Vulnerabilidade Web Encontrada no sistema ZAP Imóveis

Pentester: João Vítor Dos Santos Fontoura.
Período: 31/07/2019.
Ambiente: Web.

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

Resumo

Na presente data de 17/08/2019, foram feitas algumas observações no sistema https://www.zapimoveis.com.br/ no qual pude perceber uma falha de Cross Site Script, não me aprofundei na falha.

Nenhuma lei foi quebrada, e não foi deferido nenhum dano ao serviço referido, segue abaixo detalhes.

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

Cross Site Script (XSS)

Um Ataque XSS se refere a uma injeção de código arbitrário, Javascript, no qual é refletido ao usuário do site, permite roubo de cookies, contas, e praticamente controle do navegador do usuário.

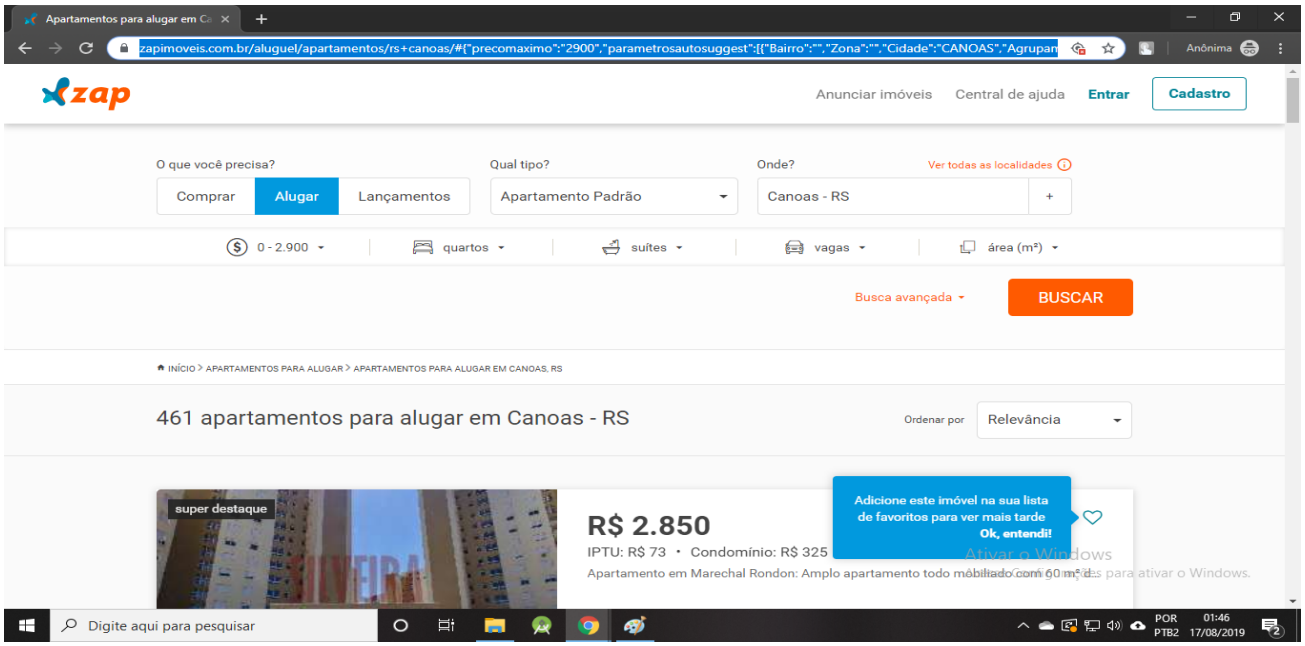
Link de Referência: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

endPoint vulnerável:

https://www.zapimoveis.com.br/aluguel/apartamentos/rs+poa/#{%22precomaximo%22:%22700%22,%22parametrosautosuggest%22:[{%22Bairro%22:%22%22,%22Zona%22:%22%22,%22Cidade%22:%22<script>alert('vulneravel')</script>%22,%22Agrupamento%22:%22%22,%22Estado%22:%22RS%22}],%22pagina%22:%221%22,%22ordem%22:%22Relevancia%22,%22paginaOrigem%22:%22ResultadoBusca%22,%22semente%22:%22348606091%22,%22formato%22:%22Lista%22}

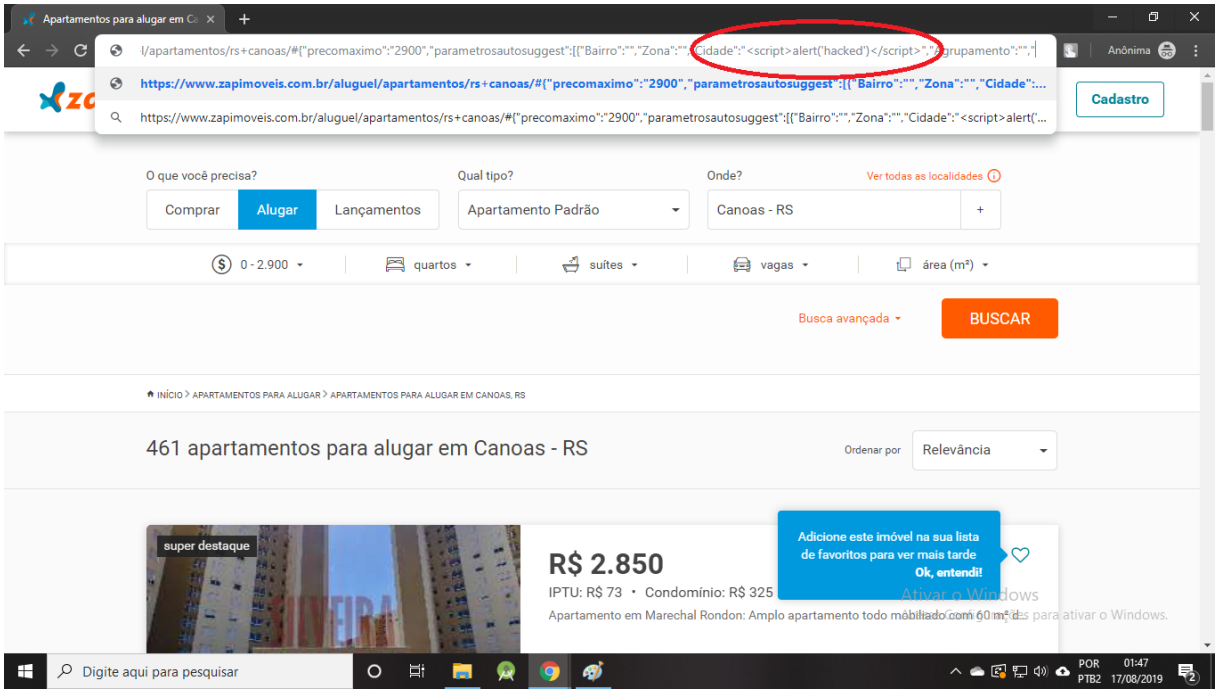
A falha está no parâmetro de cidade do json atribuído para a página, como o valor será exibido para o usuário, ele pode ser facilmente alterado e inserido scripts para a manipulação do navegador. Creio que mais parâmetros podem ser modificados, mas não cheguei a testá-los.

Imagens: *antes do teste

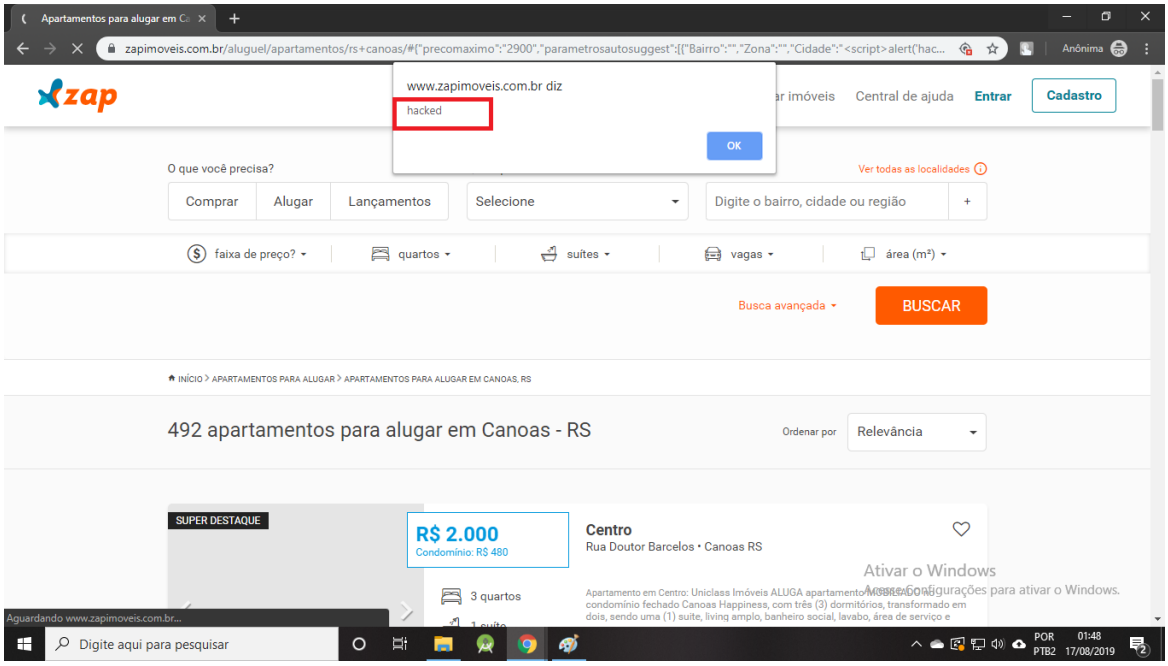


*Injetando o Script

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



* Resultado (página executando o script):



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