

# **Teste de Segurança Web**

## **no sistema de alistamento do Exército Brasileiro.**

**Pentester:** João Vítor Dos Santos Fontoura.

**Período:** 12/03/2019.

**Ambiente:** Web.

## 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://brasilcidadeao.gov.br>" por exemplo).

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

## Vulnerabilidades

As vulnerabilidades abaixo foram caracterizadas com o padrão [OWASP](#).

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

João Vítor S. Fontoura, Desenvolvedor Web e Analista de Segurança Ofensiva.

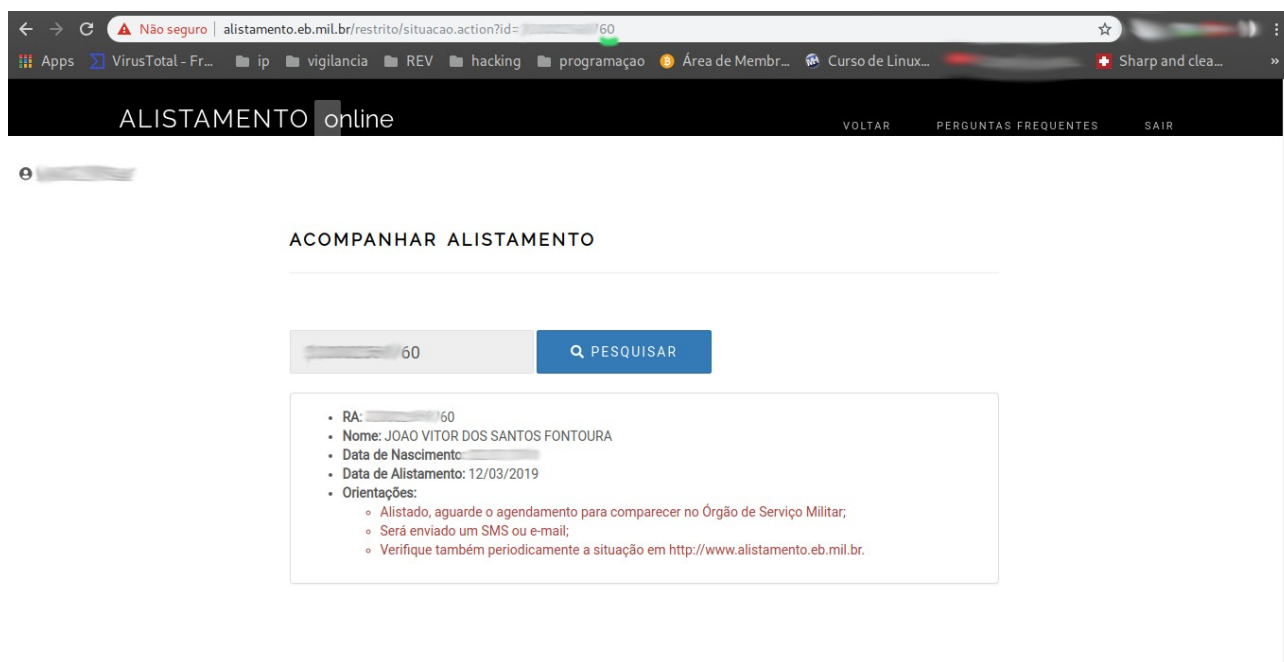
<https://joao-b4.github.io>

Contato: joaosfontoura555@gmail.com

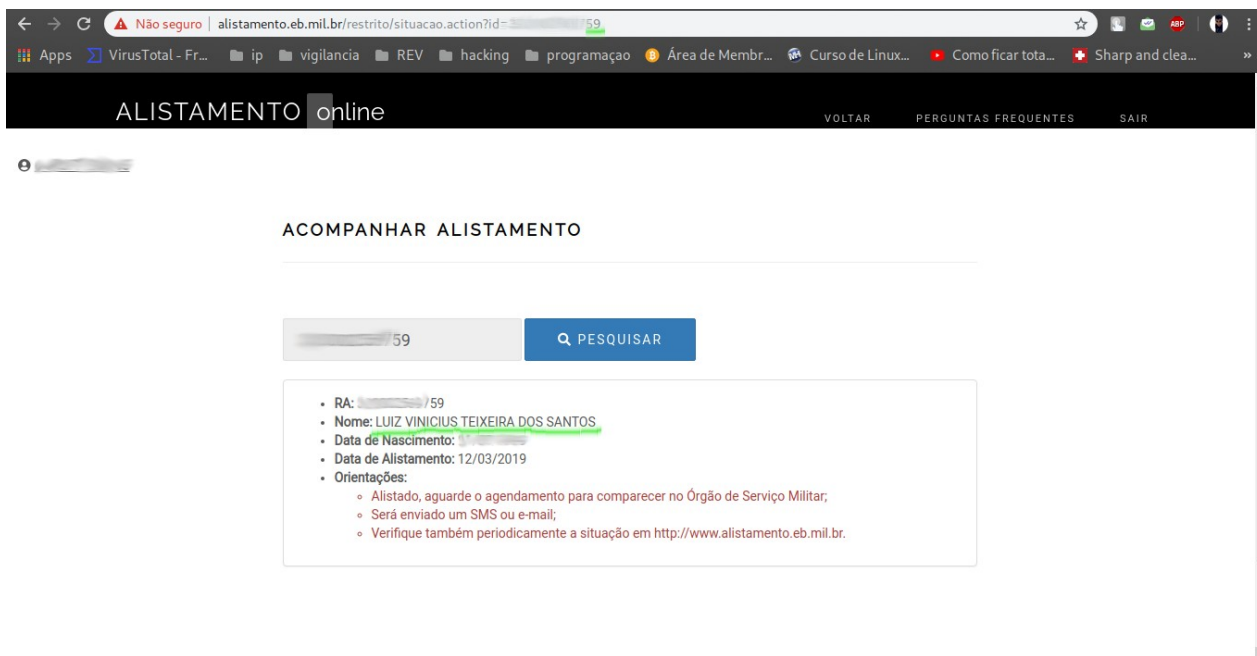
				<a href="#">SS)</a>

## 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.

### CERTIFICADO DE ALISTAMENTO ONLINE

Informe um RA ou CPF válido. X

	<b>Válido até</b> 31/12/2019
<b>MINISTÉRIO DA DEFESA</b>	
<b>Tipo de Documento</b> Certificado de Alistamento Militar	
<b>RA</b> [REDACTED]	<b>CPF</b> [REDACTED]
<b>Nome</b> JOAO VITOR DOS SANTOS FONTOURA	
<b>Filiação</b> [REDACTED]	
<b>Local e Data de Nascimento</b> RS	
<b>Situação</b> Consulte sua situação no sítio: <a href="http://www.alistamento.eb.mil.br">http://www.alistamento.eb.mil.br</a>	
<b>Informações</b> Válido com a apresentação do documento de identidade.	

Agora, se alterarmos o parâmetro 'campo', presente na primeira imagem, receberemos os dados de outro usuário:

The screenshot shows a web browser window with the URL <https://www.alistamento.eb.mil.br/restrito/certificado.action?campo=>. The page header includes the text "ALISTAMENTO online" and navigation links: "VOLTAR", "PERGUNTAS FREQUENTES", and "SAIR". The main content area is titled "CERTIFICADO DE ALISTAMENTO ONLINE" and features a search form with a "PESQUISAR" button. A red error message below the form reads: "Informe um RA ou CPF válido." The footer contains the copyright notice "©2019 DSM", the logo for "SERMILMOB SISTEMA ELETRÔNICO DE RECRUTAMENTO MILITAR E MOBILIZAÇÃO", and the text "Diretoria de Serviço Militar | Direitos Reservados".

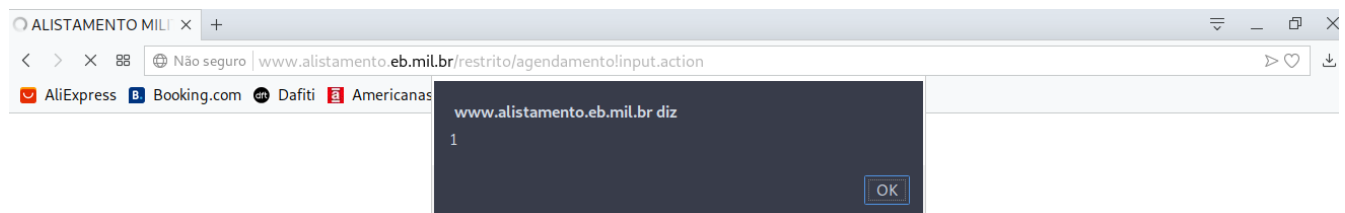
The screenshot displays a military enlistment certificate from the "MINISTÉRIO DA DEFESA". The certificate is valid until "31/12/2019". The holder's name is "LUIZ VINICIUS TEIXEIRA DOS SANTOS". The document type is "Certificado de Alistamento Militar". The RA and CPF fields are redacted. The birth location is listed as "BA". The situation is "Consulte sua situação no sítio: <http://www.alistamento.eb.mil.br>". The certificate is valid with the presentation of an identity document. The background features the coat of arms of the Brazilian Republic, with the text "REPÚBLICA FEDERATIVA DO BRASIL" and "15 de Novembro de 1889".

## 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.



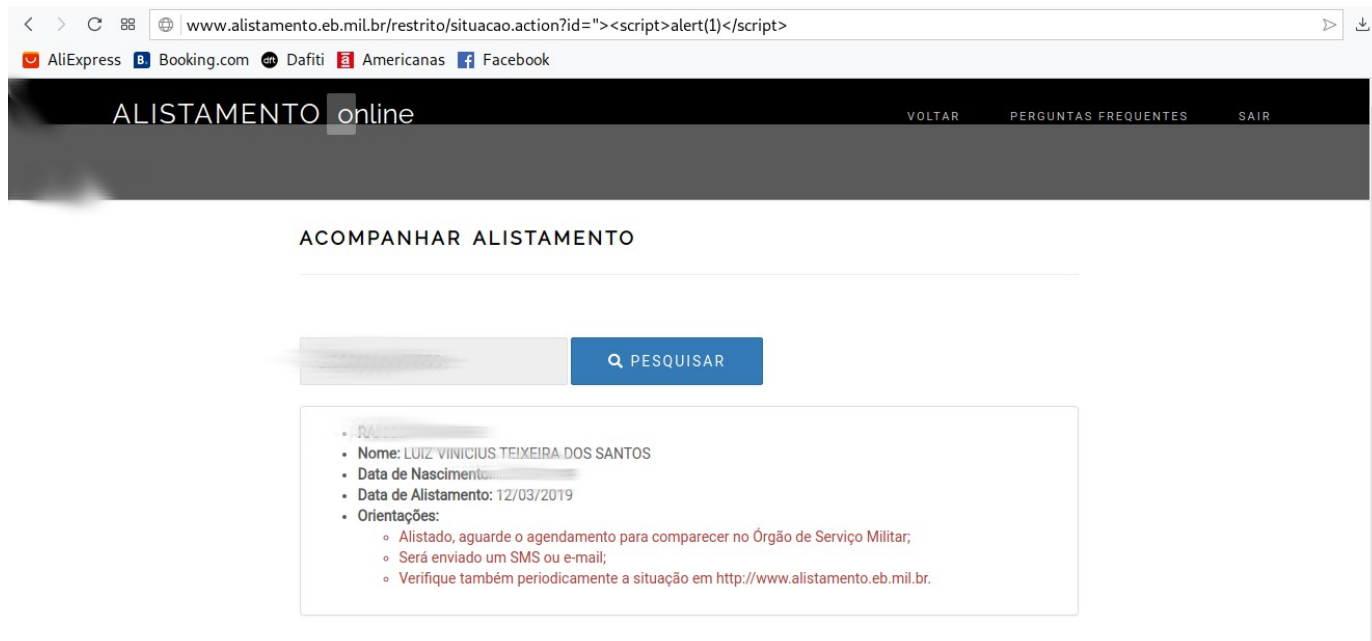
Após inserir o código JavaScript, o navegador interpretou na própria página, permitindo o controle do navegador.



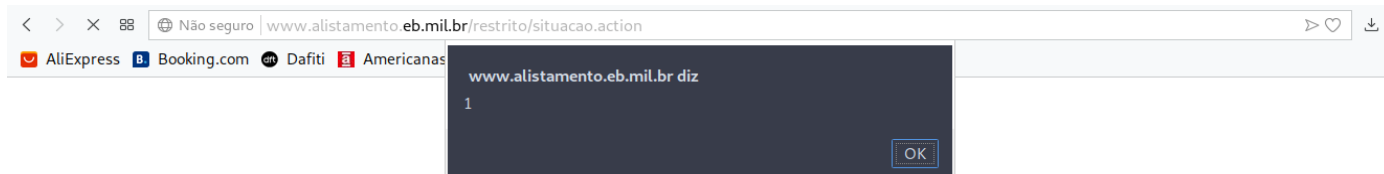


## Vulnerabilidade '004':

Vulnerabilidade 'XSS' que atinge a mesma página da Vulnerabilidade '001':



E novamente, o código é interpretado pelo navegador.



---

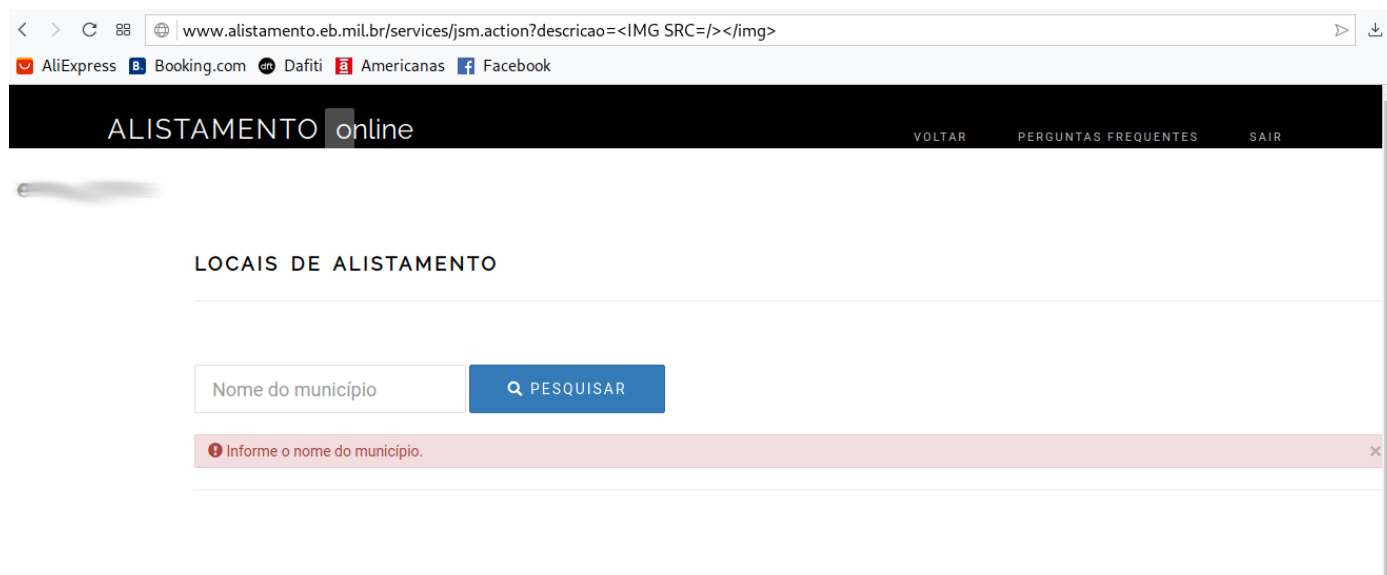
João Vítor S. Fontoura, Desenvolvedor Web e Analista de Segurança Ofensiva.

<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.