HUMANITIES
MANAGEMENT, ARTS
EDUCATION &
THE SOCIAL SCIENCES
Research Journal

Vol 11, No. 4, 2023

Security and Privacy Concerns in E-Learning

Maxwell Amparbeng
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration Greenhill, Accra, Ghana
E-mail: amparbengMaxwell@gmail.com

ABSTRACT

The growth of Information and Communication Technology (ICT) is having a huge impact on everyone around the world. This growth allows people to connect with each other, especially through the internet. Today, the Internet itself is dramatically changing the delivery of services and products due to its immediacy, openness, ubiquity, and global reach. Additionally, eservices are widely adopted. As such, the education industry is fully reaping new possibilities as a permanent learning tool from the capabilities of the Internet in the form of web applications and the like. This industry is poised to become one of the largest sectors in the global economy. E-learning is the implementation of technology that assists the learning process in which knowledge and information can be acquired using communication technology. The learning process can continue as long as the content is available on his web. E-learning as a component of flexible learning consisting of a wide range of applications and processes using all available electronic media to deliver education and training. These include computer-based learning, web-based learning, virtual classrooms, and digital collaboration. In this paper we review antecedents and associated concepts and principles in the e-learning ecosystem viz-a-viz privacy and security issues and provide a reference content for further research

Keywords: E-Learning, Students, Teachers, Lecturers, Privacy, Security, Institutions.

Journal Reference Format:
Maxwell Amparbeng. (2023): Security and Privacy Concerns In E-Learning. Humanities, Management, Arts, Education & the Social Sciences Journal. Vol. 11. No. 4, Pp 99-116. www.isteams.net/humanitiesjournal.
dx.doi.org/10.22624/AIMS/HUMANITIES/V11N4P8.

1. INTRODUCTION

Online learning has become a popular method of training and education since the technological revolution of the late 1990s. It offers unmatched convenience, flexibility and affordability in an ever more expensive and busier world. As the world becomes more globally connected, it becomes harder and harder to isolate yourself and your colleagues from work. We extend the boundaries of our learning to the outside world, gaining new knowledge from unfamiliar people. We rely on networks of others to get the information we need. We share our individual worlds with each other in order to understand the subjective aspects of the world on a deeper level. “Sharing” has become a buzzword in many fields. However, in practice, some learners may object to sharing due to privacy concerns according to Nissenbaum (2011). Previously the development of e-learning brought new ways of learning while giving equal opportunities to learners. With these learning methods available today, information and knowledge are at your fingertips, enabling students to excel in their learning.

But while the Internet is the place to get all the information and knowledge you need, it is also the arena for a new wave of illegal activities. Information on the Internet is constantly exposed to security threats. As a result of e-learning's reliance on, or its primary focus on, the Internet, some are content-focused, some are communication-focused, and some are technology-focused. One of the first definitions of eLearning was provided by the American Society for Training and Development (ASTD). ASTD proposes that eLearning covers a wide range of applications and processes, including: B. Web-Based Learning, Computer-Based Learning, Virtual Learning Classrooms, and Digital Collaboration. As we strive to share knowledge publicly in an online learning environment, we need to address learner privacy concerns. Moral tensions and ethical dilemmas surrounding privacy issues have been debated by some scholars (Drachsler et al., 2015), but there are more nuanced aspects related to privacy and restrictions on public knowledge sharing. , is not addressed. But choosing the right platform is no easy task! There are endless options, each with their own unique capabilities.

1.1 Research Problem

E-learning is widely used as a method of learning that ultimately depends on the Internet in its execution. E-Learning systems epitomize computing systems and networks of the Internet generation. These systems are complex and they aim to guarantee the satisfaction of the learner and maintain the good image of the learning process. There is clear evidence that innovative educational technologies, such as e-learning, provide unprecedented opportunities for students, trainees and educators to acquire, develop and maintain core skills and essential knowledge. However, e-Learning systems employ the Internet as a place to obtain all necessary information and knowledge. Unfortunately, the Internet has also become the venue for a new-fangled set of illegal activities, so-called cyber-crime. Information associated with the e-Learning environment, some of which might be personal, protected or confidential in nature, is then continuously exposed to security threats because e-Learning systems are open, distributed and interconnected.

E-Learning has gone through a spectacular development during the past years. E-Learning systems are diverse and widespread, with examples including Web CT, Moodle and Blackboard. They are large and dynamic with a variety of users and resources. The sharing of information, collaboration and interconnectivity are core elements of any e-Learning system. Data must then be protected in order to maintain confidentiality, integrity and availability. Protecting against data manipulation, fraudulent user authentication and compromises in confidentiality are important security issues in eLearning. Online courses are more susceptible to cyberattacks than conventional courses, particularly in terms of endpoint security, privacy, and process.

Cyber risk that can compromise the safety of online learners includes:

- Malicious software
- Hacking, ransomware and denial of service attacks
- Spoofing, fraud and data theft
- Confidentiality and integrity issues
- Human errors

These issues negatively affect productivity and could also become liabilities to educational institutions, if not curtailed.

1.2 Research Purpose

The purpose of this study is to explain how educational institutions in Ghana address security concerns after the adoption of e-learning platforms.

1.3 Research Objectives

a. To explore factors influencing the adoption of e-learning system in Ghanaian education.
b. To explain the security threats that Ghanaian educational institutions face when they adopt e-learning as part of their operations.
c. To explain how Ghanaian educational institutions mitigate security threats in adopting e-learning as part of their operations.

1.4 Research Questions

- How can educational institutions in Ghana adopt e-learning platforms or solutions as part of their operations?
- How can e –learning aid educational institutions and their students in Ghana?
- What are some of the security concerns or threats associated with the operation of e-learning platforms in educational institutions?
- How can security threats associated with the adoption of e-learning platforms be mitigated?

2. SURVEY OF RELEVANT LITERATURE

E-learning and Technology

Online learning is a term first used in 1995 when the web-based system WebCT became the first learning management system LMS was developed and later became Blackboard. In this context, online learning meant using an LMS or uploading texts and PDFs online (Bates, 2014). Since then, online learning has included various overlapping terms such as e-learning, blended learning, online education, and online courses. Online learning can be broadly defined as using the Internet to enhance teacher-student interaction. Online delivery includes both asynchronous forms of interaction such as assessment tools, delivery of web-based course materials, and synchronous interaction through conferencing tools such as e-mail, newsgroups, and chat groups. This includes both classroom learning and distance learning. Synonyms for online learning include 'web-based education' and 'e-learning' (Curtain, 2002).

More recently Miller, Topper and Richardson (2016) write that over time, as a result of the advent of new technologies has necessitated the use of new terminologies to distinguish between emerging forms of Distant education, such as online education/e-Learning and hybrid/blended education (Moore et al., 2011;Spector, 2001). When used interchangeably, online education/e-learning has generally been defined as using web-based technology to bridge the gap between teachers and students. (Lee, 2017; Moore et al., 2011; Ryan et al, 2016). Over the last decade, technology has had a firm-established role in education experience (Almahasees and Jaccomard, 2020). To deal with dramatic changes in technology, methods, techniques, and strategies of education have been revised.

There has been technological enterprises that have designed several online platforms, which are powered by the integration of technology in all walks of life (Al-Azawei et al., 2017; Englund et al., 2017; Santos et al., 2019). Technology has become part of our social, business, and educational life'. According Silva and Cartwright in 2017 the use of the Internet has a vital role in disseminating knowledge via online classes. Education has made great progress as the form of education has changed from teacher-centered education to student-centered education. In teacher-centered education, the teacher acts as the source of education and the student is the receiver of his knowledge.

In contrast, student-centered education emphasizes the role of students in knowledge production in the classroom. In the student-centered approach, the teacher's role is "the student's facilitator, creating and enforcing their own rules. Teachers respond to student challenges and encourage students to provide alternative/additional answers. Student-centered instruction now benefits from many new technologies, such as the use of the Internet and other highly technological tools to share, transmit and amplify knowledge" (Hancock, 2002). Online learning has become part of the 21st century due to the use of online platforms.

The Internet and education have merged to provide users with the skills they need for the future (Haider and Al-Salman, 2020). A study by Stec et al., 2020 shows that there are three main approaches to online teaching: augmented learning, blended learning and online approaches. Enhanced learning leverages the extensive use of technology to ensure innovative and interactive instruction. Blended learning is a combination of face-to-face and online lessons.

An online approach means that the course content is taught online. Online education is convenient for students because it provides 24-hour access to online materials (Stern, 2020). Online education transforms education into student-centered education. There, students participate in the learning process and teachers act as tutors and guides for students (Al-Salman et al., 2021). Most authors agree that technology is an important part of the definition, regardless of the terminology they use when talking about online learning. Many authors suggest different methods of communication between students and instructors, which usually involve electronic communication methods.

The key element technology was used in the following ways to define the concept of online learning:

- Learning organized or delivered through web-based or internet based technologies
- Use of the internet to enhance interaction
- Use of the internet to enhance the learning environment
- Use of information and communication technologies
- Technology-based learning
- Audio/video CD-ROM, pre-2000 era as we can see, technology is used to define online learning by describing how technology delivers content, enhances the existing learning environment, and enhances the interactions among the students or teachers.

Online platforms have a variety of tools to facilitate interactive online course delivery and reduce student turnover. Online education platforms are used to share information and coordinate classroom activities (Martín-Blas and Serrano-Fernández, 2009).
There are the most famous online interactive tools: DingTalk (an online interactive platform

developed by Alibaba Group), Hangouts Meet (a video call tool), Teams (chat, interactive meetings, video and voice calls), Skype (video and voice calls), WeChat Work (video sharing and calling especially for Chinese), WhatsApp (video and audio calling, chat and content sharing), Zoom (video and audio calling and collaboration features) (UNESCO, 2020).

2.1.Benefits of e-learning

Everyone has the chance to learn through online courses. The idea of anytime, anywhere learning encourages lifelong learning and, as a result, gets rid of the issues related to distance. The key driving force behind choosing online courses is the flexibility that e-learning provides to the students (Jain, K. K. and Ngoh, 2003). The use of technology in education will also have a number of additional benefits, including raising learning standards, expanding access to instruction and training, lowering tuition costs, and increasing the cost-effectiveness of education. E-learning offers a platform that includes an effective e-learning environment that is meaningfully disseminated, guided, and learner-centered. It is also affordable, effective, easily available, and flexible.

Additionally, students can avoid spending money, time, and travel time to collect the necessary study resources. By reading the online learning resources that are available, they can save money on printing. E-learning also expands access to educational resources. Additionally, it gives students greater access to scarce resources like e-books and e-journals. This may help the students learn more effectively. People can now take control of their own lifelong learning by removing barriers related to time, distance, and socioeconomic position. Better student access and the relationship to communication both promote increased involvement. In addition to private forums between the student and the lecturer or instructor, students can also have public forums that allow them to communicate with their peers.

Faster assessment delivery is another advantage of online learning, as instructors may provide feedback more quickly than with traditional methods and students can share feedback among themselves.

2.2 Challenges with Implementation of e-learning

E-learning implementation is a difficult task. Despite the many advantages of e-learning, there are problems and difficulties that must be overcome if e-learning is to be successful. The issues are examined from the perspectives of both the learning provider and the user, as shown in Figure 1.

Higher Learning Institutions (HLIs) are having trouble with a variety of technology concerns, such as setting up an effective infrastructure, from the standpoint of the learning provider. Since students would need these resources to access online learning resources, bandwidth and connectivity are ultimately critical. Additionally, the distribution of high bandwidth material, such digital video, to the home user is still a challenge. Since there is a dearth of prepared high-quality content, learning materials are also a problem. The creation of quality student material should take into account a variety of elements, including pedagogical considerations, user interface design, and subject matter expertise. High implementation costs are to be expected because it takes a large budget to ensure that each of these is well-prepared. Due to the lack of resources, each of these issues is far more challenging in developing nations. From the users' standpoint, the settings of preparation present difficulties.

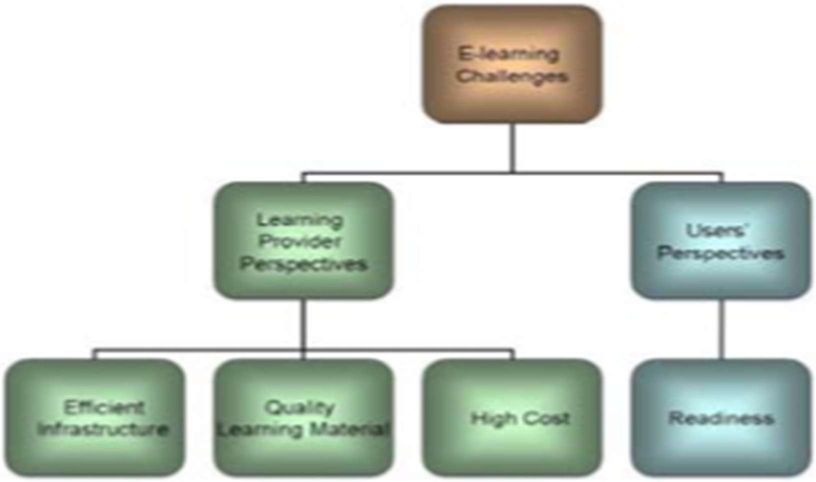

Figure 1: Showing the Challenges of E-learning

Aziz et al (2006) suggests that commitment and skills are important components in developing people's readiness. Knowledge and motivation for self-learning preparedness are both components of readiness. Due to their lack of computer literacy and self-discipline for independent learning, students are not ready for e-learning. The Technology Acceptance Model (TAM) also states that perceived usefulness and perceived usability have an impact on users' acceptance of technology use: if a student cannot see how e-learning can benefit them, they may not continue or may even enroll because they believe they will fail due to a lack of support and training from the learning provider. Instructors would also feel the same way, which leads to another reason why they don't want to use e-learning: they see little incentive or acknowledgment, despite the fact that there are numerous tasks to complete to ensure the success of e-learning.

Despite the difficulties mentioned above, the e-learning market is expanding. ELearning is expanding as a result of new institutions entering the online learning market and enduring student demand for this alternative. When creating an e-learning environment, factors including multimedia instruction, self-directed learning, instructor-led interaction, increasing learning effectiveness, and social presence must all be taken into account. When building safe and effective e-learning environments, these difficulties are somehow connected to confidentiality, accessibility, and integrity. According to Raitman et al (2005), a difficulty that is rarely highlighted in e-learning is information security, which is important. ELearning security has been neglected and abandoned.

3. E-LEARNING AND SECURITY

Online learning relies on the Internet to be carried out because it is an Internet-based learning approach (Alwi & Fan, 2010). On the other hand, there are a lot of criminal activities and security risks occurring online. As a result, the environment for online learning is invariably subject to ongoing security issues, attacks, and threats. Unfortunately, without careful preparation and without a complete grasp of the security issues of online learning, many educational institutions are rushing to embrace online learning management systems (Alwi & Fan, 2010).

A learning management system (LMS) has been used by over 88% of the schools assessed, according to a recent poll by Campus Computing and WCET (campuscomputing.net and wcet.info). Security in online learning refers to making sure that all authorized users can access learning resources when they're needed (Adams & Blandford, 2003).

Every component of an online learning system may be a possible target of hacking or attacks since online learning occurs over the Internet. This might cause instructional resources to be altered or destroyed without authorization (Zuev, 2012). The inherent security dangers of the Internet, such as identity theft, impersonation, and weak authentication, must be taken into account when teaching online (Ayodele, Shoniregun, & Akmayeva, 2011).

Cybercriminals who make a living by breaking into such networks have become interested in online learning platforms. The risk is high; as online learning systems' capabilities and features advance in sophistication, security risks grow more prevalent (Alwi & Fan, 2010). Researchers have created a number of methods and countermeasures to enhance security in online learning in response to growing risks. Protection from intentional or unintentional exploitation of resources in online learning is referred to as security (Adams & Blandford, 2003; Neumann, 1994). According to prior research, the three fundamental needs for security are availability, confidentiality, and integrity (Adams & Blandford, 2003; Serb, Defta, Iacob, & Apetrei, 2013; Weippl & Ebner, 2008). Sensitive information should be protected from unauthorized access (Serb, Defta, Iacob, & Apetrei, 2013; Adams & Blandford, 2003) and should not be disclosed without authorization (Weippl & Ebner, 2008).

A login system and a strong delimitation marking registered users and user groups are required because there are many users in any online learning environment (including students, visitors, instructors, tutors, and administrators), protecting the access to the proper user is crucial (Serb, Defta, Iacob, & Apetrei, 2013). Security measures like authentication and encryption are typically used to secure personal information. Integrity, a crucial component of security, is the "protection of data from intentional or unintentional unauthorized modifications" and "the absence of incorrect system adjustments" (Serb, Defta, Iacob, & Apetrei, 2013). (Weippl & Ebner, 2008). It guarantees that "information and data are in accurate, correct, and full original form and have not been mistakenly modified or intentionally destroyed" (Raitman, Ngo, Augar, & Zhou, 2005). The key to preserving integrity in the online learning environment is access control (Serb, Defta, Iacob, & Apetrei, 2013). The preparedness for proper service is referred to as availability (Weippl & Ebner, 2008). It implies that authorized users can access an online learning system whenever they need to (Serb, Defta, Iacob, & Apetrei, 2013).

Additionally, it guarantees that "approved personnel have timely access to reliable information and communication resources" (Raitman, Ngo, Augar, & Zhou, 2005). Denial of service and/or the inability to process data can both harm availability (Serb, Defta, Iacob, & Apetrei, 2013).Graf (2002) asserts that the use of ICT in online learning can lead to a number of security problems, including loss of confidentiality and availability, the disclosure of sensitive information, and vandalism of public information services. Because security protection techniques have been used in online learning programs, security problems with online learning are typically linked to users' inadequate understanding of security measures, inappropriate conduct, and lack of education.

For instance, to safeguard their learning resources, the major online learning providers have set up firewalls and anti-virus software in practically all institutions (Weippl & Ebner, 2008). In order to protect online learning, they also keep improving their systems' technology and content (Alwi & Fan, 2010; Srivastava & Sinha, 2013).

But in recent years, security risks including information manipulation by outsiders and insiders (by students or insiders) and loss of confidentiality still occur occasionally, despite users' increased security awareness and abilities (Dietinger, 2003). Because any risk can significantly alter students' impressions of a system's dependability and trustworthiness, security is crucial for maintaining users' trust in the online learning environment (Adams & Blandford, 2003). Therefore, it is essential to recognize the underlying causes of security problems in online learning as well as the limitations of the present security protection techniques. The security concerns associated with online learning can then be reduced by developing countermeasures.

3.1 Security And Privacy Challenges In E-Learning

E-learning is an interdisciplinary field that includes informatics and educational science (including information security). Both disciplines need to be taken into account and examined in order to have a proper understanding of the influence of information security and privacy in e-learning. Because these fields encompass such a wide range of specialized issues, research needs to be constrained in order to provide a manageable subset. In general, policy and technology work together to determine the level of e-learning security and privacy. Although policy may have an impact on the choice and application of security technologies, security and privacy technology itself supports policy by offering best practices and lessons learned.

Information security is important in e-learning systems for a number of reasons, including e-assessments, confidential data, the dependability of electronic communication, and more [6].
A safe e-examination system must be offered in the case of e-exams in order to prevent cheating. The stability and security of e-learning systems are significant factors. Because some people might try to hack the system to change their grades, it is crucial to know exactly who is logged into the system and who is permitted to do what. We might quickly return to scenarios similar to those in conventional learning, where a physical connection between the student and lecturer must be made, if information security in this context is overlooked. There hasn't been a lot of study done recently to safeguard the e-learning environment.

According to Weippl (2005), the purpose of security in e-learning is to protect authors' e-learning content from copyright infringements, teachers from students who may undermine their evaluation system by cheating, and students from being overly closely monitored by their teachers when using the software, according to one definition of security and privacy in e-learning environments. In this sense, the security of technical systems is merely one aspect of e-learning security. In other words, it is a combination of goals, people, processes, and tools. It is required to cover the full environment, including the organizational process of teaching, system management, and examining. An eLearning system is subject to all information security threats connected to computer networks.

Although these dangers are not specific to the online learning environment, they should nevertheless be taken seriously. Because the emphasis was placed more on usefulness than security while designing e-learning information systems, many of them include security problems. As a result, there are limits to the amount of security that can be provided through technical methods, and these limits should be backed by sensible management and processes. The reputation and status of educational institutions may suffer significantly if their e-learning software is compromised in any manner due to a lack of information security. Therefore, it is crucial that all essential measures be taken to guarantee that information is appropriately safeguarded within the context of e-learning. One of the main information security problems can be found by looking into the privacy protection in universities that heavily rely on e-learning systems: the openness academic culture that is promoted by the majority of those institutions. According to Anderson (2006) , this indicates that, in comparison to openness, information security frequently receives a lower priority in the academic atmosphere . Security and privacy technologies are frequently seen as barriers in this "culture of openness," despite the fact that several occurrences have demonstrated the need of privacy protection and its underlying organizational value.

3.1 Causes of Security Threats

The user side and the management side of security issues in online learning can each be examined separately. On the user side, new ICT applications and irresponsible human conduct are what primarily contribute to security problems in online learning. In addition to the inherent security concerns of the Internet, the growth of new learning technologies like Web 2.0 and social media has allowed for numerous new security breaches and a far greater impact on security (Adams & Blandford, 2003; He, 2012). The volume of dangerous content and the frequency and sophistication of cyberattacks against these new Web services are both rising quickly.

Nowadays, many instructors facilitate collaborative learning in their online courses by utilizing social media platforms like Tumblr, Facebook, Wikis, online forums, and Twitter (He, 2011; Camarero, Rodrguez, & José, 2012; Patel et al., 2012). These social media platforms, however, present a number of major security hazards and threats to naïve educators and students. Wikis, for instance, can be used for collaborative learning but also for hacking, deceit, abuse, and misuse (Patel et al., 2012). Personal information shared on social networking platforms has numerous potential uses (e.g., for virtual insult or, worse, for financial gain). Furthermore, according to recent studies, social media platforms are more likely to be exploited to spread malware than previously widely utilized email delivery techniques (Kaspersky, 2009; He, 2013).

Other academics examine security issues from the user's point of view. For instance, Adams and Blandford (2003) assert that there are two key causes of vulnerabilities to the security of online learning: 1) The security measures implemented in online learning programs are not user-friendly; or 2) The security discipline is not user-centered, which may cause users to ignore significant security threats. They make the point that the need-to-know principle, which limits access to information only to those who need it, along with security departments' reluctance to get to know their consumers, may contribute to the low usability of security systems. Many online learning systems do not give users enough feedback or control rights to allow them to preserve their data because of their poor usability (Adams & Blandford, 2003).

Additionally, inadequate user-centered security mechanism and policy design can increase insecurity and decrease users' incentive to seek security (Adams & Sasse, 1999). Online learning companies have erred in certain management-related ways. Threats in the area of online learning come from both insiders and outsiders (Alwi & Fan, 2010). Many academics contend that the inadequate security rules and ineffective security procedures utilized by online learning companies are to blame for security problems.

For instance, Serb, Defta, Iacob, and Apetrei (2013) point out that despite the fact that more students are now enrolling in online courses, the security issues associated with this type of learning have not been given adequate consideration in the actual educational setting. Alwi and Fan (2010) draw attention to the fact that many online learning providers implement information communication technology too quickly and without fully understanding the security issues involved.

Yao and Ji (2011) point out that the quality of online course content is a far bigger concern for online learning system developers than system security. Weippl and Ebner (2008) further point out that despite the fact that practically all schools have firewalls and anti-virus software to safeguard their campus resources, they frequently do not carry out proper information system security management. Sadly, online learning still prioritizes content and technology (Srivastava & Sinha, 2013). We believe that the security component of online learning needs to receive more focus. In fact, security is crucial for online learning because a lack of security would lead to a number of grave issues.

As Adams and Blandford (2003) point out, for instance, any security risk in online learning can have a significant impact on students' perceptions of the dependability and trustworthiness of online learning. As a result, online learning will be less appealing and its advancement will be impeded. User authentication is also a significant obstacle to student assessment in online learning due to ICT applications. Alwi and Fan (2010) contend that it is challenging to confirm that an assignment was finished and/or submitted by a legitimate student when grading students' assignments. The effectiveness of online learning will suffer substantially if student assessment is not carried out properly.

4. COMMON SECURITY ATTACKS AND THEIR COUNTERMEASURES

The number of attackers is continuously growing, and their attack techniques are becoming increasingly sophisticated and dangerous, which impose real security challenges on the organizations to secure their web applications. Hence, the security of web applications has become an important research area, and several solutions have been proposed to protect web applications. This section tries to identify the most severe web attacks as well as the appropriate countermeasures against each attack. The critical attacks are determined based on the most known web vulnerabilities, which were released by the OWASP project. We have reviewed the security countermeasures to provide the readers with the smallest set of protection methods that prevent the broadest range of critical attacks.

Injection

- The injection attacks can be executed by injecting (sending) untrusted information for an Interpreter. This injection is a part of an instruction: command/query. By providing malicious information, the attacker can mislead the interpreter and cause unintended commands. The most critical injection attacks are the following:
  - SQL Injection: It consists in injecting (inserting) SQL commands into input forms or queries to get access to a database (DB) or manipulate its data, for example: modification or deletion of database content.
  - Code Injection: This attack consists in injecting code that the application interprets and runs, which exploits poor processing of untrusted data.

Broken Authentication and Session Management

In case of broken authentication and session management attack, the intruder tries to exploit the vulnerabilities of the authentication procedure in order to access the WA or to use the credentials of other authorized users. This attack is classified into the following categories:

- Brute Force Attack: It consists in trying a combination of characters to guess the password of a given user.
- Dictionary Attack: If the attacker has some knowledge on the victim, he can prepare dictionary (set of valid words). Then, he combines these words to guess the victim password.
- Credential Enumeration Attack: Under this kind of attack, the intruder attempts to harvest valid usernames for a password-guessing campaign, by using verbose error of message telling whether the login is a valid username or not.
- Session Fixation Attack: In this attack, the hacker fixes the session ID, which will be used by user before the user logins into the server. – Cookie Poisoning Attack: It consists in modifying a cookie by an intruder to obtain unauthorized information about the user for the purpose to perform for example identity theft.

Cross-site Scripting (XSS)

It consists in injecting malicious code/scripts into web responses, which are returned back by the trusted WA, to be executed by the web browser. The following three main kinds of XSS exist according to the way the malicious code is injected:

- Stored XSS Attack: It takes place when the user input (such as message forum, database data, comment field, visitor log, etc.) is stored on the Web application server. Then, a victim may get back the stored data from the WA without making it safe.
- Reflected XSS Attack: It occurs when a client receives data in an HTTP request and uses the data in an unsafe manner within the immediate response.
- DOM Based XSS Attack: In this attack, the whole malicious data flow from source to sink occurs within the browser. It means that the data source is in the Document Object Model (DOM), the sink is in DOM as well, and the data flow does not leave the browser.

Insecure Direct Object References

A Direct Object Reference takes place whenever a programmer presents references to internal implementation objects. It may be a database key, directory, or file. When there is no access control or other security measures, intruders may exploit such references to reach unauthorized data. This vulnerability may lead to the following several attacks:

- Path Traversal Attack: It is a kind of attack, in which insecure direct object reference to directories and files which are placed outside the web root folder or in hidden places including system and configuration files.
- Direct Request Attack: (also called forced browsing) It consists in using brute force procedures to access unlinked contents in the main directory. The attacker may use google crawler to list hidden pages and files. – Authorization Bypass Through User-Controlled SQL Primary Key Attack: It occurs when the attacker manipulates a DB table primary key, which is used in an SQL statement, in order to reach inaccessible records.

Security Misconfiguration

Security misconfiguration problem occurs when one or more of the components of the system such as the applications, the frameworks, the application server, the web server, the DB server, the network router, and the platform are not well configured. Secure settings have to be defined, implemented, and maintained. Default settings are very often the cause of such a risk [50]. The attacker could exploit this flaw to perform several attacks. The severity of the attack depends on the misconfiguration level and place.

Sensitive Data Exposure

IT systems always store in a DB users personal data like passwords, home addresses, phone numbers, credit card details, etc. Once the systems are not properly secured from forbidden access, there is a strong likelihood of an attacker exploiting that vulnerability and stealing the information. There are three attacks, which are related to the sensitive data exposure:

- Information Leakage Attack: it occurs when a WA reveals sensitive data, such as error messages or developer comments. These sensitive data, which give an attacker useful guidance, can be exploited to attack the system.
- Transmission Attack: When the communication is not encrypted, all data exchanged between the client and the web server is sent in clear-text which leaves it exposed to interception, injection and redirection.
- Database Theft: when the sensitive data in the DB is not protected using strong encryption or access policies, attacker could steal this data. Three database attacks are possible: Brute-force attack; SQL injection and Privilege escalation.

Missing Function Level Access Control

Some Web applications check access rights to function level before making the feature available to the user. Nevertheless, once each feature is accessed, applications must achieve the same access control check for the server. Whenever requests are not checked, attackers can access the features without proper permission.

Examples of attacks that may exploit this vulnerability are the following:

- Local File Inclusion Attack: The attacker tries to find a page that receives as input a path to a file to be included in the calling page.
- Remote File Inclusion Attack: it is the same as the Local File Inclusion Attack but instead of including files located in the same server, the attacker manipulates the user input to include remote files. A Survey on Web Protection Methods 239
- Command Injection Attack: it is another attack that accesses the OS functions with unauthorized manner. The attacker tries to find a piece of code in the WA that accepts untrusted input to build OS commands without proper sanitization.

Cross-site Request Forgery (CSRF)

Web application is vulnerable to CSRF attacks (sometimes referred to as XSRF or Session Riding) when it does not verify that any request done by a trusted user has actually been intentionally done by that user only. There is a big difference between CSRF vulnerabilities and XSS vulnerabilities. The CSRF attack exploits an authenticated user to make a request on their behalf. Thus, a web site that uses cookies for authentication may be vulnerable, as well as those web application that use Basic or Digest authentications, because the browser automatically sends the cookies and the server will rely on that browser.

Using Components with Known Vulnerabilities

Software Components, like frameworks, libraries, and other kinds of modules, often execute with maximum privilege. Whenever a weak component is attacked, it may lead to serious threat. Depending on the vulnerabilities of the components, any kind of attack is eventually possible. For example, if a website is using a library vulnerable to SQL injection, the whole website will be vulnerable to such an attack. The open source libraries, framework, and content management systems (CMSs) are the source of many attacks.

Unvalidated Redirects and Forwards

Web applications usually forward and redirect users to other websites and pages, and exploit input data to identify new potential destinations. Without proper checking and authentication of the input data, users can be redirected to malware or phishing. Attackers may also exploit forwards to reach unauthorized zones. For instance, http parameter can include, or part of, a URL value, which could be exploited by the Web applications to redirect the request to the considered URL. An attacker can execute a phishing scam and capture user information by changing the URL address to a hostile site. Since the server in the updated connection has the same name as the original (trusted) site attempts at phishing look more trustworthy.

Countermeasures to common security attacks

In this section, we present the main proposed solutions to mitigate web attacks described in the previous section.

Countermeasures against XSS Attacks

A first defense line against XSS, at the server-side, is to adopt a user-input validation to enforce the security. Validation can use either blacklisting or whitelisting techniques. Moreover, once user-input is found to be malicious, it can either be sanitized or rejected [3].

However, the secure input handling method cannot achieve full protection, especially for complex website. A second defense line, which is becoming more and more implemented in web-servers, is based on Content Security Policy, which generally defines trusted origins that the browser is allowed to download resources (can be a script, a style-sheet, an image, etc.) from them.

Therefore, although an intruder is able to inject vulnerable content into the website, the CSP method may block its execution. Authors in [63] proposed a secure Web applications proxy for detecting and blocking Cross Site Scripting (XSS) attacks. The proposed framework contains a reverse proxy intercepting the returned HTML messages first, then using an altered web browser to locate vulnerable scripts.

The authors in [59] proposed to use Kullback-Leibler Divergence (KLD) measure to provide a proxy-level detection methodology for the XSS attacks. The idea is based on the intuition that legitimate WB JavaScript code should remain comparable or very similar to a rendered web page's JavaScript code. For this purpose, the authors proceed to the tokenization of the considered script code into unique elements and calculate the probabilities of their occurrences in order to construct two sets P (legitimate JS code available in the application page) and Q (observed JS code available in the response page). Then, KLD computes the distance separating these two proposed probability distributions. An XSS attack is detected in case of a significant divergence between the two sets.

Countermeasures against Insecure Direct Object References

To secure the access to the resources and the utilization of internal functions of a Web application, most of security systems have used access control mechanisms. For instance in Role-Based Access Control (RBAC) [27], programmers control objects by permissions, assign permissions to roles and assign roles to users. Permission authorizes a user for a role in a given session. The Separation of Duty Constraints prevent a user from acquiring two or more conflicting roles. For example, Cisco ACE Web application Firewall uses RBAC to define the administration roles of the WAF itself. Park et al describes an implementation of RBAC with role hierarchies on the Web by secure cookies.

The user's role information is injected in a set of secure cookies and transmitted to the corresponding Web servers. In order to verify the cookies, they use PGP (Pretty Good Privacy) to define cookie-verification procedures. Ardagna et al proposed an access control method for open web service applications. Their work is based on the eXtensible Access Control Markup Language (XACML) which belongs to the class of access control languages.

Countermeasures against Sensitive Data Exposure

As presented in Sect. 1, the following three categories of sensitive data Exposure flaw exist: – Information Leakage: As for this flaw, only the developer can improve security by paying attention to what he leaves in the code and to handle in a secure way the errors that can occur. – Transmission Attacks: this kind of attacks is mainly avoided by a strong encryption mechanism and we do not know a well-known approaches used in WAFs. – Database Thefts: to deal with this attack, cryptography is a key solution together with a good security policy to access database. In [26], the authors proposed a dynamic database security policies as a solution for this kind of attack. As conclusion, there are no known approaches that can be used by WAFs to overcome sensitive data exposure flaw.

Countermeasures Against CSRF

There are some countermeasures at the server-side to mitigate CSRF attacks. OWASP developed a project called CSRFGuard. It is a library, which implements a variant of the Synchronizer Token Pattern to minimize the risk of CSRF attacks. Jovanovic et al defined a server-side proxy named No Forge, which could be plugged into the considered system to discover and avoid CSRF attacks and it is transparent to users and applications. This proxy primarily detects and protects PHP applications against CSRF attacks. Zeller et al. enumerated the characteristics of server-side precautions to protect users. They also developed a plug-in at the server side for preventing users from the attacks.

Countermeasures against Unvalidated Redirects and Forwards

Scott et al categorized the phishing countermeasures into four categories: blacklist-based, heuristic-based, visual similarity-based, and machine learning based. The blacklist-based techniques build a repository of discovered phishing URLs, which should be updated regularly. The most representative works under this category are the Google Safe Browsing API, Phish Net, which predicts the phishing URLs based on the known phishing URLs, and Automated Individual White-List (AIWL) that keeps a list of trusted Login User Interfaces (LUI). However, this list suffers from the problem of untrusted LUI prediction. Generally, the blacklists offer good True-Positive (TP) rates but suffer from False-Positive (FP) rates. According to Fredj et al SPHERES is a WAF implemented in the Web application server based on behavior, and prevents the phishing attack by defining a profile for each parameter provided by the web client.

Table 1. Attacks classification and their countermeasures

Attacks	Sources	Sinks	Countermeasure techniques
Sql Injection	User input, cookies, server variables	Database	• Information theory based; compare the query entropy before deployment and during execution • Artificial neural network • Semantic comparison • Positive tainting and on syntax-aware Evaluation • Syntactic structures comparison of the programmer-intended query and the actual query • Software-testing techniques • The model is expressed as a grammar that only accepts legal queries • Taint based approach
Code injection		System Web site	• Technique based on multitier Compilation • Constructs a control flow graph foreach function

Attacks	Sources	Sinks	Countermeasure techniques
Brute force attack, Dictionary attack, Credential enumeration	User input	Session	Picture-based
Session hijacking, Session fixation, Cookie poisoning	Cookies	Website, URL, Session	• Time signature based • Shared secret • Token per request • Chains of nested HMAC
Stored XSS, reflected XSS, DOM XSS	User input	Data base Website	• Per-page security policies • Probability distributions of tokens extracted from the script code • Creation of shadow pages that reflects the set of scripts that a web application intends to create • XSD schema file • Reverse proxy • Boundary injection and policy generation
Attacks	Sources	Sinks	Countermeasure techniques
CSRF	User input	Database	Server side changes and captcha
Privilege escalation	Use input	Database	• Automatically instrument application source code program analysis to check for authorization state consistency in a web application
Transmission attacks	User input	ALL	Cryptography
Directory traversal attacks, Path Traversal attack, The direct request attack	User input	System, website	• Access control using RBAC • Simple filtering rule
Authorization bypass through user-controlled key	User input	DB	Access control using RBAC
Local file inclusion, Command injection, Remote file inclusion	User input	System, DB, NET, website	Access control using RBAC
Phishing attack	User input	DB (user credentials)	• Recognize fake URLs • Recognize whitelist URLs

5. GAPS FOR FUTURE RESEARCH

The impact of integrating ICT into teaching and learning depends significantly on the choices made by schools, instructors, and students about its deployment and use, as shown by the body of research and common sense. We also have proof that the relationship between the caliber of ICT learning possibilities and academic standards depends on the general caliber of instruction and the caliber of school administration (Becta, 2003b, c). Again, more needs to be done in this area. There is still much to learn about the circumstances in which ICT implementation and use have a beneficial impact, particularly the institutional circumstances supporting success. Work on modeling institutional maturity falls well here.

In terms of policy, this work is crucial because it may help schools understand the conditions that must exist for the advantages of ICT investment to materialize. However, the requirement for study goes beyond just efficacy to include efficiency. The e-Learning Strategy offers a vision of how education will change, but this must necessarily take place within the limits of the current pool of resources. Public organizations and institutions who are serious about utilizing the benefits of e-learning must carefully plan their ICT, staffing, and training needs. A key part of this picture is how the deployment of ICT affects the amount of time that frontline employees can be productive. Although rarely taken into account or costed in e-learning studies, this information is crucial for providing e-learning that is both economically viable and sustainable. Cost-benefit analyses are crucial in this situation.

REFERENCES

1. Fredj, O.B.: Spheres: an efficient server-side web application protection system. Int. J. Inf. Comput. Secur. 11(1), 33–60 (2019)
2. Cao, Y., Ye, C., Weili, H., Yueran, L.: Anti-phishing based on automated individual white-list. In: Proceedings of the 4th ACM Workshop on Digital Identity Management - DIM 2008 (2008)
3. Scott, D., Sharp, R.: Specifying and enforcing application-level web security policies. IEEE Trans. Knowl. Data Eng. 15(4), 771–783 (2003)
4. Jovanovic, N., Kirda, E., Kruegel, C.: Preventing cross site request forgery attacks. In: Securecomm and Workshops, 2006. pp. 1–10. ieeexplore.ieee.org, August 2006
5. Park, J.S., Sandhu, R., Ghanta, S.L.: RBAC on the web by secure cookies. In: Atluri, V., Hale, J. (eds.) Research Advances in Database and Information Systems
6. Security. ITIFIP, vol. 43, pp. 49–62. Springer, Boston, MA (2000). https://doi.org/ 10.1007/978-0-387-35508-5 4
7. Ardagna, C.A., di Vimercati, S.D.C., Paraboschi, S., Pedrini, E., Samarati, P., Verdicchio, M.: Expressive and deployable access control in open web service applications. IEEE Trans. Serv. Comput. 4(2), 96–109 (2011)
8. Weippl, E.R. - Security in E-Learning. Springer Verlag, New York, 2005
9. Anderson, A. - Effective Management of Information Security and Privacy, Educause Quarterly Journal, no. 1/2006, pp. 15-20
10. Security Risks and Protection in Online Learning: A Survey https://www.irrodl.org/index.php/irrodl/article/view/1632/2712
11. YongChen and Wu He - Old Dominion University, USA

12. Faculty's and Students' Perceptions of Online Learning during COVID-19 https://www.frontiersin.org/articles/10.3389/feduc.2021.638470/full#B4
13. Vanessa Pittard (2004) Evidence for e-learning policy, Technology, Pedagogy and Education, 13:2, 181-194, DOI: 10.1080/14759390400200179
14. Bates, T. (2014). A short history of educational technology. Retrieved from https://tonybates.wpengine.com/2014/12/10/a-short-history-of-educational-technology/
15. Curtain, R. (2002). Online delivery in the vocational education and training sector. Retrieved from http://www.flexiblelearning.net.au.
16. Ryan et al., (2016). The effectiveness of blended online learning courses at the Community College level. Community College Journal of Research and Practice, 40(4), pp. 285–298.
17. Lee, K. (2017). Rethinking the accessibility of online higher education: a historical review. The Internet and Higher Education, 33,15–23. doi:10.1016/j.iheduc.2017.01.001
18. Moore, J., Dickson-Deane, C., & Galyen, K. (2011). E-learning, online learning and distance learning environments: Are they the same ? The Internet and Higher Education, 14(2), 129135. doi:10.1016/j.iheduc.2010.10.001
19. Education, 33:4, 289-306, DOI: 10.1080/08923647.2019.1663082 To link to this article: https://doi.org/10.1080/08923647.2019.1663082
20. Jain, K. K. and Ngoh, L. B. (2003), 'Motivating Factors in e-learning -a Case study of UNITAR', Student Affairs Online, [Online], vol. 4, no. 1, pp.21, June, 2008 available at: http://www.studentaffairs.com/ejournal/Winter_200 3/e-learning.html.
21. Raitman, R., Ngo, L. and Augar, N. (2005), 'Security in the Online E-Learning Environment', Advanced Learning Technologies, 2005.ICALT 2005.Fifth IEEE International Conference on Advanced Learning Technologies, pp.702-706.
22. OWASP top ten project - OWASP. https://www.owasp.org/index.php/
23. OWASP Top Ten Project. Accessed 230 July 2020
24. Information security in E-learning Platforms - Defta (Ciobanu) Costinela – Luminitaa*
25. CYBER SECURITY CONCERNS IN E-LEARNING EDUCATION - I.Bandara, F.Ioras, K. Maher
26. Security Enhancement for e-Learning Portal - A. JALAL1 and Mian Ahmad ZEB2