Mohammed Awad Mohammed Ataelfadiel

Detecting vulnerabilities in universities' websites: A Security Analysis

Journal of Electrical Systems

Abstract: - Hackers use various methods to gain unauthorized entry into systems, particularly those operating on Internet platforms. This can be achieved through manual hand-held techniques, predominantly reliant on hacker experience, or by utilizing a specialized tool created either by the hacker themselves or by another information security professional. By utilizing these diverse approaches, hackers aim to pinpoint weaknesses in software, penetrate databases in order to compromise their confidentiality and utilize the information, or prevent access to and deletion of the content on the Website.

The scholar observed during his research at the institution the case study sample, highlighting various efforts to breach the electronic examination and registration systems (two subsystems within the college's primary platform). Consequently, the focus was directed towards detecting potential weaknesses in the fundamental code of the institution's website; precisely assessing the impact of these vulnerabilities. To meet the research goals, the scholar conducted vulnerability tests by inserting code into specific fields on the website pages. Upon receiving affirmative responses multiple times, the scholar proceeded to utilize the Acunetix Web Vulnerability Scanner tool (AWVS) by inputting the URL as the primary entry point and the sub inputs will be the sub links. Following an analysis of the test report, four software vulnerabilities were identified to exist based on the determination made, varying in strength from minor to moderate. These vulnerabilities were accurately pinpointed by identifying the affected areas, assessing the severity of each, and evaluating their implications on the website.

Keywords: vulnerabilities- Penetration- University URL - Cybersecurity – Penetration of Universities - Hacking college exams.

I. INTRODUCTION

The notion of implementing restrictions on a university network, including the research activities within the campus, to limit access solely to authorized personnel contradicts the fundamental principles of academia and scholarly inquiry. Unlike many corporations and certain government entities, universities typically do not prioritize confidentiality or external security in the configuration of their computer infrastructure. Conversely, academic institutions are designed to foster open collaboration, welcome visitors, cultivate international partnerships, and facilitate informal communication, thereby leading to easily accessible websites[1].

The objective of the study was to ascertain the presence of electronic susceptibilities within the coding of the college websites; facilitating potential unauthorized access and manipulation of their content. Additionally, it aimed to determine the extent to which the impacted files by these vulnerabilities can be precisely identified. This process aids in the formulation of suitable remedies and precludes their exploitation by the individuals responsible for safeguarding these websites. This ensures the requisite protection of data and site integrity prior to their exploitation by malevolent entities, given the substantial risks associated with potential complete loss of administrative control over the website.

II. LITERATURE REVIEW:

The Justice Department in Arizona state in the United States revealed on Friday the indictment of nine individuals from Iran for unauthorized access to numerous computer accounts owned by academic faculty members. These individuals were linked to an organization known as the Mabna Institute, which orchestrated extensive and synchronized cyber penetrations into the computer networks of 144 American universities as well as 176 overseas universities[1].

Hackers may have various motivations for targeting a university website, with some seeking to gain unauthorized access to databases and manipulate them (such as awarding degrees, altering grades, adjusting GPAs, among other actions), in addition to seizing control of the website's functionalities and bestowing illicit privileges. Their methods may involve accessing exams or academic outcomes, as well as targeting non-academic components like overseeing post modifications, promotions, and manipulating the benefits-related results. Irrespective of the hacker's intentions behind such endeavors, many have managed to achieve their objectives, as demonstrated by

Applied College, King Faisal university, AL-Ahsa, Kingdom of Saudi Arabia, melfadiel@kfu.edu.sa

incidents like the breach at Princess Noura University by Marjouj Al-Hazazai[2], and the case of a student at the University of Rennes II at 2011 who attempted to infiltrate the university's system to alter her Master's grades, succeeding in doing so[3].

Harvard University website has also experienced a security breach, as noted by Abigail Tracy. In her statement, Tracy highlighted that Harvard University fell victim to a cyber attack for the second time in a span of four months. The breach was disclosed by the institution on Wednesday, revealing that unauthorized access was detected in the Faculty of Arts and Sciences and Central Administration IT networks. This incident, which came to light on June 19, follows a series of prominent data breaches across the nation and closely follows an alleged takeover of Harvard's Institute of Politics website by the pro-Palestinian hacker group "AnonGhost." Tracy further elaborated that, as per Harvard's administration announcement, this recent cyber intrusion affected a total of eight schools and administrative entities within the university[4].

Damascus University, too, fell victim to cyber intrusion, where a message stating "Damascus University site has been hacked and all the results have been scanned" was discovered by students. This particular message caught the attention of a significant number of students at Damascus University as they navigated the university's official website in search of their results. The students' frustration with the delayed publication of results on the website appears to have motivated them to resort to more disruptive tactics. The hacker's motive for the breach was articulated as follows: "We refrained from disclosing our college results due to discrimination, claiming to be the disadvantaged party." The identity of the college to which the hacker belongs was left undisclosed. Notably, this issue is encountered by students across various colleges, indicating that it is not confined to a single institution[5].

A. Vulnerabilities and threats:

Vulnerability, often denoted as the absence of immunization, is commonly characterized as the susceptibility to physical or psychological damage or assault, along with the absence of safeguarding valuable assets and property. Within the realm of computer and network security, this term is used to denote weaknesses in systems that enable an adversary to launch attacks. Instances of Vulnerabilities may also arise from software malfunctions or design flaws, typically stemming from the oversight of the developer or designer. Moreover, the utilization of malicious software by an attacker can yield similar outcomes. Vulnerabilities pertaining to computer and network security are typically categorized into two distinct types[6]

a) Technical vulnerabilities stem from insufficient immunization caused by the methodologies implemented in systems and networks, leading to what is commonly referred to as a technical attack on the network.

b) Administrative vulnerabilities stem from non-technical factors, leading to attacks on the network or computer commonly referred to as social engineering attacks.

Vulnerabilities can be classified into three distinct categories based on their level of severity:

a) High-level, such as sql injections, XSS, which can be readily exploited.

b) Medium-level vulnerabilities encompass a wide range of types.

c) Low-level, are challenging to exploit, requiring substantial exertion, investment, and specialized knowledge on the part of the assailant.

B. Threats to information on the Internet:

The proliferation of benefits and information acquisition on the Internet has been noted in recent times, occurring at a significantly faster and more convenient pace compared to previous methods. These various forms of information encompass databases, research papers, emails, and others, necessitating adequate protection regardless of their storage location or form of existence on the Internet [7].

The utilization and extraction of valuable data to generate information is acknowledged as a crucial asset within any organizational setting. Enhancing the accessibility of said data and information serves to increase its usefulness to individuals, irrespective of their intentions being positive or malicious. Consequently, the increase in the population with the ability to obtain this data has resulted in a significant growth in the volume and range of cyber-attacks. With new vulnerabilities emerging daily, safeguarding this information becomes imperative to prevent loss and uphold the principles of integrity and confidentiality.

III. EMPIRICAL STUDY:

The researcher initiates the applied research by using the AWVS, a renowned tool in the realm of web vulnerability scanning. This scanner is adept at conducting penetration testing on identified vulnerabilities. Additionally, it has the capacity to analyze the source code and identify the specific line of code containing the vulnerability. [8]. he applied research unfolded through a series of sequential steps.

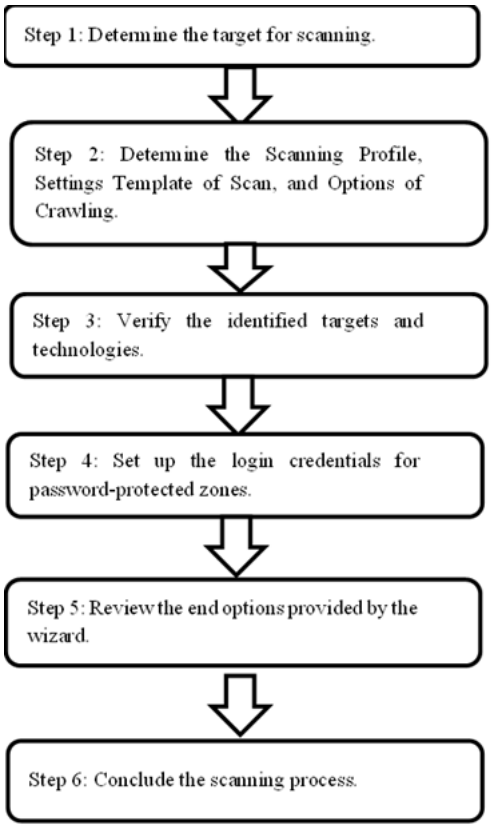

Fig. 1: steps of AWVS [9]

A. Determine the target for scanning:

The researcher delineates the specific website to undergo scanning, utilizing the website address of a developing academic institution for the research at hand. Omission of its name is implemented out of consideration for the delicate nature of the subject matter.

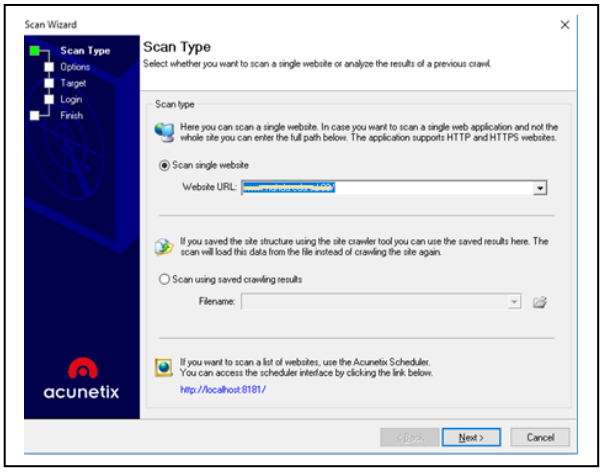

Fig. 2: Determine the target for scanning.

B. Determine the Scanning Profile, Settings Template of Scan, and Options of Crawling.:

In this stage, the scanning tool prompts the user to designate a scanning profile (such as SQL Injection or XSS) for application during the scanning process of the target website. The scanning profile is utilized to specify the vulnerability assessments that will be carried out on the website. Within the realm of research efforts, the default scanning profile was selected in order to comprehensively evaluate the website for any known web vulnerabilities.

Additionally, the tool requires the selection of scan settings, which dictate the configuration of the Crawler (utilizing the HTTP protocol and advanced crawling techniques) and the scanner settings to be used throughout the scan. For research, the researcher opted to retain the default settings in this regard.

Subsequently, the Crawling Options feature enables the manual specification of files and directories to be scanned after the crawl process. Additionally, it provides the functionality to direct the crawler to analyze URLs that are not necessarily connected to the main URL, utilizing the feature to specify a set of URLs for crawler processing from the beginning.

C. Verify the identified targets and technologies:

During the third phase, Acunetix WVS automatically conducts a preliminary analysis of the target website to extract fundamental details. By identifying the technologies in use, the web vulnerability scanner streamlines the scanning process and enhances efficiency by reducing the number of tests conducted for the identified technologies.

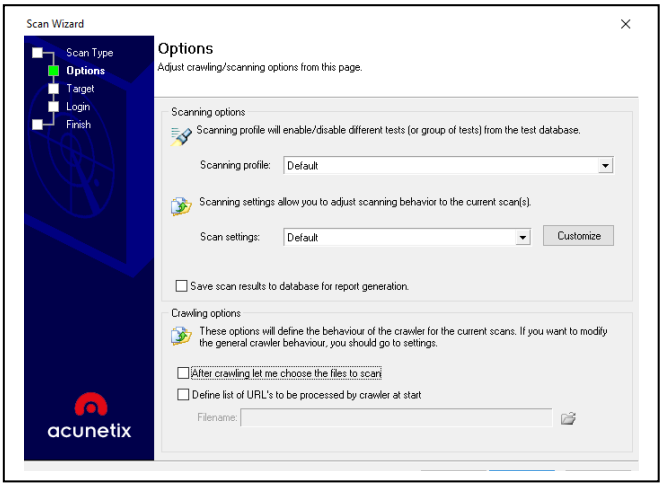

Fig. 3: Determine the Scanning Profile, Settings Template of Scan, and Options of Crawling.

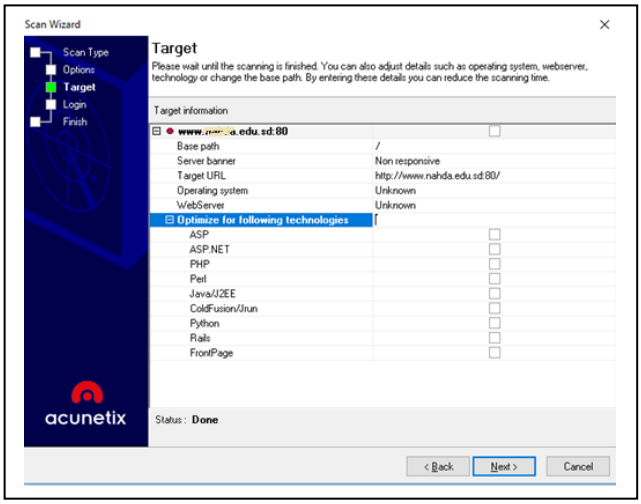

Fig. 4: Confirm Targets and Technologies Detected

D. Set up the login credentials for password-protected areas.:

There exist two prevalent authentication mechanisms utilized for the purpose of authentication.

- HTTP Authentication - The authentication of this kind is managed by the web server, leading the user to a dialogue box prompting for a password.
- Forms Authentication - This authentication method is executed through a web form, where the user's credentials are transmitted to the server and verified by a customized script.

For research, the researcher has opted to maintain this selection as the default (absence of a login sequence).

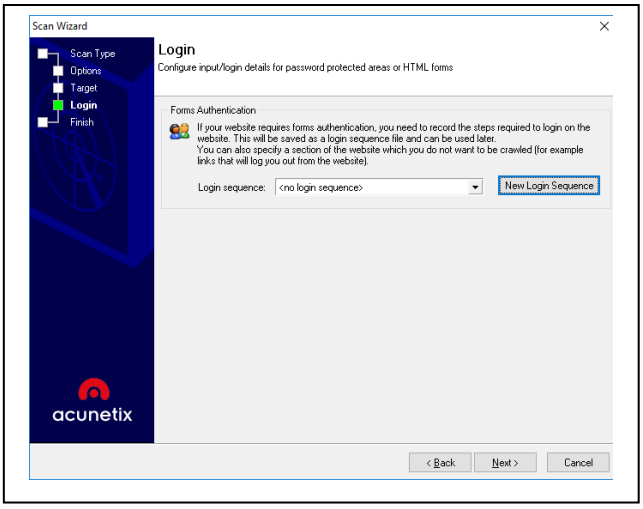

Fig. 5 : Login Configurations for Password Protected zones

E. Review the end options provided by the wizard:

The penultimate stage involves conducting an initial evaluation of the website, which can potentially alert the user to various issues such as encountering errors while trying to connect to the designated server. In cases where AWVS fails to automatically identify a pattern for a custom 404 error page, manual intervention may be required.

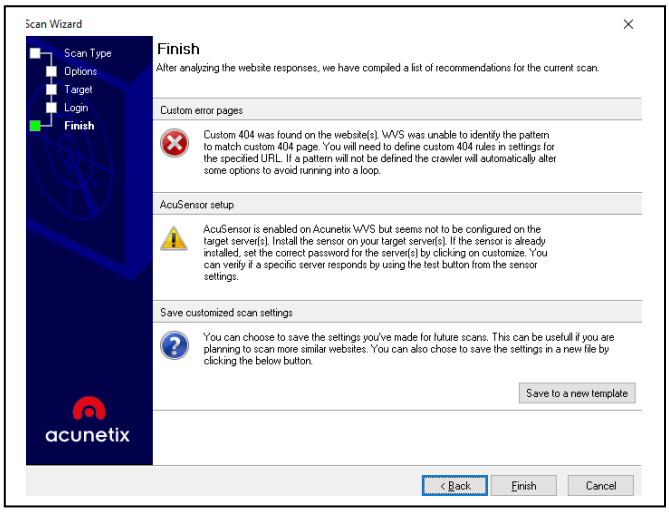

Fig. 6: Wizard last options

F. Conclude the scanning process:

The duration of a scan can vary depending on factors such as the website's size, the selected scanning profile, and the server's response time. In the specific research conducted, the scan was completed in a time frame of 35 minutes and 57 seconds.

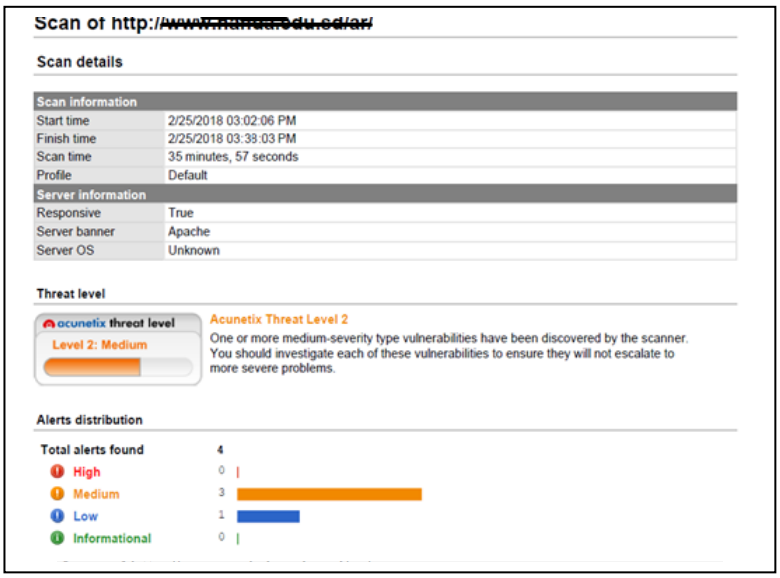

Fig. 7: Step (6): Completing the scan

IV. THE OUTCOMES ACHIEVED:

Upon successfully executing all phases of the research investigation, the researcher identified the presence of four vulnerabilities within the code of the college website under examination. These vulnerabilities included an HTML form lacking CSRF protection and a Slow HTTP Denial of Service Attack, both categorized as medium-level threats. Additionally, a Clickjacking vulnerability due to a missing X-Frame-Options header was identified as a low-level threat. These vulnerabilities pose significant risks, potentially leading to unauthorized access and control of the system.

V. RESULTS DISCUSSION:

A. Medium-risk vulnerabilities:

The scholar discovered three vulnerability within this particular tier:

1) HTML form without CSRF protection

CVSS	Base Score: 2.6 - Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: None - Integrity Impact: Partial - Availability Impact: None	
CVSS3	Base Score: 4.3 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: Required - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: Low - Availability Impact: None	
CWE	CWE-352	
Affected items		Variation
/ar		**2**

Fig. 8 :HTML form without CSRF protection vulnerabilities Classification

a) Description:

The phenomenon known as Cross-site request forgery, often referred to as a one-click attack or session riding and commonly denoted as CSRF or XSRF, entails a form of malevolent exploitation of a website where unwarranted directives originate from a user in whom the website has placed trust.

Within its assessment, Acunetix WVS identified an HTML form lacking any discernible implementation of CSRF protection.

b) Impact

Through a CSRF exploit, an assailant possesses the capability to compel a web application users to carry out actions dictated by the attacker. The successful execution of a CSRF exploit can lead to the compromise of end user data and functionalities, particularly in scenarios involving regular users. Should the targeted end user hold administrative privileges, the repercussions may extend to the entire web application.

c) Recommendation

It is advisable to scrutinize whether the form in question necessitates CSRF safeguarding, and if deemed necessary, to incorporate appropriate CSRF mitigation strategies.

d) Details of the impacted items.

Fig. 9: HTML form without CSRF protection, Details of the impacted items (1)

Fig. 10: HTML form without CSRF protection Details of the impacted items (2)

2) Slow HTTP Denial of Service Attack

CVSS3	Base Score: 5.3 - Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: None - Integrity Impact: None - Availability Impact: Low	
Affected items		Variation
Web Server		**1**

Fig. 11: Slow HTTP Denial of Service Attack vulnerability Classification

a) Description

The techniques of Slowloris and Slow HTTP POST DoS attacks exploit the inherent characteristic of the HTTP protocol, which stipulates that requests must be entirely received by the server before processing commences. In situations where an HTTP request remains incomplete or the data transfer rate is exceedingly slow, the server's resources become engaged in awaiting the remaining data. Prolonged occupation of server resources in this manner can result in a denial of service.

b) Impact

Using very little bandwidth, a single machine can obstruct another machine's web server, resulting in minimal impact on other services and ports.

c) Recommendation

It is advised to refer to reputable Web sources for guidance on fortifying your web server against such forms of attacks.

d) Details of the impacted items:

Web Server
Details
Time difference between connections: 10015 ms

Fig. 12: Slow HTTP Denial of Service Attack, Details of the impacted items.

B. Low-risk vulnerabilities:

The scholar discovered a singular vulnerability within this particular tier:

1) Clickjacking: X-Frame-Options header missing

Classification		
CVSS	Base Score: 6.8 - Access Vector: Network - Access Complexity: Medium - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: Partial - Availability Impact: Partial	
CWE	CWE-693	
Affected items		Variation
Web Server		1

Web Server
Details
No details are available.
Request headers

```
GET / HTTP/1.1
Host: www.[redacted].edu.sd
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Fig. 13: Clickjacking: X-Frame-Options header missing, Details of the impacted items

a) Description

Clickjacking, also known as User Interface redress attack or UI redress attack, is a malevolent technique aimed at deceiving a Web user into interacting with content different from what is perceived, potentially leading to the disclosure of sensitive information or unauthorized control over their computer when interacting with seemingly harmless web pages.

The absence of an X-Frame-Options header in the server's response raises concerns regarding the vulnerability of the website to clickjacking attacks. This HTTP response header, X-Frame-Options, serves to specify whether a browser is permitted to display a webpage within a frame or iframe. Websites can utilize this header to mitigate clickjacking risks by preventing their content from being embedded in other websites.

b) Impact

The impact of this issue varies depending on the specific web application that is affected.

c) Recommendation

It is recommended to set up your web server in a way that incorporates an X-Frame-Options header. Further guidance on the potential values for this header can be sought from relevant Web sources.

VI. CONCLUSION:

The utilization of the AWVS in the present research endeavor led to the identification of multiple software vulnerabilities across different risk levels, spanning from moderate to low. Following a thorough examination of the generated report, the precise locations of the vulnerabilities in the primary site files have been precisely identified for immediate attention by the relevant authorities. Additionally, recommendations have been put forth to mitigate these vulnerabilities.

REFERENCES

[1] Wolff, J. (2018, March 23). Why University Networks Are So Tempting to Foreign Hackers. Retrieved October 07, 2018, from https://slate.com/technology/2018/03/why-foreign-hackers-target-university-networks.html.

[2] Alyami, A. (2013, April 24). The University of Nora prosecuting Hacker hacked its site two years ago. Retrieved from https://www.alarabiya.net/ar/saudi-today/2013/04/24/جامعة-نورة-تقاضي-هاكر-اخترق-موقعها-منذ-عامين.html

[3] A student who penetrates the university system and grants herself the highest grades. (2011, June 04). Retrieved from http://www.alriyadh.com/638545.

[4] Tracy, A. (2015, July 02). Harvard Got Hacked, Again. Retrieved January 17, 2019, from https://www.forbes.com/sites/abigailtracy/2015/07/02/harvard-got-hacked-again/#63dc9d17214e.

[5] Damascus University- college of Arts. (16 –march-2013). In Facebook [Fan page]. Retrieved feb 2019, from https://www.facebook.com/ArtsDaUni/photos/a.421813781191757/537823516257449/?type=1&theater.

[6] Sherif Abdullah, SM (2008). Computer security (1st ed.). Khartoum, Sudan: Sudan Open University.P6

[7] Alwi, N. (2010). E-Learning and Information Security Management. Journal of Digital Society (IJDS),1(2), 151-152. Retrieved February 13, 2019.

[8] How to Use Acunetix – A Web Vulnerability Scanner For Hackers. (2016, December 16). Retrieved February 02, 2019, from https://latesthackingnews.com

[9] Acunetix Web Vulnerability Scanner Getting Started[9]. (2018). Retrieved January 17, 2019, from https://www.acunetix.com/resources.