

{{enterprise}}

**{{ title }}**  
{{ date|datetimeformat('%B %Y') }}

**Document Confidentiality:** All information contained in the present report will remain strictly confidential. It is prohibited to copy and reproduce this document or a part of it without the expressed consent of Infobyte Security Research, even after the expiration and termination of the use of the present proposal.

Report index

[Executive Summary 3](#__RefHeading___Toc585_1974154740)

[Summary of Findings 5](#__RefHeading___Toc587_1974154740)

[Technical Summary 6](#__RefHeading___Toc589_1974154740)

[Appendix 8](#__RefHeading___Toc276_1849690061)

# **Executive** Summary

Targets Overview

During the discovery phase of this assessment {{hosts\_amount}} hosts exposing {{services\_amount}} services were found.

Findings Overview

Throughout auditing, {{vulns\_grouped\_amount}} issues were found in {{hosts\_amount}} instances, resulting in {{vulns\_amount}} vulnerabilities in total.

Total vulnerabilities by severity:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **{{counter\_severity.critical.size}}** | **{{counter\_severity.high.size}}** | **{{counter\_severity.med.size}}** | **{{counter\_severity.low.size}}** | **{{counter\_severity.info.size}}** |
| Critical | High | Medium | Low | Informational |

Scope

{{p scope }}

Objectives

{{p objectives }}

Summary

{{p summary }}

Conclusions

{{p conclusions }}

Recommendations

{{p recommendations }}

Vulnerabilities overview

Vulnerabilities overview Ease of resolution overview

{{ vulnerabilities\_image}} {{ ease\_resolution\_image }}

Impact overview

{{ impact\_image}}

{% macro severity(name) -%}{% if name == "critical" %}**Critical**{% elif name == "high" %}**High**{% elif name == "med" %}**Medium**{% elif name == "low" %}**Low**{% elif name == "info" %}**Informational**{% endif %}{% endmacro %}

# **Summary of Findings**

|  |  |  |
| --- | --- | --- |
| **Id** | **Description** | **Severity** |

{% for vuln in vulns %}

|  |  |  |
| --- | --- | --- |
| {{vuln.id}} | {{ vuln.name }} | {{ severity(vuln.severity) }} |

{% endfor %}

# Technical Summary

{%p for vuln in vulns %}

|  |  |
| --- | --- |
| **Issue {{ vuln.id }}** | **{{ vuln.name }}** |
| Severity | {{ severity(vuln.severity) }} |
| Ease of resolution | {{ vuln.easeofresolution | capitalize if not None else "---" }} |
| Impact | {{ vuln.\_\_impact\_\_ or "---"}} |

{% if vuln.type == "Vulnerability" %}

|  |
| --- |
| **Target** |

{% for key,value in vuln.parent.iteritems() %}

|  |
| --- |
| {{ value.\_\_target\_\_ }} |

{% endfor %}

{% else %}

|  |  |  |  |
| --- | --- | --- | --- |
| **Target** | **Website** | **Parameter name** | **Path** |

{% for key,value in vuln.parent.iteritems() %}

|  |  |  |  |
| --- | --- | --- | --- |
| {{ value.\_\_target\_\_ or "---"}} | {{ value.\_\_website\_\_ or "---" }} | {{ value.pname or "---" }} | {{ value.path or "---"}} |

{% endfor %}

{% endif %}

**Description**

{{p vuln.desc }}

{% if vuln.first\_parent.data %}

**Data**

{{p vuln.first\_parent.data }}

{% endif %}

{% if vuln.first\_parent.request %}

**Request**

|  |
| --- |
| *{{ vuln.first\_parent.request }}* |

{% endif %}

{% if vuln.response %}

**Response**

|  |
| --- |
| *{{ vuln.response }}* |

{% endif %}

{% if vuln.resolution %}

**Resolution**

{{ vuln.resolution }}

{% endif %}

{% if vuln.refs %}

**References**

{% for ref in vuln.refs %}

{{ ref }}{% endfor %}

{% endif %}

{%p endfor %}

# Appendix

{%p for vuln in vulns %}

* Issue {{ vuln.id }}: ***{{ vuln.name }}***

{%p for key, value in vuln.parent.iteritems() %}

* Target: {{ value.\_\_target\_\_ }}

{% if value.request %}

* Request:

|  |
| --- |
| *{{ value.request }}* |

{% endif %}

{% if value.response %}

* response:

|  |
| --- |
| *{{ value.response }}* |

{% endif %}

{% if value.evidence\_subdoc %}

* Evidence:

{{p value.evidence\_subdoc }}

{% endif %}

{%p endfor %}

{%p endfor %}