Abstraction and automation of WordPress vulnerability scanning

MSc. Cybersecurity
MSCCYB1_JAN22O

Stephen Farrell
Student ID: x21132445

School of Computing
National College of Ireland

Supervisor: Vikas Sahni

National College of Ireland

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Stephen Farrell …………………………………………………………………………

Student ID: x21132445 ……………………………………………………………………………..……

Programme: MSCCYB1_JAN22O ……………………………… **Year:** 2022 ………

Module: MSc Cybersecurity ……………………………..………

Supervisor: Stephen Parsons ………………………………………………….………

Submission Due Date: 15/12/22 ……………………………………………………………………………………………….………

Project Title: Abstraction and automation of WordPress vulnerability scanning………….…………………….…………………..…………………..………

Word Count: 7913………… **PageCount** 19………………………………

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Stephen Farrell ……………………………………………………………………………………………………

Date: 05/01/23 ……………………………………………………………………………………………………

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Abstraction and automation of WordPress vulnerability scanning

Stephen Farrell
x21132445

Abstract

The purpose of this work is to increase the threat assessment coverage against the most common Content Management System (CMS) in use, WordPress. WordPress represents 63.8% of all CMS in use on the Internet. The product's ubiquity has made it a target for exploitation, with around 90,000 WordPress sites attacked every minute. This threat vector is not included in risk reports to customers and, as a result, is a critical gap in identifying and remediating risks. Using a combination of open-source tools, data format conversion and process workflow. a WordPress vulnerability service was created that abstracts the complexity of the underlying API calls and presents the output into a customer-friendly non-technical executive summary, with the findings correctly formatted to import into the risk register solution. The service increases the threat assessment coverage by adding detections for 37,627 known WordPress vulnerabilities. The human effort to scan each customer was reduced from 30 minutes to zero minutes. This solution specifically addresses WordPress; future work should address the remaining 36.2% of CMS products in order of popularity to increase detection coverage.

1 Introduction

1.1 Background and Rationale

Any organisation to prevent cyber-exploitation requires proper intelligence and prompt action to detect and manage cyber-attacks and vulnerabilities known as threats. Threat-related intelligence tends to be extracted or obtained from multiple sources like platforms of social media where threat information might be published in real-time. In the current market for threat assessment coverage, security organisations are growingly providing security analysis tools and services that are optimised and automated for the reduction of efforts in the detection and determination of threats and related vulnerabilities (Macher *et al.,* 2016; Ismagilova *et al.,* 2022; Le *et al.*, 2019).

In this context, a background study by Le *et al.* (2019) determined that security analysts perceive cyber-threat determination from social media sites as a time-taking task because of which responses to such threats might get delayed. Thus, the study explored the importance of a Twitter-based automatic threat intelligence gathering framework by utilising the model of novelty detection. This framework permitted the automated gathering of network parameters such as security vulnerabilities, I.P. addresses, and information about hackers to execute arbitrary commands (Le *et al.*, 2019). On the other hand, while looking at the real-time examples of automated security analysis tools or services, it is also found that a small Ireland-based cyber-security company provides consultancy services that involve analysis of Open-Source Threat-Intelligence for developing "security-scorecard," particularly for internet-based digital platforms like websites. The company utilises paid-for SAAS (Security-as-a-Service), i.e., also known as Black-Kite, for threat detection (Black Kite, 2022; Slashdot Media, 2022). The threat detection and assessment report constructs the base for determining customer risks and ways for remediating the risks. However, failure to the determination of the vulnerability of Security leads to failure in executing the remediation plan.

Given the users' restricted or limited skill possession regarding security technology, it is also required to put detailed and critical insights into the efficacy of automated threat detection mechanisms for minimising efforts and time invested in the entire threat assessment coverage procedure. Organisations must conduct early and effortless threat assessments for timely and effective responses to keep their data and assets protected or secure from attack. Therefore, it has been noted as essential to conduct the present study to examine the extent to which the automated and optimised security analysis tools are effective for increasing coverage of threat assessment with less possible effort and time. The service of Black Kite enables non-intrusive types of assessments for data gathering out of sources that are publicly available and executes contextualisation as well as evaluation for the conversion of data potentially into threat intelligence (Black Kite, 2022a; Black Kite. 2022).

There is an opportunity to utilise highly permissive scanning of vulnerability for conducting the detailed assessment, which might complement the service findings of Black Kite. It is also observed that various customers presently utilise applications of CMS like WordPress that do not have approval for the management of vulnerability by the service of Black Kite (Pazos *et al.,* 2020). It might be noted as the opportunity for adding vulnerability detection features by utilising tools, for example, WPScan (WordPress Security-Scanner) or similar services or tools. Paid-for security services such as Black Kite provides detailed risk rating as per the categories of risks as well as rich and high-quality reporting while, on the other part, free-for tools, such as WPScan, provide robust control upon the threat intelligence process execution; however, it lacks capabilities for delivering rich reporting (U.G., 2022; Johnson, 2019).

This research follows the qualitative methodology, wherein the data has been gathered with help of the secondary case-study method. For this purpose, four case studies have been examined and studies, namely, WordPress Scanner, Security Scorecard, Black Kite and BitSight. The case studies have been sourced from academic and authentic sources such as company reports, websites, scholarly journal papers and published articles by using keywords considered for this research. These cases have been analysed in a systematic and comprehensive manner.

For a clear understanding, the theory and findings of the study have been organized into seven sections wherein the first section, Introduction, discusses the background, rationale, aim and objectives and seeks to familiarise the readers with the purpose and focus of the study. The second section, Related Works, presents an overview of the prevailing literature on security analysis tools and threat assessment such that a theoretical and conceptual foundation can be developed for the research. The third section, Research Methodology, presents an overview of the methods used for data collection and analysis. The fourth section presents Data Specification, while the fifth section explains the Implementation wherein automated service execution and service output has been discussed. The sixth and seventh sections discuss the evaluation of the case studies and conclusion, respectively.

1.2 Aim

The research paper has the purpose of reviewing and critically analysing the current market of threat and vulnerability services and tools, to create an automated WordPress vulnerability scanning service.

1.3 Objectives

- To investigate and analyse the cases related to automation and optimisation of security analysis tools and services.
- To analyse the efficiency of optimised and automated security analysis tools and services in reducing efforts while increasing coverage of threat assessment.
- To provide strategic ways for improving detection mechanisms using open-source tools and advanced automated and optimised services for better threat detection coverage.

2 Related Work

2.1 Security Analysis Tools and Threat Assessment

One of the studies by Macher *et al.* (2016) found that for the threat assessment process, TARA (Threat-Analysis and Risk-Assessment) method has been prevalent that included the determination of threats in three phases, i.e., threat-identification, assessment of risks, and analysis of risks (Macher *et al.,* 2016). However, the manual method identified the weakness regarding high time and effort consumers so that the consumers expected automotive and advanced systems for detecting and assessing threats. In contrast, the study by Ismagilova *et al.* (2022) emphasised less time investment in the automated processing of data based on information systems for detecting security risks and threats to tangible and intangible business assets (Ismagilova *et al.*, 2022). However, this study had weaknesses in terms of failure to denote the detailed process of automated security analysis tools and their advancement over time for effort reduction in threat assessment.

A study by Lee & Lee (2018) provided specific knowledge that businesses require automated and prompt threat detection systems for keeping prevented cyber-attacks. In this regard, the study's strength is reflected as it denoted an automated security analysis tool, i.e., BitSight, which helped distinguish ransomware attacks to be posed on estimated 20,000 firms by analysing servers and industry data reporting (Lee & Lee, 2018). However, the above study shared limited data on security analysis tools. The article by Feist, Grieco & Groce (2019) explained the utility of various automatic security analysis tools for threat detection in organisations. For example, Mythril Classic has been regarded as the open-source tool for security analysis that conducts taint and concolic analysis along with control-flow monitoring for multiple security vulnerability detections. In contrast, TeEther has also been recognised as an automatic tool for threat detection that determines vulnerabilities within the smart contracts of Ethereum (Feist, Grieco, & Groce, 2019). The study also explored that Slither's open-source version has greater than an estimated 20 bug-detectors to assess bugs and threats that mainly cover shadowing, reentrancy, uninitialised variables, and known issues of Security (Feist, Grieco, & Groce, 2019). However, the study did not emphasise the effort reduction aspect of threat detection with automated security analysis tools.

The study by Waheed *et al.* (2020) emphasised that security analysis tools are being constructed based on machine-learning algorithms, due to which efforts in regard to security detection and sensing threats get reduced in organisations (Waheed *et al.*, 2020). However, more specific security-detection tools have been identified in the study by Praitheeshan *et al.* (2019). For example, PointGuard protection for the purpose of baggy-bounds checking StakeGuard for automatic detection of the overflow of buffer and EasyFlow for manifesting and protecting the threat of overflows to manage smart-contract vulnerabilities (Praitheeshan *et al.*, 2019).

On the other hand, the study of Wangen, Hallstensen & Snekkenes (2018) has highlighted the application of Microsoft Cloud Risk Decision Framework, abbreviated as MCRDF, which helps in taking effective decisions for the management of cloud-based risks (Wangen, Hallstensen & Snekkenes, 2018). Moreover, as per Cayirci *et al.* (2016), the core strength of MCRDF is that it provides an overview of the cloud-oriented areas for risk control, and it also offers examples for the application of risk mitigation strategies. Moreover, this method holds weakness in terms of its inability to control the risks that are prevalent outside the risk control areas (Cayirci *et al*., 2016). However, the overall weakness of the current research lies in terms of its lack of in-depth investigation related to the lower levels of tools for information security-oriented risk assessment.

In comparison to the above, Cherdantseva *et al.* (2016) argued that the application of Supervisory Control, as well as Data Acquisition (SCADA) systems, is helpful for the prioritisation of key components with a system in strategic relationships with their significance and vulnerability rate associated with an attack (Cherdantseva *et al*., 2016). Moreover, Maseda *et al*. (2021) explored that risk assessment in the SCADA is beneficial for the engineers and managers towards the formulation of effective security-related policies (Maseda *et al*., 2021). In this context, the current research holds strength in regard to offering a detailed understanding of the SCADA security systems as well as the interdependencies that are identified between the systems of risk assessment and SCADA.

On the other side, Alalfi, Parveen & Nazzal (2022) also evaluated that mutation testing tends to be a significant security analysis tool that tests the software based on fault identification. This system mimics the errors as well as injects the artificial errors into a system (Alalfi, Parveen & Nazzal, 2022). Further, Kintis *et al.* (2018) argued that the semantic mutation testing tool is also utilised for the identification of different types of faults in the source codes (Kintis *et al*., 2018). The core strength of mutation testing tools is to diagnose the security aspects of the software. In contrast to the above, Loise *et al.* (2017); Shi, Bell & Marinov (2019) asserted that security analysis tools named the Java mutation testing tools also help in highlighting the vulnerable areas in the programmed code by depicting the location of the security-hampering bugs. However, the research comprises weaknesses in terms of considering fewer forms of data security patterns that can be identified during the usage of open-source projects. Apart from the above, Higuera *et al.* (2020) argued that the deployment of the Security Analysis Static (SAS) tool is effective for the examination of the security-related vulnerabilities prevalent in mobile web applications. However, a repeatable methodology is selected for providing ranking as well as a critical comparison for the SAS tool.

It can be argued that WPScan is the dominant open-source WordPress vulnerability scanner, as per metrics in Table 1. WPScan is the most-rated WordPress vulnerability scanner on GitHub, with 7.2k Stars. GitHub defines staring as "shows appreciation to the repository maintainer for their work" (GitHub, 2020). WPScan has 264 "Watching", which allows users to get notifications for activity and changes to the package. There are 1.2k forks of the WPScan repository; this has two major impacts on the WPScan code. Developers take advantage of the upstream repository development work and develop independent improvements for their own use and can push these improvements back to the upstream repository as a contribution. Further developing and improving the WPScan code. There are 46 contributors to the WPScan repository that regularly and consistently contribute, as shown in Figure 1 for the last year. Figure 2 shows the contribution frequency since the creation of the package on 8 July 2012. WPScan updates its vulnerability database weekly with 38,073 entries as of 20 December 2022. It is for these reasons that WPScan is the open-source tool chosen to compare against the industry-leading security analysis tools in Table 1.

Table 1: Comparing and Contrasting Open Source WordPress Vulnerability tools.

Tool	Description	GitHub Metrics	Last Update	Strength	Weakness
WPHunter [1]	Is a WordPress Vulnerability Scanner	139 stars 10 watching 48 forks 2 contributors	Mar, 2018	Dedicated to WordPress Vulnerability Scanning	Has not been updated in over 4 yrs
Wordpresscan [2]	Was rewritten in Python and contained some WPSeku influence.	553 stars 29 watching 204 forks 8 contributors	Jun, 2021	Dedicated to WordPress Vulnerability Scanning	The repository has been archived by the owner
WPScan [3]	Performs black box WordPress vulnerability scans,	7.2k stars 264 watching 1.2k forks 46 contributors	Nov, 2022	38,061 vulnerabilities in their database, updated daily	Commercial restrictions, 75 free API calls per 24hrs
WPSeku [4]	Performs black box WordPress vulnerability scans,	18 stars 1 watching 14 forks 0 contributors	Jul, 2019	Dedicated to WordPress Vulnerability Scanning	Has not been updated in over 3 yrs
Wordstress [5]	Is a white-box vulnerability scanner.	33 stars 3 watching 5 forks 3 contributors	May, 2016	Dedicated to WordPress Vulnerability Scanning	Has not been updated in 6 years
Vane [6]	Is a forked project of WPScan.	208 stars 25 watching 64 forks 18 contributors	Apr, 2018	It is a fork of WPScan,	Has not been updated in over 4 yrs
Wpvulndb_cmd [7]	Uses WP-CLI and the WPScan vulnerability database.	30 stars 9 watching 8 forks 0 contributors	Jul, 2017	Dedicated to WordPress Vulnerability Scanning	Has not been updated in over 5 yrs
WordPress-exploit-	Provides a set of tools to assess	960 stars 61 watching	Nov, 2019	Dedicated to WordPress	A long learning

[1] https://github.com/Jamalc0m/wphunter
[2] https://github.com/swisskyrepo/Wordpresscan
[3] https://github.com/wpscanteam/wpscan
[4] https://github.com/andripwn/WPSeku
[5] https://github.com/thesp0nge/wordstress
[6] https://github.com/delvelabs/vane
[7] https://github.com/anantshri/wpvulndb_cmd

framework [8]	and exploit WordPress installations	272 forks 5 contributors		Vulnerability Scanning and Exploitation	curve, last updated 2 yrs ago.
Droopescan [9]	Supports several CMS.	1.1k stars 46 watching 243 forks 13 contributors	Jun, 2022	Supports SilverStripe, WordPress and Drupal.	The project is no longer maintained or developed
CMSeeK [10]	Detection and Exploitation suite - Scan over 180 other CMSs	1.8k stars 68 watching 457 forks 10 contributors	Aug, 2022	Broad coverage of CMS.	It is poorly updated, with fixes/ features

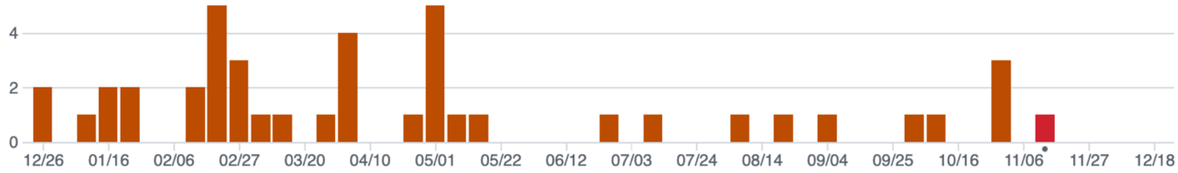

Figure 1: WPScan Github repository commits Dec 2021 – Dec 2022

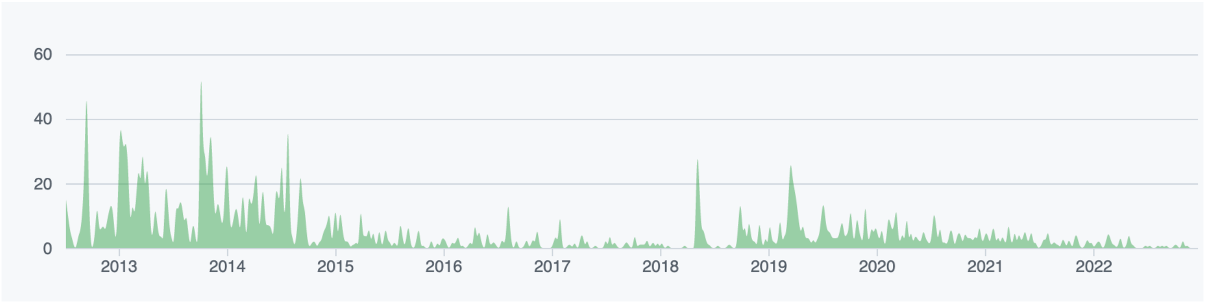

Figure 2: WPScan Github repository contribution frequency 8 July 2012 – 20 December 2022

Table 2: Comparing and Contrasting Security Analysis Tools in the Current Market

Service Analysis Tools	**Cost**	**Types of detections**	**Quantified threat coverage in numbers**	**Effort of Execution**	**Skill Required**
Black Kite	Public pricing information is not available.	Website vulnerability, attack surface and patch status, dark web,	Twenty types of threat detection (Black Kite, 2022).	Automated parsing techniques and cross-correlation measures of	Cyber-security assessment skills, technical skills about

[8] https://github.com/rastating/wordpress-exploit-framework
[9] https://github.com/SamJoan/droopescan
[10] https://github.com/Tuhinshubhra/CMSeeK

		hacktivists and information disclosure sites, web ranking, fraudulent domains, domain/I.P. reputation (Black Kite, 2022).		capability help in saving efforts and time in the execution of threat detection and assessment (Black Kite, 2022).	the Black-Kite tool, I.T. skills, analytical skills, and risk and threat assessment skills (Black Kite, 2022).
Security Scorecard	The cost rate starts from $16,500 in regard to self-assessment of threats and Security (Upguard, 2022).	Uses passive and active methods of data collection, and collected information facilitates risk indicators for detecting risks which tend to get processed by the proprietary algorithm for generating individual ratings of Security (Upguard, 2022).	It measures the performance of an organisation across ten distinct areas of cyber-security (Crowdstrike Store. 2022).	Security scorecard enhances efficacy while saving time and reducing security risk detection efforts (Britton, 2022).	Security proficiency, risk assessment, governance skill, Security Scorecard related technical skill, threat detection skills, data protection, and third-party management skills (ISACA.org, 2018).
BitSight	The cost for BigSight renders between $2,000-$2,500 for a single vendor on a yearly basis (Upguard, 2022).	Threat and risk detection regarding security diligence compromised systems, data breaches, and user behaviour (BitSight Technologies Inc, 2022).	BitSight helps in discovering approximately 23 distinct threats or risk factors (BitSight Technologies Inc, 2022).	Effective and smooth decisions regarding business security in less time and with improved quality (Chatterjee, 2020).	Automated testing skill, error detection skill, functional testing skill, risk analysis skill, quality management, and assurance skill (Chatterjee, 2020)

WPScan (WordPress scan)	Free-of-cost to be used in the non-commercial field (WPScan, 2022).	Assess WordPress-related vulnerabilities, themes, and plugin-related vulnerabilities, enumeration of usernames, detecting vulnerable timthumb-files, exposure of error logs, detecting weak passwords, enumeration of media files (WPScan, 2022).	Ten types of plugin vulnerabilities are the top ones detected by WordPress (WPScan, 2021).	Due to being automated, it reduces efforts in threat detection (Bugcrowd, 2022). It is also cost-friendly to present investment requirements for threat detection (WPScan, 2022).	Technical skill, WordPress skill, vulnerability scanning skill, security risk analysis skill (WPScan, 2022)

In the current marketplace, Black Kite has been recognised as the paid award-winning leading platform, which ensures 360^0 visibility of cyber-risks and threats for assessing vulnerabilities for organisations and developing defensible intelligence to provide prompt response to the vulnerabilities. It handles the detection of 20 or more categories of risks and confirms compliance with the standards of security analysis with automated, timely, and trustworthy efforts regarding threat or risk detection (Black Kite, 2022a). In contrast, in the marketplace, the security scorecard also has effective performance as it enables the organisation to keep a constant track of threats regarding cyber-security and address real-time security challenges with adequate measures (Snowflake Inc, 2022). Security Scorecard offers critical insights potentially into the posture of Security of the organisations and risks or threats associated with HSTS, SSL, DNS, and open ports get detected by this tool with minimal effort and less time (Security Scorecard, 2022; Upguard, 2022; Crowdstrike Store. 2022; Britton, 2022).

BitSight is also found to be efficient in detecting security risks like data breaches and security diligence in an automated manner for organisations to respond to these risks in a time-efficient or prompt way (BitSight Technologies Inc, 2022; Chatterjee, 2020). WPScan, on the distinct part, is noted to be cost-free threat detection or security analysis tool which helps in determining vulnerabilities oriented to errors, password weakness, and media-file protection (WPScan, 2022; Wpsec.com, 2022).

The above literature determined multiple security analysis tools; however, there is a lack of specific, detailed, and evidence-based knowledge on the performance, procedures, and efficacy of advanced automated and optimised tools of data security to reduce efforts in threat-assessment coverage. Therefore, the current study has been organised to investigate the case studies of optimised and automated security analysis tools, mainly Black Kite, BitSight, Security Scorecard, and WordPress Scanner, to analyse their performance efficacy and shortfalls in threat-assessment-related effort reduction.

3 Research Methodology

3.1 Data-Collection Technique and Procedure

The process for data collection utilised in the research is the secondary case-study method. The rationale for adopting the case-study method has been that it contributed towards determining and conducting an in-depth evaluation of cases related to security analysis tools (automated and optimised) that have the potential to reduce the time and effort required in threat assessment coverage. The case-study method has the capability of revealing comprehensive details, factual notions, illustrations, and reasons for the effectiveness and challenges linked to automated as well as optimised security analysis tools for the threat-assessment purpose (Bell, Bryman, & Harley, 2022; Bougie & Sekaran, 2019). Thus, it has been comprehensively determined whether the security analysis tools with the attributes of automation and optimisation are sufficient and effective for effort minimisation in the coverage of threat assessment. However, other secondary methods like systematic review or literature investigation have not been sufficient to put specific and elaborated insight into particular cases of security analysis tool's utility and efficacy which could be made possible by using the case-study method (Bougie & Sekaran, 2019).

Four case studies have been selected, including the cases of Black Kite, Security Scorecard, WordPress Scanner, and BitSight. The raw data for the research about the selected case studies have been collected by using search terms like security analysis tools, threat assessment, cybersecurity, BitSight, security scorecard, threat intelligence, Black Kite, WordPress Scanner, automation, optimisation, time-consumption, cyber-attacks, analysis techniques, risk detection, and data protection. In terms of data-collection equipment, only authentic sources like websites, company reports, published articles, scholarly journals, and research papers have been utilised for case study investigation purposes for accomplishing the research work. Primary methods, possibly interviews and surveys, were not utilised because these methods are time-taking, costly, and insufficient to give a vast knowledge pool without any boundaries or sample limits regarding the security analysis tools' automation to reduce threat assessment's efforts (Bell, Bryman, & Harley, 2022).

3.2 Data-Analysis Method

The raw data regarding the case studies have been analysed by using the case-analysis method. For case analysis, separate cases of Black Kite, WordPress Scanner, BitSight, and Security Scorecard have been analysed in a systematic and comprehensive manner by compiling facts about these automated security tools' performance for threat assessment efficacy and effort reduction and then interpreting the data findings by putting critical and detailed insights into the confronted issues with regard to these tools of security analysis (Bell, Bryman, & Harley, 2022). The case-study analysis also offered valuable knowledge regarding the businesses' threat assessment performance outcomes by using the selected security tools to identify the tools' efficacy and issues to further determine alternative solutions for mitigating the issues with the support of the present research project. The final results from the case-study analysis are generated as the determination of the performance level of security analysis tools and any shortcomings of these automated and optimised tools for threat assessment with less effort and time (Bell, Bryman, & Harley, 2022).

3.3 Ethics

Ethical concerns around authentic data source usage, citation provision, data-theft elimination, and credibility to scholars have been taken into consideration. Primary data has not been involved, so no ethical accountability was there for primary research (Bell, Bryman, and Harley, 2022).

4 Design Specification

The WordPress vulnerability scanning service has been designed to meet the requirements of the customer by being cost-effective and fully configurable by the operations team and requires no training or knowledge on how the service operates for the Security Analysts to action the vulnerability reports. The service, once configured to the needs of the customer, will execute on a scheduled basis, scanning each customer's website and sending the vulnerability reports to the Security Analysts to review and input into the Risk management service.

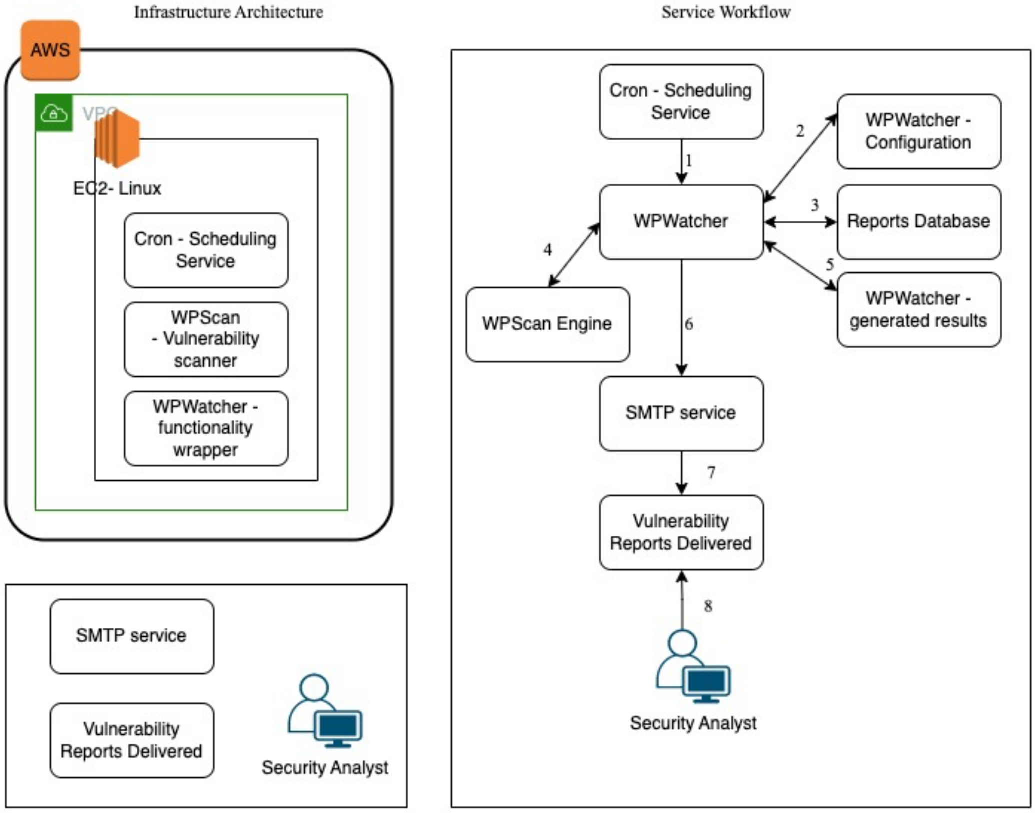
Infrastructure Architecture
AWS
VPC
EC2- Linux
Cron - Scheduling Service
WPScan - Vulnerability scanner
WPWatcher - functionality wrapper
SMTP service
Vulnerability Reports Delivered
Security Analyst
Service Workflow
Cron - Scheduling Service
1
2
WPWatcher - Configuration
WPWatcher
3
Reports Database
4
WPScan Engine
5
WPWatcher - generated results
6
SMTP service
7
Vulnerability Reports Delivered
8
Security Analyst

Figure 2: Infrastructure Architecture and Service Workflow

4.1 Infrastructure Architecture

The service is deployed in AWS and falls under the free tier offering. This allows the service to run for free for a year. Using AWS as the (CSP) Cloud Service Provider, the solution takes advantage of additional services such as EBS snapshots to take a backup of the EC2 Instance in its fully configured state to enable a service to restore in the event of a hardware failure. Leveraging Security Groups which act as an Instance level firewall, the service locks down access to administer the Instance over SSH on port 22 to restricted source I.P. range. This reduces the attack surface from malicious users. Monitoring the instance performance and availability was achieved using AWS CloudWatch.

4.2 Service Workflow

The Vulnerability scanner was built using the open-source code packages WPScan and WPWatcher. This achieves the customer's requirements while maintaining full control of the service code and its execution. Through the use of the Linux operating system, the native scheduler service was used to execute the automation. Once set, the service executes on a defined schedule and requires no human intervention.

WPScan package is used as the vulnerability scanning engine to make the API calls against WordPress websites and capture the results. This package takes scanning input parameters to define the scanning intensity and produces a JSON output of the results. With an API key, the package can also map vulnerabilities found against its database, enriching the JSON output with related information.

WPWatcher is a Python package that adds a layer of customisation and functionality on top of the WPScan engine. This package enables the use of a configuration file called wpwatcher.conf, which, when configured correctly, enables sending of reports by email and sets the parameters for each website to be scanned. This removes the need for human input so the service can run autonomously.

The SMTP service can be configured for either on-prem or hosted configuration. In this case, google mail has been chosen with the mail configuration settings to enable sending through the service using an application password. The vulnerability reports will then show as originating from the google mail server and sent to the email address defined in the wpwatcher.conf file.

5 Implementation

The scanning service hosted on a Linux EC2 instance enables full control from the O.S. level up to the packages installed. The vulnerability scan results are stored on the EC2 server. This control and data ownership are abstracted in SAS services such as BlackKite and, as a result, remove the ability to change or integrate automation at an O.S. or package level.

5.1 Automated service execution

Automating the WordPress vulnerability scanning service removes the skills required as per Table 1 (Technical skill, WordPress skill, vulnerability scanning skill, security risk analysis skill) to run the service. An entry-level security analyst can take the service results and create customer-facing reports that are structured in an easy-to-understand format.

5.2 Service outputs

Automation has reduced the engineering effort to execute a vulnerability scan from 10 minutes per website scanned to zero minutes. Removing the engineering effort to execute and format reporting allows infinite scaling of the service while removing human error in service execution.

Every service execution produces a JSON report that is stored on the server. This forms a historical record with subsequent scans appending to the file.

Each scan report email comes with a JSON file attached that contains the full vulnerability report. This JSON file can then be converted to CSV using a simple tool or website. When converted to a CSV file, the vulnerability findings can be imported into the customer's risk management solution for tracking and reporting.

The conversion of the WPScan JSON output by WPWatcher creates an email template and structures the information into sections. The Summary identifies the installed Components, the Version and the State. This format is easy for a non-technical end customer to understand the risks against their WordPress website.

6 Evaluation

6.1 Case-Study 1: Black Kit Security Tool

It is evaluated that company such as Cisco is identified as a regularly monitored vendor of the Black Kite platform. Cisco is granted a rank of C- by the Black Kite platform, which is considered an average grade among other large organisations. Cisco is identified to generate a cascading risk-related impact on its customers as well as its business partners. The threat actors comprise sensitive data about the potential clients held by Cisco, which may generate increased threats of phishing as well as credential stuffing. In regard to the above security-oriented threat, the use of the Vulnerability Software Identifier (VSI) of the Black Kite has assisted Cisco in terms of identification of the presence of vulnerable software by providing the impact analysis of the vendor. The VSI system provided by the Black Kite is capable of offering a detailed estimation of the impact as well as the probability of the cyber threat-related incident within an organisation. As per the security analysis conducted by Black Kite, it is analysed that Cisco is considered a high probability and high impact generating vendor, which means that the probability or chances of facing a cyber threat are high, and the impact generated by the cyber threat is also high (Black Kite, 2022). It is also analysed that the Cyber risk intelligence tools provided by the Black Kite are helpful for helping large companies to recognise and track their vendors that are identified to use a specific class of product. Black Kite also helps large organisations for filtering the monitored vendors by enabling the selection of the key product types (Black Kite, 2022). Hence, it is analysed that Black Kite has assisted the organisations such as Cisco in identifying the vendors as well as assuring that a cascading negative impact of the vendors upon the supply chain of Cisco is not generated.

Furthermore, it is analysed that Black Kite has provided recommendations for safeguarding the supply chain where it is essential to provide a listing of all the vendors in order to access the systems of the organisation as well as store sensitive data related to the organisation. It is also essential to filter the vendors that are identified to use the products of a specific organisation. Black Kite is also focused on issuing necessary advice about the critical phishing attacks that can occur in the company. Moreover, Black Kit further issues guidelines for determining the cyber security competence of the vendor (Black Kite, 2022).

6.2 Case-Study 2: Security Scorecard

It is reviewed that the company named SecurityScorecard has provided assistance to Modulr Finance Limited in terms of financial compliance as well as customer data threat-related risks. Modulr has experienced challenges in regard to the fulfilment of its regulatory compliance-oriented needs. Furthermore, Modulr is also identified to execute the cyber-security review as well as monitor the details regarding its vendors as well as potential customers by executing its business practices as a Business to Business financial platform. Modulr is also seeking help in terms of issuing effective levels of compliance control policies for the protection of customer-related data. It is analysed that the conventional diligence process utilised by the Modulr consumes a considerable portion of time, and it also causes a high amount of operational expenses. The vendors, as well as customers that are evaluated under Modulr are identified to be insufficient in terms of visibility levels regarding the ecosystem-oriented risks. Furthermore, it is also analysed that Modulr is reliant on the manual review system for monitoring the prominent threats. The use of manual reviews tends to increase human error-related risks. The need for a real-time monitoring system increased in Modulr to ensure the proper governance of the regulators (SecurityScorecard Inc, 2022).

Furthermore, it is also analysed that the platform offered by the SecurityScorecard has enabled the Modulr to perform an accurate review of cybersecurity-related risks. The SecurityScorecard provided security ratings to the vendors associated with Modulr. By this time, the Modulr was utilising a different security tool. However, on comparing the security Scorecard ratings with the ratings provided by Modulr's tool, it is evaluated that the cybersecurity ratings generated by the SecurityScorecard matched with the ratings of Modulr. The cybersecurity platform of SecurityScorecard comprised sufficient levels of details for due diligence, and it also offered a historical trial for the auditing system. SecurityScorecard is highly proficient in terms of generating cybersecurity scores or rankings in comparison with the other vendors; the SecurityScorecard merges Security or risk-related information in a user-friendly format. Furthermore, the reports generated by the SecurityScorecard are also comprehensive. The Atlas product of the SecurityScorecard is identified to assist Modulr in effectively exchanging the questionnaire surrounding cybersecurity and enable a real-time comparison between the external risk monitoring tools and the risk assessment process of SecurityScorecard. With the help of security ratings provided by the SecurityScorecard, Modulr is capable of creating a Partner as well as Service Provider's due diligence process (SecurityScorecard Inc, 2022).

6.3 Case-Study 3: WordPress Scanner

WPScan has been known as the highly popular open-source security scanner. As per a recent survey of W3Techs, the content management system's 63% instances utilise WPScan as well an estimated 36.4% of internet-based websites are known as sites of WordPress. In the case study analysis, the case of Acunetix, a popular WordPress scan, has been taken. Under this case, it is investigated that one of the customers of Acunetix as a WPscan is a multinational bank based in Spain, which serves customers up to 18 million. The banking business specifically depends on multiple web-based applications; however, their safety management seems to be complex and difficult. Manual scanning of all these web-application is an infeasible task. As the solution, Acunetix Premium has deployed after comparing it with other security threat scanners. While analysing the performance of this optimised and automated Acunetix Premium (WPScan) tool, it is evaluated that with reduced efforts, this tool is efficient in increasing coverage of threat assessment (Acunetix, 2022a; Acunetix, 2022). For example, this tool has shown the capability of scanning every external and internal level application potentially for the team of cyber-security by automatically handling the huge workload without needing to make manual efforts (Acunetix, 2022).

Its "thorough scanning feature" supports the team of cyber-security to determine issues within highly complicated web applications. Another feature of "Pentesting Support," Acunetix also proved to be efficient in automatically identifying every possible vulnerability, because of which penetration testers might easily analyse more complicated security issues. With less-time investment, Acunetix scans the highest possible applications due to its automation feature. Thus, the reduction of efforts in threat assessment has been made possible by Acunetix, which is a WPScan tool for security analysis (Acunetix, 2022; Acunetix, 2022a). Technology Acceptance Model (TAM) further assists in the adoption of Acunetix as this model determines that ease of utility and perceived usefulness trigger technology adoption (To and Trinh, 2021). Similarly, Acunetix proved to be highly useful for scanning numerous web applications for security risk detection, and automation features made it easily usable. Thus, Acunetix has been adopted by the banking sector for security threat and risk detection and analysis purpose (Acunetix, 2022).

However, in WPScan, some limitations have also been found that even after the identification of vulnerabilities, it tends to be difficult to derive their meaning for the operations of the business. It means WPScan might be proved as lagging behind in offering rich reporting of vulnerabilities' severity for the business. It might also be possible that all vulnerabilities are not covered, and timely updates required in the tool also raise complexities (Johnson, 2019).

6.4 Case-Study 4: BitSight's

At the global level, organisations have experienced a significant level of expansion within their network with third-party. One such organisation is Schneider Electric, i.e., known as the global leader within the industrial automation and energy management sector. For third-party-oriented cyber-risk determination and management, this organisation decided to make use of BitSight. The case study provided evidence that BitSight offered trustworthy information as well as analytics for examining the cybersecurity hygiene and postures of the partners. It is evaluated that with the support of BitSight, Schneider Electric also became capable of measuring supplier-cyber-program's success through reports that are easy to read. BitSight also detected risk-driven interactions with suppliers for the organisation to continually enhance this aspect (BitSight Technologies, Inc, 2022).

Further, BitSight also enabled sharing of a single platform with organisational suppliers for remediating the predictable risks. While making business expansion, monitoring of the highly critical types of suppliers by the use of actionable and trusted security scores supported the organisation to proactively minimise the level of risk; however, it could not be sufficient in case the organisational team did not focus on remediation. The advisors of BitSight alerted the organisation while the scores of critical suppliers got dropped, and the vectors of risks got triggered. Without much effort in extending resources and needing to provide training to the team, supply-chain risks could be well managed by BitSight for Schneider Electric. It is analysed that the collaborative and proactive input from BitSight Advisors raised alerts among the organisational team regarding supply-chain security risk, and during the occurrence of the alerts, the organisation has become capable of informing about risks and providing access to the suppliers to the platform of BitSight for supporting them to adequately minimise the risks across the business's value-chain (BitSight Technologies, Inc, 2022).

6.5 Discussion

It is discussed by referring to the research findings that in the current security industry, there are multiple security analysis tools that work on automation and optimised technologies to reduce efforts and time in threat assessment coverage for the organisations. To support the initial objective, four cases of BitSight, Black Kite, WPScan, and Security Scorecard have been investigated. After investigating these cases, in line with the second research objective, it is found that WPScan has efficiency in automatically evaluating and determining multiple ranges of security risks in the web applications by conducting internal and external level analysis

(Acunetix, 2022). This tool is free of cost and ensures saving of time and effort in determining security threats for the organisations to timely respond to them (WPScan, 2022). Furthermore, in the direction of the second objective of the research, which is aimed at exploring the efficiency levels of the automated as well as optimised tools of security analysis, it is discussed that the security tool named Vulnerability Software Identifier (VSI) provided by the company Black Kite is capable of performing the impact analysis related to the vendor. In addition to the above, the VSI tool is also highly effective towards performing descriptive monitoring of the probability of risks along with the impact that can be generated by cyber threat-oriented incidents. It is further supported by the case that the VSI system of the Black Kite is efficient in terms of highlighting the high impact and high-risk causing vendors in order to reduce the occurrence of cyber threats (Black Kite, 2022). BitSight is also noted to be a paid-for efficient security analysis tool that helps organisations to identify supply-chain-related risks, as identified in the case study of Schneider Electric (BitSight Technologies, Inc, 2022). The awareness generated regarding predictive risks by BitSight helps organisations to take significant action for reducing and eliminating security risks with a proactive approach and strong team collaboration.

However, in alignment with the third objective, the issue is also identified that security analysis tools like WPScan lacks the provision of rich reporting because it sometimes fails to denote the importance of focusing on certain vulnerabilities by the organisations. Further, prompt updates in this tool are also needed, and it might be complex to determine all the vulnerabilities in single usage (Johnson, 2019).

Further, in regard to BitSight, Black Kite and Security Scorecards, the literature also determined that for their successful usage, certain skills like functional testing skills, error-assessment skills, technical skills, quality management skills, and analytical skills are highly required (Black Kite, 2022; ISACA.org, 2018; Chatterjee, 2020; WPScan, 2022). Thus, overall, it is discussed that security analysis tools are efficient enough to reduce efforts and time for detecting threats in the threat-assessment coverage; however, constant updates requirement, skill requirement, the gap in rich reporting, and optimal usage of these tools are yet to be achieved.

7 Conclusion and Future Work

7.1 Conclusion

It is concluded for supporting the first and second research objectives that BitSight and WPScan have efficacy in determining supply-chain threats and web-applications vulnerabilities in a proficient manner with reduced time and effort because of automation and high optimisation of technology. It is also summarised that the Black Kite has improved the identification of the threat-generating vendors of Cisco by the introduction of the VIS system, which assigns high-impact and high-risk probabilities to its vendors. Moreover, the organisations such as SecurityScorecard have helped financial companies like Modulr to perform accurate cyber-security reviews. However, to support the third objective, it is also noted that issues regarding poor reporting, technical skill requirements, involved expenses, and constant updates needs reflect the downside of these security analysis tools.

7.2 Future Work

- In future studies, interviews with security analysis tool provider organisations' managers can be conducted to attain expert insight into the utility and applications of these tools (Bell, Bryman, and Harley, 2022).
- Surveys with security analysis tool user organisations can also be organised to have bias-free findings around the efficacy of these tools (Bougie and Sekaran, 2019).

7.3 Recommendations

- Security analysis tools should be improvised by adding cloud-security solutions for exploring wider vulnerabilities and offering rich reporting around vulnerabilities for organisations (Wei, Peng, and Liu, 2020).
- Security analysts should be offered proper training to gain skills in security analysis tools for successfully executing the threat assessment process (Kim *et al.,* 2021).
- Constant updating of these tools must be carried out to detect new types of vulnerabilities prevalent in organisations in a time of growing cyber-crimes (Abdiyeva-Aliyeva & Hematyar, 2022).

References

Abdiyeva-Aliyeva, G. and Hematyar, M. (2022). Statistic Approached Dynamically Detecting Security Threats and Updating a Signature-Based Intrusion Detection System's Database in NGN. Journal of Advances in Information Technology 13(5).

Acunetix. (2022). Major bank: Acunetix lets us scan many applications automatically. Available at: https://www.acunetix.com/case-studies/major-bank-acunetix-lets-us-scan-many-applications-automatically/ [Accessed on: 11 November 2022].

Acunetix. (2022) a. WordPress Security. Available at: https://www.acunetix.com/vulnerability-scanner/wordpress-security-scan/ [Accessed on: 11 November 2022].

Alalfi, M.H., Parveen, S. and Nazzal, B. (2022). A mutation framework for evaluating security analysis tools in IoT applications. Software Testing, Verification and Reliability 32(7), p.e1799.

Bell, E., Bryman, A. and Harley, B. (2022). Business research methods. Oxford university press.

Bernard, A. (2022). Black Kite: The cost of data breach averages $15 million. Available at: https://www.techrepublic.com/article/black-kite-cost-of-data-breach-averages-15-million/ [Accessed on: 11 November 2022].

BitSight Technologies Inc. (2022). Cybersecurity Report: Protecting the organisation with cybersecurity reports. Available at: https://www.bitsight.com/glossary/cybersecurity-report [Accessed on: 11 November 2022].

BitSight Technologies, Inc. (2022). Collaborating to manage vendor risk with BitSight Advisors. Available at: https://www.bitsight.com/resources/schneider-electric [Accessed on: 11 November 2022].

Black Kite. (2022). As Agile as the Adversary. Available at: https://blackkite.com/ [Accessed on: 11 November 2022].

Black Kite. (2022). CISCO CONFIRMS ATTACK BY RANSOMWARE GANG: HOW IS THE SUPPLY CHAIN AFFECTED?. Available at: https://blackkite.com/cisco-confirms-attack-by-ransomware-gang-how-is-the-supply-chain-affected/ [Accessed on: 12 November 2022].

Black Kite. (2022). Third Party Risk Intelligence. Available at: https://blackkite.com/platform/#financial-platform [Accessed on: 11 November 2022].

Black Kite. (2022) a. 360° VISIBILITY INTO THE WILD. Available at: https://blackkite.com/ [Accessed on: 11 November 2022].

Black Kite. (2022) a. STANDARDS-BASED METHODOLOGY, TRANSPARENT GRADING. Available at: https://blackkite.com/black-kites-methodology/ [Accessed on: 11 November 2022].

Bougie, R. and Sekaran, U. (2019). Research methods for business: A skill building approach. John Wiley & Sons.

Britton, A. (2022). 2022 Release Changelog. Available at: https://support.securityscorecard.com/hc/en-us/articles/4414543934363-2022-Release-Changelog [Accessed on: 11 November 2022].

Bugcrowd. (2022). WPScan Security Scanner. Available at: https://www.bugcrowd.com/glossary/wpscan-security-scanner/ [Accessed on: 11 November 2022].

Cayirci, E., Garaga, A., Santana de Oliveira, A. and Roudier, Y. (2016). A risk assessment model for selecting cloud service providers. Journal of Cloud Computing 5(1), pp.1-12.

Chatterjee, S. (2020). Top 15 Software Testing Trends to Watch Out in 2021. Available at: https://shormistha4.medium.com/top-15-software-testing-trends-to-watch-out-in-2021-ef4ecca3dc09 [Accessed on: 11 November 2022].

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. and Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. Computers & security 56, pp.1-27.

Crowdstrike Store. (2022). SecurityScorecard Cyber Risk Ratings. Available at: https://store.crowdstrike.com/apps/securityscorecard-cyber-risk-ratings [Accessed on: 11 November 2022].

Feist, J., Grieco, G. and Groce, A. (2019). Slither: a static analysis framework for smart contracts. In 2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB), pp. 8-15.

Higuera, J.R.B., Higuera, J.B., Montalvo, J.A.S., Villalba, J.C. and Pérez, J.J.N. (2020). Benchmarking approach to compare web applications static analysis tools detecting OWASP top ten security vulnerabilities. Comput. Mater. Continua 64(3), pp.1555-1577.

ISACA.org. (2018). ISACA and SecurityScorecard Define Critical Questions to Implement Continuous Assurance for Data. Available at: https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2018/isaca-and-securityscorecard-define-critical-questions-to-implement-continuous-assurance-for-data [Accessed on: 11 November 2022].

Ismagilova, E., Hughes, L., Rana, N.P. and Dwivedi, Y.K. (2022). Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. Information Systems Frontiers 24(2), pp. 393-414.

Johnson, D. (2019). How Often Should You Run a WordPress Security Scan?. Available at: https://www.bluehost.com/resources/how-often-should-you-run-a-wordpress-security-scan/ [Accessed on: 11 November 2022].

Kim, B.G., Cho, Y.S., Kim, S.H., Kim, H. and Woo, S.S. (2021). A security analysis of blockchain-based did services. IEEE Access 9, pp. 22894-22913.

Kintis, M., Papadakis, M., Papadopoulos, A., Valvis, E., Malevris, N. and Le Traon, Y. (2018). How effective are mutation testing tools? An empirical analysis of Java mutation testing tools with manual analysis and real faults. Empirical Software Engineering 23(4), pp.2426-2463.

Le, B.D., Wang, G., Nasim, M. and Babar, A. (2019). Gathering cyber threat intelligence from Twitter using novelty classification. arXiv preprint arXiv:1907.01755, pp. 1-8.

Lee, J. and Lee, K. (2018). Spillover effect of ransomware: economic analysis of web vulnerability market. Res Brief Inform Commun Technol Evol 3(20), pp. 1-11.

Loise, T., Devroey, X., Perrouin, G., Papadakis, M. and Heymans, P. (2017). Towards security-aware mutation testing. In 2017 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), pp. 97-102.

Macher, G., Armengaud, E., Brenner, E. and Kreiner, C. (2016). A review of threat analysis and risk assessment methods in the automotive context. In International Conference on Computer Safety, Reliability, and Security, pp. 130-141.

Maseda, F.J., López, I., Martija, I., Alkorta, P., Garrido, A.J. and Garrido, I. (2021). Sensors data analysis in supervisory control and data acquisition (SCADA) systems to foresee failures with an undetermined origin. Sensors 21(8), p.2762.

Pazos, J.C., Legare, J.S., Beschastnikh, I. and Aiello, W. (2020). Precise XSS detection and mitigation with Client-side Templates. arXiv preprint arXiv:2005.07826, pp. 1-15.

Praitheeshan, P., Pan, L., Yu, J., Liu, J. and Doss, R. (2019). Security analysis methods on ethereum smart contract vulnerabilities: a survey. arXiv preprint arXiv:1908.08605, pp. 1-21.

Security Scorecard. (2022). Trust begins with transparency. Available at: https://securityscorecard.com/trust [Accessed on: 11 November 2022].

SecurityScorecard Inc. (2022). CASE STUDY Modulr. Available at: https://securityscorecard.pathfactory.com/customer-reviews/case-study-modulr-se [Accessed on: 12 November 2022].

Shi, A., Bell, J. and Marinov, D. (2019). Mitigating the effects of flaky tests on mutation testing. In Proceedings of the 28th ACM SIGSOFT International Symposium on Software Testing and Analysis, pp. 112-122.

Slashdot Media. (2022). Black Kite Reviews. Available at: https://slashdot.org/software/p/Black-Kite/ [Accessed on: 11 November 2022].

Snowflake Inc. (2022). SECURITYSCORECARD: CYBERSECURITY RATINGS BY DOMAIN. Available at: https://www.snowflake.com/datasets/securityscorecard-cybersecurity-ratings-by-domain/ [Accessed on: 11 November 2022].

To, A.T. and Trinh, T.H.M. (2021). Understanding behavioral intention to use mobile wallets in vietnam: Extending the tam model with trust and enjoyment. Cogent Business & Management 8(1), p. 1891661.

UG. (2022). Black Kite vs SecurityScorecard Comparison. Available at: https://www.upguard.com/compare/black-kite-vs-securityscorecard [Accessed on: 11 November 2022].

Upguard. (2022). BitSight vs SecurityScorecard 2022 Comparison and Review. . Available at: https://www.upguard.com/compare/bitsight-vs-securityscorecard#:~:text=is%20not%20available.-,Reports%20say%20pricing%20starts%20at%20%2416%2C500%20for%20self%2Dassessment%20plus,seeking%20greater%20security%20ratings%20extensibility. [Accessed on: 11 November 2022].

Waheed, N., He, X., Ikram, M., Usman, M., Hashmi, S.S. and Usman, M. (2020). Security and privacy in IoT using machine learning and blockchain: Threats and countermeasures. ACM Computing Surveys (CSUR) 53(6), pp. 1-37.

Wangen, G., Hallstensen, C. and Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness. International Journal of Information Security 17(6), pp.681-699.

Wei, Y., Peng, M. and Liu, Y. (2020). Intent-based networks for 6G: Insights and challenges. Digital Communications and Networks 6(3), pp. 270-280.

WPScan. (2021). 2021 Mid-Year WordPress Security Report. Available at: https://wpscan.com/2021-Mid-Year-WordPress-Security-Report.pdf [Accessed on: 11 November 2022].

WPScan. (2022). WPScan WordPress Security Scanner. Available at: https://wpscan.com/wordpress-security-scanner [Accessed on: 11 November 2022].

Wpsec.com. (2022). IS YOUR WORDPRESS WEBSITE PROTECTED AGAINST ATTACKERS?. . Available at: https://wpsec.com/ [Accessed on: 11 November 2022].