ISSN 2454-8596
www.vidhyayanaejournal.org

An International Multidisciplinary Research E-Journal

Vulnerabilitiesin E-Learning system & ROLE OF Graphical password

Pratik S. Patel [1] *, Dr. Mukta Agarwal [2], DR. Ashish Chaturvedi [3] Research Scholar, Department of Computer and Informative science, Sabarmati University,

Ahmedabad, Gujarat India [1],

Asst. Prof, Department of Computer and Informative science, Sabarmati University,Ahmedabad, Gujarat India [2]

Registrar, Sabarmati University, Ahmedabad, Gujarat India [3],

ABSTRACT

This paper describes a survey of online learning which attempts to determine online learning providers' awareness of potential security risks and the protection measures that will diminishthem. The authors use a combination of two methods: blog mining and a traditional literature search. The findings indicate that, while scholars have identified diverse security risks and have proposed solutions to mitigate the security threats in online learning, bloggers have not discussed security in online learning with great frequency. The differences shown in the survey results generated by the two different methods confirm that online learning providers and practitioners have not considered security as a top priority. The paper also discusses the next generation of an online learning system: a safer personal learning environment which requires a one-stop solution for authentication, assures the security of online assessments, andbalances security and usability.

E-learning has become a need in advanced education foundations and is being sentin instructive foundations all through the world. Scientists have made a lot of accentuation onits advantages yet very little is examined on the burdens of e-learning innovation. This paper references a portion of the examination work on the impediments of e-learning innovation classifies it in five difficulties that educators are confronted with and ideas for an effective e- learning result.

Keywords: e-learning, higher education, academic challenges, attacks, users

1. INTRODUCTION

E-learning is the unifying time period to describe the fields of on line mastering, net-based education, and technology brought instruction. usually the e-gaining knowledge of term is thought as on-line courses, on line education (net-primarily based gaining knowledge of), andthe pc-based totally getting to know term can be taken into consideration as a issue of e- mastering which does no longer require a non-stop interplay with an trainer and other college students. beneath are a few traits of the e-learning systems: the learning system is achieved in a digital study room; the academic fabric is to be had on the net and includes text, pics, link to different on line assets, photos, audio and video shows; the virtual study room is coordinated by means of an trainer who plans the interest of the work institution participants, discusses aspects of the direction the use of a discussion discussion board or chat, provides auxiliary resources, etc; the studying will become a social manner; a studying network is created via the interplay and collaboration between the trainer and the workgroup contributors; most of the people of e-gaining knowledge of structures permit the activity monitoring of the members, and some of them.

As an Internet-based learning technique, web based learning relies upon the Internet for its execution (Alwi and Fan, 2010). Nonetheless, there are quite a few criminal operations and security dangers occurring on the Internet. Therefore, the e-learning climate is unavoidably presented to steady security dangers, dangers, and assaults. Sadly, numerous instructive foundations are racing into embracing web based learning the executives frameworks withoutcautious arranging and without a careful comprehension of the security parts of internet learning (Alwi and Fan, 2010). A new review directed by Campus Computing (campuscomputing.net) and WCET (wcet.info) found that practically 88% of the overviewed establishments have received.

The Internet medium is notable to play host to various dangers, including the entirety of the accompanying:

Malicious programming, for example, infections, worms,Trojan Horses

Hacking, Denial of administration assaultsMasquerading, mocking

Fraud, information robbery, vindictive harm

In light of expanding dangers, specialists have built up various countermeasures and answers for improve security in internet learning. The motivation behind this paper is to incorporate the connected conversations in the writing, to give a top to bottom audit of the security parts of internet learning, and to recognize the future patterns and difficulties to security in web based learning. At present, the conversation of security dangers of internet learning is divergent, divided, and appropriated among various sources, for example, scholarly articles, white papers, instructive reports, and news stories.

2. THREATS AND RISKS IN E-LEARNING SYSTEM

- In this section, we outline the most important cyber security risks related to higher education systems and distributed e-learning systems

- In the e-learning system, the 3 important participants are:

A: Author

- As we all know, authors can provide a wide range of students with access to books and journal articles. They can also develop and implement the content of these documents. Since only registered students can access the teacher's notes, assignments and class tests, the author is responsible for preventing unauthorized use, modification and reuse of data in different situations related to e-learning. It is an important part of any course teaching. One form of discussion can be conducted through online forums. Compared with oral discussions, one advantage of discussions in online forums is that all written documents are stored electronically on the server, but digital storage of the content of the discussion poses a great risk to the privacy of students and teachers. Although in any teaching system, maximum interaction can help students and teachers clarify their understanding, only a strong safety mechanism can lead to such interaction in the long term. The examination system includes the standardization of examination questions and a list of questions that may limit the academic freedom of individual teachers. Therefore, the related risks related to the examination are directly related to cheating; teachers must also pay attention to the availability and non-repudiation of assessments, and they must be aware that students are Risk of receiving test papers without making any changes

B.Students

- Every student must understand every document received from the college, teacher or other student. Because if the intruder edits the problem file or other important files, he will have to deal with the problem while checking.

- Store login information: User ID and password, giving attackers a great opportunity to prevent authorized students from accessing the password. E-learning servers use many attacks. The system will ask students to enter confidential information to spoof the website (due to phishing) and look like a real e-learning website.

C. Managers

• Many risks in the e-learning platform involve clumsy people posing as students and taking writing tests on behalf of registered students, and unauthorized help during writing tests online, therefore Legal issues such as copyright, online tests, sending official documents ..., can be a big problem for those participants. In this case, the administrator should pay attention to the course registration and cancel the registration when necessary. Enrolling in multiple courses for a given student can pose risks for larger organizations. There must be a backup plan and recovery process test plan, otherwise it will be difficult to update the data. Generally, e-universities must resolve issues related to student identity verification, unfair execution of tasks, theft, and copyrighted materials placed on the Internet. Therefore, the integrity of electronic resources and the normal operation of the educational computer systemmust be protected [2] .

ATTACKS PERFORM ON PORTAL

To empower sufficient insurance of understudies confirming certifications from fraud during validation, the verifying arrangement should understand the accompanying securitydestinations [8]:

- **Replay assault:** Even in a circumstance when an understudy's touchy data is undermined, itought to be pointless to the aggressor.

- **Social designing assaults:** A social designer ought not to have the option to acquire information adequate to mimic a genuine understudy. The framework ought to likewise ensure that confirmation accreditations can't be adaptable. - Dictionary assaults: The viability of word reference assaults ought to be extraordinarily decreased or totally killed.

- **Shoulder riding assaults:** Even when the validation meeting is watched at closeness (even within the sight of omnipresent visual chronicle gadgets) the data got ought not to bring about any addition to the aggressor.

- **Malware obstruction:** We should guarantee that introduced m consistently has no impact on the model in instances of replay assaults.

- **Phishing assault:** Even in the wake of noticing quite a few fruitful validations we should guarantee that an aggressor can't disguise the confirmation interface and regardless of whether the converse is the situation, at that point the data gotten ought not bring about any addition to the assailant.

- **Eavesdropping opposition:** The exertion of busybodies ought to be baffled.

- Authentication code renewal and reuse: We should guarantee that MAM makes arrangements for validation codes to be transformed and reuse without it being a disturbance for the understudy, who follows this training on various frameworks and accounts, and consistently should fail to remember old and retain new codes.

- **High entropy:** If we should depend on the entropy of a confirmation model for assurance against disconnected assault, we require a validation model that can scale with processor rates and increment appropriated joint effort. Aside from the security destinations, a validation model needs to fulfill a bunch of convenience imperatives for it to be achievable for frameworks with a huge, shifted, understudy base. We accordingly should address the accompanying convenience goals:

- **User-Friendly Interface:** The model interfaces utilized should be custom fitted for understudies with no past information on the framework. The interfaces themselves should benot the same as current passer by thoughts that are misused by phishers.

- Physically innocuous. The confirmation model should make no actual mischief or distressthe understudy regardless of whether inaccurately worked.

Memorability: The framework ought to be instinctive to utilize and ought to force no extra weight on authentic understudy memorability limit. - Login Time: The login season of the verification enrolment or approval meetings ought to be diminished to around one moment.

- **Quick preparing:** The verification model ought to be natural enough for understudies withno earlier preparation to rapidly comprehend its convenience in under five minutes.

3. LITERATURE SURVEY

In this graphical password we are using an recognition and Recall-based techniques. The main reason behind this isbecause graphic picture is more recalled than the text password.Here we are distinguishing the graphical passwordtechniques till 2009. This techniques classified into three groups as follows

1. Recognition Based Technique

2. Pure Recall Based Technique

3. Cued Recall Based Technique

1. Recognition Based Techniques:

In this techniques user is presented with a collection of image, icons or symbol. During authentication user select the set of candidate's .Its Result is (90%) majority of user to remember the password after one or two months. Dhamija and Perrig proposed a graphical authentication scheme based on the Hash Visualization technique .In this system user have toselect no of images from the set of images generated by the program.

2. Pure Recall-base Techniques:

In this method user reproduce their password without using any hint and gesture .user wouldremember their password just like DAS (1999) and Qualitative DAS (2007).It is provided With varying levels of usability and security features.

It follows many algorithms, which include:

A] Pass doodle: This method is introduced in 1999. Pass doodle method is introduce byChristopher [2]. This is a graphical password which is made up of handwritten designs.

B] Syukri algorithm (pure recall):- This method proposes a system where authentication iscounted by having user drawing their signature using mouse in 2007.Advantage of this technique is that, guessing of any ones signature properly is not easy hence it is difficult to hack the system with this technique.

C] Qualitative DAS:

To overcome the drawbacks of DAS in 2007 QDAS [2] is introducing.

D] Draw a Secret:

It introduce in 1999.In this system user allow to draw a simple picture onto 2D grid. The rectangular grid consist of size G * G. Each cell in grid was denoted by discrete rectangularcoordinates (x,y).

3. Cued Recall Based Techniques:

In this technique framework of reminder, gesture and hints are consider. Using this techniqueuser reproduces their password or reproduction becomes more accurate. It follows many algorithms, which include:

A] Grid selection (pure recall):-

In 2004, Thorpe and Oorschot further studied by impact of password length and stroke countas complexity property of a DAS scheme.

B] Blonder Scheme (cued recall):-

This method was developed by Greg. E. Blonder. To begin with a determined image ispresented to the user on a

visual display and then the user have tap regions by pointing to one or more predefinedlocations on the image as a way of pointing out his or her authorization to access the resource. This method is secure since it has a million of different regions to pick from.

C] Pass point (cued recall):-

Pass point was design in order to cover the limitation of Blonder algorithm. In this methodclick point method is used.

4. Proposed System

At the only level, authentication may be primarily based upon traditional password mechanisms. These have the gain that they may be easily carried out using software program methods and are conceptually simple for the user to understand. But, there are a number of typically ordinary weaknesses with passwords (e.g. they're regularly poorly selected, without difficulty guessed, and rarely changed) that lead them to prone to compromise. a further trouble with passwords is that there might be not anything to prevent a valid scholar from sharing their access rights with other humans. I need to endorse a machine wherein customerscan enter the password in each factor to get entry to the useful resource.

5. CONCLUSION

The availability of the Internet continues to increase, and the number of end-user devices continues to increase, which promotes the demand for online learning. The application of Web 2.0 and MOOC heralds a new era of education. Online learning brings all the security risks inherent in using the Internet. However, although more and more people are taking online courses, online learning providers are not taking security risks seriously. Many of them are eager to adopt ICT without fully understanding the relevant security issues. Scholars have identified various security risks and proposed solutions to mitigate security threats in online learning. To our surprise, our research found that security is not a hot topic in blog posts involving online learning. So far, online learning providers and professionals have not put security in the first place. This may be because serious security incidents rarely occur in the field of online learning. As more and more people learn online, online learning providers and professionals need more attention and efforts to prevent potential online learning securityloopholes before it is too late.

References

1. A.A. Mirza and M. Al-Abdulkareem, "Models of e-learning adopted in the MiddleEast". Applied Computing and Informatics, 2011. 9(2): p. 83-93.

2. T. Fujuan, et al., "International ESL Graduate Student Perceptions of On-line Learning in the Context of Second Language Acquisition and Culturally ResponsiveFacilitation". Adult Learning, 2010. 21(1/2): p. 9-14.

3. Allan, J., & Lawless, N. (2004) Understanding and reducing stress in collaborative e-Learning. Electronic Journal on e-Learning, 2(1), 121-128

4. Ally, M. (2004). Foundations of educational theory for online learning. Theory andpractice of online learning, 3-31.

5. Radwan Ali, Humayun Zafar Kennesaw State University, USA “A Security andPrivacy Framework for e-Learning”

6. Ciobanu (Defta) Costinela - Lumini a * , Ciobanu (Iacob) Nicoleta - Magdalena b “E-learning Security Vulnerabilities”