DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4220

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A SURVEY ON WEB APPLICATION ATTACK DETECTION METHODS

Kunal Gupta, Rajni Ranjan Singh
Department of CSE& IT
M.I.T.S. Gwalior, M.P. (India)

Abstract: –In the current scenario where time is money, the internet due to its versatile nature and time-saving features has influenced every age group and made them dependent on it, which has increased the internet usage exponentially. Due to a vast number of users, the internet has become more vulnerable to threats and attacks. So in this paper, we will review various existing methods to detect web application attacks that are injected by the attacker.

Keyword:–Sniffer, Deep Packet Inspection, Intrusion Detection System, Wireshark, Snort, Web Application Attack

I. INTRODUCTION

The internet by possessing innumerable features has affected the mass strongly. An individual or a corporation use the internet as their database management platform. But due to increased access to the internet worldwide, chances of exploitation have increased and hence all the classified information of any end user is vulnerable to attack and hence unfair practice by a third party [11]. Nowadays network is subjected to various Web Application attacks. Here are some of the most common Web Application Attacks that exist:

A. CROSS-SITE SCRIPTING

Cross Site Attacks are most common Network attacks across the web where we inject Payload (Malicious Code) on the client side to a website. It's a weakness found on poorly coded website which attacker exploits and tries. It uses victim's browser to deliver malicious script from a vulnerable site as vehicle. There are three actors in this attack (XSS) the attacker, the website and the victims can take use of JavaScript, Flash, VBScript and ActiveX. But mostly used is JavaScript [17].

Let us now see how does the Cross Site Scripting attack works step by step process: -

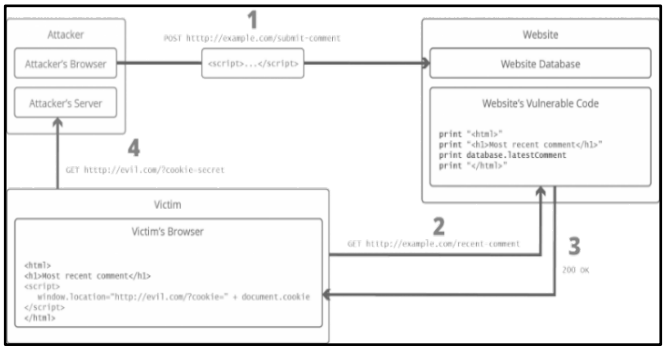


Fig. 1. – Cross Site Scripting Procedure [16]

1. Website database is infected through a payload by an attacker after submitting the form with JavaScript Code.

2. Web page from the website is requested by a victim browser.

3. Victim's Browser is served the web page that was earlier requested by the victim with the payload attached to HTML body.

4.The payload will be executed inside the Victim's browser. Now attacker server will receive the victim's cookie. Victims cookie is extracted by the attacker. He uses victim's cookie to make the HTTP request to the server. After which attacker is granted the request by the name of the victim

.

CATEGORIES OF CROSS - SITE SCRIPTING ATTACKS

1. *Stored XSS*: It takes place when a target server stores the input from the user in the form of a message a database or visited log after this data becomes the part of the website but instead of data user inputs a payload. When the stored payload is run locally, after which enables the malicious code that is saved as a data input by the user.

2. Reflected XSS: When a web application returns an error message or any other response that comprises all input provided by the user immediately after user input was made.

B. BUFFER OVERFLOW

When a process or a program attempts to write more information to block of memory or a buffer of fixed length then buffer overflow takes place. Additional information can overwrite existing data values in memory addresses next to the destination buffer except when the program contains sufficient bounds checking to flag or remove data when too much is directed to a memory buffer [22].

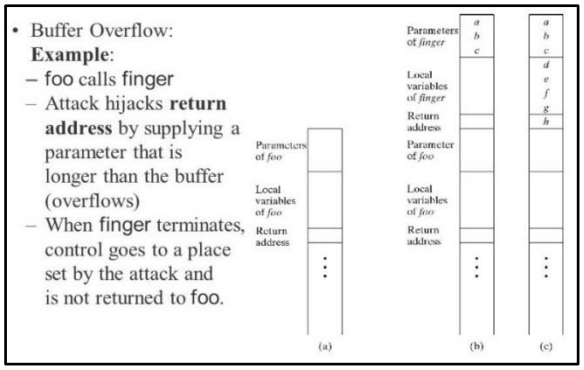


FIG. 2. – BUFFER OVERFLOW PROCEDURE USING EXAMPLE [23]

Cand C++ are liable to buffer overflow attack because they do not have built-in protection for getting into or overwriting information in some part of their memory and as actors can perform straight memory manipulation with common programming constructs. It can occur in any programming language where it is allowed to direct memory manipulation. It characterized according to the site of the buffer in the process memory, the two significant types are

1. Stack-Based Overflow:Function calls that are associated with data are used in continuous space in the memory. It also involves variables, management data, function parameters, local functions as other frameworks as welland instruction pointers.
2. Heap-Based Overflow:It is used to manage dynamic memory and is a type of memory structure. At compile time when the size of the memory is not known then heap-based overflow is used, where the volume of memory needed is too big to fit on the stack or where the memory is planned to be used in function calls.

C. SQL INJECTION

SQL injection is a security vulnerability that allows malicious users to break into the application if the application interacting with the database doesn't seem to primarily have Input Validation in place and SQL queries created using parameterized queries. Every detail which a user enters in a form while registering through a website or a payment application through a text box is stored in databases hosted by the website. SQL injection happens when the data input by the user, generally entered through text boxes, accidentally or intended deliberately to run a specific command in the database to corrupt data or to get used to potentially harming data set from the user [21].Consider for example the user is asked to enter the PAN number through a text box.

Enter Your AADHAR: _____

The user enters:ABCD12345 OR1 = 1

If the web application for front end control does not handle any additional characters and the data is directly sent to the data layer where it could get interpreted as a query.

select name, AADHAR_number from all_users where user_id = 'ABC1234' or 1=1;

This query will return all the rows from the table because 1=1 will always satisfy for all rows. There is a chance that the significant details might be showed onto the screen which the user could abuse.

We must know that the vulnerability of the system depends on how poorly each framework of the web application is designed [15]. A robust system which promptly takes care of all such susceptibilities will prevent such attacks.

D. DISTRIBUTED DENIAL OF SERVICE [DDoS]

DDoS known as Distributed Denial of Service. Is a collection of DOS (Denial of Service) attacks. It prevents legitimate users from accessing a service, generally done by a single source. It means the network is unavailable to its actual users. This can be done in various ways like flooding a web server with a large amount of fake traffic can prevent it from responding to real users. But this is helpful only when the server is weak in handling the traffics. The servers nowadays are pretty large and can handle great loads. It is not possible to attack them from a single source, so the attackers attack the server from various sources and hence it is called "Distributed Denial of Service" attack

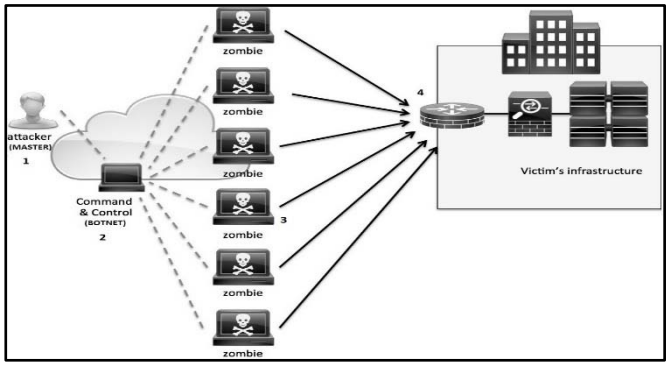


Fig. 3. – DISTRIBUTED DENIAL OF SERVICE [25]

A distributed denial of service attack uses many computers around the internet, often under control of a botnet (A botnet is a group of computers, setup for forwarding transmission of spam and viruses, generally the owner of these computers are unaware of this), to overwhelm the service.The resources of the system (bandwidth, CPU, RAM, etc) are consumed by this traffic, preventing users from accessing it.

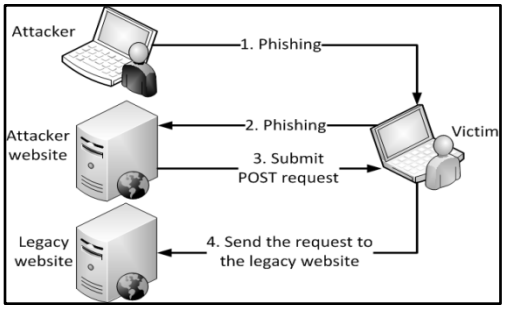


Fig. 4. – CROSS SITE REQUEST FORGERY (CSRF) PROCEDURE [24]

E. CROSS SITE REQUEST FORGERY [CSRF]

Cross-Site Request Forgery is a form of attack that arises when a malicious blog, website, email, or any other program effects a user's Web browser to execute an unwanted exploit on a trustworthy site on which a user is presently is logged on and authenticated. It works by "pretending" to be you, or more correctly, doing something with your credentials while you are completely unaware.

Due to the vast and dynamic type of attacks available on the internet we have a technology that can detect attacks that are being performed using this technology we can also create metadata of the attacks to investigate it further if needed the system that supports this technology is Intrusion Detection System (IDS). IDS uses Deep Packet Inspection Technique Let us know further about it.

INTRUSION DETECTION SYSTEM (IDS)

Intrusion Detection System inspects packets going to andfrom the network and makes a log for the packet that is involved in the attack or is vulnerable according to rules [13].

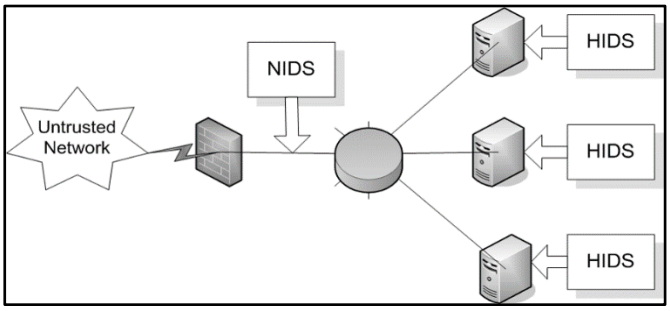


Fig. 5. –IDS ON THE BASIS OF THEIR ARCHITECTURE [20]

TYPES OF IDS ON THE BASIS OF ARCHITECTURE:

1. Host-based Intrusion Detection System (HIDS): This kind of System is placed on a Host as an Agent. They examine the activities on each host autonomously which include sniffing the Network traffic coming through and going out towards the Host.

2. Network-based Intrusion Detection System (NIDS): Thissort of System is placed on a Network. It examines the activities at the Network which include sniffing (the Cable Wire and Wireless Devices') packets and then matching them with the signature database to monitor the detection of an attack.

TYPES OF IDS ON THE BASIS OF DETECTION METHOD:

1. Signature Based Detection: This class of attack looks for a pattern or a signature to match with the incoming packets from the database. So that same attack can be prevented in future from happening again.

2. Anomaly-Based Detection: It inspects ongoing traffic and activities for any erratic behaviour on network, system that could recognize an attack.

To detect a web application, we can use signature based IDS that can help match the web application attack on the basis of its signature. Here we will review SNORT which is a signature based open source tool, it uses deep inspection for the packets to verify.

SNORT: SIGNATURE BASED IDS

Here we are using Cisco tool SNORT IDS which is lightweight and Open Source tool. We can create rules according to yourself as you need them to be [12]. We will install SNORT on the Network to inspect the network traffic data, i.e. all packets in transition and then filter out packets according to rules provided on the tool Snort. It works on the command line, it can analyze real-time traffic analysis and data flow in the network. It basically checks packet against rule written by the user. Snort rules can be written in any language, its structure is also good and it can be easily read and rules can be modified also [14].

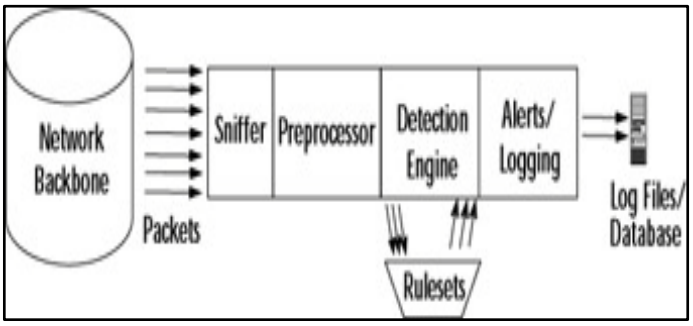


Fig. 6. – SNORT Architecture [19]

Components of Snort architecture as shown to Fig. 4.:

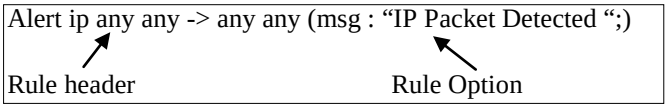
1. The Sniffer: It collects the traffic packets on the web. After collection process, it transfers the raw packet to the next component i.e. pre-processor.

2.The pre-processor: It performs certain action to conclude what kind of packet and its behaviour Snort is dealing with. After this job, packets are in transition towards detection engine.

3.The Detection Engine: It compares every packet to the predefined rule on snort.conf file. If the packets match with the rule, then it is forwarded to the output.

4. Alerts and Logging: It will trigger the alert system as well create a metadata log. The log can be saved in the variety of formats according to need. The Alert file is also generated which also contains the evidence of the attack.

RULE STRUCTURE OF SNORT



MODES IN SNORT

1. A packet sniffer: -
   In its simplest form, snort is a packet sniffer. That said, it is the easiest way to start.
2. Packet logger: -
   Snort has built-in packet-logging mechanisms that you can use to collect the data as a file, sort it into directories, or store the data as a binary file.
3. Network Intrusion Detection System: -
   To make Snort an IDS, just add one thing to the packet-logging function: the configuration file.

WIRESHARK

Wireshark is a network data packet analyser, its open source and works cross-platform (Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, etc.). It has a capability to capture packets using pcap. It has Graphical GUI and non-graphical for Linux flavours. Data can be gathered from the various interface like Ethernet, IEEE 802.11(WiFi), PPP, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and loopback. Even it can also detect VoIP calls if a compatible encoding is configured.

Wireshark has a feature for deep packet inspection of a packet at a microscopic detailed level by applying it on various levels (such as IP, MAC Address, Port No, OEM, Protocol, Length of Packet, Related Info). The live captured data packets can later be used for offline analysis [18]. It allows data to be viewed at hexadecimal level. Output can be exported in multiple formats like CSV, Plain Text, XML, etc. It is very powerful tool for forensics purpose as its very suitable for analysis.

II. EXISTING WEB APPLICATION ATTACT DETECTION TECHNIQUES

[1] Piyush A. Sonewar et al. in their work identified the threats of SQL injection and XSS Attack using .NET Framework of Windows OS. They also signified use additional security measures provision using stored procedures. The approach applied mapping model to detect SQL Injection and XSS Attack.

[2] Rathod Mahesh Pandurang et al. concluded that IDS based on a mapping model is constructed to detect and prevent SQL Injection and XSS attack. They emphasize that the restriction of the damage created by an attacker to a container will be confined to that container only if the client has itscontainer. They observed the excellence in the work of their system based on average pace time memory pages per second compared to existing one.

[3] Jinkun Pan and Xiaoguang Mao et al. found DOM XSS Micro, a Micro Benchmark for measuring DOM based XSS vulnerability also proposed a study of 6 DOM based XSS detection tools to show the use of DOM XSS Micro they plan to propose the benchmark with more betterment of each component (like complex lang. features, web framework and Libraries and Browser quirks) making it a standard benchmark.

[4] Akash Garg et al. concluded that IDS system helps in detection of dangerous attacks. Signature based IDS has usefulness for detection of known attacks whereas attack is detected by anomaly-based IDS. Snort is an open Source IDS Solution for detection if attacks as well as for prevention also by blocking the connection thus stopping entrance of any malicious attack.

[5] Hu Zhengbing et al. concluded an algorithm to find the signature of the related attack quickly, He applied scan reduction method to decrease the scanning time for a database this enables us to discover out new attacking signatures more efficiently.

[6] Vinod Kumar et al. proposes the implementation process of Snort in Debian. This IDS System showed that it can detect and analyze the intrusion. Once the Snort will identify any intrusion then it will create an alert.

[7] Hussein Alnabulsi et al. proposed a number of SNORT rules todetect SQL based attack. The SNORT rules we present show asignificant improvement in performance in detecting SQL injection attack.

[8] Mohammad Sazzadul Hoque et al.tried implemented an Intrusion Detection System by applying the geneticalgorithm to efficiently detect various types of network intrusions. To implement and measurethe performance of their system they used the standard KDD99 benchmark dataset and obtainedreasonable detection rate.

[9] Shilpi Gupta et al. They tried to detect intrusion in network for TCP protocol and detects DOS attack using packet analyser Wireshark which is an open source and cross platform tool.

[10] Yogita B. Bhavsar et al.have proposed a method of intrusion detection using SVM which can reduce the time required to build a model for classification and increase the intrusion detection accuracy when Gaussian RBF kernel is used.They have proposed a method of intrusion detection using SVM which can reduce the time required to a build model for classification and increase the intrusion detection accuracy when Gaussian RBF kernel is used. They tried to improve detection rate by some percent making it more efficient.

III. OBSERVATIONS FOR THE PAPER

- We reviewed various paper(s) and got to know that web application attack is due to vulnerable coding was done by the developer that an intruder exploits.
- The effective technique for avoiding Web application attack is to configure the security between complex and variety of devices that include Database, firewall, server, operating system, and application software.

- We also concluded that broken authentication and session management can lead to web application attack.
- IDS also produce False Positive results which sometimes can confuse Network Administrator.
- We must use proper declaration (Length and Scope) in the programming language in C and C++ to overcome Buffer Overflow attack along with best practices of defence in depth.
- CIA triad must be followed while implementing any web application to avoid any kind of web application attack.
- Web application attracts not only can lead to corrupt data for an organization but also can destroy the system by changing the personal configuration of the software, server, and other devices.
-

IV. REFERENCES

1) Piyush A. Sonewar , Nalini A. Mhetre "A Novel Approach for Detection of SQL Injection and Cross Site Scripting Attacks" International Conference on Pervasive Computing (ICPC) 2015.
2) Rathod Mahesh Pandurang, Dr. Deepak C. Karia "Impact Analysis of Preventing Cross Site Scripting and SQL Injection Attacks on Web Application" 2015 IEEE Bombay Section Symposium (IBSS)
3) Jinkun Pan, Xiaoguang Mao "DomXssMicro: A Micro Benchmark for Evaluating DOM-based Cross-Site Scripting Detection" 2016 IEEE TrustCom/BigDataSE/ISPA2324-9013/16 2016
4) Akash Garg, Prachi Maheshwari "Performance Analysis of Snort-based Intrusion Detection System" IEEE 2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS -2016), Jan. 22 – 23, 2016, Coimbatore, INDIA
5) Hu Zhengbing, Li Zhitang, Wu Junqi "A Novel Network Intrusion Detection System(NIDS) Based onSignatures Search of Data Mining" IEEE 2008 Workshop on Knowledge Discovery and Data Mining 10-16
6) Vinod Kumar, Dr. Om Prakash Sangwan "Signature Based Intrusion Detection System Using SNORT" International Journal of Computer Applications & Information Technology Vol. I, Issue III, November 2012 (ISSN: 2278-7720)
7) H. Alnabulsi, M. R. Islam and Q. Mamun, "Detecting SQL injection attacks using SNORT IDS," *Asia-Pacific World Congress on Computer Science and Engineering*, Nadi, 2014, pp. 1-7. doi: 10.1109/APWCCSE.2014.7053873
8) Mohammad Sazzadul Hoque, Md. Abdul Mukit , Md. Abu Naser Bikas "AN IMPLEMENTATION OF INTRUSION DETECTIONSYSTEM USING GENETIC ALGORITHM" International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012
9) Shilpi Gupta, Roopal Mamtora "Intrusion Detection System Using Wireshark" International Journal of Advanced Research in Computer Science and Software EngineeringVolume 2, Issue 11, November 2012.
10) Yogita B. Bhavsar, Kalyani C.Waghmare "Intrusion Detection System Using Data Mining Technique: Support Vector Machine" International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 3, March 2013)
11) Hossein Jadidoleslamy "Weaknesses, Vulnerabilities And Elusion Strategies Against Intrusion Detection Systems" International Journal Of Computer Science & Engineering Survey (IJCSES) Vol.3, No.4, August 2012.
12) Mr. Chandrapal U. Chauhan Mrs. V.A. Gulhane" Signature Based Rule Matching Technique in Network Intrusion Detection System" International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 4, April 2012.
13) Kapil Wankhade, Sadia Patka and Ravinndra Thool,"An efficient approach for intrusion detection using data mining methods", IEEE, 2013.
14) Natttawat Khamphakdee, Nunnapus Benjamas andSaiyan Saiyod, "Improving intrusion detectionsystem based on snort rules for network probe attackdetection", International conference on informationand communication technology, IEEE, 2014.
15) Alnabulsi, H.; Islam, M.R.; Mamun, Q., "Detecting SQL injectionattacks using SNORT IDS," Computer Science and Engineering (APWCon CSE), 2014 Asia-Pacific World Congress on, vol., no., pp.1,7, 4-5Nov. 2014.
16) OWASPhttps://www.owasp.org/index.php/Top 10 2013-Top10".
17) Johari, R.; Sharma, P., "A Survey on Web Application Vulnerabilities(SQLIA, XSS) Exploitation and Security Engine for SQL Injection,"Communication Systems and Network Technologies (CSNT), 2012 InternationalConference on, vol., no., pp.453,458, 11-13 May 2012.
18) Dukes, L.; Xiaohong Yuan; Akowuah, F., "A case study on web applicationsecurity testing with tools and manual testing," Southeastcon, 2013Proceedings of IEEE, vol., no., pp.1,6, 4-7 April 2013.
19) Snort's Features http://flylib.com/books/en/3.100.1.200/1/
20) Types of IDS (NIDS and HIDS) https://keamanan-informasi.stei.itb.ac.id/2013/10/30/menangani-serangan-intrusi-menggunakan-ids-dan-ips/
21) Alnabulsi, H.; Islam, M.R.; Mamun, Q., "Detecting SQL injectionattacks using SNORT IDS," Computer Science and Engineering (APWCon CSE), 2014 Asia-Pacific World Congress on, vol., no., pp.1,7, 4-5, Nov. 2014.
22) http://searchsecurity.techtarget.com/definition/buffer-overflow
23) http://slideplayer.com/slide/2771594/10/images/7/Types+of+Attacks+Buffer+Overflow:+Example:+foo+calls+finger.jpg
24) (CSRF)https://devnet.kentico.com/getattachment/Articles/2015-03/Protection-against-Cross-site-request-forgery-(CSR/CSRF_UX_general_Flip.png
25) http://www.cisco.com/c/dam/en_us/about/security/images/csc_child_pages/white_papers/ddos_fig02.jpg