Web Security Technical Issues Related With Internet

Santosh Kumar [1, 2] , Karuna Shankar Awasthi[2] and Laxmi Shankar Awasthi[3]

[1] Ph.D. Research Scholar, Department of Computer Science and Engineering, School of Engineering and Technology, Shridhar University, Pilani-Chirawa Road, Pilani, Rajasthan- 333031 (India).

[2] Assistant Professor, Department of Computer Science, Lucknow Public College of Professional Studies, Vinamra Khand, Gomti Nagar, Lucknow - 226010 (India).

[3] Associate Professor, Department of Computer Science, Lucknow Public College of Professional Studies, Vinamra Khand, Gomti Nagar, Lucknow - 226010 (India).

ABSTRACT : The World Wide Web (or genuine World-Wide Web; shortened as WWW or W3, and popularly known as the Web) is an interconnected hypertext document system accessible via the Internet. A web browser allows you to see web pages with text, photos use hyperlinks to move between videos and other material. The operation of many components of the Internet and computer information sharing are all examples of the World Wide Web. defined by a number of formal standards, other technical specifications, and software. The World Wide Web Consortium (W3C), led by Berners-Lee, is responsible for many of the publications, although others were created by the Internet Engineering Task Force (IETF) and other organizations. When it comes to web standards, the following publications are usually considered foundational: W3C recommendations for markup languages, particularly HTML and XHTML. Hypertext documents' structure and interpretation are defined by these. The W3C has made some recommendations concerning style sheets, particularly CSS. Ecma International's ECMAScript (typically in the form of JavaScript) standards. The W3C's Document Object Model Recommendations. Online sites and web applications (webapps) face a variety of security concerns. Data centres and other assets used to host websites and their associated systems must be safeguarded against any threats. Application threat modelling should be used to identify threats, which should subsequently be analysed using a vulnerability assessment. Vulnerabilities can be eliminated or decreased, and countermeasures can be implemented to reduce the impact of an incident if it occurs. Security policies, the use of technology, and content filtering are just a few of them.

KEYWORDS: SECURITY, INTERNET, WEB, VULNERABILITY

INTRODUCTION: The World Wide Web (or genuine World-Wide Web; shortened as WWW or W3, and popularly known as the Web) is an interconnected hypertext document system accessible via the Internet. A web browser allows you to see web pages with text, photos, videos, and other material, and use hyperlinks to navigate between them. The operation of many components of the World Wide Web, the Internet, and computer information exchange is defined by a number of formal standards, other technical specifications, and software.

The World Wide Web Consortium (W3C)[1], led by Berners-Lee, is responsible for many of the papers, but others were created by the Internet Engineering Task Force (IETF) and other organizations[4].
When it comes to web standards, the following publications are usually considered foundational:

- W3C recommendations for markup languages, particularly HTML and XHTML. Hypertext documents' structure and interpretation are defined by these.
- W3C recommendations for stylesheets, particularly CSS.
- Ecma International's ECMA Script (typically in the form of Java Script) standards.
- Recommendations for the Document Object Model from the World Wide Web Consortium.

Other important technologies for the World Wide Web are defined in additional publications, which include, but are not limited to, the following:

- Uniform Resource Identifier (URI), a universal standard for referencing Internet resources like hypertext documents and photos. The IETF's RFC 3986 / STD 66: Uniform Resource Locators (URIs) defines URIs, also known as URLs.
- HTTP particularly as defined by RFC 2616: HTTP/1.1 and RFC 2617: HTTP Authentication, which specify how the browser and server authenticate each other.
- Uniform Resource Identifier (URI): Generic Syntax, as well as its predecessors and numerous URI scheme-defining RFCs. The number of security vulnerabilities has increased as email and online technologies combine, both in terms of inventiveness and effectiveness [2].

For IT administrators and computer users, web-based dangers are proving to be a nightmare. Although technology aids in the fight against these risks, a more comprehensive approach is required, including stringent and enforceable policies as well as an effective awareness programme. WS-Security (Online Services Security or WSS) is a feature-rich and extensible SOAP extension for securing web services. It was produced by OASIS and is part of the WS-* family of web service specifications. The protocol specifies how messages' integrity and secrecy can be ensured, as well as how different security token formats, such as SAML, Kerberos, and X.509, can be communicated. Its main focus is on end-to-end security using XML Signature and XML Encryption.

Three main mechanisms are described by WS-Security:

- How to ensure the integrity of SOAP messages by signing them. Non-repudiation is another benefit of signed messages.
- How to ensure the confidentiality of SOAP messages by encrypting them.
- How to use security tokens to verify the identity of the sender.

- The specification supports a wide range of signature formats, encryption techniques, and numerous trust domains, as well as a wide range of security token types, including X.509 certificates, Kerberos tickets, UserID/Password credentials, SAML-Assertion, and Custom defined tokens.

The accompanying profile documents specify the token forms and semantics. In the application layer, WS-Security includes security characteristics in the header of a SOAP message. These technologies do not provide a complete security solution for Web services by themselves. Instead, this standard serves as a foundation that may be combined with other Web service extensions and application-specific protocols at a higher level to support a wide range of security models and technologies. In general, WSS does not provide any assurance of security on its own. It is the responsibility of the implementer to guarantee that the framework and syntax are not susceptible when they are implemented and used. Transport Layer Security (no WS-security), other situations include end-to-end security, non-repudiation, alternative transport bindings, reverse proxy/common security token, and more. However, the following factors may have a significant impact:[11]

- The overhead of XML SIG and XML ENC is high, if the two parties exchange messages frequently between the service provider and the consumer. If end-to-end security is necessary, a protocol like WS-Secure Conversation can help. Use only encryption or signing if necessary, as the combination of the two is substantially slower than the sum of the individual operations.[5] See the Performance section for further information.
- Merging multiple XML schemata such as SOAP, SAML, XML ENC, and XML SIG may result in Depends on different library function versions such as canonicalization and parsing, which can be challenging to handle in an application server.[7]

Online sites and web applications (web apps) face a variety of security concerns [3]. Data centres and other assets used to host websites and their associated systems must be safeguarded against any threats. Application threat modelling should be used to identify threats, which should subsequently be analysed using a vulnerability assessment.[6] Vulnerabilities can be eliminated or reduced, and countermeasures can be implemented to lessen the impact of an incident if the threat is realised[6]. The following are the most common types of threats to web systems:

- ➢ Loss or damage to equipment due to fire, smoke, water, and other fire suppressants, dust, theft, and physical impact are all examples of physical hazards. Physical impact can occur as a consequence of a collision or as a result of intentional or unintentional damage by individuals. Depending on the sort of backup power available and how reliable it is, power outage will influence the ability of servers and network equipment to operate [16]. Operator or user errors such as inadvertent data deletion or destruction of software programmes, setups or hardware are examples of human errors. People also make the mistake of leaving software with flaws (vulnerabilities).

- This can include privilege escalation, by passable authentication, wrong encryption implementation, inability to check input and output data, poor session management, incorrect error handling, and so on. Good programming methods can help to reduce the vulnerabilities that can be exploited by human mistake. A website or web application's functioning can be harmed by both equipment and software malfunctions [8]. To be able to assess the threats, all assets essential for the online system's operation must be recognized. Program failure is frequently caused by poor development techniques, such as the absence of security in the software development life cycle.
- Malware, often known as harmful software, comes in a variety of forms. Web servers are common targets for assisting in the propagation of such programmes, as are sites with vulnerabilities that allow this. Spoofing, in which a machine adopts the identity of another and masquerading, in which a user assumes the identity of another, usually with higher privileges, can be used to poison data, deny service, or harm online systems[10]. Prior to an attack, online systems are typically scanned as part of network or application fingerprinting, but brute force and dictionary attacks on usernames, passwords, and encryption keys are also common. Data monitoring (on the network or on the displays of users) can be used to discover passwords and other sensitive information.
- Examining 'discovered' data from publicly available sources including the internet, search engines, and garbage. Although the real target information may be discovered, scavenging is most commonly used to identify other threats for online system vulnerabilities that are known to exist. Excessive traffic overloading might result in denial of service for other users or system failure. Using network attack techniques like tunneling to get access to low-level system functions, a router or server can be taken over[9]. Once an attacker gets control, he or she can utilize it to attack other assets needed to keep a website running.
- **Phishing:** The word refers to attacks in which the target is induced to assume that he or she is on a legal website when, in fact, it is a clone of the original. This assault takes use of the fact that anyone can make a website or any other website can look like any other. Phishing attempts have been reported on workplace email websites (webmail), public email websites (such as Gmail), and prominent websites such as Amazon and eBay[13]. A phishing website can be identified in a variety of ways. The first step is to examine the URL. Another effective preventative strategy is to never click on links in emails and instead type them in or bookmark them. Although not perfect, these techniques make it more difficult for scammers to succeed.
- **Web browser exploits:** Cybercriminals have also created websites that take advantage of security flaws in web browsers. This method allows them to acquire access to the victim's computer without the victim's knowledge. Web browsers are sophisticated pieces of software. They must deal with a variety of file formats, including graphics, sound, and HTML, as well as Javascript and a variety of other technologies[17]. All of these characteristics increase the attack surface of the web browser, making it rather vulnerable in terms of security.

- **Third party add-ons:** Third-party add-ons such as Adobe Flash player and Acrobat Reader are required by the majority of websites. Cybercriminals have turned their attention to both of these frequently utilised goods. It is becoming more difficult to utilise web browsers as an attack vector as more administrators and home users update their devices provides the most recent browser security updates and patches, as well as the ability to automate the procedure. However, while they may be updating their browser software, many consumers neglect to update third-party add-ons like Flash Player.[8] The PDF file format, Adobe Acrobat, Flash, a variety of ActiveX components, and Java were all abused by malware "in the wild" (on the Internet) in 2009[13]. These third-party add-ons are used to direct users to other infected websites. While attackers are attracted to automating remote code execution, there are situations when this level of sophistication is not required to compromise end-user systems. Some assaults, in fact, still rely on end users downloading executable files. Legitimate websites, some of which are well-known, are being hacked to aid attackers. As soon as these sites are infested, malware can be served, taking advantage of a user's predisposition to trust content based on its reputation. Many people will oblige if a respectable news site asks them to download an executable file (e.g., codec) in order to view an interesting video. Malware authors employ a variety of tactics to persuade users to visit poisoned websites, search results, and download executables[17]. Users are advised to either download software to keep up in process of seeing the material or else malware will be downloaded while they are viewing it.
- **Hybrid attack:** While the web provides far more opportunities for attackers, email remains a potent tool. When the hazards are multiplied via the internet, the risk of the user becoming a willing prey is very great. Using current events to disseminate malware spam is a popular tactic. Emails ostensibly offering exclusive news, films, or files are common online traps that lead to the opening of harmful attachments or redirection to infected or false websites. When a workstation becomes infected, some administrators may feel compelled to just reinstall the operating system; however, a prudent system administrator or security analyst would first analyse and assess the problem. Each of these jobs necessitates the expenditure of time and resources[12]. People must quit working, and hardware must be replaced, among other things. Furthermore, some malware is designed to cause a denial of service, raising the risk of an attack on the organization's infrastructure. While most businesses recognize the impact of denial of service on productivity, many overlook the impact on confidentiality and integrity[14]. Attackers have been known to steal sensitive information from hacked systems in order to carry out more sophisticated network attacks. If they gain access to the organization's data, they can benefit by selling it to outside parties. Modern malware can develop an automated procedure for harvesting data from a compromised network. Because most networks trust systems on the inside, an attacker's work is substantially easier once he or she is on the inside. This is why the bad guys find targeting online visitors via compromised websites so appealing. The internal network already has end-users and their web browsers. In contrast to traditional network-based attacks, the victim connects to the

attacker rather than vice versa[16]. Most defenses, even today, are still focused on stopping attackers from connecting to the target, i.e., protecting the perimeter. As a result, the following are the most important requirements:

- **Security policies:** Education is insufficient on its own. Organizations require enforceable security and user policies. These standards must be reasonable, allowing personnel to conduct their jobs but restricting acts that could compromise security. Because many security rules and solutions have an influence on usability, this is easier said than done. As a result, a skilled security analyst faces a difficult task in balancing security and assisting employees in delivering and being productive[15]. When standards are overly strict, employees will discover ways to go around them or become less productive, which is an unsustainable and intolerable position for a corporation. Security policies are necessary, but they are only effective if they are followed and users are aware of them.

- **Using technology:** Although administrators are adept at working with technology, they are constrained when it comes to dealing with people. Policies and education are necessary, yet there are still many who do not care. They will open a file or click on a link if they want to. As a result, administrators must add technology to their arsenal. Anti-spam and anti-phishing software, for example, will minimise the amount of unsolicited email that reaches the end-user, lowering the chance of phishing scams and email redirects. End-users cannot (and should not) be counted on to adhere to policies to the letter. One of the most fundamental approaches for detecting unauthorised online traffic is bandwidth monitoring. If an employee only visits a few websites each day on average, but this behaviour changes dramatically, the administration should investigate[14]. It's possible that the employee's surfing habits have changed, but it's also possible that the machine has been compromised. For network and security professionals, bandwidth monitoring is a critical tool.
- **Content filtering:** While bandwidth monitoring provides a broad picture of what is going on, it does not provide a detailed analysis. Administrators can choose web material by file type and location using content filtering technologies for the web. Because the bad guys prefer certain file types on the internet, filtering content by file type is a powerful tool. approach to safeguard web browsers without compromising usability. For example, this type of solution could be used to prevent web content from executing on the client, such as exe files or installation files[16]. Filtering content does not alleviate all of the security issues that come with web clients. Malicious attackers, in fact, make use of file types or site addresses that are more vulnerable. In reality, malicious attackers frequently utilise file types or site addresses that are also used for legal purposes. HTML, for example, does not usually include any dangerous code. Attackers often evade most content filtering that depends on restricting certain file types by embedding exploit code in HTML files. As a result, having an antivirus solution – preferably with multiple antivirus engines – is still quite useful, particularly if the antivirus solution is good at

catching this type of harmful content. Antivirus software installed at a strategic location, such as a web gateway or proxy, has a number of advantages. It may be administered from a central location and is distinct from the computer of the end-user, which may already be infected[18]. Prevention is merely one component of a comprehensive strategy to combat web-based risks. Regular monitoring and auditing will aid in the detection of any security breaches. Some security situations are handled incorrectly, which is one reason why they are more serious than they should be. An incident response strategy is generally used in case of web threats. An incident response plan for web threats often includes items like roles and duties as well as processes for responding to occurrences, including instructions on preparedness, identification, containment, and recovery.

CONCLUSION: The phenomena of the World Wide Web now known as W3C have been concluded. Actually, this study found that multimedia plays a vital role in the dynamism of information technology, which has transformed the world entire world on the same platform, although certain constituents support it in order to be closer to modernization. The World Wide Web Consortium (W3C), led by Berners-Lee, is responsible for many of the publications, although others were created by the Internet Engineering Task Force (IETF) and other organizations. When it comes to web standards, the following publications are usually considered foundational: W3C recommendations for markup languages, particularly HTML and XHTML. These determine how hypertext documents are structured and interpreted[18]. W3C recommendations are for markup languages particularly HTML and XHTML. These determine how hypertext documents are structured and interpreted. Recommendations for style sheets particularly CSS from the W3C ; Ecma International's Standards for ECMAScript (typically in the form of JavaScript); and the W3C's Recommendations for the Document Object Model. Online sites and web applications (webapps) face a variety of security concerns. Centers of data and other assets used to host websites and their associated systems must be safeguarded against any threats.

REFERENCES

[1] NCSA Mosaic — September 10, 1993 Demo. Totic.org. http://totic.org/nscp/demodoc/demo.html. Retrieved July 27 **(2012)**

[2] Vice President Al Gore's ENIAC Anniversary Speech, Cs.washington.edu. February 14, 1996. http://cs.washington.edu/homes/lazowska/faculty.lecture/innovatio n/gore.html. Retrieved July 27, **(2009)**

[3] Internet legal definition of Internet, West's Encyclopedia of American Law, edition 2, Free Online Law Dictionary, July 15, 2009. http://legal-dictionary.thefreedictionary.com/Internet, Retrieved November 25, **(2008)**

[4] WWW (World Wide Web) Definition, TechTerms, http://techterms.com/definition/www. Retrieved february 19 **(2010)**

[5] The W3C Technology Stack, World Wide Web Consortium. http://www.w3.org/Consortium/technology.

Retrieved April 21, **(2009)**

[6] Hamilton Naomi, (July 31, 2008), The A-Z of Programming Languages: JavaScript, Computerworld, IDG, http://computerworld.com.au/article/255293/- z_programming_languages_javascript. Retrieved May 12, **(2009)**

[7] Buntin Seth, (23 September 2008), jQuery Polling plugin, http://buntin.org/2008/sep/23/jquery-polling-plugin/, Retrieved 2009-08-22 **(2009)**

[8] Berners-Lee, Tim, Frequently asked questions by the Press, W3C, http://w3.org/People/Berners-Lee/FAQ.html, Retrieved July 27, **(2009)**

[9] automatically adding www.____.com, mozillaZine. May 16, 2003. http://forums.mozillazine.org/viewtopic.php?f=9&t=10980. Retrieved May 27, 2009.

[10] Masnick Mike, (July 7, 2008), Microsoft Patents Adding 'www.' And '.com' To Text, Techdirt, http://techdirt.com/articles/ 20080626/0203581527.shtml, Retrieved May 27, **(2009)**

[11]. Kruegel, C., Kirda, E., Mutz, D., Robertson, W., Vigna, G.: Polymorphic Worm Detection Using Structural Information of Executables. In: Valdes, A., Zamboni, D. (eds.) RAID 2005. LNCS, vol. 3858, pp. 207–226. Springer, Heidelberg (2006)

[12]. Qassrawi, M.T., Zhang, H.: Client honeypots: approaches & challenges. In: 4th International Conference on New Trends in Information Science and Service Science, NISS (2010)

[13]. Kruegel, C., Vigna, G., Robertson, W.: A multi-model approach to the detection of web- based attacks. Computer Networks 48(5) (July 2005)

[14]. Wurzinger, P., Bilge, L., Holz, T., Goebel, J., Kruegel, C., Kirda, E.: Automatically Generating Models for Botnet Detection. In: TR-iSecLab-0609-001

[15]. Raffetseder, T., Kirda, E., Kruegel, C.: Building Anti-Phishing Browser Plug-Ins: An Experience Report. In: The 3rd International Workshop on Software Engineering for Secure Systems (SESS 2007). IEEE Computer Society Press, Minne apolis (2007)

[16]. Mitterhofer, S., Platzer, C., Kruegel, C., Kirda, E.: Server-Side Bot Detection in Massive Multiplayer Online Games. In: COPublished by the IEEE Computer and Reliability Societies (May/June 2009)

[17]. Ludl, C., McAllister, S., Kirda, E., Kruegel, C.: On the Effectiveness of Techniques to Detect Phishing Sites. In: Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA) 2007 Conference, Lucerne, Switzerland (July 2007)

[18]. Stringhini, G., Kruegel, C., Vigna, G.: Detecting Spammers on Social Networks. In: 26th Annual Computer Security Applications Conference, (ACSAC 2011), Austin (December 2010)Google Scholar