ADOPTION OF INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY (ITIL) FRAMEWORK TO MITIGATE VULNERABILITIES IN A CLOUD-BASED PLATFORM

Hammed, O. Jimoh[1], Sunday O.Asakpa[1], and Mubarak, O. Ahmed [2]
[1]Department of Cybersecurity and Data Protection, Federal Polytechnic, Offa
[2]Cisco Nigeria Limited, Lagos

Abstract

This paper discusses how integrating the Information Technology Infrastructure Library (ITIL) governance framework with Open Web Application Security Project (OWASP) techniques can enhance vulnerability management in cloud environments. The framework will be used on one of the cloud technologies called "Docker." On this cloud platform, OWASP Juice Shop, which is a vulnerable website, will be installed to demonstrate a hands-on exploitation of critical vulnerabilities, such as broken access control, security misconfiguration, and injection, among other vulnerabilities. This will be executed in a virtualization environment with the use of Kali Linux embedded in the virtual machine and a tool called Burp Suite as a proxy for interception. Each vulnerability triggered formal ITIL processes: Incident Management for containment, Problem Management for root-cause analysis, Change Control for secure code deployment (e.g., parameterized queries, CSP headers), and CSI for knowledge retention. The work proves that embedding defensive coding practices and automated scanning within governed workflows transforms reactive patching into an actionable intelligent approach to improve the security posture of the cloud environment and ensure best practices are strictly adhered to within an organization.

Keywords: docker, burp suite, ITIL, incident management and problem management

Introduction

Cloud computing has become the dominant paradigm for deploying and managing information systems in both private and public sectors. It offers unmatched scalability, flexibility, and economic efficiency through shared infrastructure and on-demand resource provisioning. However, the same characteristics that make cloud environments appealing also introduce substantial cybersecurity challenges. Multi-tenancy, virtualization, and remote management expand the attack surface, making cloud infrastructures prime targets for data breaches, insider threats, and configuration-based vulnerabilities (Armbrust, et al., 2010). The shared responsibility model inherent in cloud services further complicates governance: while cloud service providers secure the infrastructure, customers remain responsible for safeguarding data, managing identities, and configurations of application layers (Amazon Web Services, 2023). Traditional perimeter-based defenses are no longer sufficient in dynamic, distributed environments where assets may exist across multiple geographic and administrative domains. As organizations continue their migration to cloud ecosystems, cybersecurity governance the structured framework through which policies, responsibilities, and controls are defined and enforced, has emerged as a foundational pillar of enterprise resilience (Mell & Grance, 2011). Governance ensures that cybersecurity activities align with organizational strategy, comply with regulatory requirements, and maintain accountability across all layers of digital service delivery. The Information Technology Infrastructure Library (ITIL) provides a globally recognized framework for IT service management (ITSM) that emphasizes structured processes, clear ownership, and continual improvement (AXELOS, 2019). ITIL's recent iterations, particularly ITIL v4, integrate service management principles with risk, security, and governance domains, offering a holistic

blueprint for managing technology services securely and efficiently. By applying ITIL's service design, service operation, and continual service improvement processes to cybersecurity, organizations can transition from reactive incident handling to proactive, metrics-driven governance (Nissen & Demin, 2020). In parallel, the OWASP Juice Shop project, an intentionally vulnerable web application developed by the Open Web Application Security Project, has become a standard training and testing platform for cybersecurity research (Braun, 2018). It embodies common vulnerabilities such as Broken Access control, Cryptographic failure, injection, insecure design and security misconfiguration, many of which correspond to the OWASP Top 10. When deployed in a cloud environment, Juice Shop provides a realistic and controlled testbed for studying the behavior of vulnerabilities under cloud-specific conditions, such as containerized orchestration, distributed storage, and web API exposure. In this paper, OWASP Juice Shop will be used as a benchmark to assess vulnerabilities within a cloud-based environment and to apply ITIL-driven governance practices to their detection, analysis, and remediation. The objective is not limited to identifying only technical flaws but also to demonstrate how ITIL's structured processes, such as Incident Management, Problem Management, Change Control, and Continual Service Improvement, can systematize vulnerability management. By integrating ITIL with vulnerability assessment workflows, this paper proposes a governance-based approach that improves traceability, accountability, and repeatability of cybersecurity processes in the cloud. Conclusively, this paper will greatly bridge the gap between technical cybersecurity operations and strategic governance oversight, fostering a unified model of security management for modern cloud infrastructures.

Related Works

The review of related works cross-examines prior detailed research on OWASP's contributions to application security, especially in cloud-based environments, as well as the implementation of ITIL to ensure compliance and conformity within the cybersecurity governance model. Both ITIL and OWASP are underpinned by Risk Management Theory, which emphasizes the identification, assessment, mitigation, and continuous monitoring of threats within an organization's information systems. ISO 31000 defines risk management as a systematic approach to addressing uncertainty in pursuit of objectives. Within the ITIL framework, risk management is implemented through structured procedures for Change Evaluation, Service Continuity, and Security Management, ensuring that all services undergo risk assessment before deployment (ISO, 2018). From a technical standpoint, OWASP complements this with actionable methodologies such as threat modeling, vulnerability scanning, and penetration testing, which directly target software-level risks (Shostack, 2014).

ITIL in IT Service Management

A substantial body of research affirms ITIL's contribution to improving IT service efficiency, governance, and reliability. ITIL-aligned organizations experience measurable improvements in incident response times, process standardization, and service quality (Van Loon & Van Fenema, 2010). Similarly, ITIL adoption enhances transparency and operational accountability within organizations, leading to better customer satisfaction and compliance outcomes (Al-Hadi & Al-Samarraie, 2017). The Information Security Management (ISM) process within ITIL embeds risk assessment and mitigation directly into service delivery, ensuring that vulnerabilities are systematically managed throughout the service lifecycle (Cater-Steel et al., 2009). In higher education and financial sectors, ITIL has been linked to improved service continuity and reduced operational downtime, translating into stronger institutional resilience. However, several challenges have been documented. Research in developing contexts identifies barriers such as limited executive support, inadequate funding,

cultural resistance to procedural change, and a shortage of certified ITIL practitioners (Ogundele & Adebayo, 2020). Within Nigeria, adoption remains relatively low due to the high cost of certification and a lack of institutional enforcement mechanisms (Akinwale et al., 2020). Despite these barriers, many organizations express interest in ITIL-based maturity models, recognizing their potential to professionalize IT governance and integrate cybersecurity principles effectively.

OWASP and Application Security

OWASP has become an authoritative standard for web and application security worldwide. Its Top Ten and Application Security Verification Standard (ASVS) serve as practical guides for software engineers, auditors, and organizations to systematically identify and mitigate vulnerabilities such as injection flaws, security misconfigurations, and insecure deserialization (Zalewski, 2020). Empirical studies indicate that incorporating OWASP standards during development can reduce exploitable vulnerabilities by 40–60%, especially when paired with automated testing tools (McGraw, 2006). OWASP's free tools such as Zed Attack Proxy (ZAP) and Dependency-Check support continuous vulnerability scanning within DevOps pipelines, enabling organizations to detect and fix security flaws earlier. In the Nigerian context, where cyber-attacks on e-government portals, fintech applications, and educational systems are increasing, OWASP-based frameworks have proven highly applicable. Training developers and IT professionals using OWASP guidelines has been shown to enhance security awareness and reduce breach incidents (Okafor & Okoye, 2022). These successes demonstrate that OWASP's open-access model is adaptable to diverse environments, providing both a technical foundation and an educational platform for capacity building in cybersecurity.

Integration of OWASP and ITIL Framework

Recent research highlights the value of integrating ITIL's governance-driven structure with OWASP's technical rigor to create a Secure IT Service Management (SecITSM) model. A methodology was proposed to embed OWASP verification controls within ITIL's Continual Service Improvement (CSI) cycle to enable ongoing vulnerability management and reduce recurring security incidents (Sánchez-Gordón & Colomo-Palacios, 2021). Similarly, such integration fosters improved collaboration among developers, operations staff, and security teams, resulting in enhanced system reliability and faster incident recovery (Williams & Rao, 2021).

Figure 1: *Devsecops Workflow for Owasp and ITIL Integration*

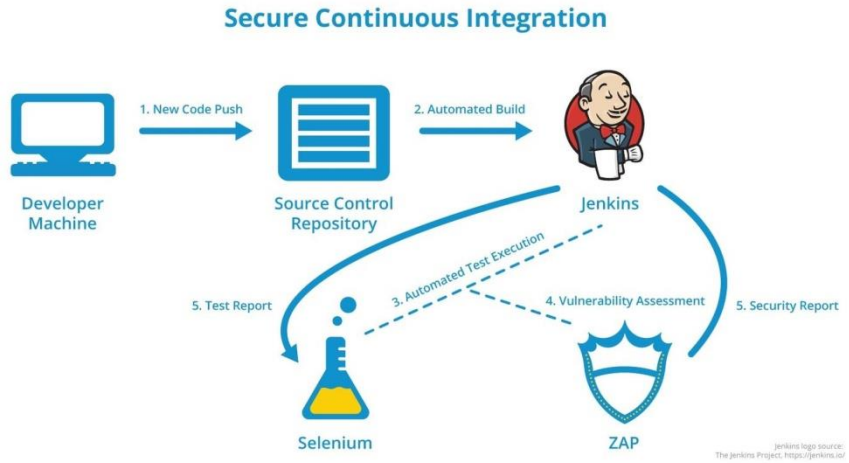


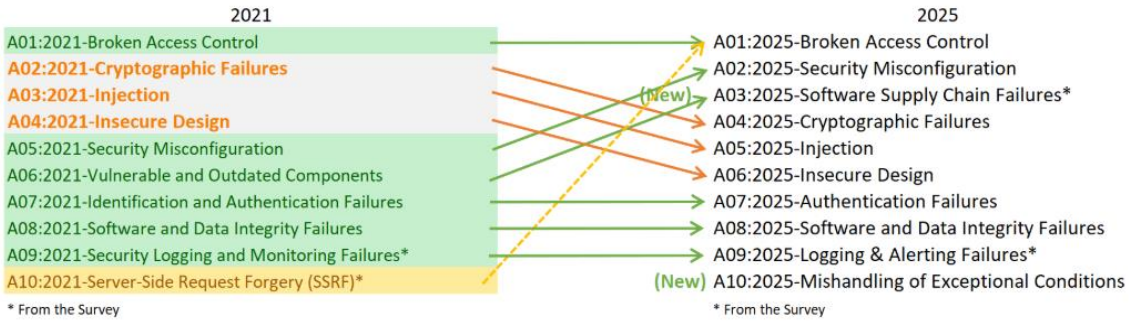
Figure 1 displays the integrated model of alignment with development, security and operations (DevSecOps) that ensures ITIL processes discipline and traceability, while OWASP injects technical validation into each lifecycle stage from service design to deployment. They all coexist under shared accountability. This hybrid approach bridges the long-standing gap between compliance (what organizations should do), and technical assurance (what systems actually do). An organization can achieve a measurable, auditable and improved security posture that aligns with both business and technical objectives if OWASP's vulnerability testing and the metrics are embedded into ITIL service processes.

System Design, Methodology and Results

System Design

The system is designed as a practical model that integrates ITIL's governance structure with OWASP's technical security practices. The goal is to create a bridge between service management and application security, ensuring that both organizational processes and technical controls work together to reduce vulnerabilities. To demonstrate this integration, the study makes use of OWASP Juice Shop, an intentionally insecure web application widely used for testing and teaching web security. OWASP Juice Shop can be run on various cloud platforms such as Docker, Kubernetes, Heroku, etc. But for this paper, we will be benchmarking our lab on Docker. Moreso, the OWASP Juice shop contains real-world vulnerabilities that simulate the kinds of security flaws commonly found in modern applications. OWASP has top ten vulnerabilities, which change almost every 3 – 4 years but the most recent is 2025, as shown in figure 2.

Figure 2: *2021-2025 OWASP Top Ten Vulnerabilities (Snyder, 2025)*



The above diagram shows the variation of the OWASP top ten between 2021 and 2025. However, for this paper, we will be testing the vulnerability of A01:2025, Broken Access Control, A02:2025, and Security Misconfiguration. Using Juice Shop allowed this study to illustrate how ITIL processes such as Change Management, Incident Management, and Continual Service Improvement (CSI) can be combined with OWASP techniques to prevent and manage security risks.

However, the system model consists of three layers: the Governance Layer, the technical layer and the integration layer. The first layer strictly adheres to the ITIL principle by defining policies, structures, and workflows for handling incidents. While the second layer applied the OWASP testing and remediation methods to detect and fix vulnerabilities. The third layer connects governance and technical activities, ensuring that vulnerability findings from technical tests are well documented, prioritized and approved through ITIL processes.

Methodology and Results

The design methodology employed for this paper is done in a virtualized environment. The virtual machine (VM) deployed here within is the Oracle VirtualBox. Within the Virtual Machine, we will install Kali Linux operating system (OS).Once this is successfully installed, we have to open a terminal within Kali Linux to download, install, and run Docker.

Installation of OWASP Juice Shop in Cloud Environment

You can find some less common installation variations as well as instructions to run Juice Shop on a variety of cloud computing platforms such as Node.js, Docker Container, and Vagrant. But for this paper, we will be using a Docker Container. A Docker is a software that allows you to build, test, and deploy applications quickly into any environment. It can be installed on Windows, Linux and Mac OS Operating System. To install and run a Docker container, it is imperative to have a Kali Linux virtualization software such as Oracle VirtualBox or VMware.

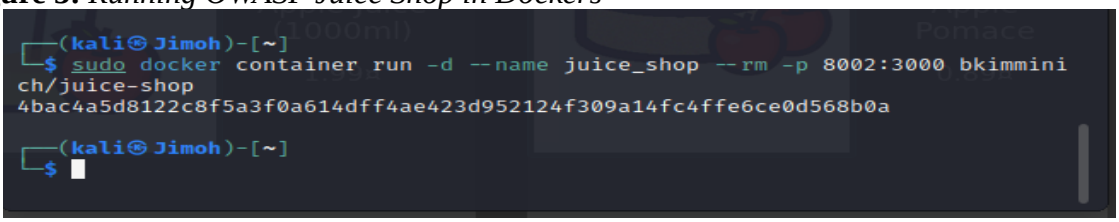
In Kali Linux, to install Docker, you type the following command

"sudo apt install docker.io"

After successful installation, you can then run OWASP Juice Shop, using the following command as shown in figure 3.

"sudo docker container run -d --name juice_shop --rm -p 8002:3000 bkimminich/juice-shop"

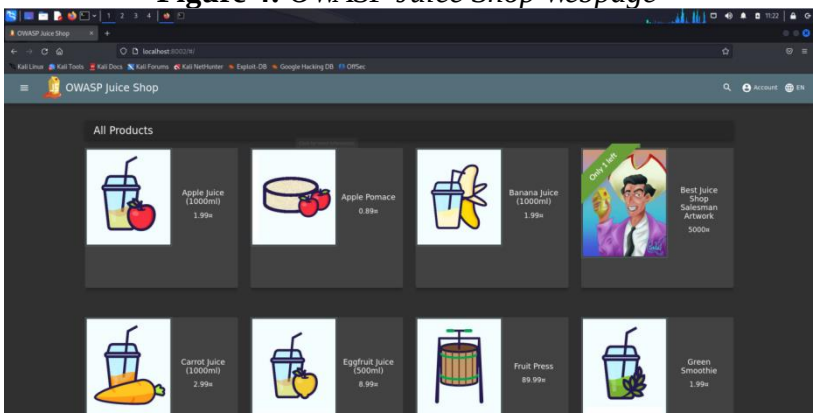
Figure 3: *Running OWASP Juice Shop in Dockers*



The Figure 3 image showsthe running of the OWASP Juice Shop within the cloud environment platform, Docker. The hash value displayed is significant to verify the authenticity and integrity of the platform.

While the command is running, we can open a browser (Mozilla Firefox) within Kali Linux, and type the local host (http://localhost:8002) or (http://localhost:3000). Figure 4 displays the OWASP Juice Shopwebsite.

Figure 4: *OWASP Juice Shop Webpage*



After the display of the webpage, we can set up Burp Suite and Foxy Proxyon the same localhost. Burp Suite allows us to intercept user credentials, while Foxy Proxy allows us to save proxy profiles, enables us to easily switch to a Burp Suite profile in a matter of clicks and makes disabling the proxy easy.

Performing OWASP-Based Vulnerability Assessments and Results

Three critical vulnerabilities from OWASP Juice Shop were selected to demonstrate system operation:

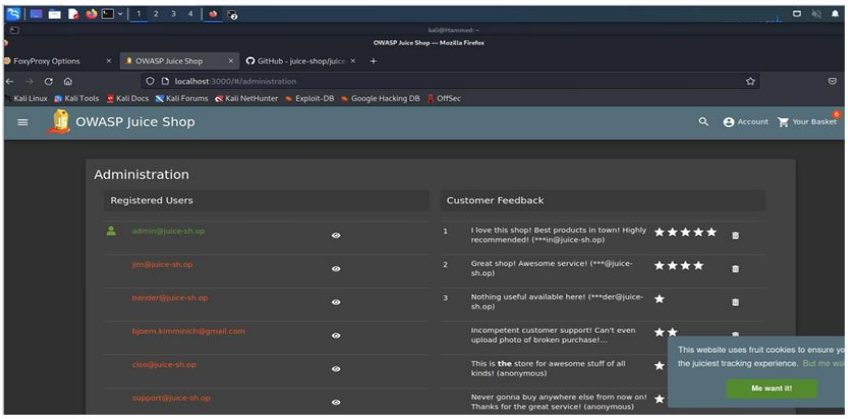
- Broken Access Control (A01:2025)
- Security Misconfiguration (A02:2025)

Broken Access Control

This occurs when a user can gain unauthorized access to resources meant for the administrator on a web application. Upon successful exploitation of credentials, it can lead to data breaches and security issues such as privilege escalation, data modification and leakage.

To perform this on the OWASP Juice-shop, the main code of the website needs to be accessed via the web developer tool and searched for the debugger. The debugger can be used to identify any errors in coding at various stages of the operating system or application development. From the developer's tool, the credentials of the admin can be accessed. A successful compromise will reveal the username and password of the admin. If the details revealed are added to the administration path of the URL, as shown in Figure 5, we will have access to unauthorized information about the store and customers.

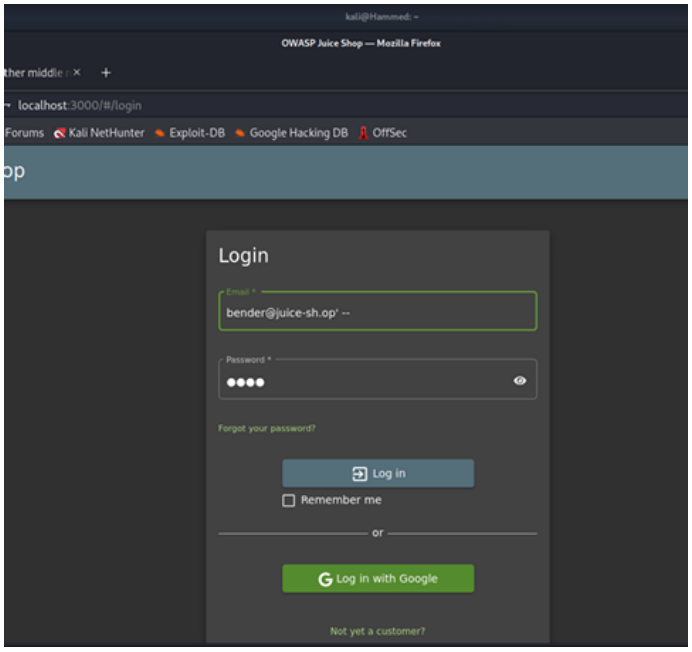
Figure 5: *Broken Access Control*



Security Misconfiguration

This occurs when some security controls or features are not properly configured or left insecure. An attacker can inject the web application while leveraging on the lapses of the developer to access sensitive data. To perform this vulnerability, we will be using an account "Bender" found during our walk-through. We must first ensure that Burp Suite is launched and the "interception mode" is ON. Under normal circumstances, the email address of "Bender" found on the website is "bender@juice-sh.op, but we will be logging in by sending a request to the server with an injected code as depicted by figure 6.

Figure 6: ***Logging to Bender's Account***



From the above image, a code was injected to the credentials bender@juice-sh.op by adding "—" to the username to check its security configuration. Since interception is ON in Burp Suite, we can check our request and response as shown in figures 7 and 8.

Figure 7: ***Burp Suite Request Page***

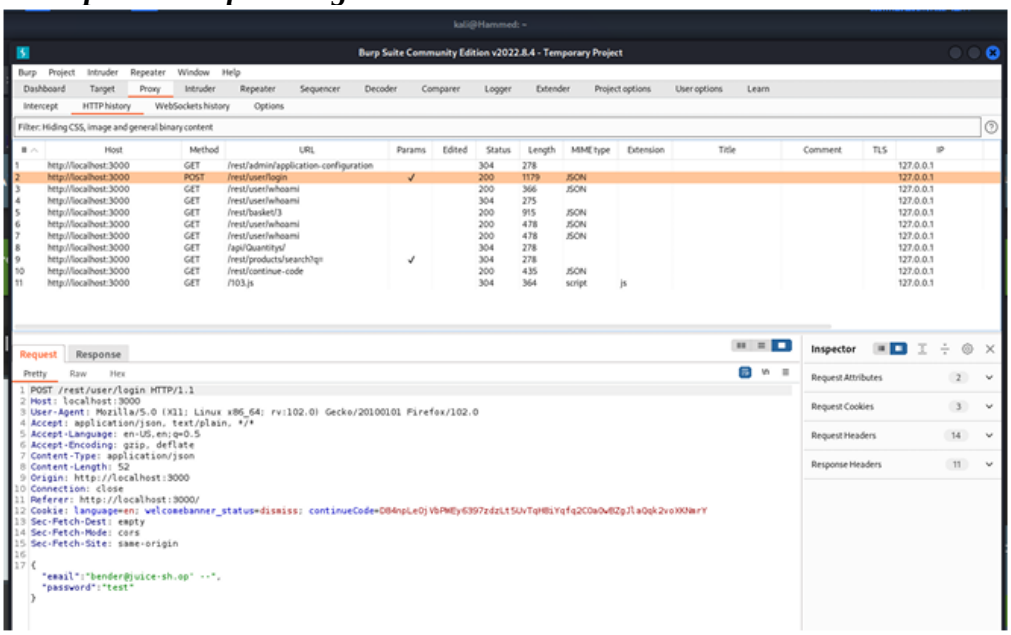


Figure 8: ***Burp Suite Response Page***

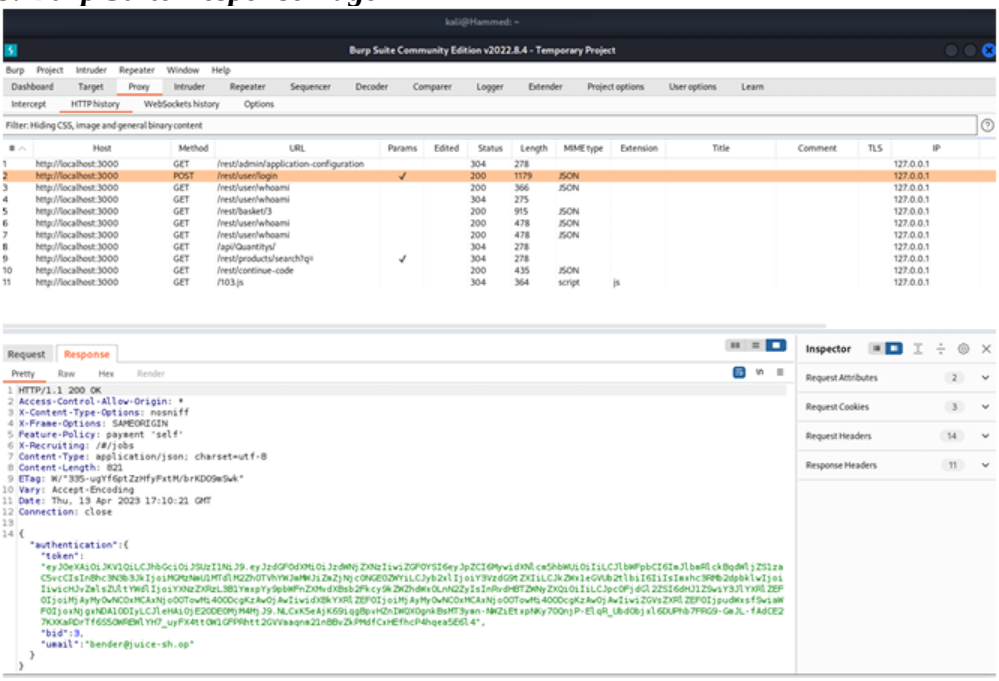
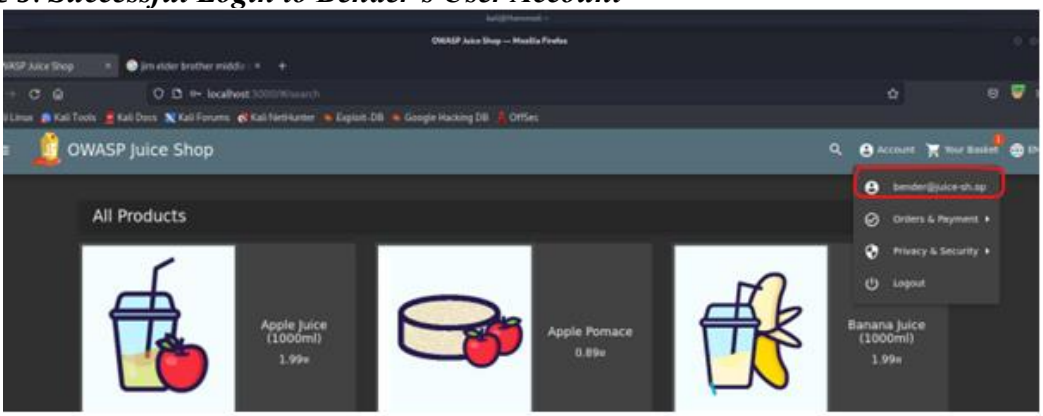


Figure 7 shows that the injected code was accepted and going to figure 8, to continually click on the forward button in Burp Suite, till nothing is left to forward again, it will automatically log us into Bender's user account as shown in figure 9.

Figure 9: ***Successful Login to Bender's User Account***



After the successful demonstration of the OWASP vulnerability on the cloud platform, all findings were logged to simulate an ITIL incident register that includes fields such as Incident ID, Severity, Detection source and Resolution Status.

Mapping Results to ITIL Processes

Each technical vulnerability triggered a corresponding ITIL process, which in turn, ensures structured governance alignment as shown in Table 1.

Table 1: ***ITIL Processes Result Against OWASP Vulnerability***

Vulnerability	ITIL Process Triggered	Action Taken
Security Misconfiguration	Change Management	Code modification request logged and reviewed before deployment
Broken Access Control	Access Management → Risk Management	Access control policies updated and reviewed by the security manager

The change approval and post-resolution reviews were simulated within the continual service improvement (CSI) process, ensuring that lessons learned were properly documented and used to refine secure coding standards

Conclusion

The convergence of cybersecurity and service governance remains a critical frontier in modern cloud operations. This paper affirms that vulnerabilities in cloud applications are rarely caused by technological shortcomings alone; rather, they stem from gaps in process ownership, inconsistent remediation workflows, and the absence of feedback mechanisms. By integrating ITIL's process rigor with OWASP's technical precision, organizations can shift from reactive patching to proactive, metrics-driven cybersecurity governance. Thus, the study concludes that cybersecurity resilience in the cloud is as much about *how* vulnerabilities are managed as it is about detecting them and ITIL provides the missing governance scaffolding for OWASP's technical excellence.

References

Akinwale, S. O., Oyeleye, K. A., & Falade, F. O. (2020). Assessing IT service management maturity in Nigerian universities: An ITIL perspective. *J. Inf. Technol. Educ. Res.,, 19*, 451-472. doi:10.28945/4651

Al-Hadi, I. A., & Al-Samarraie, R. H. (2017). The impact of ITIL implementation on IT service quality: Evidence from Jordanian Banks. *International Journal of Inf. Manage, 37*(6), 659-667. doi:10.1016/j.ijinfomgt.2017.07.004

Amazon Web Services. (2023).*AWS shared responsibility model*. https://aws.amazon.com/compliance/shared-responsibility-model/

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., . . . Patterson, D. A. (2010). A view of cloud computing. *Commununication of the ACM, LIII*(4), 50-58. doi:10.1145/1721654.1721672

AXELOS. (2019). *ITIL 4 foundation*(1st éd.). TSO (The Stationery Office), available online at www.tsoshop.co.uk.

Braun, B. (2018). OWASP juice shop: A modern, intentionally insecure web application. *International Conference on Availability, Reliability and Security (ARES), 13*, 1-8. doi:10.1145/3230833.3233264

Cater-Steel, N., Toleman, E., & Tan, M. (2009). ITIL v3 and ISO/IEC 20000: Towards a unified framework for IT service management. *20th Australasian Conference on Information Systems (ACIS)*,1-10.

International Organization for Standardization. (2018). *ISO 31000:2018 – Risk Management.* ISO - Guidelines. https://www.iso.org/standard/63787.htm

McGraw, G. (2006). *Software Security: Building Security.* Addison-Wesley.

Mell, P., & Grance, T. (2011). T*he NIST definition of cloud computing*. NIST Special Publication 800-145. doi:10.6028/NIST.SP.800-145

Nissen, C. F., & Demin, P. (2020). *ITIL 4: Drive stakeholder value.*AXELOS.

Ogundele, O. A., & Adebayo, A. A. (2020). Critical success factors and barriers to ITIL adoption in Nigerian organizations.*African Journal Inf. Syst.* , *12*,56-74. Récupéré sur https://digitalcommons.kennesaw.edu/ajis/vol12/iss2/4

Okafor, U. E., & Okoye, C. I. (2022). Adoption of OWASP security practices in Nigerian fintech startups. *Proc. IEEE International Conference on Cybersecurity and Cloud Computing (CSCloud)*,215 - 221. doi:10.1109/CSCloud55409.2022.00045

Sánchez-Gordón, A., & Colomo-Palacios, R. (2021). Integrating OWASP ASVS into the ITIL continual service improvement process for enhanced web application security. *Proc. 22nd Int'l Conf. on Software Process Improvement and Capability Determination (SPICE)*,215–226. Springer. doi:10.1007/978-3-030-71434-5_18

Shostack, D. (2014). *Threat Modeling: Designing for Security.* Wiley.

Snyder, C. (2025). OWASP update elevates software supply chain and misconfiguration risk. *Récupéré sur.* https://eclypsium.com/blog/owasp-top-10-2025-software-supply-chain-risk/

Van Loon, D., & Van Fenema, M. (2010). *Exploring ITIL implementation in practice: An empirical study* (Vol. III). Int. J. IT/Business Alignment.

Williams, J. G., & Rao, K. R. (2021). SecITSM: A framework for secure IT service management using ITIL and DevSecOPS. *J. Cyber Secur. Mobil.*, *10*(4), 421-444. doi:10.13052/jcsm2245-1439.1042

Zalewski, M. (2020). Empirical evaluation of OWASP top 10 mitigation techniques in real-world applications. *IEEE Access, 8*, 178956–178969. doi:10.1109/ACCESS.2020.3027337