{{$root := .}}

Penetration

Test

Activity

Report

{{image .Customer.LogoReference}}

**Customer**: {{.Customer.Name}}

**Assessment Type**: {{.Assessment.Type.Full}}

**Prepared by**: Kryvea Team

**Date**: {{formatDate .DeliveryDateTime "UTC" "US"}}

**Version**: 1.0 (Final)

Table of Contents

[2 Executive Summary 3](#_Toc211197362)

[2.1 Result Summary 3](#_Toc211197363)

[3 Engagement Summary 7](#_Toc211197364)

[3.1 Rules 7](#_Toc211197365)

[3.1.1 Scope 7](#_Toc211197366)

[3.1.2 Methodology 7](#_Toc211197367)

[3.1.3 Information shared 7](#_Toc211197368)

[3.1.4 Exclusions 7](#_Toc211197369)

[3.1.5 Timeline 8](#_Toc211197370)

[4 Detailed Findings 9](#_Toc211197371)

[5 Appendices 19](#_Toc211197382)

[5.1 Appendix A - Vulnerability Severity Rating 19](#_Toc211197383)

[5.2 Appendix B - References 20](#_Toc211197384)

# Executive Summary

The penetration test against {{.Customer.Name}} was conducted between {{formatDate .Assessment.StartDateTime}} - {{formatDate .Assessment.EndDateTime}}.

The objective was to assess the security posture of {{.Assessment.Name}} and identify potential vulnerabilities that could be exploited by a malicious actor.

## Result Summary

{{if (index .Assessment.CVSSVersions "3.1")}}The most severe issue identified was a vulnerability with **{{(index .MaxCVSS "3.1").Severity}}** severity with an assigned CVSSv3.1 score of {{(index .MaxCVSS "3.1").Score}}/10.0.

**Figure 1 - Total findings**

{{end}}{{if (index .Assessment.CVSSVersions "4.0")}}The most severe issue identified was a vulnerability with **{{(index .MaxCVSS "4.0").Severity}}** severity with an assigned CVSSv4.0 score of {{(index .MaxCVSS "4.0").Score}}/10.0.

**Figure 2 - Total findings**

{{end}}

{{.Customer.Name}} responded promptly to our preliminary notifications and began remediation before the end of the testing period.

The table below provides a summary of the identified vulnerabilities and their status. {{if and (index .Assessment.CVSSVersions "3.1") (index .Assessment.CVSSVersions "4.0")}}

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Vulnerability** | **Status** | **CVSS Version** | **CVSS Score** | **Severity** | **Target** |
| {{range .Vulnerabilities}} |  |  |  |  |  |
| {{.Category.Identifier}} - {{.Category.Name}} {{if ne .DetailedTitle ""}}({{.DetailedTitle }}){{end}} | {{.Status}} | v3.1 | {{.CVSSv31.Score}} | {{tableSeverityColor .CVSSv31.Severity}}{{inlineStyledText .CVSSv31.Severity "b" "#FFFFFF"}} | {{if ne .Target.IPv4 ""}}{{.Target.IPv4}} - {{end}}  {{.Target.FQDN}} |
| v4.0 | {{.CVSSv4.Score}} | {{tableSeverityColor .CVSSv4.Severity}} {{inlineStyledText .CVSSv4.Severity "b" "#FFFFFF"}} |
|  |  |  |  |  | {{end}} |

{{else if (index .Assessment.CVSSVersions "3.1")}}

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vulnerability** | **Status** | **CVSSv3.1 Score** | **Severity** | **Target** |
| {{range .Vulnerabilities}} |  |  |  |  |
| {{.Category.Identifier}} - {{.Category.Name}} {{if ne .DetailedTitle ""}}({{.DetailedTitle }}){{end}} | {{.Status}} | {{.CVSSv31.Score}} | {{tableSeverityColor .CVSSv31.Severity}}{{inlineStyledText .CVSSv31.Severity "b" "#FFFFFF"}} | {{if ne .Target.IPv4 ""}}{{.Target.IPv4}} - {{end}}  {{.Target.FQDN}} |
|  |  |  |  | {{end}} |

{{else}}

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vulnerability** | **Status** | **CVSSv4.0 Score** | **Severity** | **Target** |
| {{range .Vulnerabilities}} |  |  |  |  |
| {{.Category.Identifier}} - {{.Category.Name}} {{if ne .DetailedTitle ""}}({{.DetailedTitle }}){{end}} | {{.Status}} | {{.CVSSv4.Score}} | {{tableSeverityColor .CVSSv4.Severity}}{{inlineStyledText .CVSSv4.Severity "b" "#FFFFFF"}} | {{if ne .Target.IPv4 ""}}{{.Target.IPv4}} - {{end}}  {{.Target.FQDN}} |
|  |  |  |  | {{end}} |

{{end}}

# Engagement Summary

## Rules

### Scope

The assessment involved the following targets: {{range .Assessment.Targets}}

* {{if ne .IPv4 ""}}{{.IPv4}} - {{end}}{{.FQDN}}{{end}}

### Methodology

The engagement followed a {{.Assessment.TestingType}} testing methodology based on:

* OWASP Testing Guide v4 - https://owasp.org/www-project-web-security-testing-guide/
* NIST SP 800-115
* PTES (Penetration Testing Execution Standard)

### Information shared

{{.Customer.Name}} shared the following information:

* Targets {{if eq .Assessment.TestingType "Gray box"}}
* Credentials{{end}}

### Exclusions

* Denial-of-Service (DoS) attacks
* Social engineering campaigns
* Physical access assessments

### Timeline

Planning activities timeline

|  |  |
| --- | --- |
| **Date** | **Activity** |
| {{formatDate .Assessment.KickoffDateTime}} | Kick-off & Scope confirmation |
| {{formatDate .Assessment.StartDateTime}} | Technical activities start |
| {{formatDate .Assessment.EndDateTime}} | Technical activities end |

# Detailed Findings {{if (index .VulnerabilitiesOverview "3.1").Critical}}

## Critical Severity{{range .Vulnerabilities}}{{if (and (index $root.Assessment.CVSSVersions "3.1") (eq .CVSSv31.Severity "Critical"))}}

### {{.Category.Identifier}} - {{.Category.Name}} {{if ne .DetailedTitle ""}}({{.DetailedTitle }}){{end}}

#### Generic vulnerability description

{{breakParagraph .GenericDescription.Text}}

#### Detailed description

{{breakParagraph .Description}}

#### Proof of Concept{{range .Poc.Pocs}}{{if eq .Type "request/response"}}

{{preserveNewline .Description}}

*{{.URI}}*

***HTTP Request***

{{range .RequestHighlighted}}{{preserveNewline (shadeTextBg .Text .Color)}}{{end}}

***HTTP Response***

{{range .ResponseHighlighted}}{{preserveNewline (shadeTextBg .Text .Color)}}{{end}}

*{{end}}{{if eq .Type "image"}}*

{{preserveNewline .Description}}

*{{.URI}}*

*{{image .ImageReference}}*

**Figure 3 – {{.ImageCaption}}**

*{{end}}{{if eq .Type "text"}}*

{{preserveNewline .Description}}

*{{.URI}}*

{{range .TextHighlighted}}{{preserveNewline (shadeTextBg .Text .Color)}}{{end}}

*{{end}}{{end}}*

#### Impact and {{if and (index $root.Assessment.CVSSVersions "3.1") (index $root.Assessment.CVSSVersions "4.0")}}CVSSv3.1 and CVSSv4.0{{else if (index $root.Assessment.CVSSVersions "3.1")}}CVSSv3.1{{else}}CVSSv4.0{{end}} score

{{if (index $root.Assessment.CVSSVersions "3.1")}}{{.CVSSv31.Description}}

CVSSv3.1 score: ***{{ .CVSSv31.Score }}***

CVSSv3.1 vector: ***{{ .CVSSv31.Vector }}***{{end}}{{if (index $root.Assessment.CVSSVersions "4.0")}}

{{.CVSSv4.Description}}

CVSSv4.0 score: ***{{ .CVSSv4.Score }}***

CVSSv4.0 vector: ***{{ .CVSSv4.Vector }}***{{end}}

#### Recommendations

{{breakParagraph .GenericRemediation.Text}} {{breakParagraph .Remediation}}

#### References

{{range .Category.References}}{{.}}

{{end}}{{range .References}}{{.}}

{{end}}{{end}}{{end}}{{end}}{{if (index .VulnerabilitiesOverview "3.1").High}}

## High Severity{{range .Vulnerabilities}}{{if (and (index $root.Assessment.CVSSVersions "3.1") (eq .CVSSv31.Severity "High"))}}

### {{.Category.Identifier}} - {{.Category.Name}} {{if ne .DetailedTitle ""}}({{.DetailedTitle }}){{end}}

#### Generic vulnerability description

{{breakParagraph .GenericDescription.Text}}

#### Detailed description

{{breakParagraph .Description}}

#### Proof of Concept{{range .Poc.Pocs}}{{if eq .Type "request/response"}}

{{preserveNewline .Description}}

*{{.URI}}*

***HTTP Request***

{{range .RequestHighlighted}}{{preserveNewline (shadeTextBg .Text .Color)}}{{end}}

***HTTP Response***

{{range .ResponseHighlighted}}{{preserveNewline (shadeTextBg .Text .Color)}}{{end}}

*{{end}}{{if eq .Type "image"}}*

{{preserveNewline .Description}}

*{{.URI}}*

*{{image .ImageReference}}*

**Figure 4 – {{.ImageCaption}}**

*{{end}}{{if eq .Type "text"}}*

{{preserveNewline .Description}}

*{{.URI}}*

{{range .TextHighlighted}}{{preserveNewline (shadeTextBg .Text .Color)}}{{end}}

*{{end}}{{end}}*

#### Impact and {{if and (index $root.Assessment.CVSSVersions "3.1") (index $root.Assessment.CVSSVersions "4.0")}}CVSSv3.1 and CVSSv4.0{{else if (index $root.Assessment.CVSSVersions "3.1")}}CVSSv3.1{{else}}CVSSv4.0{{end}} score

{{if (index $root.Assessment.CVSSVersions "3.1")}}{{.CVSSv31.Description}}

CVSSv3.1 score: ***{{ .CVSSv31.Score }}***

CVSSv3.1 vector: ***{{ .CVSSv31.Vector }}***{{end}}{{if (index $root.Assessment.CVSSVersions "4.0")}}

{{.CVSSv4.Description}}

CVSSv4.0 score: ***{{ .CVSSv4.Score }}***

CVSSv4.0 vector: ***{{ .CVSSv4.Vector }}***{{end}}

#### Recommendations

{{breakParagraph .GenericRemediation.Text}} {{breakParagraph .Remediation}}

#### References

{{range .Category.References}}{{.}}

{{end}}{{range .References}}{{.}}

{{end}}{{end}}{{end}}{{end}}{{if (index .VulnerabilitiesOverview "3.1").Medium}}

## Medium Severity{{range .Vulnerabilities}}{{if (and (index $root.Assessment.CVSSVersions "3.1") (eq .CVSSv31.Severity "Medium"))}}

### {{.Category.Identifier}} - {{.Category.Name}} {{if ne .DetailedTitle ""}}({{.DetailedTitle }}){{end}}

#### Generic vulnerability description

{{breakParagraph .GenericDescription.Text}}

#### Detailed description

{{breakParagraph .Description}}

#### Proof of Concept{{range .Poc.Pocs}}{{if eq .Type "request/response"}}

{{preserveNewline .Description}}

*{{.URI}}*

***HTTP Request***

{{range .RequestHighlighted}}{{preserveNewline (shadeTextBg .Text .Color)}}{{end}}

***HTTP Response***

{{range .ResponseHighlighted}}{{preserveNewline (shadeTextBg .Text .Color)}}{{end}}

*{{end}}{{if eq .Type "image"}}*

{{preserveNewline .Description}}

*{{.URI}}*

*{{image .ImageReference}}*

**Figure 5 – {{.ImageCaption}}**

*{{end}}{{if eq .Type "text"}}*

{{preserveNewline .Description}}

*{{.URI}}*

{{range .TextHighlighted}}{{preserveNewline (shadeTextBg .Text .Color)}}{{end}}

*{{end}}{{end}}*

#### Impact and {{if and (index $root.Assessment.CVSSVersions "3.1") (index $root.Assessment.CVSSVersions "4.0")}}CVSSv3.1 and CVSSv4.0{{else if (index $root.Assessment.CVSSVersions "3.1")}}CVSSv3.1{{else}}CVSSv4.0{{end}} score

{{if (index $root.Assessment.CVSSVersions "3.1")}}{{.CVSSv31.Description}}

CVSSv3.1 score: ***{{ .CVSSv31.Score }}***

CVSSv3.1 vector: ***{{ .CVSSv31.Vector }}***{{end}}{{if (index $root.Assessment.CVSSVersions "4.0")}}

{{.CVSSv4.Description}}

CVSSv4.0 score: ***{{ .CVSSv4.Score }}***

CVSSv4.0 vector: ***{{ .CVSSv4.Vector }}***{{end}}

#### Recommendations

{{breakParagraph .GenericRemediation.Text}} {{breakParagraph .Remediation}}

#### References

{{range .Category.References}}{{.}}

{{end}}{{range .References}}{{.}}

{{end}}{{end}}{{end}}{{end}}{{if (index .VulnerabilitiesOverview "3.1").Low}}

## Low Severity{{range .Vulnerabilities}}{{if (and (index $root.Assessment.CVSSVersions "3.1") (eq .CVSSv31.Severity "Low"))}}

### {{.Category.Identifier}} - {{.Category.Name}} {{if ne .DetailedTitle ""}}({{.DetailedTitle }}){{end}}

#### Generic vulnerability description

{{breakParagraph .GenericDescription.Text}}

#### Detailed description

{{breakParagraph .Description}}

#### Proof of Concept{{range .Poc.Pocs}}{{if eq .Type "request/response"}}

{{preserveNewline .Description}}

*{{.URI}}*

***HTTP Request***

{{range .RequestHighlighted}}{{preserveNewline (shadeTextBg .Text .Color)}}{{end}}

***HTTP Response***

{{range .ResponseHighlighted}}{{preserveNewline (shadeTextBg .Text .Color)}}{{end}}

*{{end}}{{if eq .Type "image"}}*

{{preserveNewline .Description}}

*{{.URI}}*

*{{image .ImageReference}}*

**Figure 6 – {{.ImageCaption}}**

*{{end}}{{if eq .Type "text"}}*

{{preserveNewline .Description}}

*{{.URI}}*

{{range .TextHighlighted}}{{preserveNewline (shadeTextBg .Text .Color)}}{{end}}

*{{end}}{{end}}*

#### Impact and {{if and (index $root.Assessment.CVSSVersions "3.1") (index $root.Assessment.CVSSVersions "4.0")}}CVSSv3.1 and CVSSv4.0{{else if (index $root.Assessment.CVSSVersions "3.1")}}CVSSv3.1{{else}}CVSSv4.0{{end}} score

{{if (index $root.Assessment.CVSSVersions "3.1")}}{{.CVSSv31.Description}}

CVSSv3.1 score: ***{{ .CVSSv31.Score }}***

CVSSv3.1 vector: ***{{ .CVSSv31.Vector }}***{{end}}{{if (index $root.Assessment.CVSSVersions "4.0")}}

{{.CVSSv4.Description}}

CVSSv4.0 score: ***{{ .CVSSv4.Score }}***

CVSSv4.0 vector: ***{{ .CVSSv4.Vector }}***{{end}}

#### Recommendations

{{breakParagraph .GenericRemediation.Text}} {{breakParagraph .Remediation}}

#### References

{{range .Category.References}}{{.}}

{{end}}{{range .References}}{{.}}

{{end}}{{end}}{{end}}{{end}}{{if (index .VulnerabilitiesOverview "3.1").Informational}}

## Informational {{range .Vulnerabilities}}{{if (and (index $root.Assessment.CVSSVersions "3.1") (eq .CVSSv31.Severity "Informational"))}}

### {{.Category.Identifier}} - {{.Category.Name}} {{if ne .DetailedTitle ""}}({{.DetailedTitle }}){{end}}

#### Generic vulnerability description

{{breakParagraph .GenericDescription.Text}}

#### Detailed description

{{breakParagraph .Description}}

#### Proof of Concept{{range .Poc.Pocs}}{{if eq .Type "request/response"}}

{{preserveNewline .Description}}

*{{.URI}}*

***HTTP Request***

{{range .RequestHighlighted}}{{preserveNewline (shadeTextBg .Text .Color)}}{{end}}

***HTTP Response***

{{range .ResponseHighlighted}}{{preserveNewline (shadeTextBg .Text .Color)}}{{end}}

*{{end}}{{if eq .Type "image"}}*

{{preserveNewline .Description}}

*{{.URI}}*

*{{image .ImageReference}}*

**Figure 7 – {{.ImageCaption}}**

*{{end}}{{if eq .Type "text"}}*

{{preserveNewline .Description}}

*{{.URI}}*

{{range .TextHighlighted}}{{preserveNewline (shadeTextBg .Text .Color)}}{{end}}

*{{end}}{{end}}*

#### Recommendations

{{breakParagraph .GenericRemediation.Text}} {{breakParagraph .Remediation}}

#### References

{{range .Category.References}}{{.}}

{{end}}{{range .References}}{{.}}

{{end}}{{end}}{{end}}{{end}}

# Appendices

## Appendix A - Vulnerability Severity Rating

Follows the severity description:

|  |  |
| --- | --- |
| Severity | Description |
| Critical | Exploitable remotely, full compromise |
| High | Significant impact, may require some condition |
| Medium | Partial compromise, limited scope |
| Low | Minimal impact or information disclosure |
| Informational | No direct impact but useful to attackers |

## Appendix B - References

General references about the methodology and scoring:

* + OWASP Top 10 2021 - https://owasp.org/www-project-top-ten/
  + CWE - https://cwe.mitre.org/
  + CVSS Calculator - https://www.first.org/cvss/calculator/3.1