http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (19): 5097-5101, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.5097.5101

Research and Design of System Security Strategy Based on NET Platform

Jing Zhou and Yu-Rong Guan
Huanggang Normal University, Huanggang, 438000, Hubei, China

Abstract: This study tells the story of in order to effectively resist the invasion of external .NET platform system, improve system security, it must establish the prevention and monitoring technologies improve system security system. System programmer and administrators only in the system design stage, to do a safety prevention programs and solutions to security applications; finally put forward the platform system safety prevention programme. in addition, this study analyzes the study of the .NET application process, three elements of security (authentication, authorization, fake) their own characteristics; Secondly, in detail .NET environment based on common security vulnerabilities and security architecture .NET environment; Finally, the study of the IIS and .NET authentication mode application and authorization mechanisms and their intranet and internet environment to achieve the security policy configuration and design.

Key words: Architecture, process, strategy, platform system, security issues, security analysis, prevention programme

INTRODUCTION

As Web applications become increasingly widespread, more and more systems and services using B/S structure. At the same time high performance and reliability of the application process has been the goal pursued by the developer, how to make better use of share some resources to better improve application performance and reliability of their developers have become key issues for consideration. With the intranet and internet applications and popular in all walks of life, security is a growing web application developer concerns, but to protect the safety of web applications become more complex, developers using NET technology, on the other hand, NET technology itself provides authentication, authorization and other security features (Zhou and Liu, 2008). In addition ,Based on .NET platform system structure under Web mode application system reliability and high security has been the developer and user goal, although the computer hardware configuration is more and more high and the price is lower and lower, upgrading hardware to be to improve the performance of the system is the most direct, convenient way; but in the current NET platform system Web model the application system is more and more huge, developers and users demand continuous upgrading of circumstances, to rely solely on the upgraded hardware cannot obtain satisfactory effect. How to make better use of the possession of resources, better improve Web mode application system performance and safety have become the key problems.

PROBLEM OF SYSTEM SECURITY STRATEGY

The NET programmers is to bring a vast new program of space, but because it contains many new technologies, in terms of each There are still a lot of programmers need to learn, programming, they also inevitably some flaws, mainly.

Excessive trust of user input: The .NET that page as an intermediary with the user interaction, the user will enter the website legal information and therefore the user's input does not carry out verification and inspection, in fact, now many hackers will attack with a lot of methods and tools to the input box, enter the specific information with a bad purpose, to achieve its other objectives. This vulnerability is easy to be hackers to SQL injection attacks and XSS attacks and thus defrauding the trust and access to confidential data on servers and other hazards. This vulnerability is the low level of security loopholes (Zhou and Liu, 2008).

Use of information leakage caused by Cookies: To use the Cookies, do not need to programmatically create and read them explicitly. If you use session state and forms authentication implementation will implicitly use the Cookies. of course, NET support without Cookies session state, but if ID can be embedded in the URL, so it's more vulnerable.

Corresponding Author: Jing Zhou, College of Mathematics and Computer Science, Huanggang Normal University, 438000, Huanggang, Hubei, China Tel: 86-139953933457

To pass parameters from the URL: Using a variety of development languages used by Web programmers almost all URL parameters passed by value, with the NET programming, too, it can easily get to the next page on the page associated with a value, simplify code writing, however, left it vulnerable to hacker attack vulnerability.

Page directly script language: Many programmers are accustomed to a web page (that is.Aspx file) to add language to deal with Script pages the user insertion of information (such as form input), without any network transfer data back and forth, so when the user enters a items of information, it need not pass through the server address and transmits it back to the process, the client directly can be handled by the application. This can speed up access to a good speed (Zhou and Yuan, 2009a).

Since, it is generally only the client implementation and its source code client can directly see, with the server client is not necessary connection, but it can be in the client offline, so hackers can easily attacked, so from security considerations should be avoided.

User login security issues: Users of the NET framework Web mode application system registered user information (such as a user name and password) is stored in the database. Need to verify that the browser will need to verify identity information is sent to the application server, application server database read in corresponding field and form the received data are compared. If consensus is that the user is a legal user access system, otherwise it is mandatory to guide to verify interface. User login process system on the name and the password of the user into the validator is not prevented all by modifying the parameters of the implementation of the attack. In the implementation of numerical range check should be based on the input domain requirements for data types to specify the appropriate Type attribute.

Back-end SQL security issues: User input data is the main source of HTML submitted in a form parameter. User input parameters content contains only" normal" username and password data, but does not contain special characters. An attacker can use some special meaning character changing query intention, then call any functions or processes, cheat server database execute malicious query to obtain a back-end database to save any information(Zhou and Yuan, 2009b).

Inject malicious script security issues: Inject malicious script refers to a malicious user information is embedded into the response page. The NET framework Web mode application system, if not well processing user input information, it may allow the user to put their own client script into the database server, which performs an illegal operation.

Information leakage security issues: In the .NET framework Web mode application system in almost all HTML page hidden fields can be found in the application of relevant information. The attacker can easily decode the BASE 64 data can be hidden fields provides detailed information. By default, the hidden field data will contain: from the page control dynamic data; developers in view state explicitly saved data; data cryptographic signature (Zhou, 2012a).

STUDY OF SYSTEM SECURITY STRATEGY

There are three elements are the basis for security implementation

Authentication: Authentication is the user credentials from the client to obtain and verify the credentials of the process. The purpose of authentication is to confirm the identity of the client, the identity is verified, the authorization process will determine the identity can access a given resource.

Windows authentication is completed through IIS, all the web clients through IIS with NET application, communication, all requests need to go through us and then sent to NET application to verify the request. If the requirement resourced to allow anonymous access that is not authenticated. If the requirement resourced to require the user has certain privileges while customers have been verified and authorized, then IIS will send the request to the NET process to deal with, if the status is not authorized by or are not denied access. IIS always maps to the windows user account credentials and use it to authenticate users. In IIS, there are three different types of authentication: basic, digest and integrated Windows authentication (Zhou, 2012b).

Licensing: The purpose is to determine whether authorization should be granted to a user on a given type of resource access request. There are two basic ways to grant access to a given resource: File authorization and URL authorization.

After authentication the user to determine the identity, but also the decision by the authorized processing module whether this user has access to this resource. Authority is divided into "file under" and "URL authorization" and each authorization method is divided into user-based authorization and role-based authorization, role-based authorization can greatly simplify the licensing workload.

Document authorized by file authorization module executed by windows operating system Access Control List (ACL) to control user or group on the file or folder access rights to achieve, windows authentication mode of user or role (group) is authorized by file authorization to implement and document authentication, authorization forms and passport does not work even under authentication. Authorization implementation file, the file system must be configured to NTFS format, FAT32 format cannot be achieved in the ACL.

Fake: Fake identification in the context of other users to execute code of the process, that is disabled by default fake and Win2000 environment. All .NET codes are in the Domain and NET runs under the user account that can be set in the web.config is to enable fake. The main purpose is to simplify the fake work authorization rather than authentication. Note that only windows authentication mode can use the fake and so on in the form authentication mode is not fake at all.

The Web service is programmable components, it is through the HTTP technology and standard on the Internet function to open for public use. It provides in a scalable, loosely coupled and platform specific environment the ability to exchange information, information exchange such as the use of HTTP, XML, SOAP and WSDL, standard protocol (Wei, 2008).

The security of a Web system should at least include two aspects, one is refers to the news of the confidentiality and integrity of the transmission in the process will not be stolen and tamper; two refers to the subscriber identification and the system resource access is granted to prevent system and data illegal use or destroy. Typically, a web system can be divided into the operating system, the web server, network system, database and application in four layers, any link occurrence problem can be on the web system caused a fatal blow.

The Web application will be several types of attack, its destructive effect due to the procedure itself is different. Therefore, the safety is associated with the program uses and users with their functional interaction mode is closely related to the. The .NET platform provides some built-in code to the user and operation for authentication and authorization, authentication and authorization mechanism and the IIS, .NET Framework and the underlying operating system security service is connected.

Security analysis of proxy service: From six to ensure that Web system development environment security: Security user account security. Defining user roles, permissions in web creation and management of user or group of users must be careful. For each account setting complex password, do not let more users share the same account; setting the appropriate NTFS permissions. Ensure that the Front Page website file directory of inheriting permissions, to ensure that the anonymous user account does not have permission to write to any site; timely installation systems and development tools software patches; log. Regular inspection and finishing every log file; setting up the development environment of IP restriction; disable creation support (Chu, 2007).

Security analysis of Database: SQL injection attacks against SQL, the use of SQL system parameter API programming environment, let the bottom of API to construct the query; the user name and password are divided into two steps to verify, when the user name is legal, ran for password authentication, which are legitimate before they can proceed to the next step of the operation; use validation controls is setting the regular expression on the user input content filtering, to filter out quotes, equal sign sensitive symbol.

To prevent the database password theft solution is encrypted password, password information should be stored in a database and do not exist in plaintext, prevent interception. Use scripting languages in the management of the client user submitted encryption after the transfer, server database directly to the encrypted code storage.

Using stored procedure to realize the operation of the database approach to improve efficiency and ensure the operation of the database parameters properly embedded. The security of database connection string: using the system authentication to access the database using the database system itself; storage function of the connection to the database encryption is stored in the NET file (Zhou, 2010).

To prevent the user from data on the operation of ultra vires, should guarantee the page access security, need in the page to access control, reduce the use of program code to control user data access.

CONCLUSION

The security program of intranet application design: When developing an application is running in the intranet environment and access to the user windows account, the application authentication on the IIS to perform and if the client is using Microsoft Internet Explorer, then use the integrated windows identity verification.

Intranet's security configuration is as follows:

- **Authentication:** (1) NET Web application configured to use windows authentication, no simulation: the virtual path editing application directory, such as

web.comfig. element is set to which to ensure that analog is turned off, (2) By IIS using integrated windows authentication against Web application's virtual root directory for anonymous access.

- Authorized to: (1). NET Web application is configured to use the "file under", (2) To configure the web server user license the right to limit the use of resources, in order to simplify the management of the user to the windows group and the use of groups in the ACL, (3) NET web application according to documents related to permissions that using the client's implementation of the access check

The implementation of the IIS integrated windows authentication to use internet explorer. In a mixed browser environment, you can use other authentication scheme, such as basic authentication and SSL, client certificates, forms authentication, in these programs, the authentication must use encrypted communications: SSL.

Security program of internet application design: Most Web applications are based on internet users, the application have the following characteristics: ① Users have many different browser types, ② Anonymous users can browse the unrestricted application page, ③ Users must register or log in to have access to restricted pages, ④ SQL server database according to validate the user credentials.

Based on these features, common safety measures are:

- **Authentication:** (1) HS configured to allow anonymous access, (2) NET web applications configured for forms authentication. (3) Use the database to store user name and password
- **Authority:** The NET Web application is configured to "URL authorization". Forms Authentication, you must use SSL to protect the initial login credentials, the same time, the resulting forms authentication ticket must be protected, you can use SSL for all pages to protect the votes, it can be web.config surface element protection attribute is configured to All or Encrypt, to encryption. web server URL authorization allows unauthenticated users to view web pages unrestricted and restricted the page to force authentication

The effective use of the NET framework of safety prevention design: Microsoft NET framework and IIS work together to provide a Web mode application security. The authentication, authorization and simulations of these three elements are the basis of the implementation of security. The NET framework in Web mode application by using the authentication provider to achieve authentication, the authentication provider is the authentication credentials and other security features code module. The .NET framework system supports Windows authentication, forms authentication and Password three authentication provider.

System code of safety prevention design: Using the .NET platform has a security access levels and set security level can to a certain extent, protect the security code, in addition, it can be combined with other methods to better protect the security code. Use programming logic component technology will be encapsulated into the DLL, the procedures of dynamic library add to project references can be achieved in a function call, the user cannot see the real code, can be well protected the security code; using the .NET platform Script Encode on all code and data encryption; to be in the application Global.asax file to the appropriate user or group of users set NTFS file permissions.

System data security solution: In the data transmission security, security strategies should enable data encryption function; in the manipulation of data security, security strategies should enable access control function. The calibration technology of safety prevention design: Verification code check is when a user accesses the web server request to enter the login interface, web server in response to client requests at the same time, generating a series of randomly generated numbers or symbols and the string of numbers or symbols to generate a picture, a picture with some interference pixel in order to prevent, this picture with the response content together. To the client browser, by the user identify the naked eye wherein the authentication code information, filling in the verification code box and then submitted to the server authentication, after the successful verification can use a feature.

Database technology is the use of stored procedure check encryption code method or use the system comes with the encryption methods to achieve. Users of the client to fill in the user name and password, the information is sent to the web server, web server will get information as being verified content is added into the execution module, module for web server and database server interaction code user fill in the User ID in the database corresponding to the Password and the user to fill out the password comparison, this process by all the web server operation, code is allowed to log in.

Backstage database of safety prevention design: For the data input prevention, using validation controls to the user's input to check. The validation controls in order to

be able to join the webpage, the input to the server controls the data validation operation. Some input range, format can be varied by the control combination to achieve check control. In this way the efficiency and precision is much higher than the use of program code to check the status.

For data output prevention, check output device is working properly, the device driver is installed correctly; the correct resolution of the display device, font attributes such as size, avoid garbled; installation related format reading software; correct authorization to users for each user, system control display content. For SQL attack prevention, using domain verifier let the. NET developers to domain values limiting mechanism, for example, restrict the user input field values must match the specific expression in response to the attack, security can be used to limit the input fields must belong to a valid character set.

ACKNOWLEDGMENTS

First and foremost, I would also like to thank reviewers for constructive reviews and suggestions that improved the quality of this manuscript. This work was funded by the project of Science and Technology of Huanggang (2013020203, 2013019903) and the project of Science and Technology of Hubei Province Department of Education research (B2013138).

REFERENCES

Chu, Y., 2007. NET application security flaws and prevention strategies. J. Anhui. Anhui.

Wei, Y. X., 2008. Network invasion examination system key technologies research. Beijing University of Posts and Telecommunications Doctorate Study.

Zhou, J. and Q.J. Liu, 2008. The system safety research and design based on NET Framework. Commun. Technol., 5: 112-113.

Zhou, J. and Y. Fang, 2009. The component code of each call analyze and compare based on. NET. Proceedings of the 3rd International Symposium on Intelligent Information Technology Application, November 21-22, 2009, Nanchang, pp: 689-691.

Zhou, J. and Y. Fang, 2009. The examinational technology of invasion analysis based on network security. Proceedings of the International Conference on Control, Automation and Systems Engineering, July 11-12, 2009, Zhangjiajie, pp: 624-627.

Zhou, J., 2010. The analysis of XML technology in network security. Proceedings of the International Symposium on Intelligence Information Processing and Trusted Computing, November 1-4, 2009, Washington, DC., USA., pp: 701-704.

Zhou, J., 2012. The analysis of the safety defects based on ASP.NET. Proceedings of the International Conference on ICCIC, Vol. 231, September 17-18, 2011, Wuhan, China, pp: 71-75.

Zhou, J., 2012. The research of system security based on.NET Platform. Proc. Eng., 190-191: 205-208.