

# **1 Executive Security Assessment Report**

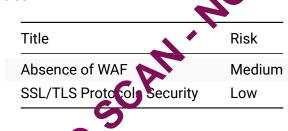
## 1.1 Introduction

The security assessment was conducted on the domain **gw-cpep.esailcloud.com**. The analysis was initiated on **April 24th at 11:45** and concluded in **00h:10m:59s**. The scope of the work included a basic security scan focusing on identifying High and Medium-risk vulnerabilities within the web application and its infrastructure. The methodology employed adheres to OWASP and OSCP standards, ensuring a comprehensive evaluation of potential security risks.

## **1.2 Short Summary of Main Issues**

The security assessment identified a total of **19 issues**, categorized as **0 High-risk**, **1 Medium-risk**, **1 Low-risk**, and **17 informational**. The most critical finding is the absence of a Veb Application Firewall (WAF) on **100%** of analyzed hosts, significantly increasing the risk of orber-attacks, particularly injection-based attacks, which could lead to unauthorized data access and system compromise. Additionally, the SSL/TLS protocols are generally secure, the Support for TLS 1.3 and TLS 1.2, but vigilance is required to maintain this standard. The L wrisk issue pertains to SSL/TLS protocol security, which is currently acceptable but should be monitored for any changes in standards. Actionable insights include implementing a WAF to mitigate attack risks and maintaining current SSL/TLS configurations to ensure one conserve.

## 1.3 Key Security Issues



### 1.3.1 Absence of WAF

### Description

The absence of a Web Abulication Firewall (WAF) was identified on the domain **gw-cpep.esailcloud.com**. This lack of protection results in a **100% vulnerability rate**, significantly elevating the risk of successful cyber-attacks, particularly injection-based attacks. Without a WAF, the application is susceptible to valuation data access, data breaches, and potential system compromise.

Affected Arsots

## Domain-gw-pep.esailcloud.com

Total Husts Analyzed: 1

Host without WAF: 1

# Recommendations

It is recommended to implement a Web Application Firewall (WAF) to provide an additional layer of security against common web-based attacks. A WAF can help detect and block malicious traffic, reducing the risk of data breaches and unauthorized access.

## 1.3.2 SSL/TLS Protocols Security Assessment

## Description

The SSL/TLS protocol security assessment revealed that the domain supports both TLS 1.3 and TLS 1.2, which are considered secure by current standards. No endpoints were found using deprecated protocols such as SSLv3, TLS 1.0, or TLS 1.1, indicating no immediate risk from these outdated protocols.



MC

<text><text><text><text>