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/AAA1 |
| Data de conclusão dos testes | DD/MM/AAA2 |
| 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 | n\_critical | n\_high | n\_medium | n\_low | n\_info |

## 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** |

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