Teste de Segurança Web

no sistema de alistamento do Exército Brasileiro.

Pentester: João Vítor Dos Santos Fontoura.

Período: 12/03/2019.

Ambiente: Web.

João Vítor S. Fontoura, Desenvolvedor Web e Analista de Segurança Ofensiva.
https://joao-b4.github.io
Contato: joaosfontoura555@gmail.com

Resumo

No presente momento do dia 12/03/2019, foi feito algumas observações e testes não ‘letais’ no sistema de domínio “https://alistamento.eb.mil.br”, gostaria de fazer algumas observações, as vulnerabilidades encontradas podem não só afetar o domínio testado, mas também afetar outros sistemas usando o próprio como vetor de ataque (usando o formulario do “https://brasilcidadao.gov.br” por exemplo).

Abaixo deixarei as URL’s testadas e as vulnerabilidades encontradas.

João Vítor S. Fontoura, Desenvolvedor Web e Analista de Segurança Ofensiva.
https://joao-b4.github.io
Contato: joaosfontoura555@gmail.com

Vulnerabilidades

As vulnerabilidades abaixo foram caracterizadas com o padrão OWASP.

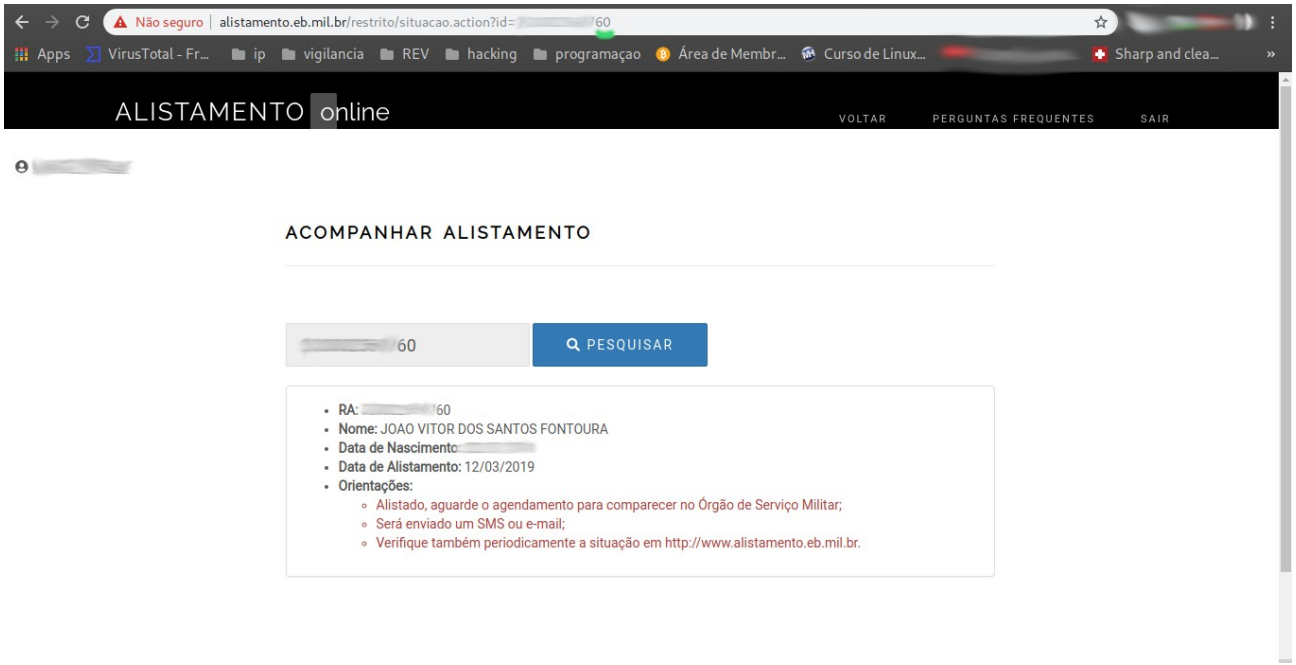
Código	Vulnerabilidade	Host	Impacto	Referência
001	A4 - Insecure Direct Object References (**idor**)	https://www.alistamento.eb.mil.br/restrito/situacao.action?id=	Moderado	https://www.owasp.org/index.php/Top_10_2013-A4-Insecure_Direct_Object_References
002	A4 - Insecure Direct Object References (**idor**)	https://www.alistamento.eb.mil.br/restrito/certificado.action?campo=	Moderado	https://www.owasp.org/index.php/Top_10_2013-A4-Insecure_Direct_Object_References
003	A7-Cross-Site Scripting (**XSS**)	https://www.alistamento.eb.mil.br/restrito/agendamento!input.action?cpf=	Alto	https://www.owasp.org/index.php/Top_10-2017_A7-Cross-Site_Scripting_(XSS)
004	A7-Cross-Site Scripting (**XSS**)	https://www.alistamento.eb.mil.br/restrito/situacao.action?id=	Alto	https://www.owasp.org/index.php/Top_10-2017_A7-Cross-Site_Scripting_(XSS)
005	A7-Cross-Site Scripting (**XSS**)	https://www.alistamento.eb.mil.br/services/jsm.action?descricao=	Alto	https://www.owasp.org/index.php/Top_10-2017_A7-Cross-Site_Scripting_(X

João Vítor S. Fontoura, Desenvolvedor Web e Analista de Segurança Ofensiva.
https://joao-b4.github.io
Contato: joaosfontoura555@gmail.com

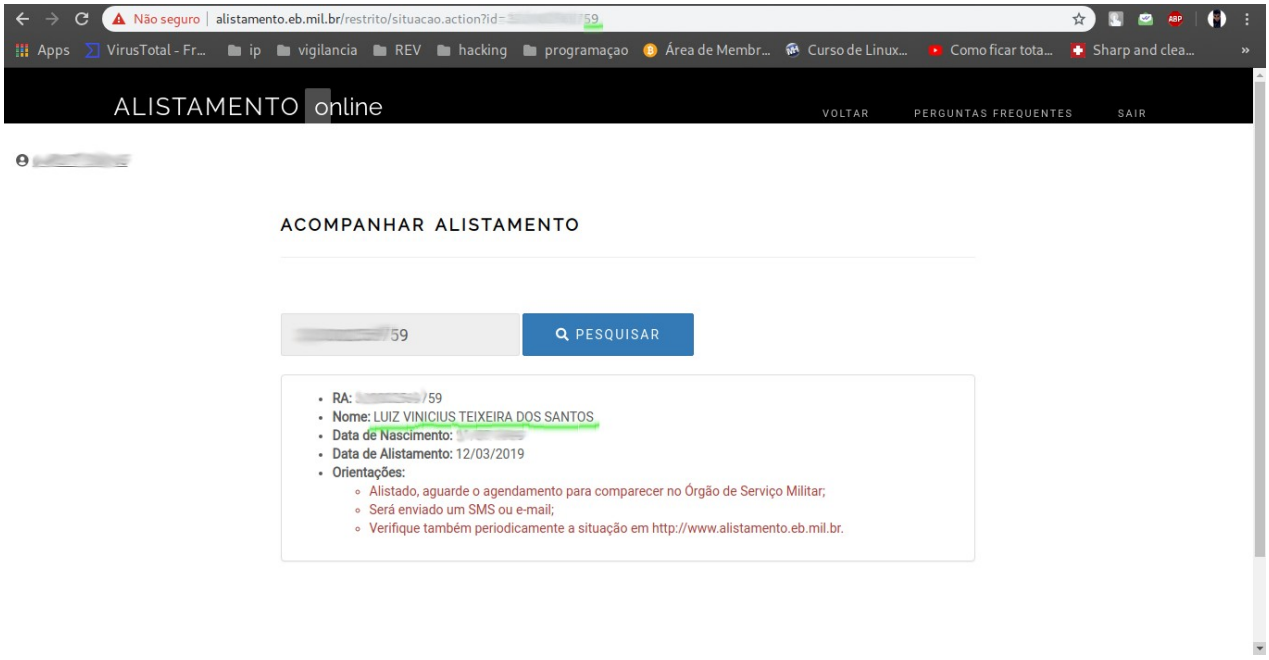
				SS)

Vulnerabilidade ‘001’:

Permite a obtenção de dados do alistamento de outras pessoas, simplesmente alterando o parametro passado por ID na URL.



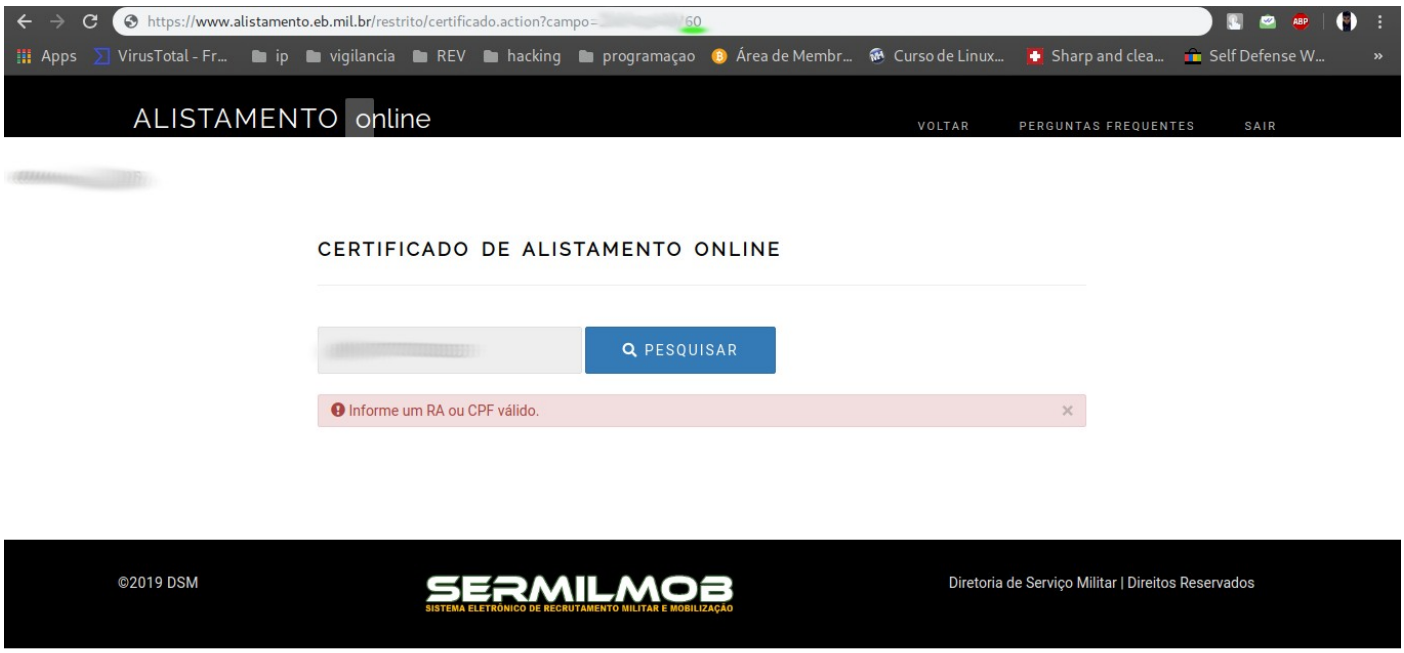
Após trocar o final do RA de 60 para 59, recebmos os dados de outro usuario.



Vulnerabilidade ‘002’:

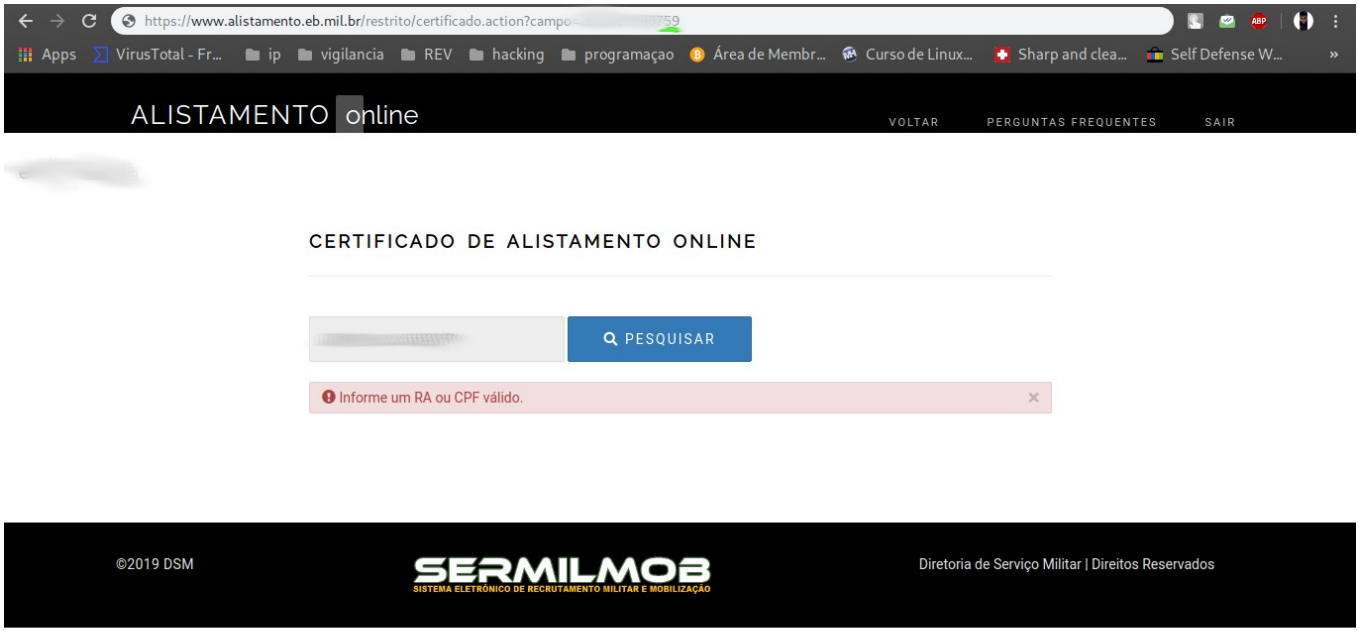
Neste caso, a vulnerabilidade é a mesma, porém exibe mais detalhes, baixando o certificado de alistamento online.

João Vítor S. Fontoura, Desenvolvedor Web e Analista de Segurança Ofensiva.
https://joao-b4.github.io
Contato: joaosfontoura555@gmail.com



João Vítor S. Fontoura, Desenvolvedor Web e Analista de Segurança Ofensiva.
https://joao-b4.github.io
Contato: joaosfontoura555@gmail.com

Agora, se alterarmos o paramêtro ‘campo’, presente na primeira imagem, receberemos os dados de outro usuario:

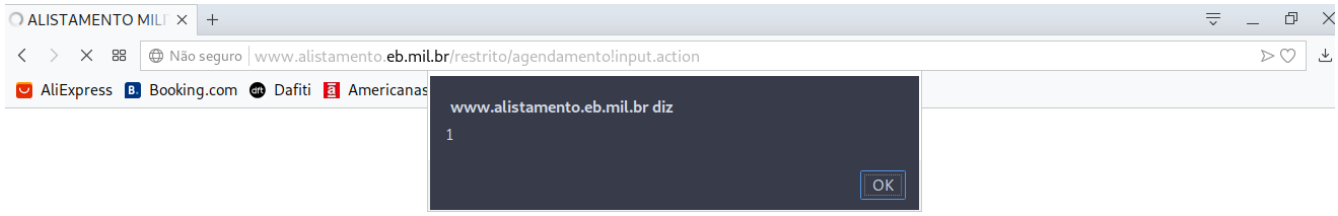


João Vítor S. Fontoura, Desenvolvedor Web e Analista de Segurança Ofensiva.
https://joao-b4.github.io
Contato: joaosfontoura555@gmail.com

Vulnerabilidade ‘003’:

Vulnerabilidade ‘XSS’, permite desde roubar cookies de sessões do navegador, até controle total do browser. Nesse teste foi utilizado o navegador “Opera” com a proteção “XSS Auditor” desligada, para facilitar os teste, porém essa proteção pode ser burlada sem muitas dificuldades e em alguns navegadores é inexistente.

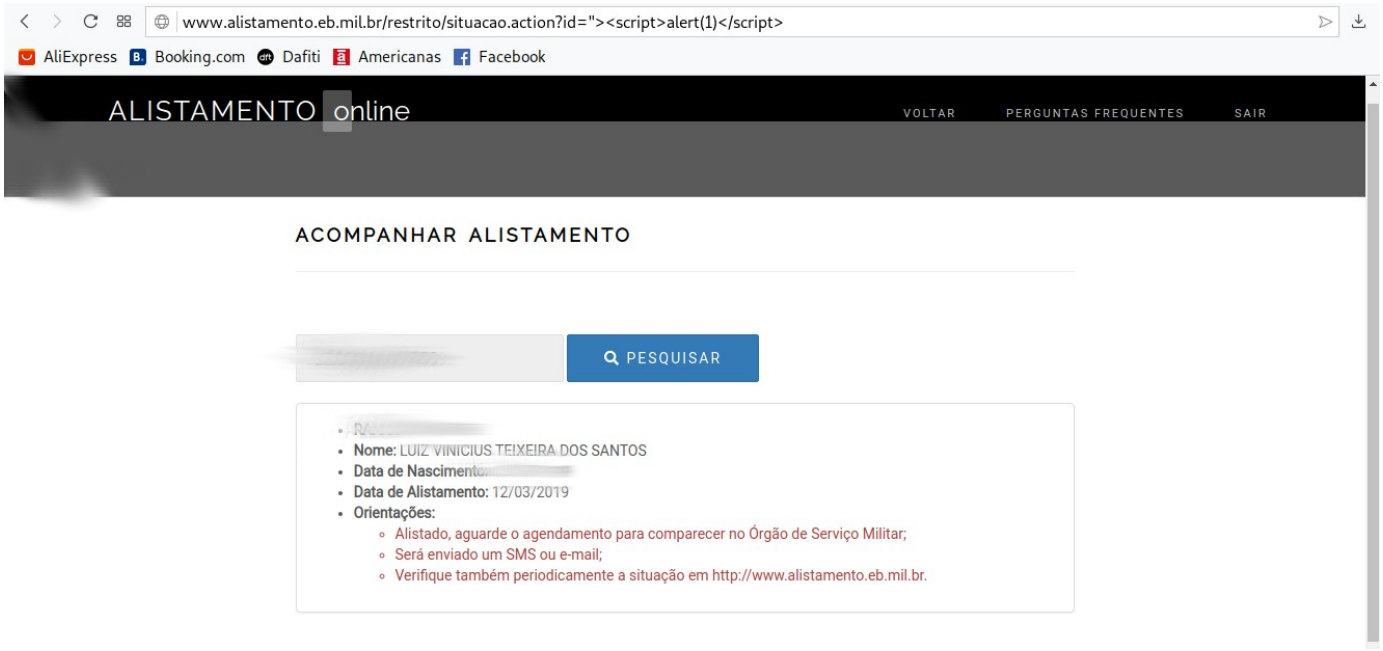
Após inserir o codigo JavaScript, o navegador interpretou na própria página, permitindo o controle do navegador.



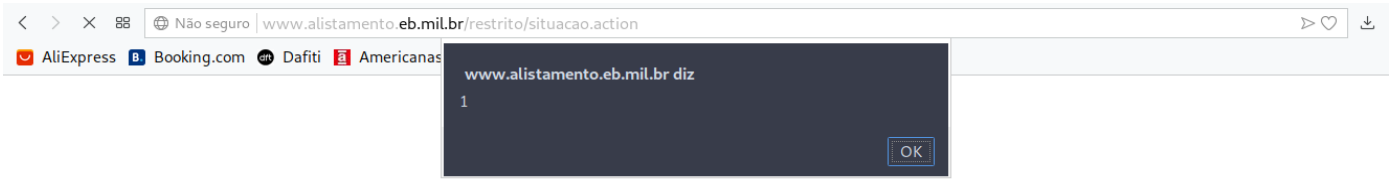
João Vítor S. Fontoura, Desenvolvedor Web e Analista de Segurança Ofensiva.
https://joao-b4.github.io
Contato: joaosfontoura555@gmail.com

Vulnerabilidade ‘004’:

Vulnerabilidade ‘XSS’ que atige a mesma página da Vulnerabilidade ‘001’:



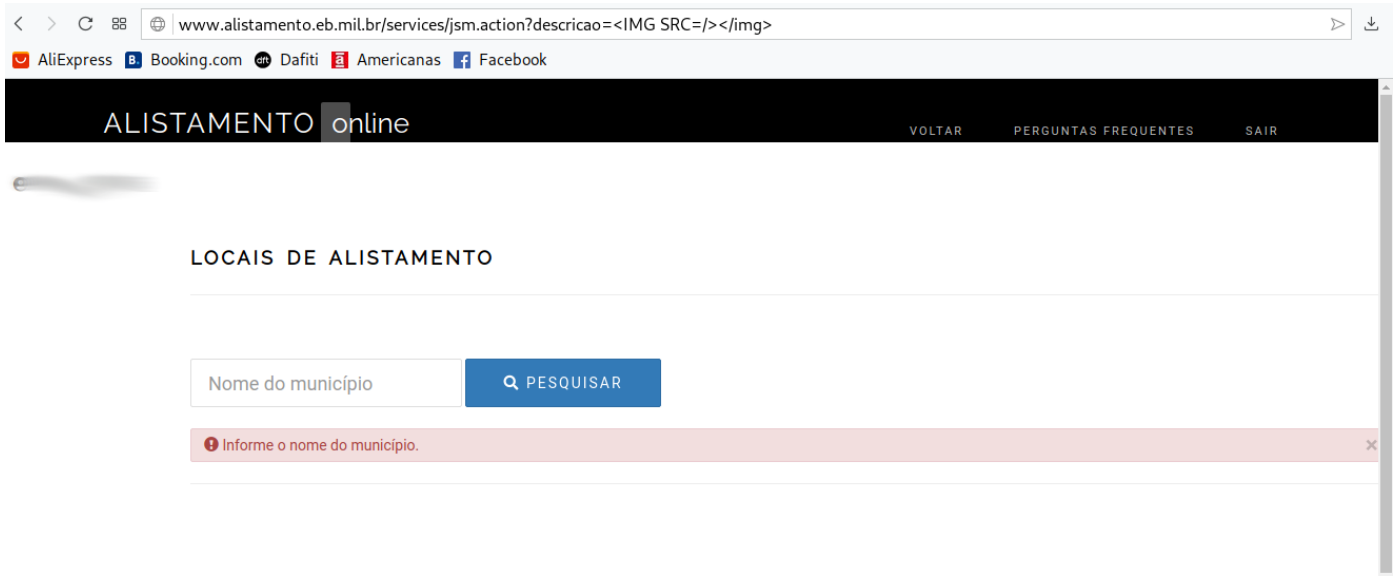
E novamente, o código é interpretado pelo navegador.



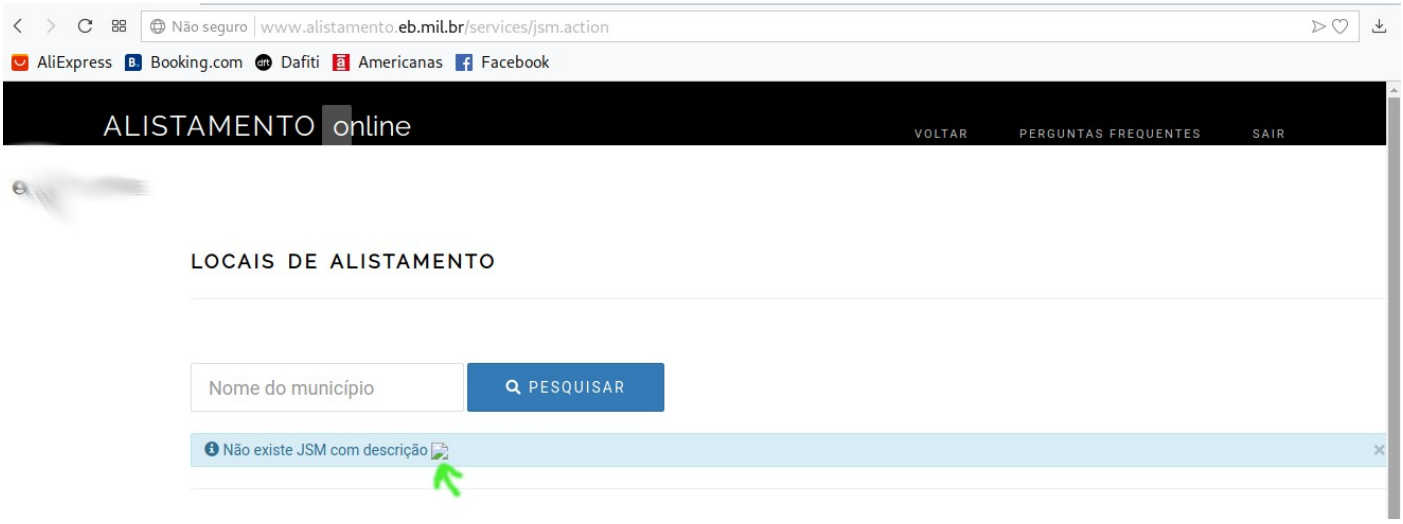
João Vítor S. Fontoura, Desenvolvedor Web e Analista de Segurança Ofensiva.
https://joao-b4.github.io
Contato: joaosfontoura555@gmail.com

Vulnerabilidade ‘005’:

Desta vez variei o código, inseri um HTML, mas a vulnerabilidade também permite JavaScript.



Como pode se ver, a imagem foi inserida no corpo da página.



João Vítor S. Fontoura, Desenvolvedor Web e Analista de Segurança Ofensiva.
https://joao-b4.github.io
Contato: joaosfontoura555@gmail.com

Conclusão

Como pode se observar, são vulnerabilidades criteriosas, podem permitir o roubo de contas de usuarios administradores, tomar o controle do navegador do usuario, roubar cookies de sessões, a extração de dados sensíveis, etc. Estes teste foram feitos sem se aprofundar no sistema, e encontrados ‘sem querer’, já que as falhas ocorrem em diversas páginas, creio que possa haver mais pontos de ataque que devem ser investigados.

João Vítor S. Fontoura, Desenvolvedor Web e Analista de Segurança Ofensiva.
https://joao-b4.github.io
Contato: joaosfontoura555@gmail.com