choi****, Yu-Jin Jung*****,
Eui-Seong Moon******,
*Software QA team, AhnLab,
**Dept. of Information Technology Engineering, Gangneung-Wonju National University,
***Dept. of Computer Science, University of Seoul,
****Dept. of Information and Communication Engineering, Hankuk University of Foreign Studies,
*****Dept. of Computer Engineering, Gachon University,
******Dept. of electric enginerring, Kwangwoon University

요 약

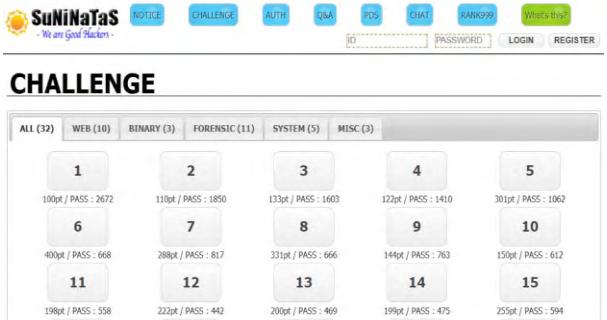
최근 보안적 이슈에 따른 피해가 지속적으로 늘어남에 따라 사람들이 보안에 관심이 많아 지기 시작했다. 모의해킹 분야의 경우 기존에 문제 풀이 웹 사이트들이 존재하지만 회원 가입 단계부터 입문자들이 시작하기에는 높은 진입장벽이 존재한다. 본 연구에서는 방 탈출 게임의 컨셉을 모의해킹에 적용하여 모의해킹 문제를 게임을 푸는 방식으로 접근하여 입문자들도 쉽게 모의해킹 분야를 시작할 수 있도록 하였다. 웹 서버는 오픈소스 웹 방화벽인 ModSecurity[1]와 Spring Security 로 서버 보안을 강화하였다.

1. 서론

최근 워너크라이, 나야나 사건 등 Ransomware 보안 사고는 사회적으로 큰 이슈로 부각되었다. 이러한 사회적 분위기 속에서 정보 기술에 대한 기반 지식이 낮은 사람들도 보안에 관심이 많아지기 시작했다. 하지만 보안이라는 분야가 진입장벽이 매우 높고 기존의 모의해킹 사이트 역시 진입 장벽이 높아 입문자들이 쉽게 접하기에는 많은 어려움이 존재한다. 이를 극복하는 방법으로 누구나 쉽고 재미있게 배울 수 있는 시스템을 구축하고자 한다. 이를 통해 모의해킹을 경험함으로써 정보보호를 이해할 수 있는 계기를 제공한다. 본 연구는 기존의 오프라인 형태의 방 탈출 게임 concept 을 온라인 웹 어플리케이션에 적용하여 STAGE 와 난이도의 개념을 더하여 보안 공부를 하는데 흥미를 유발하고 어렵게 다가 올 수 있는 모의해킹을 게임으로 구성해 보안 이슈를 친숙하게 느끼고 체험해 볼 수 있게 했다.

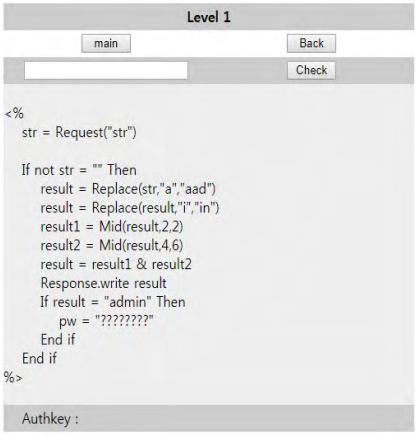
2. 모의해킹 웹 사이트의 필요성

모의해킹을 공부하는 전공자들은 DVWA 나 webgoat 를 개인 서버에 직접 설치하여 학습하거나 기존의 모의해킹 사이트를 이용한다. 전공자들이 많이 찾는 모의해킹 웹사이트 중 대표적인 예로는 webhacking.kr, Suninatas, hackthisssite.org 가 있다.



(그림 1) Suninatas challenge 목차

(그림 1)과 같이, WEB, Binary, Forensic, System, MISC 등의 취약점을 기준으로 문제가 나뉘어져 있어 특정 기술을 공부하고자 하는 전문가에게는 도움이 된다. 하지만 초보자는 보안에 대한 지식이 낮기 때문에 특정 기술 용어를 이해하는 것부터 시작해야 하는 어려움이 있다.

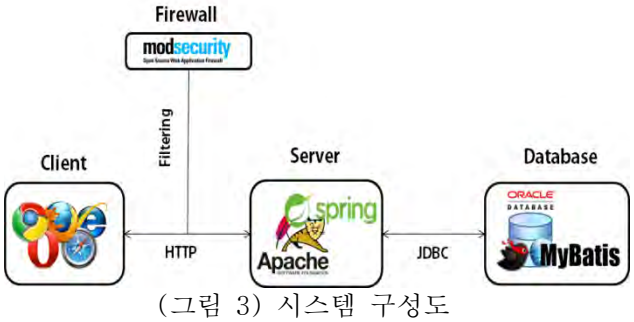


(그림 2) Suninatas Web Challenge Level 1

또한 낮은 수준의 문제 풀이를 시도할 경우에도 (그림 2)와 같이 Level 1 의 문제임에도 프로그래밍언어인 ASP 와 프로그램 구조 등의 전반적인 IT 지식이 요구된다. 이와 같이 보안에 대한 배경지식을 갖추고 있지 않다면 웹 상에 TIP 이나 문제풀이 없이 직접 문제를 해결하기에는 실질적으로 불가능 하다.

때문에 기존의 웹 사이트의 문제점을 해결하기 위해서는 기초적인 보안 지식을 보완 해줄 수 있는 학습 도구가 필요하다. 여기에 단순히 보안 문제 풀이가 아닌 스토리를 제공하여 재미있는 요소를 추가하고 스토리에 몰입할 수 있는 웹 UI 를 제공함으로써, 게임형식으로 보안 문제를 풀 수 있는 Escape The Site 를 제작 하였다.

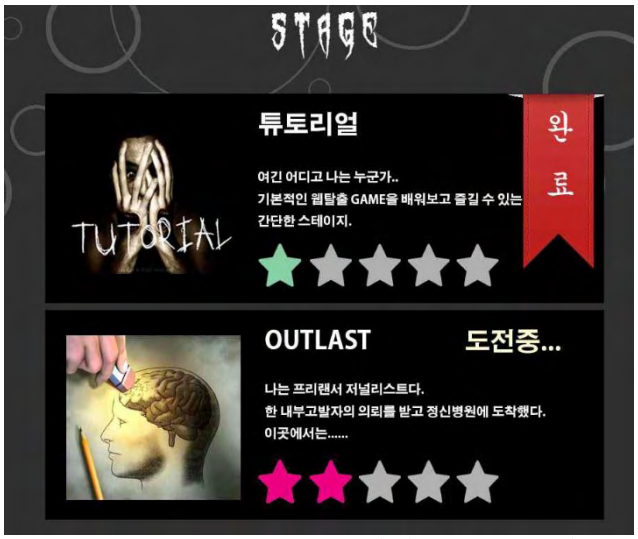
3. Escape The Site 사이트 디자인 및 설계



(그림 3) 시스템 구성도

본 연구는 클라이언트-서버 구조의 웹 서비스로 되어 있다. 클라이언트측 개발 언어는 HTML[2], JavaScript, Java, CSS 이고 JQuery 를 이용해서 사용자 PC 해상도에 맞게 동적으로 조절되는 반응형 웹을 구축했다. 웹 사이트 서버측 OS 는 Ubuntu 14.04, 웹 어플리케이션으로 Tomcat 8.5 버전을 사용했다. 개발 언어는 JAVA 이고 DB 는 Oracle DBMS 를 사용했다. JAVA spring framework 를 이용하여 서버 유지보수를 편리하게 하였고 DTO 를 통한 클라이언트 서버 간의 데이터 전송을 간단하게 했다. 또한 MyBatis 를 이용하여 상황에 따른 Query 문 전달을 쉽게 하고 트랜잭션 기능을 사용하여 데이터 무결성을 높였다. 클라이언트와 서버간 통신언어로는 JSON 을 이용했다. 개발 도구는 SQL Developer 로 DB 접근하였고, Maven 으로 Library 를 관리하였다. 개발 환경은 Eclipse Neon, STS(Spring Tools Suite)에서 수행하였다. Spring Security 를 이용하여 사용자의 정보를 암호화시켜 DB 에 저장했다. 그리고 XML 문서를 통해 보안이 필요한 페이지를 명시함으로써 웹 페이지 간의 세션과 인증 관리를 체계적으로 했다. 또한 웹 방화벽인 ModSecurity 를 사용해서 요청, 필터링, 우회 방지 기술, POST payload 분석, 감사 로깅, HTTPS 필터링 등의 다양한 기능을 사용했다.

Escape The Site 디자인은 기존의 방 탈출 게임을 포맷으로 했다. STAGE 는 다양한 스토리를 즐길 수 있도록 OUTLAST, BioHazard, WonderLand 등 흥미로운 주제를 바탕으로 7~10 개의 문제가 있는 page 를 구성했다. 참여자는 page 를 탈출하기 위해 문제를 풀고 참여자의 문제풀이에 도움이 될 수 있는 hint 를 각 page 마다 적절하게 배치했다. 또한 다양한 실력의 참여자가 학습하도록 난이도가 다른 STAGE 를 구성하여 난이도를 점차 높여가며 실력향상에 대한 성취도를 갖도록 하였다.

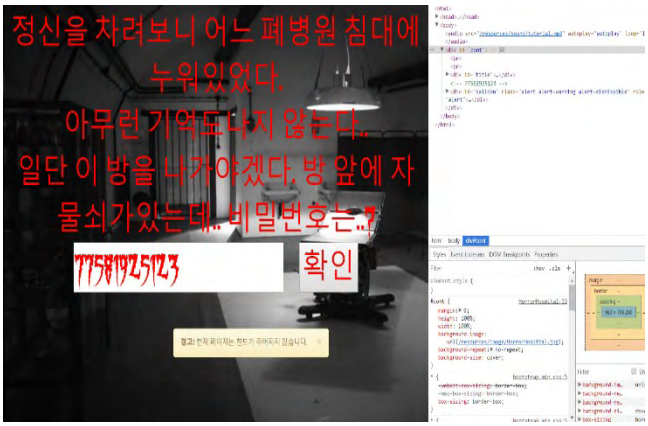


(그림 4) Escape The Site 사이트 STAGE 화면

Escape The Site 는 기존의 게임과 유사한 방식을 제공하기 위해 게시판 기능과 회원들의 문제풀이 현황을 알 수 있는 알림 기능, 랭킹 시스템을 유지했다. 또한 계속해서 문제를 이어 갈 수 있도록 이어하기 기능을 추가했다. 이론적으로 모의해킹을 학습할 수 있도록 각 STAGE 마다 해답과 문제풀이 방법을 제공하고 Help 메뉴를 통해 해킹 Tool 의 목적과 사용 방

법 등 기능을 추가했다.

모의해킹 문제는 STAGE 별로 난이도를 조정하여 낮은 난이도의 문제는 도구를 사용하지 않고 풀 수 있도록 하고 높은 난이도는 웹 보안의 취약점들을 빈도수와 중요도 순으로 정리한 OWASP TOP 10[3]을 바탕으로 취약성이 높고 현재 이슈가 많이 되는 보안상 취약점을 기반으로 출제했다. Burp suite[4], Paros 를 사용하여 풀 수 있는 문제들을 통해 모의해킹 시에 기본이 되는 도구들의 사용법을 익힐 수 있게 했다.



(그림 5) 튜토리얼의 2 번문제 풀이

예를 들어 튜토리얼의 2 번문제는 (그림 5)와 같이 비밀번호를 찾는 문제이다. 이 경우 웹 브라우저 개발자 도구를 통해 웹 사이트의 소스코드를 확인하고, 소스코드에서 주석으로 처리된 비밀번호를 찾아서 해결하는 낮은 수준의 문제로서 웹 브라우저의 기본적인 내용을 학습할 수 있다. 또 다른 예로는 OUTLAST 의 높은 난이도의 문제로 Brute force 공격 방식을 사용하는 문제이다. 이 경우 Python 과 같은 Script 언어로 서버와의 통신을 반복적으로 수행하는 프로그램을 작성하여 문제를 해결한다. (그림 5)의 문제와 같이 간단한 인터넷 소스코드를 보는 방법을 활용하는 문제부터 Script 언어를 이용하는 OUTLAST 의 높은 난이도 문제까지 다양한 난이도의 문제를 구성했다. 따라서 입문자부터 전문가까지 자신의 수준에 맞는 학습이 가능하다.

4. 결론

본 논문은 사회적으로 관심이 점점 높아지고, 이슈가 되는 보안 사건과 관련하여 보안에 대한 전반적인 지식과 사람들의 보안 수준을 높일 수 있는 방안을 연구했다. 특히 최근 가장 이슈화 되고 취약한 부분을 정리한 OWASP TOP 10 을 바탕으로 현 시점에서 가장 필요하고 가장 중요한 부분의 취약점을 공부할 수 있는 학습도구를 제시했다.

Escape The Site 는 서버에 보안성 향상을 위해 JAVA 보안 Framework 와 ModSecurity 웹 방화벽을 이용했다. Escape The Site 를 통해 사용자는 기본적인 웹 브라우저에 대한 이해부터, 보안에 대한 지식까지 점진적으로 학습할 수 있다. 흥미로운 시나리오와 기존의 방 탈출 게임 concept 를 배경으로 한 UI 를 바탕으로, 보안에 대한 공부를 조금 더 친숙하고, 재미있게 할 수 있다.

해당 논문은 점점 이슈화 되는 사회적 분위기에 맞춰 보안에 대한 지식을 일반인들이 학습할 수 있게 했고 전문가의 모의해킹 실력 향상에 도움이 되도록 다양한 문제를 제시했다. 나아가 일반인의 보안 지식 향상을 통해 최근에 이슈되고 있는 보안 문제를 이해하고 이에 대한 경각심을 일깨워 주는 데에 도움이 된다.

참고문헌

[1] ModSecurity, Open Source Web Application Firewall https://modsecurity.org/
[2] W3Schools.com The World's Largest Web Developer Site https://www.w3schools.com
[3] OWASP, The Free and Open Software Security Community https://www.owasp.org/index.php/Top_10_2017-Top_10
[4] Burp suite Download and basic contents https://portswigger.net/burp

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