

PAPER • OPEN ACCESS

The design and implementation of network attack and defense platform based on cloud desktop

To cite this article: Zining Yan *et al* 2017 *J. Phys.: Conf. Ser.* **887** 012038

View the [article online](#) for updates and enhancements.

You may also like

- [Testing the quality of images for permanent magnet desktop MRI systems using specially designed phantoms](#)
Jianfeng Qiu, Guozhu Wang, Jiao Min et al.
- [Application of improved PSO to attack–defense decision models in power systems](#)
Ying Ling, Ming Xie, Jieke Lu et al.
- [Research on application of cloud desktop virtualization for computer laboratories in universities](#)
Qiufeng Yao, Yanbo Wu and Jiangming Gao

The design and implementation of network attack and defense platform based on cloud desktop

Zining Yan¹, Yunhan Wang², Shijiao Shao³ and Boquan Li⁴

¹Embedded System Lab. College of Computer Science and Technology, Harbin, China, E-mail: 954277966@qq.com

²Embedded System Lab. College of Computer Science and Technology, Harbin, China, E-mail: 2224206409@qq.com

³Embedded System Lab. College of Computer Science and Technology, Harbin, China, E-mail: 769351769@qq.com

⁴Institute of Information Engineering Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences

Key Laboratory of Network Assessment of Technology, Chinese Academy of Sciences, Beijing, China, E-mail: liboquan@iie.ac.cn

Abstract. This paper discusses the cloud desktop technology, virtualization technology and penetration testing technology used in the network attack and defense training platform, and introduces the design and implementation process of the network attack and defense training platform. This paper focuses on the cloud desktop construction scheme based on B/S structure, and aims to enhance the flexibility and convenience of network attack and defense training platform.

1. Introduction

Network security incidents occur frequently so that the importance and key of network security are self-evident, to enhance the network attack and defense technology is the most effective means to prevent and solve the problem of network security. In order to improve the network attack and defense technology, the country has opened the research and construction of network shooting field, the United States has launched "cyberspace Manhattan Plan" with a budget up to 30 billion dollars, the US Defense Advanced R & D Program launched the "National Cyber Range" [1], to provide training and training field for the US network attack and defense. For China, network security has gradually become an important issue associated with national military and economic development. Therefore, to construct the network attack and defense exercise system and to enhance security technician's network attack and defense capabilities, is an important foundation for the construction of China's network information security.

Though we have done much research in the field of network attack and defense exercise platform at home and abroad, there are still some ubiquitous problems among the existing platform, like too elaborate to operate, excessive construction costs, maintenance difficulties and etc. On account of the above problems, this paper uses the XenServer system as the underlying virtualization server system to build the cloud desktop based on the B / S structure and realizes the network attack and defense exercise platform based on the cloud desktop. The user can operate the remote desktop through browser so as to reduce resources, and enhance the flexibility and convenience of the offensive and defensive exercise platform.



Section 1 of this paper introduces the research background and significance of this subject. In Section 2, the key technologies such as penetration testing technology, virtualization technology, and cloud desktop technology are studied. Section 3 introduces the remote control technology of cloud desktop based on B / S Structure, analyzes the construction of virtual environment based on XenServer, and the realization process of cloud desktop platform based on B / S Structure. Section 4 describes the process of the design and implementation of the exercise system, Section 5 analyzes the platform function and performance tests.

2. Key Technical Analysis

2.1. Penetration Testing Technology

Penetration testing exercise system is the most common way of network attack and defense exercise. The network penetration test is a method of evaluating the security of a computer network system by simulating a malicious hacker's attack method. The security technician detects the network security from the attacker's point of view [2] and takes the initiative to analyze the system vulnerabilities, defects, and other weaknesses. A penetration test can effectively check out the existence of network security problems, help to block the attack that the network may be suffered, so that network security is more secure.

The process of penetration testing is similar to the hacker attack process and requires vulnerabilities or technical flaws in exploiting the system. Testers need to exploit vulnerabilities or defects to carry out penetration testing while ensuring the least destructive nature of the network environment and target systems. Penetration testing is a step-by-step process with a certain rule [3].

A penetration test can not only detect whether the protective measures of the target system are perfect but also can restore the security problems existing in the system. Testers can solve the problem in time according to the test results and adjust the repair mode in time to provide a reliable basis for the safety protection mechanism of the target system.

2.2. Cloud Desktop Technology

2.2.1. Cloud Desktop Technology Introduction. Cloud desktop technology is the user's desktop environment associated with the terminal equipment, the complete desktop environment stored in the server. Users can access remote desktops with other end devices that can connect to the network [4]. Cloud desktop technology will put all the resources processing into the background server, the system maintainers through the background allocation center manage a variety of desktop unify, this process reduces the system maintenance time and workload, while control management of the desktop set enhances system security. Cloud desktop technology schematic diagram is shown in Figure 1.

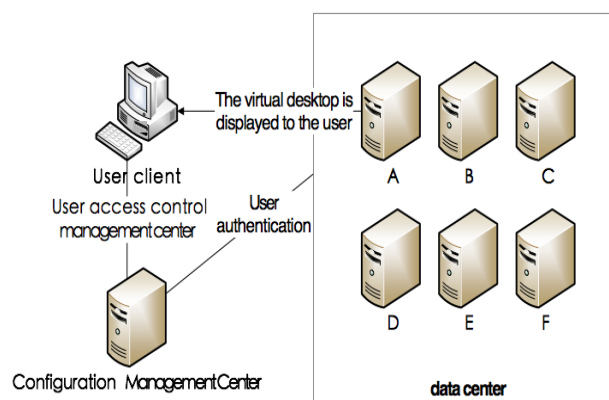


Figure 1. Cloud desktop technology schematic

As can be seen from the figure, the principle of cloud desktop technology is mainly: the user through the terminal equipment use the network connection to the configuration management center, configuration management center will verify the identity of the user, if verified through, the user will access the data center server to access and control Remote cloud desktop [5].

2.2.2. VNC remote control tool. When a user accesses a remote cloud desktop, the client needs to support the Remote Desktop Protocol for the purpose of controlling cloud desktop access. VNC (Virtual Network Computing) protocol is a remote control to achieve the remote desktop protocol, which provides a remote management function that displays the entire desktop of the remote server on the client side. VNC remote control tool based on C / S (Client / Server) architecture, made up of the VNC Server and VNC Viewer two parts. The schematic diagram is shown in Figure 2.

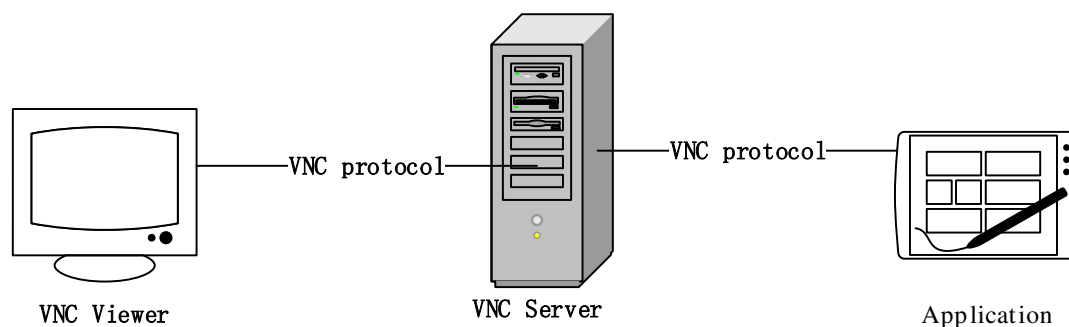


Figure 2. Remote control tool schematic

As can be seen from the above figure, VNC Server allows the application in the system to run on the desktop of the VNC Server through the X protocol, so that the user client installed VNC Viewer can access and control the remote desktop through the VNC protocol. The nature of VNC Viewer is a monitor program, through the VNC protocol, the user client's monitor program can communicate with the remote server, and the server connect to a number of hardware devices and run a number of applications, so Users can monitor and operate the hardware and applications of remote desktops with VNC Server [6].

2.3. Xenserver Server Virtualization Solution

Server virtualization technology is the process of abstracting the physical resources of a server into logical resources, isolating a server into multiple virtual servers, or merging multiple servers into a single server [7]. Server virtualization technology to achieve the CPU, memory, I / O, disk, and other hardware dynamic management, improve the utilization of resources, so that the system management is more flexible and simpler.

XenServer is a server virtualization solution of standalone virtualization [8]. The underlying layer is based on Linux, so XenServer is also a special Linux system. XenServer has the advantages of compatibility and security, source code opening and free features [9], so it is widely used by companies or research organizations for critical applications or secondary development.

XenCenter is a tool for managing XenServer that can operate easily the creation, start, stop, and generation of virtual machine lifecycles. The graphical interface interacts well with users. The XenServer virtualization solution efficiently completes the goals that server virtualization needs to meet, allowing enterprise, individuals or any user to use.

3. Cloud Desktop Platform Based On B/S Structure

3.1. Cloud Desktop Remote Control Technology based on B/S Structure

The remote control technology of cloud desktop based on B/S structure is mainly realized by Guacamole project. Guacamole is a WEB application based on HTML 5. Users can access the Web application in the server through a browser and access and control the remote desktop in conjunction with the Remote Desktop Transport Protocol (VNC or RDP) or Remote Login Session Protocol (SSH). Its working principle is shown in figure 3.

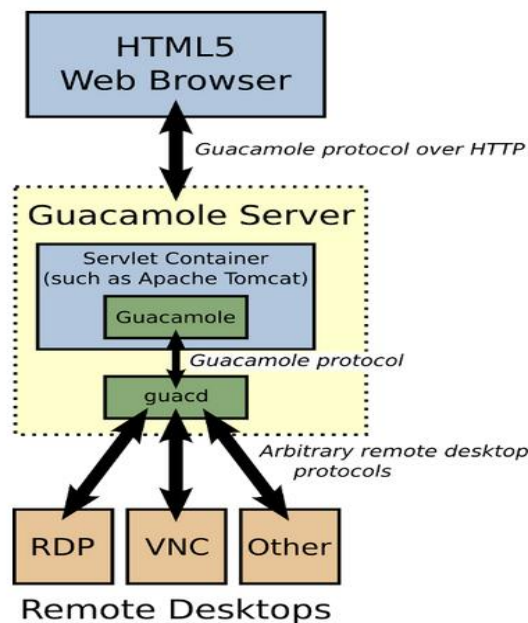


Figure 3. Guacamole working schematic

As can be seen from Figure 3, when the users visit Guacamole server through the browser, Guacamole server with WEB application server (such as Apache Tomcat) provides services to users. Guacd helps to deploy the application in the Guacamole server to parse the Guacamole protocol and helps to identify which desktop transport protocol (RDP, VNC, etc.) is used for remote desktop applications. When each step goes smoothly, the user can communicate with the server via HTTP.

In the Guacamole project, the Guacamole protocol is a remote display and interactive protocol that is responsible for displaying and rendering messages, web applications deployed in the Guacamole server allow the application itself to support other desktop transport protocols (RDP, VNC, etc.) by parsing the Guacamole protocol. WEB application is written in Java, front-end is realized by html5 and java script implementation, the WEB application cannot achieve any desktop protocol by itself, but rely on the entire project core Guard (plug-in dynamic support Remote Desktop Protocol) to resolve the Guacamole protocol and identify other desktop transport protocol.

The desktop transform protocol used in this topic is the VNC protocol. Guacamole replaces the VNC Viewer in the VNC remote control tool with a browser, allowing users to access remote desktops with any operating system or even mobile devices.

3.2. The Construction of Cloud Desktop Platform

3.2.1. Server virtualization environment. The network attack and defense exercise platform need to provide each user with the same desktop environment so that each user can conduct network attack and defense exercises in the same environment. Server virtualization technology achieves to divide a server into a number of virtual servers and assign to each user a virtual machine. While using XenServer virtualization solutions for virtual machine cloning and porting and other functions, a well-deployed exercise environment is cloned into a number of exercise environment to achieve the same conditions for each user's exercise condition. The server virtualization environment architecture is shown in Figure 4.

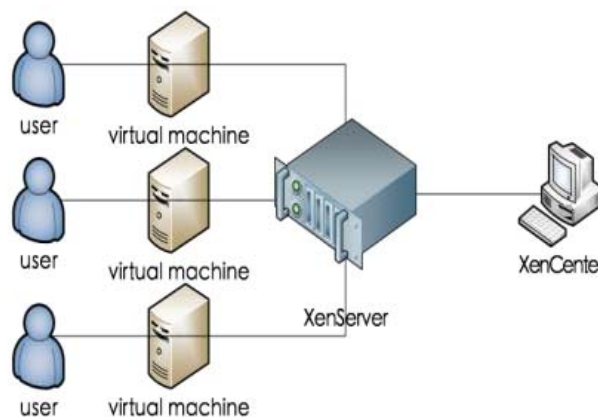


Figure 4. Server Virtualization Environment Architecture

3.2.2. WEB application server. A key link of the construction of the cloud platform based on the B/S structure is to realize the remote cloud desktop access through the browser. The cloud desktop is evolved into a WEB application, through accessing to WEB applications to indirectly access the remote cloud desktop. This topic uses Guacamole to connect the browser with VNCServer and uses Guacamole Server as the medium to access and control the remote cloud desktop through VNC remote desktop protocol.

WEB application server store the application and data files for the network attack and defense exercise platform, providing online information browsing service, which is the system and user interaction hub, but also for the entire network attack and defense exercise platform design and implementation laid the foundation.

4. Design and Implementation of Exercise System

4.1. Vulnerability Database

Vulnerabilities are the root of the system and application security issues. Therefore, the construction of the exercise system vulnerability database is the basis of system development. The vulnerability database should contain the basic information, characteristics, hazards and protection programs of the security vulnerabilities. The vulnerability database has some reference value to the research of the penetration test technology and the network attack and defense technology. At the same time, it can help the attack and defense technician to master the characteristics of the vulnerabilities better and develop the corresponding repair plan according to the characteristics of the vulnerabilities, and also can have some guiding effect on the system protection.

Based on the investigation of the main security vulnerabilities involved in the current penetration test, this system has constructed a database of typical vulnerabilities including brute force, command execution

vulnerability, cross-site request forgery, SQL injection, file upload vulnerability, cross-site scripting attack, etc. The vulnerability database contains two parts, the document, and program. The documents and programs in the vulnerability database will be directly applied to the development of the exercise environment, which make the system's development and operation more flow and formal. It is the basis of the system exercise function. The construction of the vulnerability database is a continuous process, with the update and development of applications, vulnerabilities should continue to add the newly discovered vulnerabilities.

Through the collection, programming, writing documents and other processes to build typical vulnerabilities in the exercise process, and develop the corresponding exercise environment for each vulnerability by using PHP language, the program, and documentation contained in the vulnerabilities database will be applied directly to the development of exercise system and exercise environment. The main vulnerabilities currently contained in this project are shown in Table 1.

Table 1. Network vulnerability typical vulnerability information table

Vulnerability name	Vulnerability description
Brute force	Test continuously the system password or command and other verification information for several times, until you use the correct authentication information to log on to the system.
Command execution vulnerability	Through the browser to the function filter does not submit the implementation of the order, causing the attacker by changing the system path or other program environment.
Cross station request forged	The use of the site to the browser's trust, the temptation of users in the WEB application has been registered on the implementation of non-intended operation.
SQL injection	Enter the malicious SQL statement in the Web form to get the data in the server database.
File upload vulnerability	Upload files that contain malicious code and be executed by the server by using the Upload File feature.

4.2. Penetration Test Exercise Environment

Penetration test exercise environment includes six typical vulnerabilities: Brute force, command execution vulnerability, cross-site request forgery, SQL injection, file upload vulnerability, and cross-site scripting. Each vulnerability achieves low-level and advanced two exercise environments according to the degree of filtering. Each vulnerability is specifically designed and implemented as follows:

The main way of brute force is to guess the password for the system and other authentication information and try a number of logins until you enter the correct authentication information log on the system or get important data. The exercise environment of brute force vulnerability is a basic form that contains only the username and password. When the user enters the correct username and password, the user is prompted passing, the system will give a prompt when the username and password do not match. Users can help brute force through the system's pre-provided Brute tool.

The exercise environment of brute force sets the difficulty based on the degree of filtering of the characters entered in the form. The main code for filtering user names and passwords for special characters is as follows:

```
$user = mysql_real_escape_string( $user );
$pass = mysql_real_escape_string( $pass );
```

The system uses the `mysql_real_escape_string()` function to escape special characters in the string

used in the SQL statement, which filters out the special characters to increase the difficulty of brute force.

The exercise principle for the command execution vulnerability is through the browser to submit an execution command to the server that does not filter functions, which cause the attacker to change the system path or other program environments. An exercise environment is a form that prompts for an IP address. The system feeds back related information to users based on user-submitted commands.

In command execution vulnerability exercise environment, the input comment is not filtered by low difficulty level. With the difficulty level increasing "&&", ";", and other characters are filtered out. The main code for filtering the input characters is as follows:

```
$substitutions = array ('&&' => "&&", ';' => ";");
```

```
$target = str_replace(array_keys($substitutions), $substitutions, $target);
```

The system will add special characters to the blacklist, when the user input sensitive characters, it will automatically replace the sensitive characters so that the input command of the system will not be able to perform.

The main principle of cross-site requests forgery vulnerabilities is to take advantage of the site's trust in the browser and entice the user to perform unintended operations on the logged-in web application. An exercise environment is a form that prompts you to change the password, and the system feeds back the correct password to the user according to the correctness of the user's password.

The exercise environment of cross-site request forged vulnerabilities, any judgment for the input content is not made by the exercise environment at the low difficulty level, the password can be changed whether the original password input is right or not. The environment at the high level using the specific functions to determine the source of the request. The main source of the judgment of request source is as follows:

```
If (ereg ("127.0.0.1", $_SERVER ['HTTP_REFERER'])) {}
```

High-level difficulty using \$_SERVER ['HTTP_REFERER'] function judge the source for the user request, so that users need a certain means to modify the password.

The SQL injection vulnerability is done by entering a malicious SQL statement in the Web form to get the data in the server database. An exercise environment is a form that prompts the user to enter an ID, where the system feeds back the information to the user according to the ID entered in the database.

Similar to the command execution vulnerability, the SQL injection exercise environment also sets the difficulty by filtering special characters. The main code for filtering characters is as follows:

```
$id = mysql_real_escape_string ($id);
```

The system through the MySQL built-in escaping function filter special characters, the user needs to bypass the escape function in a way for SQL injection attacks.

The main way of file upload vulnerability exercise is uploading the file, which contains malicious code and can be executed by the server, to the server through the way that application upload files. The file is executed by the application to achieve the purpose of malicious attacks. The file upload vulnerability exercise environment provides an entry for uploading files and submitting, and the system stores the files uploaded by the user to the server.

Difficulty is set by way of whitelist filtering to verify the properties of the uploaded picture or file. The main code for white list filtering is as follows:

```
$uploaded_name = $_FILES ['uploaded'] ['name'];
```

```
$uploaded_type = $_FILES ['uploaded'] ['type'];
```

```
$uploaded_size = $_FILES ['uploaded'] ['size'];
```

```
If (($uploaded_type == "image/jpeg") && ($uploaded_size < 100000)) {}
```

The system first gets the file name, file format, and file size of the uploaded file. If the uploaded file meets the requirements, the file can be uploaded, otherwise the file will not be uploaded.

Cross-site scripting attacks are divided into two types: reflection and storage. The main principle of storage-type cross-site scripting attacks is to enter the malicious executable code to the web form, which makes users access the page that is, execute malicious code, through the browser. While reflective cross-

site scripting attacks have no database connection, the environment is in the form that can directly return the input .after the system execute the malicious code, the successful attack is proved by the pop-up window.

Reflective cross-site scripting exercise environment is a form that prompts for a name. The system will directly feedback the input content to the user in the form.

In a reflection-type cross-site scripting attack, the system uses the `str_replace ()` function to filter out keywords and symbols that may appear in the popup window. Filter Keyword The main code is as follows:

```
Str_replace ('<script>', '', $_GET ['name'])
```

Storage-type cross-site scripting attack environment is a message board. The system will store the name and message content entered by the user in the database.

Similar to the reflective cross-site scripting attack, the system also uses the `str_replace ()` function to filter out keywords and symbols that may appear in the user's name, and the message form uses a relatively complex filtering function. The user needs to first select the form of the attack and try to choose a breakthrough form to attack.

5. System Function Test and Case Analysis

5.1. Functional Testing of Cloud Desktop Platform Based on B/S Structure

This section examines the functionality and performance of the cloud desktop platform with personal computers (desktop or laptop), tablet PCs, and smartphones, and analyzes the test results.

Personal computer access to the cloud desktop test with the Firefox browser. The test results are shown in figure 5.

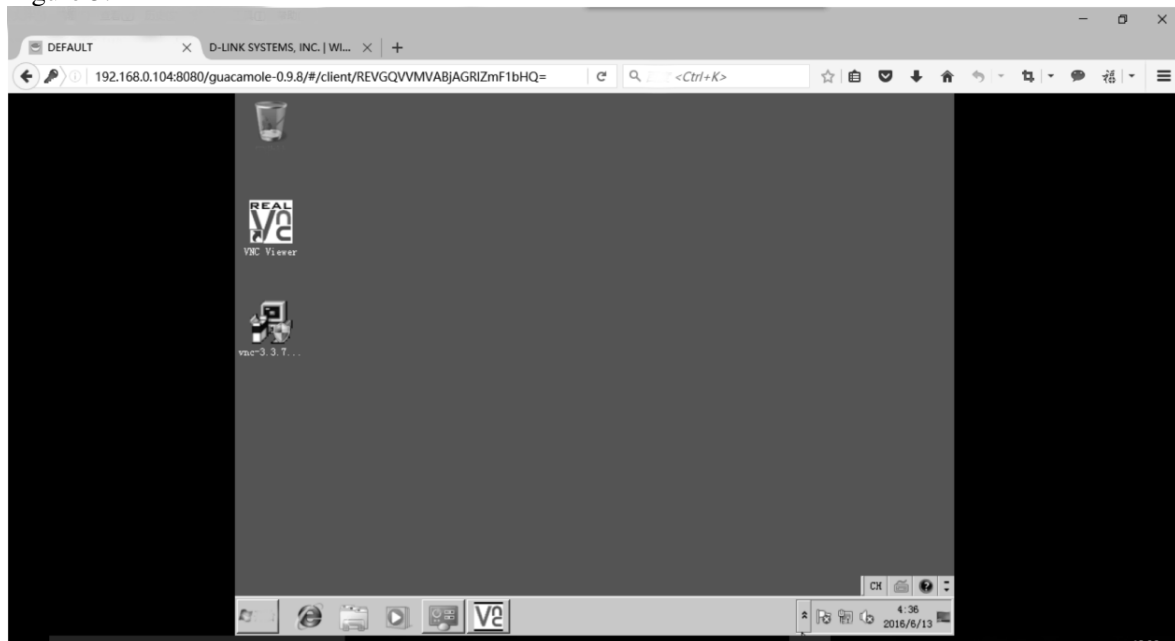


Figure 5. Personal computer visit the cloud desktop interface through the browser

In the test of Tablet PC visiting the cloud desktop, this test with the Tablet PC comes with Safari browser, the test results shown in Figure 6.

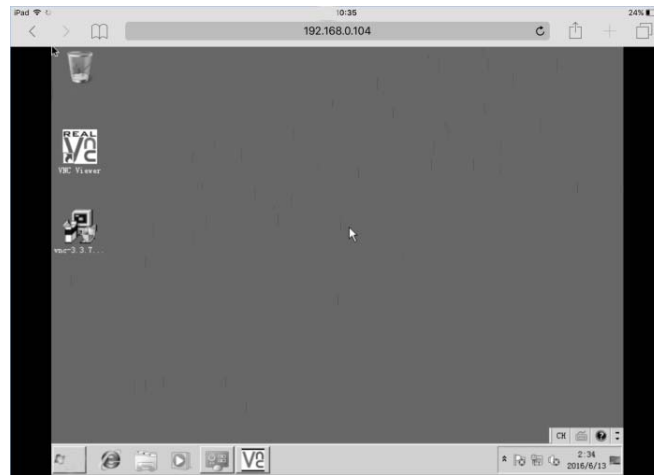


Figure 6. Tablet PC access the cloud desktop interface through the browser

In the smartphone access to the cloud desktop test, the same with the smartphone Safari browser for testing. The test results are shown in Figure 7.



Figure 7. Smartphone through the browser to access the remote cloud desktop

Through the test results can be seen, the cloud desktop platform can be stable on the server to run, and through personal computers, tablet PCs, mobile phones and other devices to access the remote cloud desktop browser, the screen is stable and clear, which achieve the desired results and demand.

5.2. Functional Testing and Case Analysis of the Exercise System

The exercise system is a dynamic website of the B/S structure developed by using the combination of Apache + MySQL + PHP. Its function is mainly to drill up to set the difficulty of the drilling environment and select the appropriate type of vulnerabilities to drill. This section will select the storage-type cross-site scripting vulnerability as an example, to drill the identity of the user login training system, the difficulty set to primary, complete a complete exercise process. The exercise environment is shown in Figure 8:



Figure 8. Storage type XSS attacks interface

Submit the following malicious code to the form:

```
<<SCRIPT>alert ("XSS") ;//<< /SCRIPT>
```

JavaScript code of the original system is modified, cross-site scripting attacks successfully executed. Successful attack system interface is shown in Figure 9.

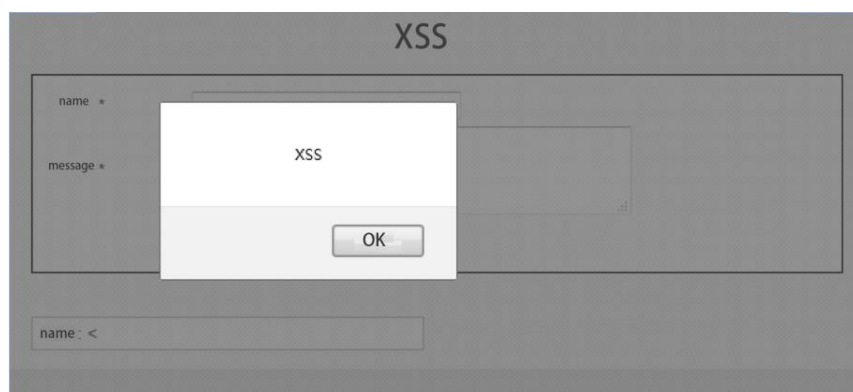


Figure 9. Cross-site scripting attack successful interface

Cross-site scripting attacks is a kind of Web applications attacks, an attacker trying to inject malicious script code into a trusted site to perform malicious operations. In a cross-site scripting attack, malicious code is executed on the browser side of the affected user and has an impact on the user.

This example interface appears pop-up, indicating that malicious script has been stored in the database, and successfully executed in the browser to achieve the desired results.

6. Conclusion and Prospect

In the process of the platform design and implementation, using XenServer as the underlying virtualization server system can improve the resource utilization.

With the help of the Guacamole project to build a cloud desktop platform based on B/S structure, the system's convenience and flexibility are improved. The good interaction between the exercise system and the user is achieved. The vulnerability database has some reference value to the research of the penetration test technology and the network attack and defense technology and can help the security technicians to improve the network attack and defense ability. Although XenServer virtualization solutions are used to manage resources efficiently, they still need to install XenCenter on a Windows-based computer to manage them. In the future, the XenServer management client based on the B / S architecture can be developed for the features of XenCenter, allowing the entire drill system to be managed only by the browser, making the operation more flexible. At the same time, the system only for the current penetration test drills in the typical loopholes in the exercise environment development, need to continue to vulnerabilities to add other vulnerability information. In the future, the above shortcomings can be further improved.

7. References

- [1] Information Security Vulnerability Report (2015) [EB / OL]. [Http: //www.cnnvd.Org.cn/news/jklbz/id/CNNVD](http://www.cnnvd.org.cn/news/jklbz/id/CNNVD) Situation Report.
- [2] Yan-Guang L I.Design and Realization of Network Attack and Defense Simulation System Terminal Subsystem [J] .Computer & Modernization, 2014 (3): 169-172,185.
- [3] Chang Yan, Wang Guan. Network security penetration test research [J]. Information Network Security, 2012 (11): 3-4.
- [4] Divorra Escoda O, Espinola Torrent D.CLOUD DESKTOP SYSTEM WITH MULTI-TOUCH CAPABILITIES: US, US 20130047095 A1 [P] .2013.
- [5] Design and Implementation of Virtual Desktop Platform Based on Cloud Computing [D]. Fudan University, 2012.Kalje R A,Kosbatwar S P.Android Based Remote Control of Mobile Devices Using VNC System[J].International Journal of Computer Science & Information Technolo,2014.
- [6] Kaur L,Kakkar H.A Review On optimization technique in Server Virtualization[J].International Journal of Computer Science & Information Technolo,2014.
- [7] Machida F,Dong S K,Trivedi K S.Modeling and analysis of software rejuvenation in a server virtualized system with live VM migration[J]. Performance Evaluation, 2013, 70(3):212-230.
- [8] Shirinbab S,Lundberg L,Ilie D.Performance Comparison of KVM, VMware and XenServer using a Large Telecommunication Application[J].2014.
- [9] Guacamole [EB/OL]. <http://guacamole.incubator.apache.org/>. Woo Yun- 2011- 02330[EB/OL]