Web Application Attack Detection and Forensics: A Survey

Mohammed Babiker
Computer Engineering Department.
Anadolu University
Eskisehir, Turkey
mohammedbabiker@anadolu.edu.tr

Enis Karaarslan
Computer Engineering Department.
Mugla Sitki Kocman University
Mugla, Turkey
enis.karaarslan@mu.edu.tr

Yasar Hoscan
Computer Engineering Department.
Anadolu University
Eskisehir, Turkey
hoscan@anadolu.edu.tr

***Abstract*— Web application attacks are an increasingly important area in information security and digital forensics. It has been observed that attackers are developing the capability to bypass security controls and launch a large number of sophisticated attacks. Several attempts have been made to address these attacks using a wide range of technology and one of the greatest challenges is responding to new and unknown attacks in an effective way. This study aims to investigate the techniques and solutions used to detect attacks, such as firewalls, intrusion detection systems, honeypots and forensic techniques. Data mining and machine learning techniques, which attempt to address traditional technology shortcomings and produce more effective solutions, are also investigated. It was aimed to contribute to this growing area of research by exploring more intelligent and convenient techniques for web application attack detection by focusing on the data mining techniques in forensics.**

Keywords*— Web application attacks; Digital forensics; Data mining; Web application attack detectionl; Web application forensics

I. INTRODUCTION

Web applications are essential for a wide range of applications, including e-governments, e-commerce, social network sites, blogs, content management systems, and web emails, etc., which are accessed by millions of Internet users on a daily basis. The richness of web applications and advanced functionality, as well as ease of access and availability has led most businesses to rely on them more heavily. Unfortunately, for the same reasons, web applications have become a target by attackers. Major security weaknesses have made web applications vulnerable to numerous serious and successful attacks, and there are several studies in the literature that confirm the gravity of web applications in lunching seriousness attacks against them [1–9]. It has been reported that 92% of web-based applications are vulnerable and 75% of all attacks on information security was targeted using web applications [10], 70% of web-based attacks are successful [11], and web applications experience up to 27 attacks per minute [12]. Consequently, there are also numerous reports of successful security breaches and exploitations according to the latest statistics from Impreva [13] and Symantec [14].

The process of tracking and detecting web attacks has become complex and traditional methods are ineffective [15]. Moreover, web attack forensics faces challenges caused by the huge amount of data being generated by networks. It is difficult for forensic investigators to set aside time to analyze the massive amount of data within an intrusion detection system and firewall logs, as well as logs generated by network services and applications [16].

This paper aimed to investigate the techniques used in the detection and forensics of web application attacks, which will be used in upcoming studies.

This paper begins by focusing the fundamentals, such as the main reasons for web application attacks, and data mining and machine learning; Section 3 will focus on the detection techniques; Section 4 will discuss the forensic challenges and methods; and finally, the results and possible future work will be discussed.

II. FUNDAMENTALS

A. Web Application Attacks

The term “web application attack” refers to an attack where the weakness of the web application code is exploited, and taken as an advantage to compromise the security of the back-end systems [17]. Consequently, numerous classifications are used to classify web application attacks, and the most common classifications are OWASP top 10 [18] and Sans top 25 [19]. Widely varying web attacks taxonomy will almost certainly more evolve in the future; thereby, precise framework will contribute and assist in the development of detection applications.

In recent years, there have been an increasing interest in web application security, but security weaknesses are also increasing. Integration technologies in the web application, such as client-side, server-side code, application logic and database back-end hosting, may have been an important factor in the security weakness [20]. Figure 1 reveals that there has been a marked weakness in web server, security controls, and database server. The most likely causes of this weakness are:

978-1-5386-3449-3/18/$31.00 ©2018 IEEE

Authorized licensed use limited to: ULAKBIM UASL - Mugla Universitesi. Downloaded on February 01,2021 at 07:44:56 UTC from IEEE Xplore. Restrictions apply.

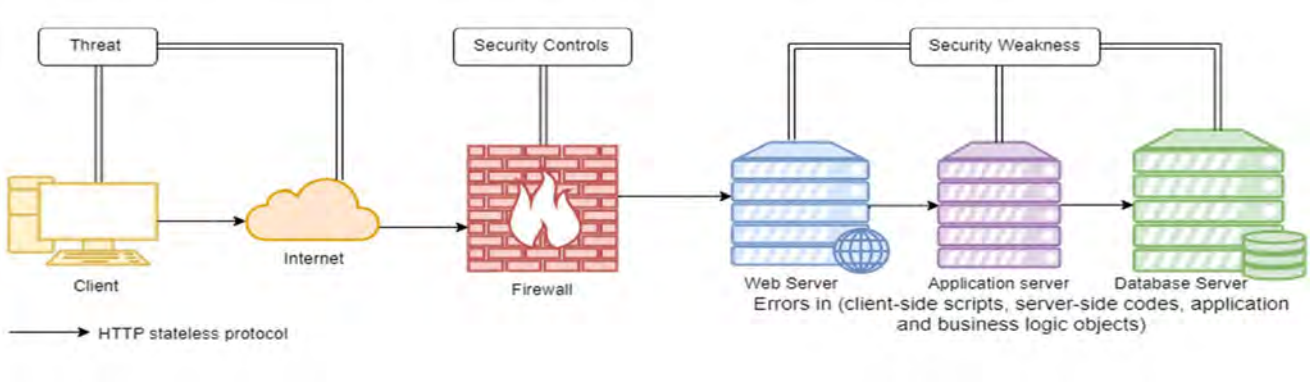

Fig. 1. Security Weakness and Threats in the Multi-Layer Web Application Architecture.

- Poor coding and misconfiguration [21-22].
- Hypertext transfer protocol (HTTP) design, which fails to keep pace with today complex structures of web applications [23].

Current methods of s security have proven to be unreliable, and an accessible web application in front end could be exploited by various types of attacks [23].

B. Data Mining

Data mining has been used to refer to methods in which interesting knowledge or pattern from large-scale of data extracted in order to help in decision making [24]. As consequence of the availability of massive-data with the urgent need to analyze and extract useful information, classical data analysis techniques are insufficient and better solutions had to be found [26]. Therefore, data mining integrated different fields such as statistics, machine learning, database and artificial intelligence [27]. The specific objective of data mining techniques is to create a descriptive model or a predictive model [28]. The descriptive model usually builds to characterize the general descriptive properties of datasets with helping of statistics techniques [29]. By contrast, predictive model analyzes dataset to build models in order to predict the future actions of new coming data. Predictive data mining includes: association rules, classification, regression analysis, and trend analysis [25]. Data mining is proved to be effective and worth in many applications because it contains techniques to process computerized search and to extract a pattern from large-scale, also analysis a large amount of data to find a logical relationship and transform data in a new way to be understood for further use.

C. Machine Learning

"Machine Learning", which is implicitly programming computers by applying the theory of statistic and mathematical models for better optimization using example data or past experience [30]. A key aspect of machine learning is the ability to automate solving of problems and tasks [31]. In order to achieve this desired goal, two methods of learning are used: supervised learning includes (classification, support vector machines, neural networks) and unsupervised learning includes (clustering, dimensionality reduction, recommender systems, distance, and normalization). Despite the similarity between the learning methods in the practical, though the difference lies on the reason of usage. For example, in the absence of prior knowledge of the dataset unsupervised learning is used while the supervised learning is used if the prior knowledge exists [32].

III. DETECTION OF THE WEB APPLICATION ATTACKS

Many researchers are making efforts on detection and prevention of web application attacks. Thus far, a variety of techniques have developed to solve this emerging problem. There are two basic detection methods currently being adopted in research [33]:

- Anomaly-based: Anomaly-based techniques are able to detect unknown attacks due to the ability to learn. Regrettably, anomaly-based sacrifices performance and accuracy with high false positive.
- Signature-based: Signature-based techniques rely on predefined rules of attack signatures which allow it to achieve very high accuracy in detect known attacks and less prone to false positives; however, it fails in the detection of new and unknown attacks.

Both anomaly-based and signature-based are applied on many security solutions [34]. Generally, they take place in analyze attack in HTTP traffic from the external behavior of an application perspective [35].

The following part of this paper moves on to describe in greater detail the current detection techniques. Those techniques may be divided into three main technologies which are:

- Web Application Firewall
- Application Intrusion Detection System
- Web Application Honeypots

A. Web Application Firewall

Web application firewall (WAF) is one of the most widely used solutions for detection and prevention web application attacks. Besides, the ability to work in the application-level layer may have been an important factor in control traffic on web

Authorized licensed use limited to: ULAKBIM UASL - Mugla Universitesi. Downloaded on February 01,2021 at 07:44:56 UTC from IEEE Xplore. Restrictions apply.

server and detect malicious one [36]. Many scholars hold the view that WAF effective in preventing breaches and mitigate attacks [37]. Even so, it suffers from some serious weakness.

Over the past 10 years, there have been a significant criticism of web application firewall. These criticisms against both specific implementation and commercial products [38], also in the ability to evade WAF by some attacks [39]. The past decade has seen the rapid development and enhancement of the WAF as software and hardware [40]. Notwithstanding, there are still shortcomings as a result of predefined rules technique and inability to recognize high-level application logic.

There are many limitations of web application firewall which make it an inefficient solution. These are high false negatives and high false positives rates, low accuracy and inability to detect unknown attack, in addition to increase of operational cost and manual efforts [41-44]. Recently, these web application firewall limitations have been addressed by researchers in many ways. For example, applying automation techniques, such as machine learning and data mining algorithms as in [45] [46]; however, it will raise the question of performance as the web applications work in real-time with high traffic. Paradoxically, applying techniques to enhance the performance of data mining and machine learning algorithms will also result in a reduction of accuracy [45]. Likewise, deploying hardware web application firewall to withstand the pressure of the performance can result to a high cost.

B. Application Intrusion Detection System

The researchers emerged to new types of detection system called an Application Intrusion Detection System (AIDS) to overcome the limitations of the WAF [47]. As a matter of fact, AIDS overcome network based IDS problems [48]. Furthermore, AIDS can work side by side with the firewalls to enhance the protection and add a new layer of security to impede the web attacks.

In general, IDS use signature-based or anomaly based detection techniques, sometimes mix between those two methods. It has become commonplace to distinguish 'signature-based' from 'anomaly-based' methods of detection. Likewise, there is a widely held view that signature-based outperforms anomaly-based in known attacks. Owing to that, signature-based has adopted in the commercial products while there is less use of anomaly-based in commercial. Anomaly-based has more focus in research, because of its ability to combat unknown attacks.

AIDS was built and improved by a number of techniques as in [49-51]. Otherwise, criticisms of much of the literature on AIDS in suffering from some serious limitation. For example, multi-level encoding attack and encrypted traffic could evade and bypass Intrusion Detection Systems [52-53], coupled with low performance, high cost and weak detection accuracy [54]. More recently, literature has emerged data-mining and machine learning to settle AIDS shortcomings. Algorithms such as decision tree, support vector machine, logistic regression, feature extraction and pattern recognition have proven their potential in attaining high attack detection accuracy with good performance and low false rates [55-56]. On the contrary, association rules, frequent episodes and clustering methods like k-means, fuzzy c-mean in addition to naïve-bayes fail in accuracy and introduce more complexity [78].

C. Web Application Honeypot

Turning now to Honeypot, WAF and IDS are close and use same techniques as it can be seen in the Table 1. In contrast honeypot uses techniques which are fundamentally different. Its value becomes evident during attacks or probes. It plays decoy and trap role for malicious traffic in order to supply unique information which cannot be obtained from the other techniques [57]. Honeypot is categorized into two types; research and product honeypot. The goal of the product honeypot is to directly secure the companies or organizations. The research honeypot aims to collect information about attackers and attacks to provide indirect security. Meanwhile, honeypot can be categorized according to the level of interaction, depending on the services it simulates and resources, to high interaction honeypots and low interaction honeypots [58].

Honeypot addresses the problem of false positives, which are experienced with WAF and IDS, by reducing the false positives resulting of gathering small but high valuable amount of information. However, the risk factor of these honeypots makes them move away from being a direct attack detection solution. The past decade has seen considerable number of projects developed on web application honeypots [59-63] which focused on the enhancement of concealment and deception. In recent years, researchers have investigated honeypot as a catalyst in the attack detection through automatic generation of signatures to IDS [64-65], observing and analysis web attacks [66], learning about tactics and motives of the attacker [67-68]. Taken together, honeypot will help in fighting cyber-crime, detect attacks and track criminals, which will improve web application detection techniques and web application forensic.

TABLE I. COMPARISON OF THE WEB APPLICATION ATTACK DETECTION TECHNIQUE FEATURES

Features	**Web Application Attack Detection Techniques**			
	Web Application Firewall	***Application Intrusion Detection System***	***Web Application Honeypot***	***Web Application Forensic***
Methods	signature-based, anomaly detection.	signature-based, anomaly detection	emulation	manual and automated log analysis
Encrypted traffic inspection	yes	no	yes	yes
Types of attacks	known web application attacks	known and unknown network and application layer attacks	known and unknown web application layer attacks	known and unknown attacks
Accuracy/False Positive	medium accuracy/high false positive	medium accuracy/high false positive	high accuracy/low false positive	high accuracy/too low false positive
Challenges	easy to bypass, cost, maintenance	high false alarm, encrypted traffic	great risk if detected	time, massive amount of data, legal constraints

Authorized licensed use limited to: ULAKBIM UASL - Mugla Universitesi. Downloaded on February 01,2021 at 07:44:56 UTC from IEEE Xplore. Restrictions apply.

IV. WEB APPLICATION FORENSICS

Web application forensic may be defined as the branch of digital forensic which is collected and analysis events, in order to trace back the source of security attacks or other incidents on a web application [69]. For example, forensic study can be needed at a failure of web application technique implementation which inevitably caused systems to be compromised. Whether these incidents need internal investigation for violating the organization's policy or a forensic investigation for violating the law, the underline techniques are similar, as well the causes of the defect must be investigated.

From a technical point of view web application forensics can be considered as:

- a posterior detection technique for attacks.
- evidence finder of the attack occurrence, investigate causes and motives of the attack afterwards.
- deep information gatherer looks for more information than the other detection techniques.

The techniques which are currently used rely heavily on the expertise and skill of the forensic investigator, also the increasing number of attacks and massive data made evidence analysis hard task even with the help of traditional forensic tools. The main source to find evidence is the log file which is collected from different servers and security devices [70].

In a recent study [71], a comprehensive survey of web application forensic tools is given. According to the survey, most of the tools focus on the compressed data, correlation of the various sources and reporting. However, a massive amount of data generated from heavy web traffic is leading traditional methods and tools to become ineffective; accompanied by increasing in time, cost and efforts [72]. As a result, researchers started to search for more effective solutions.

In order to solve mentioned challenges, researchers resorted to data mining for digital forensic analysis where the focus on extracting digital evidence from massive data with ensuring of integrity [73-74]. Decision-making process and better guidance will increase efficiency [75-76] with the attention to the goal of the forensic investigation. Thereupon, data mining helps investigators [77], digital forensics professionals and law enforcement officers. However, few pieces of research have been able to draw on any data mining application into web application forensic.

V. DISCUSSION AND CONCLUSION

Web application attacks are highly aggressive and have a higher tendency to impact business. Available detection techniques, such as web application firewalls and application intrusion detection systems have a high accuracy and performance rate for known attacks. This is due to their reliance on predefined rules and signature-based technology, which have been adopted in most commercial devices. However, the majority of available techniques were developed to progressively combat new and unknown attacks. The techniques used for anomaly-based attacks still evolving to reach the desired effectiveness. The integration of anomaly- and signature-based detection technology will significantly reduce attacks.

In this survey, we highlighted the web application forensic and web application honeypots as a post-detection technique. The differences between them and the other detection technologies are covered in detail in this paper. Those technologies have relatively limited real-time detection, but they offer valuable insights into attack detection through the analysis of successful attacks and the discovery of the unknown ones. This has contributed to other real-time attack detection technologies, such as web application firewalls and application intrusion detection systems. Web application forensics and honeypots collect a massive amount of data. Data-mining can be applied to this data with a number of criteria, such as the preservation of digital evidence and data analysis, accuracy, and reliability. Descriptive and predictive data modeling could help in limiting the investigation resources, anomaly detection of the attacks, and behavioral profiling. Together, these mining techniques have the potential to lead to a significant improvement in the efforts of detecting attacks. Future studies will include testing the effectiveness of data mining in the web application attack forensics and feature- selection for web application attacks evidence.

REFERENCES

[1] Watson. David, "The evolution of web application attacks," Network Security. Vol. 11, pp. 7-12. 2007.

[2] Fogie Seth, Jeremiah Grossman, Robert Hansen, Petko D. Petkov, and Anton Rager, "XSS Exploits: cross site scripting attacks and defense," US: Syngress, 2007.

[3] Fonseca J., Vieira M., Madeira H., "Vulnerability & attack injection for web applications," International Conference on Dependable Systems & Networks, IEEE/IFIP, 2009. 93-102, July 2009.

[4] Dwen Ren Tsai, Chang, A.Y., Peichi Liu, Hsuan Chang Chen, "Optimum tuning of defense settings for common attacks on the web applications," International Carnahan Conference on Security Technology, 43rd Annual. 89-94, 5-8 Oct. 2009.

[5] Martin Szydlowski, Christopher Kruegel, EnginKirda., "Secure Input for web Applications," Twenty Third Annual Computer Security Applications Conference .2007.375-384.

[6] Yu-Chin Cheng, Chi-Sung Laih, Gu-Hsin Lai, Chia-Mei Chen, Tsuhan Chen., "Defending On-Line Web Application Security with User-Behavior Surveillance," Third International Conference on Availability, Reliability and Security. 2008. 410-415.

[7] D. Gollmann, "Securing Web Applications," Information Security Technical Report, vol. 13, issue. 1, Elsevier Advanced Technology Publications Oxford, 2008.

[8] S. McClure, J. Scambray, and G. Kurtz, Hacking Exposed: Network Security Secrets and Solutions, 4th ed. Emeryville, CA: McGraw-Hill/ Osborne, 2003.

[9] W. Halfond, A. Orso and P. Manolios, "WASP: Protecting Web Applications Using Positive Tainting and Syntax-Aware Evaluation," in IEEE Transactions on Software Engineering, vol. 34, no. 1, pp. 65-81, Jan.-Feb. 2008.

[10] M. A. Wazzan and M. H. Awadh, "Towards Improving Web Attack Detection: Highlighting the Significant Factors," IT Convergence and Security (ICITCS), 2015 5th International Conference on, Kuala Lumpur, 2015, pp. 1-5.

Authorized licensed use limited to: ULAKBIM UASL - Mugla Universitesi. Downloaded on February 01,2021 at 07:44:56 UTC from IEEE Xplore. Restrictions apply.

[11] A. Tekerek, C. Gemci and O. F. Bay, "Development of a hybrid web application firewall to prevent web based attacks," Application of Information and Communication Technologies (AICT), 2014 IEEE 8th International Conference on, Astana, 2014.

[12] D. Appelt, C. D. Nguyen and L. Briand, "Behind an Application Firewall, Are We Safe from SQL Injection Attacks?," Software Testing, Verification and Validation (ICST), 2015 IEEE 8th International Conference on, Graz, 2015, pp. 1-10.

[13] Impreva, "2015 Web Application Attack Report (WAAR)" Impreva, 2015.: Retrieved December 25, 2017, from Impreva website: https://www.imperva.com/docs/HII_Web_Application_Attack_Report_Ed6.pdf.

[14] Symantec, "Symatec`s Internet Security Threat Report" Symantec, 2017 Volume 22 (Rep.). Retrieved December 25, 2017, from Symantec website: https://www.symantec.com/security-center/threat-report

[15] D. Mitropoulos, P. Louridas, M. Polychronakis and A. D. Keromytis, "Defending Against Web Application Attacks: Approaches, Challenges and Implications," in IEEE Transactions on Dependable and Secure Computing, vol. PP, no. 99, pp. 1-1.

[16] P. K. Khobragade and L. G. Malik, "Data Generation and Analysis for Digital Forensic Application Using Data Mining," 2014 Fourth International Conference on Communication Systems and Network Technologies, Bhopal, 2014, pp. 458-462.

[17] Justin Crist, "Web Based Attacks, SANS Institute," Sans 2007: Retrieved December 25, 2017 from http://www.sans.org/reading_room/whitepapers/application/web-based-attacks_2053.

[18] OWASP, "OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risks," 1st ed. The open web security project, 2017, pp. 1-25.

[19] B. Martin, M. Brown, A. Paller and D. Kirby, "CWE/SANS top 25 most dangerous software errors," The MITRE Corporation, 2011. Michele Bugliesi, Stefano Calzavara, Riccardo Focardi, Formal methods for web security, Journal of Logical and Algebraic Methods in Programming, Volume 87, 2017, Pages 110-126.

[20] Michele Bugliesi, Stefano Calzavara, Riccardo Focardi, "Formal methods for web security," Journal of Logical and Algebraic Methods in Programming, Volume 87, 2017, Pages 110-126.

[21] M. K. Gupta, M. C. Govil and G. Singh, "Static analysis approaches to detect SQL injection and cross site scripting vulnerabilities in web applications: A survey," International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), Jaipur, 2014, pp. 1-5.

[22] N. Antunes and M. Vieira, "Detecting SQL Injection Vulnerabilities in Web Services," 2009 Fourth Latin-American Symposium on Dependable Computing, Joao Pessoa, 2009, pp. 17-24.

[23] Z. Ghanbari, Y. Rahmani, H. Ghaffarian and M. H. Ahmadzadegan, "Comparative approach to web application firewalls," 2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), Tehran, 2015, pp. 808-812.

[24] A. Alzahrani, A. Alqazzaz, Y. Zhu, H. Fu and N. Almashfi, "Web Application Security Tools Analysis," 2017 IEEE 3rd international conference on big data security on cloud (bigdatasecurity), IEEE international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids), Beijing, 2017, pp. 237-242.

[25] J. Han and M. Kamber, Data Mining: Concepts and Techniques. Morgan Kaufman, 2001.

[26] R. J. Roiger and M. W. Geatz. Data Mining: A Tutorial Based Primer. Addison-Wesley, 2003.

[27] N. Mirza, B. Patil, T. Mirza and R. Auti, "Evaluating efficiency of classifier for email spam detector using hybrid feature selection approaches," 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, 2017, pp. 735-740.

[28] D. K.S and A. Kamath, "Survey on Techniques of Data Mining and its Applications," International Journal of Emerging Research in Management &Technology, vol. 6, no. 2, pp. 198-201, 2017.

[29] N. Jain and V. Srivastava, "Data Mining Techniques: a Survey Paper" International Journal of Research in Engineering and Technology, vol. 2, no. 11, pp. 116-119, 2013.

[30] E. Alpaydin, Introduction to machine learning, 3rd ed. Cambridge (USA): MIT Press, 2014, p. 4.

[31] K Chellapilla, and P Simard, "Using Machine Learning to Break Visual Human Interaction Proofs (HIPs)," Advances in Neural Information Processing Systems 17, Neural InformationProcessing Systems (NIPS), MIT Press, 2004.

[32] Andreas Hotho, Andreas Nurnberger, Gerhard Paaß, Fraunhofer AiS, "A Brief Survey of Text Mining," Knowledge Discovery Group Sankt Augustin, May 13, 2005s

[33] T. Kokkonen, "Anomaly-based online intrusion detection system as a sensor for cyber security situational awareness system" PH.D, University of Jyväskylä, 2016.

[34] R. Kozik, M. Choras, R. Renk, W. Holubowicz, "Patterns Extraction ´ Method for Anomaly Detection in HTTP Traffic" in Herrero A., Baruque B., Sedano J., Quintan H., Corchado E. (Eds), International Joint Conference CISIS'15 and ICEUTE'1.

[35] M. Cova, D. Balzarotti, V. Felmetsger, and G. Vigna, "Swaddler: An Approach for the Anomaly-Based Detection of State Violations in Web Applications," Proc. Int'l Symp. Recent Advances in Intrusion Detection (RAID '07), 2007.

[36] M. Solaiman, H. Mohd Husny, D. Abdullah and N. Seid, "Web Application Firewall With Telegram Bot Integration" Journal of Computing Technologies and Creative Content, vol. 2, no. 1, pp. 46-55, 2017.

[37] O. Olawumi, A. Väänänen, K. Haataja and P. Toivanen, "security issues in smart home and mobile health system: threat analysis, possible countermeasures and lessons learned" International Journal on Information Technologies & Security, vol. 9, no. 1, pp. 31-50, 2017.

[38] Justin Clarke, SQL Injection Attacks And Defense, Syngress Publishing Inc., 2009.

[39] P. Byrne, "Application firewalls in a defence-in-depth design" Network Security, vol. 2006, no. 9, pp. 9-11, 2006.

[40] Helen Kapodistria, Sarandis Mitropoulos, Christos Douligeris, (2011) "An advanced web attack detection and prevention tool", Information Management & Computer Security, Vol. 19 Iss: 5, pp.280 – 299

[41] W. C. Jia, R. G. Hu and F. Shi, "Feature Design and Selection Based on Web Application-Oriented Active Threat Awareness Model," 2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC), Harbin, 2016, pp. 597-600.

[42] S. Prandl, M. Lazarescu, and D.-S. Pham, "A Study of Web Application Firewall Solutions," in Information Systems Security, ed: Springer, 2015, pp. 501-510.

[43] D. Shugrue, "Fighting application threats with cloud-based WAFs" Network Security, Vol.2017(6), pp.5-8, 2017

[44] D. Appelt, A. Panichella and L. Briand, "Automatically Repairing Web Application Firewalls Based on Successful SQL Injection Attacks," 2017 IEEE 28th International Symposium on Software Reliability Engineering (ISSRE), Toulouse, 2017, pp. 339-350.

[45] H. T. Nguyen, C. Torrano-Gimenez, G. Alvarez, S. P etrovic, and K. Franke., "Application of the generic feature selection measure in detection of web attacks." In The 4th International Conference, Computational Intelligence in Security for Information Systems, CISIS, pages 25-32, 2011.

[46] W. K. G. Fan, "An adaptive anomaly detection of WEB-based attacks," 2012 7th International Conference on Computer Science & Education (ICCSE), Melbourne, VIC, 2012, pp. 690-694.

[47] Yong Joon Park; Jaechul Park, "Web Application Intrusion Detection System for Input Validation Attack," Convergence and Hybrid Information Technology, 2008. ICCIT '08. Third International Conference on , vol.2, no., pp.498,504, 11-13 Nov. 2008.

[48] G. Vigna, W. Robertson, Vishal Kher and R. A. Kemmerer, "A stateful intrusion detection system for World-Wide Web servers," 19th Annual Computer Security Applications Conference, 2003. Proceedings., 2003, pp. 34-43.

Authorized licensed use limited to: ULAKBIM UASL - Mugla Universitesi. Downloaded on February 01,2021 at 07:44:56 UTC from IEEE Xplore. Restrictions apply.

[49] GarcíaAdeva, J. J. and Pikatza Atxa, J. M.. Intrusion detection in web applications using text mining. Eng. Appl. Artif. Intell.2007. 20(4):555-566.

[50] S. Niksefat, M. M. Ahaniha, B. Sadeghiyan, and M. Shajari, “Toward specification-based intrusion detection for web applications,” in Proc. Int. Conf. Recent Adv. Intrusion Detection, 2010, pp. 510–511.

[51] Y. Park and J. Park, "Web Application Intrusion Detection System for Input Validation Attack," 2008 Third International Conference on Convergence and Hybrid Information Technology, Busan, 2008, pp. 498-504.

[52] Yang, C. H., & Shen, C. H. (2009). Implement web attack detection engine with snort by using modsecurity core rules. Graduate Institute of Information and Computer Education, National Kaohsiung Normal University Kaohsiung, TAIWAN.

[53] A. Andrekanic and R. Gamble, "Architecting Web Service Attack Detection Handlers," 2012 IEEE 19th International Conference on Web Services, Honolulu, HI, 2012, pp. 130-137.

[54] Fang-Yie Leu and Tzu-Yi Yang, "A host-based real-time intrusion detection system with data mining and forensic techniques," IEEE 37th Annual 2003 International Carnahan Conference onSecurity Technology, 2003. Proceedings., 2003, pp. 580-586.

[55] A. D. Khairkar, D. D. Kshirsagar and S. Kumar, "Ontology for Detection of Web Attacks," 2013 International Conference on Communication Systems and Network Technologies, Gwalior, 2013, pp. 612-615.

[56] I. Corona and G. Giacinto, “Detection of server-side web attacks,” in Workshop on Applications of Pattern Analysis, pp. 160–166, 2010.

[57] S. Tahir and W. Iqbal, "Big Data An evolving concern for forensic investigators," Anti-Cybercrime (ICACC), 2015 First International Conference on, Riyadh, 2015, pp. 1-6.

[58] M. K. Gupta, M. C. Govil and G. Singh, "An approach to minimize false positive in SQLI vulnerabilities detection techniques through data mining," Signal Propagation and Computer Technology (ICSPCT), 2014 International Conference on, Ajmer, 2014, pp. 407-410.

[59] D. Watson and J. Riden, “The Honeynet Project: Data collection tools, infrastructure, archives and analysis,” in Proc. IEEE WOMBAT Workshop Inf. Security Threats Data Collect. Sharing, 2008, pp. 24–30.

[60] Chen, T.M. Buford, J. "Design considerations for a honeypot for SQL injection Attacks". IEEE 34th Conference on Local Computer Networks, IEEE.2009.

[61] M. M¨uter, F. Freiling, T. Holz, and J. Matthews. "A generic toolkit for converting web pplications into high-interaction honeypots". Technical report, 2007.

[62] *Glastopf Project*. Lukas Rist, 2010. Retrieved August 19, 2017, from http://glastopf.org/.

[63] A. I. Rana and B. Jennings, "Semantic Uplift of Monitoring Data to Select Policies to Manage Home Area Networks," 2012 IEEE 26th International Conference on Advanced Information Networking and Applications, Fukuoka, 2012, pp. 368-375.

[64] S. Djanali, F. Arunanto, B. A. Pratomo, A. Baihaqi, H. Studiawan and A. M. Shiddiqi, "Aggressive web application honeypot for exposing attacker's identity," 2014 The 1st International Conference on Information Technology, Computer, and Electrical Engineering, Semarang, 2014, pp. 212-216.

[65] A. Ghourabi, T. Abbes and A. Bouhoula, "Design and implementation of Web service honeypot," SoftCOM 2011, 19th International Conference on Software, Telecommunications and Computer Networks, Split, 2011, pp. 1-5.

[66] D. Miyamoto, S. Teramura, and M. Nakayama, “INTERCEPT: Highinteraction Server-type Honeypot based on Live Migration,” in Proceedings of the 7th International ICST Conference on Simulation Tools and Techniques, Mar 2014.

[67] D. K. Rahmatullah, S. M. Nasution and F. Azmi, "Implementation of low interaction web server honeypot using cubieboard," 2016 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC), Bandung, 2016, pp. 127-131.

[68] S. Djanali, F. Arunanto, B. A. Pratomo, A. Baihaqi, H. Studiawan and A. M. Shiddiqi, "Aggressive web application honeypot for exposing attacker's identity," 2014 The 1st International Conference on Information Technology, Computer, and Electrical Engineering, Semarang, 2014, pp. 212-216.

[69] A. K. Kyaw, F. Sioquim and J. Joseph, "Dictionary attack on Wordpress: Security and forensic analysis," 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec), Cape Town, 2015, pp. 158-164.

[70] Chinyang Henry Tseng, Chun-Wei Lai, Tong-Ying Juang, "Automatic Web-Log Filtering Mechanism for Web Attack Digital Forensics," Journal of Internet Technology, vol. 18, no. 6 , pp. 1451-1459, Nov. 2017.

[71] A. Lazzez and T. Slimani, 'Forensics Investigation of Web Application Security Attacks', International Journal of Computer Network and Information Security (IJCNIS), vol. 7, no. 3, p. 10, 2015.

[72] P. K. Khobragade and L. G. Malik, "Data Generation and Analysis for Digital Forensic Application Using Data Mining," Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on, Bhopal, 2014, pp. 458-462.

[73] K. K. Sindhu and B. B. Meshram, Digital Forensics and Cyber Crime Data Mining, Journal of Information Security, Vol. 3 No. 3, 2012, pp. 196-201.

[74] M. Quintana, S. Uribe, F. Sánchez and F. Álvarez, "Recommendation techniques in forensic data analysis: a new approach," Imaging for Crime Prevention and Detection (ICDP-15), 6th International Conference on, London, 2015, pp. 1-5.

[75] Mouhtaropoulos, P. Dimotikalis and Chang-Tsun Li, "Applying a Digital forensic readiness framework: Three case studies," Technologies for Homeland Security (HST), 2013 IEEE International Conference on, Waltham, MA, 2013, pp. 217-223.

[76] N. H. Ab Rahman, W. B. Glisson, Y. Yang and K. K. R. Choo, "Forensic-by-Design Framework for Cyber-Physical Cloud Systems," in IEEE Cloud Computing, vol. 3, no. 1, pp. 50-59, Jan.-Feb. 2016.

[77] Beebe, N. and J. Clark, A hierarchical, objectives-based framework for the digital investigations process Digital Investigation, Elsevier, 2005. 2: p. 147-167.

[78] T. S. Pham, T. H. Hoang and V. C. Vu, "Machine learning techniques for web intrusion detection — A comparison," 2016 Eighth International Conference on Knowledge and Systems Engineering (KSE), Hanoi, 2016, pp. 291-297.

Authorized licensed use limited to: ULAKBIM UASL - Mugla Universitesi. Downloaded on February 01,2021 at 07:44:56 UTC from IEEE Xplore. Restrictions apply.