Web application attacks prevention essay

- Understanding the risk associated with application layer attacks Secondly, by pro-actively responding to “ kill” or block the attack, it does not allow the attack to be completed. Management should create new default user accounts instead of created installed one. The list of software that creates when, user accounts are been created should carried a more secure implementation on the operating system. Enhancing these username and password is all you need properly certify and permissions requirements must address any change. The rooted formation in creation of administrator account requires to be renamed where Admin and password is not easily detected. Most circumstances permission given of administrator accessing there should be certification to the web server everyone should own user account, and apply the correct rights of use privileges needed.
- A developer for Aim Higher College is creating a Web server form for submission of calendar events to the College’s event calendar. What protective measures would you suggest to ensure its security?

It is common sense to have a good security practice, by having everyone assigned to their own user accounts a positive start for Aim Higher College. Having the uses of a scanner removes lots of initial problem before they begin. Aim Higher College needed such handy tools that help them automate and ease the process of any discrepancy in securing web server and web applications. Lists of Web Vulnerability Scanner are such as the uses of Sam Spade whois list where the performances of additional whois quires are performed.

The uniqueness is also considerable size with a port scanner; the collection is well fitted preview features will port scan the web server hosting, the web application. There are other area can rise problematic for security where the scanning is needed. Similarly to port scan is the network security scanner. Port scanner tool has the clarity to recognize available services that is functioning on the server; it uses the current known IP packets to determine the ports that are open on a server or the type of OS (Operating System) and to identify the type of firewall instillation. Acunetix Web Vulnerability scanner is powerful to have it makes sure website and web server been safe by having the appropriate examination for SQL Injection; not limited but extremely important Cross site scripting, web server configuration problems and other vulnerabilities. Additionally the verifying of password strength on authentication pages are automatically audits good enough for Aim Higher College is creating a Web server.

Database administrators from Aim Higher College’s central Information Technology (IT) group have contacted the security team noting that they are finding odd entries in a Web application’s backend database. Some of the entries appear to be SQL commands such as “ UNION” and “ JOIN” which cause them to think that an attacker is probing the Web application. What recommendations would you provide to protect both the application and the back end database? Web application’s backend database recommendations would be to provide useful protection for both the application and the back end database. They do this by discovering for all web vulnerabilities have in the listings including SQL injection and Cross site scripting along with others

availability. SQL injection definition is straight forwarded it is hacking technique that has changes in SQL commands.

This action taken is with intension to achieve entry into the information in the database. Cross site scripting on the other hand occurrences serves as a means for a hacker to accomplish a evil script on guest's browser. Advanced record submissions have in customary to split the records and the programming segments using part for a first-end database and the other for the last back-end database. Conversely, the operation has a movement where the front-end embraces the total product encoding. By simulating movement along the principal routes the gains is in " scalability, performance" and property of systems in which several computations are executing simultaneously. The basic input and output has entails which is resides in huge strength on the developer's contribution. Furthermore, overtime it is advisable to preserve and advancement with new versions. The processes in the front-end have the ability to install self-sufficiently of the back-end database. Nevertheless both are not requiring for the front and back-end databases always to have the similarity in types. " For example, it is possible to use a Microsoft Access front-end with a Microsoft SQL Server back-end."

It is no news that developers discovered current database application with growth in difficulty or practice to the fact that using separate saves more time and best performance for front and back-end databases. There is even Microsoft Access with delivery of record Splitter Wizard to simplify the procedure of severe Access submission. Additionally, detection of these susceptibilities requires a refined finding engine. Utmost to web

defenselessness scan has nothing to do with the amount of outbreaks a scanner finds. It has the difficulty and carefulness with the transformed receipts," launches SQL injection, Cross Site scripting and other attacks." Defenselessness detection has affirmative action institution engine delivers vulnerabilities with fewer problems in its findings. The uniquely in this effortless application will be a mistake to pass up on therefor it's in right frame of mind to have find CRLF injection, Code execution, Directory Traversal, File inclusion, checks for vulnerabilities in File Upload forms and much more.

A scan of Aim Higher College's primary Web server from using a Nikto shows a large number of default configuration files and sample files on many of the older servers. What is wrong with this, and what should be done about it?

Nikto, principle is similar to other non-trivial software package where the interest is a requirement of knowing how to perform with present situation. The customary is the setting the default configuration information will work. The wrong is in cases where there is problem sometimes; additional is need like tuning assist to some extent, or modification maybe the answer. The configuration file is search for by Nikto in three places wherever information is found the application will make in the order below. There can be a bit of file overriding in return value set to the most recent version configured on file.

Works Cited For This Essay:• acunetix. com/websitesecurity/webserver-security/. Combating the Web Vulnerability Threat. 2013.• http://www. acunetix. com/websitesecurity/webserver-security/ (accessed October 21,

2013).• cirt. net/nikto2-docs/configuration. html. Chapter 5. Configuration Files. n. d. http://cirt. net/nikto2-docs/configuration. html (accessed October 21, 2013).• Mark, Heather. Web Application Attacks: Attempted Prevention or Detection & Response? . May 2008.• http://www. transactionworld. net/articles (accessed Octuber 21, 2013).