1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a comprehensive security assessment conducted on the domain **uat.cbreresidencial.es**. The analysis was initiated on **June 15th at 22:45** and concluded in a duration of **00h:09m:30s**. The assessment, identified by tracking ID **071e6c52f47e**, was performed using a Basic scan type, focusing on identifying High and Medium-risk vulnerabilities. The objective was to evaluate the security posture of the web application and infrastructure following OWASP and OSCP methodologies.

1.2 Summary of Key Issues

The security assessment identified **1** High-risk, **2** Medium-risk, **2** Low-risk, and **14** informational issues. The most critical finding is a Denial of Service (DoS) vulnerability with a **97.74%** timeout rate across HTTP and HTTPS services, posing a significant threat to service availability and requiring immediate mitigation. Medium-risk issues include the absence of a Web Application Firewall (WAF) on **100%** of analyzed hosts, increasing susceptibility to injection attacks, and sensitive subdomain exposure that could lead to unauthorized access. Low-risk findings highlight potential brute force vulnerabilities on SSH services. Immediate actions include implementing DoS protection, enhancing WAF coverage, and securing sensitive subdomains to mitigate these risks effectively.

1.3 Key Security Issues

Title	Risk
Denial of Service (DoS) Assessment	High
Absence of WAF	Medium
Subdomain Naming Security	Medium
Services Vulnerable to Brute Force	Low
Shared Hosting Environment	Low

1.3.1 Denial of Service (DoS) Assessment

Description:
A high-severity DoS vulnerability was identified with a **97.74%** timeout rate across HTTP and HTTPS services. This indicates a significant risk to service availability, potentially leading to service disruptions.
Affected Assets:
- Endpoint: **uat.cbreresidencial.es:80**
Recommendations:
- Implement specific DoS protection measures. - Review and optimize security configurations. - Apply firewall rules to limit excessive connections. - Monitor server performance during peak events.

1.3.2 Absence of WAF

Description:
The absence of a Web Application Firewall (WAF) was detected on **100%** of the analyzed hosts, resulting in increased vulnerability to injection-based attacks and unauthorized data access.

Affected Assets:
- Host: **uat.cbreresidencial.es**

Recommendations:
- Deploy a robust WAF solution to protect against common web application attacks. - Regularly update WAF rulesets to address emerging threats. - Conduct periodic security reviews to ensure effective WAF configuration.

1.3.3 Subdomain Naming Security

Description:
A sensitive subdomain associated with development/staging environments was identified which may expose unpatched vulnerabilities or debug information, increasing the risk of unauthorized access.

Affected Assets:
- Subdomain: **uat.cbreresidencial.es**

Recommendations:
- Restrict access to sensitive subdomains using IP whitelisting or VPN. - Regularly audit subdomains for exposure of sensitive information. - Implement strict access controls and monitoring on development environments.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to implement comprehensive security measures such as regular vulnerability assessments, continuous monitoring, and incident response planning. Additionally, adopting a defense-in-depth strategy will provide layered protection against potential threats. Regular training for staff on security best practices is also advised to mitigate human-related risks.