Ilkogretim Online - Elementary Education Online, 2020; Vol 19 (Issue 4): pp. 4765-4775
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2020.04.764882

Investigation A Web Application And Detecting Vulnerabilities Using Machine Learning

Majeda Sultana
M. Tech. Scholar
School of Engineering and I.T., MATS University, Raipur
Dr. Abhishek Badholia
Associate Professor
School of Engineering and I.T., MATS University, Raipur

Abstract: This is a report concerning Security flaws in web applications, seem to be problematic for a variety of purposes. A firm's branding as well as prestige may be harmed as a result of a significant compromise. Standards like GDPR have considerably upped the stakes in terms of financial fines and data leakage notifications in an era when confidentiality is more crucial than ever. The danger scenario has altered in tandem with the evolution of the internet. On the user end, the internet browser has evolved into a sophisticated environment that could be exploited to breach users' privacy, steal their money, or even mine cryptocurrencies using their CPU. As a result, intruders will have a wider range of targets to compromise. This is especially true given the ineffectiveness of standard network-layer security defences like firewalls and intrusion detection systems (IDS) un identifying and blocking web app assaults. The goal of this article is to provide you an overview of the most prevalent web application and network perimeter vulnerability. Moreover, as a harbinger of where online vulnerability security will be in the coming years.

Keywords: Vulnerabilities, security, intrusion detection, web services, cryptography, database.

I. INTRODUCTION

The findings of autonomous website applications and networks peripheral vulnerability scanning conducted from a digital, SaaS, cloud-based internet and security protocols scanners were used to compile and analysis the information for this research. This information was gathered over a twelve month period from 10,000 scanning points that were chosen randomly. The objectives of this research work do not include evaluative scanning on the purposely misconfigured Acunetix testing web apps.

The Anatomy of an Automated Web Scan:- Black box or Dynamic Application Security Testing (DAST) scanning make up the majority of Online's automatic web app scanning. This implies the web scanner has no idea what the back-end coding on the webpage or web app it's about to scan is like. Using embedded sensors, Online can also conduct grey box or Interactive Applications Security Testing (IAST) scans. This is a server-side sensor which could be used with Java, ASP.NET, and PHP web apps. Detector combines the greatest aspects of dynamically analysis by transmitting input from detectors inside the source code as it is being executed. In several businesses, automatic web app protection assessment and vulnerabilities handling procedures following 4 key steps. Each one is described in detail here.

Crawling and Scanning: - Crawling a webpage or online apps is the initial step in inspecting it. By scanning for connections and entries and executing Js as a genuine browsers, crawlers examines the architecture of a web app. HTML5 and ES6 and 7 technology are supported by the crawlers. In contrast to the standard GET and POST arguments, it can identify frequently utilised JSON & XML inputting methods, and more unusual inputting mechanisms include GWT. Because the scanners cannot analyze a website for vulnerability unless it is aware of its existence, an accurate crawl is critical for a scan to have excellent coverage throughout. After finishing a crawl, it checks each webpage it discovers for myriad of cybersecurity breaches.

Reporting: - The next stage is to analyse the facts discovered by the scanners after the scan has returned specific conclusions. The findings are presented in real time on the Dashboards, and you may begin engaging on these even before the scanning is completed. Scanning findings may also be transferred to a variety of management and regulatory reporting, such as PCI DSS, OWASP Top 10, HIPAA, ISO 27001, as well as other standards.

Remediation: - Appropriate scanning findings are useless until and unless the vulnerability are addressed. It also offers out-of-the-box vulnerability handling techniques and connections with issue trackers like Atlassian, JIRA, and GitHub, in addition to extensive details regarding identified weaknesses. By setting standard Web App Firewalls, it may practically fix weaknesses. Jenkins and other Continuous Integration (CI) and Continuous Deployment (CD) systems connect seamlessly. Finally, it enables Continous Diagnostics, which involves conducting a short check each day in contrast towards more thorough scan once a week to guarantee that any vulnerability are quickly remedied.
The information in this analysis comes from web platform's automatic web and network perimeter checks. This study's research is mostly focused on large and mid-intensity vulnerabilities, and also perimeter networks vulnerabilities information.

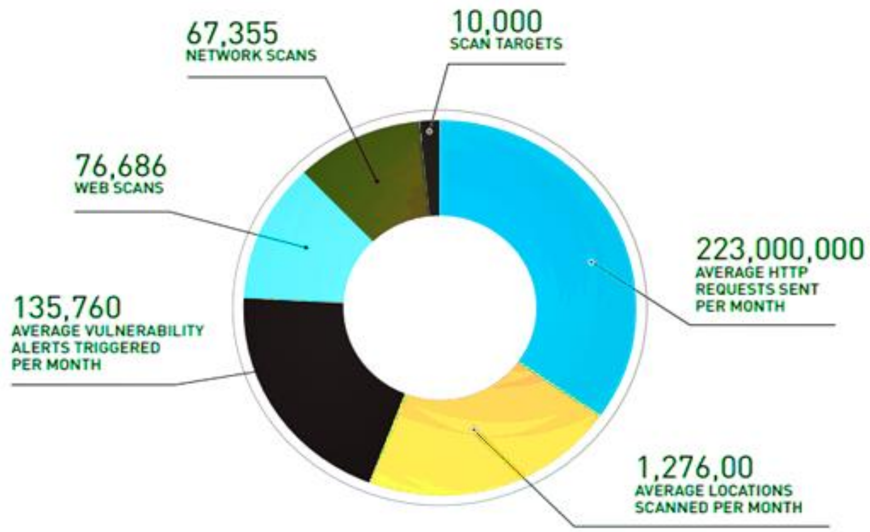


Figure1:- The Dataset Analysis

Case Study:

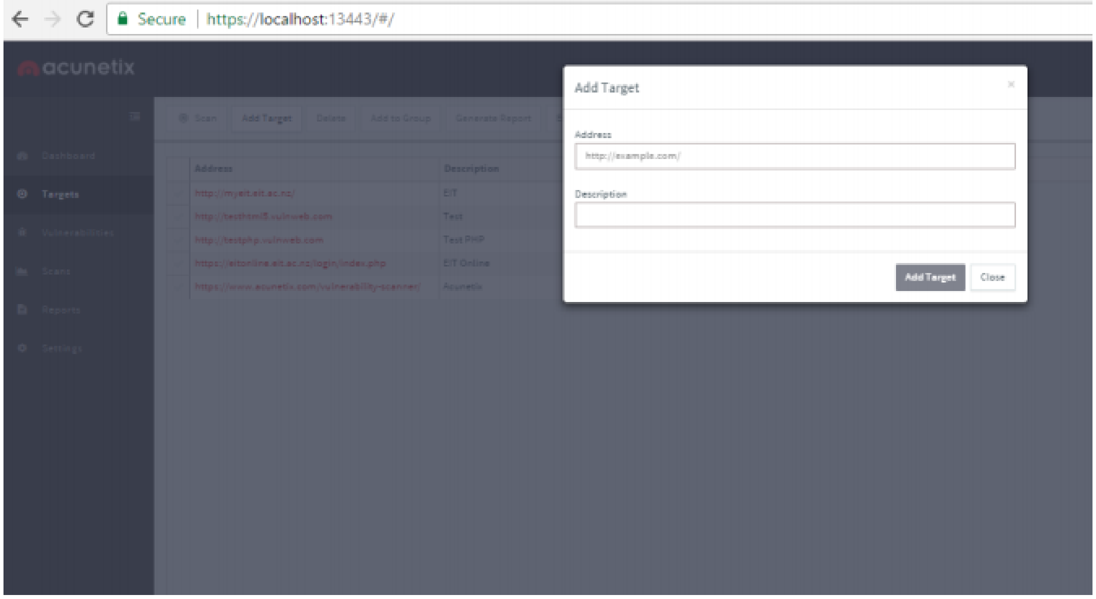
Acunetix: It's a web vulnerabilities analyzer that examines any online app or webpage which uses the HTTP or Network protocol and can be accessed via a web browser. It checks webpages for weaknesses like SQL injection and cross-site scripting, among others. The versions, pricing, and other information of Acunetix utilised in this work are listed in the table below (Table 1). The majority of the webpages included in the tour are test webpages rather than institutional webpages. Acunetix comes in four different flavours: online, standard, pro, & enterprises.

Table 1: Version and platform of Acunetix used

Version	Acunetix 11 Trial
Platform	Windows 8
Cost	Free

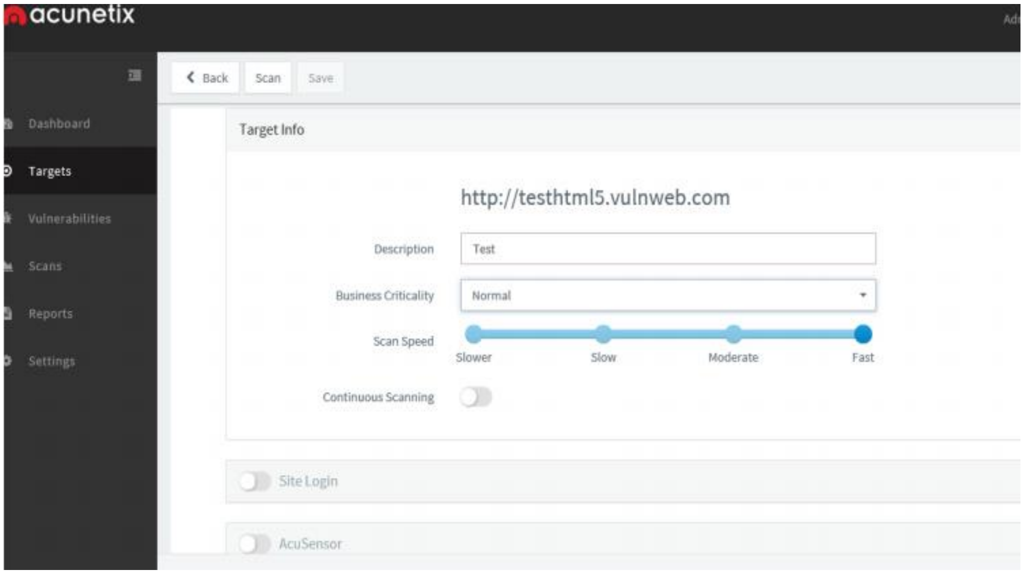
Trial period	14 days trial
Test websites	http://testasp.vulnweb.com http://testhtml5.vulnweb.com http://testphp.vulnweb.com

The objective may include the url of a webpage or online app which wants to be examined When adding the target, you may also include a descriptions of the webpage. A snapshot of adding a target with a statement is shown in Figure 2.



Address	Description
http://myeit.eit.ac.nz/	EIT
http://testhtml5.vulnweb.com	Test
http://testphp.vulnweb.com	Test PHP
https://eitonline.eit.ac.nz/login/index.php	EIT Online
https://www.acunetix.com/vulnerability-scanner/	Acunetix

Figure 2:- Screenshot of adding target.



http://testhtml5.vulnweb.com

Description: Test

Business Criticality: Normal

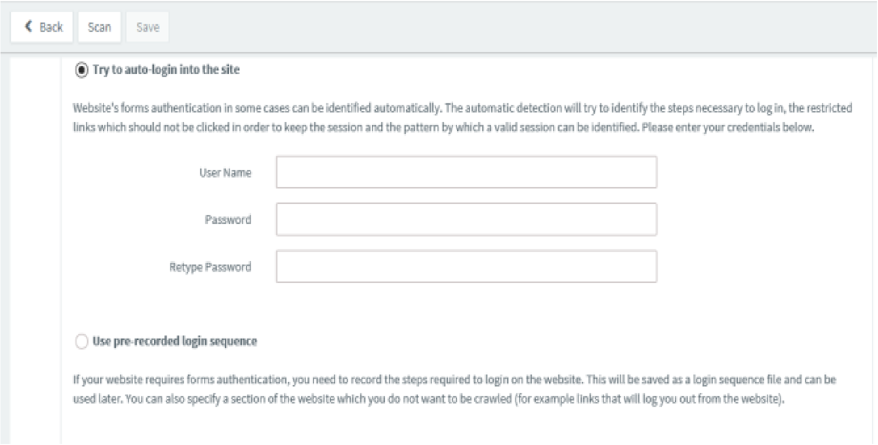
Scan Speed: Fast

Continuous Scanning

Figure 3:- Screenshot of setting target information

The webpage is now available for checking once you've added the objective. Alternatives for establishing the organization criticality scan speed and other parameters are provided, as shown in Figure 3. Continuously checking may be done with webpages as well as online apps.

Acunetix has a function that attempts to autologin to the specified website, as illustrated in Figure 4. There are two options for implementing this functionality. The testers have the option of individually entering the login credentials or using a pre-recorded authentication procedure for automatic login.



● Try to auto-login into the site

Website's forms authentication in some cases can be identified automatically. The automatic detection will try to identify the steps necessary to log in, the restricted links which should not be clicked in order to keep the session and the pattern by which a valid session can be identified. Please enter your credentials below.

User Name

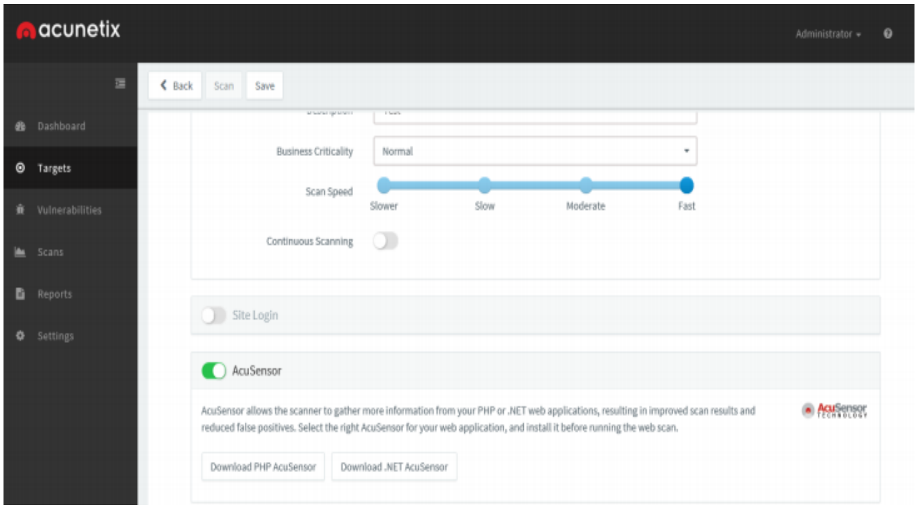
Password

Retype Password

○ Use pre-recorded login sequence

If your website requires forms authentication, you need to record the steps required to login on the website. This will be saved as a login sequence file and can be used later. You can also specify a section of the website which you do not want to be crawled (for example links that will log you out from the website).

Figure 4:- Setting auto login option.



Business Criticality: Normal

Scan Speed: Slower Slow Moderate Fast

Continuous Scanning

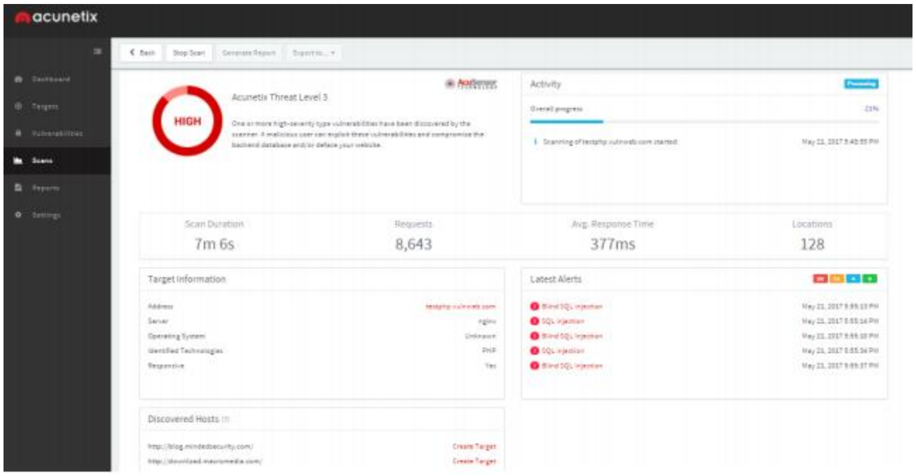
Site Login

AcuSensor

AcuSensor allows the scanner to gather more information from your PHP or .NET web applications, resulting in improved scan results and reduced false positives. Select the right AcuSensor for your web application, and install it before running the web scan.

Figure 5:- Enabling Acu-Sensor

The scanner findings could be enhanced through obtaining & applying the appropriate Acu-Sensor when the intended website uses PHP or.NET. Acu-Sensor is enabled in Diagram given above. Acunetix offers statistics upon that targeted and scan status, length, numbers of request issued, and avg responses rate throughout checking. It also lists the most recent vulnerability discovered, as well as their priority. Acunetix assigns a danger rating to a webpage relying upon on vulnerability found. A snapshot of Acunetix conducting a scans is shown in Figure 6.



Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Overall progress 21%

Scanning of testphp.vulnweb.com started

Scan Duration	Requests	Avg. Response Time	Locations
7m 6s	8,643	377ms	128

Target Information

Address	testphp.vulnweb.com
Server	nginx
Operating System	Unknown
Identified Technologies	PHP
Responsive	Yes

Latest Alerts

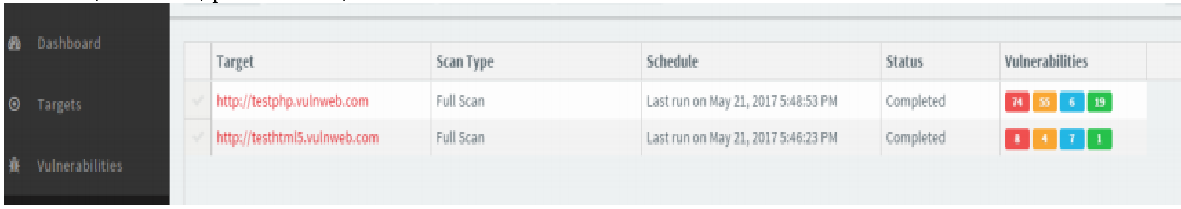
- Blind SQL injection
- SQL injection
- Blind SQL injection
- SQL injection
- Blind SQL injection

Discovered Hosts

http://blog.mindedsecurity.com/	Create Target
http://download.macromedia.com/	Create Target

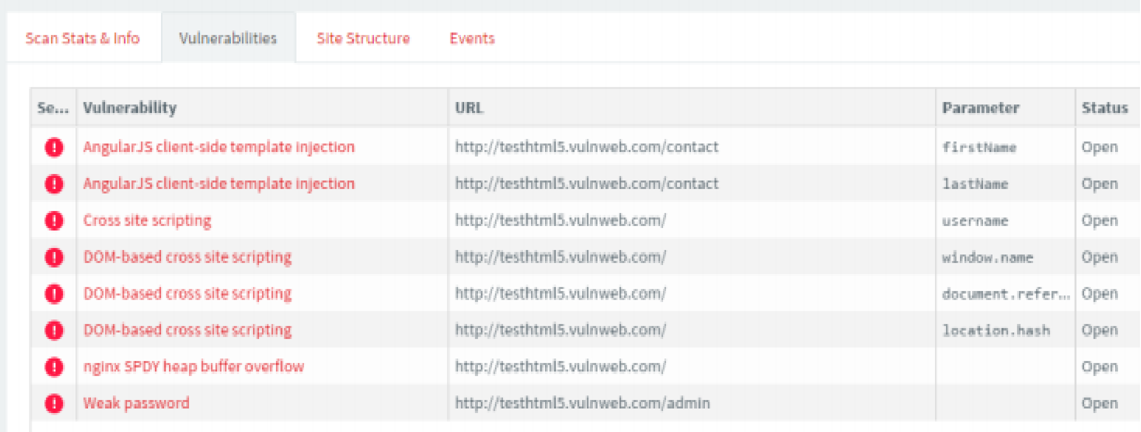
Figure 6:- Scanning website

After the checking is complete, Acunetix generates a list of the vulnerability discovered sorted by severity. The title, Address, parameters, and condition of the risk discovered are all listed.



Target	Scan Type	Schedule	Status	Vulnerabilities
http://testphp.vulnweb.com	Full Scan	Last run on May 21, 2017 5:48:53 PM	Completed	74 55 6 19
http://testhtml5.vulnweb.com	Full Scan	Last run on May 21, 2017 5:46:23 PM	Completed	8 4 7 1

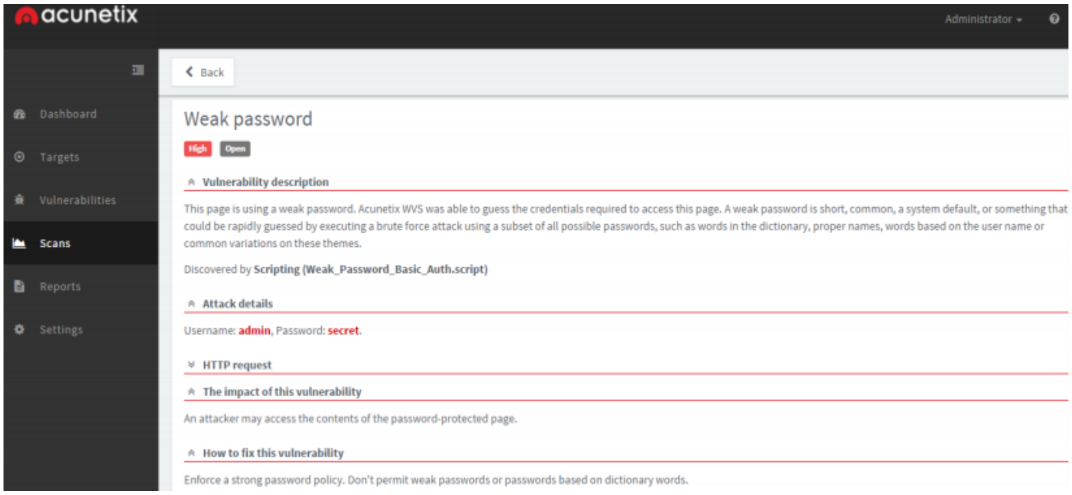
Figure 7:- Scan result



Se...	Vulnerability	URL	Parameter	Status
!	AngularJS client-side template injection	http://testhtml5.vulnweb.com/contact	firstName	Open
!	AngularJS client-side template injection	http://testhtml5.vulnweb.com/contact	lastName	Open
!	Cross site scripting	http://testhtml5.vulnweb.com/	username	Open
!	DOM-based cross site scripting	http://testhtml5.vulnweb.com/	window.name	Open
!	DOM-based cross site scripting	http://testhtml5.vulnweb.com/	document.refer...	Open
!	DOM-based cross site scripting	http://testhtml5.vulnweb.com/	location.hash	Open
!	nginx SPDY heap buffer overflow	http://testhtml5.vulnweb.com/		Open
!	Weak password	http://testhtml5.vulnweb.com/admin		Open

Figure 8:- Vulnerabilities identified during the scan

All vulnerabilities found has a detailed explanation, an effect, and helpful recommendations for resolving the issue. This also includes the HTTP request that was sent, that may be used to assist patch &analyze that specific vulnerability. The descriptions and consequences of the vulnerabilities "poor passcode" are shown in Figure 9.



Weak password

Vulnerability description

This page is using a weak password. Acunetix WVS was able to guess the credentials required to access this page. A weak password is short, common, a system default, or something that could be rapidly guessed by executing a brute force attack using a subset of all possible passwords, such as words in the dictionary, proper names, words based on the user name or common variations on these themes.

Discovered by Scripting (Weak_Password_Basic_Auth.script)

Attack details

Username: admin, Password: secret.

HTTP request

The impact of this vulnerability

An attacker may access the contents of the password-protected page.

How to fix this vulnerability

Enforce a strong password policy. Don't permit weak passwords or passwords based on dictionary words.

Figure 9:- Vulnerability description

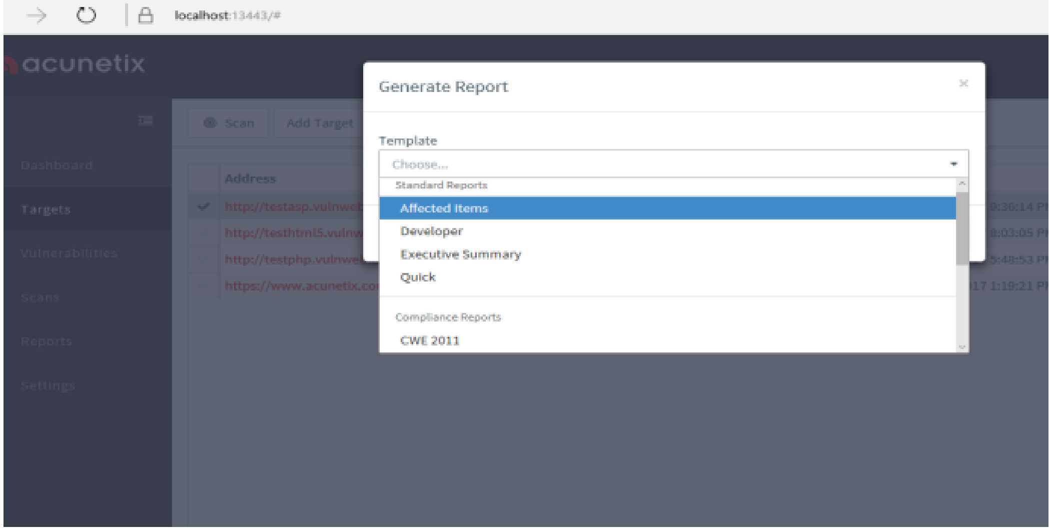
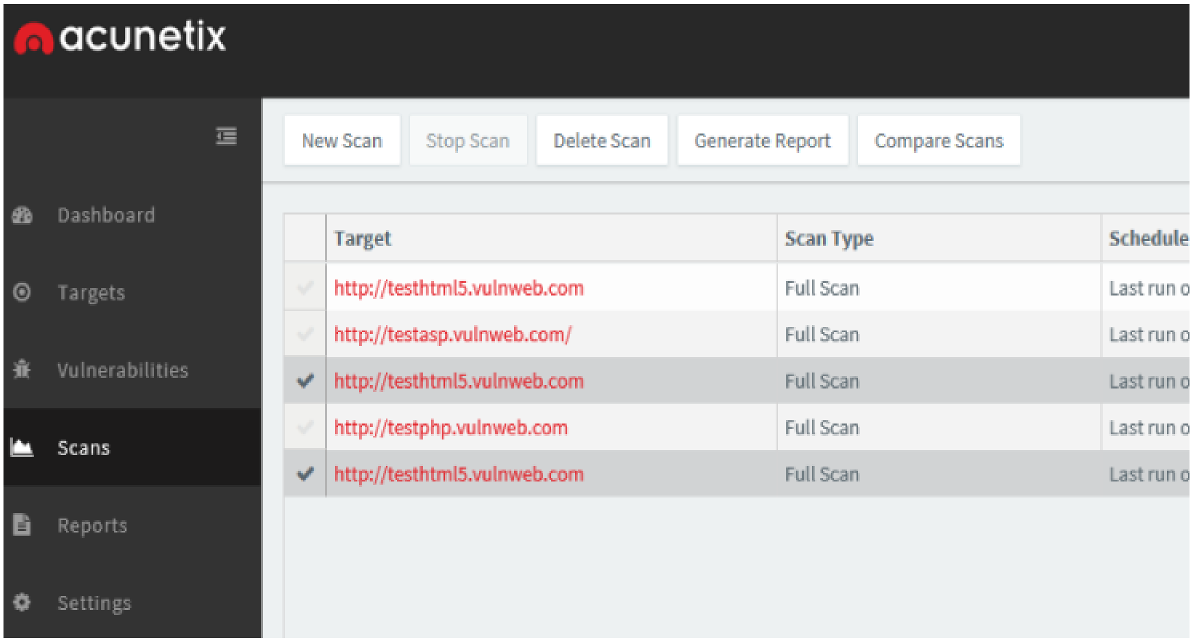


Figure 10:- Selecting report template

Relying upon on scan findings, scanning reports can be created. Statistics may be created in a variety of formats, including impacted items, programmer, summary, and numerous compliance statistics. All created statistics would be accessible via the findings page and may be retrieved at a later time. The choices for producing findings are shown in Figure 10.

Acunetix could evaluate various scan results for one specific target and provide a comparative result. It can be useful in determining yet if the risk remedies are operating properly and if the solutions do not introduce new vulnerability. Figure 11 demonstrates that when two scanning on the same objective are selected, the "compare scans" option is activated.



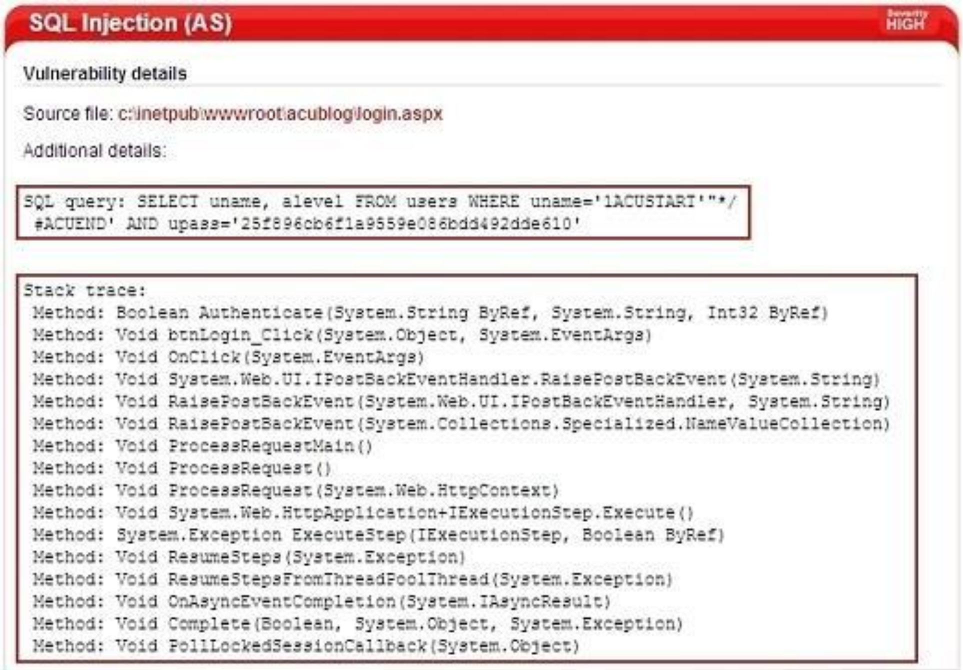
	Target	Scan Type	Schedule
	http://testhtml5.vulnweb.com	Full Scan	Last run o
	http://testasp.vulnweb.com/	Full Scan	Last run o
✓	http://testhtml5.vulnweb.com	Full Scan	Last run o
	http://testphp.vulnweb.com	Full Scan	Last run o
✓	http://testhtml5.vulnweb.com	Full Scan	Last run o

Figure 11:- Screenshot of comparing scan results

Vulnerabilities: - Cross-site scripting (XSS), SQL injection, Blind SQL injection, and directories traversal are just a few of the high-priority security flaws found by Acunetix. XSS involves injecting suspicious coding into the victim's website such that the dangerous scripts code is performed whenever the victim accesses the web app [10]. A attacker infuses malware into evolving online sites which alters the websites whenever the script is launched inside the browser [10]. An XSS attack attempts to gain entrance to the customer tokens or even other confidential material required to validate the user towards the webpage [10]. Clients' workstations submit HTTP requests to websites, with fields containing details of respective platforms &os versions. Visitors might be routed to the smartphone edition of the webpage premised upon that data which, together with specific composition, must have various vulnerability. This has a lot of ramifications when it comes to detecting XSS problems. As a result, Acunetix tries to crawl several versions of each page using various user agents. A SQL injection weakness may expose any confidential material in a website databases, containing usernames, passwords, and credit card information [12]. By utilising specific attributes and putting those into the programme, the SQL offender began to integrate a portion of dangerous SQL instructions. The website then transmits those suspicious instructions to the database system on the webserver, which performs it by using valid request for a different reason [1]. In addition to gain access to the susceptible code, a blind SQL injection requires requesting the databases a sequence of true or false statements. It's worth noting that simply discovering susceptible programs isn't enough for attackers. Phishing is also frequently used to gain extended user information [6]. These data could then be utilised in a SQL attack to retrieve unauthorised data from a database online. Directory traversing (formerly abbreviated as location traversing) is an exploit which tries to "obtain files and folders located out of the website root directory" [14]. This vulnerabilities can be found inside the program of the remote server or perhaps the script of the web app. This gives the hacker accessibility to protected folders and the ability to run instructions upon this remote server.

Technologies: - Acunetix achieves superior diagnostic findings by utilising technology such as Acu-Senor and Acu-Monitor. AcunetixAcu-Sensor Solution is a protection technique which enables for better exploiting vulnerabilities while reducing false positives. It also gives diagnostic data as well as indicating the specific place of the source where vulnerabilities are found. To attain greater precision, this method integrates black box scanning methods with response through embedded sensors within the program code. The Acu-Sensor technology discovered SQL injection (Figure 12) and PHP vulnerability (Figure 13) as can be seen in pictures below. It shows the stack trace of a SQL injection risk as well as the file name including line numbers for such

PHP malicious codes, allowing programmers to quickly identify and address problems. It could also assist programmers in better understanding weaknesses, allowing them to create more secured programmes.



SQL Injection (AS)

Vulnerability details

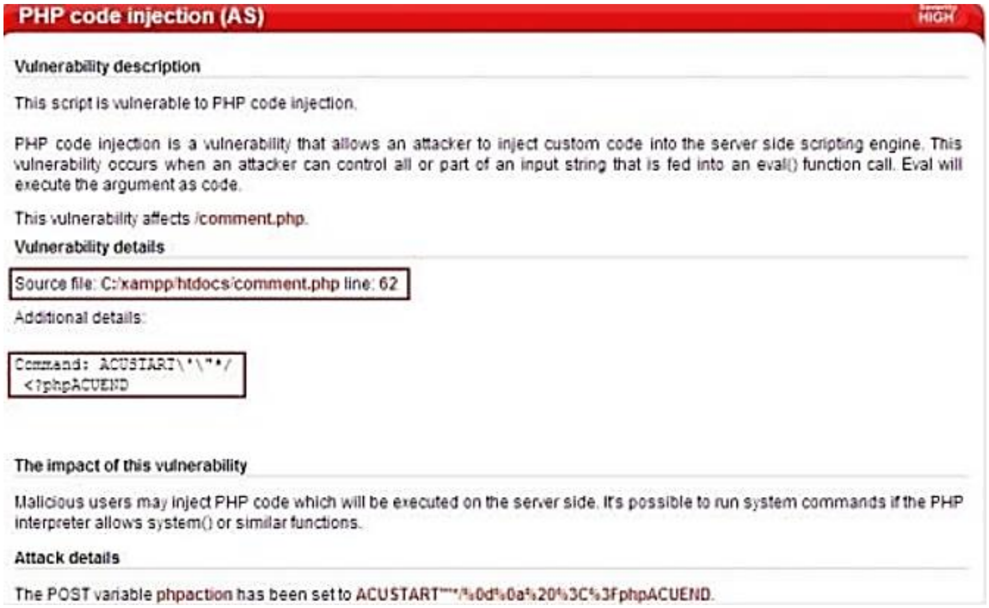
Source file: c:\inetpub\wwwroot\acublog\login.aspx

Additional details:

```
SQL query: SELECT uname, alevel FROM users WHERE uname='1ACUSTART'"*/
 #ACUEND' AND upass='25f896cb6f1a9559e086bdd492dde610'
```

```
Stack trace:
 Method: Boolean Authenticate(System.String ByRef, System.String, Int32 ByRef)
 Method: Void btnLogin_Click(System.Object, System.EventArgs)
 Method: Void OnClick(System.EventArgs)
 Method: Void System.Web.UI.IPostBackEventHandler.RaisePostBackEvent(System.String)
 Method: Void RaisePostBackEvent(System.Web.UI.IPostBackEventHandler, System.String)
 Method: Void RaisePostBackEvent(System.Collections.Specialized.NameValueCollection)
 Method: Void ProcessRequestMain()
 Method: Void ProcessRequest()
 Method: Void ProcessRequest(System.Web.HttpContext)
 Method: Void System.Web.HttpApplication+IExecutionStep.Execute()
 Method: System.Exception ExecuteStep(IExecutionStep, Boolean ByRef)
 Method: Void ResumeSteps(System.Exception)
 Method: Void ResumeStepsFromThreadPoolThread(System.Exception)
 Method: Void OnAsyncEventCompletion(System.IAsyncResult)
 Method: Void Complete(Boolean, System.Object, System.Exception)
 Method: Void PollLockedSessionCallback(System.Object)
```

Figure 12:- SQL Injection Reported by Acu-Sensor Technology



PHP code injection (AS)

Vulnerability description

This script is vulnerable to PHP code injection.

PHP code injection is a vulnerability that allows an attacker to inject custom code into the server side scripting engine. This vulnerability occurs when an attacker can control all or part of an input string that is fed into an eval() function call. Eval will execute the argument as code.

This vulnerability affects /comment.php.

Vulnerability details

Source file: C:/xampp/htdocs/comment.php line: 62

Additional details:

```
Command: ACUSTART\'\"*/
 <?phpACUEND
```

The impact of this vulnerability

Malicious users may inject PHP code which will be executed on the server side. It's possible to run system commands if the PHP interpreter allows system() or similar functions.

Attack details

The POST variable phpaction has been set to ACUSTART'"*/%0d%0a%20%3C%3FphpACUEND.

Figure 13:- PHP Code Injection Reported by Acu-Sensor Technology

Acu-Monitor Technologies is also another Acunetix tool. Generally, during evaluating web apps, the scanners makes a query to a target, gets a reaction, examines it, and then triggers a warning depending upon its inspection. Certain flaws were n't detected when using "request/response" testing methodology because they do not respond to a scanner while analysis (out-of-band vulnerabilities evaluation). The detection of these flaws necessitates the use of an intermediate services which a scanners may use. Acunetix, in conjunction with Acu-Monitor, automates the identification of certain flaws.

Discussion:

Acunetix enables for several inspections to be performed at the same time, although this may lengthen the scanning process. The length of time it takes to scan a certain webpage or web applications is determined by the target website's technology and complexity. Acunetix also lets you to scan for security flaws, such as XSS, which you may specify before initiating the scan. This is a benefit since it is considerably faster than a comprehensive scan and may allow programmers to focus on a specific weakness and solve it. Another useful function is report generating, which allows you to reuse the scan findings. Numerous sources enable you to obtain findings depending on your unique requirements. Despite the fact that Acunetix minimises false positives, scanning results still may include them. Programmer must double-check the scanning findings to ensure that they aren't false positives, which might take a long time. Scanning results might have been improved with fewer false positives if Acunetix included a tool to individually identify erroneous positives and exclude them from subsequent scanning results. During analyzing, Websites Vulnerability Scanners (WVS) introduce trash values into the databases [14]. WVS performs automatic inspection and various actions on a databases in order to detect SQL injections as well as other database-related risks. Hundreds of HTTP requests are sent to the remote server by an automatic vulnerabilities tester. Vulnerability testers frequently make these queries via many concurrent channels in effort to speed up their evaluation. If a server is unable to handle all the queries, this could slow it down and cause a denial of service [5]. Deep inspection is possible with automatic WVS. This happens when a WVS tries to access all of the website's routes and connections. When scanning into confidential URLs, this can be a problem. Crawling sensitive URLs, such as delete, might result in the destruction of vital data [5]. Several webpages, for instance, include a "contact us" option that allows users to send emails. Numerous messages could be forwarded to a single recipient during analyzing such webpages, which is known as a massive emailing attack or email bombing [5]. The challenges mentioned previously have a limited range of suggestions. Rather than evaluating in a manufacturing environment, staging environments may hopefully minimize denial-of-service issues inside the release atmosphere [5]. This also prevents trash values from being inserted into the manufacturing databases. In a production setting, DoS can be mitigated. The use of CAPTCHAs in message forms may assist to avoid message overloading. A WVS such as Acunetix also enables you to prevent vulnerable URLs from becoming crawled [5].

Mobile Device Aspects

In regarding web protection, mobile devices continuing to face certain hazards to consumers. These systems actually deal with a variety of communication links, credentials that have been stored or retained, and personal memos and messages. Because these pieces of information are kept on smart phones, these could be vulnerable to theft via online browser. The educational industry has the greatest and fastest-growing number of smartphone users. Educators, staff, and learners depend upon their websites and internet teaching materials all of the time, and they are regularly attacked by hackers [13]. More than ever, clients of academic information management must be vigilant and well-versed on security issues. Institutions' IT support must improve their protection capabilities and implement innovative protection procedures. Experts and programmers of educative apps must also consider smartphone and online protection issues by considering cybersecurity a significant necessity and development factor [7].

Conclusions:-

Website Vulnerability Scanners (WVS) aid in the speeding up of the vulnerabilities assessment procedure for websites and web applications. Acunetix is a famous automatic weakness analyzer that not only detects flaws but often provides recommendations for how to fix them. Acu-Sensor technology additionally concentrates on decreasing false positive reports for webpages built using PHP and.NET technologies. Acunetix might become much more precise in the long term by incorporating new behavioural analytic tools. Numerous programmers find that using Acunetix or a comparable WVS is highly beneficial because it enables detecting risks simpler among security newbies. Using a trial version can assist you in determining how long you want to pay for the premium membership in the future. Users may pick an appropriate subscription choice based on their needs thanks to the many options. WVS may be used by website and application developers during development and testing to guarantee that a web application is extremely secure before it is deployed into the production environment. This case study, which uses Acunetix as an example, is useful for familiarising students with the fundamentals of a WVS. Some security systems are focused at analysing company websites, while others are oriented toward controlling the company's mobile devices. Scanning mobile devices for security vulnerabilities and highlighting unsafe apps is beneficial for both app makers and IT support [15]. More technical research might be done to evaluate different vulnerability scanners, their efficacy, and their unique capabilities, which would aid developers in selecting the best WVS for each online application.

References:

[1] Abdulqader, F. B., Thiyab, R. M., & Ali, A. M. (2017). The impact of SQL injection attacks on the security of databases. In Proceedings of the 6th International Conference on Computing and Informatics (pp. 323-331).

[2] Tarun Dhar Diwan, Dr. Siddhartha Choubey, Dr.H.S.Hota, “A Detailed Analysis on NSL-KDD Dataset using various Machine Learning Techniques for Intrusion Detection” published in International Journal of Turkish Journal of Computer and Mathematics Education Vol.12 No. 11 (2021), pp.2954- 2968 ISSN: 1309-4653.

[3] Acunetix - Website security - keep in check with Acunetix. (n.d.). Retrieved from https://www.acunetix.com

[4] AcuMonitor: For detecting an XXE attack, Blind XSS and SSRF - Acunetix. (n.d.). Retrieved from https://www.acunetix.com/vulnerability-scanner/acumonitor-technology/

[5] Cloud Security Alliance. (2016). The Treacherous 12: Cloud Computing Top Threats. Retrieved from https://downloads.Cloudsecurityalliance.org/assets/research/topthreats/Treacherous-12_Cloud-Computing_Top-Threats.pd

[6] Tarun Dhar Diwan, Dr. Siddhartha Choubey, Dr.H.S.Hota, “A Novel Hybrid Approach for Cyber Security in IoT network Using Deep Learning Techniques” Publication in International Journal of Advanced Science and Technology ISSN:2394-5125, ISSN: 2005-4238.

[7] Darmanin, G. (2014, May 5). Negative impacts of automated vulnerability scanners and how to prevent them. Retrieved from https://www.acunetix.com/blog/articles/negativeimpacts-automated-vulnerability-scanners-prevent

[8] Tarun Dhar Diwan, Dr. Siddhartha Choubey, Dr.H.S.Hota, “Development of Real Time Automated Security System for Internet of Things (IoT)” Publication in International Journal of Advanced Science and Technology Vol. 29, No. 6s, (2020), pp. 4180 – 4195, ISSN: 2005-4238

[9] Erturk, E. (2012). Two Trends in Mobile Malware: Financial Motives and Transitioning from Static to Dynamic Analysis. Infonomics Society.

[10] Tarun Dhar Diwan, Dr. Siddhartha Choubey, Dr.H.S.Hota, “An Experimental Analysis of Security Vulnerabilities in Industrial Internet of Things Services” published in International Journal of Information Technology in Industry (IT in Industry) Vol. 9, No.3, 2021, pp.592–612, ISSN: 2203-1731.

[11] Erturk, E. (2013). An intelligent and object-oriented blueprint for a mobile learning institute information system. International Journal for Infonomics (IJI), 6(3/4), 736-743.

[12] Tarun Dhar Diwan, Dr. Siddhartha Choubey, Dr.H.S.Hota, “Multifactor Authentication Methods: A Framework for Their Selection and Comparison” published in International Journal of Future Generation Communication and Networking Vol. 13, No. 3, (2020), pp. 2522–2538, ISSN: 2233-7857.

[13] Gupta, S., & Gupta, B. B. (2015). PHP-sensor. Proceedings of the 12th ACM International Conference on Computing Frontiers - CF '15. doi:10.1145/2742854.2745719.

[14] Tarun Dhar Diwan, Dr. Siddhartha Choubey, Dr.H.S.Hota, "An Investigation and Analysis of Cyber Security Information Systems: Latest Trends and Future Suggestion" published in International Journal of Information Technology in Industry (IT in Industry), Vol. 9, No.2, 2021, pp.477–492, ISSN: 2203-1731.

[15] InfoSec Institute. (2014, September 24). 14 best open source Web Application Vulnerability Scanners. Retrieved from http://resources.infosecinstitute.com/14-popular-webapplication-vulnerability-scanners/#gref

[16] Jasmine, M. S., Devi, K., & George, G. (2017). Detecting XSS based Web Application Vulnerabilities. International Journal of Computer Technology & Applications, 8(2), 291-297.

[17] Jeeva, S., Raveena, K., Sangeetha, K., &Vinothini, P. (2016). Web Vulnerability Scanner using Software Fault Injection Techniques. International Journal of Advanced Research Trends in Engineering and Technology, 3(2), 637-649. Retrieved from https://www.researchgate.net/publication/303756552_WEB_VULNERABILITY_SCANNER_USING_SOFTWARE_FAULT_INJECTION_TECHNIQUES

[18] Khalid, A., & Yousif, M. F. (2016). Dynamic analysis tool for detecting SQL injection. International Journal of Computer Science and Information Security, 14(2), 224-232. Retrieved from https://www.researchgate.net/publication/311081330_Dynamic_Analysis_Tool_for_Detecting_SQL_Injection

[19] Levin, D. (2017, March 14). How Should We Address the Cybersecurity Threats Facing K12 Schools? Retrieved from https://www.edtechstrategies.com/blog/how-should-weaddress-cybersecurity-threats-facing-k-12-schools/

[20] OWASP [Open Web Application Security Project]. (2015, October 6). Path Traversal. Retrieved from https://www.owasp.org/index.php/Path_Traversal.

[21] Revankar, M. (2015, October 15). Mobile Device App Inventory Auditing with Nessus 6.5. Retrieved from https://www.tenable.com/blog/mobile-device-app-inventoryauditing-with-nessus-65

[22] Saeed, F. A. (2014). Using WASSEC to evaluate commercial Web Application Security Scanners. International Journal of Soft Computing and Engineering, 4(1), 177-181. Retrieved from https://www.researchgate.net/profile/Fakhreldeen_Saeed2/publication/311310455_Using_WASSEC_to_Evaluate_Commercial_Web_Application_Security_Scanners/links/5879149c08ae9275d4d91b83/Using-WASSEC-to-Evaluate-Commercial-WebApplication-Security-Scanners.pd

[23] Schupak, A. (2015, March 24). One in three top websites at risk for hacking - CBS News. Retrieved from http://www.cbsnews.com/news/one-in-three-websites-at-risk-for hacking

[24] Suteva, N., Anastasov, D., &Mileva, A. (2014, April). One unwanted feature of many Web Vulnerability Scanners. Paper presented at Proceedings of the 11th International Conference on Informatics and Information Technologies.

[25] Warman, M. (2013, January 15). 90 per cent of passwords 'Vulnerable to Hacking'- Business Insider. Retrieved from https://www.businessinsider.com.au/90-percent-ofpasswords-vulnerable-to-hacking-2013-1?r=US

[26] Mishra, A., Jain, H., Biswas, P., Thowseaf, S., & Manikandan, R. (2021). Integrated solution for optimal generation operation efficiency through dynamic economic dispatch on Software Technological Park of India. Materials Today: Proceedings. Published. https://doi.org/10.1016/j.matpr.2021.05.019

[27] Shukla, A., Kalnoor, G., Kumar, A., Yuvaraj, N., Manikandan, R., & Ramkumar, M. (2021). Improved recognition rate of different material category using convolutional neural networks. Materials Today: Proceedings. Published. https://doi.org/10.1016/j.matpr.2021.04.307