김일성종합대학학보
(자연과학)
주체103(2014)년 제60권 제9호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 60 No. 9 JUCHE103(2014).

웨브봉사기에 대한 자동화된 요청을 차단하기 위한 한가지 방법

황인호, 조성순

위대한 령도자 **김정일**동지께서는 다음과 같이 지적하시였다.

《과학자, 기술자들은 현실에 튼튼히 발을 붙이고 사회주의건설의 실천이 제기하는 문제들을 연구대상으로 삼고 과학연구사업을 진행하여야 하며 연구성과를 생산에 도입하는데서 나서는 과학기술적문제들을 책임적으로 풀어야 합니다.》(《**김정일**선집》 제15권 증보판 492페지)

정보산업의 시대인 오늘날 해킹에 의한 파괴 및 공격행위는 급격히 늘어나고있으며 모든 기업활동이 망을 통하여 진행되고있는것으로 하여 그로 인한 피해는 치명적이다.

론문에서는 싸이트에 설치된《함정》과 modsecurity를 리용하여 해커들이 공격에 앞서 웨브봉사기에 대한 취약점조사로 리용하는 도구들의 기능을 막기 위한 한가지 방법에 대하여 고찰하였다.

1. 선행연구고찰 및 문제설정

콤퓨터가 우리 생활의 필수적인 요소로 되고있는 오늘날 웨브봉사를 떠난 기업의 정보화에 대해서는 생각할수 없다. 그런것만큼 전송층공격보다 응용층공격의 피해의 후과는 상상을 초월하게 된다.

세계적으로 응용층준위의 공격방법들이 수많이 나오고있으며 그 수법 또한 다양해지고있는데 대표적으로 SQL Injection, Directory Traversal, Cross Site Scripting(XSS), Cross Site Request Forgery(CSRF), Distributed Denial of Service(DDoS) 등을 들수 있다.[4]

그러므로 웨브응용프로그람의 약점을 리용하여 진행하는 공격을 막기 위해서는 modsecurity와 같은 웨브응용프로그람방화벽(Web Application Firewall: WAF)을 반드시 설치하여야 한다.

웨브응용프로그람들은 다른 응용프로그람들과는 달리 망에서 봉사기/의뢰기모형으로 동작하기때문에 망에 존재하는 임의의 사용자에 의해서 접근가능하다.[1, 2] 또한 웨브응용프로그람들은 흔히 일반개발자들에게 의뢰하여 개발되기때문에 전문개발자들이 개발하는 기성쏘프트웨어보다 보안상 많은 결함들을 가지고있게 된다.

그러므로 웨브응용프로그람에 대한 충분한 보안검사를 진행하여야 할 필요성이 제기된다.

하지만 웨브응용프로그람이 보안적인 측면에서 어떤 취약점들을 가지고있는가를 수동

적으로 검사하는것은 매우 복잡하고 오랜 시간이 걸리며 동시에 보안에 대한 충분한 전문지식을 가질것을 요구하는 어려운 문제이다.

바로 이러한 문제를 해결하기 위해서 개발된 acunetix와 같은 도구들은 자동화된 웨브응용프로그람취약점검사도구들로서 전체 웨브싸이트를 훑으면서 자동적으로 웨브싸이트를 목표로 하여 공개된 공격들을 진행하는 방식으로 웨브응용프로그람에 존재하는 보안상의 결함들을 찾아주는 아주 유용한 프로그람이다.[2, 3]

그러나 웨브싸이트에 대하여 이러한 도구들을 싸이트관리자가 아닌 공격자가 리용하는것은 허용되지 말아야 한다.

웨브봉사기를 목표로 공격을 진행하는 해커들은 먼저 해당 봉사기의 취약점을 찾아내기 위하여 acunetix와 같은 취약점검사도구로 해당 싸이트를 조사한다. 다음 찾아낸 취약점에 맞는 공격도구를 리용하여 봉사기를 공격하여 자료를 절취하거나 봉사기의 기능을 마비시킨다.

우리는 웨브싸이트에 설치된《함정》과 modsecurity규칙을 리용하여 웨브봉사기에 자동적으로 요청을 보내는 취약점검사도구들과 웨브싸이트내리적재도구들을 막기 위한 한가지 방법을 제안하고 실현하였다.

2. 웨브봉사기에 대한 자동화된 요청의 막기

1) 취약점검사도구들과 웨브싸이트내리적재도구

취약점검사도구들은 검사하려는 웨브싸이트에 대하여 요청할수 있는 가능한 모든 페지들을 결정하여 요청해보면서 웨브싸이트의 취약점들을 알아낸다.

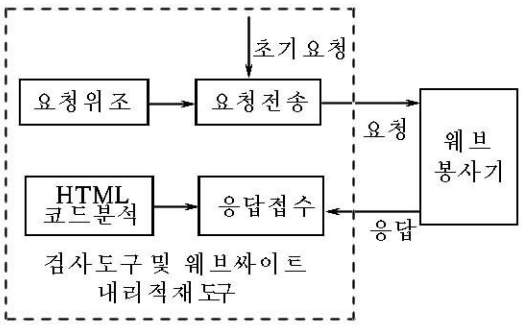

그림. 취약점검사도구들과 웨브싸이트 내리적재도구들의 동작과정

취약점검사도구들은 요청가능한 모든 페지들을 결정하기 위하여 봉사기에 대한 요청의 결과로 얻어지는 응답페지의 HTML원천코드를 분석하여 자기가 다시 요청할수 있는 요청페지들을 결정한다.(그림)

또한 웨브싸이트의 내용을 정적화일들로 내리적재하는 webzip도구도 이와 같은 방식으로 봉사기에 자동적으로 요청을 보내고 그 결과로 받는 응답자료를 리용하여 자기의 기능을 실현한다.

대표적인 HTML코드들과 Javascript코드들은 다음과 같다.

HTML코드

```
<a href="./register.php"> </a>
<form method="post" action="viewContent.php">
```

Javascript코드

```
document.location=”logout.php”
window.location=”welcome.php”;
window.open(“../viewArticle.php”);
```

하지만 이러한 도구들에도 치명적인 결함이 있다.

그것은 이 도구들이 요청할 페지들을 결정할 때 HTML코드만을 분석하며 HTML코드에 포함되지 않는 CSS(Cascading Style Sheet)의 내용은 분석하지 않는다는것이다.

2) CSS를 리용하여 페지에 《함정》 작성

웨브싸이트의 페지들을 작성할 때 개발자들은 CSS를 리용하여 해당 HTML요소들에 대한 여러가지 속성을 설정한다.[2]

실례로 Javascript, HTML, CSS코드들을 고찰하자.

Javascript코드

```
function onRegister() {
    var form = document.getElementById('form_id');
    form.action = "user/system_admin_login_class.php";
    form.submit();
}
```

HTML코드

```
<input type="button" id="hidden_button" value="새로 등록" onclick="onRegister()">
```

CSS코드

```
#hidden_button {
 display:none;
}
```

우의 코드들로 작성한 웨브페지를 현시하면《새로 등록》이라는 단추는 대면부에 현시되지 않기때문에 대면부에서 단추나 하이퍼련결을 리용하여 페지이동을 진행하는 정상적인 사용자는 그 단추를 누를수 없으며 결과 system_admin_login_class.php화일을 요청할 수 없다.

3) modsecurity를 리용한 검출

modsecurity는 HTTP요청의 요청행에서 요청한 화일을《함정》페지이름과 비교하여 공격자의 IP주소를 알아낸다. 여기에 해당한 구체적인 방화벽규칙은 다음과 같다.

```
SecRule REQUEST_FILENAME "system_admin_login_class.php" "phase:1,auditlog,log,id:'999921',drop,msg:'Crawler Attack Identified'"
```

맺 는 말

《함정》페지들을 웨브싸이트의 여러 페지들에 설치하고 시험해본 결과 acunetix, webzip와 같은 도구들이 웨브싸이트에 대한 조사를 진행하지 못하였다.

참 고 문 헌

[1] http://ssrg.site.uottawa.ca/docs/ICWE2012.pdf.

[2] http://ssrg.eecs.uottawa.ca/docs/CASCON2012.pdf.

[3] http://www.cs.coiumbia.edu/~dai/paper/baseline_submission.pdf.

[4] http://www.owasp.org/index.php? Title=Top_1_2013.

주체103(2014)년 5월 5일 원고접수

A Method to Block Automated Requests to the Web Server

Hwang In Ho, Jo Song Sun

We propose a method to block crawling request of web vulnerability scanners which is used in scanning web server and application's vulnerabilities.

We prepare "hole" pages in the web pages and monitor requests on the pages with the modsecurity.

Key word: web vulnerability