Index

[1 Executive Summary 2](#_Toc55508767)

[1.1 Severity index 2](#_Toc55508768)

[2 Technical Report 4](#_Toc55508769)

[2.1 Penetration Test perimeter 4](#_Toc55508770)

[2.2 Findings 5](#_Toc55508771)

[2.2.1 Security Misconfiguration 6](#_Toc55508772)

[2.2.2 System software and applications not updated 10](#_Toc55508773)

[2.2.3 HTTP Response Headers 13](#_Toc55508774)

[2.2.4 Lack of protection mechanism in cookies 17](#_Toc55508775)

[2.2.5 Lack of protection mechanisms against Clickjacking attacks 19](#_Toc55508776)

[2.2.6 Transport layer without the use of encryption 21](#_Toc55508777)

[2.2.7 Use of compromised or risky cryptographic algorithms 23](#_Toc55508778)

[2.2.8 Information Leak 26](#_Toc55508779)

[2.3 Technical Annex 28](#_Toc55508780)

# Executive Summary

## Severity index

In Table 1 the qualitative severity associated with each of the vulnerabilities and threats detected on the application owned by Acme are shown, in respect to the analysis carried on, as described in paragraph 0.

|  |  |  |
| --- | --- | --- |
| VULN. CODE | VULNERABILITY | SEVERITY |
| ABU-F | Abuse of functionality | **EXTREME** |
| CONC-WK | Weaknesses in the mechanisms for managing competition | **EXTREME** |
| CRED-WK | Weak access credentials | **EXTREME** |
| IN-WK | Weaknesses in the neutralization of the input provided by the user | **EXTREME** |
| IV-WK | Weaknesses in the validation of the input provided by the user | **EXTREME** |
| PRIV-ESC | Privilege escalation | **EXTREME** |
| AUTH-WK | Weaknesses in the authorization management mechanisms | **HIGH** |
| CRED-CT | Authentication credentials transmitted in clear text | **HIGH** |
| CRYP-WK | Use of compromised or risky cryptographic algorithms | **HIGH** |
| IDO-REF | Insecure Direct Object Reference | **HIGH** |
| ISP-WK | Infrastructure security perimeter not adequately configured | **HIGH** |
| MGMT-EXP | Exposed management interfaces | **HIGH** |
| PWD-CHK | Absence of password robustness verification mechanisms | **HIGH** |
| PWD-CL | Clear passwords in memory | **HIGH** |
| PWD-NC | Access credentials stored without the use of cryptography | **HIGH** |
| RED-WK | Insecure Redirect | **HIGH** |
| SEC-MISC | Security Misconfiguration | **HIGH** |
| SEG-WK | Weaknesses in the segregation of the System | **HIGH** |
| S-WK | Weaknesses in session management mechanisms | **HIGH** |
| CTOK-WK | Using insecure cryptographic tokens | **MODERATE** |
| NOCRYPTT | Transport layer without the use of encryption | **MODERATE** |
| PWD-BF | Absence of anti-guessing mechanisms for access credentials | **MODERATE** |
| SSAP-NU | System software and applications not updated | **MODERATE** |
| XSRF-PROT | Weakness in the protection mechanisms against XSRF attacks | **MODERATE** |
| CJK-PROT | Lack of protection mechanisms against Clickjacking attacks | **LOW** |
| IN-LEAK | Information Leak | **LOW** |
| RESP-H | HTTP Response Headers | **LOW** |
| SCK-PROT | Lack of protection mechanisms in cookies | **LOW** |

Table 1 – Risk index for found vulnerabilities

The Table 2 shows the metric of qualitative evaluation for vulnerabilities and threats.

|  |  |
| --- | --- |
| SEVERITY | DEFINITION |
| EXTREME | Vulnerabilities that allow full compromising of the system. This risk level applies when the exploitation of the vulnerability allows unauthorized access to the resources, information and critical business data or personal and sensitive data regarding privacy and security |
| HIGH | Vulnerabilities that allow compromising of the system by gaining some non-privileged access. This level of vulnerability also applies when the attack has an impact on the availability of the services. |
| MODERATE | Vulnerabilities that allow non-direct compromising of the system. This level of vulnerability also applies to indicate the use of insecure communication protocols or the use of protocols that were not designed for the network being used. |
| LOW | Vulnerabilities that expose non-critical or sensitive information only to local users of a system. It is applied when a very high effort is not required to exploit vulnerabilities or if the impact consists in the accidental disclosure of less sensitive information. |

Table 2 – Metric of qualitative evaluation for vulnerabilities

# Technical Report

The Penetration Test activities were carried out without taking any actions in order to hide, modify or remove the evidence of the access. In the following paragraphs, we will provide an overview of the attack vector and perimeter analyzed during the course of the activities.

## Penetration Test perimeter

Table 3 shows the targets on which we focused our analysis.

| Target URI | Target Host/IP |
| --- | --- |
| https://www.pippo.it/app1 | 11.22.33.44 |

Table 3 – Site analyzed during the course of the activities

## Findings

In the following paragraphs, the identified vulnerabilities will be describedon the analyzed application.