情 報 保 護 學 會 誌
第 15 卷 第 1 號, 2005. 2

웹 어플리케이션 보안 기술 동향

이 영 석*, 서 정 석**, 조 상 현*

요 약

웹(World Wide Web)은 사용자들간의 정보 전달에서부터 e-commerce, 인터넷 쇼핑몰, 인터넷 뱅킹 등으로 그 서비스의 사용이 확대되어 가고 있다. 웹 서비스의 증가와 더불어 최근 해킹 사고의 대부분은 웹 어플리케이션의 취약점을 이용한 사례가 증가하고 있다. 이러한 현상은 웹 서비스가 공개적으로 서비스를 제공하는 형태로 설계되었으며, 대부분의 웹 어플리케이션이 보안을 고려하지 않고 설계되었기 때문이다. 본 논문에서는 웹 어플리케이션의 취약 사례와 취약성 특징을 알아보고, 이러한 취약점을 방지할 수 있는 보호 노력들에 어떠한 것들이 있는지 얘기해보고자 한다.

Ⅰ. 서 론

최근 기업이나 국가 기관의 다양한 서비스 제공 요구와 함께 웹 서비스의 유용성과 용이성이 맞물려 전자 상거래, 인터넷 뱅킹, 인터넷 쇼핑몰등 웹 서비스 사용량은 증가하고 있다. 웹 서비스의 증가와 더불어 웹 취약성을 이용한 공격이 증가하고 있다. 2004년말부터 급증하고 있는 웹 페이지 변조 공격과 같이 웹 어플리케이션의 취약점을 노린 해킹 사건들이 봇물을 이루고 있다. 웹 서비스는 대부분이 정보 제공이나 서비스 제공을 목적으로 하기 때문에 다른 인터넷 서비스들과는 달리 접근 제어(access control)이나 방화벽 등으로 보호하기 어렵다. 또한 웹 서비스의 구조는 웹 서버, 웹 어플리케이션 소프트웨어, 데이터베이스 등의 복잡한 계층적 구조를 이루고 있기 때문에 한 위치에서 한 가지 보호 기법을 적용하여 전체 웹 서비스를 보호하는 것은 적합하지 않은 방법이다. 결국 웹 서비스를 효과적으로 보호하기 위해서는 웹 서비스에 특화된 웹 어플리케이션 보안 기술과 도구들이 필요하다.

각 기관들이 웹 어플리케이션 및 웹 서비스의 보안을 이행하고 향상시키는 것을 돕기 위한 단체인 Open Web Application Security Project(OWASP)에서는 가장 심각한 10가지 웹 어플리케이션 보안 취약점을 발표하였다. OWASP Top 10 리스트는 정부와 기업이 직면한 가장 심각하지만 종종 간과되어 오던 위험을 직접적으로 조망하고 있다. OWASP Top 10이전에는 아주 신뢰할 만한 기관이 웹 어플리케이션의 본안 문제에 관련된 통계를 발표한 일이 없다는 점에서 OWASP의 프로젝트는 웹 어플리케이션 보안에 큰 기여를 했다고 할 수있다. 아래는 OWASP에서 제시한 가장 심각한 10가지 웹 어플리케이션 보안 취약점이다.

- 입력값 검증 부재
- 취약한 접근 통제
- 취약한 인증 및 세션 관리
- 크로스 사이트 스크립팅(XSS) 취약점
- 버퍼 오버플로우
- 삽입 취약점
- 부적절한 에러 처리
- 취약한 정보 저장 방식
- 서비스 거부 공격 (Denial of Service)
- 부적절한 환경 설정

OWASP는 10가지 가장 심각한 웹 어플리케이션 취약점 및 데이터베이스 보안 취약점, 그리고 이 문제들을 해결하는 가장 효과적인 방법에 대한 자료들을 제공하고 있다. 어플리케이션 보안은 종종 간과되고

* 한국과학기술원 ({yslee, shcho}@dependable.kaist.ac.kr)
** 한국과학기술원 (jsseo@salmosa.kaist.ac.kr)
한국정보보호학회 조기경보시스템연구회 WG12 "웹 어플리케이션 보안 시스템" 운영자

있지만 네트워크 보안만큼이나 중요한 문제이다. 모든 기업들이 여기서 언급되는 일반적인 취약점들을 없애고자 노력한다면 기업환경과 인터넷은 매우 안전해질 것이다. 본 논문의 구성은 제2장에서 웹 환경 어플리케이션 취약사례를 설명하고, 제3장에서는 웹 어플리케이션 보안을 위한 접근 방법인 취약성 분석을 4장에서는 침입 탐지 기법에 대해 살펴보겠다. 5장에서는 결론을, 그리고 6장에서 WG12에 대한 간단한 소개로 마친다.

II. 웹 어플리케이션 취약점

1. Hidden Manipulation

Hidden Manipulation은 입력값을 수정할 수 있다는 웹 어플리케이션의 취약점을 이용한 것이다. 이를 이용한 공격들은 제품의 가격을 변경하여 원래 값보다 싸게 사는데 이용되었다. 그림 1은 $129.35제품을 Hidden Manipulation을 이용해서 $1.95에 사는 공격의 과정을 보여주고 있다.

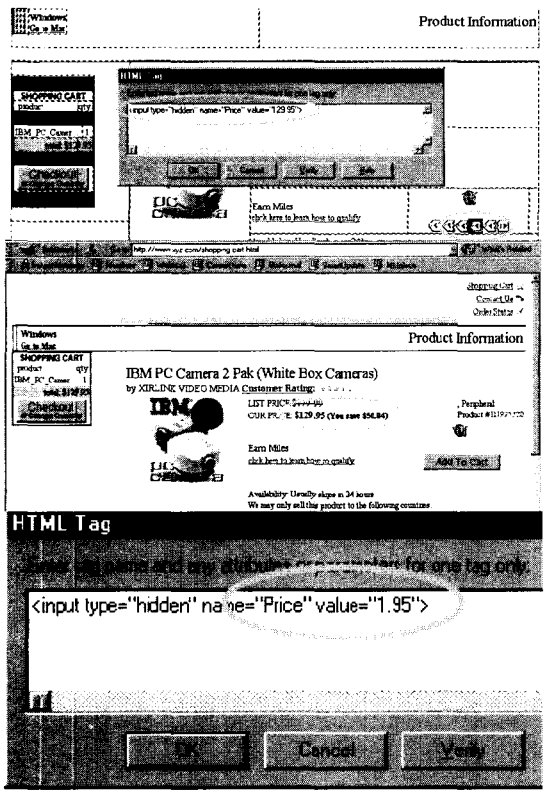


그림 1. Hidden Manipulation의 예

2. SQL Injection 공격에 의한 홈페이지 관리자 권한 획득

SQL Injection 공격은 모든 웹 어플리케이션 환경이 SQL 요청과 같은 외부 명령어 실행을 허용한다는 취약점을 이용한 공격이다. 악의적인 SQL 명령어를 삽입함으로써, 공격자는 웹 홈페이지 관리자 권한을 획득한다. 이 공격 기법은 수행하기 어렵지 않으며 해당 취약점을 찾아주는 다양한 툴들이 지속적으로 발전해나가고 있다. 이 공격의 예를 들어보면, 홈페이지의 ID, Password입력부분에 "OR 1=1"을 입력할 경우 '1=1' 이 항상 참이므로 ID나 Password를 몰라도 홈페이지 관리자 권한을 획득할 수 있다. 이는 SQL 쿼리를 조작하여 where절에 비교식을 더 집어넣음으로써 (이 예에서는 "OR 1=1") 인가받지 않은 데이터를 획득하거나 조작하는 방법이다.

3. XSS (Cross Site Scripting)

XSS라고 불리우는 크로스 사이트 스크립팅(Cross Site Scripting)은 사용자의 입력을 받아들여서 별도의 입력값 검증 없이 반환하는 웹 어플리케이션의 경우에 찾아볼 수 있는 공격이다. 신뢰되지 않은 공격자로부터 웹서버가 데이터를 받아 이를 다른 사용자 어플리케이션에 넘겨주게 되는데, 이 데이터로 인해서 사용자의 어플리케이션에 피해를 준다. 그림 2는 XSS의 예를 보여준다.

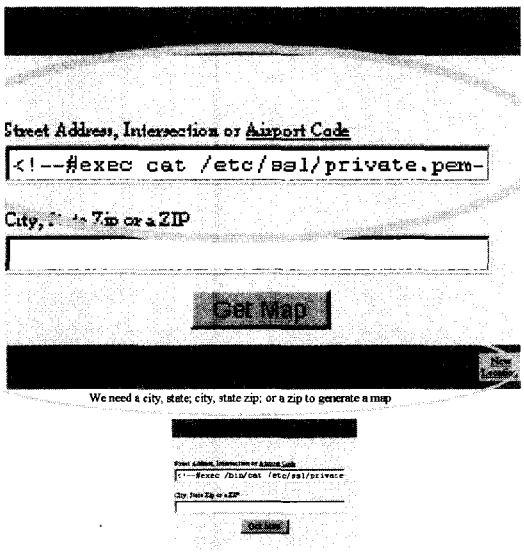


그림 2. XSS의 예

4. 파일 업로드 취약점

일반적으로 웹 서비스에는 게시판이나 자료실과 같은 파일을 첨부하는 기능을 포함한다. 이때 txt, jpg, doc와 같은 파일종류 이외에 악의적으로 제작된 스크립트 파일등의 업로드 및 다운로드를 통하여 해킹에 이용될 수 있다. 악의적인 의도로 제작된 파일을 게시판에 업로드하여 쉘을 실행시켜 공격자의 의도대로 수행되도록 한다.

5. IIS WebDAV 설정 취약점

WebDAV는 MS의 원격 웹서버 파일 관리 프로그램이다. 그림 1과 같이 개발자가 웹 프로그래밍시 홈 디렉토리(wwwroot)를 Everyone에게 쓰기 가능하도록 설정해 놓기 때문에 발생하는 취약점이다. 이러한 취약점 때문에 공격자는 홈페이지 변조가 가능한 것이다. 이러한 취약점을 제거하기 위해서는 wwwroot에서 Everyone의 "쓰기" 권한을 삭제하거나 WebDAV를 사용하지 않는 것이다.

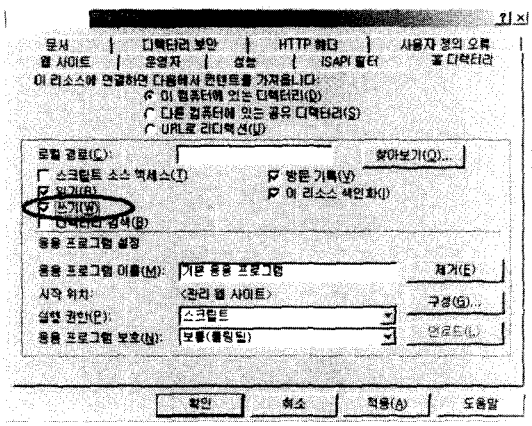


그림 3. WebDAV 설정 화면

6. Unbound File Calls

상위 디렉토리 접근에 대한 통제가 없다는 취약점을 이용하여 민감한 정보가 해커에게 노출 될 수 있다. 예를 들어 게시판 등에 올려진 첨부된 파일의 절대경로가 아래와 같다고 가정해보자.

http://hackerIP/aaa/test.php?file=/data/test_board/test.txt

공격자는 '../'을 이용하여 상위 디렉토리에 접근하는 방법으로 다음과 같이 이용할 수 있다.

http://hackerIP/aaa/test.php?file=../../../../../etc/passwd

'../'에 대해 필터링 하지 않는 경우 위와같이 상위 디렉토리로 접근하여 루트 디렉토리까지 도달 가능하게 되고 패스워드 파일 등의 민감한 정보가 노출될 수 있다.

Ⅲ. 웹 취약성 분석 방법

3.1 웹 취약성 분석 방법

웹 어플리케이션 내에 존재하는 취약점을 분석하는 방법은 크게 2가지로 나눌 수 있다. 한 가지는 어플리케이션 코드 레벨에서 알려진 취약점들을 찾아내는 방법이다. 이 방법은 직접 어플리케이션 코드를 검색하며 알려진 취약점 패턴을 찾아내는 방법으로 속도가 빠르며 정확하다는 장점이 있다. 아래 표 1은 SQL 삽입 취약점이 있는 어플리케이션 코드의 일부이다.

표 1. SQL Injection attack

```
$result = mysql_query("SELECT id FROM
$usr_table WHERE id='$id' and pass='$pass'");

$kid = mysql_fetch_array($result);
If(isset($kid[id]) && $kid[id]!="")
{ login process }
```

이 어플리케이션에 "**HTTP://my.com/login.php?id=admin'--;&pass=123**" 이라는 요청을 하면 내부적으로 mysql_query 문의 파라미터로 "**SELECT id FROM user_table WHERE id='admin'--;&pass and ...**"가 넘겨지게 되고 "--" 문 뒤는 SQL 문의 주석으로 처리되어 결국 admin 계정의 사용자로 로그인된다. 이런 공격을 탐지하기 위해서는 어플리케이션 코드 레벨에서 프로그래밍 분석이 필요하게 된다. mysql_query라는 함수의 파라미터에 사용되는 변수들 ($usr_table, $id, $pass) 중에서 $usr_table은 상수로부터 정의되는 변수이다. 하지만 $id, $pass 변수는 사용자 입력으로부터 받아들여져서 msyql_query 함수의 파라미터에 바로 사용되므로 위험한 취약점을 내포하는 원인이 된다. 이와 유사한 취약점으로는 Stealth Commanding 취약점, Scripting Attack 취약점 들이 있으며, 이들의 원인이 되는 함수 - 예로 php의 경우 mysql_query(), exec(), passthru(), ... 등 - 들

에 대한 데이터 흐름 분석이 필요하게 된다. 같은 방법으로 Cookie Poisoning 취약점, Content Manipulation 취약점, Hidden Value Manipu- lation 취약점은 특정 데이터가 웹 클라이언트에서 변조됨으로서 발생하게 되고 클라이언트로의 데이터 흐름을 분석하여 취약점 분석을 수행할 수 있다.

두 번째 방법은 어플리케이션에 직접 공격을 시도하여 취약점 여부를 찾아내는 방법이다. 전자의 방법이 수동적인 방법으로 취약점을 찾아낸다면 이 방법은 적극적으로 공격을 시도하고 성공 여부로 취약점의 존재 여부를 탐지해 내는 방법이 된다. 예를 들어 사용자 입력 부분에 긴 문자열을 삽입하여 서비스 에러가 발생하는지 여부를 통해 Application Buffer Overflow 취약점이 존재하는 지를 검사할 수 있다. 이런 검사 항목으로는 주로 BoF취약점, Weak Password 취약점, SQL Injection 취약점, XSS 취약점, Directory/File/System Information Indexing 취약점, .bak/.log/.org 백업 파일 누출 취약점, 알려진 CGI 취약점, Script Insertion 취약점 등을 검사할 수 있다. 이 방법의 취약점 검사는 어플리케이션 소스 코드를 알지 못하여도 취약점 분석을 수행할 수 있다는 장점이 있지만, 취약점 분석 도구가 오히려 웹 공격을 수행하기 위한 도구로 오용될 수 있다는 단점이 있다.

Ⅳ. 웹 어플리케이션 침입 탐지 기법 연구

웹 어플리케이션 IDS를 흔히 산업계에서는 Content Filter혹은 Application Firewall의 일부로 보고 있는데, 이를 포함한 Content Security 시장

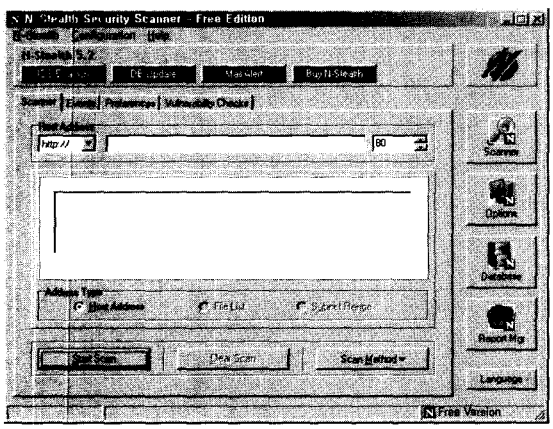


그림 4. 웹 취약점 분석도구 N-Stealth

표 2. 해외 출시 Content Security 제품

개발사	제품명
8E6 Technologies	TurboPipe NP
Akonix Systems, Inc	Akonix L7 Enterprise
Breach Security	BreachGate
Cerberian, Inc.	Blue Coat ProxySG
CLEARSWIFT	MIMEsweeper ™
Imlogic	IM Manager ™
IronPort Systems	IronPort Messaging Gateway ™
NetContinuum, Inc	NC-1000
SAGE, Inc.	BRICKServer®
Sentryware	HIVE
Solinus,Inc	MailFoundry ™
SurfControl	SurfControl RiskFilter ™
Teros	Teros Gateway
Websense, Inc.	Websense Enterprise®
BorderWare Technologies Inc	MXtreme Mail Firewall

은 2004년 Gartner 보고서에 따르면, 2007년까지 매년 16% 이상의 고성장을 지속할 것으로 전송된다. Content Security 분야는 과거의 어플리케이션 방화벽에서 발전되었으며, 각각의 어플리케이션을 흔히 웹, 이메일, 메신저 등으로 나누는데, 국내의 경우 대부분 바이러스, 웜, 스팸 등에 메일 부분에 비중을 두고 있는 편이다. 웹 어플리케이션 IDS의 경우 표 2에 소개된 바 있는 제품들이 국내에 공급되는 상황이다.

웹 어플리케이션 IDS의 접근 방법은 기존의 전통적인 네트워크 기반의 침입 탐지 기법과 동일하게 특정한 시그너쳐의 패턴을 탐지하는 오용 탐지 기법들이 주로 활용되었으나, 웹 어플리케이션의 복잡성과 다양성등의 원인으로 인해 비효율적이다. 대표적인 공개 IDS인 Snort의 경우에도 전체 탐지 시그너쳐의 상당 부분을 CGI스캐닝을 포함한 전형적인 패턴을 찾는 방식으로 접근하였다. 이 경우 요청 형태에 변형이 발생하거나, 새로운 형태의 웹 취약성 악용 시도가 있을 경우 대응하지 못하는 근본적인 한계를 가지게 된다.

최근에는 프로파일을 통한 이상 탐지도 많이 시도되고 있는데, 일부 제품의 경우 웹 어플리케이션과 연동되는 SQL서버 등의 로그 등을 연관 분석하여 비정상적인 행위 등을 탐지하는 기능을 가지고 있다. 이는 기존의 패턴 기반의 접근 방법이 가지는 한계인 변형되거나 새로운 형태의 공격에 대한 대응 능력 부족과, 이상 탐지 기법이 가지는 False positive의 비율을

적절히 개선하고 있다. 예를 들어, 웹 요청에 대해 프로파일링을 통해 이상이 탐지될 경우, 좀 더 정확한 판단의 위해 SQL서버의 상태나, query특성들도 고려하여 결론을 내려준다.

학계에서는 초기에, 호스트 중심이 아닌 네트워크 관점에서 네트워크 트래픽의 이상 현상을 통계적으로 탐지하려는 시도로 진행되었는데, 주로 IP패킷의 헤더 값의 비정상적인 분포를 탐지하고 있다. 대표적인 연구로서 Mahoney[5]과 Krugel[6]의 연구가 있다. 물론 이러한 시도는 시그너쳐를 이용하여 비교적 정확히 어떤 공격인지 탐지하는 오용 탐지에 비해 특정 공격 현상을 명확히 설명하지는 못하지만, 알려지지 않은 새로운 현상들의 발생을 탐지해 낼 수 있다는 장점을 가지고 있다. 또한 이들의 연구는 네트워크 계층에서 네트워크 패킷의 헤더 상의 이상 유무를 파악하는데 초점을 두었고 이를 통하여 최근에 유행하고 있는 웜 기반의 다양한 변형의 분산 서비스 거부 공격을 효과적으로 탐지할 수 있는 기반을 마련해 주었다.

Mahoney[5]는 IP패킷의 헤더 값을 프로파일링하기 위해 패킷마다 패킷 이상 점수를 산출한다. 패킷 이상 점수는 패킷 필드의 각 값을 1~4 bytes로 나타낸 후 이들에 특정한 해쉬값을 적용하거나 클러스터링을 통해 얻은 값을 이용하여 패킷 내의 필드 값의 발생 확률이 낮고, 최근 발생기간이 오래될수록 즉, 최근에 발생한 적이 없을수록 이상 점수가 높도록 설계하였다. 공격이 없는 상태의 데이터를 가지고 일정 기간 트래픽을 분석한 후 공격이 있는 일정 기간의 데이터의 트래픽을 대조하여 공격을 탐지하는 방법으로 실험을 진행하였다. 이들은 이러한 식으로 패킷 이상 점수를 산출하여 DARPA의 IDS평가 데이터로 실험한 결과, 우수한 성능을 보여주었으나, IP패킷 필드의 값만 이용하기 때문에 패킷의 데이터(payload)에 들어있게 되는 HTTP나 SMTP과 같이 어플리케이션 레벨에서 이루어지는 공격의 탐지가 불가능하다는 단점을 가지고 있다.

Krugel은 빈도가 낮은 서비스 요청일수록, 그리고 요청의 길이가 평균보다 클 경우에 침입으로 판단할 확률을 높게 평가하였다. 또한 요청의 데이터 부분의 값의 분포 역시 빈도순으로 정렬하면, 일반적인 상태에서는 그 감소폭이 비교적 완만하나, 비정상적일 경우 특정 값의 분포가 급격히 늘어났기 때문에 감소폭이 상당히 급함을 볼 수 있으므로 분포의 유사성을 이상 점수에 반영하였다. 이는 님다 웜 공격의 예에서도 확인할 수 있는데, 공격은 쉘 코드를 서비스 요청 시

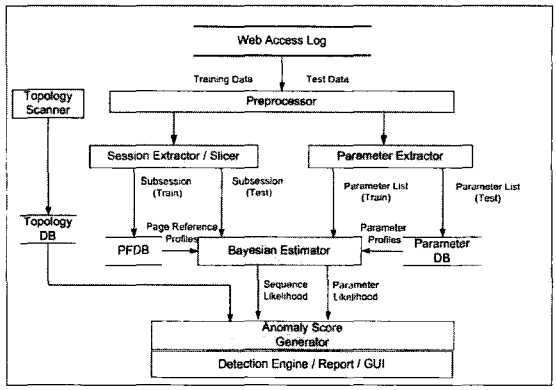


그림 5. SAD 구조도

데이터 부분에 넣어서 보내기 때문에 공격 코드의 특정 문자값들이 일시적으로 많이 증가하는 것을 볼 수 있었다. 한편, 기존의 시그너쳐 기반의 침입 탐지 시스템은 대표적인 SQL Injection 공격을 탐지하기 위한 시그너쳐로 입력값에 '문자가 들어올 경우 이를 필터링하는 방법으로 대응할 수 있는데, 필요에 따라서는' 문자를 사용해야하는 어플리케이션도 있기 때문에 곤란한 면이 있다.

이러한 앞서의 두 가지 예 에서처럼 웹 어플리케이션 공격은 다양한 원인과, 특성을 가지고 있기 때문에 기존의 시그너쳐 기반의 방법에서와 같이 특정한 패턴을 찾아내기 곤란하며, 오히려 웹 어플리케이션이에게 전달되는 파라미터 값의 형태를 프로파일링 하는 것이 필요하다.

Krugel[7]의 연구에서는 각 웹 어플리케이션 모듈에 전달되는 파라미터 값의 길이, 값의 문자 분포, 파라미터 변수의 존재 유무 등의 특징을 활용하여 이상 탐지 시스템을 만들었으나, 현재까지 알려진 일부 공격(Buffer Overflow, Code Red)의 특성에만 초점을 잡고 있다. 따라서, 향후 발생 가능한 파라미터 값의 변형을 통한 공격에는 대응하기 곤란하다.

한편, 국내에서는 SAD[8]연구에서 웹 어플리케이션 콘텐츠의 요청 순서나 전달 파라미터의 유형을 프로파일링하여, 비정상적인 순서를 보이는 요청 혹은 기존의 요청과는 다른 형태의 파라미터를 전달하는 연결을 탐지하는 방법으로 접근하고 있다.

V. 결 론

웹 어플리케이션의 복잡성과 다양성 그리고 이를 활용하는 인프라의 대중화로 인해 웹 어플리케이션 보

호를 위한 노력이 많이 요구되고 있다. 그러나, 국내의 경우 주로 외산 제품에 의존하며, 자체의 솔루션 확보에는 아직은 부족하다고 볼 수 있다. 특히 웹 어플리케이션의 취약성 분석 등은 많은 기반 지식을 요구하기에 국내외적인 지식 공유 특히 웹 프로그래밍 개발자와 보안 연구자들간의 교류를 통해 사전에 취약성을 발견하고 대응할 수 있는 여건이 마련되어 져야 한다. 특히 웹 어플리케이션 보안에 대한 접근 시도는 기존의 범용 침입 탐지 시스템과는 다른 형태의 이슈가 많이 발생하는데, 이를 위해 산, 학, 연의 밀접한 공동 연구가 요구된다.

Ⅵ. WG 12 소개

한국조기경보포럼의 WG 12는 최근 들어 가장 큰 이슈로 등장하고 있는 웹 어플리케이션을 보호하기 위한 취약성 분석 기법 및 침입 탐지 방법을 연구하는 한 분과이다. 이 분과에서는 국내외적으로 새롭게 등장하는 웹서비스 관련 취약성을 분석하고, 이에 대한 효과적인 대응 방법을 연구하고, 보안 연구자, 보안 서비스 제공자, 웹 개발자 그리고 웹 서비스 관련 종사자들간의 폭넓은 정보 공유를 목표로 하고 있다.

⊙ 연구 방향
- 국내외 웹 어플리케이션 취약성 분석 기법 및 도구 분석
- 국내외 웹 어플리케이션 IDS (contents security)접근 기법 연구 및 제품 특징 분석
- 효과적인 웹 관련 취약성 분석 기법 및 침입 탐지 기법의 제안

⊙ 분과 운영
- 월 1회 오프라인 모임 및 온라인 모임을 갖고 연구 주제를 토론
- 희망 과제를 부여하고 자유롭게 발표

참 고 문 헌

[1] The Open Web Application Security Porject (OWASP) Top Ten Most Critical Web Application Security Vulnerabilities, http://www.owasp.org ,2004

[2] Sanctum, Inc., Web Perversion and Application Manipuation based on Real Cases http://www.sanctuminc.com

[3] 인터넷침해사고대응지원센터 정현철, 최근 웹 해킹 동향, 2004.12

[4] 디지털타임스, "특집-웹어플리케이션 보안", 2005. 1. 18

[5] Matthew V. Mahoney and Philip K. Chan. Phad: Packet header anomaly detection for indentifying hostile network traffic. Florida Tech. CS-2001-4, 2001.

[6] Thomas Toth Christopher Krugel and Engin Kirda. Service specific anomaly detection for network intrusion detection. In Proceedings of Symposium on Applied Computing, March 2002.

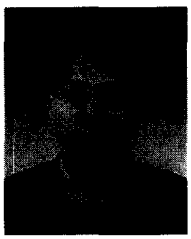
[7] C. Krugel and G. Vigna. Anomaly Detection of Web-based Attacks. In Proceeding of CCS'03

[8] Sanghyun Cho and Sungdeok Cha. SAD: web session anomaly detection based on parameter estimation. Computers & Security Journal, Elsevier Co,. Ltd. May 2004.

〈著 者 紹 介〉

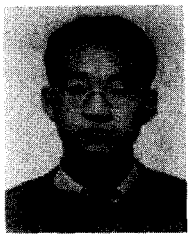
이 영 석 (Young-Seok Lee)

2003년 8월 : 숭실대학교 컴퓨터학부 졸업(학사)
2004년~현재 : 한국과학기술원 전산학과 석사과정
〈관심분야〉 웹 보안, 침입 탐지, 네트워크 보안



서 정 석 (Jeong-Seok Seo)

2001년 2월 : 인하대학교 전자계산공학과 졸업(학사)
2002년 8월 : 한국과학기술원 전산학과 졸업(석사)
2002년 9월~현재 : 한국과학기술원 전산학과 박사과정
〈관심분야〉 웹 보안, 취약성 분석, 이상 탐지



조 상 현 (Sang-Hyun Cho)

1997년 2월 : 고려대학교 컴퓨터과 졸업(학사)
1999년 2월 : 한국과학기술원 전산학과 졸업(석사)
2005년 2월 : 한국과학기술원 전산학과 졸업(박사)
〈관심분야〉 컴퓨터 보안, 침입 탐지, 이상 탐지, 취약성 분석