International Journal of Multidisciplinary Education and Research
ISSN: 2455-4588
Impact Factor: RJIF 5.12
www.educationjournal.in
Volume 3; Issue 2; March 2018; Page No. 21-22

Web Security, Site and Network

Sunny Kumar
Research Scholar, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India

Abstract
Nowadays, the web service has become the emerging communication technology where the interaction of each user is performed through the World Wide Web. However, the performance of the web service mechanism is degraded due to security flaws that occur throughout the Internet. The user or service requester may not attain the relevant web service for their requirement. Web sites are unfortunately prone to security risks. And so are any networks to which web servers are connected. Setting aside risks created by employee use or misuse of network resources, your web server and the site it hosts present your most serious sources of security risk. Web servers by design open a window between your network and the world. The care taken with server maintenance, web application updates and your web site coding will define the size of that window, limit the kind of information that can pass through it and thus establish the degree of web security you will have.

Keywords: network, web security, security analysis

Introduction
Security analysis allows one to delimit the security perimeter of a computer system. In service oriented architectures, such task is intrinsically complex, due to the many architectural layers, technologies and communication protocols involved. The security analysis must also consider the particular implementation for a given SOA. In this deliverable we first introduce different kind of attacks that are related to web-services and embedded devices, to then cover threats that appear in presence of service composition. SOA settings, which allow an analysis of specific categories related to SOA with the security analysis. Web sites are unfortunately prone to security risks. And so are any networks to which web servers are connected. Setting aside risks created by employee use or misuse of network resources, your web server and the site it hosts present your most serious sources of security risk. Web servers by design open a window between your network and the world. The care taken with server maintenance, web application updates and your web site coding will define the size of that window, limit the kind of information that can pass through it and thus establish the degree of web security you will have.

Review of Literature
Bernd Resch (2014) Security has recently become a major concern in distributed geo-infrastructures for spatial data provision. Thus, a lightweight approach for securing distributed low-power environments such as geo-sensor networks is needed. The first part of this study presents a survey of current security mechanisms for authentication and authorisation. Based on this survey, a lightweight and scalable token-based security infrastructure was developed, which is tailored for use in distributed geo-web service infrastructures. The developed security framework comprises dedicated components for authentication, rule-based authorisation and optimised storage and administration of access rules. For validation purposes, a prototypical implementation of the approach has been created.

Jaap Gordijn (2005) this study introduces a design methodology for business modeling from two perspectives. The value-web perspective models the creation, distribution, and consumption of goods or services of economic value in a network of multiple enterprises and end-consumers. The goal is to create a shared understanding for all the actors and to assess profitability. The trust perspective describes how value webs can be expanded with trustworthy control procedures. The goal is to enhance the mutual confidence of the actors so as to enable trading. A formal theory for the design of trustworthy control procedures in the setting of the e³value methodology is outlined.

S.-H. Tang (2004) in this study, a multi-application and feature-oriented database framework for web-based CAx applications is proposed based on client-server architecture. The web server provides a multi-view data access interface (MDAI) through which distributed users can access product and process information via data network. Application server can provide feature-modeling facilities on the basis of a geometric modeling kernel as well as DB manager. To enable information sharing among different applications for collaborative engineering, a four-layer information model is proposed. The entire product model (EPM) covers information of product entire life cycle. Sub-models, coming from CAx applications, can be accommodated as specific views of the EPM from an application-specific viewpoint. Mapping mechanisms are investigated to convert the EXPRESS-defined feature object information model to the database schemas. The generic feature representation and geometrical data representation in database is given on the basis of the proposed mapping mechanisms. The information workflow and mechanisms to control concurrency and to validate

features are also discussed.

Web Security Significance

Hacked websites, security breach, leaked data, loss of customer's trust and eventually loss of business, these terms are certainly nightmare for any business owner who is running online business.

Just like any technology, web security is also made up of many layers. Hence only keeping a password for your admin page is not enough. Below is the list of different security layers -

- Password protected user accounts
- Secure file location
- Appropriately set permissions for user accounts
- Protected application forms
- Encryption for traffic to and from the website
- Securely written site code
- A secured location for your server
- Upgraded site code
- Upgraded server applications
- Upgraded server operating system

Hackers do not choose websites that they attack

No matter how big your business is, it is best to keep it safe. The common misconception of some website owners is that they feel less threatened as their websites are small and cannot be easily noticed by these hackers. The truth is that these hackers can get into your system and can easily find your website to be vulnerable to attack. To be safe, invest on securing your website by constantly updating your security program with the help of your web developer.

Relationships with clients can be in danger

Hackers can get into your system and steal information of your clients like their names, emails and even their credit card details. Without securing your website, you are putting your clients' personal information in grave danger. Clients lose their trust if their information is hacked. Losing clients' trust is a great blow to your business.

Identity theft is rampant and dangerous

Hackers may use your personal details or your clients' personal information to make purchases online. In the recent years, many people have been sending complaint letters to credit card companies saying that a number of purchases on their credit cards were not made by them. This is the reason why websites send PIN codes to credit card users through their mobiles to confirm a purchase being done online.

Hackers can crash your website

Once your website is not working, you will be losing customers every single minute that passes. For business websites, sales per day will be greatly affected. The return of investment is sure to decrease and it might take some time before you totally recover all the data lost because of the poor security on your website.

Website security and Website maintenance makes your clients secured

It is the website's responsibility to keep the identity and personal information of these people confidential at all times. When they feel safe with your website, they are most likely to continue patronizing your brand and recommend it to others who are interested in your brand.

Conclusion

Once you think you have done all you can then it's time to test your website security. The most effective way of doing this is via the use of some website security tools, often referred to as penetration testing or pen testing for short. There are many commercial and free products to assist you with this. They work on a similar basis to scripts hackers will use in that they test all know exploits and attempt to compromise your site using some of the previous mentioned methods such as SQL injection.

Some free tools that are worth looking at:

- Netsparker (Free community edition and trial version available). Good for testing SQL injection and XSS
- OpenVAS. Claims to be the most advanced open source security scanner. Good for testing known vulnerabilities, currently scans over 25,000. But it can be difficult to setup and requires a OpenVAS server to be installed which only runs on *nix. OpenVAS is fork of a Nessus before it became a closed-source commercial product.
- SecurityHeaders.io (free online check). A tool to quickly report which security headers mentioned above (such as CSP and HSTS) a domain has enabled and correctly configured.
- Xenotix XSS Exploit Framework A tool from OWASP (Open Web Application Security Project) that includes a huge selection of XSS attack examples, which you can run to quickly confirm whether your site's inputs are vulnerable in Chrome, Firefox and IE.

References

1. James G, Lollar *et al*. A Comparative Study of Web-Based Technology Applications in Corporations, Journal of Promotion Management. 2010; 16(3):316-330.
2. David Ben-Arieh *et al*. Web-based cost estimation of machining rotational parts, Production Planning & Control. 2003; 14(8):778-788.
3. Edmundas Kazimieras Zavadskas *et al*. multiple criteria decision support web-based system for building refurbishment, Journal of Civil Engineering and Management. 2004; 10(1):77-85.
4. Indranil R, Bardhan *et al*. An Interdisciplinary Perspective on it Services Management and Service Science, Journal of Management Information Systems. 2010; 26(4):13-64.
5. Sheila M, McAllister *et al*. Organizational Influences and Constraints on Community College Web-based Media Relations, Community College Journal of Research and Practice. 2012; 36(2):93-110.