ISSN- 2394-5125 VOL 10, ISSUE 02, 2023

Enhance MOODLE Platform Security Against Denial of Service Attack (DoS)

Kamal Aldin Yousif Yaseen
Department of Information System, CEMIS College, University of Nizwa, Nizwa, Oman
E-Mail: k.yousif@unizwa.edu.om

Abstract- E-learning systems are used by almost every educational institution and the system is upgrading day-by-day (e.g. traditional monolithic e-learning system to modern eLearning ecosystem or cloud-based system). E-learning system provides a lot of benefits in the educational process, at the same time security is one of the important concern for e-learning systems. To prevent loss of user's data and to prevent from any kind of damage, a secured e-learning system is a must. Every system has some security issues and challenges.
Moodle is a wide spreading learning platform designed to provide educators, administrators and learners with a single robust, secure and integrated system to create personalised learning environments. According to the opinion of most researchers of serious attack threaten the Moodle availability is a denial-of-service attacks, hence the Moodle platform is one of the most famous and most used of these platforms, this paper looks at how to secure this platform from this type of attack.
Keywords- Moodle, Platform, cybersecurity, E-learning, threats, online, DOS, firewall

Introduction:

E-learning is using the internet technology in the learning process through mobile phones or computers, and this process allows the learner to learn at anytime and anywhere, and includes e-learning Displaying texts, video, audio clips, animations and virtual environments, forming a very rich learning environment that can outperform the traditional classroom environment. With the use of many effective designs and the guarantee of a highly qualified and specialized educational team; E-learning becomes an ideal learning environment and an attractive and valuable means for students, which is an opportunity to learn at any time, in addition to the fact that e-learning includes the introduction of computers, smartphones and tablets into the classroom and offices and makes use of them on a large scale [1].
Modular Object-oriented Dynamic Learning Environment(MOODLE) is a leading learning platform which is considered one of the best e-learning environments, and is gaining wide fame around the world, and is used by a large number of educational and academic institutions around the world. What distinguishes the Moodle platform is that it is a free and open source platform that anyone or Educational Institution get access to training courses and great educational benefits once you register on the site [2].

Types of e-learning

E-learning includes three basic types, which are as follows:
Simultaneous education: This type includes the interaction of the teacher and his students via the Internet at the same time, through video communication, audio conference, or through chat

ISSN- 2394-5125 VOL 10, ISSUE 02, 2023

and instant messaging, and through this it is possible Type of education Recording all lectures and playing them at a later time and keeping track of all the activities required during them. The teacher can also monitor his students, correct their mistakes, and allocate to each student what he wants to teach him. Students also have the opportunity to communicate and cooperate with each other. **Asynchronous education:** This education includes the interaction of the teacher and his students via the Internet at different times and not at the same time, so that educational courses and lectures are available on computers, in CDs, or through dedicated websites that can be accessed through the Internet, and this education allows learners to access They can access courses whenever they need them and at their own pace, and they can interact with each other via message boards, bulletin boards and discussion forums[6].

Blended education: It is a type that combines synchronous and asynchronous education, so that the teacher and students interact via the Internet at the same time that the training courses are given, then these courses are transferred to CDs for later use for self-study separately from the teacher[7].

Denial of service attack (DoS)

It's kinds of computer attacks aims to shut down the services, machines and website servers also has another type distributed denial of service (DDoS) attacks seek to knock websites or online services offline by overwhelming them with enormous quantities of fake traffic. Such attacks have been taking place for the past couple of decades. However, over the last year, as the COVID-19 pandemic meant people than ever were more reliant on the internet for everything from shopping to remote learning, the number of attacks have increased. That's bad news for those lacking the necessary protection in the form of safeguards like Web Application Firewalls (WAF), on which we will elaborate below. Not only are attacks larger in size and more frequent than ever, but they are also attacking new sectors with unprecedented ferocity. One of these is the education sector. DDoS attacks aimed at education aren't entirely new. In fact, the first recorded DDoS attack in history, which took place in July 1999, was used to attack a computer system at the University of Minnesota in the United States. But for much of the time following this, DDoS has been used to attack businesses, rather than schools. That's changing now. According to some reports, the number of attacks per organization taking place in the academic sector far outpaces the average across all sectors in the United States. Similar trends are seen elsewhere in markets like Europe and Asia. Of these attacks, DDoS attacks account for the majority[8].

To avoid denial of service attack

- **Perform a network vulnerability audit**: In order to properly defend your network, you have to understand its weaknesses. Do a complete review of all the devices on your network. This process includes defining their function within the network, recording the system information, and outlining their existing vulnerabilities. This level of visibility allows you to understand your network's deficiencies, prioritize them by urgency, and patch any holes to keep them from being exploited. Audits are time-consuming

ISSN- 2394-5125 VOL 10, ISSUE 02, 2023

- **Secure your infrastructure**: To successfully defend against a DoS attack, you need to make sure your castle's walls are fully fortified. For this, it is essential to have multi-level protection strategies that use intrusion prevention and threat management systems. These systems can use anti-spam, content filtering, VPN, firewalls, load balancing, and security layers to spot and block attacks before they overwhelm your network. That said, software cannot do the job alone: You need a hardware component. Edge micro segmentation — which we will cover in the next point — is one of the most powerful ways of protecting your network from DoS attacks[9].
- **Reduce the attack surface:** One of the most effective strategies against DoS attacks is to reduce the size of the available attack area. The smaller the attack surface, the easier it is to defend. While there are many ways of implementing this strategy, micro segmentation is an innovative approach gaining traction in the industry. Micro segmentation spits a network into granular zones and protects each zone separately. The net effect is a higher overall security profile. Byos has built a powerful edge micro segmentation solution that uses hardware-enforced isolation to secure endpoints on small microsegments, maximizing the defensive capabilities of the network as a whole. Ready to learn more? Get started here.
- **Create a DoS response plan**: Benjamin Franklin once said, "If you fail to plan, you are planning to fail," and this principle holds with DoS attacks. The purpose of the plan is to ensure that your current setup is secure, that you can detect an attack as soon as possible, that everyone on your team knows their role should an attack occur, and that escalation and resolution procedures are all clear.
- **Know the warning signs:** The earlier you can spot the onset of a DoS attack, the more likely it is that you will be able to defend against it successfully. Common warning signs of the beginning of an attack are poor connectivity, network slowdown, repeated site crashes, or any sustained disruption of performance[10], [11].

Related works

MOODLE Platform vulnerable to a lot of attacks types such as XSS, SQL injection and DOS which is more crucial attack I will present the related works as following:

Tawfiq Barhoom and Hijazi, M.I [2] proposed a guidance for matures to prevent XSS attacks in open CMS, they analyzed some of websites created on Joomla and Wordpress as CMS using some of scanning tools to extract the security issues especially XSS attacks. Due to the lack of details from scanning tools they injected manually different ten cases of malicious XSS codes in both Joomla and Wordpress pages to get more details of XSS attacks then they proposed defense way for each of attack case. The attacks and defense have been learned by matures to secure their websites.

Hernández, J.C.G et al. [3] proposed an object oriented model of MOODLE using Unified Model Language (UML) which is represented into three models: analysis, design and components. Then they discussed some of security vulnerabilities and its solutions in MOODLE such as session hijacking, session fixation, prediction of username and password. Their solutions to the proposed

ISSN- 2394-5125 VOL 10, ISSUE 02, 2023

vulnerabilities depend on modifying certain portions of code and adding new functions. The represented research provided some of MOODLE's vulnerabilities with recommended solutions which may help MOODLE's users to protect MOODLE against the previous vulnerabilities but they didn't handle cross side scripting vulnerability in MOODLE and how to protect MOODLE against such attacks.

Wurzinger, P. et al. [4] introduced SWAP (Secure Web Application Proxy) which is able to detect and prevent XSS attacks, SWAP operates on a reverse proxy installed in front of web server which relay all traffic between clients and web server and intercepts all HTML responses from server and subject them to analysis by JavaScript detection component. Their solution is utilizing the reverse proxy for mitigation of XSS attacks also their solution didn't require any modification on client side but SWAP might not be suitable for high performance web service. Their solution is different from our proposed solution because they didn't handle MOODLE as target, while our model is focus on it and working to increase its security.

Methodology:

This study is based on a group of previous studies that examined the importance of securing educational platforms and contribute to adopting the necessary security policies and spreading awareness. The contribution of this paper would be explanation the protection tool called "Solar Winds Security Event Manager" it's very helpful and free charge.

Objectives:

The main objective of this paper is to make the Moodle platform more secure by adopting the solid security policies, awareness of the e-learning stakeholder's students, administration staff and the faculty.

ISSN- 2394-5125 VOL 10, ISSUE 02, 2023

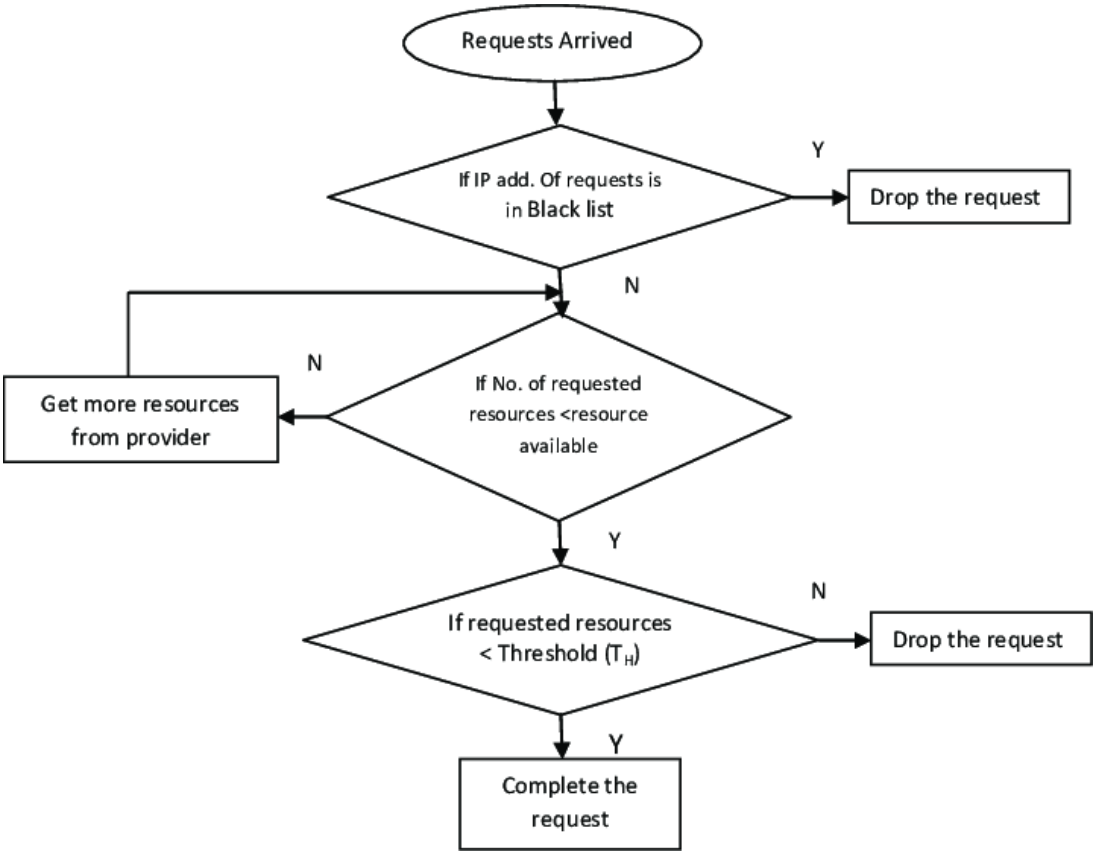

Figure1: Denial of service attack mitigation algorithm

Discussion:

One notable cyberattacks disrupted the initial week of the new school year for students at Miami-Dade County Public Schools in the US. The DDoS attacks overloaded school networks with traffic, stopping faculty and students logging into the My School Online platform, a platform that allows teachers to set homework, disseminate learning materials, carry out quizzes, and more. The DDoS attack stopped up to 17,000 users from gaining access to the platform for remote learning purposes. Ultimately, authorities in Miami arrested a 16-year-old student from South Miami Senior High School While most of the DDoS attacks reported so far in this sector have seemingly been focused on causing disruption, many of the alternative educational cyberattacks have involved ransomware malware. These have blocked users from being able to gain access to the crucial files and systems they need unless they are willing to pay a ransom, typically paid in Bitcoin. In more recent years, there has been a big uptick in the number of threatened DDoS attacks in which attackers will try and extort money by promising to bring down a website or online service unless they are paid a ransom. This, too, is something that schools, colleges, and other educational institutions must now be wary of[12].

The previous studies poof that the education sector is one of the sectors most targeted by attacks, as the percentage of attacks reached 19% compared to other sectors, and the percentage of attacks targeted educational platforms is 7%, including the Moodle platform. To eliminate this type of attacks completely, also utilizing the protection tools such as Low and slow attack tools,

ISSN- 2394-5125 VOL 10, ISSUE 02, 2023

Application layer (L7) attack tools, Protocol and transport layer (L3/L4) attack tools, Low Orbit Ion Cannon (LOIC), High Orbit Ion Cannon (HOIC), Slowloris, R.U.D.Y (R-U-Dead-Yet) should be very helpful to prevent the DOS attacks.

According to Cloud flare, in Q3 of 2022 ransom DDoS attacks increased by 67 percent year-on-year and 24 percent quarter-on-quarter, online industries received the most application-layer DDoS attacks, recording a 131 percent increase quarter-on-quarter (and 300 percent year on year) rise in the number of attacks. Gaming and gambling companies were the most targeted by network-layer attacks, with a huge 405 percent increase in Mirai botnet attacks from Q2 to Q3 2022.

The paper research showing regionally-specific spikes in DDoS attacks, 2022 saw the government of Montenegro fend off state-sponsored ransom DDoS attacks, allegedly from Russia. Meanwhile, the Albanian government dealt with a similar situation, though all signs point to Iran as the culprit in this instance in Q3 2021, a wave of large-scale DDoS attacks swept across New Zealand. Ransom DDoS attacks on VoIP providers in Q3 affected companies in Britain, Canada, and the US. In early and mid-July, threat actors flooded the resources of the security agencies of Russia and Ukraine with junk traffic, in mid-August, attackers tried to stop users from accessing the web resources of the Philippine human rights organization Karapatan. At the end of August, the website of Germany's Federal Returning Officer was briefly targeted in connection with the September 26 elections to the Bundestag[13].

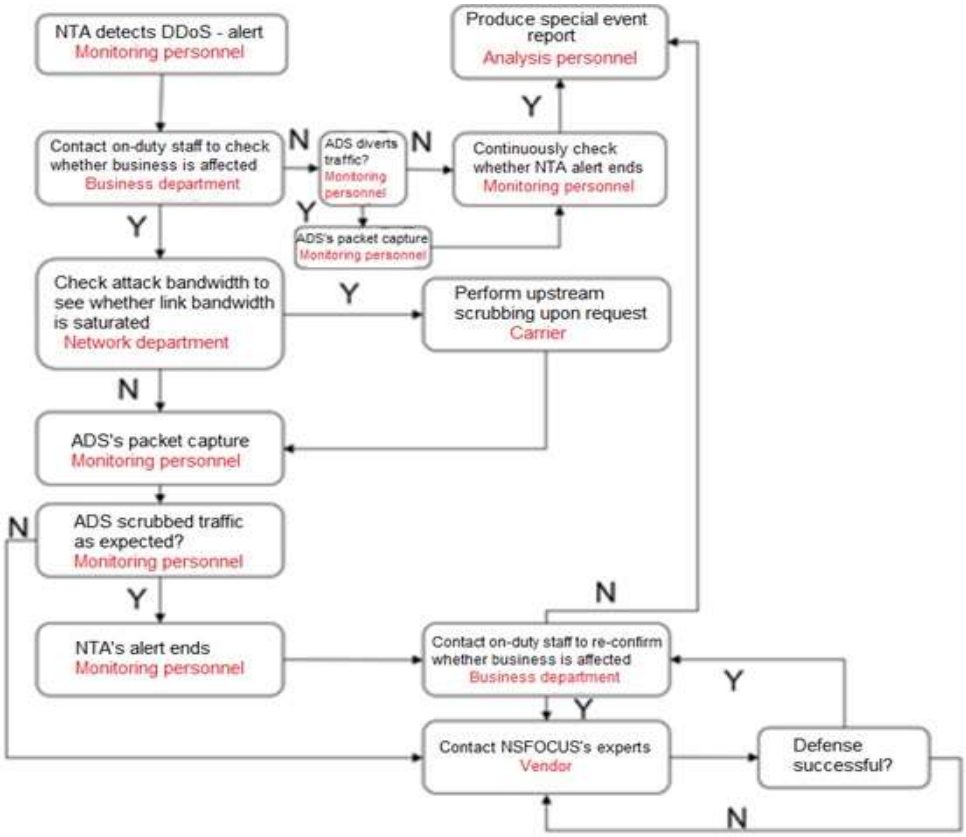

Figure2: Denial of service protection and response plan

Acknowledgment

The thanks will be to all previous research in this area really they help me a lot to achieve this paper.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

Conclusion

MOODLE platform and other e-learning platforms are vital to the education sector and it's so important to prevent them from those kinks of attacks, specially the common risk is rising day by day as the attackers developing their techniques and tools, hence the institutions must adopt the solid security policies and evolve their tools to protect themselves.

The contribution of this paper is important in terms of highlighting the risks that threaten the most important e-learning platforms and describing the steps to address the problem by imposing educational plans and programs and using tools that reduce the risk possibilities and thus end it completely.

References

[1] Yousif Yaseen, K. A. (2022) "Importance of Cybersecurity in The Higher Education Sector 2022", *Asian Journal of Computer Science and Technology* , 11(2), pp. 20–24. doi: 10.51983/ajcst-2022.11.2.3448

[2] Tawfiq Barhoom and Hijazi, M.I., "Exploring Guidance for prevent against XSS attacks in open CMS", Palestine Technical College Scientific journal: Gaza, Vol 2, 2016.

Hernandez, J.C.G. and M.A.L.n. Ch ́ivez, "MOODLE security vulnerabilities", Electrical engineering, computing science and automatic control, 5th international conference, IEEE, 2008.

[4] Wurzinger, P., et al. SWAP," Mitigating XSS attacks using a reverse proxy", Proceedings of ICSE Workshop on Software Engineering for Secure Systems, IEEE Computer Society, 2009.

[5] Meike, M., J. Sametinger, and A. Wiesauer, "security in Open source Web Content management systems", IEEE Computer Society, Vol 7, Issue 4, PP: 44-51, July/August 2009.

[6] Arakelyan, A., Vulnerable Security Problems in Learning Management System (LMS) MOODLE. Institute for Informatics and Automation Problems of NAS of RA.

[7] Kumar, S. and K. Dutta, "Investigation on security in LMS MOODLE", International Journal of Information Technology and Knowledge Management, Vol 4, Issue 1, PP: 233-238, 2011.

[8] Shar, L.K. and H.B.K. Tan, "Defending against cross-site scripting attacks", Computer, (3): PP: 55-62.

[9] Mewara, B., S. Bairwa, and J. Gajrani, "Browser's defenses against reflected cross-site scripting attacks", Signal Propagation and Computer Technology (ICSPCT), IEEE, 2014.

[10] Yousif Yaseen, K. A. (2022). Digital Education: The Cybersecurity Challenges in the Online Classroom (2019-2020). *Asian Journal of Computer Science and Technology*, *11*(2), 33–38. https://doi.org/10.51983/ajcst-2022.11.2.3450

[11] Halfond, W., J. Viegas, and A. Orso. "A classification of SQLinjection attacks and countermeasures", Proceedings of the IEEE International Symposium on Secure Software Engineering, IEEE, 2006.

ISSN- 2394-5125 VOL 10, ISSUE 02, 2023

[12] Cowan, C., et al. "Protecting systems from stack smashing attacks with StackGuard", in Linux Expo, 1999.
[13] Shahriar, Hossain, and Mohammad Zulkernine. "Injecting comments to detect JavaScript code injection attacks." Computer Software and Applications Conference Workshops (COMPSACW), 2011 IEEE 35th Annual. IEEE, 2011.

Author profile

Kamal Aldin Yousif Assistant professor Nizwa University- Oman, he got B.Sc. computer science from Sudan University-Sudan (2003), and he has master degree in computer science from Aljazeera university Sudan (2007), PHD of information technology John hiver academy UK (2010), PHD computer science-cybersecurity Umdorman Islamic University (2018).