웹 스캔을 이용한 웹서버 취약성 파일 분석 도구

유두훈, 소우영
한남대학교

Vulnerable File Analysis Tool Using Web Scanning for Web Server

Du-Hun Yu. Woo-Young Soh
Dept. of Computer Science, Hannam University

요 약

최근 웹 서버에 대한 해킹이 다양하고 지능적인 웜의 형태로 시도되고 있다. 이러한 웹 서버 해킹은 대개 웹을 통하여 접근할 수 있는 취약성 파일에 악의적인 코드를 삽입하여 전파시킴으로써 웹서버에 피해를 주며 급속히 확산된다. 따라서 이러한 취약성이 있는 파일을 조사할 수 있는 자동화된 도구가 요구되며, 본 논문에서는 웹으로 공유되어 있는 디렉토리 내에 웹 스캔을 이용하여 취약성 파일을 조사하는 방법으로 웹 서버 내의 취약성을 알아내는 분석도구를 개발하였다.

1. 서론

웹 서버 환경에서 웹 사용자들의 환경 특성이나 활동 내역을 TCP/IP 프로토콜에 따라 시스템 로그(log)로 남긴다. 로그에는 클라이언트(Client)의 활동과 접속 시 클라이언트들에 대한 정보가 기록되어 있다. 접속을 통한 행동을 조사해보면 그에 따른 불법적 침입 행동에 대해서 분석할 수 있다. 이러한 로그에 따르면 웹서버의 불법적 침입은 접근 방법에 따라 두 가지로 구분할 수 있다. 첫째는 웹서버의 취약성을 이용한 접근방법이며, 둘째는 웹서버에 공유된 디렉토리의 취약성 파일 문제를 이용한 접근으로 구분할 수 있다. 서버의 취약성은 패치를 통해 문제를 해결할 수 있지만 취약성 파일은 파일에 대한 문제점을 파악하여야 하며, 사내 또는 공공기관에서 사용하는 상용 프로그램의 파일일 경우는 원인제공의 문제점과 관계되는 파일을 조사하여야 한다. CERT[1]에서는 침해 사고들에 대한 권고문을 배포하고 있으며, 최근에 문제시되고 있는 웹서버의 버그나 바이러스에 대해서도 권고하고 있다. 한국 정보보호 진흥원, 한국리눅스그룹[2], FSU[3], NTFAQ[4]에서는 웹 비즈니스인 웹 컨텐츠를 가진 IT업계의 사업자들에게 보안에 관한 다양한 방법의 자료를 제공한다. 이러한 침해 관련 문제들은 단순 패치를 통해서 해결하는 것 보다 관리 적인 측면에서 취약성 파일에 대한 정보를 수집하여 다음에 일어 날 수 있는 문제를 보고하거나 신속한 대응 방안을 마련하는 것이 중요하다. 또한 로그 분석을 통해 접근의 성공과 실패를 확인하여 불법적인 접근을 조사한다. 다음 장에서는 웹서버와 클라이언트의 동작 원리를 응용한 불법적인 취약성 파일 분석 방법에 대하여 기술한다.

2. 웹서버와 클라이언트의 동작 방식

웹 클라이언트 도구인 브라우저를 가진 사용자가 HTTP프로토콜을 사용하여 웹 서버에서 정의된 MIME-TYPE으로 문서를 요청하면 웹 서버는 요청한 클라이언트에게 문서를 전송한다[5-7]. 클라이언트가 웹 서버에게 웹 페이지를 요청할 때 쓰이는 프로토콜은 HTTP 프로토콜로 클라이언트의 URL에 주소(IP Address)를 입력하면 이를 인코딩하여 네트워크를 통하여 웹 서버에 전송한다. [그림 1]은 이러한 방식을 도식화 한 것이다.

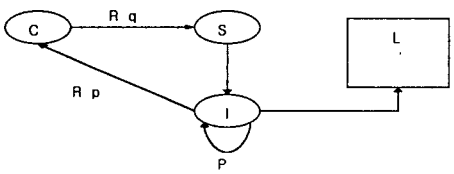

그림 1. 웹 로그 생성방식

가. Rq : Request 클라이언트의 요청
나. Rp : Response 서버로부터의 응답
다. C : Client 클라이언트(웹 브라우저)
라. S : Web Server 서버(NT/2000)
마. I : Web Server Process 응답처리
바. P : Process 처리
사. L : LogFiles 처리 결과 기록

웹 로그는 Date, time, src_ip(접근자 IP Address), c_user(접근자 컴퓨터 이름), Port(접근 포트), uri_stem(접근 대상 페이지), Query(질의), agent(클라이언트 이름), Status(접근 상태코드) 등의 필드로 기록되며, [표 1]은 로그 기록 필드에 대한 사항을 나타내며 ⑨는 사용자가 웹브라우저를 통해서 웹으로 공유되어있는 디렉토리 내에 요청된 페이지에 대한 기록을 남기는 필드이며 웹서버 취약점 파일 분석도구의 중요한 방법을 제시하는 필드이다.

표 1. 로그기록 필드

1) date : 접속자가 접속한 날짜
(형식 - 01-06-22)
,,,,,,,,,,,,,,,,, 중략 .....
9) cs-uri-query : 서버에 요청한 쿼리
(형식 - 다른 특정한 쿼리가 없을 경우
에는 -로 표시가 되며 그렇지 않은 경
우에는 그에 대한 쿼리가 나타난다)
10) sc-status : 클라이언트
(웹 브라우저, telnet등 80에 접속하는
모든 클라이언트가 서버에 접속을
시도하여 정상적인 컨넥션인지에 대한
체크 상태 표시가 나타난다.

이러한 쿼리를 통해 ⑩의 상태코드와 일치하는지 확인한다. 요청된 쿼리가 정상적일 경우는 200이라는 코드를 출력하며 이러한 경우 웹서버에는 요청한 파일이 웹으로 공유되어 있는 디렉토리에 위치해 있음을 알려준다. 이 원리를 통해 취약성이 있는 파일을 미리 조사하여 분석하는 도구를 설계한다.

3. 취약성 파일 분석도구 설계

[표 2]는 웹으로 공유되어 있는 파일 중 특정 문자열에 대한 해석을 하지 못하여 서버의 정보 유출, 도스 공격, 스팸 메일 등의 취약성이 있는 파일이며 설명 항목은 취약성에 대한 설명이다. 이러한 취약성 파일들은 2장에서 기술된 웹 로그 형식 중 cs-uri-stem이라는 필드에 기록되며 취약성 파일에 대한 접근 유무를 알 수 있는 부분이다[8-10]. 이러한 쿼리를 분석하여 웹 컨텐츠 기반의 IT업체에서 정의된 파일에 대한 요청이 아닌 시스템 파일이나 [표 2]에 기술된 파일을 요청하는 경우는 접속자의 행위를 분석하여 취약성 파일 접근 사용자들의 불법 행위 여부를 살펴볼 필요가 있다. [표 2]의 설명 항목은 요청 파일들의 불법행위 유형을 기술하고 있다.

표 2. 취약성이 있는 파일 목록

번호	요청된 화일명	설명
1	carbo.dll	iCat Carbo Server
2	uploader.exe	Websites
3	search97.vts	search97
4	newdsn.exe	Remore File create, IIS Dos

..... 중략 .....

예를 들어 [표 2]의 요청된 파일 중에 번호 1에 해당하는 carbo.dll 파일의 취약성은 ..\..\에 대한 문자열 처리를 제대로 하지 않아 발생하는 문제로 서버의 설정 파일인 Win.ini 파일의 정보를 보는 방법을 나타낸다.

```
예제)
http://host/carbo.dll?icatcommand=..\..\winnt\win.ini&catalogname=catalog
```

예제)의 접근 방법을 통해 서버에 접근하면 서버의 기록된 로그는 표 2와 같이 기록된다. 클라이언트가 웹서버에 접속할 경우 80번 포트를 통하여 정상적인 접속을 하면 접속 코드에는 200이라는 숫자를 기록하게 된다. 아래 표 2는 정상적인 접속을 시도하여 쿼리를 서버에 요청하여 처리되는 경우를 나타낸다.

[표 2]의 쿼리내용 "icatcommand=..\..\winnt\win.ini &catalogname=catalog" (경로의 표시)은 현재 위치로부터 상위 두 단계 위의 경로로 이동하여 서버의 환경 설정 파일인 win.ini를 클라이언트에서 실행함을 의미한다. 이 경우 클라이언트는 win.ini를 해석하여 브라우저에 보여주는 취약성이 있다.

이러한 취약성 파일에 대한 접근과 정상적인 코드 번호 200을 받았을 경우 서버의 취약성이 노출됨을 알 수 있다.

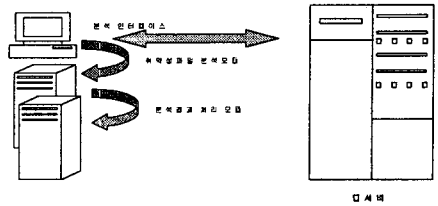

그림 2. 취약성 파일 분석도구 설계

[그림 2]는 제안된 취약성 파일 분석도구이며 크게 세 가지 모듈로 구성된다. 즉, 취약성 파일 분석 인터페이스, 취약성 파일 분석 모듈 및 취약성 파일 분석 결과 처리 모듈로 구성된다. 첫째, 취약성 파일 분석 인터페이스는 분석하고자 하는 IP 주소와 포트 번호를 입력받는다. 둘째, 취약성 파일 분석 모듈은 해당 IP로부터 하위 255번까지의 IP 대역을 검사하여 웹서버를 운용하는 IP에 대하여 웹서버의 버전 및 취약성 파일에 대하여 분석한다. 셋째, 취약성 파일 분석결과 처리 모듈은 취약성에 대한 분석결과를 관리자에게 알려주는 역할을 하며 취약성 파일 발견 시에 관리자에게 경고 메시지를 출력한다. [표 2]의 취약성 목록들을 침입유형 패턴으로 하여 취약점 분석을 하고자 하는 서버에 요청을 하며 각 서버에 따라 서버의 상태를 확인하여 상태정보를 확인하는 절차를 보여준다.

4. 취약성 파일 분석도구 구현

본 논문에서 제안된 취약성 분파일 분석도구는 2장의 웹서버 로그 생성 방식에 기초하여 3장의 취약성 파일 분석 방법에 의하여 구현되었다. 제안된 취약성 파일 분석도구는 위치에 상관없이 인터넷을 이용할 수 있는 장소에서 서버의 취약성을 분석할 수 있도록 웹기반으로 구현되어 있으며 관리자 이외의 사용자들이 악용할 위험성을 고려해 암호화된 인증을 통하여 관리자만 접근하도록 웹에 대한 접근을 통제한다. 3장의 세 가지 인터페이스를 토대로 취약점 분석 대상인 서버의 하위 255번까지의 IP대역을 확장 검사하도록

설계되어 있다. 같은 대역 내에 다른 웹서버의 취약성 또한 조사 분석할 수 있는 통합적인 기능을 갖고 있으며 관리자에게 취약성 파일을 발견하여 경고 메시지를 주어 공유된 디렉토리로부터 파일을 삭제할 수 있도록 함으로써 사전 조치를 취해 피해를 축소할 수 있는 장점이 있다. [그림 3]은 테스트 서버에서 취약성을 가진 파일을 검색한 예를 보여주고 있다. 대상은 리눅스 서버이며 리눅스 서버의 취약성이 있는 파일들을 공유한 cgi-bin 디렉토리에서 test-cgi라는 취약성 파일을 발견한 결과이며 발견된 취약성 파일은 적색의 FOUND 메시지로 출력하여 경고한다. 이와 같은 취약성 파일을 발견한 관리자는 파일을 수정하거나 삭제할 수 있다.

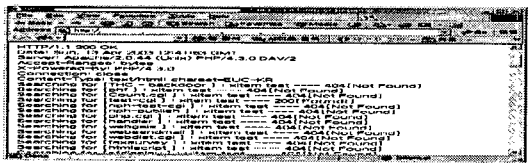

그림 3. 취약성 파일 분석 결과

5. 결론

최근 웹 서버의 사용이 증가하고 있으며 이를 이용한 해킹 등 각종 불법적인 접근이 사회 문제화되고 있다. 따라서 해킹 피해 여부 및 그 상황을 신속히 분석/조치 할 수 있는 취약성 분석 방법이 요구나 그 절차나 기법이 복잡하고 대개 부정확하다. 따라서 본 논문은 취약성 파일 분석 방법을 제시했으며, 또한 이 취약성 파일 분석 방법의 타당성을 분석하기 위하여 웹 취약성 파일분석 도구를 개발하고 피해분석 예를 보였다. 취약성이 있는 파일은 계속 증가하고 있으며, 새로운 취약성 파일은 현재 수작업에 의하여 개발되고 추가되고 있다. 향후 취약성 파일 업데이트 방법으로 자동화 등의 효율적인 기법 개발이 요구된다.

[참고문헌]

[1] http://www.cert.org

[2] http://linux.co.kr

[3] http://fsu.or.kr

[4] http://ntfaq.co.kr/

[5] 한석재, "리눅스 기반의 실시간 침입탐지 시스템 설계 및 구현", pp.35-43, 2002

[6] Protor, Paul E., "The Pratical Intrusion Detection", Prentice Hall, 2000

[7] Flanklin, Iain. "Protecting Web Server And Applications", Computr & Security, 2001, pp.32-35

[8] Richard, Barber. "The Evolution of Intrusion Detection Systems - The Next Step, ", Computer & Security, 2001, pp133-145

[9] 최용락외 3인, "컴퓨터 통신 보안", 그린출판사, pp.603-606

[10] ICU, "공무원 정보보호 제 3부 침입탐지 시스템", 한국정보 통신 대학원, 2001, pp.316