

REPORT  
of Penetration testing

{{project[‘name’]}}

Оглавление

[1 System information summary 2](#_Toc533741943)

[2 Breaf conclusion 2](#_Toc533741944)

[3 List of vulnerabilities 3](#_Toc533741945)

[3.1 Vulnerability name 3](#_Toc533741946)

[3.1.1 Example 1 3](#_Toc533741947)

[3.1.2 Example 2 4](#_Toc533741948)

# System information summary

|  |  |
| --- | --- |
| **Amount of hosts:** | {{ hosts|length }} {% set all\_hosts=hosts.keys() | list %} {% set half1=all\_hosts[::2] %} {% set half2=all\_hosts[1::2] %} |
| **List of hosts:** | |  |  | | --- | --- | | {%tr for host in half1 %} | | | {{host}} | {{half2[loop.index-1]}} | | {%tr endfor %} | | |
|  |  |
| **The work was carried out according to the OWASP methodology using the WASC recommendations.** | |

## Brief conclusion

|  |  |  |
| --- | --- | --- |
|  | **Risk level** | **Vulnerability{% set criticality = {'critical':0,'high':0,'medium':0,'low':0,'info':0} %}{% for issue\_id in issues %} {% set a = criticality.update({issues[issue\_id]['criticality']:(criticality[issues[issue\_id]['criticality']]+1)}) %}{% endfor %}** |
|  | Critical | {% if not criticality['critical'] %}Not found.{% else %}{{criticality['critical']}} vulnerabilities.{% endif %} |
|  | High | {% if not criticality['high'] %}Not found.{% else %}{{criticality['high']}} vulnerabilities.{% endif %} |
|  | Low | {% if not criticality['medium'] %}Not found.{% else %}{{criticality['medium']}} vulnerabilities.{% endif %} |
|  | Minor | {% if not criticality['low'] %}Not found.{% else %}{{criticality['low']}} vulnerabilities.{% endif %} |

## Testing results

Final results

# Testing process

## First start

1234

## Second step

1234

{% set image\_count = [1] %} {% set text\_count = [1] %}

# List of vulnerabilities {% for group\_issue\_name in grouped\_issues %}

## {{group\_issue\_name}}{% for issue\_id in grouped\_issues[group\_issue\_name] %}

### Example {{ grouped\_issues[group\_issue\_name].index(issue\_id)+1 }}

|  |  |  |
| --- | --- | --- |
| Risk level: | {{ issues[issue\_id]['criticality'].replace('critical','Critical').replace('high', 'High').replace('medium','Medium').replace('low','Low') }} | |
| Description: | | {{ issues[issue\_id]['description'] }} |
| Attacker type: | | {{ issues[issue\_id]['intruder'] }} |
| Vulnerable scenario: | | {{ issues[issue\_id]['url\_path'] }} |
| Vulnerable parameter: | | {{ issues[issue\_id]['param'] }} |
| CWE: | | {{ issues[issue\_id]['cwe'] }} |
| CVE: | | {{ issues[issue\_id]['cve'] }} |
| Technical information: | | {{ issues[issue\_id]['technical'] }} |
| Risks details: | | {{ issues[issue\_id]['risks'] }} |
| Fix recommendations: | | {{ issues[issue\_id]['fix'] }} |
| References: | | {{ issues[issue\_id]['references'] }} |
| Vulnerable servers: | | {% for port\_id in issues[issue\_id]['services'] %}{% if issues[issue\_id]['services'][port\_id]['is\_ip'] %}{{issues[issue\_id]['services'][port\_id]['ip']}}{% if ports[port\_id]['port'] != 0 %}:{{ports[port\_id]['port']}}{% endif %}{% if not loop.last %}  {% elif issues[issue\_id]['services'][port\_id]['hostnames'] %}  {% endif %}{% endif %}{% for hostname\_id in issues[issue\_id]['services'][port\_id]['hostnames'] %}{{hostnames[hostname\_id]['hostname']}}{% if ports[port\_id]['port'] != 0 %}:{{ports[port\_id]['port']}}{% endif %} {% if not loop.last %}  {% endif %} {% endfor %}{% endfor %} |
| {% if issues[issue\_id]['pocs'] %}Proof of Concept:{% endif %} | |  |

{% if issues[issue\_id]['pocs'] %}{% for poc\_id in issues[issue\_id][‘pocs’] %}{% if pocs[poc\_id][‘priority’] == 1 %}{% if pocs[poc\_id]['filetype']=='text' %}

|  |
| --- |
| {{ pocs[poc\_id]['content'] }} |

List of code {{text\_count[0]}} - {{pocs[poc\_id]['comment']}} {% if text\_count.append(text\_count.pop() + 1) %}{% endif %}{% elif pocs[poc\_id]['filetype']=='image' %}

|  |
| --- |
| {{ docx\_image(poc\_id, width=170) }} |

Image {{image\_count[0]}} - {{pocs[poc\_id]['comment']}} {% if image\_count.append(image\_count.pop() + 1) %}{%endif%}{%endif%}{%endif%}{%endfor%}{% endif %}

{% endfor -%}

{% endfor -%}