Diretoria de Segurança Corporativa

Superintendência de Segurança da Informação

Gerência de Engenharia de Segurança da Informação

**Relatório de análise de vulnerabilidade WEB**



Tabela de Conteúdo

[1. Informações 3](#_Toc481660339)

[2. Uso Deste Relatório 3](#_Toc481660340)

[3. Limitações 3](#_Toc481660341)

[4. Vulnerabilidades 3](#_Toc481660342)

[4.1. Representação das vulnerabilidades 4](#_Toc481660343)

[4.2. Classificação de vulnerabilidades OWASP Top 10 (2013) 5](#_Toc481660344)

[4.3. Sumário Executivo 6](#_Toc481660345)

[5. Descrição Técnica dos Resultados 7](#_Toc481660346)

[5.1. Detalhamento das Vulnerabilidades 7](#_Toc481660347)

[6. Sumário da Classificação de Risco 12](#_Toc481660348)

[6.1. Parâmetros para classificação de severidade 12](#_Toc481660349)

[7. Prazos para correção das vulnerabilidades encontradas 13](#_Toc481660350)

# Informações

|  |  |
| --- | --- |
| Contato | DSC\_SSI\_GESI\_EGV@correio.itau.com.br |
| Data de início dos testes | DD/MM/AAAA |
| Data de conclusão dos testes | DD/MM/AAAA |
| URL analisada | [URL] |
| Escopo da análise | [Incluir escopo] |

# Uso Deste Relatório

Este relatório tem por objetivo enumerar as vulnerabilidades encontradas na aplicação no momento da análise e auxiliar na mitigação destas.

Nossa análise não se destina a buscar ou expressar um parecer de auditoria nos processos de informação e procedimentos e não constitui, portanto, uma auditoria, e não deve ser considerada como tal.

Este relatório destina-se exclusivamente para o uso do Banco Itaú.

# Limitações

Salientamos que o resultado apresentado neste relatório reflete apenas o momento em que o site/aplicação foi analisado(a) e aponta vulnerabilidades encontradas, sem contudo garantir que todas as possíveis vulnerabilidades existentes no site/aplicação estejam relatadas neste documento.

# Vulnerabilidades

A análise identificou os seguintes números quanto às vulnerabilidades:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Vulnerabilidade(s) identificada(s) Classificação do Risco | Crítico | Alto | Médio | Baixo | Informativo |
| Quantidade | 0 | 0 | 0 | 0 | 0 |

## Representação das vulnerabilidades

|  |  |  |
| --- | --- | --- |
| **AN[[1]](#footnote-1)- Título da Vulnerabilidade** | | |
| **Número e título da CWE** | | |
| **Cor do Risco** | **Nível de Risco** | **Código de Cor** |
| Crítico |  |
| Alto |  |
| Médio |  |
| Baixo |  |
| Informativo |  |
| **Ativo, Aplicação ou URL afetado** | | |
| URL afetada. | | |
| **Vulnerabilidade** | | |
| Descrição da Vulnerabilidade. | | |
| **Risco** | | |
| O possível impacto se a vulnerabilidade for explorada com sucesso. | | |
| **Resultados e informações adicionais** | | |
| Prova de Conceito (se houver). | | |
| **Mitigação do Risco e Recomendações** | | |
| Soluções de contorno para mitigar/eliminar o risco. | | |
| **Referências** | Referências online, informações sobre a vulnerabilidade e possíveis soluções ou contramedidas. | |

## Classificação de vulnerabilidades OWASP Top 10 (2013)

|  |  |
| --- | --- |
| **AN** | **Descrição - OWASP Top 10 (2013)** |
| **A1** | **Injection** |
| **A2** | **Broken Authentication and Session Manegement** |
| **A3** | **Cross-Site Scripting** |
| **A4** | **Insecure Direct Object Reference** |
| **A5** | **Security Misconfiguration** |
| **A6** | **Sensitive Data Exposure** |
| **A7** | **Missing Function Level Access Control** |
| **A8** | **Cross-site Request Forgery** |
| **A9** | **Using Components with Known Vulnerabilities** |
| **A10** | **Unvalidate Redirects and Forwards** |

## Sumário Executivo

A tabela abaixo demonstra quais as vulnerabilidades encontradas, assim como seu impacto e risco:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nº** | **Risco** | **Vulnerabilidade** | **Impacto** | **Status** |
|  | **Crítico** | **Nome da Vulnerabilidade** | Descrição do impacto |  |
|  | **Alto** | **Nome da Vulnerabilidade** | Descrição do impacto |  |
|  | **Médio** | **Nome da Vulnerabilidade** | Descrição do impacto |  |
|  | **Baixo** | **Nome da Vulnerabilidade** | Descrição do impacto |  |
|  | **Informativo** | **Nome da Vulnerabilidade** | Descrição do impacto |  |

# Descrição Técnica dos Resultados

## Detalhamento das Vulnerabilidades

|  |
| --- |
| **Vulnerabilidades Críticas** |

|  |  |  |
| --- | --- | --- |
|  | **Título da vulnerabilidade** | **Crítica** |
| **CWE-** | **Título da CWE** |

**Ativo, Aplicação ou URL afetado**

<inserir URL>

**Vulnerabilidade**

Descrever vulnerabilidade encontrada.

**Risco**

Descrever risco/impacto que a vulnerabilidade oferece.

**Resultados e informações adicionais**

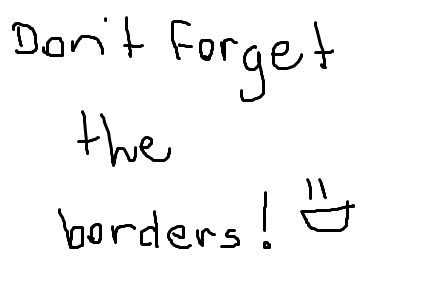
****

Figura – Legenda

**Recomendações de correção**

Mitigações para a vulnerabilidade.

**Referências**

Colocar referências.

|  |
| --- |
| **Vulnerabilidades Altas** |

|  |  |  |
| --- | --- | --- |
|  | **Título da vulnerabilidade** | **Alta** |
| **CWE-** | **Título da CWE** |

**Ativo, Aplicação ou URL afetado**

<inserir URL>

**Vulnerabilidade**

Descrever vulnerabilidade encontrada.

**Risco**

Descrever risco/impacto que a vulnerabilidade oferece.

**Resultados e informações adicionais**

**Recomendações de correção**

Mitigações para a vulnerabilidade.

**Referências**

Colocar referências.

|  |
| --- |
| **Vulnerabilidades Médias** |

|  |  |  |
| --- | --- | --- |
|  | **Título da vulnerabilidade** | **Média** |
| **CWE-** | **Título da CWE** |

**Ativo, Aplicação ou URL afetado**

<inserir URL>

**Vulnerabilidade**

Descrever vulnerabilidade encontrada.

**Risco**

Descrever risco/impacto que a vulnerabilidade oferece.

**Resultados e informações adicionais**

**Recomendações de correção**

Mitigações para a vulnerabilidade.

**Referências**

Colocar referências.

|  |
| --- |
| **Vulnerabilidades Baixas** |

|  |  |  |
| --- | --- | --- |
|  | **Título da vulnerabilidade** | **Baixa** |
| **CWE-** | **Título da CWE** |

**Ativo, Aplicação ou URL afetado**

<inserir URL>

**Vulnerabilidade**

Descrever vulnerabilidade encontrada.

**Risco**

Descrever risco/impacto que a vulnerabilidade oferece.

**Resultados e informações adicionais**

**Recomendações de correção**

Mitigações para a vulnerabilidade.

**Referências**

Colocar referências.

|  |
| --- |
| **Vulnerabilidades Informativas** |

|  |  |  |
| --- | --- | --- |
|  | **Título da vulnerabilidade** | **Informativa** |
| **CWE-** | **Título da CWE** |

**Ativo, Aplicação ou URL afetado**

<inserir URL>

**Vulnerabilidade**

Descrever vulnerabilidade encontrada.

**Risco**

Descrever risco/impacto que a vulnerabilidade oferece.

**Resultados e informações adicionais**

**Recomendações de correção**

Mitigações para a vulnerabilidade.

**Referências**

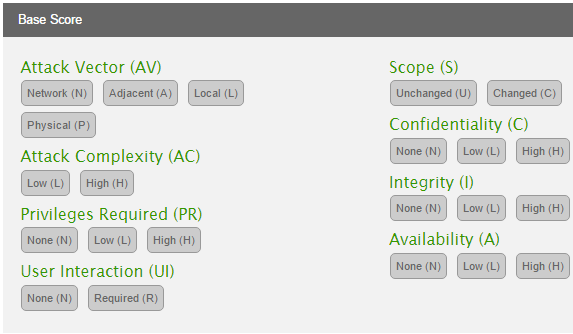
Colocar referências.

# Sumário da Classificação de Risco

Nossa análise de risco é baseada em recomendações do “National Institute of Standard and Techonology” - NIST no documento “Guide for Information technology Systems” disponível no endereço http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, na lista de 2013 de Top 10 Vulnerabilidades mais frequentes da Open Web Application Security Project (OWASP) no endereço https://www.owasp.org/index.php/Top\_10\_2013-Top\_10 e na classificação de risco disponível na circular interna “Gestão de Riscos em Segurança da Informação”.

## Parâmetros para classificação de severidade

Os parâmetros utilizados para a classificação são baseados na metodologia aplicada pelo CVSS (Common Vulnerability Scoring System).



A pontuação base (Base Score) representa as características intrínsecas de uma vulnerabilidade que são constantes. É composta de dois conjuntos de métricas: as métricas de exploração e as de impacto.

As métricas de exploração são: vetor de ataque (rede, redes adjacentes, local, físico), complexidade de ataque (baixa, alta), privilégios requeridos (nenhum, baixo, alto), interação de usuário (nenhuma, requerida).

As métricas de impacto são: impacto na confidencialidade (nenhum, baixo, alto), impacto na integridade (nenhum, baixo, alto), impacto na disponibilidade (nenhum, baixo, alto).

A métrica global considerada é o escopo (muda, não muda), ou seja, se a exploração da vulnerabilidade levaria a uma mudança no escopo pretendido da funcionalidade.

Ao final, é calculada a severidade generalizada da vulnerabilidade, a qual utilizamos como base para informar a severidade dentro do contexto em que a aplicação se insere.

|  |  |
| --- | --- |
| **Severidade** | **Exemplos de classificação de vulnerabilidades** |
| Crítica | **SQL Injection com usuário da aplicação possuindo privilégio de DBA.**  A exploração desta vulnerabilidade comprometeria simultaneamente a disponibilidade, integridade e confidencialidade das informações, caracterizando um impacto crítico. |
| Alta | **XSS (Cross-Site Scripting)**  A exploração desta vulnerabilidade comprometeria a integridade e confidencialidade das informações, caracterizando um impacto alto. |
| Média | **Mecanismo de bloqueio de conta.**  A exploração desta vulnerabilidade comprometeria a disponibilidade da funcionalidade de login da aplicação através de um ataque de Negação de Serviço, caracterizando um impacto médio. |
| Baixa | **Vazamento de informações através de mensagens de erro.**  A exploração desta vulnerabilidade não comprometeria diretamente a aplicação, porém as informações obtidas podem ser utilizadas para realizar ataques mais elaborados à aplicação. |

# Prazos para correção das vulnerabilidades encontradas

Prazo para correção de acordo com o documento Procedimento Análise de Vulnerabilidade disponível no link:

http://sscorp2.itau/sites/dsc/lib\_seguranca\_informacao\_canais/pages/analise\_vulnerabilidade.aspx

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Novas aplicações | | | | | |
| Plano de ação | Ação | Crítica | Alta | Média | Baixa |
| Elaboração | Correção | N/A | N/A | N/A | 15 dias |
| Comunicação para Superintendente | N/A | N/A | N/A | 25 dias pós produção |
| Comunicação para Diretor | N/A | N/A | N/A | 35 dias pós produção |
| Abertura de OY | N/A | N/A | N/A | 45 dias pós produção |
| Correção | Prazo para conclusão | Imediata | Imediata | Imediata | Imediata pós prazo |
| Abertura de OY | Imediata pós produção | Imediata pós produção | Imediata pós produção | 15 dias pós prazo |

1. Classificação de vulnerabilidade baseada na OWASP Top 10 no ano de 2013. Para consulta da descrição ver seção 3.3. [↑](#footnote-ref-1)