



**Ministério
da Economia**

Documento Relatório de Teste

Prova de Conceito – TaxiGov - RN

Ministério da Economia
Diretoria de Tecnologia da informação - DTI
Coordenação-Geral de Sistemas

Versão 1.0

Sumário

1	Controle de Revisão.....	2
2	Identificação da Demanda	2
3	Finalidade	2
4	Escopo	2
4.1	Não Escopo	3
5	Recursos Necessários	3
5.1	Recursos Humanos.....	3
6	Resultados Obtidos.....	3
6.1	Requisitos de Acessibilidade.....	3
6.2	Requisitos de Funcionalidade.....	4
6.3	Requisitos de Disponibilidade.....	6
6.3.1	Disponibilidade de 96%	6
6.3.2	Desempenho – 25 corridas.....	9
6.4	Requisitos de Segurança.....	12
6.4.1	Hospedagem.....	13
6.4.2	Segurança Injection e Cross-site.....	13
6.4.3	Perfis	19
7	Referências	19
8	Conclusão	20

1 Controle de Revisão

Data	Versão	Descrição	Autor	Área
03/12/2020	1.0	Elaboração do documento	Leonardo Oliveira	Fábrica de Teste

2 Identificação da Demanda

Número da OS:	020	Sistema/Módulo:	TaxiGov
Líder do Projeto:	Wellington Palmeira	Analista de Teste:	
Dono do Produto:	Luis Guilherme Izycki		

3 Finalidade

O objetivo deste é sintetizar os resultados obtidos na execução dos serviços de Teste e Qualidade de Software relativos à Prova de Conceito para contratação de transporte terrestre ou agenciamento/intermediação de transporte terrestre dos servidores, empregados e colaboradores a serviço dos órgãos e entidades da Administração Pública Federal – APF.

4 Escopo

Os serviços de teste e qualidade compreendem a execução das seguintes atividades para a solução tecnológica apresentada pelo CONTRATADA, com o objetivo de identificação de possíveis falhas e defeitos, em conformidade com o processo licitatório e os itens de avaliação elencados no Anexo E do Termo de Referência:

- Requisitos de Acessibilidade
- Requisitos de Funcionalidade
- Requisitos de Disponibilidade
- Requisitos de Segurança

Soluções apresentadas:

Soluções apresentadas:

Web: <https://portal.huby.com.br/>

Mobile

IOS

<https://apps.apple.com/br/app/99-carro-particular-e-t%C3%A1xi/id553663691>

IPA fornecido pela CONTRATADA

Android

https://play.google.com/store/apps/details?id=com.taxis99&hl=pt_BR

APK fornecido pela CONTRATADA

4.1 Não Escopo

Não se aplica.

5 Recursos Necessários

5.1 Recursos Humanos

Responsável	Papel	Responsabilidades
Leonardo Gonçalves de Oliveira	Coordenador de Operações	Responsável pela coordenação dos testes e andamento do projeto
Rodrigo Teixeira Pimentel	Especialista em Teste	Responsável pela execução dos testes funcionais previstos para o projeto
Iago Silva Alencar	Especialista em Automação	Responsável pela execução dos testes não funcionais previstos para o projeto
Luiz Henrique Cavalcante Wurli	Especialista em Segurança	Responsável pela execução dos testes de segurança do projeto

6 Resultados Obtidos

6.1 Requisitos de Acessibilidade

Esta atividade compreende na avaliação dos seguintes itens:

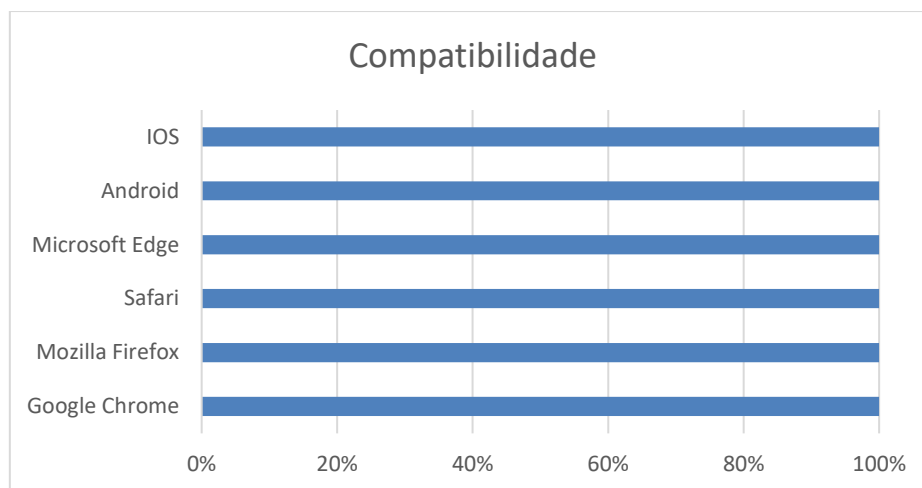
- Acesso à solução tecnológica por meio de aplicação web compatível com Google Chrome
- Acesso à solução tecnológica por meio de aplicação web compatível com Mozilla Firefox
- Acesso à solução tecnológica por meio de aplicação web compatível com Safari
- Acesso à solução tecnológica por meio de aplicação web compatível com Microsoft Edge
- Acesso à solução tecnológica por meio de aplicação web compatível com Android
- Acesso à solução tecnológica por meio de aplicação web compatível com IOS

Tipo de avaliação: Conformidade

Estratégia de teste: Verificação manual

Status: **Aprovado**

Item Avaliado	Versão	Resultado
Google Chrome	87.0.4280.66	OK
Mozilla Firefox	83.0	OK
Apple Safari	14.0.1	OK
Microsoft Edge	87.0.664.47	OK
Android	10	OK
IOS	14.2	OK



6.2 Requisitos de Funcionalidade

Esta atividade compreende na avaliação dos seguintes itens:

- Acesso à solução tecnológica por meio de login e senha pessoal
- Cadastramento de órgãos e entidades na solução tecnológica por meio da aplicação web
- Cadastramento de unidades administrativas na solução tecnológica por meio da aplicação web
- Cadastramento de gestores e usuários na solução tecnológica por meio da aplicação web
- Solicitação de serviço por meio da aplicação web e do aplicativo mobile
- Acompanhamento de solicitações de serviço e de atendimentos em andamento, por meio da aplicação web e do aplicativo mobile, incluindo imagem geoprocessada do percurso
- Cancelamento de solicitações de serviço por meio da aplicação web e do aplicativo mobile
- Consultas e relatórios com informações sobre solicitações de serviço e atendimentos

Tipo de avaliação: Conformidade

Estratégia de teste: Verificação manual

Status: **Aprovado**

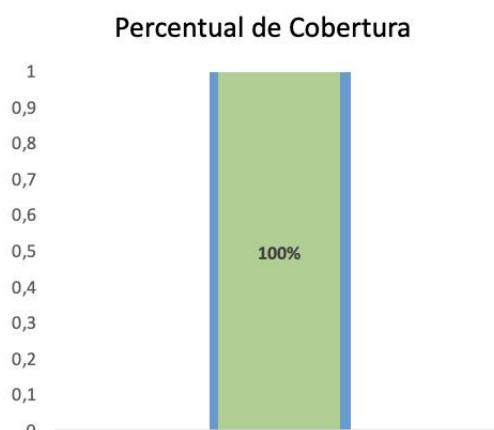
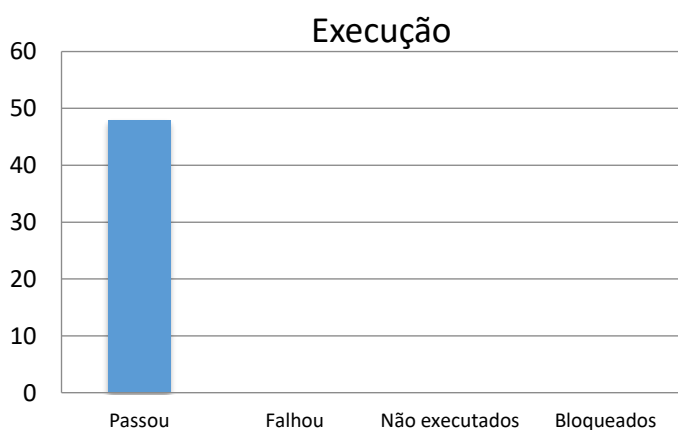
Item Avaliado	Chrome	Firefox	Edge	Safari	Android	IOS
Acesso à solução tecnológica por meio de login e senha pessoal	OK	OK	OK	OK	OK	OK
Cadastramento de órgãos e entidades na solução tecnológica por meio da aplicação web	OK	OK	OK	OK	OK	OK
Cadastramento de unidades administrativas na solução tecnológica por meio da aplicação web	OK	OK	OK	OK	OK	OK
Cadastramento de gestores e usuários na solução tecnológica por meio da aplicação web	OK	OK	OK	OK	OK	OK

Solicitação de serviço por meio da aplicação web e do aplicativo mobile	OK	OK	OK	OK	OK	OK
Acompanhamento de solicitações de serviço e de atendimentos em andamento, por meio da aplicação web e do aplicativo mobile, incluindo imagem geoprocessada do percurso	OK	OK	OK	OK	OK	OK
Cancelamento de solicitações de serviço por meio da aplicação web e do aplicativo mobile	OK	OK	OK	OK	OK	OK
Consultas e relatórios com informações sobre solicitações de serviço e atendimentos	OK Com Melhoria	OK Com Melhoria	OK Com Melhoria	OK Com Melhoria	OK	OK

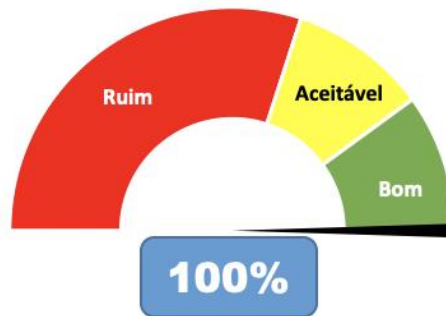
Melhoria - sugerimos revisão no relatório por Departamento, pois o mesmo não apresenta o nome do departamento e, ao filtrar por um departamento, o resultado apresenta dados de outros departamentos.

Funcionalidade	Ciclo	Cobertura	Qualidade	Resultados da Execução					Incidentes por Gravidade					
				Planejados	Com Defeito	Com Sucesso	Bloqueados	Não Executados	Crítico	Alto	Médio	Baixo	Melhoria	
Web	1	100%	100%	32	0	32	0	0	0	0	0	0	0	4
Mobile	1	100%	100%	16	0	16	0	0	0	0	0	0	0	0

Total Geral: **100%** **100%** **48** **0** **48** **0** **0** **0** **0** **0** **0** **0** **4**



Indicador de Conformidade



6.3 Requisitos de Disponibilidade

Esta atividade compreende na avaliação dos seguintes itens:

- Disponibilidade da solução tecnológica mínima de 96% (noventa e seis por cento) do período de tempo utilizado para aplicação da PoC
- Desempenho medido por tempo de resposta (RESPONSE TIME TESTING) correspondente a até 5 segundos para 25 solicitações de serviços (corridas) na aplicação web.
- Desempenho medido por tempo de resposta (RESPONSE TIME TESTING) correspondente a até 5 segundos para 25 solicitações de serviços (corridas) no aplicativo mobile

6.3.1 Disponibilidade de 96%

Web

Tipo de avaliação: Automatizada

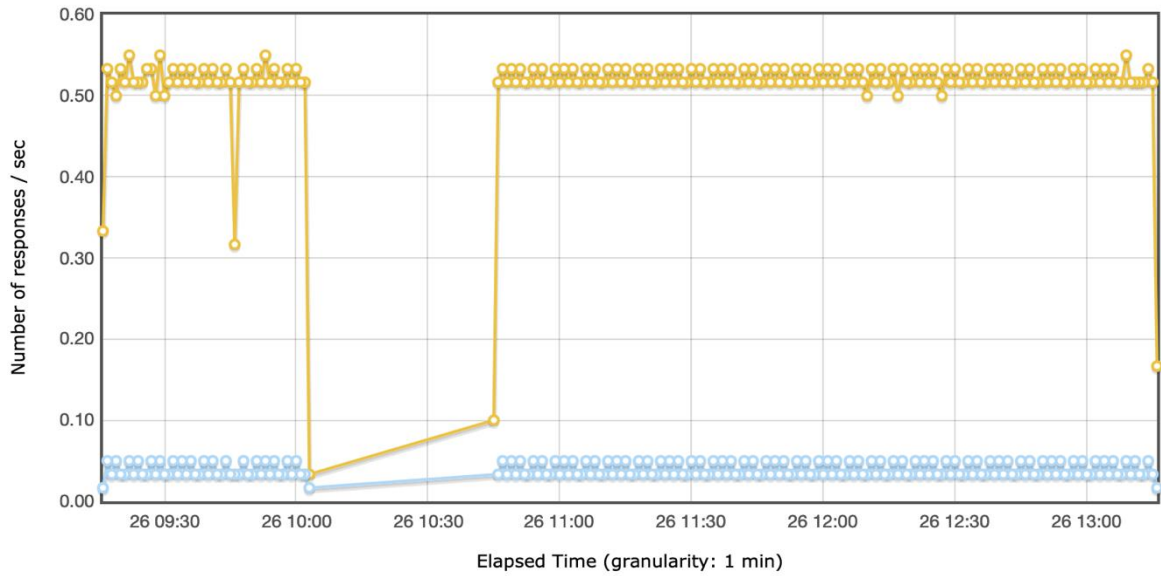
Estratégia de teste: Script de disponibilidade

Tempo de Execução: 03:30

Status: **Aprovado**

Códigos por Segundo

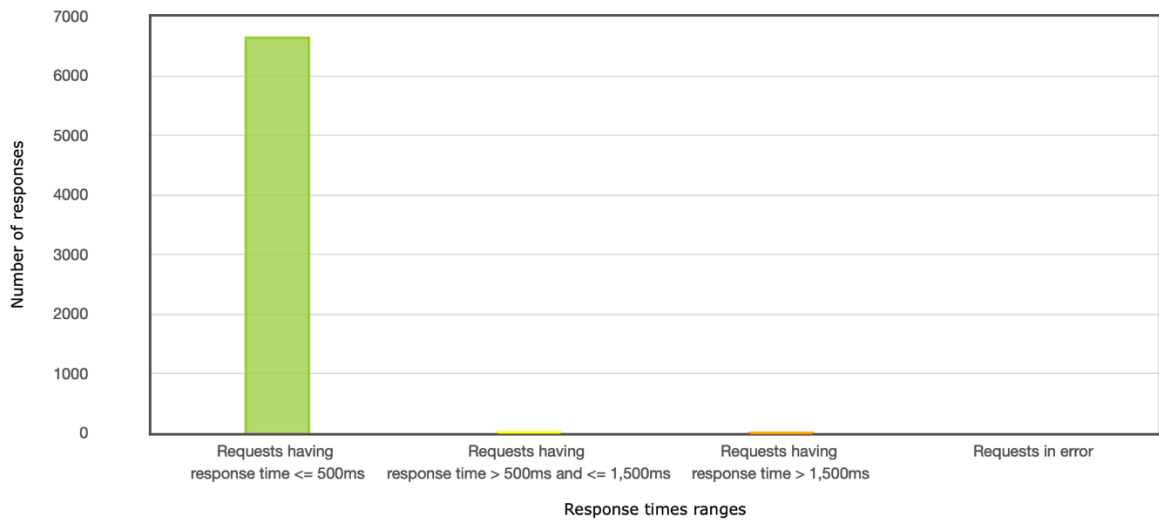
O relatório de tempo de resposta por tempo de execução exibe dados sobre o comportamento das páginas/requisições durante o tempo de execução do teste de uma forma gráfica. Apresentando de uma maneira bem simples todos os valores recuperados tanto para cima quanto para baixo:



200 302

Visão Geral do Tempo de Resposta

Este gráfico representa a distribuição das requisições nas faixas de tempo de resposta definidas:



Requests having response time <= 500ms Requests having response time > 1,500ms Requests having response time > 500ms and <= 1,500ms Requests in error

Mobile

Tipo de avaliação: Automatizada

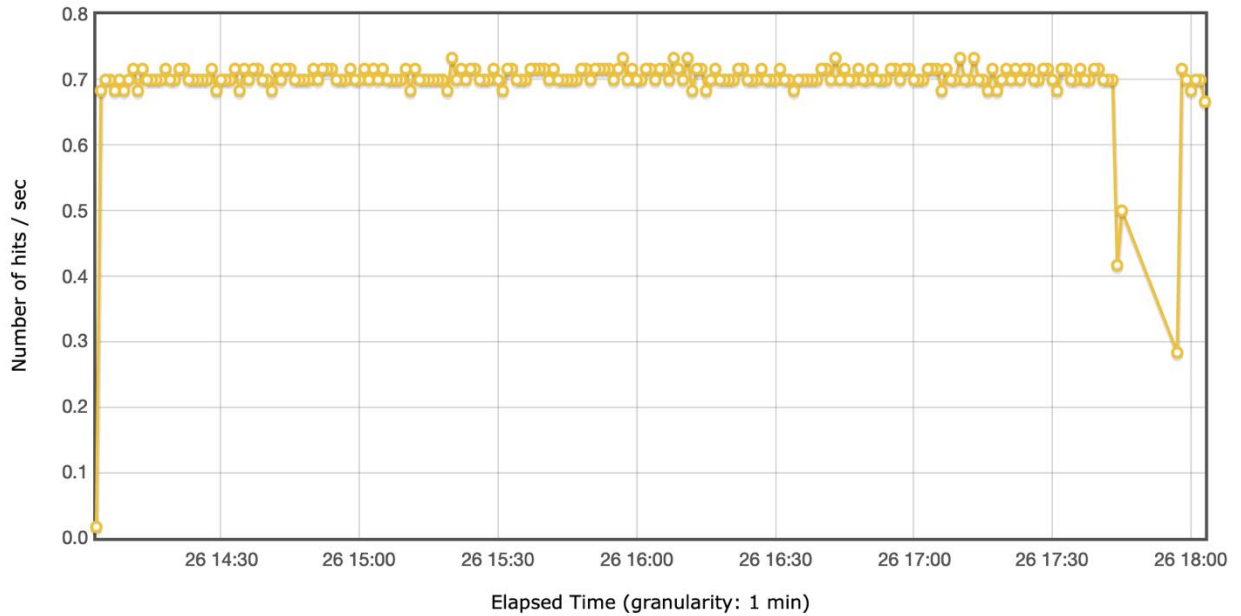
Estratégia de teste: Script de disponibilidade

Tempo de Execução: 03:30

Status: **Aprovado**

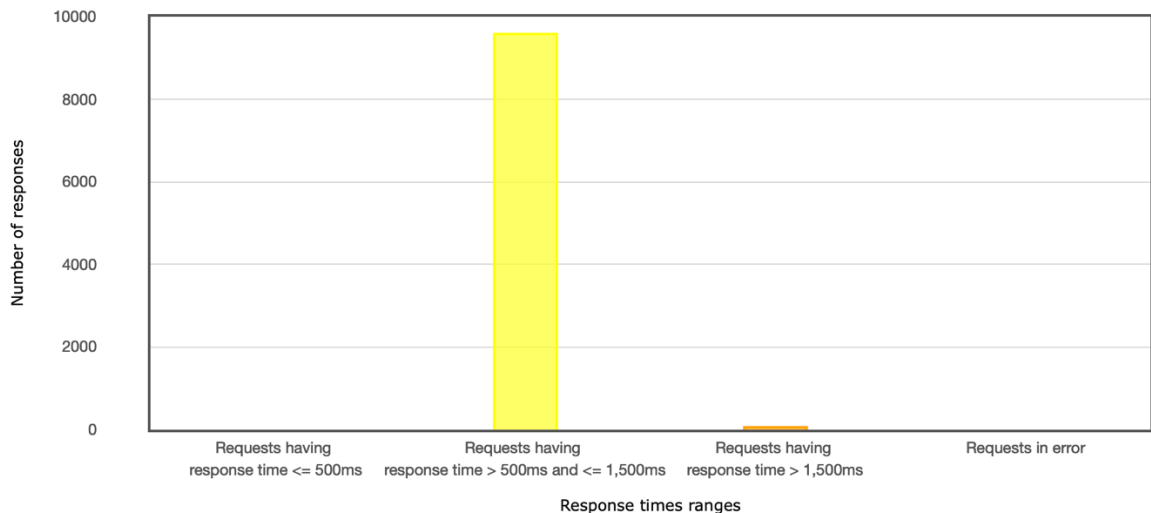
Códigos por Segundo

O relatório de tempo de resposta por tempo de execução exibe dados sobre o comportamento das páginas/requisições durante o tempo de execução do teste de uma forma gráfica. Apresentando de uma maneira bem simples todos os valores recuperados tanto para cima quanto para baixo:



Visão Geral do Tempo de Resposta

Este gráfico representa a distribuição das requisições nas faixas de tempo de resposta definidas:



■ Requests having response time <= 500ms ■ Requests having response time > 1,500ms ■ Requests having response time > 500ms and <= 1,500ms ■ Requests in error

6.3.2 Desempenho – 25 corridas

Web

Tipo de avaliação: Automatizada

Estratégia de teste: Script de desempenho

Tempo da requisição: 5,9 segundos

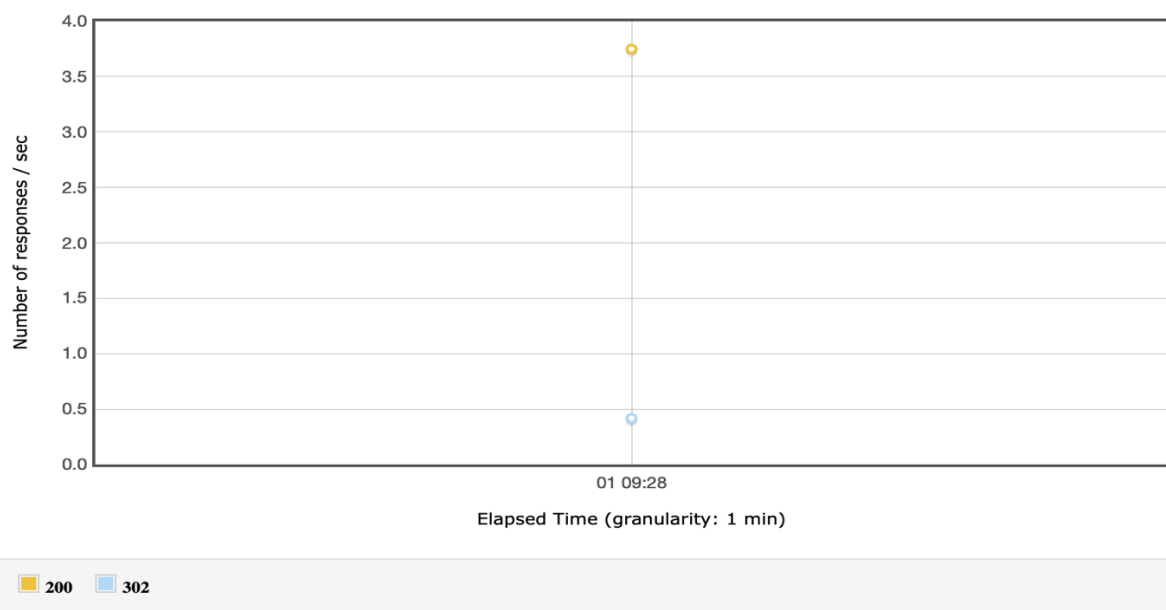
Status: **Reprovado**

Relatório Resumo

Descrição	Amostras	% de Erro	Média	Mínimo	Máximo
01 - Fluxo Login	25	0.00%	2,042	1,437	3,041
01.1 - Home	25	0.00%	1,676	1,197	2,034
01.2 - Login	25	0.00%	0,366	0,154	1,167
01.2 - Login-0	25	0.00%	0,302	0,09	1,136
01.2 - Login-1	25	0.00%	0,061	0,031	0,087
02 - Fluxo Solicitar Corrida	25	0.00%	10,106	7,898	12,206
02.1 - Default	25	0.00%	0,039	0,031	0,051
02.2 - Novo atendimento	25	0.00%	0,419	0,194	1,165
02.3 - Busca Nome	25	0.00%	0,440	0,209	0,640
02.4 - Busca cep - Origem	25	0.00%	1,362	0,245	2,298
02.5 - Busca cep - Destino	25	0.00%	1,851	1,333	2,633
02.6 - Confirmar	25	0.00%	5,995	5,297	7,003

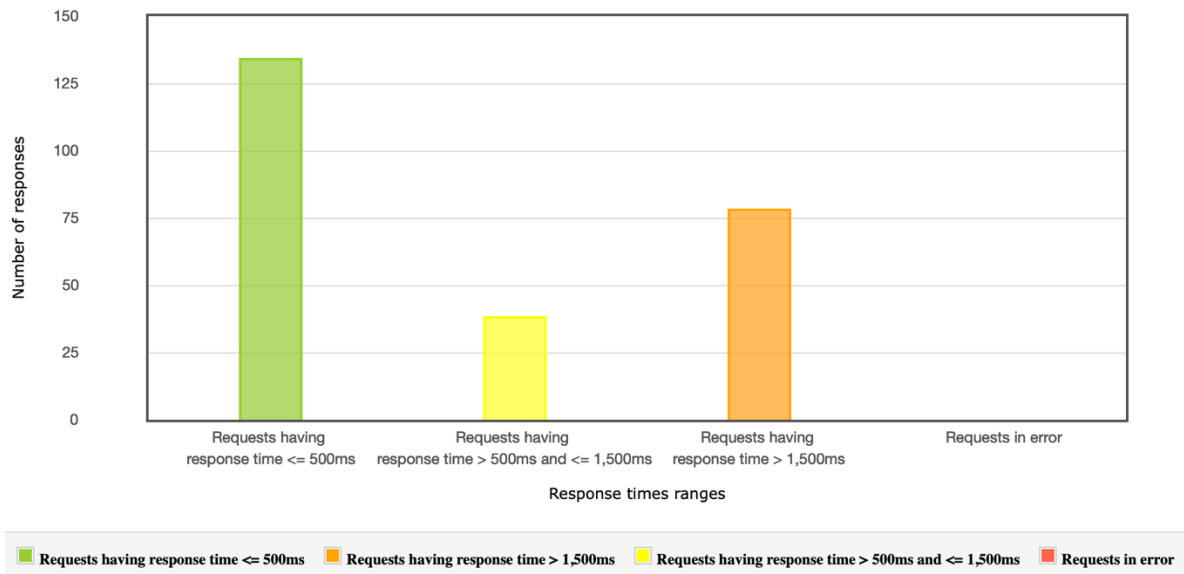
Códigos por segundo

O relatório de tempo de resposta por tempo de execução exibe dados sobre o comportamento das páginas/requisições durante o tempo de execução do teste de uma forma gráfica. Apresentando de uma maneira bem simples todos os valores recuperados tanto para cima quanto para baixo:

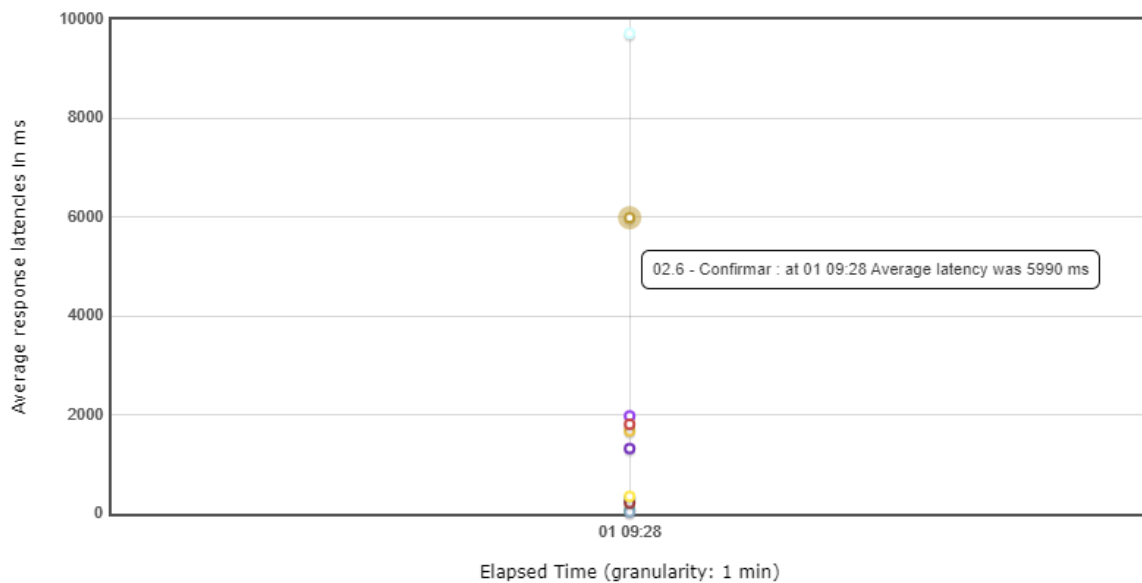


Visão Geral do Tempo de Resposta

Este gráfico representa a distribuição das requisições nas faixas de tempo de resposta definidas



Este gráfico representa o tempo de resposta médio da requisição responsável por Solicitar Corrida:



Mobile

Tipo de avaliação: Automatizada

Estratégia de teste: Script de desempenho

Tempo da requisição: 3,8 segundos

Status: **Aprovado**

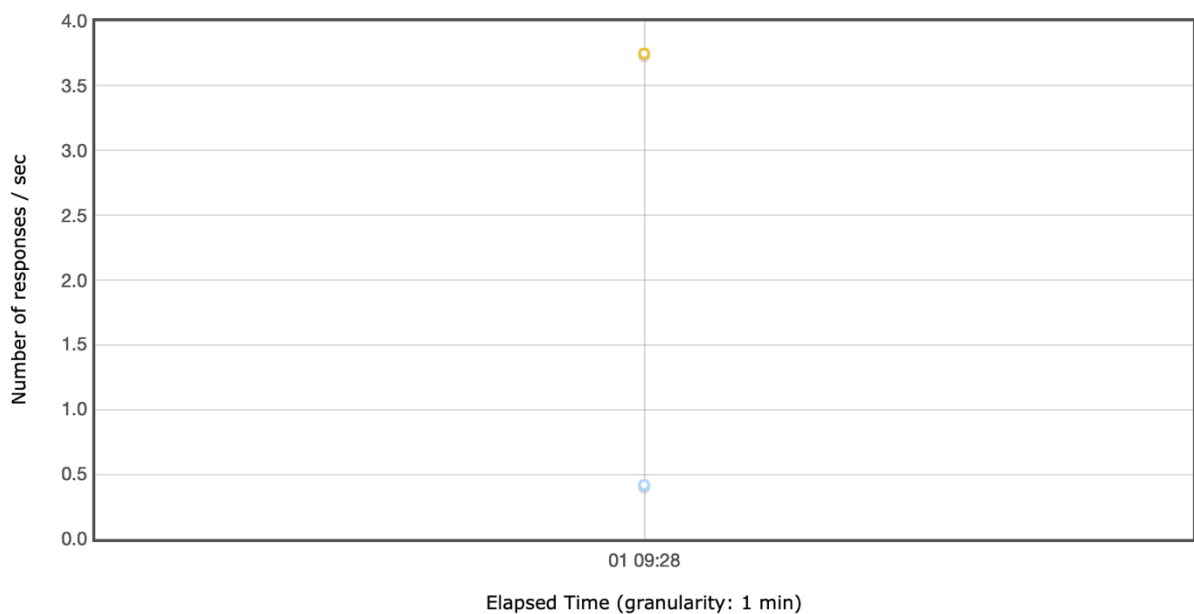
A execução foi realizada utilizando a API Corrida, onde foram coletados os resultados abaixo:

Resultado Geral

Requisições	Execução		Tempos de Resposta		
Nome	Amostras	% de Erro	Média	Min.	Max
Solicitar Corrida	25	0.00%	3,811	3,057	4,330

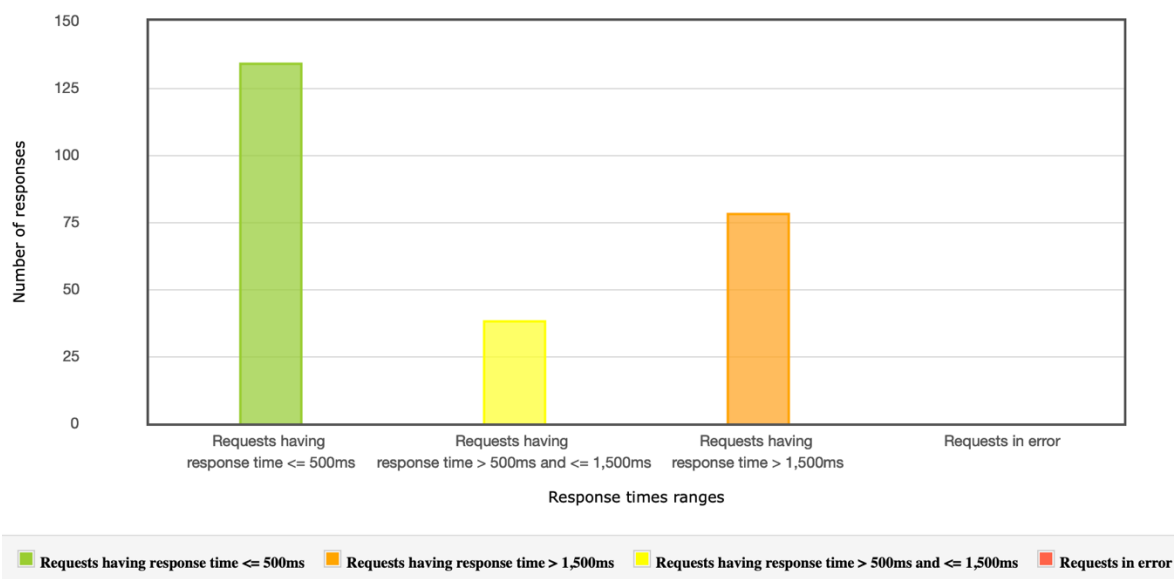
Códigos por segundo

O relatório de tempo de resposta por tempo de execução exibe dados sobre o comportamento das páginas/requisições durante o tempo de execução do teste de uma forma gráfica. Apresentando de uma maneira bem simples todos os valores recuperados tanto para cima quanto para baixo:

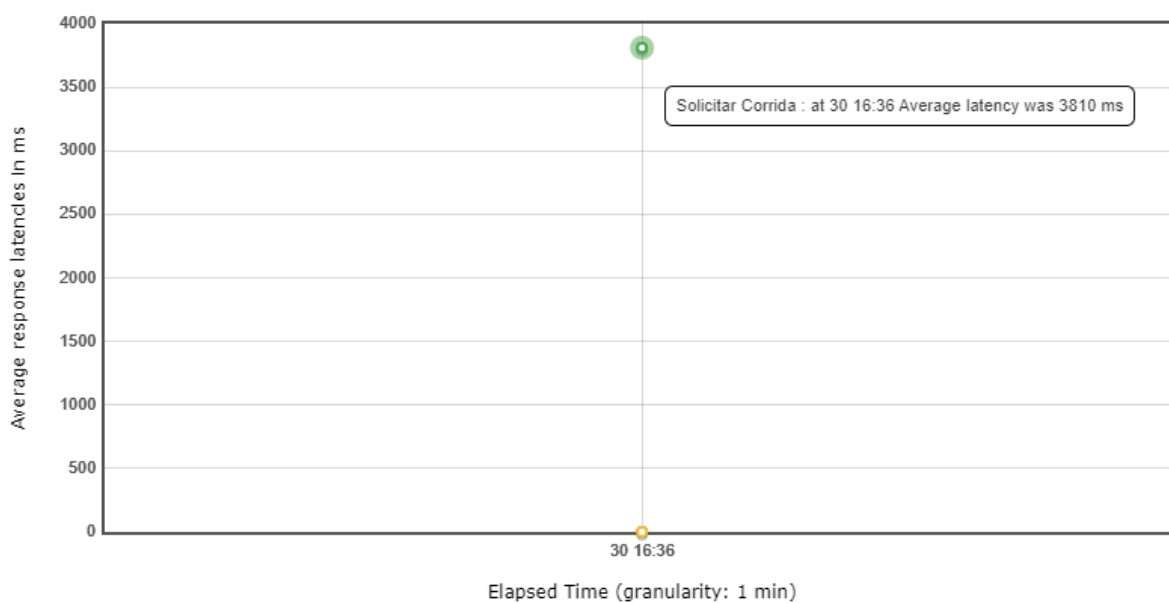


Visão Geral do Tempo de Resposta

Este gráfico representa a distribuição das requisições nas faixas de tempo de resposta definidas



Este gráfico representa o tempo de resposta médio da requisição responsável por Solicitar Corrida:



6.4 Requisitos de Segurança

Esta atividade compreende na avaliação dos seguintes itens:

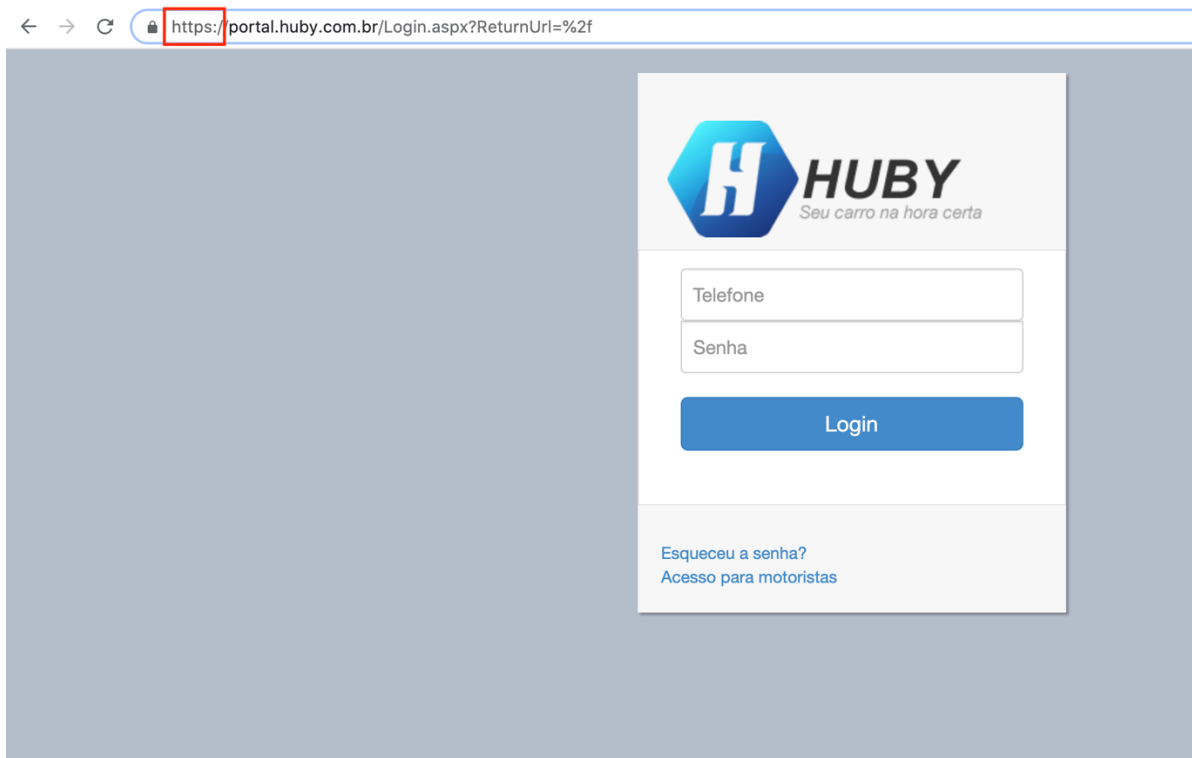
- Site de hospedagem da solução tecnológica com certificado SECURE SOCKETS LAYER
- Solução tecnológica resistente a CROSS-SITE REQUEST FORGERY
- Solução tecnológica resistente a CROSS-SITE SCRIPTING
- Solução tecnológica resistente a INJECTION
- Acesso às funcionalidades da solução tecnológica de acordo com perfis de usuários

6.4.1 Hospedagem

Tipo de avaliação: Conformidade

Estratégia de teste: Verificação manual

Status: **Aprovado**



6.4.2 Segurança Injection e Cross-site

██████████ Web

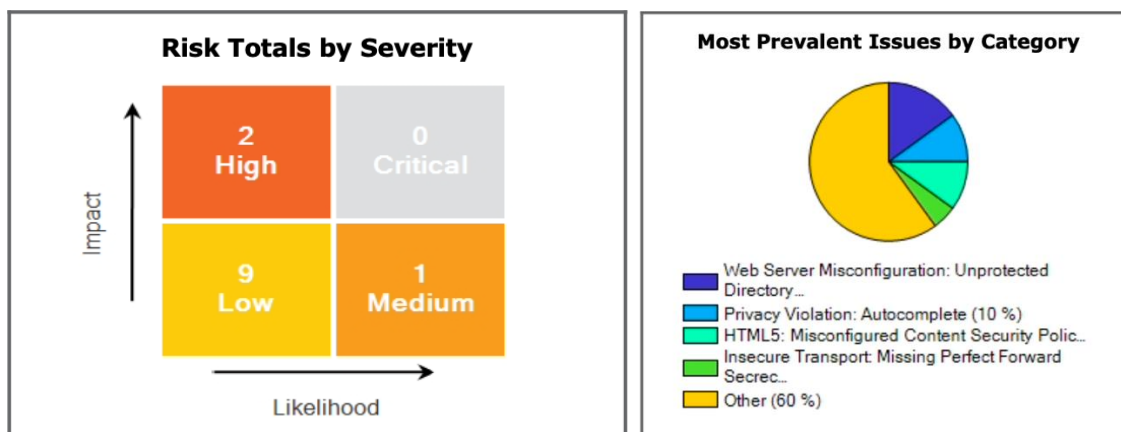
Tipo de avaliação: Automatizada

Estratégia de teste: Validação de segurança

Status: **Aprovado**

Resumo de Inconsistências identificadas na avaliação de Segurança

Tipo	Quant. de Defeitos por Gravidade						Total defeitos
	Impeditiva	Crítica	Alta	Média	Baixa	Muito Baixa	Erros
Segurança	0	0	2	1	9	8	20



Detalhamento

Rating	Category	Test Type	
High	Insecure Transport	Dynamic	1
High	Often Misused: Login	Dynamic	1
Medium	Path Manipulation: Relative Path Overwrite	Dynamic	1
Low	Cookie Security: Missing SameSite Attribute	Dynamic	1
Low	HTML5: Misconfigured Content Security Policy	Dynamic	2
Low	Insecure Transport: Channel Mixing	Dynamic	1
Low	Privacy Violation: Autocomplete	Dynamic	1
Low	Web Server Misconfiguration: Server Error Message	Dynamic	1
Low	Web Server Misconfiguration: Unprotected Directory	Dynamic	3
Best Prac...	Compliance Failure: Missing Privacy Policy	Dynamic	1
Best Prac...	Insecure Transport: Missing Perfect Forward Secrecy	Dynamic	1
Best Prac...	Privacy Violation: Autocomplete	Dynamic	1
Best Prac...	Session Management: Easy-to-Guess Session Identifier Name	Dynamic	1
Info	Hidden Field	Dynamic	1
Info	Insecure Deployment: Known Technology Fingerprint	Dynamic	1
Info	Session Management: Session Token Discovery	Dynamic	1
Info	Web Server Misconfiguration: OPTIONS HTTP Method	Dynamic	1

Avaliação de segurança do código contra técnicas de exploração de vulnerabilidades:

CROSS-SITE REQUEST FORGERY

A falsificação de solicitação entre sites (CSRF) é um tipo de ataque que ocorre quando um site, e-mail, blog, mensagem instantânea ou programa mal-intencionado faz com que o navegador da web do usuário execute uma ação indesejada em um site confiável quando o usuário é autenticado. Um ataque CSRF funciona porque as solicitações do navegador incluem automaticamente todos os cookies, incluindo os de sessão. Portanto, se o usuário estiver autenticado no site, ele não poderá distinguir entre solicitações legítimas e falsificadas.

Nenhuma vulnerabilidade encontrada

CROSS-SITE SCRIPTING

Falhas XSS ocorrem sempre que um aplicativo inclui dados não confiáveis em uma nova página da Web sem validação ou escape adequado ou atualiza uma página da Web existente com dados fornecidos pelo usuário usando uma API do navegador que pode criar HTML ou JavaScript. O XSS permite que os invasores executem scripts no navegador da vítima, o que pode sequestrar sessões do usuário, desfigurar sites, redirecionar o usuário para sites mal-intencionados, etc.

Nenhuma vulnerabilidade encontrada

INJECTION

Falhas de injeção, especialmente de injeção SQL, são comuns em aplicativos Web. A injeção ocorre quando os dados fornecidos pelo usuário são enviados para um intérprete como parte de um comando ou consulta. Os dados hostis do invasor enganam o intérprete e o forçam a executar comandos não pretendidos ou a alterar dados.

Nenhuma vulnerabilidade encontrada

Mobile

6.4.2.2.1 Android

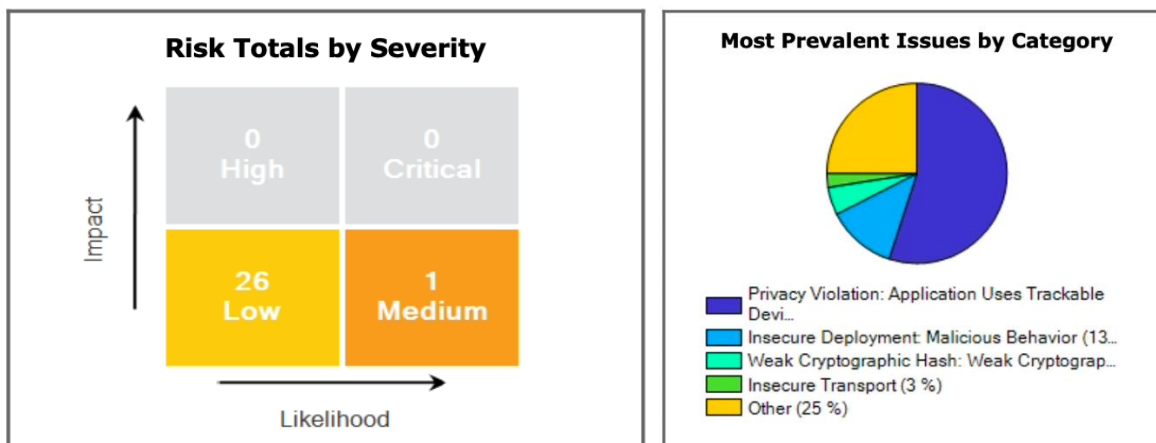
Tipo de avaliação: Automatizada

Estratégia de teste: Validação de segurança

Status: **Aprovado**

Resumo de Inconsistências identificadas na avaliação de Segurança

Tipo	Quant. de Defeitos por Gravidade						Total defeitos
	Impeditiva	Crítica	Alta	Média	Baixa	Muito Baixa	Erros
Segurança	0	0	0	1	26	13	40



Detalhamento

Rating	Category	Test Type	
Medium	Weak Encryption: Weak Code-signing Certificate	Mobile	1
Low	Android Bad Practices: Encryption Secret Held in Static Field	Mobile	1
Low	Insecure Transport	Mobile	1
Low	Privacy Violation: Application Uses Trackable Device Identifiers	Mobile	22
Low	Weak Cryptographic Hash: Weak Cryptography	Mobile	2
Info	Insecure Deployment: Malicious Behavior	Mobile	5
Info	Insecure Storage: Android Data Storage	Mobile	1
Info	Often Misused: Ad/Analytics Frameworks	Mobile	1
Info	Privacy Violation: Address Book	Mobile	1
Info	Privilege Management: Android Camera	Mobile	1
Info	Privilege Management: Android Record Audio	Mobile	1
Info	Privilege Management: Bluetooth	Mobile	1
Info	Privilege Management: Geolocation	Mobile	1
Info	System Information Leak: Internal	Mobile	1

Avaliação de segurança do código contra técnicas de exploração de vulnerabilidades:

CROSS-SITE REQUEST FORGERY

A falsificação de solicitação entre sites (CSRF) é um tipo de ataque que ocorre quando um site, e-mail, blog, mensagem instantânea ou programa mal-intencionado faz com que o navegador da web do usuário execute uma ação indesejada em um site confiável quando o usuário é autenticado. Um ataque CSRF funciona porque as solicitações do navegador incluem automaticamente todos os cookies, incluindo os de sessão. Portanto, se o usuário estiver autenticado no site, ele não poderá distinguir entre solicitações legítimas e falsificadas.

Nenhuma vulnerabilidade encontrada

CROSS-SITE SCRIPTING

Falhas XSS ocorrem sempre que um aplicativo inclui dados não confiáveis em uma nova página da Web sem validação ou escape adequado ou atualiza uma página da Web existente com dados fornecidos pelo usuário usando uma API do navegador que pode criar HTML ou JavaScript. O XSS permite que os invasores executem scripts no navegador da vítima, o que pode sequestrar sessões do usuário, desfigurar sites, redirecionar o usuário para sites mal-intencionados, etc.

Nenhuma vulnerabilidade encontrada

INJECTION

Falhas de injeção, especialmente de injeção SQL, são comuns em aplicativos Web. A injeção ocorre quando os dados fornecidos pelo usuário são enviados para um intérprete como parte de um comando ou consulta. Os dados hostis do invasor enganam o intérprete e o forçam a executar comandos não pretendidos ou a alterar dados.

Nenhuma vulnerabilidade encontrada

6.4.2.2.2 IOS

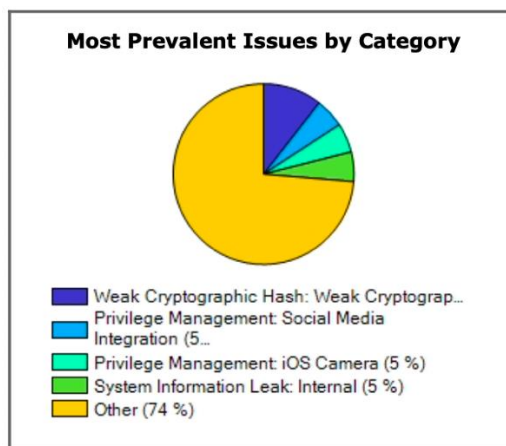
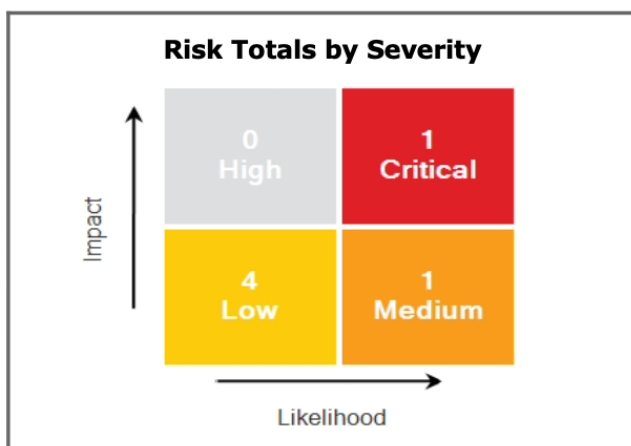
Tipo de avaliação: Automatizada

Estratégia de teste: Validação de segurança

Status: **Aprovado**

Resumo de Inconsistências identificadas na avaliação de Segurança

Tipo	Quant. de Defeitos por Gravidade						Total defeitos
	Impeditiva	Crítica	Alta	Média	Baixa	Muito Baixa	Erros
Segurança	0	1	0	1	4	13	19



Detalhamento

Rating	Category	Test Type	
Critical	Insecure Transport: Disabled App Transport Security	Mobile	1
Medium	Often Misused: Weak SSL Certificate	Mobile	1
Low	Insecure IPC: Cross Application Communication (URL Scheme)	Mobile	1
Low	Insecure Storage: Shared Keychain	Mobile	1
Low	Weak Cryptographic Hash: Weak Cryptography	Mobile	2
Info	External Content: Frameworks In Use	Mobile	1
Info	Insecure Deployment: Malicious Behavior	Mobile	1
Info	Insecure Storage: Missing Encryption on Stored Private Media	Mobile	1
Info	Insecure Transport	Mobile	1
Info	Often Misused: Push Notifications	Mobile	1
Info	Privacy Violation: Address Book	Mobile	1
Info	Privilege Management: Bluetooth	Mobile	1
Info	Privilege Management: Geolocation	Mobile	1
Info	Privilege Management: In-App Purchasing	Mobile	1
Info	Privilege Management: iOS Camera	Mobile	1
Info	Privilege Management: Microphone Usage	Mobile	1
Info	Privilege Management: Social Media Integration	Mobile	1
Info	System Information Leak: Internal	Mobile	1

Avaliação de segurança do código contra técnicas de exploração de vulnerabilidades:

CROSS-SITE REQUEST FORGERY

A falsificação de solicitação entre sites (CSRF) é um tipo de ataque que ocorre quando um site, e-mail, blog, mensagem instantânea ou programa mal-intencionado faz com que o navegador da web do usuário execute uma ação indesejada em um site confiável quando o usuário é autenticado. Um ataque CSRF funciona porque as solicitações do navegador incluem automaticamente todos os cookies, incluindo os de sessão. Portanto, se o usuário estiver autenticado no site, ele não poderá distinguir entre solicitações legítimas e falsificadas.

Nenhuma vulnerabilidade encontrada

CROSS-SITE SCRIPTING

Falhas XSS ocorrem sempre que um aplicativo inclui dados não confiáveis em uma nova página da Web sem validação ou escape adequado ou atualiza uma página da Web existente com dados fornecidos pelo usuário usando uma API do navegador que pode criar HTML ou JavaScript. O XSS permite que os invasores executem scripts no navegador da vítima, o que pode sequestrar sessões do usuário, desfigurar sites, redirecionar o usuário para sites mal-intencionados, etc.

Nenhuma vulnerabilidade encontrada

INJECTION

Falhas de injeção, especialmente de injeção SQL, são comuns em aplicativos Web. A injeção ocorre quando os dados fornecidos pelo usuário são enviados para um intérprete como parte de um comando ou consulta. Os dados hostis do invasor enganam o intérprete e o forçam a executar comandos não pretendidos ou a alterar dados.

Nenhuma vulnerabilidade encontrada

6.4.3 Perfis

Tipo de avaliação: Conformidade

Estratégia de teste: Verificação manual

Status: **Aprovado**

Item Avaliado	Versão	Resultado
Perfil Gestor Master	Visualiza todas as funcionalidades do sistema. Visualiza as corridas, reclamações do centro de custo e de todos os usuários e departamentos.	OK
Perfil Gestor Secundário	Visualiza todas as funcionalidades do sistema, exceto o relatório de auditoria. Visualiza somente as corridas, reclamações, usuários do seu departamento.	OK
Perfil Colaborador	Visualiza somente as funcionalidades de corrida, reclamações, rede credenciada e relatório de corridas finalizados somente de seu usuário.	OK

7 Referências

Evidências e Relatórios completos encontram-se disponíveis no repositório GIT do Ministério da Economia.

Link: <https://git.economia.gov.br/rsi/rsi/-/tree/master/TAXIGOV>

Para acessar ao repositório, clique na aba "Standard" e insira login e senha.

Login: consultataxigov

Senha: W9rhv67S3KKxrvmd

8 Conclusão

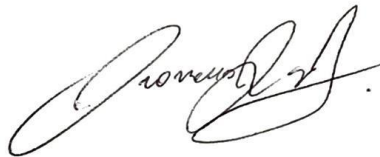
Após análise de qualidade da solução tecnológica apresentada pela CONTRATADA referente a Prova de Conceito do processo licitatório para contratação de transporte terrestre - TaxiGov, percebe-se que a solução apresentada **não** está de acordo com critérios definidos no Item “4 Escopo” deste documento e Anexo E do Termo de Referência.

Performance

Web

Fica evidente que a solução tecnológica apresentou tempos de resposta mais elevados na requisição referente à Solicitar Corrida, onde consta média de 5,9 segundos. Logo em desconformidade com os requisitos da prova de conceito que sugere o tempo médio de 5 segundos.

Diante do exposto, sugere-se que a solução seja devolvida para correção das desconformidades e ajustes apontados nos testes realizados.



Leonardo Gonçalves de Oliveira
Coordenador de Projetos
RSI - Informática