

Protect a University Website from the Different Types of Outside Attacks

By

Razibul Hasan

MIEEE, Baridhara, Dhaka-1206, Bangladesh

kustia@gmail.com

ABSTRACT

A university website design and maintain its security are very important issues. University networks and websites are decentralized which makes it difficult to ensure consistent the security levels. One department employs a guarded security infrastructure while other departments lack security measures. Depending on the security strength of the servers and computer network systems, attackers can either succeed or fail in their attempt to gain unauthorized access into the website. The word security means protection against malicious attack by outsiders and by insiders. Security threats can originate from a diverse group of sources including hackers and thieves residing outside the campus as well as students with technical knowledge and university staff members associated with the university. In this paper author has focus on the university websites challenges and vulnerabilities as well different protection methods.

General Terms

Networks Information Security, Data Security, Internet and Web Applications, Systems Security

Keywords

Semantic Web, Website Security, Hacking, SQL Injection, DDoS, Website Data Protection, University Website Standard.

1. INTRODUCTION

The web server environment of a university presents a unique set of challenges. A typical university is comprised of dozens of departments, hundreds perhaps thousands of faculty members and administrative staff, tens of thousands of students, as well as thousands of servers and computers that may or may not have adequate security protection. All of these users and devices are connected to the network and are all potential targets of network attacks. Network threats are everywhere and not just from the outside world of spammers, hackers, and thieves. Profound network threats also reside within the campus environment originating from professors and students alike. Combining the threats posed by both external and internal sources with a large multipurpose university website creates a daunting

challenge for network administrators trying to enable interoperability and communications but at the same time secure their network. Higher education institutions face greater risks malware, phishing, infrastructure attacks, social network targeting, and peer-to-peer information leakage are not potential threats they're everyday issues. Most universities financial, administrative, research and clinical systems are accessible through a campus network. Overall, there are many university institutions that have fallen victims to data breaches resulting in a growing concern over privacy. The motives behind these attacks vary but more importantly hackers are able to discover critical weaknesses and loopholes in the web server. Websites offer a creative, interactive means of publicizing the strengths of the university and offering services to others. Web pages should be developed within the context of the audience they serve. An unfortunate user experience regarding misinformation or poor content is not just an impediment for the particular website. The purpose of these standards is to ensure that the university is represented with consistency and integrity on the Websites of all of universities departments, schools, facilities, organizations, and affiliates.

Flexible role assignment allows users to be given only the editing rights they need. Content approval system allows content to be reviewed prior to publication on important pages runs on industry-standard secure apache servers. Detailed auditing of actions and tracking of deleted information nightly database backups allow rollback in emergencies. Authentication integrated with main password system to ensure that only university members are able to view the site, and all pages viewed are logged. Page access can be restricted to university members only or to a specified group of user's virus checking of all uploaded resources password-protected file downloads for secure provision to external users. Content protected against simultaneous editing without the need for an explicit and need to check out previous versions of text can easily be reverted to prevent web-based spam. Multiple content types allowing easy entry and maintenance of a wide variety of content, including: Image galleries allow images to be categorized and grouped for easy browsing. Several other content types including FAQ, site maps, seminar listings.

Any file like PDF, Word, Excel, etc. can be associated with a content item for easy download. Easy image upload and image library, with thumbnail creation and automatic management of unused images.

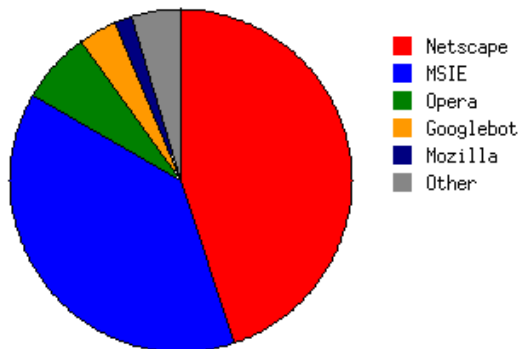


Fig 1: percentage of accessing web server by source

This graph provides a summary of the accesses to a departmental web server. The majority (about 70%) of these accesses are from within the university network. The graph was on 2003 statistics of Durham university - similar graphs for current accesses to sites on the main University website are available from the access logs reports while the numbers have changed, the variety of browsers has only increased. As can be seen from the graph, a large proportion of page views to this departmental web server are from neither Netscape nor Internet explorer. We need to remember that if only 1% of users are unable to access the site due to their choice of browser, it is equivalent to 3.5 days of web server failure each year. Simple contact form allows comments, feedback and change requests to be received and handled. Messages are automatically and flexibly sent to the nominated departmental contact(s), or easily directed into compatible ticketing systems such as Remedy or Request Tracker. Integrated with Google Search Appliance for fast and accurate searching consistent and accessible appearance helps new users navigate the sites automatic creation of redirects when pages move helps users and search engines.

The Staff Profile Research database system is a central store of information which may be used to populate a central online Directory of Expertise, departmental web pages, and staff profile pages. Information in the database may be updated by individual staff members or designated departmental administrators. Today, Semantic Web technologies are used for a wide range of applications, both on the Web and internally within various organizations. While Semantic Web usage on the Web is mostly about publishing and consuming data, Semantic Web technologies are also being applied within enterprises for a much broader set of applications.

2. UNIVERSITY WEBSITES SECURITY CHALLENGES

Internet access to University resources and University access to Internet resources are both important elements in

sustaining the University's primary missions of instruction, research, and public service. University networks play host to student and alumni data, research data, advanced networking technology and enormous amounts of bandwidth, thus representing a very attractive target for hackers. Universities are a virtual treasure trove of all types of data which reside on network-connected servers that are most likely unattended and often unprotected. Hackers set their sights on specific types of targets such as personal and research data, which can be used for all types of identity theft as well as criminal or even terrorist activities. In addition, hackers aggressively try to compromise network-connected devices and use them to launch attacks while hiding among legitimate applications within a vast and under protected network. Therefore, university networks must be protected and actively monitored for a variety of constantly evolving threats.

2.1 Personal financial information

Students and their families provide information about their finances for purposes of determining tuition assistance and scholarships. They trust that this confidential data will remain private.

2.2 Payment records

This information specifies what students have paid and what they owe. Besides the privacy issue, this data, as well as the personal financial information held could be used for spear phishing attacks and other scams.

2.3 Credit card information

Students use credit cards for everything from paying tuition and fees to purchases in campus stores and cafeterias/restaurants. As a consequence, colleges and universities are subject to the strictures of PCI DSS, with all its highly prescriptive security controls.

2.4 Protected Health Information

Many large universities support major medical centers that are responsible for protecting patient protected health information (PHI) under HIPAA.

2.5 Personally identifiable information

All of the college entities conducting various transactions with students, their families and the population at large collect personally identifiable information of every type - names, addresses, email, phone numbers, etc. These records carry a vast and heavy protection burden, as a moral responsibility and the risk of huge expenditures and reputation damage in the event of a major data breach.

2.6 Student records

Academic information is protected as private, to be released only with students' permission. Other private information may include counseling sessions and other sensitive matters.

2.7 Research data

Universities are home to some of the most critical and sensitive research, both theoretical and applied. Scientific and medical investigation, including development of

pharmaceuticals, make university labs and research centers attractive targets for espionage by firms seeking a competitive edge. In the same vein, much of the most important defense-related research is conducted at universities under the aegis of defense contractors and/or the federal government.

3. TYPES OF ATTACK ON UNIVERSITY WEBSITE

The University website is scanned every day from the Internet. Much of this scanning is done to determine the number and location of potentially vulnerable systems on the campus network. Denial of Service (DOS) attacks from the Internet has occurred in the past, and will most likely be attempted again in the future against University systems.

Risks to our academic mission are most apparent. The loss or corruption of data or unauthorized disclosure of information on research and instructional computers, student records, financial systems, or any other aspect of University operations is unacceptable. The University also has a legal responsibility to secure its computers and networks from misuse. It is the responsibility of the Office for Information and Technology Services (ITS) to take the necessary steps to provide a reliable network.

3.1 Vulnerabilities

Vulnerabilities in network security can be summed up as the “soft spots” that are present in every network. The vulnerabilities are present in the network and individual devices that make up the network. Networks are typically plagued by one or all of three primary vulnerabilities or weaknesses: Technology weaknesses, Configuration weaknesses and Security policy weaknesses. Technological Weaknesses Computer and network technologies have intrinsic security weaknesses. These include TCP/IP protocol weaknesses, operating system weaknesses, and network equipment weaknesses. Configuration Weaknesses Network administrators or network engineers need to learn what the configuration weaknesses are and correctly configure their computing and network devices to compensate. Security Policy Weaknesses can create unforeseen security threats. The network can pose security risks to the network if users do not follow the security policy.

3.2 Threats

Unstructured threats consist of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers. Even unstructured threats that are only executed with the intent of testing and challenging a hacker’s skills can still do serious damage to a company. Structured threats come from hackers who are more highly motivated and technically competent. These people know system vulnerabilities and can understand and develop exploit code and scripts. They understand, develop, and use sophisticated hacking techniques to penetrate unsuspecting businesses. These groups are often involved with the major fraud and theft cases reported to law enforcement agencies. External threats can arise from

individuals or organizations working outside of a company. They do not have authorized access to the computer systems or network. They work their way into a network mainly from the Internet or dialup access servers. Internal threats occur when someone has authorized access to the network with either an account on a server or physical access to the network. According to the FBI, internal access and misuse account for 60 percent to 80 percent of reported incidents.

3.3 Worms, Viruses, and Trojan Horses

Malicious software is inserted onto a host to damage a system; corrupt a system; replicate itself; or deny services or access to networks, systems or services. They can also allow sensitive information to be copied or echoed to other systems. Trojan horses can be used to ask the user to enter sensitive information in a commonly trusted screen. For example, an attacker might log in to a Windows box and run a program that looks like the true Windows logon screen, prompting a user to type his username and password. The program would then send the information to the attacker and then give the Windows error for bad password. The user would then log out, and the correct Windows logon screen would appear; the user is none the wiser that his password has just been stolen. Trojan horse an application written to look like something else that in fact is an attack tool. Worm an application that executes arbitrary code and installs copies of itself in the memory of the infected computer, which then infects other hosts. Virus is malicious software that is attached to another program to execute a particular unwanted function on the user workstation.

3.4 Phishing

Phishing is a type of social-engineering attack that involves using e-mail or other types of messages in an attempt to trick others into providing sensitive information, such as credit card numbers or passwords. The phisher masquerades as a trusted party that has a seemingly legitimate need for the sensitive information. Frequent phishing scams involve sending out spam e-mails that appear to be from common online banking or auction sites. These e-mails contain hyperlinks that appear to be legitimate but actually cause users to visit a phony site set up by the phisher to capture their information.

3.5 Malicious Code

The primary vulnerabilities for end-user workstations are worm, virus, and Trojan horse attacks. A worm executes arbitrary code and installs copies of itself in the infected computer’s memory, which infects other hosts. A virus is malicious software that is attached to another program to execute a particular unwanted function on a user’s workstation. A Trojan horse differs only in that the entire application was written to look like something else, when in fact it is an attack tool.

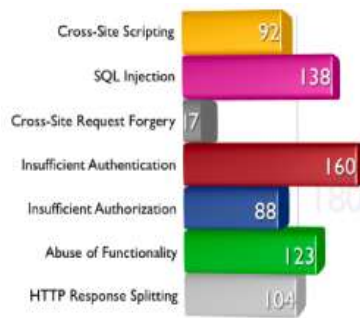


Fig 2: Average Time to Fix by Class of Attack Measured in Days

Web server and security administrators in university environments face a daunting challenge; they need powerful solutions including granular network visibility and prompt alert capabilities to enable quick corrective responses. The different types of vulnerabilities discussed here are SQL injection, cross-site scripting, information disclosure, path disclosure, and buffer overflows. Successful exploitation of these vulnerabilities can lead to a wide range of results.

3.6 Password Attacks

Password attacks can be implemented using several methods, including brute-force attacks, Trojan horse programs, IP spoofing, and packet sniffers. Although packet sniffers and IP spoofing can yield user accounts and passwords, password attacks usually refer to repeated attempts to identify a user account, password, or both. These repeated attempts are called brute-force attacks.

3.7 The Distributed Denial of Service

A common component of such an attack is to execute the distributed denial-of-service (DDoS) attack against one end-point to stop it from responding. This attack can be either against the machine to force it to crash, or against the network connection to force heavy packet loss. Distributed denial of service attacks on root name servers are Internet events in which distributed denial-of-service attacks target one or more of the thirteen Domain Name System root name server clusters. The root name servers are critical infrastructure components of the Internet, mapping domain names to Internet Protocol (IP) addresses and other resource record (RR) data. Attacks against the root name servers could, in theory, impact operation of the entire global Domain Name System, and thus all Internet services that use the global DNS, rather than just specific websites. However, in practice, the root name server infrastructure is highly resilient and distributed, using both the inherent features of DNS, a combination of any cast and load balancer techniques used to implement most of the thirteen nominal individual root servers as globally distributed clusters of servers in multiple data centers.

The denial of service attack is one of the best examples of impacting site availability. It involves getting the server to perform a large number of mundane tasks, exceeding the

capacity of the server to cope with any other task. For example, if everyone in a large meeting asks you your name all at once, and every time you answer, they ask you again. You have experienced a personal denial of service attack. To ask a computer its name, you use ping. You can use ping to build an effective DoS attack.

3.8 SQL Injection

SQL Injection is an attack method using the application vulnerability. Because the present encryption protection only can guarantee the security of data transmitting on the internet, but can not check the data content any input data in the page form which was filled by the user, can be send to the web server [7]. If the attacker has filled the data that include the vicious SQL query instruction in the web page form, these query instruction together with HTML file will drill through the firewall and arrive to web server. Once they are run at web server, the important information will be revealed or modified. A successful SQL injection attack enables a malicious user to execute commands in our application's database by using the privileges granted to our application's login.

3.9 Cross Site scripting

Cross site scripting is one of the more prevalent security flaws found within Web applications today. Cross-site scripting is an attack that takes advantage of a Web site vulnerability in which the site displays content that includes un-sanitized user-provided data. For example it could copy user cookies and then send those cookies to the attacker. Cross-site scripting attacks occur when an attacker takes advantage of such applications and creates a request with malicious data that is later presented to the user requesting it. The malicious content is usually embedded into a hyperlink, positioned so that the user will come across it in a web site, a Web message board, an email, or an instant message.

4. BASIC WEB SECURITY

In view of the numerous potential and actualized security incidents plaguing educational institutions, it is critical that university networks be protected and actively monitored around-the-clock. Without capable network security technology that delivers complete network visibility with threat management, universities are forced to operate in a reactive mode after attacks have occurred. In order to manage and protect a vast number of computer network and servers, network administrators must capitalize on security technology that can monitor networks, correlate events and deliver real-time alerts and analysis.

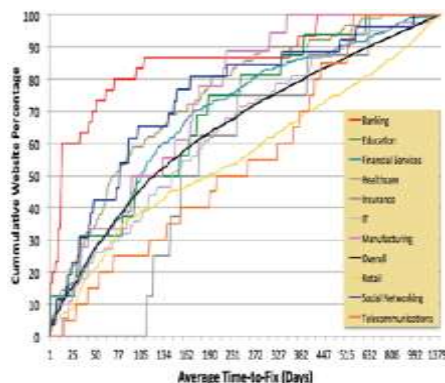


Fig 3: Average time to fix vulnerability by sector

4.1 Keep Code Up to Date

We should up to date the source code of any website. In security system there is no better protection than keeping your code up to date. Old versions of Word Press, old installs of PHP and MySQL, even old browsers, all of these are security issues because most updates of software these days are security patches. So please help the good guys by upgrading whenever a new version is out. We should up-to-date not only the code of any application software but also services provider software. If we use PHP MySQL and Apache, we should always up-to-date the PHP version, MySQL & Apache server.

4.2 Remove unnecessary services

Default operating system installations and configurations, are not secure. In a typical default installation, many network services which won't be used in a web server configuration are installed, such as remote registry services, print server service, RAS etc. The more services running on an operating system, the more ports will be left open, thus leaving more open doors for malicious users to abuse. Switch off all unnecessary services and disable them, so next time the server is rebooted, they are not started automatically. Switching off unnecessary services will also give an extra boost to your server performances, by freeing some hardware resources.

4.3 Remote access

Although nowadays it is not practical, when possible, server administrators should login to web servers locally. If remote access is needed, one must make sure that the remote connection is secured properly, by using tunneling and encryption protocols. Using security tokens and other single sign on equipment and software, is a very good security practice. Remote access should also be restricted to a specific number of IP's and to specific accounts only. It is also very important not to use public computers or public networks to access corporate servers remotely, such as in internet public place or public wireless networks.

4.4 Web application and server side scripting

The web application or website files and scripts should always be on a separate partition or drive other than that of

the operating system, logs and any other system files. Through experience we've learnt that hackers who gained access to the web root directory, were able to exploit other vulnerabilities, and were able to go a step further and escalate their privileges to gain access to the data on the whole disc, including the operating system and other system files. From there onwards, the malicious users have access to execute any operating system command, resulting in complete control of the web server.

4.5 User accounts

Unused default user accounts created during an operating system install should be disabled. There is also a long list of software that when installed, user accounts are created on the operating system. Such accounts should also be checked properly and permissions need to be changed required. The built in administrator account should be renamed and is not to be used, same for the root user on a linux or unix installation. Every administrator accessing the web server should have his own user account, with the correct privileges needed. It is also a good security practice not to share each other's user accounts.

4.6 Remove unused modules and application extensions

A default Apache installation has a number of pre-defined modules enabled, which in a typical web server scenario are not used, unless they are specifically needed. Turn off such modules to prevent targeted attacks against such modules. The same applies for Microsoft's web server, Internet Information Services. By default, IIS is configured to serve a large number of application types, e.g. ASP, ASP.NET and more. The list of application extensions should only contain a list of extensions the website or web application will be using. Every application extension should also be restricted to use specific HTTP verbs only, where possible.

4.7 Always logout from the website administration control panels

Always logout from the website administration control panels. Staying logged in while not using a system is dangerous. Other websites you surf to can check that you are logged in and then click jack you to make you do something you don't mean to or aren't aware of. This is especially dangerous with social media because everything you do will be sent to all your friends and probably replicated by them. It is a snowball effect.

4.8 Use correct forms of passwords

Password policy is another issue for protect your web site. We should use proper format password. That means complex password. And password should be changed after a certain time. I have changed my passwords every week. Ensure that password policies are enforced for shoppers and internal users. A sample password policy, defined as part of the Federal Information Processing Standard (FIPS) is shown in the table below. We may choose to have different policies for shoppers versus our internal users. For example, we may choose to lockout an administrator after 3 failed

login attempts instead of 6. These password policies protect against attacks that attempt to guess the user's password.

4.9 Turn off Folder Listing

Folder listing is another issue of vulnerabilities of any website. We should hide of folder listing of any web site. From this listing any one can try to find the structure of any site, folder path, and content of any site.

4.10 Turn off Error Messages

It's another issue to find out the problem of any software. From the error message we can find the problem. But it should stop to view for all users. Lot of servers is set up to show you error messages when the browser encounters a problem. These messages often look cryptic, but they are a great source of information for attackers. By the error message any hackers can attack the server and the web application which is harmful for the application.

4.11 Web Server Firewall

A web server or web application firewall, either a hardware appliance or software solution, is placed in between the client end point and the web application. Web application firewalls protect cardholder data because all web layer traffic is inspected looking for traffic that is meant to exploit known vulnerabilities as well as patterns that may suggest a zero-day exploit being launched against the application. A firewall is like the moat surrounding a castle. It ensures that requests can only enter the system from specified ports, and in some cases, ensures that all accesses are only from certain physical machines. All of the data packets that come from the Internet is first received by the Firewall, and are inspected. The security level to be established on the Firewall depends upon the level of security you want to implement to protect university web Server.

4.12 Installing Recent Patches

Software bugs and vulnerabilities are discovered every day. Even though many of them are discovered by security experts, rather than attackers, they may still be exploited by attackers once they became a public knowledge. That's why it is important to install all software patches as soon as they become available.

4.13 Use Scanners

Scanners are handy tools that help you automate and ease the process of securing a web server and web applications. Web Vulnerability Scanner is also shipped with a port scanner, which when enabled will port scan the web server hosting the web application being scanned. Web Vulnerability scanner ensures website and web server security by checking for SQL Injection, Cross site scripting, web server configuration problems and other vulnerabilities. It checks password strength on authentication pages and automatically audits, forms, dynamic Web 2.0 content and other web applications. As the scan is completed, the software produces detailed reports that pinpoint where vulnerabilities exist.

5. CONCLUSIONS

In this paper author has described possible ways to protect data and web of university website. University institutions can successfully protect themselves against external attacks, internal threats and malware outbreaks. University private data must be stored on University owned computers unless a contract approved by an authorized University representative exists with the non-university business, person, or entity. This will not happen until we get all the parties, including IT, Administration, Finance and Teachers, involved in a process of constructive dialogue. This process of constructive dialogue will need to involve a process of education for all those involved. University computers and devices must be installed and actively maintained on an ongoing basis so that they protect the data stored or accessed through them and meet University compliance requirements and pertinent external regulations. The safest approach to securing user input is to never trust what is being submitted and always treating the data as a possible attack. This is known as a white list approach. User input generally originates from a form in which data is needed to be processed by the application. A good place to start validating user input is with the creation of the form itself. With the use of an input tag, there are a few attributes which can help secure data before a script processes the information. Some computers and devices require additional enhanced protection measures. One possible way to create a more secure environment is to filter the incoming data. One can do this by only accepting the correct values and providing a default scenario for any data other than the accepted.

6. REFERENCES

- [1] P. Sousa and D. Garlan, "Apache HTTP Server Version 2.0 Documentation," The Apache Software Foundation, 1995–2005.
- [2] L. D. Stein, "Web Security: A Step-by-Step Reference Guide," Addison Wesley Professional, 1998.
- [3] J. Pieprzyk, T. Hardjono and J. Seberry, "Fundamentals of Computer Security," Springer-Verlag, 2003.
- [4] Top ten database threats, http://www.schell.com/Top_Ten_Database_Threats.pdf
- [5] DDoS, http://en.wikipedia.org/wiki/Distributed_denial_of_service_attacks_on_root_nameservers
- [6] SQL Injection, http://en.wikipedia.org/wiki/SQL_injection
- [7] Apache Software Foundation, "Filters - Apache HTTP Server," [http://httpd.apache.org/docs-2.1 /filter.html](http://httpd.apache.org/docs-2.1/filter.html), Nov.2004.
- [8] Web standards, http://www.uky.edu/Home/WebPublishers/web_standards.html
- [9] University web standards, <http://www.famu.edu/index.cfm?a=universitywebstandards>
- [10] Cross site scripting, http://en.wikipedia.org/wiki/Cross-site_scripting

- [11] Web Services,
<http://www.dur.ac.uk/cis/web/cms/features/>
- [12] Standards checklist
https://itservices.uchicago.edu/groups/webservices/best_practices/standards_checklist/index.shtml
- [13] Web, <http://www.ohio.edu/brand/web/>
- [14] The University: so much at risk,
http://www.corero.com/en/solutions/public_sector
- [15] Semantic web on the web,
<http://www.cambridgesemantics.com/semantic-university/semantic-web-on-the-web>
- [16] Example of semantic web application,
<http://www.cambridgesemantics.com/semantic-university/example-semantic-web-applications>
- [17] Web server security,
<http://www.ibm.com/developerworks/linux/library/s-wssec.html>
- [18] The National Security Agency, Security Enhanced Linux, <http://www.nsa.gov/selinux>
- [19] S. Smith and S. Weingart. "Building a high-performance, programmable secure coprocessor. Computer Networks," April 1999.
- [20] Web standards,
http://en.wikipedia.org/wiki/Web_standards
- [21] Web application security,
<http://www.acunetix.com/websitesecurity/webserver-security.htm>
- [22] Mark Curphey, Joel Scambray and Erik Olson
"Improving Web Application Security," Threats and Countermeasures, 2004.