https://revistas.ucr.ac.cr/index.php/ingenieria/index
www.ucr.ac.cr / ISSN: 2215-2652

Ingeniería

Revista de la Universidad de Costa Rica

ENERO/JUNIO 2025 - VOLUMEN 35 (1)

EDITORIAL UCR

Ingeniería. Revista de la Universidad de Costa Rica

Vol. 35, No. 1: 11-23, Enero-Junio, 2025. ISSN: 2215-2652. San José, Costa Rica

Ingeniería Eléctrica

A Comprehensive Analysis of Cybersecurity Infrastructure in Academic Environments

Un análisis integral de la infraestructura de ciberseguridad en ambientes académicos

Holger Santillán [1,2], *Julio Andrés Arévalo Satán* [3], *Peregrina Wong* [4]

[1] *Universidad Politécnica Salesiana, Grupo de Investigación en Sistemas de Telecomunicaciones – GISTEL, Guayaquil, Ecuador, correo: hsantillan@ups.edu.ec*

[2] *Universidad de las Palmas de Gran Canaria, Las Palmas de Gran Canaria, Spain, correo: holger.santillan101@alu.ulpgc.es*

[3] *Universidad Politécnica Salesiana, Grupo de Investigación en Sistemas de Telecomunicaciones – GISTEL, Guayaquil, Ecuador, correo: jarevalos5@est.ups.edu.ec*

[4] *Universidad de las Palmas de Gran Canaria, Las Palmas de Gran Canaria, Spain, correo: peregrina.wong101@alu.ulpgc.es*

Keywords:

Cybersecurity, Kali Linux, Nessus, phishing, vulnerabilities.

Abstract

This paper addresses a comprehensive analysis of cybersecurity systems in academic environments taking as a case study the domains: “www.ups.edu.ec”, “cas.ups.edu.ec”, “virtual.ups.edu.ec” y “dspace.ups.edu.ec”, of the Salesian Polytechnic University, using specialized tools such as Kali Linux and Nessus. Through these technologies, critical aspects of the system’s security are evaluated: its ability to resist attacks, how effective its defense mechanisms are, and its capacity to identify exploitable weak points. A novel methodology is applied to evaluate the security of the system, using emerging technologies and innovative techniques.

During the research, several vulnerabilities were identified covering the four studied domains. These were classified using the CVSS (Common Vulnerability Scoring System) rating protocol, which allowed the most critical ones to be prioritized and addressed first. In addition, a scan of open ports was performed to recognize possible unauthorized access points. As part of the security testing, a simulation of an email phishing attack was carried out by cloning the Salesian University access website, in order to assess users’ susceptibility to this threat.

Domain security analysis revealed critical vulnerabilities, including an outdated version of PHP and possible remote code execution (CVSS 9.8-10) in “virtual.ups.edu.ec”. SSL/TLS security issues were also detected, such as the use of weak ciphers and outdated versions of TLS (CVSS up to 7.5). In addition, medium risks related to lack of HSTS and vulnerabilities in PHP and jQuery were found, along with weaker SSH configurations of lesser impact (CVSS 2.6-3.7). These results show the need for security updates and improvements.

Recibido: *21/05/2024*
Aceptado: *23/08/2024*

Palabras Clave:

Kali Linux, Nessus, phishing, seguridad cibernética, vulnerabilidades

Resumen

This paper addresses a comprehensive analysis of cybersecurity systems in academic environments taking as a case study the domains: “www.ups.edu.ec”, “cas.ups.edu.ec”, “virtual.ups.edu.ec” y “dspace.ups.edu.ec”, of the Salesian Polytechnic University, using specialized tools such as Kali Linux and Nessus. Through these technologies, critical aspects of the system’s security are evaluated: its ability to resist attacks, how effective its defense mechanisms are, and its capacity to identify exploitable weak points. A novel methodology is applied to evaluate the security of the system, using emerging technologies and innovative techniques.

During the research, several vulnerabilities were identified covering the four studied domains. These were classified using the CVSS (Common Vulnerability Scoring System) rating protocol, which allowed the most critical ones to be prioritized and addressed first. In addition, a scan of open ports was performed to recognize possible unauthorized access points. As part of the security testing, a simulation of an email phishing attack was carried out by cloning the Salesian University access website, in order to assess users’ susceptibility to this threat.

Domain security analysis revealed critical vulnerabilities, including an outdated version of PHP and possible remote code execution (CVSS 9.8-10) in “virtual.ups.edu.ec”. SSL/TLS security issues were also detected, such as the use of weak ciphers and outdated versions of TLS (CVSS up to 7.5). In addition, medium risks related to lack of HSTS and vulnerabilities in PHP and jQuery were found, along with weaker SSH configurations of lesser impact (CVSS 2.6-3.7). These results show the need for security updates and improvements.

DOI: 10.15517/ri.v35i1.60075

I. INTRODUCTION

Educational centers manage the education and training of new professionals worldwide, and they must keep the integrity of user information safe and protected from cybersecurity attacks in their academic environments. Therefore, this paper aims to analyze the cybersecurity vulnerabilities and threats presented by a laboratory environment in an educational setting, as well as the security measures to be implemented. The results of the analysis will be used to propose recommendations to improve security in a virtual laboratory environment.

Specifically, this study evaluates the cybersecurity systems in academic environments taking as a case study the laboratories of the Salesian Polytechnic University (Universidad Politécnica Salesiana: UPS) in its four main websites, showing vulnerabilities and threats found using the Kali Linux operating system and the tools Nessus and Mozilla Observatory [1].

The choice of Kali Linux in the cybersecurity arena is underpinned by its reputation as a highly specialized operating system, backed by a wide range of integrated tools that have been specifically developed to perform comprehensive penetration testing and thorough security analysis [2]. This platform has set up itself as an industry standard due to its ability to address the unique challenges faced by cybersecurity professionals and technicians, offering a combination of versatility and effectiveness in detecting and mitigating vulnerabilities [3]. Its use is also justified by its specialization and integrated toolset for penetration testing and security analysis. It provides a stable and reliable platform for activities such as vulnerability assessment, security audits, and penetration testing, offering indispensable resources for professionals in this field [4].

In addition, Nessus is a widely used tool in the field of cybersecurity, it stands out in this field for its comprehensive ability to detect vulnerabilities in systems and networks, covering even those very simple technical situations that could be exploited by malicious attackers, thanks to its ability to schedule scans and the generation of detailed reports on the events found in the study scenario [5]. Its advanced features, such as scan scheduling and detailed report generation, make it a versatile and powerful tool [6].

Additionally, Mozilla Observatory, with its specialized focus on the web and its ability to detect and counteract a wide range of threats, is positioned as an indispensable tool to protect sensitive user information, essential in identifying vulnerabilities in websites by providing real-time analysis and recommendations to strengthen the security of the problems found during the analysis of vulnerabilities [7]. Its web-oriented approach and its ability to show and mitigate threats make it a valuable tool for protecting users' information [8].

These network and web monitoring tools have proven to be highly effective and widely recognized in the field of cybersecurity, which has given them a solid reputation due to their ability to identify and assess vulnerabilities in systems and networks with accuracy and reliability. This is why these tools (Kali Linux, Nessus, and Mozilla Observatory) are essential for the development of this project. The efficiency, familiarity, and experience of the user community with these tools guarantee an effective implementation and a correct interpretation of the results obtained, which contributes to the credibility and validity of the research findings [9].

The choice to use exclusively the tools implemented in this work for the vulnerability scanning study is based on various key factors. These tools have proven to be highly effective and recognized in the cybersecurity field. Also, by limiting the scope to these specific tools, consistency and comparability of the results obtained are ensured, easing an accurate assessment of the effectiveness of the scanning techniques used [10].

That being said, the exponential increase in security attacks is having a considerable impact on today's systems, potentially triggering dangerous consequences. In this context, penetration testing appears as a crucial solution to mitigate the effect of such attacks. Therefore, the main purpose of this article is to detail both the technical and non-technical aspects of penetration testing [11].

In today's era of increasing digitalization, information is available to everyone through computing and mobile devices. This advancement has introduced useful and efficient technologies and services into everyday life, such as web applications, cloud computing, online communication platforms, and e-commerce, among others. While a handful of users access this information with legitimate intentions, others seek ways to gain unauthorized access to destroy or steal valuable data, either from a website or from a physical environment. It is commonly known that the term "penetration testing" also refers to "ethical hacking" [12].

In contemporary society, where every interaction, conversation, and transaction can be checked, found, and analyzed, there is a growing concern for security, especially about the concept of ethical hacking. Despite the benefits brought by the digital era, it has also led to unintended consequences, such as the increase of hacking incidents in social networks, bank accounts, and data theft, among others, which supports the methods and analysis tools chosen in this study [13].

For a better understanding of cybersecurity concepts, it is important to note the following concepts.

Cybersecurity in Web Systems

Cybersecurity refers to the protection of computer systems, networks, and data against attacks, damage, or unauthorized access. In the context of web systems, this includes defending against threats that can compromise the integrity, confidentiality, and availability of online services [14].

Vulnerability Management

The ongoing process of identifying, assessing, addressing, and reporting vulnerabilities in an organization's systems and applications. Its goal is to reduce the risk of exploitation of such vulnerabilities by malicious actors, ensuring that threats are mitigated before they can be exploited.

CVSS (Common Vulnerability Scoring System)

An open standard is used to assess the severity of vulnerabilities in software systems. CVSS provides a numerical score (from 0 to 10) that reflects the relative risk of a vulnerability, helping to prioritize corrective actions according to the threat level [15].

CVE (Common Vulnerabilities and Exposures)

A list of public references that uniquely find known vulnerabilities in software and hardware. Each CVE is associated with a unique identifier and is used to document and communicate vulnerabilities, helping coordination between organizations to apply solutions.

Impact on the Availability of IT Resources

Failure to properly track and manage vulnerabilities can lead to the exploitation of critical flaws, resulting in the interruption of services, loss of data, and security compromises. This directly affects the availability of IT resources, as successful attacks can degrade or completely disable affected systems, negatively affecting operational continuity [15].

According to the Threat Metrix Cybercrime Report, the COVID-19 pandemic has highlighted the vulnerabilities of the digital space in Latin America and the Caribbean, where increased digital activity has made the region a hotspot for fraud, especially account creation. With millions of inexperienced users connecting to the Internet every year today with IoT applications, including those related to education, many of them without sufficient technological capabilities, the risk of cyberattacks has increased, making the region an important target and source of these attacks [16]. This growth in cyber threats has generated greater interest in cybersecurity, with a notable increase in searches and demand for courses and training on the subject, reflecting a growing awareness of the importance of protecting oneself in the digital environment [17].

Despite the lag in cybersecurity in Latin America and the Caribbean, the "Cybersecurity Report 2020" of the OAS (Organization of American States) and the IDB (Inter-American Development Bank) shows considerable progress in the last four years. The evaluation, based on 49 indicators, reveals that the region has improved its cybersecurity average to 39.88 points. Countries such as Brazil, Chile, Colombia, Uruguay, and Mexico stood out with notable advances. However, Mexico faced serious cyber incidents in 2019 and 2020, showing a lack of resilience to attacks, despite reported improvements. These events highlight the urgent need to strengthen cybersecurity capabilities in the region through a robust national strategy and ongoing training [18].

Individual country efforts in Latin America to develop cybersecurity policies and capabilities are based on metrics and reports from the OAS and IDB (2016; 2020). Where a static view of the cybersecurity context in the countries of the region is provided, the OAS and IDB reports offer a dynamic analysis of its evolution. The method covers twelve indicators that include the development of cybersecurity policies, the protection of essential services, and the response to cyber incidents. Among these, eight are related to national security and foreign policy. Despite improvements in areas such as anti-cybercrime legislation and cyber incident response capabilities, significant challenges remain, as evidenced by some countries' low scores in developing critical cyber capabilities [19].

Types of confidential information in a virtual education environment:

1. personal information: personal data of students/ collaborators (ID, home address, family references, health);
2. financial information: financial data such as payment methods, and credit/debit cards;
3. educational information: assignments, projects, academic history.

This information can be useful for attackers, who could use it to impersonate identities, commit financial fraud, and cause damage in the educational field. That is why this study evaluates the cybersecurity of the main websites of the study case to detect and examine vulnerabilities and threats.

2. MATERIALS AND METHODS

This study will consider the analysis as a case study of the Salesian Polytechnic University (UPS), which, according to the Rector's Accountability Report for the year 2023, has an enrollment of 24 776 students, of which 7 103 belong to degree programs at the Guayaquil campus. With this student population, the substantial amount of data managed by the university is evident, covering the personal information of students, digital repositories of projects and academic documents, grade histories, as well as financial and legal aspects linked to the corresponding department of the UPS.

The laboratories of the Salesian Polytechnic University are a critical environment where confidential information is handled, therefore, these laboratories must have security measures to protect students from cyberattacks and malicious people looking to steal their credentials. It is also important to mention that this is a quantitative and descriptive study, because the variables to be examined are vulnerabilities.

Domains to be audited

This analysis is based on recognizing and finding security breaches in the laboratory environment of an educational center, where students use the university's website to access their virtual environment (AVAC), so the case study domains to be audited are set up. These domains are presented below:

1. "www.ups.edu.ec": It is the official website of the Salesian University; therefore, it is a page regularly visited by

students who wish to know their grades, make applications, visit the virtual library, and enter the AVAC.

2. "cas.ups.edu.ec": The acronym "CAS" is associated with "Central Authentication Service," which is a protocol used for user authentication. Therefore, this domain provides access to an authentication system for students to access the university's online services.
3. "virtual.ups.edu.ec": The term "virtual" refers to a virtual environment used by UPS to provide study materials, discussion forums, and educational resources that complement students' studies.
4. "dspace.ups.edu.ec": The term "dspace" denotes the existence of a digital content management platform called DSpace which is an application designed to manage and preserve digital repositories. UPS uses this domain to store digital content such as scientific articles, theses, academic papers, research, and other resources [20].

In the context of vulnerability scanning with Nessus, each scale value stands for the level of risk associated with an identified vulnerability, in terms of its potential impact. These are the values:

1. *Critical.* These vulnerabilities are an extremely elevated risk, allowing remote code execution or full control of the affected system without prior authentication. They are a priority for immediate remediation.
2. *High.* Vulnerabilities that can be exploited to cause significant impact, such as access to sensitive data or service interruption. Their exploitation is relatively straightforward, and their impact is considerable, making them a high priority for mitigation [21].
3. *Medium.* These vulnerabilities can be exploited, but generally require more specific conditions or a higher level of access to the system. Although their impact is lower compared to the earlier ones, they can be used in conjunction with other vulnerabilities to increase the overall risk.
4. *Low.* Vulnerabilities that present a minimal risk, with limited impact, and are difficult to exploit. Although their resolution is less urgent, it is still important to improve the overall security of the system [21].

In addition, for the development of this exploration process, we have the following arguments to consider these tools as part of the method in this research. Both Kali Linux and Nessus are widely recognized and used tools in the cybersecurity community and their use ensures that the analysis is based on tools that have been evaluated and confirmed by experts. Kali Linux offers an extensive range of pre-installed security tools, allowing for a comprehensive assessment of system security from multiple angles, including network, system, and application analysis. Nessus, on the other hand, is known for its ability to find vulnerabilities at the software and configuration level with comprehensive coverage, ranging from server configuration flaws to specific application vulnerabilities [22].

Both tools are regularly updated to include the latest techniques and vulnerability definitions. Kali Linux is highly configurable and can be customized to suit the specific needs of the study, allowing the execution of custom scripts or the integration of new scanning tools. Also, Nessus offers flexibility through customized scanning policies, allowing detailed analysis according to the specific environment being assessed [23].

To evaluate the effectiveness of the tools used, a method structured in four phases will be followed: planning, data collection, data analysis, and presentation of results, as detailed below.

A) Planning Phase

The planning phase of the vulnerability analysis system involves the following activities:

1. *Gathering of information on the case of analysis:*

During this stage, a comprehensive collection of relevant information about the Salesian Polytechnic University (UPS) is conducted. This includes data on the technological infrastructure, computer systems, networks, web applications, and any other relevant information that may influence the security of the organization.

2. *Tools and Techniques Selection:*

In this activity, the most proper tools and techniques are selected to analyze vulnerabilities in the UPS. This involves evaluating different options available on the market, considering factors such as the specialization of the tools, their compatibility with the UPS environment, and their ability to find a wide range of vulnerabilities.

B) Data Collection Phase

The data collection phase of the vulnerability analysis system involves conducting the following activities:

1. *Identification of Open Ports in the Case Study Systems:*

During this stage, a comprehensive scan of Salesian Polytechnic University (UPS) systems is performed to name open ports and associated services. This provides an overview of the attack surface and helps detect potential entry points for malicious attacks.

2. *Vulnerability Assessment of Institutional Websites:*

In this activity, a detailed assessment of the vulnerabilities present in UPS institutional websites is conducted. This includes the search for common vulnerabilities, such as SQL injections, XSS (Cross-Site Scripting) vulnerabilities, and other possible points of exploitation that may compromise the security of the websites.

3. *Analysis of Private Documentation and its Exposure:*

During this stage, private UPS documentation is analyzed to show potential exposure to confidential information. This may include documents stored on internal servers, shared file repositories, or any other location where sensitive information may be stored and potentially exposed to unauthorized access.

4. *Identification of Vulnerabilities that Have Allowed Unauthorized Access:*

In this activity, vulnerabilities that have allowed unauthorized access to UPS systems are investigated and documented. This includes analyzing earlier security incidents, identifying the root causes of the attacks, and recommending corrective actions to prevent future intrusions.

C) Data Analysis Phase

The data analysis phase of the vulnerability analysis system involves conducting the following activities:

1. *Processing and Analysis of the Collected Data:*

The information gathered during the earlier phase is processed and analyzed during this stage. This may include the review of scan logs, penetration test results, and vulnerability analysis reports, among others. The goal is to show significant patterns, trends, and findings that help to understand the current security posture and possible areas for improvement.

2. *Identification and Classification of Vulnerabilities and Threats:*

In this activity, vulnerabilities and threats detected during the information analysis are found and classified. This involves categorizing vulnerabilities according to their type, severity level, and potential impact on the security of the organization's systems and networks.

3. *Evaluation of the Severity of the Vulnerabilities Detected:*

During this stage, the severity of the vulnerabilities detected is assessed using predefined criteria, such as CVSS (Common Vulnerability Scoring System) or other industry standards. This allows for prioritizing mitigation actions and distributing resources efficiently to address the most critical and urgent vulnerabilities. In addition, specific recommendations are provided to remediate each identified vulnerability and improve the overall security posture of the organization.

D) Presentation of Results Phase

The presentation of results phase of the vulnerability analysis system includes the following activities:

1. *Presentation of Research Results:*

During this stage, the results obtained during the vulnerability analysis are presented clearly and concisely. This includes details on the vulnerabilities found, their severity, the systems or areas affected, and any other relevant findings. Graphs, tables, and other visual resources are used to help the understanding of the information by stakeholders.

2. *Detailed Discussion on the Implications of the Vulnerabilities:*

In this activity, a thorough discussion is conducted on the implications of the vulnerabilities detected in the case study of the Salesian Polytechnic University. The potential impact of these vulnerabilities on the security of UPS systems and networks, as well as on the integrity and confidentiality of sensitive information, is analyzed.

3. *UPS Cybersecurity Mitigation and Enhancement Proposals:*

During this stage, concrete proposals are presented to mitigate the identified vulnerabilities and improve cybersecurity at UPS. These recommendations include implementing security patches, updating network configurations, access policies, and personnel training, among other measures.

The summary of the method proposed for this work is presented in TABLE I below.

TABLE I
PROJECT METHOD

VULNERABILITY ANALYSIS IN AN EDUCATIONAL ENVIRONMENT	
SECTIONS	ACTIVITIES
Planning Phase	• Gathering Information on the UPS. • Choice of Tools and Techniques.
Data Collection Phase	• Identification of Open Ports in UPS Systems. • Evaluation of Vulnerabilities in Institutional Web Sites. • Analysis of Private Documentation and its Exposure. • Identification of Vulnerabilities that have allowed unauthorized access.
Data Analysis Phase:	• Processing and Analysis of Collected Information. • Identification and Classification of Vulnerabilities and Threats. • Evaluation of the Severity of the Vulnerabilities Detected.
Results Presentation Phase	• Presentation of the Research Results. • Detailed discussion on the Implications of Vulnerabilities. • Proposals for Mitigation and Improvement of Cybersecurity at UPS.

Evaluation model for security posture

The current work presents a vulnerability scan, based on the robustness and versatility of the Kali Linux operating system, combined with the use of recognized tools such as Nessus and Mozilla Observatory.

This comprehensive solution is proposed as an effective method to conduct an exhaustive security assessment of systems and websites. Through this combination of tools, the prototype provides a detailed and comprehensive view of potential risks, as well as recommendations to strengthen the security posture of the assessed infrastructures. This approach provides an initiative-taking strategy to mitigate risks and ensure the protection of critical information assets in increasingly complex and dynamic technology environments.

The flowchart of the analysis prototype is as follows, shown in Fig. 1.

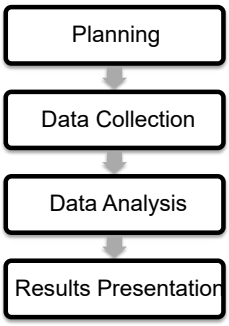

Fig. 1. Prototype flow diagram.

The tools used and the process for performing the vulnerability scan are described below.

Mozilla Observatory Scanning

This study incorporates a comprehensive approach to analyzing the security of a specific domain, using the Mozilla Observatory tool. This tool, developed by Mozilla, has become a standard in the evaluation of a website's security configuration, providing a score based on digital security best practices.

The security assessment using Mozilla Observatory offers a detailed view of the robustness of the security practices implemented in the domains "ups.edu.ec", "virtual.ups.edu.ec", "dspace.ups.edu.ec", and "cas.ups.edu.ec". The rating obtained is based on multiple aspects, including HTTPS configuration, implementation of content security policies (CSP), and management of security headers, among others.

Vulnerability Scanning with Nessus

Nessus is a flexible tool widely used in cybersecurity due to its ability to detect vulnerabilities in systems and networks. Scan scheduling and report generation features are among its advanced functions [24].This tool offers a vulnerability report based on the CVSS (Common Vulnerability Scoring System) standard providing a numerical score standing for the severity of a vulnerability on a scale from 0 to 10, where 0 shows a non-critical vulnerability and 10 indicates a critical vulnerability [24]. Nessus was used to scan for vulnerabilities in the web "pages ups.edu.ec" and "virtual.ups.edu.ec" with IP addresses 45.235.140.7 and 34.231.199.89, respectively.

Credential Theft Using Social Engineering and Phishing Techniques

Phishing can take various forms, from fraudulent emails to fake websites, and its impact on digital security is undeniable, affecting individuals, organizations, and educational institutions alike [25].Social Engineering Attacks are techniques used to trick people into revealing confidential information. In this case, these techniques are used to obtain access credentials to the UPS website [26].For this section, cloning of the UPS credentials access website is conducted, as well as spoofing and phishing techniques to send institutional emails with malicious content. This process is performed with the Kali Linux operating system and the Toolkit tool.

3. RESULTS ANALYSIS

A) Vulnerability Analysis and Reporting with Nessus

First, Nessus is used to scan for vulnerabilities on the website "www.ups.edu.ec", with IP address 45.235.140.7. At the end of the scan, Nessus provides a detailed report of the results, as shown in Fig. 2, from which we obtain: 1 high vulnerability (High), 3 medium vulnerabilities (Medium), and 37 recommendations (Info).

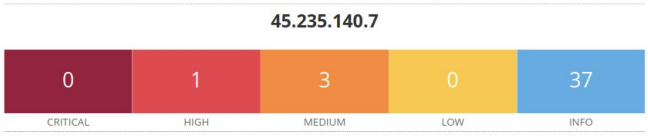

Fig. 2. Vulnerabilities in "ups.edu.ec".

The second site analyzed is "virtual.ups.edu.ec". Then, the scan is performed on the address "virtual.ups.edu.ec", with IP address 34.231.199.89. Once the scan is done, the Nessus report details the following: 2 critical vulnerabilities (Critical), 2 high vulnerabilities (High), 5 medium vulnerabilities (Medium), 2 low vulnerabilities (Low), and 40 recommendations (Info), as shown in Fig. 3.

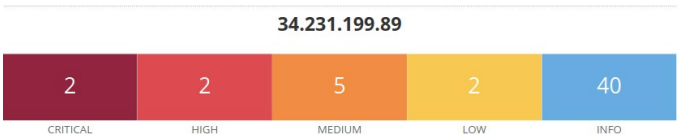

Fig. 3. Vulnerabilities in "virtual.ups.edu.ec".

TABLE II below presents a detailed summary of the vulnerabilities named and classified according to the CVSS scoring system, based on their criticality and potential risk.

TABLE II
NESSUS VULNERABILITIES RESULT

Danger level	Domain	Vulnerability	CVSS
Critic	virtual.ups.edu.ec	PHP Unsupported Version Detection.	10
Critic	virtual.ups.edu.ec	PHP Remote Code Execution (CVE-<version>).	9.8
High	ups.edu.ec y virtual.ups.edu.ec	SSL Medium Strength Cipher Suites Supported (SWEET32).	7.5
High	virtual.ups.edu.ec	PHP Multiple Vulnerabilities (CVE-<version>).	7.5
Medium	virtual.ups.edu.ec	HSTS Missing from HTTPS Server.	6.5
Medium	virtual.ups.edu.ec y ups.edu.ec	TLS Version 1.0/1.1 Protocol Detection and Deprecation.	6.5
Medium	virtual.ups.edu.ec	JQuery Multiple XSS (CVE-<version>).	6.1
Medium	virtual.ups.edu.ec	PHP Email Header Injection (CVE-<version>).	5.3
Medium	ups.edu.ec	nginx Information Disclosure (CVE-<version>).	5.3
Low	virtual.ups.edu.ec	SSH Weak Key Exchange Algorithms Enabled.	3.7
Low	virtual.ups.edu.ec	SSH Server CBC Mode Ciphers Enabled.	2.6

B) Mozilla Observatory Scanning Results

In the interpretation of the results obtained from the analysis with Mozilla Observatory for the UPS domains, it is seen that several security aspects have been favorably addressed. The findings for each category are highlighted below.

1. *Favorable Results*

After conducting a thorough evaluation through Mozilla Observatory in the four main domains of the UPS, highly favorable results have been found, as detailed in TABLE III below.

TABLE III
FAVORABLE RESULTS OF THE SCAN WITH MOZILLA OBSERVATORY

Test	Domain	Evaluation
Cookies	• UPS.EDU.EC VIRTUAL.UPS.EDU.EC DSPACE.UPS.EDU.EC	The use of the Secure flag ensures that cookies are transmitted exclusively over secure connections, while the HTTP Only flag helps prevent scripting attacks, thus strengthening cookie protection [27].
Cross-origin Resource Sharing	• UPS.EDU.EC VIRTUAL.UPS.EDU.EC DSPACE.UPS.EDU.EC CAS.UPS.EDU.EC	Proper CORS configuration shows that content is not visible through files or resource-sharing headers between sources. This helps prevent security risks associated with cross-domain requests [28].
X-Content-Type-Options	• UPS.EDU.EC VIRTUAL.UPS.EDU.EC DSPACE.UPS.EDU.EC	The X-Content-Type-Options header is set to "no sniff", which helps prevent MIME sniffing attacks, ensuring that the browser interprets the content type correctly [29].

Test	Domain	Evaluation
X-XSS-Protection	• UPS.EDU.EC VIRTUAL.UPS.EDU.EC DSPACE.UPS.EDU.EC CAS.UPS.EDU.EC	The X-XSS-Protection value on "1" shows that the browser is configured to activate the anti-XSS filter, helping to prevent cross-site scripting attacks and protecting against possible malicious code injections [30].
X-Frame-Options	• DSPACE.UPS.EDU.EC	The presence of established X-Frame-Options such as SAMEORIGIN or DENY means that measures are taken to prevent clickjacking attacks by controlling how content is embedded in frames. This improves security by preventing possible manipulation of the user interface [31].
Redirection	• VIRTUAL.UPS.EDU.EC DSPACE.UPS.EDU.EC CAS.UPS.EDU.EC	The first redirection from HTTP to HTTPS on the same host, with the final destination being HTTPS, reflects good security practices. This measure helps to ensure secure connections and prevent possible attacks based on redirection manipulation [32].

TABLE IV
UNFAVORABLE RESULTS OF THE SCAN WITH MOZILLA OBSERVATORY

Evaluate	Domain	Evaluation
Content Security Policy	• UPS.EDU.EC VIRTUAL.UPS.EDU.EC • DSPACE.UPS.EDU.EC • CAS.UPS.EDU.EC	The absence or inadequate configuration of the Content Security Policy (CSP) could leave the site vulnerable to code injection attacks [33].
HTTP Strict Transport Security	• UPS.EDU.EC • VIRTUAL.UPS.EDU.EC • DSPACE.UPS.EDU.EC • CAS.UPS.EDU.EC	Failure to implement HTTP Strict Transport Security (HSTS) could leave the site exposed to downgrade and man-in-the-middle attacks [34].
Redirection	• UPS.EDU.EC	Improperly configured redirection can introduce vulnerabilities, especially if the first HTTP to HTTPS redirection is to a different host [34].
Subresource Integrity	• VIRTUAL.UPS.EDU.EC • DSPACE.UPS.EDU.EC	Failure to implement Subresource Integrity (SRI) leaves the site susceptible to security risks related to the integrity of the external resources [35].
X-Content-Type-Options	• CAS.UPS.EDU.EC	Incorrect configuration of the X-Content-Type-Options header can introduce security risks, allowing possible attacks based on content type manipulation [35].
X-Frame-Options	• CAS.UPS.EDU.EC	Lack of X-Frame-Options configuration or inadequate configuration may expose the site to clickjacking attacks [36].

The detailed interpretation of each favorable category highlights the strong security practices adopted in the assessed domains, providing a robust foundation for continued cyber security at Salesian Polytechnic University.

2. *Unfavorable Results*

After the exhaustive evaluation by Mozilla Observatory in the four main domains of the UPS, certain unfavorable aspects clearly require immediate attention to strengthen the security of the websites, as detailed in TABLE IV below.

The detailed interpretation of each unfavorable category offers valuable guidance to direct the necessary corrective actions and improve the safety posture of the assessed domains.

C) Credential Theft Using Social Engineering and Phishing Techniques

The term phishing derives from the similarity with fishing for confidential information using deception, presenting itself in multiple variants, from misleading emails to fake web pages affecting both individuals and organizations [18] .Social Engineering Attacks are techniques used to trick people into revealing confidential information. In this case, these techniques are used to obtain login credentials to the UPS website [19] .

1. *Website Cloning*

Kali Linux Tool Kit tool is used to perform cloning of the UPS credential authentication website. Website cloning is a simple and widely used practice by phishing attackers who use social engineering to cover up credential theft.

The next phase is to steal the access credentials to the university's digital sites, this process consists of a series of steps explained below:

a) Clone UPS website:

Using Tool Kit, the website "cas.ups.edu.ec" was cloned.

Fig. 4 shows a representation of the fake website compared to the original page of the case study. It is evident that it is the same

as the original website shown in Fig. 5, which, in a hypothetical attack on users of the website, would generate an intrusion to the access credentials and other sensitive data.

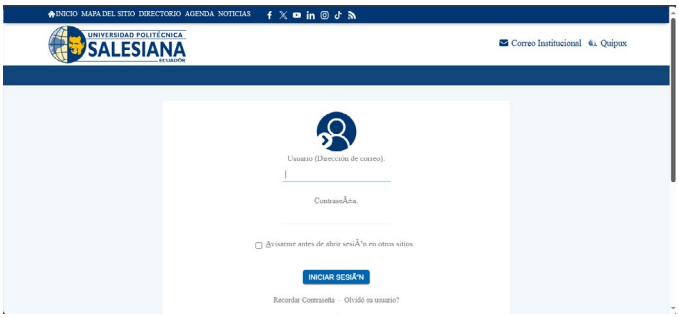

Fig. 4. Cloned website.

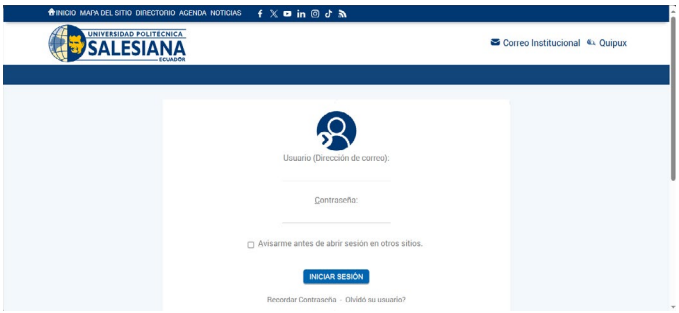

Fig. 5. Original UPS authentication website.

b) Using social engineering to get UPS personnel to enter their login credentials on the fake website:

It involves using social engineering and techniques such as phishing in order to get the fake website to the victim and make them enter their login credentials.

c) Collect the information entered on the fake website:

The victim enters his credentials into the fake website as shown in Fig. 6.

Fig. 6. Victim enters his credentials into the cloned website.

Once the victim enters his username and password and presses “Login”, these credentials reach the intrusion system on the designated console, as shown in Fig. 7, generating a security leak.

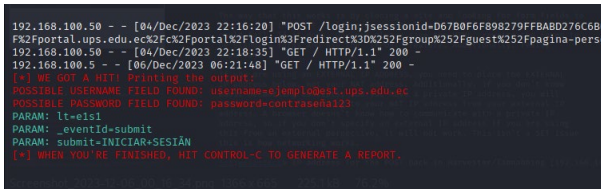

Fig. 7. Intercepted credentials.

As an example, in Fig. 6 the credentials “ejemplo@est.ups.edu.ec” were entered and in password: “password123”. As shown in Fig. 7, the Tool Kit found the credentials entered by the victim and displayed them in the console, this being an effective proof of a failure of the system analyzed during this study.

2. *Phishing Attack:*

With all the information obtained previously, a phishing test is conducted via email, impersonating the domain “notificacionesgye@ups.edu.ec” using spoofing techniques. The attack is conducted in the following stages:

a) Information gathering:

In this stage, information is collected from the victims. For this project, this information was obtained through Google Dorks, as shown in Fig. 8. A list of students was obtained, where private information such as full names, career, ID, cell phone number, and personal and institutional mail was found, thus proving the vulnerability of the institution to access sensitive user data and its subsequent exploitation and attacks on these accounts or networks.

CAMPUS GIRON

NOMBRE	DIGNIDAD	CORREO ELECTRONICO PERSONAL	CORREO ELECTRONICO INSTITUCIONAL	CEDULA	NUMERO DE CELULAR	NUMERO CONVENCIONAL
MATEO [redacted] - COMUNICACIÓN	PRESIDENTE/A	[redacted]@gmail.com	[redacted]@est.ups.edu.ec	17[redacted]	96[redacted]	2[redacted]
ESTEFAN [redacted] – ADMINISTRACIÓN	VICEPRESIDENTE/A	[redacted]@outlook.es	[redacted]@est.ups.edu.ec	17[redacted]	98[redacted]	5[redacted]
KATHERINE [redacted] – EDUCACIÓN BÁSICA	TESORERO/A	[redacted]@hotmail.com	[redacted]@est.ups.edu.ec	17[redacted]	96[redacted]	2[redacted]
ASLY [redacted] – BIOTECNOLOGÍA	SECRETARIO/A	[redacted]@gmail.com	[redacted]@wsl.ups.edu.ec	17[redacted]	98[redacted]	34[redacted]
NO SE CANDIDATIZO	PRIMER VOCAL					
PAMELA [redacted] – PSICOLOGÍA	SEGUNDO VOCAL	[redacted]@outlook.com	[redacted]@est.ups.edu.ec	17[redacted]	99[redacted]	2[redacted]

Fig. 8. FEUPS Board personal information.

b) Spoofing for identity theft:

In this part, the domain and sender impersonations are performed. The domain “ups.edu.ec” is used to make the email appear to be legitimate from a university authority. The sender used by UPS to send notifications to students (“notificacionesgye@ups.edu.ec”) is utilized. This increases the success rate of phishing mail. Also, to use spoofing in Kali Linux, the “send email” tool is used, which has abundant commands that are necessary for this purpose. Once the commands are ready, the phishing mail is sent, as shown in Fig. 9.

c) Sending phishing emails:

Once the previous steps are completed, the phishing mail is sent, as shown in Fig. 10. As it was said before, the sender is “notificacionesgye@ups.edu.ec” and the recipient would be the users of the list of students obtained in Google Dorks. However,

following the guidelines of ethical hacking, the email of the authors is used to perform this scenario.

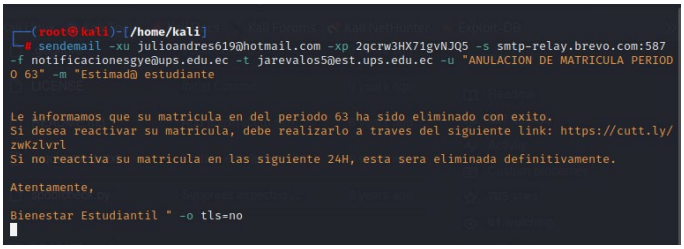

Fig. 9. Command line for sending spoofing mails.

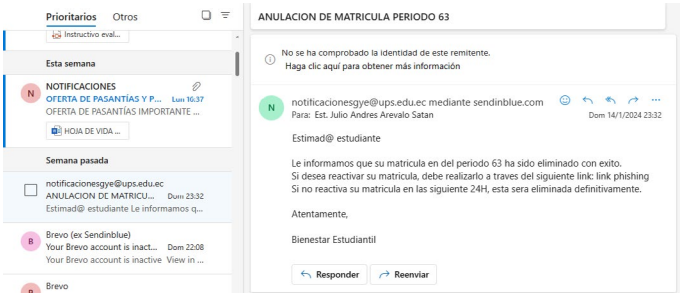

Fig. 10. Mail inbox.

This exercise proved how users can be susceptible to manipulation techniques, highlighting the need for ongoing education on finding potential phishing threats. In addition, it underlines the importance of implementing initiative-taking security measures, such as email filters and phishing detection systems, to mitigate the risk of users falling into cyber traps.

Analysis of vulnerabilities in the university websites reveals issues that could severely affect the academic community. Identified deficiencies, such as critical PHP and security configuration weaknesses, could leave students and staff exposed to cyberattacks, including credential theft and exploitation of personal information. Analyses conducted with Nessus and Mozilla Observatory highlight both positive aspects and problem areas in website security, underlining the urgent need to implement corrective measures. The lack of robust policies and exposure to phishing techniques emphasize the importance of strengthening cybersecurity to safeguard the information and integrity of the university community. Taking into consideration that the security recommendations are essential to prevent vulnerabilities that could compromise the privacy and protection of all users, these results apply to any institution, not only in the academic field.

Fig. 11 presents a summary of the vulnerabilities detected in the domains “virtual.ups.edu.ec” and “ups.edu.ec”, classified according to their level of danger and the Common Vulnerability Scoring System (CVSS). Two critical vulnerabilities are highlighted in the “virtual.ups.edu.ec” domain, including the detection of an unsupported version of PHP (CVSS 10) and the possibility of remote PHP code execution (CVSS 9.8), which reveals significant risks to system security. In addition, high-risk vulnerabilities are found, such as support for medium-strength SSL cipher suites (SWEET32) and multiple PHP vulnerabilities (both with a CVSS of 7.5), affecting both domains.

Vulnerabilities classified as medium-risk, such as the lack of HSTS on the HTTPS server and the detection of obsolete TLS versions, also represent considerable threats. Finally, low-risk vulnerabilities are shown, such as enabling weak algorithms for SSH key exchange and CBC ciphers on the SSH server, which, although less critical, are still important to address in order to strengthen the overall security of the system.

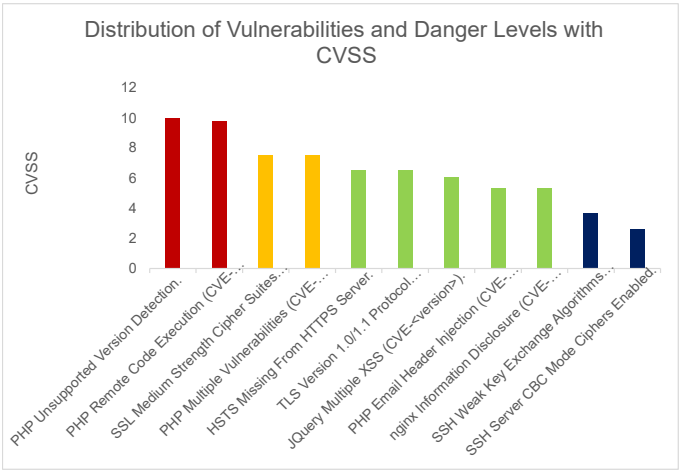

Fig. 11. Distribution of Vulnerabilities.

4. DISCUSSION

Vulnerabilities found in the study include web defacement, SQL injection, XSS (Cross-Site Scripting) vulnerabilities, and directory listing issues [32]. These represent significant risks to the security of the websites analyzed.

The present vulnerability analysis found that one of the analyzed websites had an XSS vulnerability, which allowed the execution of malicious scripts in the user’s browser. An attacker could have exploited this vulnerability to steal confidential information or take control of user sessions on the analyzed website: the UPS portal.

The “virtual.ups.edu.ec” website also presented the XSS vulnerability, which is one of the most common web vulnerabilities according to the Internet Security Foundation (ISSF) in its Web Security Vulnerabilities Report 2022, which points out that XSS represented 50.9 % of all reported web vulnerabilities [33].

In [34], the authors found vulnerabilities in the Apache server, XSS (Cross-Site Scripting), untrusted SSL certificates, obsolete TLS protocols, and disclosure of internal IP addresses, among others.

It is interesting to note that when performing the security analysis in the domains “ups.edu.ec” and “virtual.ups.edu.ec”, it was found that they presented the same vulnerability in terms of obsolete TLS protocols, indicating a common concern in the

security of both platforms and that such protocols should be improved and updated.

According to the authors of [37], they found in their study vulnerabilities of the HTTP Server type, versions 5.4 - 5.4.42, they also detected several applications used in the web portal being executed with a very old version, which makes vulnerabilities easy to exploit and facilitates the intrusion of an attacker. In the present study, where vulnerabilities in the UPS website were also analyzed, the use of obsolete versions in several applications that are in operation was identified. These versions are a significant risk because they have vulnerabilities that could facilitate the intrusion of an attacker in the UPS system. Therefore, making the necessary software patches with their respective updates is suggested.

When compared with [38], there is a clear connection between the identification of vulnerabilities in websites and the need to prove contingency and response plans for cyberattacks in organizations. In our work, we highlight critical vulnerabilities such as Cross-Site Scripting (XSS) and the use of obsolete TLS protocols, which represent significant risks to the security of computer systems, particularly for the integrity of web platforms such as the UPS portal.

5. CONCLUSIONS

This research shows that the implementation of Kali Linux as a tool for detecting vulnerabilities allowed a comprehensive assessment of the security infrastructure of educational environments such as the Salesian Polytechnic University, managing to show a wide range of vulnerabilities that should be strengthened to minimize the risk of possible attacks.

After the analysis, it was possible to classify the vulnerabilities found according to their level of danger and their rating according to the CVSS standard, obtaining 2 critical vulnerabilities, 2 high vulnerabilities, and 6 medium vulnerabilities. Using this methodology allowed prioritizing mitigation actions focusing on the vulnerabilities with the highest impact.

The results of the research revealed that the virtual environment of the Salesian Polytechnic University is exposed to a series of cyber threats and, as in this case of analysis, the probability of having similar situations in other study centers is greater than 50 %, due to the low budget in infrastructure, software, and training of technical staff that manages these processes in the different academic institutions in the South American region. Therefore, it is crucial to have always updated control systems and trained administrators of the networks and websites in order to mitigate this problem and keep the educational environments and their users safe.

The implementation of Kali Linux using a 4-phase method had a significant impact on the evaluation and strengthening of security at the Salesian Polytechnic University. This approach allowed us to comprehensively find and classify the vulnerabilities detected, which helped the prioritization of corrective actions, focusing on those with the highest risk according to CVSS ratings. In addition to reducing risks, this strategy provided a structure that can be adapted and applied in other educational institutions with similar characteristics.

The relevance of this method in other educational settings is considerable, as countless institutions face familiar challenges, such as budget constraints and the need to improve the technical training of staff. Adopting this 4-phase approach in other institutions could enable a more accurate assessment of their IT security, helping to reduce risks and effectively protect users and sensitive information.

In Costa Rica, although it has been proven that cybersecurity is booming, there is no cybersecurity content in the curricula of universities. However, these institutions should consider options such as adding additional courses, adapting the existing structure or creating complementary programs to address the lack of cybersecurity training, essential to adequately prepare future professionals. This shows that in Latin America we are still in the process of developing academic projects to strengthen the security structures in educational and private environments [39].

In the future, it may be recommended to continue the research in larger educational entities and small business environments, following the methodology of this study. This will help to validate the approach in different contexts, identifying common patterns related to cybersecurity in order to generate mitigation measures applicable to such environments. In addition, this will make it possible to suggest security policies at the regional level to guarantee the service, while also analyzing the potential economic impact that this entails.

ROLES OF THE AUTHORS

Holger Santillán: Conceptualization, Ideas, Research, Methodology, Project Management, Supervision, Validation, Writing – revision and editing.

Julio Andrés Arévalo: Research, Resources, Software, Writing – original draft.

Peregrina Wong: Methodology, Supervision, Research, Writing – revision and editing.

REFERENCES

[1] K. S. Tapiawala and X. Wang, “Knowledge Exploration: Teaching Cyber-Security Using Controlled Web-Based Laboratories,” in *The 24th Annual Conference on Information Technology Education*, New York, NY, USA, Oct. 2023, pp. 216–217, doi: 10.1145/3585059.3611443.

[2] J. R. R. Kumar, D. G. Bhalke, S. Nikam, S. Chobe, S. Khidse, and K. Kale, “Evaluation of the extent and demanding roles of ethical hacking in cybersecurity,” *Journal of Autonomous Intelligenc*e, vol. 7, no. 1, pp. 1-10, Sep. 2023, doi: 10.32629/jai.v7i1.1246.

[3] V. Vlachos, I. Katsidimas, E. Kerimakis, S. Nikoletseas, S. Panagiotou, and P. Spirakis, "ASPIDA: A client-oriented platform for assessing websites security practices adoption and reward," in *2021 29th Telecommunications Forum (TELFOR)*, Belgrade, Serbia, Nov. 2021, pp. 1–4, doi: 10.1109/TELFOR52709.2021.9653275.

[4] A. Aibekova and V. Selvarajah, "Offensive Security: Study on Penetration Testing Attacks, Methods, and their Types," in *2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, Ballari, India, Apr. 2022, pp. 1–9, doi: 10.1109/ICDCECE53908.2022.9792772.

[5] M. Liu, Z. Xue, X. Xu, C. Zhong, and J. Chen, "Host-Based Intrusion Detection System with System Calls," *ACM Comput Surv*, vol. 51, no. 5, pp. 1–36, Sep. 2019, doi: 10.1145/3214304.

[6] G. Vishnuram, K. Tripathi, and A. Kumar Tyagi, "Ethical Hacking: Importance, Controversies and Scope in the Future," in *2022 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, Jan. 2022, pp. 01–06, doi: 10.1109/ICCCI54379.2022.9740860.

[7] M. A. M. Nieto et al., "Web Service to Retrieve and Semantically Enrich Datasets for Theses From Open Educational Repositories," *IEEE Access*, vol. 8, pp. 171933–171944, Sep. 2020, doi: 10.1109/ACCESS.2020.3024614.

[8] L. Gallo, D. Gentile, S. Ruggiero, A. Botta, and G. Ventre, "The human factor in phishing: Collecting and analyzing user behavior when reading emails," *Comput. Secur.*, vol. 139, p. 103671, Apr. 2024, doi: 10.1016/j.cose.2023.103671.

[9] Y. Zhang, "Uncovering threats from the surface web and darknet: A qualitative analysis of content relating to cybersecurity and critical infrastructure," M.A. Thesis, Simon Fraser Univ., Burnaby, BC, Canada, 2022.

[10] S. C. Sethuraman, D. P. V S, T. Reddi, M. S. T. Reddy, and M. K. Khan, "A comprehensive examination of email spoofing: Issues and prospects for email security," *Comput. Secur.*, vol. 137, p. 103600, Feb. 2024, doi: 10.1016/j.cose.2023.103600.

[11] H. Ahmetoglu and R. Das, "A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions," *Internet of Things*, vol. 20, p. 100615, Nov. 2022, doi: 10.1016/j.iot.2022.100615.

[12] A. Jones, "Security Posture: A Systematic Review of Cyber Threats and Proactive Security," Senior Honors Thesis, Liberty Univ., Lynchburg, VA, USA, 2022.

[13] J.P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Ethical hacking for IoT: Security issues, challenges, solutions and recommendations," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 280–308, 2023, doi: 10.1016/j.iotcps.2023.04.002.

[14] O. Morozova, A. Nicheporuk, A. Tetskyi, and V. Tkachov, "Methods and technologies for ensuring cybersecurity of industrial and web-oriented systems and networks," *Radioelectronic and Computer Systems*, no. 4, pp. 145–156, Nov. 2021, doi: 10.32620/reks.2021.4.12.

[15] M. Walkowski, J. Oko, and S. Sujecki, "Vulnerability Management Models Using a Common Vulnerability Scoring System," *Applied Sciences*, vol. 11, no. 18, p. 8735, Sep. 2021, doi: 10.3390/app11188735.

[16] H. Santillán, M. Suárez, and D. Cárdenas, "Desarrollo de una herramienta IoT para optimizar el control de la humedad en el cultivo de cacao," *Memoria Investigaciones en Ingeniería*, vol. 25, pp. 246–265, Dec. 2023, doi: 10.36561/ING.25.14.

[17] Banco Interamericano de Desarrollo and Organización de Estados Americanos, "Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe," Washington, DC, USA, Jul. 2020, doi: 10.18235/0002513.

[18] J. M. Aguilar Antonio, "La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas," *Revista de Estudios en Seguridad Internacional*, vol. 6, no. 2, pp. 17–43, Dec. 2020, doi: 10.18847/1.12.2.

[19] J. M. Aguilar Antonio, "Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior," *Estudios Internacionales*, vol. 53, no. 198, p. 169, Apr. 2021, doi: 10.5354/0719-3769.2021.57067.

[20] D. R. Denslin Brabin and S. Bojjagani, "A Secure Mechanism for Prevention of Vishing Attack in Banking System," in *2023 International Conference on Networking and Communications (ICNWC)*, Chennai, India, Apr. 2023, pp. 1–5, doi: 10.1109/ICNWC57852.2023.10127561.

[21] N. I. Daud, K. A. Abu Bakar, and M. S. Md Hasan, "A case study on web application vulnerability scanning tools," in *2014 Science and Information Conference*, London, UK, Aug. 2014, pp. 595–600, doi: 10.1109/SAI.2014.6918247.

[22] M. Al Ismaili, "Enhancing Cybersecurity: Exploring Effective Ethical Hacking Techniques with Kali Linux," in *Research and Applications Towards Mathematics and Computer Science*, vol. 5, E.M. Abo-Dahab Khedary, Ed. India: B P International, 2023, pp. 135–152, doi: 10.9734/bpi/ratmcs/v5/5118C.

[23] Y. Alkhurayyif and Y. Saad Almarshdy, "Adopting Automated Penetration Testing Tools," *Journal of Information Security and Cybercrimes Research*, vol. 7, no. 1, pp. 51–66, Jun. 2024, doi: 10.26735/RJJT2453.

[24] A. O. Bryushinin, A. V. Dushkin, and M. A. Melshiyan, "Automation of the Information Collection Process by Osint Methods for Penetration Testing During Information Security Audit," in *2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)*, Saint Petersburg, Russian Federation, Jan. 2022, pp. 242–246, doi: 10.1109/ElConRus54750.2022.9755812.

[25] E. Chatzoglou, V. Kouliaridis, G. Kambourakis, G. Karopoulos, and S. Gritzalis, "A hands-on gaze on HTTP/3 security through the lens of HTTP/2 and a public dataset," *Comput. Secur.*, vol. 125, p. 103051, Feb. 2023, doi: 10.1016/j.cose.2022.103051.

[26] D. Guaman, F. Guaman, D. Jaramillo, and M. Sucunuta, "Implementation of techniques and OWASP security recommendations to avoid SQL and XSS attacks using J2EE and WS-Security," in *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)*, Lisbon, Portugal, Jun. 2017, pp. 1–7, doi: 10.23919/CISTI.2017.7975981.

[27] R. Palacios, A. F. Fernandez-Portillo, E. F. Sanchez-Ubeda, and P. Garcia-De-Zuniga, "HTB: A Very Effective Method to Protect Web Servers Against BREACH Attack to HTTPS," *IEEE Access*, vol. 10, pp. 40381–40390, Apr. 2022, doi: 10.1109/ACCESS.2022.3166175.

[28] V. Vlachos, Y. C. Stamatiou, and S. Nikoletseas, "The Privacy Flag Observatory: A Crowdsourcing Tool for Real Time Privacy Threats Evaluation," *Journal of Cybersecurity and Privacy*, vol. 3, no. 1, pp. 26–43, Jan. 2023, doi: 10.3390/jcp3010003.

[29] T. Wróbel, M. Kędziora, M. Szczepanik, P. P. Jóźwiak, A. M. Jóźwiak, and J. Mizera–Pietraszko, "Progressive Mobile Web Application Subresource Tampering During Penetration Testing," in *Proc. 35th International Conference on Advanced Information Networking and Applications (AINA-2021) Volume 1*, Toronto, ON, Canada, May 2021, pp. 297–306, doi: 10.1007/978-3-030-75100-5_26.

[30] S. Shukla, M. Misra, and G. Varshney, "HTTP header based phishing attack detection using machine learning," *Transactions on Emerging Telecommunications Technologies*, vol. 35, no. 1, Jan. 2024, doi: 10.1002/ett.4872.

[31] J. Rawat, I. Kumar, N. Mohd, A. Maheshwari, and N. Sharma, "Analysis of Top Vulnerabilities in Security of Web-Based Applications," in *Proc. International Conference on Innovative Computing and Communications (ICICC-2023) Volume 1*, Delhi, India, Feb. 2023, pp. 723–736, doi: 10.1007/978-981-99-3315-0_55.

[32] E. B. Setiawan and A. Setiyadi, "Web vulnerability analysis and implementation," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 407, p. 012081, Sep. 2018, doi: 10.1088/1757-899X/407/1/012081.

[33] S. Sharma and N. S. Yadav, "A multilayer stacking classifier based on nature-inspired optimization for detecting cross-site scripting attack," *International Journal of Information Technology*, vol. 15, no. 8, pp. 4283–4290, Dec. 2023, doi: 10.1007/s41870-023-01459-5.

[34] T. Singh and A. Kumar, "Analyzing Security and Privacy issues for Multi-Cloud Service Providers Using Nessus," in *2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, Erode, India, Feb. 2023, pp. 01–08, doi: 10.1109/ICECCT56650.2023.10179727.

[35] G. Vishnuram, K. Tripathi, and A. Kumar Tyagi, "Ethical Hacking: Importance, Controversies and Scope in the Future," in *2022 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, Jan. 2022, pp. 01–06, doi: 10.1109/ICCCI54379.2022.9740860.

[36] M. Ashraf, A. Zahra, M. Asif, M. Bin Ahmad, and S. Zafar, "Ethical Hacking Methodologies: A Comparative Analysis," in *2021 Mohammad Ali Jinnah University International Conference on Computing (MAJICC)*, Karachi, Pakistan, Jul. 2021, pp. 1–5, doi: 10.1109/MAJICC53071.2021.9526243.

[37] Rodríguez Matías, "Análisis de Vulnerabilidades del Portal Web utilizando Metodologías de Hacking Ético para un GAD Municipal de la Provincia de Santa Elena," Bachelor's Thesis, Univ. Estatal de la Península de Santa Elena, La Libertad, Ecuador, 2021.

[38] I. N. Coello Ochoa, "Análisis de ciberataques en organizaciones públicas del Ecuador y sus impactos administrativos," Degree Thesis, Univ. Politécnica Salesiana, Guayaquil, Ecuador, 2021.

[39] C. Artavia Madrigal, M. Guevara García, I. Mora Zumbado, T. Murillo Murillo, M. Ramírez González, and V. Solano Ruiz, "Un Análisis del sistema educativo costarricense: Desafío crítico para la ciberseguridad del país," *Rhombus*, vol. 3, no. 2, pp. 1-19, Sep. 2023. [Online]. Available: https://revistas.ulacit.ac.cr/index.php/rhombus/article/view/89