{%p set \_ = "" %}**NAMESPACES**

{%p set ss=namespace(type\_string="") %}

{%p set bb=namespace(type\_boolean=false) %}

{%p set nn=namespace(type\_integer=0) %}

{%p set ff=namespace(type\_float=0) %}

{%p set \_ = "" %}**COLOR CODES**

{%p set ss.color\_table\_header = “430086” %}

{%p set ss.color\_CRITICAL = "8E0000" %}

{%p set ss.color\_HIGH = "FF0000" %}

{%p set ss.color\_MEDIUM = "FFC000" %}

{%p set ss.color\_LOW = "00B050" %}

{%p set ss.color\_INFORMATIONAL = "00B050" %}

{%p set \_ = "" %}**FONT COLOR CODES**

{%p set ss.font\_moderado = “000000” %}

{%p set \_ = "" %}**OPTION DEFINITIONS**

{%p set nn.cover\_page\_option = 1 %}

{%p set bb.strict\_narratives = true %}

{%p set nn.summary\_table\_option = 2 %}

{%p set nn.detailed\_findings\_option = 1 %}

{%p set bb.display\_informationals = true %}

{%p set bb.include\_raw\_evidence = false %}

{%p set ss.scope\_prefix = “” %}

{%p set bb.page\_break\_between\_findings = false %}

{%p set nn.newlines\_between\_findings = 3 %}

{%p set bb.display\_port\_data = false %}

{%p set \_ = "" %**GENERIC MACROS**

{%p macro set\_report\_field\_variable(label,error=false) %}

{%p set bb.field\_not\_found = true %}

{%p set ss.report\_field\_value = “” %}

{%p if REPORT\_INFO.fields.items() %}

{%p for key, data in REPORT\_INFO.fields.items() %}

{%p if data.label == label %}

{%p if data.value %}

{%p set ss.report\_field\_value = data.value %}

{%p set bb.field\_not\_found = false %}

{%p endif %}

{%p endif %}

{%p endfor %}

{%p endif %}

{%p if bb.field\_not\_found and error %}

{%p set ss.report\_field\_value = “NOT SET” %}

{%p endif %}

{%p endmacro %}

{%p macro set\_severity\_color(f) %}

{%p set ss.severity\_color = “” %}

{%p if f.severity == “Crítico” %}

{%p set ss.severity\_color = ss.color\_CRITICAL %}

{%p elif f.severity == “Alto” %}

{%p set ss.severity\_color = ss.color\_HIGH %}

{%p elif f.severity == “Moderado” %}

{%p set ss.severity\_color = ss.color\_MEDIUM %}

{%p elif f.severity == “Baixo” %}

{%p set ss.severity\_color = ss.color\_LOW %}

{%p elif f.severity == “Informational” %}

{%p set ss.severity\_color = ss.color\_INFORMATIONAL %}

{%p endif %}

{%p endmacro %}

{%p macro display\_spacing\_between\_findings(line\_amount) %}

{%p if bb.page\_break\_between\_findings %}

{%p else %}

{%p for i in range(line\_amount) %}

{%p endfor %}

{%p endif %}

{%p endmacro %}

{%p macro set\_cvss(f) %}

{%p set ss.cvss\_score = “” %}

{%p set ss.cvss\_vector\_string = “” %}

{%p set ss.new\_cvss3\_score = “--” %}

{%p set ss.new\_cvss3\_vector = “--” %}

{%p set ss.new\_cvss3\_subscore\_base = “--” %}

{%p set ss.new\_cvss3\_subscore\_env = “--” %}

{%p set ss.new\_cvss3\_subscore\_temp = “--” %}

{%p if f.risk\_score and f.risk\_score.CVSS3\_1 and f.risk\_score.CVSS3\_1.overall %}

{%p set ss.new\_cvss3\_score = f.risk\_score.CVSS3\_1.overall %}

{%p endif %}

{%p if f.risk\_score and f.risk\_score.CVSS3\_1 and f.risk\_score.CVSS3\_1.vector %}

{%p set ss.new\_cvss3\_vector = f.risk\_score.CVSS3\_1.vector %}

{%p endif %}

{%p if f.risk\_score and f.risk\_score.CVSS3\_1 and f.risk\_score.CVSS3\_1.subScore %}

{%p if f.risk\_score.CVSS3\_1.subScore.base != “” %}

{%p set ss.new\_cvss3\_subscore\_base = f.risk\_score.CVSS3\_1.subScore.base %}

{%p endif %}

{%p if f.risk\_score.CVSS3\_1.subScore.environmental %}

{%p set ss.new\_cvss3\_subscore\_env = f.risk\_score.CVSS3\_1.subScore.environmental %}

{%p endif %}

{%p if f.risk\_score.CVSS3\_1.subScore.temporal %}

{%p set ss.new\_cvss3\_subscore\_temp = f.risk\_score.CVSS3\_1.subScore.temporal %}

{%p endif %}

{%p set ss.new\_cvss3\_vector = f.risk\_score.CVSS3\_1.vector %}

{%p endif %}

{%p if f.risk\_score and f.risk\_score.CVSS3\_1 and f.risk\_score.CVSS3\_1.vector %}

{%p set ss.new\_cvss3\_vector = f.risk\_score.CVSS3\_1.vector %}

{%p endif %}

{%p if f.risk\_score and f.risk\_score.CVSS3\_1 and f.risk\_score.CVSS3\_1.vector %}

{%p set ss.new\_cvss3\_vector = f.risk\_score.CVSS3\_1.vector %}

{%p endif %}

{%p if f.fields and f.fields.scores and f.fields.scores.cvss3 and f.fields.scores.cvss3.value %}

{%p set ss.cvss\_score = f.fields.scores.cvss3.value %}

{%p elif f.fields and f.fields.scores and f.fields.scores.cvss and f.fields.scores.cvss.value %}

{%p set ss.cvss\_score = f.fields.scores.cvss.value %}

{%p else %}

{%p set ss.cvss\_score = “--” %}

{%p endif %}

{%p if f.fields and f.fields.scores and f.fields.scores.cvss3 and f.fields.scores.cvss3.calculation %}

{%p set ss.cvss\_vector\_string = f.fields.scores.cvss3.calculation %}

{%p elif f.fields and f.fields.scores and f.fields.scores.cvss and f.fields.scores.cvss.calculation %}

{%p set ss.cvss\_vector\_string = f.fields.scores.cvss.calculation %}

{%p else %}

{%p set ss.cvss\_vector\_string = “--” %}

{%p endif %}

{%p endmacro %}

{%p macro set\_finding\_number() %}

{%p set nn.index = nn.index + 1 %}

{%p set ss.finding\_number = nn.index|string %}

{%p endmacro %}

{%p macro summary\_table\_style\_web() %}

| **Resumo das vulnerabilidades - Web** | | | |
| --- | --- | --- | --- |
| **ID#** | **Descrição da vulnerabilidade** | **Risco** | **Reteste** |

{%p set nn.index = 0 %}

{%p for group in FINDINGS\_web %}

{%p for f in group.FINDINGS\_web %}

{{p set\_finding\_number() }}

{{p set\_severity\_color(f) }}

|  |  |  |  |
| --- | --- | --- | --- |
| 2.1.{{ ss.finding\_number }} | {{ f.title }} | **{% cellbg ss.severity\_color %}{%p if f.severity == “Moderado” %}**  **{{f.severity}}**  **{%p else %}**  **{{f.severity}}**  **{%p endif %}** | - |

{%p endfor %}

{%p endfor %}

{%p endmacro %}

{%p macro summary\_table\_style\_infra() %}

| **Resumo das vulnerabilidades – Infraestrutura [Externa/Interna]** | | | |
| --- | --- | --- | --- |
| **ID#** | **Descrição da vulnerabilidade** | **Risco** | **Reteste** |

{%p set nn.index = 0 %}

{%p for group in FINDINGS\_infra %}

{%p for f in group.FINDINGS\_infra %}

{{p set\_finding\_number() }}

{{p set\_severity\_color(f) }}

|  |  |  |  |
| --- | --- | --- | --- |
| 2.1.{{ ss.finding\_number }} | {{ f.title }} | **{% cellbg ss.severity\_color %}{%p if f.severity == “Moderado” %}**  **{{f.severity}}**  **{%p else %}**  **{{f.severity}}**  **{%p endif %}** | - |

{%p endfor %}

{%p endfor %}

{%p endmacro %}

{%p macro summary\_table\_style\_mobile() %}

| **Resumo das vulnerabilidades - Mobile** | | | |
| --- | --- | --- | --- |
| **ID#** | **Descrição da vulnerabilidade** | **Risco** | **Reteste** |

{%p set nn.index = 0 %}

{%p for group in FINDINGS\_mobile %}

{%p for f in group.FINDINGS\_mobile %}

{{p set\_finding\_number() }}

{{p set\_severity\_color(f) }}

|  |  |  |  |
| --- | --- | --- | --- |
| 2.1.{{ ss.finding\_number }} | {{ f.title }} | **{% cellbg ss.severity\_color %}{%p if f.severity == “Moderado” %}**  **{{f.severity}}**  **{%p else %}**  **{{f.severity}}**  **{%p endif %}** | - |

{%p endfor %}

{%p endfor %}

{%p endmacro %}

{%p macro display\_findings\_web() %} {#This macro is the controller for displaying summary tables. Based on the summary\_table\_style presented, it will call the appropriate format #}

{{p summary\_table\_style\_web() }}

{%p endmacro %}

{%p macro display\_findings\_infra() %} {#This macro is the controller for displaying summary tables. Based on the summary\_table\_style presented, it will call the appropriate format #}

{{p summary\_table\_style\_infra() }}

{%p endmacro %}

{%p macro display\_findings\_mobile() %} {#This macro is the controller for displaying summary tables. Based on the summary\_table\_style presented, it will call the appropriate format #}

{{p summary\_table\_style\_mobile() }}

{%p endmacro %}

{%p macro detailed\_findings\_body\_1(f) %}

{%p if f.affected\_assets %}

{%p if bb.display\_port\_data == true %}

**Affected Assets:**

{%p for asset\_id, asset\_data in f.assets.items() %}

{{asset\_data.name}}{% if asset\_data.ports %}: {% for port\_id, port\_data in asset\_data.ports.items() %}{{ port\_id}}{% if port\_data.protocol %} / {{port\_data.protocol}}{% endif %}{% if port\_data.service %} / {{port\_data.service}}{% endif %}{% if port\_data.version %} / {{port\_data.version}}{% endif %}{% endfor %}{% endif %}

{%p endfor %}

{%p else %}

**Affected Assets:** {% for asset\_id, asset\_data in f.assets.items() %}{{ asset\_data.name }}{% if not loop.last %}, {% endif %}{% endfor %}

{%p endif %}

{%p endif %}

{%p if f.fields %}

{%p for custom\_field in f.fields %}

{%p if f.fields[custom\_field].label and f.fields[custom\_field].value%}

**{{ f.fields[custom\_field].label }}**

{{p f.fields[custom\_field].value }}

{%p endif %}

{%p endfor %}

{%p endif %}

{%p if f.recommendations %}

**Recommendations:**

{%p for rec in f.recommendations %}

{{p rec }}

{%p endfor %}

{%p endif %}

{%p if f.references %}

**References:**

{%p for ref in f.references %}

{{p ref }}

{%p endfor %}

{%p endif %}

{%p if bb.include\_raw\_evidence == true %}

{%p if f.code\_samples %}

**Code Samples:**

{%p for sample in f.code\_samples %}

{%p if sample.code %}

{{ sample.code }}

{%p endif %}

{%p if sample.caption %}

{{ sample.caption }}

{%p endif %}

{%p endfor %}

{%p endif %}

{%p endif %}

{%p if f.common\_identifiers and f.common\_identifiers.CVE %}

{%p for field in f.common\_identifiers.CVE %}

{%p if field.name and field.year and field.id and field.link %}

**CVE (Name|Year|ID|Link):**

{{ field.name }}|{{ field.year }}|{{ field.id }}|{{ field.link }}

{%p elif field.name and field.year and field.id %}

**CVE (Name|Year|ID):**

{{ field.name }}|{{ field.year }}|{{ field.id }}

{%p elif field.name and field.year %}

**CVE (Name|Year):**

{{ field.name }}|{{ field.year }}

{%p elif field.name %}

**CVE (Name):**

{{ field.name }}

{%p endif %}

{%p endfor %}

{%p endif %}

{%p if f.common\_identifiers and f.common\_identifiers.CWE %}

{%p for field in f.common\_identifiers.CWE %}

{%p if field.name and field.id and field.link %}

**CWE (Name|ID|Link):**

{{ field.name }}|{{ field.id }}|{{ field.link }}

{%p elif field.name and field.id %}

**CWE (Name|ID):**

{{ field.name }}|{{ field.id }}

{%p elif field.name %}

**CWE (Name):**

{{ field.name }}

{%p endif %}

{%p endfor %}

{%p endif %}

{{p display\_spacing\_between\_findings(nn.newlines\_between\_findings) }}

{%p endmacro %}

{%p macro detailed\_findings\_style\_1() %}

{%p set nn.index = 0 %}

{%p for group in FINDINGS %}

{%p for f in group.FINDINGS %}

{{p informational\_finding\_checker(f) }}

{%p if bb.informational\_evaluation\_result %}

{{p set\_finding\_number() }}

{{p set\_severity\_color(f) }}

{{p set\_cvss(f) }}

|  |  |
| --- | --- |
| {% cellbg ss.severity\_color %}{{ ss.finding\_number }}: {{ f.title }} | {% cellbg ss.severity\_color %}**{{ f.severity }}** |

{%p if ss.cvss\_score != “--” and ss.cvss\_vector\_string != “--” %}

|  |
| --- |
| {% cellbg ss.severity\_color %}***CVSS:*** *{{ ss.cvss\_score }} |* *{{ ss.cvss\_vector\_string }}* |

{%p elif ss.cvss\_score != “--” %}

|  |
| --- |
| {% cellbg ss.severity\_color %}***CVSS:*** *{{ ss.cvss\_score }}* |

{%p endif %}

{%p if ss.new\_cvss3\_score != “--” and ss.new\_cvss3\_vector != “--” %}

|  |
| --- |
| {% cellbg ss.severity\_color %}***CVSS:*** *{{* *ss.new\_cvss3\_score }}* / *{{ ss.new\_cvss3\_vector }}* |

{%p elif ss.new\_cvss3\_score != “--” %}

|  |
| --- |
| {% cellbg ss.severity\_color %}***CVSS:*** *{{ ss.new\_cvss3\_score }}* |

{%p endif %}

{%p if ss.new\_cvss3\_subscore\_base != “--” and ss.new\_cvss3\_subscore\_env != “--” and ss.new\_cvss3\_subscore\_temp != “--” %}

|  |
| --- |
| {% cellbg ss.severity\_color %}***CVSS-Sub Score (base|env|temp):*** *{{ ss.new\_cvss3\_subscore\_base }} | {{ ss.new\_cvss3\_subscore\_env }} | {{ ss.new\_cvss3\_subscore\_temp }}* |

{%p elif ss.new\_cvss3\_subscore\_base != “--” and ss.new\_cvss3\_subscore\_env != “--” %}

|  |
| --- |
| {% cellbg ss.severity\_color %} ***CVSS-Sub Score (base|env):*** *{{ ss.new\_cvss3\_subscore\_base }} | {{ ss.new\_cvss3\_subscore\_env }}* |

{%p elif ss.new\_cvss3\_subscore\_base != “--” %}

|  |
| --- |
| {% cellbg ss.severity\_color %} ***CVSS-Sub Score(base):*** *{{ ss.new\_cvss3\_subscore\_base }}* |

{%p endif %}

|  |
| --- |
| {{p f.description }} |

{{p detailed\_findings\_body\_1(f) }}

{%p endif %}

{%p endfor %}

{%p endfor %}

{%p endmacro %}

{%p macro display\_detailed\_findings() %}

{{p detailed\_findings\_style\_1() }}

{%p endmacro %}



**MINUTA**

{{cliente\_nome}}

**{{teste\_titulo}}**

**Teste de invasão {{teste\_ambiente}}**

**{{teste\_tipo}} Box**

**{{data\_capa}}**

Documentação e revisão do documento

**MINUTA**

**Histórico de versão**:

|  |  |  |
| --- | --- | --- |
| **Versão** | **Autor** | **Data** |
| 0.1 | {{consultor\_nome}} | {data\_versao} |
| 0.2 |  |  |
| 0.3 |  |  |
| 0.4 |  |  |
| 0.5 |  |  |

Este documento foi revisado por:

|  |  |  |  |
| --- | --- | --- | --- |
| **Versão** | **Revisor** | **Data da Revisão** | |
|  | {{revisor\_nome}} | | {{data\_revisao}} |
|  |  | |  |
|  |  | |  |
|  |  | |  |
|  |  | |  |

**Conteúdo**

[1 Sumário Executivo 2](#_Toc123827440)

[1.1 Objetivo e Escopo 2](#_Toc123827441)

[1.2 Limitações do escopo e responsabilidade 9](#_Toc123827442)

[1.3 Classificação de riscos 9](#_Toc123827443)

[1.4 Resumo das vulnerabilidades 14](#_Toc123827444)

[1.5 Considerações finais 16](#_Toc123827445)

[2 Relatório detalhado 19](#_Toc123827446)

[2.1 Análise de infraestrutura 19](#_Toc123827447)

[2.1.1 Nome da vulnerabilidade 19](#_Toc123827448)

[2.1.2 Nome da vulnerabilidade 22](#_Toc123827449)

[2.1.3 Nome da vulnerabilidade 24](#_Toc123827450)

[2.1.4 Nome da vulnerabilidade 26](#_Toc123827451)

[2.2 Análise de aplicação 28](#_Toc123827452)

[2.2.1 Nome da vulnerabilidade 28](#_Toc123827453)

[3 Retestes 29](#_Toc123827454)

[3.1 Reteste [web/mobile/infra] dd/mm/aaaa 29](#_Toc123827455)

[2.1.1 Nome da vulnerabilidade 29](#_Toc123827456)

[4 Anexo 33](#_Toc123827457)

[4.1 Reteste [web/mobile/infra] dd/mm/aaaa 33](#_Toc123827458)

[2.1.1 Nome da vulnerabilidade 33](#_Toc123827459)

[5 Limitações de Escopo e Responsabilidade 35](#_Toc123827460)

[6 Contatos 37](#_Toc123827461)

Ao {{cliente\_nome}}

São Paulo, SP

{{data\_carta}}

Conforme nossa proposta, referente à prestação de serviços profissionais relacionados à assessoria em segurança da informação, nosso trabalho foi efetuado no período entre {{data\_inicio\_testes}} e {{data\_fim\_testes}}, e a emissão deste relatório confirma a conclusão parcial de nosso serviço.

Este relatório é destinado exclusivamente ao uso interno da **[RAZÃO SOCIAL]** (“**{{cliente\_nome}}**” ou [**“****Empresa”**]), portanto não poderá ser distribuído externamente a terceiros, parcialmente ou em sua íntegra, nem utilizado para outros fins sem o prévio consentimento por escrito da KPMG.

A KPMG não se responsabiliza por perdas, danos ou gastos incorridos por qualquer pessoa decorrentes da circulação, da publicação, da reprodução ou do uso não autorizados de nosso relatório.

Agradecemos a atenção dispensada e a colaboração recebida durante a realização deste trabalho e permanecemos à disposição de V.Sas. para prestar quaisquer esclarecimentos adicionais necessários.

Atenciosamente,

|  |  |
| --- | --- |
| Leandro Augusto  Sócio Líder | Luis Falconi  Gerente Sênior |

Sumário Executivo

## Objetivo e Escopo

Introdução

O **{{cliente\_nome}}** tem grande preocupação em manter um ambiente de tecnologia atualizado, primando pela segurança de seus dados e dos dados de seus clientes. Os testes de segurança EHT (Ethical Hacking Test) visam prevenir ações não autorizadas com a exploração de vulnerabilidades decorrentes de falhas ou más práticas de codificação em aplicações, falhas de configurações de infraestrutura, com relevância às informações em banco de dados, manipulação de informações e indisponibilidade.

Escopo

Com o objetivo de avaliar a segurança da {{teste\_ambiente}} executamos as atividades nos seguintes endereços:

{%p if display\_web %}

|  |  |
| --- | --- |
| **Endereço** | **IP** |
| (endereço web) |  |
|  |  |
|  |  |

{%p endif %}

{%p if display\_mobile %}

|  |  |  |
| --- | --- | --- |
| **Aplicativo** | **Versão** | |
|  | |  |
|  | |  |
|  | |  |

{%p endif %}

{%p if display\_infra %}

|  |  |  |
| --- | --- | --- |
| **Ambiente** | **IP** | |
| (interno/externo) | |  |
|  | |  |
|  | |  |

{%p endif %}

{%p if display\_infra %}

Testes de Infraestrutura [externa e/ou interna]

Nesta etapa do projeto, o nosso escopo foi voltado em mapear e analisar o ambiente do {{cliente\_nome}}, que contratou o serviço de teste de invasão [White/grey/black] box, informando os endereços listados na tabela de escopo. Foram executadas as seguintes atividades:

* Enumeramos todas as informações disponíveis do ambiente Internet e interno a partir da listagem de endereços fornecida pelo {{cliente\_nome}}.
* Mapeamos os estados das portas (TCP/UDP) de comunicação dos sistemas identificados.
* Utilizamos diferentes mecanismos de scans para ultrapassar eventuais controles de segurança e alerta.
* Analisamos por vulnerabilidades na infraestrutura e/ou aplicações que sejam escopo do projeto.
* Exploramos e reportamos as vulnerabilidades classificando em quatro diferentes níveis de risco: crítico, alto, moderado e baixo.

{%p endif %}

{%p if display\_mobile %}

Teste de invasão em aplicativos móveis

Realizamos a análise de segurança do aplicativo [nome do aplicativo], disponível para smartphones na plataforma [Android/IOS]. Buscamos por possíveis brechas de segurança no aplicativo e na comunicação com os diversos recursos do aparelho ou serviços externos.

Nossa análise em aplicativos móveis contemplamos os seguintes itens:

Captura de dados e informações

* Análise de arquitetura e framework;
* Análise de interface de comunicação;
* Análise de protocolos de comunicação;
* Análise de componentes de hardware utilizados pelo aplicativo;
* Análise da interação do aplicativo com outros serviços externos (ex: iCloud, Dropbox etc); e
* Análise de APIs utilizadas.

Análise estática

* Engenharia reversa do aplicativo instalado;
* Análise de permissões dos aplicativos aos recursos do sistema operacional;
* Análise das requisições a serviços externos, tais como web services, SMS etc.;
* Análise do processo de autenticação;
* Análise do processo de autorização;
* Análise do processo de gerenciamento de sessão;
* Análise dos dados armazenados no dispositivo;
* Análise de logs, caches e exceções;
* Análise de injeção de códigos; e
* Análise da rede e camada de transporte.

Análise dinâmica

* Análise de criptografia;
* Testes de aplicação web;
* Análise de arquivos de sistema;
* Análise da memória;
* Análise das informações trafegadas durante a utilização do aplicativo;

Análise de lógica de negócio

* Testes de análise de negócios para as seguintes transações executadas a partir do aplicativo mobile;
* Consulta de dados;
* Alteração de cadastro;
* Contratação de serviço.

Análise de segurança do servidor de back end

* Avaliar possíveis vulnerabilidades no servidor de back end (recebe as requisições dos dispositivos mobile);
* Avaliar os controles existentes contra injeção de pacotes (SQL Injection, Cross-site scripting, XML Injection etc);
* Avaliar o processo de autenticação para acesso aos serviços expostos;
* Avaliar os controles de segurança disponíveis nos serviços; e
* Avaliar o tratamento de erros e exceções.

{%p endif %}

{%p if display\_web %}

Testes de invasão na aplicação Web

Nesta etapa do projeto, o nosso escopo será voltado à execução da análise de vulnerabilidades nos domínios da {{cliente\_nome}}. Analisaremos por vulnerabilidades em seus ativos e classificaremos os riscos e as vulnerabilidades encontrados em cada uma das aplicações com uma visão Black Box (sem utilização de usuários válidos). Nossas análises utilizam práticas reconhecidas de mercado como base, conforme indicações abaixo do OWASP Testing Guide v4 (Open Web Application Security Project). Em nossos procedimentos, executaremos:

Coleta de Informações

* Condução de buscas e entendimento da aplicação (OTG-INFO-001)
* Fingerprint do servidor Web (OTG-INFO-002)
* Revisão de Metafiles do Web server (OTG-INFO-003)
* Enumeração de aplicações no Web server (OTG-INFO-004)
* Revisão de comentários e metadados nas páginas Web (OTG-INFO-005)
* Identificação de pontos de entrada da aplicação (OTG-INFO-006)
* Mapeamento de endereços da aplicação (OTG-INFO-007)
* Fingerprint do framework da aplicação (OTG-INFO-008)
* Fingerprint da aplicação Web (OTG-INFO-009)
* Mapeamento da arquitetura da aplicação (OTG-INFO-010).

Teste de gerenciamento de configuração e implementação

* Teste de configuração de infraestrutura de rede (OTG-CONF-001)
* Teste de configuração da plataforma da aplicação (OTG-CONF-002)
* Teste de extensão de arquivo (OTG-CONF-003)
* Teste de arquivos arquivos não referenciados ou de backup (OTG-CONF-004)
* Enumeração de interface administrativa (OTG-CONF-005)
* Teste de métodos HTTP (OTG-CONF-006)
* Teste HTTP *Strict Transport Security* (OTG-CONF-007)
* Teste de *Cross Domain Policy* (OTG-CONF-008)
* Teste de permissão de arquivos (OTG-CONF-009)
* Teste de *Subdomain Takeover* (OTG-CONF-010)
* Teste de armazenamento em *cloud* (OTG-CONF-011)

Teste de gestão de identidade

* Teste de definição de funções (OTG-IDNT-001)
* Teste do processo de registro de usuários (OTG-IDNT-002)
* Teste de processos de provisionamento de contas (OTG-IDNT-003)
* Teste de enumeração de contas (OTG-IDNT-004)
* Teste de política de criação de usuários (OTG-IDNT-005)

Teste de Gestão de acessos

* Teste de envio de credenciais por canal criptografado (OTG-ATHN-001)
* Teste de credenciais-padrão (OTG-ATHN-002)
* Teste para mecanismos fracos de bloqueio (OTG-ATHN-003)
* Teste para bypass de autenticação (OTG-ATHN-004)
* Teste de funcionalidade de lembrete de senha (OTG-ATHN-005)
* Teste para cache de senhas no navegador Web (OTG-ATHN-006)
* Teste para política de senha fraca (OTG-ATHN-007)
* Teste para perguntas e respostas - Reset de senha (OTG-ATHN-008)
* Testes de mecanismos fracos de reset e alteração de senha (OTG-ATHN-009)
* Teste de autenticação fraca em canais alternativos (OTG-ATHN-010)

Teste de autorização

* Teste de directory traversal/file include (OTG-ATHZ-001)
* Teste de bypass do esquema de autorização (OTG-ATHZ-002)
* Testes de escalação de privilégios (OTG-ATHZ-003)
* Testes para referências inseguras a objetos (OTG-ATHZ-004)

Testes de controle de sessão

* Teste para *bypass* do esquema de controle de sessão (OTG-SESS-001)
* Testes para atributos do cookie de sessão (OTG-SESS-002)
* Testes de fixação de sessão (OTG-SESS-003)
* Testes para variáveis de sessão expostas (OTG-SESS-004)
* Testes para *Cross-Site Request Forgery* (CSRF) (OTG-SESS-005)
* Testes para funcionalidade de logout (OTG-SESS-006)
* Testes para timeout de sessão (OTG-SESS-007)
* Testes para *Session puzzling* (OTG-SESS-008)
* Teste de roubo de sessão (OTG-SESS-009)

Testes para validação de dados de entrada

* Teste para Cross-Site Scripting Reflected (OTG-INPV-001)
* Teste para Stored Cross-Site Scripting (OTG-INPV-002)
* Teste para HTTP Verb Tampering (OTG-INPV-003)
* Teste para HTTP Parameter pollution (OTG-INPV-004)
* Teste para SQL Injection (OTG-INPV-005)
* Teste para LDAP Injection (OTG-INPV-006)
* Teste para XML Injection (OTG-INPV-007)
* Teste para SSI Injection (OTG-INPVAL-008)
* Teste para XPath Injection (OTG-INPVAL-009)
* Teste para IMAP/SMTP Injection (OTG-INPVAL-010)
* Teste para Code Injection (OTG-INPVAL-011)
* Teste para Command Injection (OTG-INPVAL-012)
* Teste para Format String Injection (OTG-INPVAL-013)
* Teste para vulnerabilidades incubadas (OTG-INPVAL-014)
* Teste para HTTP Splitting/Smuggling (OTG-INPVAL-015)
* Teste para HTTP Incoming Request(OTG-INPVAL-016)
* Teste para Header Injection (OTG-INPVAL-017)
* Teste de Server Side Template Injection (OTG-INPVAL-018)
* Teste de Server-Side Request Forgering (OTG-INPVAL-019)

Testes de manipulação de erro

* Análise de tratamento de códigos de erros (OTG-ERRH-001)
* Análise de *Stack Traces* (OTG-ERRH-002).

Testes de criptografia fraca

* Teste para cifras fracas SSL/TLS (OTG-CRYP-001)
* Teste para Padding Oracle (OTG-CRYP-002)
* Teste para envio de informações sensíveis via canais sem criptografia (OTG-CRYP-003)
* Teste de criptografia fraca(OTG-CRYP-004)

Business Logic Testing

* Teste para validação de dados de lógica de negócio (OTG-BUSL-001)
* Teste para forjar requisições (OTG-BUSL-002)
* Teste para checagem de integridade (OTG-BUSL-003)
* Teste para Process Timing (OTG-BUSL-004)
* Teste para limite de uso de funcionalidades (OTG-BUSL-005)
* Teste para verificação de Work Flows (OTG-BUSL-006)
* Teste de defesa contra mal uso da aplicação (OTG-BUSL-007)
* Teste de upload de extensões de arquivos inesperadas (OTG-BUSL-008)
* Teste de upload de arquivos maliciosos (OTG-BUSL-009).

Teste para Client Side

* Teste para DOM based Cross-Site Scripting (OTG-CLNT-001)
* Teste para JavaScript Execution (OTG-CLNT-002)
* Teste para HTML Injection (OTG-CLNT-003)
* Teste para Client Side URL Redirect (OTG-CLNT-004)
* Teste para CSS Injection (OTG-CLNT-005)
* Teste para Client Side Resource Manipulation (OTG-CLNT-006)
* Teste para Cross Origin Resource Sharing (OTG-CLNT-007)
* Teste para Cross-Site Flashing (OTG-CLNT-008)
* Teste para Clickjacking (OTG-CLNT-009)
* Teste para WebSockets (OTG-CLNT-010)
* Teste para Web Messaging (OTG-CLNT-011)
* Teste para Browser Storage (OTG-CLNT-012).
* Teste para Cross Site Script Inclusion (OTG-CLNT-013).

{%p endif %}

## Limitações do escopo e responsabilidade

Ressaltamos que, por não ter sido requisitado pela **{{cliente\_nome}}**, não fez parte do escopo deste trabalho a aplicação de testes para avaliar a precisão e/ou a valorização dos dados ou das informações geradas a partir dos sistemas da **{{cliente\_nome}}**, como:

* Validação dos procedimentos e das rotinas de cálculos implementados nos sistemas;
* Consistência e avaliação dos tipos de indexadores, taxas e/ou fórmulas parametrizadas nos sistemas;
* Verificação e análise dos procedimentos e controles voltados à execução dos backups e recuperação das informações armazenadas;
* Procedimentos e tecnologia utilizada para atualização tecnológica dos ambientes computacionais;
* Avaliação dos controles e procedimentos operacionais para o acionamento do ambiente de contingência;
* Avaliação dos controles de acesso físicos implementados nos ambientes computacionais.

Nosso escopo de atuação abrangeu especificamente os descritos acima não contemplando outros procedimentos que os não descritos neste documento.

## Classificação de riscos

As vulnerabilidades identificadas foram classificadas em quatro diferentes níveis de risco: crítico, alto, moderado e baixo. O critério utilizado leva em consideração os seguintes fatores:

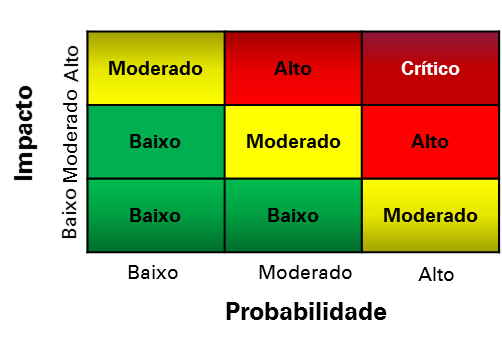
**Impacto**: consequência negativa que uma vulnerabilidade pode trazer ao ambiente tecnológico e/ou ao negócio. A composição do impacto é dada pelos seguintes fatores:

* Impacto para o negócio: consequências negativas para o negócio caso o risco seja materializado;
* Impacto técnico: consequências negativas no ambiente tecnológico após a exploração de uma vulnerabilidade e a materialização do risco;
* Materialização do risco: define se um risco é potencial (pode acontecer), real (risco existente) ou se foi materializado;
* Informação capturada: define a criticidade e a relevância das informações obtidas durante o ataque;
* Risco a imagem: impactos causados para os clientes no caso da exploração das vulnerabilidades.

**Probabilidade**: expectativa para que uma determinada falha seja explorada. Os seguintes critérios são utilizados para compô-la:

* Conhecimento técnico: define o nível de conhecimento técnico do atacante para explorar uma vulnerabilidade;
* Ambiente: nível de exposição do ambiente, facilidade de acesso e controles existentes para proteção do perímetro;
* Facilidade de descoberta: divulgação de uma determinada falha e/ou esforço necessário para encontrar uma vulnerabilidade no ambiente;
* Facilidade de exploração: mecanismos utilizados para explorar uma vulnerabilidade, tais como ferramentas, desenvolvimento de scripts etc.;
* Motivação: fator motivação do atacante para exploração de uma vulnerabilidade ou obtenção de informações.

Todos esses critérios de classificação seguem padrões de mercado, tais como: CVSS, NIST800-39, ISO27005 e OWASP.



As tabelas a seguir representam os critérios utilizados para classificar a probabilidade e impacto das vulnerabilidades:

A tabela a seguir representa os critérios utilizados para classificar o **impacto**:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risco** | **Impacto para o negócio** | **Impacto tecnológico** | **Materialização do risco** | **Informação capturada** | **Risco a imagem** |
| **Alto** | * Alteração de regras de negócio ou fraudes * Causar impactos financeiros ou risco de imagem * Riscos de continuidade para o negócio | * Indisponibilidade de sistemas críticos * Acesso a recursos computacionais com privilégios elevados | * Risco materializado | * Informações confidenciais * Dados relevantes de clientes * Dados que possam causar impacto de *compliance* | * Impacto na reputação da marca * Rescisão dos serviços contratados |
| **Moderado** | * Impactos financeiros ou fraudes, porém existem controles compensatórios de monitoramento | * Acesso limitado a recursos computacionais * Falhas de controles que podem levar a explorações de outras vulnerabilidades * Indisponibilidade de sistemas não críticos | * Risco real | * Acesso parcial a informações confidenciais * Informações técnicas relevantes | * Perda de confiança da marca |
| **Baixo** | * Não causam impactos para o negócio | * Conhecimento técnico do ambiente e arquitetura (mapeamento) | * Risco potencial | * Dados técnicos de baixa relevância * Dados do negócio ou clientes, mas sem relevância * Informação criptografada * Informações públicas | * Baixa ou nenhuma insatisfação do cliente |

A tabela a seguir representa os critérios utilizados para classificar a **probabilidade**:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risco** | **Conhecimento técnico** | **Ambiente** | **Facilidade de descoberta** | **Facilidade de exploração** | **Motivação** |
| **Alto** | * Conhecimentos básicos de tecnologia | * Ambiente público (internet) * Camada única de proteção * Ausência de controles tecnológicos nos *endpoints* | * Vulnerabilidades facilmente identificadas, seja de forma manual ou por meio de ferramentas automatizadas * Google *Hacking* | * *Exploits* publicados na internet * Ferramentas de mercado, sendo a maior parte open *source* * Manipulação de ferramentas simples * Requer baixa capacidade computacional * Sem necessidade de credenciais especiais * Facilidade para execução de ataques em massa | * Acesso as informações em tempo real * Acesso a informações sensíveis ou dados de clientes * Ganhos financeiros * Sequestro de informações (*ransomware*) * Acesso a informações da concorrência * Hacktivismo |
| **Moderado** | * Conhecimentos em técnicas de *pen test* * Usuários avançados em tecnologia | * Ambiente público com controles elevados de proteção (chegando a um rápido bloqueio) * Ambiente interno com controles frágeis * Mais de uma camada de proteção * Redes segregadas, mas de fácil acesso físico | * Falhas escondidas * Necessidade de conhecimento prévio do ambiente | * Ferramentas de mercado, sendo algumas pagas ($) * Necessário algum tipo de acesso lógico * A exploração leva a provas de conceito (POC) | * Necessita persuadir ou atacar terceiros * Baixo retorno financeiro ou pulverizado |
| **Baixo** | * Conhecimentos de linguagens de programação de baixo nível * Desenvolvimento de *exploits* | * Ambiente interno controlado * Controles na rede que impeçam o uso de equipamentos não autorizados * Segregação de redes com acessos restritos | * Vulnerabilidades *zero-day* | * Não possui *exploits* ou requerem modificações * Ferramentas de mercado pagas ($$$$) * Desenvolvimento de ferramentas específicas * APT | * Requer muito tempo para chegar a um resultado * Sem retorno financeiro |

## Resumo das vulnerabilidades

Na tabela abaixo apresentamos a vulnerabilidades identificadas:

{%p if display\_web %}

{{p display\_findings\_web()}}

{%p endif %}

{%p if display\_infra %}

{{p display\_findings\_infra()}}

{%p endif %}

{%p if display\_mobile %}

{{p display\_findings\_mobile()}}

{%p endif %}

## Considerações finais

Este relatório descreve as vulnerabilidades encontradas na análise {{teste\_tipo}} Box (Simulando um ataque real feito por um Hacker) do cliente “{{cliente\_nome}}”.

Tais vulnerabilidades foram classificadas de acordo com o impacto que podem gerar e a probabilidade de ocorrência, de modo que se pôde obter o fator de risco associado a cada uma delas. Deste modo, será possível tratar da maneira mais apropriada os riscos ao seu negócio com o objetivo de reduzir e/ou mitigar situações que possam gerar incidentes que tragam perdas por vazamento de informações, acessos indevidos, alterações não autorizadas e qualquer outra situação que exponha negativamente os usuários desses sistemas e/ou a imagem da KPMG.

Na análise, foram identificados diversas vulnerabilidades que podem comprometer o [sistema/ambiente], sendo as principais:

{%p if display\_web %}

Aplicações Web: Na análise das aplicações Web, foram identificados diversas vulnerabilidades que podem comprometer o sistema, sendo as principais: [título e breve descritivo das vulnerabilidades, => moderado], [título e breve descritivo das vulnerabilidades, => moderado], entre outras vulnerabilidades descritas em mais detalhes neste relatório.

{%p endif %}

{%p if display\_mobile %}

Aplicações Mobile: Na análise das aplicações Mobile, foram identificados diversas vulnerabilidades que podem comprometer o sistema, sendo as principais: [título e breve descritivo das vulnerabilidades, => moderado], [título e breve descritivo das vulnerabilidades, => moderado], entre outras vulnerabilidades descritas em mais detalhes neste relatório.

{%p endif %}

{%p if display\_infra %}

Infraestrutura Externa: [título e breve descritivo das vulnerabilidades, => moderado], [título e breve descritivo das vulnerabilidades, => moderado], entre outras vulnerabilidades descritas em mais detalhes neste relatório.

Infraestrutura Interna: [título e breve descritivo das vulnerabilidades, => moderado], [título e breve descritivo das vulnerabilidades, => moderado], entre outras vulnerabilidades descritas em mais detalhes neste relatório.

{%p endif %}

Recomendamos à direção da **{{cliente\_nome}}** que enderece as correções dessas vulnerabilidades, priorizando seu tratamento de acordo com o nível de risco associado a cada uma delas, demonstrando diligencia ao gerir os riscos do seu negócio de maneira adequada, visando acima de tudo, a manutenção da integridade de seus dados e da confidencialidade de suas informações.

Durante a fase de retestes, foi verificado que todas as vulnerabilidades foram corrigidas.

Relatório detalhado

{%p if display\_infra %}

## Análise de infraestrutura [Externa/Interna]

{% for i in range(1, num\_pontos\_infra+1) %}

### Nome da vulnerabilidade

|  |  |  |
| --- | --- | --- |
| Probabilidade | Impacto | Risco |
| **Alto** | **Alto** | **Crítico** |

Descrição

[DESCRIÇÃO].

Impacto

[IMPACTO].

Recomendação

[RECOMENDAÇÃO].

Referência técnica

[REFERÊNCIA].

Evidências



Figura 1 - Legenda de Imagem



Figura 2 - Outra legenda da imagem

Hosts vulneráveis

|  |  |
| --- | --- |
| Hosts | Portas |
|  |  |
|  |  |
|  |  |

{% endfor %}

{%p endif %}

{%p if display\_web %}

## Análise de Aplicação Web

{% for i in range(1, num\_pontos\_web +1) %}

### Nome da vulnerabilidade

|  |  |  |
| --- | --- | --- |
| Probabilidade | Impacto | Risco |
| **Alto** | **Alto** | **Crítico** |

Descrição

[DESCRIÇÃO].

Impacto

[IMPACTO].

Recomendação

[RECOMENDAÇÃO].

Referência técnica

[REFERÊNCIA].

Evidências



Figura 1 - Legenda de Imagem



Figura 2 - Outra legenda da imagem

Hosts vulneráveis

|  |  |
| --- | --- |
| Hosts | Portas |
|  |  |
|  |  |
|  |  |

{% endfor %}

{%p endif %}

{%p if display\_mobile %}

## Análise de Mobile

{% for i in range(1, num\_pontos\_mobile+1) %}

### Nome da vulnerabilidade

|  |  |  |
| --- | --- | --- |
| Probabilidade | Impacto | Risco |
| **Alto** | **Alto** | **Crítico** |

Descrição

[DESCRIÇÃO].

Impacto

[IMPACTO].

Recomendação

[RECOMENDAÇÃO].

Referência técnica

[REFERÊNCIA].

Evidências



Figura 1 - Legenda de Imagem



Figura 2 - Outra legenda da imagem

Hosts vulneráveis

|  |  |
| --- | --- |
| Hosts | Portas |
|  |  |
|  |  |
|  |  |

{% endfor %}

{%p endif %}

Retestes

## Reteste [web/mobile/infra] dd/mm/aaaa

| **Resumo das vulnerabilidades – [Web/Mobile/Infraestrutura]** | | | |
| --- | --- | --- | --- |
| **ID#** | **Descrição da vulnerabilidade** | **Risco** | **Reteste** |
| 2.1.1 | Nome da Vulnerabilidade | **Crítico** | **Corrigido** |
| 2.1.2 | Nome da Vulnerabilidade | **Alto** | **Corrigido** |
| 2.1.3 | Nome da Vulnerabilidade | **Moderado** | **Não Corrigido** |
| 2.1.4 | Nome da Vulnerabilidade | **Baixo** | **Não Corrigido** |

### 2.1.1 Nome da vulnerabilidade

|  |  |  |
| --- | --- | --- |
| Risco | Reteste | |
| **Crítico** | | **Corrigido** |

Descrição

Durante o reteste foi identificado que [DESCRIÇÃO].

Evidências

Figura 1 - Legenda de Imagem



Figura 2 - Outra legenda da imagem

Hosts vulneráveis

Anexo

## Reteste [web/mobile/infra] dd/mm/aaaa

| **Resumo das vulnerabilidades – [Web/Mobile/Infraestrutura]** | | | |
| --- | --- | --- | --- |
| **ID#** | **Descrição da vulnerabilidade** | **Risco** | **Reteste** |
| 2.1.1 | Nome da Vulnerabilidade | **Crítico** | **Corrigido** |
| 2.1.2 | Nome da Vulnerabilidade | **Alto** | **Não Corrigido** |
| 2.1.3 | Nome da Vulnerabilidade | **Moderado** | **Não Corrigido** |
| 2.1.4 | Nome da Vulnerabilidade | **Baixo** | **Não Corrigido** |

### 2.1.1 Nome da vulnerabilidade

|  |  |  |
| --- | --- | --- |
| Risco | Reteste | |
| **Crítico** | | **Corrigido** |

Descrição

Durante o reteste foi identificado que [DESCRIÇÃO].

Evidências



Figura 1 - Legenda de Imagem



Figura 2 - Outra legenda da imagem

Hosts vulneráveis

|  |  |
| --- | --- |
| Hosts | Portas |
|  |  |
|  |  |
|  |  |

Limitações de Escopo e Responsabilidade

Os resultados apresentados neste relatório representam a situação encontrada durante nossos levantamentos, no período compreendido entre {{data\_inicio\_testes}} e {{data\_fim\_testes}} divididos em suas respectivas etapas conforme detalhado em outros capítulos deste relatório e de acordo com os respectivos itens de escopo apresentados neste relatório, não considerando eventuais aspectos de controle ou fragilidades que eventualmente venham a ser manifestados após esse período.

Durante os nossos trabalhos, não realizamos testes de capacidade, de alta performance ou stress testing para aferição de métricas do tempo de resposta das aplicações e/ou dos recursos computacionais utilizados pelo {{cliente\_nome}}e/ou Impactos que o seu uso possa acarretar às aplicações corporativas.

A **KPMG** não assegura nem assegurará o {{cliente\_nome}} o sucesso da implementação do resultado dos serviços nem assegura ou assegurará que tal se verifique em qualquer prazo tampouco responderá por eventuais oportunidades que deixem de ser identificadas, apresentadas ou exploradas, independentemente dos motivos ou das razões para tais ocorrências.

O {{cliente\_nome}} reconhece que os serviços objeto do presente não constituem uma auditoria de sistemas, e os resultados deles decorrentes não deverão ser assim interpretados ou utilizados para os fins a que se prestaria um processo ou resultado de uma auditoria.

Limitações de divulgação deste relatório

A utilização deste relatório deverá servir exclusivamente para uso interno da Administração do {{cliente\_nome}}. Portanto, este relatório não poderá ser distribuído externamente a terceiros, parcialmente ou em sua íntegra, nem utilizado em eventual processo judicial sem o prévio consentimento por escrito da **KPMG.**

Esclarecemos que quaisquer conselhos, recomendações e informações, no âmbito da prestação dos serviços pela **KPMG**, são fornecidos em caráter confidencial. Considerando que a **KPMG** não pode controlar, intervir ou gerir o uso de informações orais ou escritas transmitidas pelo {{cliente\_nome}}, V.Sas. concordam que o uso ou a revelação, pelo {{cliente\_nome}}, de qualquer parte deste relatório, em qualquer hipótese e para qualquer finalidade, ocorrerá exclusivamente com base na avaliação da conveniência e da oportunidade que o {{cliente\_nome}}realizar por seus administradores ou assessores e, portanto, sob risco e responsabilidade totais e exclusivos do {{cliente\_nome}}.

Nesses termos, fica certo e ajustado entre a **KPMG** e o {{cliente\_nome}} que o ato de o {{cliente\_nome}} usar ou revelar qualquer parte dos resultados apresentados neste relatório implicará a automática concordância deste, e a assunção da obrigação correspondente, em responder por ele, pela **KPMG** ou por terceiros, incluindo os profissionais da **KPMG** e outras pessoas jurídicas ou naturais que vierem a ser alocadas à execução dos serviços pela **KPMPG,** por qualquer consequência, dano ou prejuízo resultante de tal uso ou revelação do material.

A **KPMG** não se responsabiliza por nenhuma perda, dano ou gasto incorrido por qualquer pessoa decorrente da circulação, da publicação, da reprodução ou do uso não autorizados de nosso relatório.

Contatos

Leandro Antonio

Sócio Líder

Cyber Security

**T:** +55 11 3940-3740

**E:** lantonio@kpmg.com.br

Luis Falconi

Gerente Sênior

Cyber Security

**T:** +55 11 3940-4115 / 98176-9340

**E:** lfalconi@kpmg.com.br