# Developing Online Self-Training Information Security Program for Web Hosting Administrators Using Virtual System

KIHO LEE, WANSOO LEE, SANGSOO JANG
Korea Information Security Agency,
78, Garak-Dong, Songpa-Gu, Seoul 138-803,
KOREA

*Abstract :* Recently, many enterprises have been providing a web service for the advertisement of their assets or customer relationship. However, they do not have enough human resources due to an insufficient budget and awareness of security. This situation is not really different from the web hosting service providers that manage many websites for customers. In reality, if a web service is attacked, many customers' personal information and companies' confidential information can be disclosed, causing immeasurable damage that cannot be counted in terms of money. This paper describes how to develop a program that enables home page developers and administrators to be trained in methods of preventing new hacking attacks and dealing with viruses

*Key-Words:* Hacking, Viruses, Home page, Web, Vulnerability, Online training

## 1 Overview

It is a fact that most organizations are ready to take effective action against Internet security incidents. It is also true that the persons responsible for information security or system administrators rarely have the chance to apply the incident response skill to the actual system. Even though domestic universities are also aware of the importance of information security and offer regular training courses in order to foster specialists, it is not easy to find a course that provides on-the-job training for incident response.

To address this situation, the Korea Information Security Agency operates the Online Information Security Training Lab, which enables security managers or IT engineers to acquire and apply know-how about hacking/virus prevention and response technology within a short period of time.

The training lab is composed of a vulnerability analysis training space, management and defense training space, spam mail response training space, infringement incident response space, multiple-choice question bank, small and medium enterprises training space, Windows training space, and a Web (home page) training space. It provides various data and services related with information security

### 1.1 Background to and Objectives of Lab Establishment

According to the KISA security report, more than 75% of cyber attacks and Internet security violation incidents are caused by vulnerabilities in Internet web application.

Korea is one of the countries with a widespread high-speed Internet network, established in line with the rapid growth in IT. In addition, the sensitive information data of private enterprises and public agencies have now mostly been computerized, and online bank transactions have increased sharply through Internet banking. Most of these Internet services are provided on the web, and most websites are incorporating an attractive interface, which has resulted in a more complex web application structure of enormous size.

Generally, infringement incidents on the web are attributable to a lack of security review with regard to database access, administrator authentication and user authentication, and a web application design method at the time of web application design

In addition, the web service, unlike other services or Firewall, cannot be protected by the IDS, as attacks mainly occur at the application layer rather than the physical layer. Although the web fire solutions capable of protecting the web server from web application vulnerability have appeared one by one, their functionalities are not robust enough to protect web services in too diverse an environment, and there are many cases where the web server is not protected from vulnerabilities, since the intruder bypasses the web firewall solution using the detour technique.

If the web server is open to infringement incidents, enormous amounts of personal and sensitive

information of both customers and companies risk being disclosed, which could cause immeasurable damage, including the deterioration of public trust in the organization.

There is also a large number of attack techniques related with CGI, as the size of web-related CGI is considerable. Therefore, it is difficult for administrators to detect vulnerabilities and block intrusion by themselves. To assist administrators in getting properly trained, a vulnerable web environment that is actually running is provided, enabling them to experience it in such a way that they can understand the type of attacks launched against the web and the defensive techniques that can be deployed against them.

After the training, administrators can apply security measures in their own web environments. This project is designed to implement a response training system that supports these training exercises.

### 1.2 Contents and Scope of Development

This project opened a training lab for two groups – a Windows series server user group and a Linux series server user group. The training lab was opened for administrators and developers who have experience in developing web services using IIS in Windows series servers, so that they could create a security code for Windows-based ASP script language. For the Linux server user group, the training lab was opened for administrators and developers who run a web server based on the Apache web server and the PHP script language, so that they could learn how to set security and create a security code.

- Communication server between users and training server
  - ✓ Applies a remote control application that is similar to the Windows virtual terminal service.
  - ✓ Applies a program that automatically assigns the developed and available training system to the user.
- Implementation of the training program by scenario
  - ✓ Implements the training scenario in the training environment, using the program.
  - ✓ Implements a Windows-based OS image and a Linux-based OS image.
- Development of a real-time correct answer check function
  - ✓ Users are able to check whether they can defend the attack that corresponds to the question, by making an actual attack on the training web server.
  - ✓ Developed a program that determines whether users have a problem.
- Application of an automatic recovery function
  - ✓ Applied the existing automatic backup and system recovery method.
- Development of a web interface
  - ✓ Added menus and question items to the web server that is currently running.

### 1.3 Development Environment

Tables 1 show the development tools and environment that were designed to implement the learning space system for home page (web) developers and administrators.

Other training labs provide questions that are limited to a specific operating system. However, this training space for home page(web) developers and administrators uses the Windows and Linux operating system as the web servers respectively, thereby reflecting the actual web server operation environment in Korea. In addition, trainees are educated to resolve fundamental problems by modifying the erroneous source code, without using expensive information security products like Firewall or an intrusion detection system.

Table 1 The Development tools and Environment

| System / Program | | Description |
|---|---|---|
| Client PC | O/S | Windows XP Professional (SP2) |
| | Browser | Internet Explorer 6.0 SP1 |
| Delay Server | O/S | Fedora Core 4 |
| | Web Server | Apache-Tomcat-4.1.31 |
| Training Server | O/S | Windows XP Professional (SP2)<br>Fedora Core 4 |
| | Remote Server | TightVNC Program v1.2.9 |

## 2 Technologies Used to Implement the Online Information Security Training Lab

### 2.1 VMWare

The training server uses VMWare (virtual machine) to recover the server and to minimize malicious use. The

virtual PC program VMWare is installed in the Unix/Linux main platform of the training server, while the Windows 2000 Server system is installed as VMWare's virtual machine. To perform remote control of the Windows 2000 Server, the TightVNC server program and a training scenario program are configured and installed.

Since the VMWare solution supports the saving of the virtual machine's state as a file, it can be restored quickly if an error occurs or if the system is broken. Therefore, the training server system can be restored quickly even in the event that the users destroy it, if VMWare is employed in the Windows training space system.

The benefits of using the VMWare solution are that it:

- Is easy to deploy and manage, as it is installed as an application program;
- Is easy to integrate Microsoft Windows and Linux host environment;
- Supports a wide range of host and guest operating systems;
- Support devices inherited from the host operating system;
- Is a Hardware independent virtual machine that provide high portability; and
- Supports advanced clustering.

### 2.2 Technology Related with Remote Control

The remote control technology currently used in the Windows training lab is based on VNC, which is configured to provide the GUI that makes the remote user feel as if he/she is locally connected to the image inside the training server.

The VNC (Virtual Network Computing) is one of the protocols designed to transmit the GUI environment information of the remote computer, as well as the events that users generate locally, such as keyboard and mouse operation.

At present, the TightVNC open source program is in use, which implements the VNC protocol. TightVNC is a remote control freeware package based on the VNC software. TightVNC enables the user to control the graphic desktop environment of the remote PC, using the keyboard and mouse of the local PC.

The benefits of using the TightVNC program include:

- File transmission function
  - ✓ Supports file upload and download between the local PC and the remote PC.
  - ✓ Effective compression algorithm
  - ✓ Users can perform remote control in the network environment in almost real-time, while using a small amount of network traffic.
- Compression mode setting function
  - ✓ The environment can be configured to fit into the connection speed and processor capability, as the compression ratio and the encoding speed can be adjusted.
- Java Applet Viewer
  - ✓ With Java Applet Viewer, the user can access the HTTP server, and control the remote server using the Internet browser.
- 2 password types are supported.
  - ✓ Rights for the remote server can be set by password (full control or read-only).

## 3 Architecture Design of Technology Training Lab

### 3.1 Architecture Design

The entire web education space system is composed of the relay server (including a web server and DB server) and the training server, as described below. Figure 1 shows the hardware and network configuration of the education space system, whereas Figure 2 shows the software configuration.

Fig.1 Hardware and Network Configuration

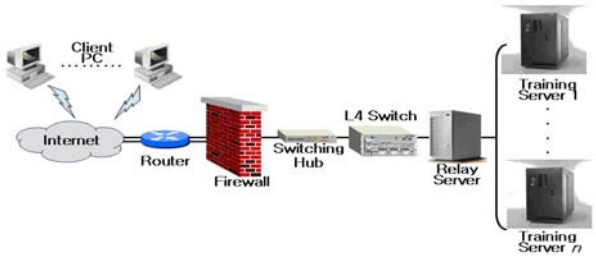
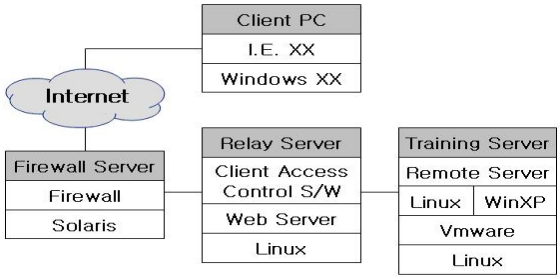



Fig.2 Software Configuration

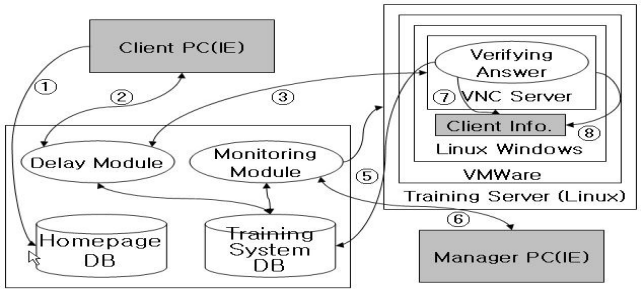



The web education training question is composed of 21 items: 10 Linux-related questions and 11 Windows-related questions. When the trainee accesses

the training server to answer the question, the trainee is automatically logged in to the account that corresponds to the question concerned. The trainee can answer the question and check the correct answer using the answer check program. If the trainee provides the correct answer, the training system database is updated, which can be checked by the relay server.

Figure 3 shows the interface of the web training systems, including the training server, relay server, homepage database, training system database, and the web server.

Fig. 3 Interface of the Web Training Systems




① User login in the SIS home page: Obtains the data required for user authentication from the home page database.

②, ③ Relay between user client and VNC server.

④ Monitoring for the administrator.

⑤ Saves the user's answer status in the user training database of the relay server.

⑥ Invokes the reset function of the training server from the monitoring module.

⑦ The correct answer check program saves/retrieves the user's training information in/from the training server OS.

⑧ TightVNC server programs the information logged-in user as a file.

User management - such as new user registration - is performed by the web server. The trainee can check the questions and answer status by logging into the web server.

## 3.2 Relay Server Module

The relay server module is broadly composed of three parts in this project.

The first part relays packets between the remote control server and the user client viewer. The TightVNC program, the remote control software for this project, has a limitation in that the client viewer cannot access the server if it is located inside NAT or a private IP environment. To solve this problem, the relay module is implemented in the relay server to support communication between the server and the client.

The second part assigns the training server to the user. When the user logs into the system via the web, the server assignment module searches the available training server and connects the user to the proper training server.

The last part is the monitoring module, which enables the administrator to monitor the Windows training system. The administrator can retrieve the system access user status, the training status by the access user, and the status information of the training server, and can also initialize the training server.

Figure 4-5 shows the module configuration diagram of the relay server.

## 3.3 Design of the Question

**Focuses on the vulnerability of OWASP-based web application**

Questions are mainly related with 10 vulnerabilities of the OWASP.

OWASP (Open Web Application Security Project), the international web security association, classifies and defines web vulnerabilities into 10 types. The following figure 4 describes 10 of the vulnerabilities selected by OWASP.

Fig. 4 10 of the vulnerabilities by OWASP

| Client PC | |
|---|---|
| 1. Unvalidated Input | 6. Injection Flaws |
| 2. Broken Access Control | 7. Improper Error Handling |
| 3. Broken Authentication & Session Management | 8. Insecure Storage |
| | 9. Denaial of Service |
| 4. Cross-site Scriting(XSS) | 10. Insecure Configuration Management |
| 5. Buffer Overflows | |

**Several web development environments are considered**

In consideration of the various web development environments, questions are grouped in such a way that the trainee can be trained about vulnerabilities and countermeasures in a Windows-based web development environment and a Unix-based web development environment.

**Focused on the understanding of vulnerabilities**

As with the phrase "To know thy enemy is to win the battle," questions are composed in such a way that the

trainee can understand the reasons behind the occurrence of vulnerabilities, and the possibility of damage to both the system and the database that can arise because of such vulnerabilities.

If the basic concept of vulnerability is not properly understood, a rough estimate is used for security, which will lead to the repetition of damages. Therefore, one question contains two items so that the trainee can understand the notion of vulnerability properly.

**Various difficulties**

Diverse questions are offered – from the question that can remove vulnerability by server setting or simple operation to the one that requires understanding of the problem and manual modification of the source code.

## 4 Conclusion

In conclusion, the security code should be written at the web application development stage, and the developed web application should modify the code to apply security, in order to provide a secure web service. To perform a series of works like this, web developers should be trained so that they can understand general hacking techniques and find solutions to them by themselves. To achieve these objectives, a training space service is needed for home page (web) developers and administrators.

This project was utilized as a user training program for the Online Information Security Training Lab, and was provided to persons working at the web hosting area or home page related developers. This lab created an environment in which users can learn by themselves from actual experience, rather than through a theoretical and abstract approach. Consequently, it provided a base for the fostering of new personnel, and enables trainees to learn how to reduce the damage caused by malicious attackers.

*References:*

[1] Scambray, *Hacking Exposed Web Application*, McGraw Hill, 2006
[2] Mike Andrew, *How to Break Web Software*, Addison Wesley, 2006
[3] Securityfocus, http://www.securityfocus.com
[4] OWASP, http://www.owasp.org
[5] Yoo Gang, *Hacking & Security*, Publishing House, 19XX
[5] Flickenger, Linux Server Hacks, O'Reilly, 2005
[6] Yang Dae Il, *ITCOOKBOOK : Network Hacking and Security*, Hanbit Press, 2003.
[7] Yang Dae Il, *ITCOOKBOOK : System Hacking and Security*, Hanbit Press, 2004.
[8] Park Jae Hong, *NETWORK HACKING & SECURITY*, Hanbit Press, 2003
[9] Scambray, *Hacking Windows Server 2003 Exposed*, McGraw Hill, 2003
[10] McClure, *Hacking Exposed*, McGraw Hill, 2005
[11] Scambray, *Hacking Exposed Web Application*, McGraw Hill, 2006
[12] KISA Homepage, http://www.kisa.or.kr