CYBERSECURITY FOR ONLINE EDUCATION

MARKO KOMPARA, MARKO HÖLBL

University of Maribor, Faculty of Electrical Engineering and Computer Science
marko.kompara@um.si, marko.holbl@um.si

Abstract Online education has become very popular, and like anything online, it is also prone to cyberattacks from malicious adversaries. Cybersecurity in online education is important primarily because of the participants' sensitive personal information such systems hold and the damage and impact a successful attack could cause (e.g., the loss of progress and any grades students have received so far in their education and potentially lost records of graduates). This work presents the cybersecurity challenges and problems in online education. It shows the most relevant issues for education attendees and education providers. The manual introduces some important properties of a security system and gives some recommendations on how to achieve them. The content is aimed more at personnel that manage or want to establish an online learning environment. Still, the users (students or teachers) can also get useful information on how to design their passwords and how to use them, multi-factor authentication, and how their human nature puts them at risk of being exploited.

Keywords:
cybersecurity, online learning, online education, e-learning, learning management system

University of Maribor Press

DOI https://doi.org/10.18690/um.1.2023.2
ISBN 978-961-286-693-8

1 Introduction

Online learning allows everyone the opportunity to improve their education. Online learning is a form of distance learning where the participants and the instructors are physically not together, and the interaction is mostly asynchronous. By leveraging information and communication technologies, online learning offers advantages over traditional learning, like learning at any time and (almost) anywhere. This eliminates scheduling and distance problems that are often limiting in the modern, fast-paced, globalised world. It also improves access to education and training. It reduces the costs for the organisations providing the education (e.g., no need for physical classrooms) and students (e.g., no travelling to school or renting a place to stay while at school), which also removes socioeconomic status barriers. All these advantages and the flexibility of online learning are often the driving motivators for choosing online education over traditional in-person forms of education.

Online learning is typically implemented using a Learning Management System (LMS). LMS is in some ways similar to much more common Content Management Systems (CMS) that are used for managing websites. A learning management system supports the administration, documentation, tracking, reporting, automation, and delivery of educational courses or training programs. An LMS provides virtual classrooms in which students and teachers interact. It hosts educational material and distributes it to students over the Internet (in the form of a webpage). Learning materials can include text, images, audio and video presentations, and link to other (outside) resources. The teachers manage the virtual classroom, upload any learning materials, assign students their assignments, and guide students in their work. To breach the communication challenge of distance learning, LMS systems provide good communication links between teachers and students. An example of such a learning management system is Moodle, which is the main topic of this manual.

However, like everything else that functions over the internet, online learning is also threatened by malicious actors. The main risks involve loss of confidentiality, availability, trust, exposure of critical data, and vandalism of the provided service. To defend against these risks, cybersecurity must be employed. Cybersecurity is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber-attacks.

Table 1 presents security issues in online learning and consequently relevant in learning management systems. The table is based on the work done by S. M. Furnell and T. Karweni (2001) and, in addition to the security issues, also shows which are relevant for the system's majority users (i.e., students) and which are predominately crucial for the organisation providing and managing an education program together with the learning management system.

Table 1: Security issues in online learning and whether they are essential for students and the education provider.

Security Issues	Student Interest	Education Provider Interest
Privacy and confidentiality of personal data	✓	✓
Security of service usage – Authentication and accountability – Access control – Protection from malware	✓	✓ ✓ ✓
Human aspects (e.g., phishing)	✓	✓
Security of payment (i.e., enrolment fees, if any)	✓	✓
Security of data – Authentication – Confidentiality – Integrity – Non-repudiation	✓ ✓ ✓ ✓	✓ ✓ ✓
Secure communication	✓	✓
Security of educational materials – Prevention of unauthorised access – Prevention of unauthorised distribution – Software licence control		✓ ✓ ✓
Confidentiality and secure conduct of knowledge assessments	✓	✓
Proof of completing the education – Verification of education provider – Verification of the integrity	✓	✓ ✓
Reliability and availability of education environment	✓	✓
Maintenance		✓
Backups	✓	✓

The remainder of this manual addresses issues raised in Table 1 and what cybersecurity techniques and solutions can be applied to protect against them. Not all the problems mentioned in the table will be directly addressed, as some are not primarily in the domain of education providers (e.g., security of payments or

software licence control), and others have the same underlying technologies (e.g., access control and prevention of unauthorised access).

In this manual, we also wish to support some other work done in the Cyber F-IT project. Other outputs include information on privacy, information security management in higher education, and configuration and use of Moodle learning management system. This manual aims to give the readers some context to how privacy and security are connected but mainly presents some basic security concepts and mechanisms that must be put in place to secure an environment, such as an LMS. With this knowledge following the options shown in the configuration process of Moodle platform, readers will better understand what individual options are for and why they are required. Most of this manual would be more interesting to education providers; however, end-users, like students and teachers, could also gain valuable information from it. For them, we recommend reading sections 3.1, 3.2, 5, and 7.

2 Privacy

The educational environment is full of valuable personal data. It is the institution's responsibility that is providing the education not to exploit this data (but to use it only for its intended purposes) and to protect it from other malicious entities. Privacy relates to one's right to control personal information and how it is used. Security, on the other hand, is about how data is protected. The two are connected because cybersecurity is what protects an individual's privacy (i.e., personal data). Personal data is any data relating to an identifiable person. A privacy policy is one of the most important aspects of ensuring user privacy. This manual defines all the ways in which an organisation (i.e. education provider) gathers, uses, discloses, and manages users' (i.e., students') data. Especially in more recent times, the protection of personal information has become a big issue, and legislation was put in place to ensure that anybody processing personal data keeps them safe in suitable ways and uses them in a responsible manner. You can learn more about this in the chapters Personal Data Security (Directives of Education Institutions and Students) and Information Security Management in Organisational Settings and Higher Education Institutions.

3 Authentication, Authorisation, and Access Control

Authentication is the process of confirming somebody's identity. The most common authentication method is the username and password combination, which we discuss in more detail below. However, there are others: biometry, smart cards, one-use tokens, etc. Authentication credentials can be done based on what one knows (e.g., password), what they are (e.g., fingerprint), and/or what they have (e.g., a smart card). The problem, especially when it comes to examinations in an online setting, is the prevention of possible sharing of credentials to have somebody else taking the exam instead of the designated participant. This is most serious in the case of the "what you know" and "what you have" credentials that can be more easily shared but are not entirely avoided in the case of "what you are" credentials either (e.g., the participant takes the examination together with the helper). When it comes to examinations, the authentication process is, therefore, often more complex and involves sharing a live feed of the participant's web camera (for the duration of the examination) together with showing a form of personal identification. Ultimately, this problem of verifying whether or not the right person did the assignment/examination is one of the significant reasons why remote learning has not spread as much for formal education purposes.

The authorisation comes after authenticating a user and defining what a specific user has access to. Participants need access to all their courses, learning materials, any work they have submitted or grades they have received, etc. Still, at the same time, they must not have access to the back end of the used education platform, assignments their classmates might have submitted, grades they might have received, classes they are not enrolled in, etc. For teachers, it is similar, but they must have access to all the submitted work and grades of everybody in their course (usually, they should not get access to courses they do not teach), and they also get the option to add and change the content of the course as well as give grades etc. Course administrators (not system administrators) usually do not get access to course content, but they can add and remove participants and teachers from courses. Finally, system administrators have access to the back end (e.g., configuration) of the platform and have, in general, the highest authorisation level. Strong authentication practices are especially important for system administrator accounts because unauthorised access can cause the most damage. It is, therefore, the best practice to enable all the available security features for the administrator accounts.

Access control is the broadest concept of the three presented here. It includes authentication and manifests the rules set by the authorisation and many more things. At its simplest, access control protects front-end and back-end data and system resources. An access control scheme should protect against unauthorised viewing or any form of data changes. Access control mechanisms can also help limit malicious code execution or unauthorised actions by an attacker exploiting infrastructure vulnerabilities. Access control can be based on physical attributes, sets of rules, lists of individuals or systems (i.e., access list), or other, more complex means (e.g., intrusion detection system). Role-based authorisation is the most commonly used model of restricting the system access of unauthorised users. It allows defining groups, assigning users into groups or even groups into other groups. This model allows for flexible and granular control of the access rights of each user. The permissions themselves (i.e., what somebody can do and access) are assigned roles (teacher, student, course administrator, unregistered user, system administrator, etc.). System users are assigned particular roles, from which they acquire the permissions to perform particular system functions. Since the users do not have the permissions directly assigned to them, management of individual user rights is simpler and more reliable from a management standpoint.

3.1 Passwords

Passwords are the prevalent authentication method because they are the easiest for developers to implement and users to understand and use. However, some conceptual weaknesses are associated with using passwords (namely, when they are poorly selected, easily guessed, etc.). The U.S.A.'s National Institute of Standards and Technology (NIST) regularly updates its recommendations for creating and managing passwords (see NIST Special Publication 800-63B - Digital Identity Guidelines: Authentication and Lifecycle Management by Grassi, P. et al.). In one of the recent shifts in the paradigm of password security, they have suggested that users focus on password length over complexity (combinations of special characters, numbers, lowercase or capital letters) because complex passwords are hard to remember. Consequently, users tend to achieve complexity in predictable ways (e.g., adding the number 1 at the end of a password). One way to achieve length is with nonsensical passphrases, where words are in a sequence with no meaning. For the same reason, NIST no longer recommends strict character composition rules when creating a password. However, they recommend regularly comparing passwords (or

at least any new passwords) to a list of compromised passwords to identify already revealed and weak passwords. Nevertheless, the recommended minimum length of a password is still eight characters. While regular changes of passwords were recommended in the past, this is no longer the case. This makes users less likely to remember their passwords after changes and instead start using the same passwords with minor alterations. The minimum protection of the stored passwords should include hashing and the use of salts (salt is a random value that prevents identical passwords from hashing into the same value and specific attacks). Additionally, NIST suggests locking a user out of the system if they use an incorrect password too many times (e.g., after three unsuccessful tries, a user cannot try again for one minute), allowing emojis, ASCII, and Unicode characters in passwords, and allowing copy and paste functions in the password fields to make using password managers and multi-factor authentication, which we will both address shortly, more convenient.

Finally, although you can use technical measures to ensure users choose robust passwords, it is impossible to control what users do with them. They can write it on paper next to their computer, share it with others, or use it for other accounts. The latter is dangerous, as using the same password across multiple accounts will compromise all of them if any of the services using the same passwords are breached. This means that if you use the same password for accessing your library and e-mail account if somebody breaches the security of the library (which should be a lot easier than the servers of a large e-mail service provider – e.g., Google) and steals the password, they can use that information to gain access to your e-mail account. Educating the users is the only real solution to prevent such bad practices. Therefore, users should be educated (on how) to create strong passwords, not to write them anywhere accessible, and never to reuse the same password.

One of the best solutions for remembering or, better said, storing a large number of passwords and any other authentication-related information (e.g., private keys) are password managers. A password manager is a software solution (online or local) that stores all your credentials (typically username and password) in a secure way by encrypting them. Access to the list is protected in any possible ways we have discussed (password, fingerprint, multi-factor authentication, etc.). The "master password" that protects access to all the other passwords must be very secure (for obvious reasons). The advantage of such a setup is that the user must only remember

one very good password to gain access to any number of services that use a different password stored with the manager. Password managers can also generate completely random values for users to use as passwords (random values are the best possible passwords). There is no longer a need for such passwords to be memorised.

A final consideration when using passwords in an educational setting is the possibility of sharing a password. A student can give their password to somebody else, who can log in as them and participate and/or submit any assignments, examinations, etc., in the credential holder's name. Multi-factor authentication is one way to make this more challenging (how much harder credentials sharing becomes depends on the factors used).

3.2 Multi-Factor Authentication

Multi-factor authentication (MFA) is authentication using at least two different factors (what you know, what you are, and what you have). Two-factor authentication (2FA) is basically the same, but precisely two factors are used. Nowadays, if MFA is used, it is almost always 2FA. Typically, the first factor is a password or a PIN (something you know), and the second is usually a bank card, SMS, or a code generated by a mobile app (what you have - i.e., your mobile device). Using fingerprints, retina scans, etc. (what you are) is an option, but it is less often used because additional hardware is required (with higher cost).

Multi-factor authentication is a good way to mitigate the risk and reduce the chances of compromised credentials. For example, let us look at a password and app code combination. Even if the site itself is compromised or a password is obtained from somewhere else, the attacker cannot log in because while they can provide the appropriate username and password, they cannot provide the code generated on the mobile device. The stolen password becomes useless (unless the attacker steals the mobile device as well, but that is not a scalable attack and, therefore, not a serious threat to most people). Meanwhile, the system administrators can still detect unsuccessful attempts to log in and ask a specific user to change their password or all of their users if their system was compromised and all the passwords leaked.

4 Confidentiality, Integrity, and Non-Repudiation

Confidentiality, Integrity and Availability (CIA) are considered to be the three primary pillars of information security. Confidentiality is the principle of keeping data confidential/private. One part of this is the previously discussed access control, where access to data is limited. The second part deals with situations where anybody can access information, but it must remain confidential. In this case, confidentiality is achieved with encryption. Confidentiality is important in any system, and the same is true for online learning systems. Any work students submit should stay confidential (except for teachers grading the assignment), and any grades received should not be publicly accessible (even to other students).

The integrity of data prevents unauthorised modifications to data. Technically this is implemented in a way that any change is easily detectable (because it is impossible to prevent changes in some environments). Integrity is essential for establishing trust in the system. Students, for example, must be assured about the integrity (i.e., correctness) of grades or that assignments that they submitted were not changed (on purpose or by mistake) during transmission or while on the server. To guarantee confidentiality and integrity, the security of network communications is paramount.

Even though confidentiality and integrity of data are important, the data or service is of little use if it is unavailable. We will discuss availability together with reliability shortly.

Non-repudiation ensures that users cannot deny they have carried out an action. For example, if a teacher were to remove a student from a course, it should be possible to track who removed them. The audit trail (e.g., log files) must be reliable and tamper-proof to ensure integrity and non-repudiation.

5 Secure Communications

We have discussed how the security of data at rest (e.g., on a system) is important. However, the security of data while in transit is just as important, if not even more so, because while data is in transit (e.g., on the Internet), it is not under any ones' control, and it can be eavesdropped on or modified. Therefore, using methods that ensure confidentiality and integrity to prevent this from happening is essential. The

standard way to access online education is over HTTP (Hypertext Transfer Protocol). However, this protocol only concerns how data is transported between the client (e.g., a browser of a student, teacher, or system administrator) and the server. HTTPS (Hypertext Transfer Protocol Secure) should be used to protect the data while in transit. This is basically the same as the original protocol but also provides data confidentiality, integrity, and authentication. HTTPS is the standard method used today. Anyone using the Internet (for education or otherwise) should stick to web pages using this protocol, especially if any personal information is sent to a web page or the page requires a login.

The protocol used within the HTTPS that protects communication through end-to-end encryption is called Transport Layer Security (TLS). For TLS to work to its full potential, the service providers must obtain a TLS certificate, which helps authenticate the server (clients are typically not authenticated in this way). This helps prevent fake websites from pretending to be legitimate. Users can check this in their browsers by clicking on a lock icon next to their URL bar. Systems like those for online learning can have connections to multiple external systems or databases containing information on all the students and teachers, their activities on the platform, course catalogues, etc. Any such connections also must be protected in the same way.

6 Reliability and Availability

Reliability is defined as the probability of a system or a system part performing its intended function under stated conditions without failure for a given period (Stallings, 2023). In other words, the reliability of a system supporting online learning is the property of a system to produce consistently correct responses/outputs to given actions/inputs. Reliability in a learning environment can also be looked at from the perspective of course materials (they are correct, current, and relevant), but that is fundamentally a question of data integrity (the materials were not corrupted) and the quality of data itself.

Availability is the third pillar of the CIA triad mentioned previously. Availability is the assurance that the environment or service (e.g., remote learning) is accessible (to authorised users) whenever required (Stallings, 2023). One of the main advantages of online learning (if it is not in person) is that the time and work distribution is

largely flexible to the needs and requirements of participants/students. For this to be a realisable advantage, availability is essential. Access to study materials and the possibility to submit any assignments must be available at all times for online education to reach its full potential and to give all participants equal possibilities of engagement. For example, online learning is desirable to people who already have jobs or other commitments that do not allow them to attend a class every day. Availability of the course allows them to do their work after they finish their jobs, in the evenings or at the weekends and can therefore be extremely important for online learning. Disruption of availability (even for a short time) can cause a loss of revenue, customer dissatisfaction, and/or reputation damage. The majority of threats to availability are not malicious and can include any number of hardware, software and/or network issues. A typical attack that targets the availability of resources is a Denial of Service (DoS) attack, which we will discuss in more detail later. Measures to ensure better availability include backups, hardware, systems and potentially location redundancy, firewalls, network monitoring and appropriate routing, etc.

7 Human Aspects

In cybersecurity, it is often said that people are the weakest link in the security of a system. This is because while the technical security of systems is constantly improving, we cannot really improve people other than educating them on the proper ways to use a system and how to avoid behaviours that could put them or the system they use at risk. However, in the end, users still try to make their life easier when possible or do what they believe is the right thing at a given moment, even if it is not. Attackers are well-aware of this and will try and exploit these characteristics.

We have already discussed one good example of this in the section on passwords. Even though rules on how passwords should be constructed and stored are well-known, users often ignore them because it is easier to remember a simpler password, write it on a piece of paper next to the computer, or use the one and the same password for everything. As a result, attackers successfully guess passwords (because users use simple and similar passwords) and use discovered passwords to attack other services the user might use.

The second major way attackers exploit human nature is through social engineering. Social engineering is the psychological manipulation of people to do what the attacker wants or divulge confidential information (Stallings, 2023). Examples of social engineering include scareware (using false alarms and fictitious threats), pretending to be an authority, pretending there is an emergency, impersonating specific people, etc. Possibly the most common, however, is phishing. Users should be wary of unsolicited messages, links and attachments in e-mails from an unknown source or offers that are too good to be true, etc.

7.1 Phishing

Phishing is a type of social engineering attack where the attacker sends the victim a deceptive message to have them reveal some information or cause them to deploy malicious software. Phishing attacks are untargeted (similar targeted attacks are called spear phishing), meaning they are sent to many people simultaneously. Their aim is not to fool everybody or even a majority, but a small success rate is already good enough because the messages are sent to so many people. Phishing can be done over voice (e.g., phone calls), social media, SMS, and most commonly, e-mail. Phishing e-mails often have spelling errors, poor grammar, bad graphic design, are very generic or get your name wrong (typically based on the e-mail address). However, not all phishing suffers from these deficiencies; therefore, vigilance is still key.

Phishing is often the first step of an attack, used to convince a user to deploy some other malicious software on their device and then use that malware to do the actual damage. This can include traditional viruses and worms, cryptocurrency-mining malware, lately prevalent ransomware (it renders the victim's computer files useless by encrypting them and demands ransom for their decryption), etc.

Organisations can do a lot to alleviate the risks of phishing (e.g., firewalls, spam filters, required MFA, etc.); however, some messages will almost certainly still make it to the end-users. To protect themselves, users should:

- verify the sender by checking their e-mail address,
- check any links before clicking them,

- do not provide any personal information if they do not trust the source,
- do not rush or panic react to a message (e.g., quickly opening an attachment because the message was marked as urgent),
- delete any received phishing messages without interacting with them (e.g., opening attachments or clicking on links) and report them (this can help prevent others from being affected by the same attack).

8 Maintenance

When any vulnerabilities are discovered, patches (i.e., updates that address security vulnerabilities) are made. If the system producer discovers the vulnerability, users will probably have some time to update their systems before the vulnerabilities are announced to the public. However, when malicious attackers discover vulnerabilities, the time it takes to produce and apply patches is critical in limiting the damage.

Modern LMS require many other components like operating systems, web services, content management systems, databases, and plugins. A typical Moodle install will have a Linux operating system, web server software, PHP, MySQL and any number of plugins. System administrators must constantly monitor, maintain, and upgrade all components to ensure everything works as it should. They should pay special attention to possible security patches and apply them as soon as possible. When there are major upgrades, a good option is to first test them in a staging environment before applying them to the live environment, just in case the new update breaks something.

Good maintenance practices extend beyond the web servers, as switches and firewalls should also be maintained with the same vigour and attention. Special attention should also be paid to plugins and extensions, which are often forgotten. They are usually not professional products created by an organisation that regularly updates them but hobby projects created by individuals. As such, they should be regularly checked, any plugins/extensions no longer in use should be removed, and unnecessary plugins/extensions should not be installed.

9 Backups

Backups are the ultimate recovery solution after a system has been compromised and, as such, are extremely important. The safest mindset is to assume you will be hacked or there will be some crucial hardware malfunction or a natural disaster, after which the only solution to re-establish the environment as it was before the event will be from a backup. A bug in the LMS can also cause a loss of data. In any of these cases, it is very important to recover all the learning materials, any work students have done so far, and their grades. If any of this data is lost, it would mean a lot of lost effort for the students and teachers and a big reputation hit for the educational institution.

A sound backup system regularly saves backups in different locations and frequencies. Other locations are required so that, for example, one natural disaster does not destroy all the backups. Meanwhile, having backups from different time points is necessary because compromises are not always immediately discovered. Therefore, a backup from yesterday, a week or a year ago might be necessary to establish an environment where the cause for the ultimate failure was not already present. However, just having backups is not enough. Procedures for testing the backups and recovering from them in a timely fashion are necessary for backups to work and be useful when you need them.

10 Malware

Malware (a portmanteau of malicious software) is software intentionally designed to be harmful to computers and computer systems. Many types of malware are based on their operation and end goal.

Viruses were the original malware back when all malicious programs were called viruses. They are self-replicating programs that infect files (i.e., imbed malicious code into existing files).

Worms also self-replicate but do not require a host program to do so. They spread over networks and can potentially infect all the devices within a network.

Trojans disguise themselves as legitimate and useful non-malicious software to gain access to a system. Once there, they typically deploy their malicious functions while still performing their "useful" function to avoid arousing suspicion. Trojans typically do not self-replicate.

Spyware runs secretly while collecting and reporting any information on the system or about the activities of the users. They usually target sensitive information (e.g., personal information, financial information, or credentials).

Adware also collects information on the user but primarily to display advertisements that the users are more likely to be interested in. Adware can be the least dangerous type of malware on the list, but it can open doors for other malicious software and hinder the performance of the infected device.

Ransomware encrypts files on the system after gaining access to it. Users must pay a ransom if they want to recover inaccessible data. Data is typically unlocked after paying the ransom, but not always.

A variety of solutions are used to detect and prevent malware. The most basic one, and the one everybody can and should have on their machine, is the antivirus/antimalware program. Other measures (more interesting for use in organisations – e.g., education providers) include firewalls, network intrusion prevention systems, deep packet inspection, unified threat management systems, antivirus and anti-spam gateways, virtual private networks, content filtering, and data leak prevention systems.

11 Vulnerabilities/Attacks

There are many vulnerabilities and possible attacks. This section will briefly introduce some of the more common types of vulnerabilities/attacks.

A brute force attack is an attack of guessing. It is the most basic of attacks and very inefficient. Still, brute force attacks can offer good results when the security level is small enough or the secret is predictable enough. Brute force attacks are typically done on passwords but can be done on all types of secrets (e.g., PINs or cryptographic keys). The best defence against a brute force attack is to limit the

number of attempts in a given time. For example, suppose an attacker (or a legitimate user) enters the wrong password five times. In that case, the account is automatically locked for one minute, and no more attempts are possible during this time. In this way, the strength of a brute force attack is basically nullified because modern hardware is capable of trying a vast range of possibilities in a very short time (which is no longer true after introducing the limit), and the system resources are not abused by having to check the validity of the latest attempt constantly.

SQL injection is a relatively simple attack as well, and vulnerabilities that allow for the attack are quite easy to avoid by some basic coding practices; however, SQL injections are still very successful types of attack. In a SQL injection, the attacker passes SQL (Structured Query Language) code to an online application through an input field or HTTP parameters to gain unauthorised access to a database. The idea is to get the application to run the sent code, which does something malicious. It can allow (read and write) access to unauthorised data, bypass authentication, or shut down/delete the database regardless of whether the database is on the same or a different server as the web page. To prevent SQL injections, any receiving data must be adequately sanitised. This means that the data must be checked for anything that should not be there (e.g. unexpected SQL code) or only use prepared statements, which basically limit what the database will accept as a valid query.

Cross-Site Scripting (XSS) is a client-side injection attack. It commonly targets scripts embedded in a page on the user's web browser. The vulnerabilities are caused by the internet security weaknesses of client-side scripting languages (i.e., HTML and JavaScript). XSS manipulates client-side scripts of a web application to achieve the malicious purposes of the attacker. The embedded script can then be executed every time a page is loaded or an associated event is triggered. XSS can be used to gather sensitive or personal information, redirect the user to other malicious sites, steal users' session cookies (which allows the attacker to impersonate the victim), alter the browser functionalities, deface a web page, or perform a DoS attack. XSS vulnerabilities are easy to find and fix by proper data validation across the website.

As its name suggests, Denial of Service (DoS) attacks are designed to make a service inaccessible. This is typically done by flooding the target with a large volume of traffic, making it slow and potentially crashing. While handling all the fake requests, the server's capacity to timely respond to legitimate requests is diminished or

completely halted. Distributed Denial-of-Service (DDoS) attack is an enhanced version of DoS. While DoS uses one attacking source, DDoS is an organised attack from multiple machines (often from a botnet). In addition to the possibility of generating larger amounts of traffic with a larger number of machines, DDoS is also useful for hiding the origin of the attack.

12 Protective Measures and Recommendations

Many of the protective measures organisations should take to prevent possible vulnerabilities, and attacks have already been mentioned in other chapters of this manual. Therefore, this is more or less a summary.

Ensure to educate and orientate your users, employees (teachers and administrative staff), and system administrators on the importance of sound and secure passwords, their role and responsibilities in recognising and preventing security threats and risks, and how to identify attacks and attempts at exploiting them. This is especially true for system administrators, who, in addition, are often not very experienced and have a lot to learn - configuring the operating system and LMS, managing users and their permissions, managing firewall rules, web server configuration, etc. All these factors are critical to security, so support their education and training to improve their skills.

Consider implementing multi-factor authentication. Use secure communication channels for all forms of communications/connections. Maintain your software so it is up to date and any newly discovered vulnerabilities are patched. Establish and regularly create new backups. Also, ensure the backups are working and that you can quickly reintroduce them into your live environment. Make sure to implement malware prevention mechanisms in your organisation.

Any larger organisation should define privacy policies, user security policies, and organisational structures and implement organisation-wide approaches for managing their information security risks, identify the data controls, define secure information sharing, etc.

13 Conclusion

In this manual, we have presented some of the most essential cybersecurity considerations to consider in the process of establishing and/or attending online learning. The content is primarily interesting for online learning providers, but useful information for students and teachers is included.

We have looked at the security issues that face users and administrators of Learning Management Systems (LMS) from the conceptual properties that must be achieved in order to establish a secure learning environment online, through threats that are present to, finally, some suggestions and recommendations on how effectively to protect the online learning environment.

We aimed to use this manual to connect with some other results produced in the Cyber F-IT project centred around privacy, information security management in higher education, and the configuration of the Moodle learning management system. Hopefully, this work will contribute to understanding how privacy and security are connected and give readers some background and understanding of what some of the security options in the configuration of Moodle are, why they are necessary, and how they help secure the system.

References

Alwi, N. H. M., & Fan, I.-S. (2009). Information security management in E-learning. International Conference for Internet Technology and Secured Transactions, ICITST 2009. https://doi.org/10.1109/ICITST.2009.5402507

Bandara, I., Ioraş, F., & Maher, K. (2014). CYBER SECURITY CONCERNS IN E-LEARNING EDUCATION.

Buck, D. (n.d.). CMS Security: How to Keep Your Website Safe. Retrieved December 10, 2021, from https://www.brandextract.com/Insights/Articles/CMS-Security-How-to-Keep-Your-Website-Safe/

Costinela-Luminita, D. (2011). Information security in E-learning Platforms. Procedia - Social and Behavioral Sciences, 15, 2689–2693. https://doi.org/10.1016/J.SBSPRO.2011.04.171

Cybersecurity Risks in eLearning. (2021). Virtru. https://www.virtru.com/blog/cyber-security-risks-e-learning/

Daniels, D. (2020, July 28). What Is SSL, TLS and HTTPS? https://blog.gigamon.com/2019/09/06/gigamons-guide-to-communications-security-what-is-ssl-tls-and-https/

Furnell, S. M., & Karweni, T. (2001). Security issues in Online Distance Learning. VINE, 31(2), 28–35. https://doi.org/10.1108/03055720010803998

Grassi, P., Newton, E., Fenton, J., Perlner, R., Regenscheid, A., Burr, W., Richer, J., Lefkovitz, N., Danker, J., Choong, Y.-Y., Greene, K., & Theofanos, M. (2017). NIST Special Publication 800-63B - Digital Identity Guidelines: Authentication and Lifecycle Management. In Special Publication (NIST SP) - 800-63B. https://doi.org/10.6028/NIST.SP.800-63B

Hilmi, M. F., Pawanchik, S., Mustapha, Y., & Ali, H. M. (2013). Information Security Perspective of a Learning Management System. International Journal of Knowledge Society Research, 4(2), 9–18. https://doi.org/10.4018/JKSR.2013040102

How to Secure Your Content Management System. (n.d.). Retrieved December 10, 2021, from https://www.makeuseof.com/how-to-secure-your-content-management-system/

Malware | What is Malware & How to Stay Protected from Malware Attacks. (n.d.). Palo Alto Networks. Retrieved December 22, 2021, from https://www.paloaltonetworks.com/cyberpedia/what-is-malware

Mening, R. (n.d.). 4 Security Tips To Help You Secure Your Online Learning Platform - eLearning Industry. Retrieved November 22, 2021, from https://elearningindustry.com/secure-your-online-learning-platform-4-security-tips-help

Miguel, J., Caballé, S., & Prieto, J. (2013). Providing information security to MOOC: Towards effective student authentication. Proceedings - 5th International Conference on Intelligent Networking and Collaborative Systems, INCoS 2013, 289–292. https://doi.org/10.1109/INCOS.2013.52

Nair, V. S. (2020). CMS Vulnerabilities: Why are CMS platforms common hacking targets? https://beaglesecurity.com/blog/article/cms-vulnerabilities.html

Phishing Scams & Attacks - How to Protect Yourself. (n.d.). Kaspersky. Retrieved December 21, 2021, from https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips

Rupaneliya, M. (n.d.). Data Security In Online Learning - eLearning Industry. Retrieved November 22, 2021, from https://elearningindustry.com/understanding-data-security-in-online-learning

Rupareliya, M. (2020). Layman's Guide to Understanding Data Security In Online Learning. https://elearningindustry.com/understanding-data-security-in-online-learning

Singh, B., & Kumar, B. (2020). Role of Cyber Security in E-Learning Education. International Journal of Advanced Science and Technology, 29(4s), 3172–3178. http://sersc.org/journals/index.php/IJAST/article/view/22699

Stallings, W. (2023). Cryptography and Network Security Principles and Practice, 8ed, Global Edition, Pearson Education.

Weippl, E. (2005). Security in E-Learning (Vol. 16). Springer-Verlag. https://doi.org/10.1007/B136702

What is Malware? (n.d.). Cisco. Retrieved December 22, 2021, from https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html