Security Vulnerabilities in Sudanese Universities Websites
الثغرات الأمنية في مواقع الجامعات السودانية

Prepared by

Dr .Mohammed Awad Mohammed Ataelfadiel

Computer Science Dept. Imam Mohammad Ibn Saud Islamic University, AL-Ahsa, KSA

Maataelfadiel@imamu.edu.sa

Abstract

Hackers use many ways to have unauthorized access to systems, especially those based on Internet platforms, either by manual hand-held attempts which based primarily on the hacker's experience, or by using a special tool that is either designed by the hacker himself or programmed by another professional in information security. Through these different ways, hackers try to identify vulnerabilities in software and access databases to violate their confidentiality and exploit them, or to prevent access to or destruction of the contents of the Website. The researcher has noted through his work in Nahda College the sample of the study that there are several attempts to penetrate the system of electronic examinations and electronic registration (two subsystems within the main site of the college). Therefore, the researcher has focused on finding out the existence of vulnerabilities in the basic code of the college's website; Affected by these vulnerabilities accurately. In order to achieve the research objectives, the researcher used to search for vulnerabilities by injecting some code in certain fields within the pages of the site, and since the response was positive in a number of times, has moved to the use of the Acunetix Web Vulnerability Scanner tool using the website address as a basic entry and the titles of internal links as sub-entries; after analysis of the resulting test report, it has been concluded that there are four software vulnerabilities that differed in their vulnerability between weak and medium. They have been accurately identified by identifying the affected parts, and determine the seriousness of each of them and their impact on the site. Finally, there are certain recommendations based on the results of the study.

Keywords:
Vulnerabilities; University websites; Information security; Breakthrough; Universities hacking.

1. Introduction

The idea of locking down a university network is inaccessible non-authorized. To some extent, universities do not usually design their computer systems to prioritize secrecy or security from the outside world. On the contrary, universities are intended to welcome and enable frequent collaboration, regular visitors, and informal international partnerships and communication, so it is too easy to access their websites.(Wolff, J. 2018)

Al-Nahda college is one of the newly emerging Sudanese colleges, which has started in the aspect of e-learning strongly since its inauguration; Primarily, it is unexpected that the local and international universities in the exposure of attempts to penetrate the targeted the site of electronic tests; these attempts despite repeated did not succeed but caused confusion and constant tension for those who are responsible for information security in the college.

The research problem is to determine the existence of electronic vulnerabilities in the college sites code; through which this site can be hacked and tampering with its content; and to which extent the files affected by these vulnerabilities can be accurately identified, which helps to develop appropriate solutions and avoid them by those responsible for the security of these sites to provide the required protection of data and location information before it discovers those who misuse it, because of the great risk that can lead to complete loss of control over the site.

2. Literature review

The Department of Justice in USA Arizona state announced Friday charging nine Iranians with compromising thousands of computer accounts belonging to university professors. They were affiliated with a company called the Mabna Institute, which “conducted massive, coordinated cyber intrusions” into the computer systems of 144 U.S. universities and another 176 foreign universities. .(Wolff, J. 2018)

Hackers may have many reasons to hack a university website, some of them aim at accessing databases and modifying them (such as granting degrees or modifying marks or modifying the GPA and others), including the purpose of controlling the site's powers and granting illegal powers. It’s a way to access tests or results and so on; also, what is aimed at access to non-academic aspects such as control the modification of a post and promotions and manipulation of the results of the beneficiaries ... etc. Whatever the purpose of the hackers from this attempt, many of them succeeded in carrying out their ambitions, as was the case with Princess Noura University in Saudi Arabia in 2013, where Marjouj Al-Hazazai broke through its position and

succeeded. (Alyami, A. 2013) , as did the University of Rennes II in France in 2011 Where a university student tried to penetrate the university site and modify her grades in the Masters and succeeded in that. http://www.alriyadh.com/638545

Harvard University website also has been hacked where Abigail Tracy pointed out that "For the second time within four months, Harvard University was hacked On Wednesday, the school announced that it discovered a breach in its Faculty of Arts and Sciences and Central Administration IT networks. The news of the hack—which was discovered on June 19— comes on the heels of a handful of high-profile data breaches throughout the country and just months after Harvard's Institute of Politics website was allegedly taken overby "AnonGhost," a pro-Palestinian hacker group." And she continues saying "According to the announcement from Harvard's administration, this most recent cyber attack on the school's system impacted a total of eight schools and administrative organizations." (Tracy, A. 2015)

Also, Damascus University was one of the Victims of penetration by hackers, where students found a phrase "Damascus University site has been hacked and all the results have been scanned". This sentence, which was read by most students at Damascus University when they entered to search for their results on the university's official website. The students' resentment at the delay in presenting the results on the site seems to have led them to try to draw more attention to harmful means. The reason for the hacking was due to the hacker's record: "We did not publish the results of our college because of discriminatory and we were the sons of the black duck" without mentioning the name of the college in which he is studying. It is worth mentioning that this problem is faced by students of most colleges and the problem is not limited to one college . https://www.facebook.com/ArtsDaUni/photos/a.421813781191757/537823516257449/?type=1&theater.

2.1 Vulnerabilities and threats

Vulnerability (or lack of immunization) generally defined as the sensitivity of physical or psychological harm or attack. It also means the lack of protection for valuable property and assets. In computer and network security, the expression is used to refer to vulnerabilities in systems that allow an attacker to attack them. Software malfunctions or design malfunctions also may cause vulnerabilities, as a result of the negligence of the programmer or designer. Also, using of malicious software by an attacker may cause the same result. Vulnerabilities in

computer and network security can be classified by type into two categories. (Abdullah, SM, 2008).

A) Technical vulnerabilities:

Due to weak immunization resulting from the techniques used in systems and networks, in this case the attack on the network is known as technical attack.

B) Administrative Vulnerabilities:

They are the result of non-technical reasons and the attack on the network or the computer in this case is known as the social engineering attack.

Also, terms of severity vulnerabilities can be divided into three categories:

A) High-level Vulnerabilities which are easy to exploit, such as XSS and injection vulnerabilities.

B) Medium level Vulnerabilities, and their types are too many.

C) Low level Vulnerabilities: This type of Vulnerabilities is difficult to exploit and requires a lot of effort, resources and experience by the attacker.

2.2. Internet Information Threats

People have recently acquired many benefits and information through the Internet much faster and easier than before; this information is in many forms such as databases, research papers, e-mail and others. Regardless of how such information exists on the Internet or where it is stored electronically, it should be adequately protected. (Alwi, N. 2010).

The information used and derived from useful data is considered to be an important asset in any organization, while enhancing the accessibility of such data and information will be useful to anyone who is in his or her hand, regardless of good or bad faith for that person; and as a result of this increase in people who can access this information there is greatly increased in the number and type of attacks, as many new vulnerabilities appear every day, so this information must be protected to avoid loss and ensure confidentiality and integrity.

3. Applied Study

The researcher starts the applied study by using the Acunetix web vulnerability scanner which is one of the famous web vulnerability scanners out there. It can be used to perform penetration testing against the detected issues and also during the scanning process, it can analyze the source code and pinpoint the exact line of code that has the vulnerability in it.

https://latesthackingnews.com The Applied study was carried out in several steps as follows:

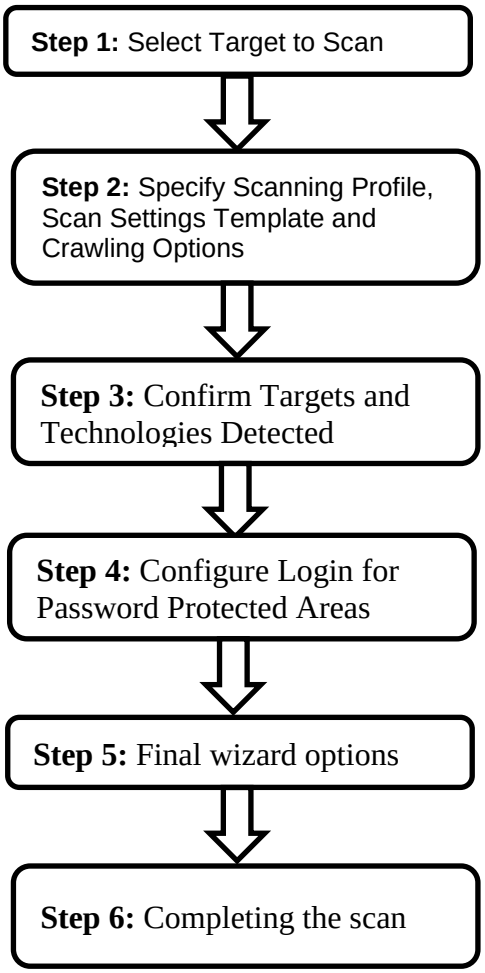

Figure 1: Acunetix Web Vulnerability Scanner scanning steps . https://www.acunetix.com/resources

3.1. Select Target to Scan

Here the researcher specifies the website to be scanned, and for the research needs the researcher use the website address of Al-Nahda College www.nahda.edu.sd/

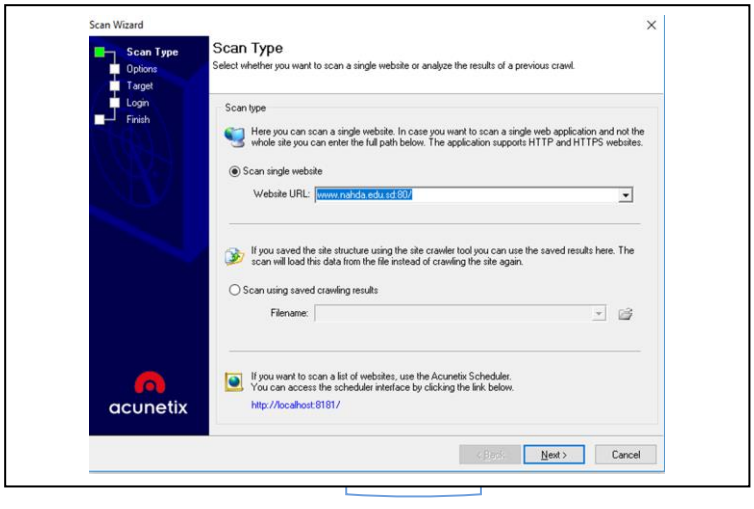

Figure2: Step (1): Select Target to Scan

3.2. Specify Scanning Profile, Scan Settings, template and Crawling

Here the scanner asks to select a scanning profile (e.g. SQL Injection or XSS) to be used when scanning the target website. A scanning profile defines which vulnerability checks will be launched against the website. For the research purposes the "default scanning profile" choice is chosen to test the website for all known web vulnerabilities.

Also, at this step the tool asks to choose scan settings, which used to determine what Crawler (HTTP protocol, advanced crawling) and scanner settings to be used during a scan. For the research purposes the researcher let this choice as default.

Finally, the Crawling Options is used to manually select which files and directories should be scanned after the crawl, also select to have the crawler process URLs which might not be linked from the main URL by using the Define list of URLs to be processed by crawler at start option.

3.3. Confirm Targets and Technologies Detected

In the 3rd step Acunetix WVS automatically fingerprint the target website for basic details. The web vulnerability scanner will optimize and reduce the scan time for

the selected

technologies by reducing the number of tests performed.

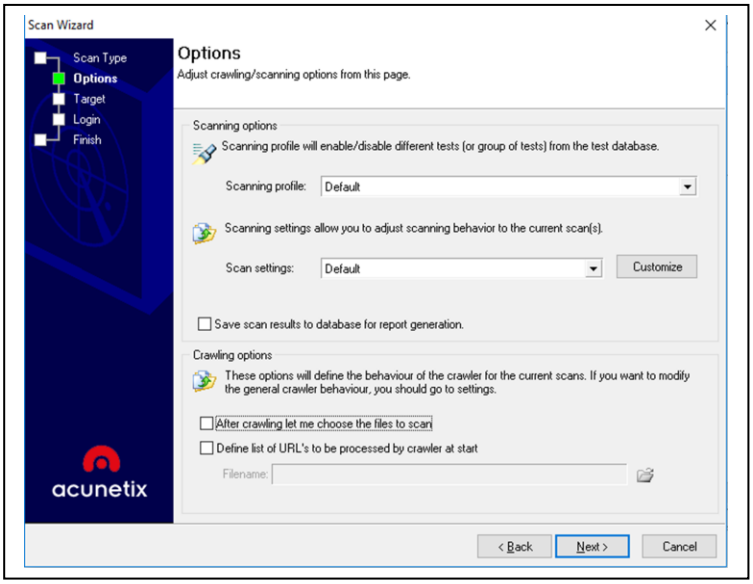

Figure3: Step (2): Specify Scanning Profile, Scan Settings Template and Crawling

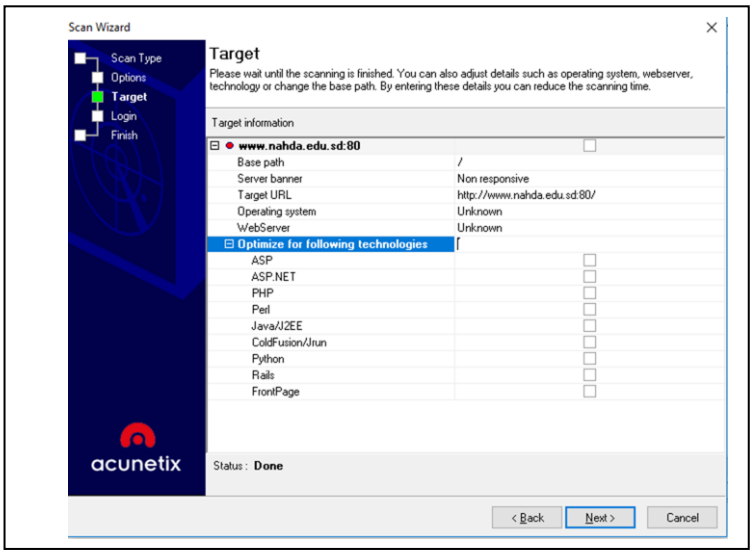

Figure4: Step (3): Confirm Targets and Technologies Detected

3.4. Configure Login for Password Protected

There are 2 common types of Authentication mechanisms used authenticate.

- HTTP Authentication - This type of authentication is handled by the web server, where the user is prompted with a password dialog.

- Forms Authentication - This type of authentication is handled via a web form. The credentials are sent to the server for validation by a custom script.

For the research purposes, the researcher chooses to let this choice as default (no login sequence).

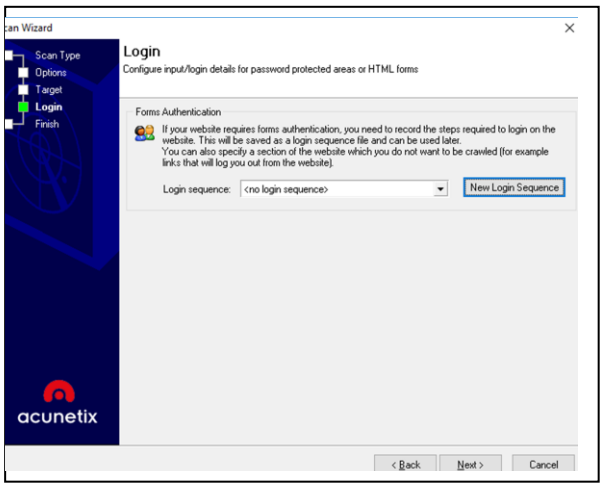

Figure5: Step (4): Configure Login for Password Protected

3.5. Final wizard options

The semi-final step is making an initial analysis of the website and it might alert the user to some issues e.g. error is encountered while connecting to the target server, If Acunetix WVS is unable to automatically detect a pattern for the custom 404 error page automatically…etc.

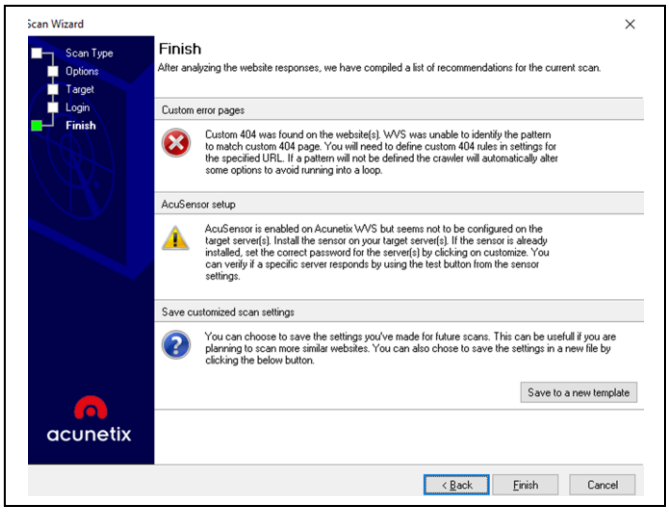

Figure6: Step (5): Final wizard options

3.6. Completing the scan

Depending on the size of the website, scanning profile chosen and the server response time, a scan may take up to several hours. For the current research scan time was 35 mins' and 57 sec.

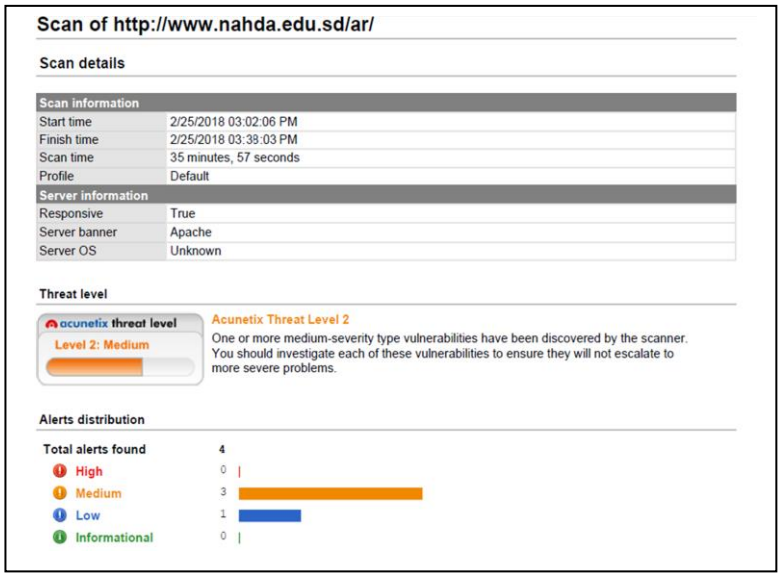

Figure7: Step (6): Completing the scan

4. Results

After completing all stages of the applied research study, the researcher found that there were four vulnerabilities threats in the code of the college website under study, which was HTML form without CSRF protection vulnerability and Slow HTTP Denial of Service Attack vulnerability which are classified as medium vulnerabilities, and Clickjacking: X-Frame-Options header missing vulnerability which classified as low vulnerability. Through these vulnerabilities the system could be hacked and controlled.

5. Results discussion

5.1 Medium-risk vulnerabilities

The researcher has found three vulnerabilities of this level:

5.1.1 **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**

Table1: HTML form without CSRF protection vulnerabilities Classification

5.1.1.1 Description

Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found an HTML form with no apparent CSRF protection implemented.

5.1.1.2 Impact

An attacker may force the users of a web application to execute actions of the attacker's choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

5.1.1.3 Recommendation

Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.

5.1.1.4 Affected items details

/ar

Details

Form name: <empty>
Form action: http://www.nahda.edu.sd/ar/
Form method: POST

Form inputs:

- g-recaptcha-response [TextArea]
- submit [Submit]

Request headers

```
GET /ar/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Host: www.nahda.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: */*
```

Figure 8: HTML form without CSRF protection affected item (1) details

/ar

Details

Form name: <empty>
Form action: http://www.nahda.edu.sd/ar/
Form method: POST

Form inputs:

- submit [Submit]

Request headers

```
GET /ar/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Host: www.nahda.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: */*
```

Figure 9: HTML form without CSRF protection affected item (2) details

5.1.2 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**

Table2: Slow HTTP Denial of Service Attack vulnerability Classification

5.1.2.1 Description

Slowloris and Slow HTTP POST DoS attacks rely on the fact that the HTTP protocol, by design, requires requests to be completely received by the server before they are processed. If an HTTP request is not complete, or if the transfer rate is very low, the server keeps its resources busy waiting for the rest of the data. If the server keeps too many resources busy, this creates a denial of service.

5.1.2.2 Impact

A single machine can take down another machine's web server with minimal bandwidth and side effects on unrelated services and ports.

5.1.2.3 Recommendation

Consult Web references for information about protecting your web server against this type of attack.

5.1.2.4 Affected items details

Web Server
Details
Time difference between connections: 10015 ms

Figure 10: Slow HTTP Denial of Service Attack affected item details

5.2 Low-risk vulnerabilities:

The researcher found one vulnerability at this level:

5.2.1 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**

Table3: Clickjacking: X-Frame-Options header missing vulnerability Classification

5.2.1.1 Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an X-Frame-Options header which means that this website could be at risk of a click jacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid click jacking attacks, by ensuring that their content is not embedded into other sites.

5.2.1.2 Impact

The impact depends on the affected web application.

5.2.1.3 Recommendation

Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.

5.2.1.4 Affected items details

Web Server
Details
No details are available.
Request headers

```
GET / HTTP/1.1
Host: www.nahda.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: */*
```

Figure 11: Clickjacking: X-Frame-Options header missing affected item details

6. Conclusion:

Through the current applied study, the Acunetix web vulnerability scanner, a number of software vulnerability are found at varying levels of risk ranging from the average to the weak. After a comprehensive analysis of the resulting report the places of the infection in the main site files have been accurately identified so that it can be addressed by the responsible authorities. Also, recommendations proposed to avoid these vulnerabilities.

Recommendations:

Check if the HTML form shown in figure 5.1.1 requires CSRF protection and implement CSRF countermeasures if necessary; Then consult web references for information about protecting your web server against “Slow HTTP Denial of Service” Attack; Finally configure your web server to include an X-Frame-Options header.

7. References

1. 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
2. Alwi, N. (2010). ***E-Learning and Information Security Management***. Journal of Digital Society (IJDS),1(2), 151-152. Retrieved February 13, 2019.
3. Sherif Abdullah, SM (2008). **Computer security** (1st ed.). Khartoum, Sudan: Sudan Open University .P6
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. 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.
6. Acunetix Web Vulnerability Scanner Getting Started [9]. (2018). Retrieved January 17, 2019, from https://www.acunetix.com/resources.
7. How to Use Acunetix – A Web Vulnerability Scanner for Hackers. (2016, December 16). Retrieved February 02, 2019, from https://latesthackingnews.com
8. A student who penetrates the university system and grants herself the highest grades. (2011, June 04). Retrieved from http://www.alriyadh.com/638545.
9. 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.