



**AppSec Brasil '11**

1st Global Appsec Latin  
America Conference

Porto Alegre - Rio Grande do Sul



**The OWASP Foundation**

<http://www.owasp.org>

# Segurança em Sites de Compras Coletivas: Economizando dor de cabeça!

Magno Logan

[magno.logan@owasp.org](mailto:magno.logan@owasp.org)

*Líder do capítulo [OWASP Paraíba](#)*

*Membro do [OWASP Portuguese Language Project](#)*

# Quem sou eu?



- Desenvolvedor Java EE (+2 anos)
- Líder do Capítulo OWASP Paraíba
- Interesses em Segurança em Aplicações Web e Forense Computacional
- Praticante de Artes Marciais

# Paraíba?!



# Agenda

- Compras Coletivas?
- Vulnerabilidades
- Ataques
- Contramedidas



# Compras Coletivas



Promoções por tempo limitado

# Quantidade de Sites de Compras Coletivas no Brasil

Fonte: [www.bolsadeofertas.com.br](http://www.bolsadeofertas.com.br)





# Vulnerabilidades



# Senhas e + Senhas

- Sem restrição de tamanho mínimo
- Mas com restrição de tamanho máximo!
- Como lembrar de todas elas?
- Usuários utilizam a mesma senha para diversos sites e serviços!



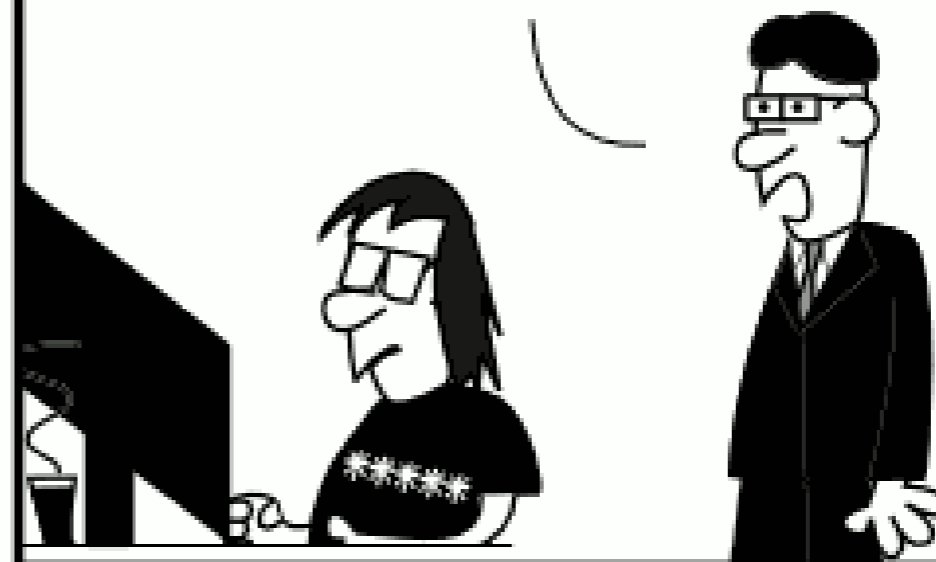
# VIDA DE PROGRAMADOR

.COM.BR



#286

VOCÊ NÃO DISSE QUE O SISTEMA QUE VOCÊ FEZ ERA SEGURO? CONSEGUIRAM ACESSAR COM O MEU USUÁRIO E COLOCAR COISAS LÁ QUE NÃO FUI EU...



DEIXA EU DAR UMA OLHADA. QUAL A SUA SENHA?

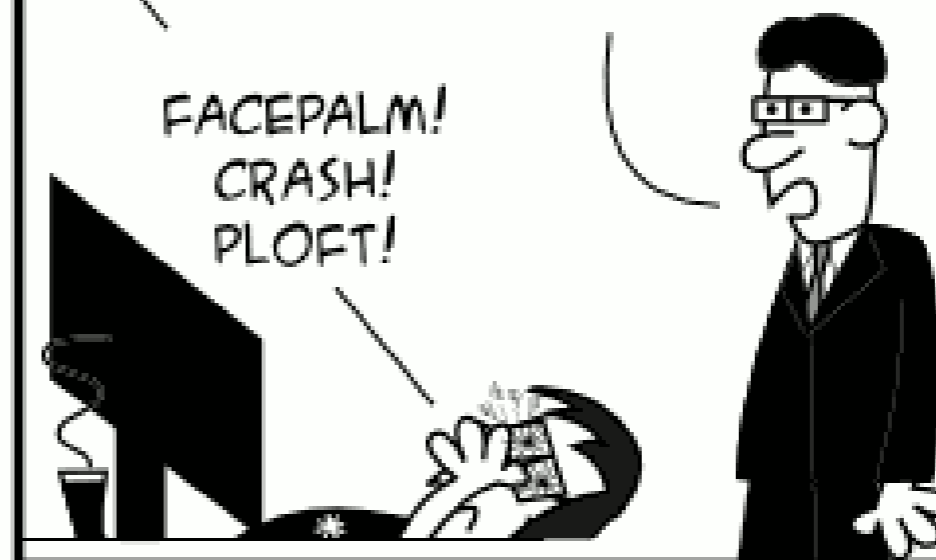
"UM"...



"UM" É O QUE MAIS?

SÓ. COLOCO SÓ O NÚMERO 1 PARA NÃO ESQUECER...

FACEPALM!  
CRASH!  
PLOFT!



# Senhas e + Senhas

- Senhas são armazenadas em texto plano ou em hash MD5
- Como sabemos?!
- Opção “esqueci minha senha” envia sua senha pelo email
- Já ouviram falar de Rainbow Tables?

# XSS

- São muito comuns nos sites de compras coletivas!
- Pressa para colocar no ar - "Time is money!"
- Permite ao atacante obter os cookies de sessão do usuário
- Acessar como outro usuário e obter os cupons dele

# SQL Injection

- Permite ao atacante acessar os dados do sistema
- Obter nomes, usuários, senhas e o mais importante: os códigos dos cupons
- O atacante pode copiar o código de um cupom e gerar seu próprio cupom
- Muito fácil hoje em dia devido às ferramentas disponíveis

# Ainda não aprendemos!

- Lista de sites de compras coletivas já são distribuídos em fóruns de "hacking"

<http://www...com.br/rio-de...idpromocao=976>  
<http://www...com.br/ofertaDoDia.asp?oferta=50>  
<http://www...tas.com.br/index.php?cod=91>  
<http://www...n.br/?pagina=oferta&id=72>  
<http://www...a.com.br/home/...em=1&oferta=22>  
<http://www...com.br/ofertas...info.php?id=55>  
[http://www...n.br/mostra\\_oferta.php?id=99](http://www...n.br/mostra_oferta.php?id=99)  
<http://www...vantagens.com.br/index.php>  
<http://www...n.br/compra-col... .php?cidade=2>  
<http://www...com.br/oferta... localidade=90>  
<http://www...ao.com.br/?p=of...d cidade=10695>  
<http://www...ahora.com.br/de...es&id cidade=1>  
<http://www...om.br/ofertas.php?idOferEnc=423>  
<http://www...com.br/site/?cidade id change=0>

# Falhas Lógicas

- Estabelecimentos não checam a identidade do possuidor do cupom
- Alguns estabelecimentos solicitam apenas o código da promoção (não precisa imprimir o cupom!)
- Sites permitem alterar o nome do dono do cupom depois da compra

# Sites prontos

- Facilidade em ganhar \$\$
- Senhas default conhecidas
- Uma falha grave no sistema afeta todos que possuem!

99% PORTUGUÊS - AINDA EM TRADUÇÃO

COMPRE CONOSCO E GANHE ATUALIZAÇÕES GRATUITAS!

# Script Clone

## CompraColetiva

CLONE

100% editável

com painel adm

**A Oportunidade é Agora!**  
Comece seu negócio online.  
Ao adquirir o site de compra coletiva, prestaremos suporte por e-mail.

Integrado botão pagseguro pagseguro UOL

Se tiver dúvidas, **pergunte** antes de comprar.  
Se tiver dúvidas após adquirir o Site de **CompraColetiva**, **prestamos suporte** por e-mail.

# Falha no



- Plataforma aberta de comércio eletrônico
- 790 mil sites afetados, 17 mil só no Brasil
- Distribuição de malwares através falhas conhecidas: 2 Java, 1 IE, 1 Win, 1 AR
- E se o seu site for assim?!



Depois não vai chorar...





# Cadê o protocolo seguro?



http://pechinhadodia.com/conheca.pchxa

| Onde compra...



Além disso, você compra com total segurança. Utilizaremos protocolo seguro de transferência de dados, que impede que suas informações sejam interceptadas por terceiros. Trabalhamos com as principais bandeiras de cartões e redes bancárias através do Pagamento Digital.

Para quaisquer outras dúvidas entre em [contato](#) conosco. Envie sua pergunta e nossa equipe terá o prazer de atendê-lo.

Faça seu [cadastro](#) gratuitamente e esteja sempre informado sobre novas ofertas.

# Por que não criptografar?!

- HTTP não é seguro!
- Dados trafegam abertamente na rede
- Sites dizem utilizar “protocolo seguro”
- Porque não utilizar HTTPS?
- “Porque é lento” não é desculpa!

# Únicos que utilizam?!



Mas ainda de maneira errada!

# Cadastro sem HTTPS?

www.peixurbano.com.br/conta/Criar

 João Pessoa ▼ Cadastre-se | Login

Oferta do dia Como funciona ✉ Receba e-mail diário 👤 Ganhe R\$10

## Atualize seus dados e receba novidades

O Peixe Urbano sempre está em contato com o Cardume, com ofertas inacreditáveis. Para que você receba sempre novidades, é importante manter seus dados atualizados em nossa base.

**Dados Pessoais** Você possui uma conta no Facebook? [f Register with Facebook](#)

E-Mail:

Nome:

Sobrenome:

Senha:

Repetir Senha:


Receba e-mail para:  ▼

Data de Aniversário:  (ex: 20/10/1980)

Sexo:  Feminino  Masculino

Bairros:

# Falso senso de segurança

 <https://www.groupon.com.br/login>

**GROUPON** Escolha sua Cidade:  
**João Pessoa** ▼

Cadastre-se e receba R\$ 12

[Oferta do dia](#) [Ofertas anteriores](#) [Como funciona](#) [MeuGroupon](#)

**Já sou membro**

Email  Senha

efetuar o login automaticamente

**Login**

[Esqueceu a senha?](#)

# Cadê a segurança?

www.groupon.com.br/ofertas/joaopessoa

**GROUPON** Escolha sua Cidade: **João Pessoa**

Ganhe R\$ 12 a cada recomendação bem sucedida!

Receba ofertas para João Pessoa:  
Informe seu endereço de email

Oferta do dia | Ofertas anteriores | Como funciona | MeuGroupon

Olá Joao da Silva (Sair) | Minha conta

Receba R\$ 12 se recomendar esta oferta! Orkut Facebook Twitter E-Mail

**Praia de Carapibus/PB: 2 diárias para 2 ou 5 pessoas, a partir de R\$ 110, na Pousada Bangalôs de Carapibus. Parcele em até 6x**

**Compre agora!**

**Valor: A partir de R\$ 110,00**

|              |                           |
|--------------|---------------------------|
| Desconto 50% | Você economiza R\$ 110,00 |
|--------------|---------------------------|

Presenteie um amigo



**Hotéis e Viagens** Ver

**Oferta Nacional:**

R\$ 75,00 em vez de R\$ 150,00: 2 travesseiros NASA Magic com Ultra Fresh antimicrobiano

**R\$ 75,00** em vez de R\$ 150,00 Ver



**Mais descontos**

R\$ 35,00 em vez de R\$ 140,00: Hidratação L'Oréal + corte + escova + limpeza de pele

**R\$ 35,00**





# Ataques







Oferta para: **Rio de Janeiro**

outras cidades

Digite o seu e-mail

Rio de Janeiro

**CADASTRAR**

Como adquirir  
seus créditos

OFERTA  
DO DIA

OFERTAS  
RECENTES

COMO  
FUNCIONA

MINHA  
CONTA

FALE  
CONOSCO



**50%**  
desconto

DE: ~~R\$ 10,00~~

POR:

**R\$ 5,00**

economize R\$ 5,00

**COMPRAR**

Divulgue para  
seus amigos e  
receba o valor  
da oferta em

**CRÉDITOS\***

**INDIQUE AQUI**

### Oferta de Hoje

Vende-se esse anão de R\$ 10,00 por R\$ 5,00



#### Destaque

- Anão semi novo com poucos anos de uso
- 100% revisado

#### Regulamento

- Mínimo de 5 compradores para a ativação da oferta
- Dias e horários para a utilização do cupom de Segunda à sexta das

### Oferta Nacional



52% OFF 5 dias e 4 noites para 2 pessoas + 1 criança de até 5 anos + café da manhã, de R \$1.200,00 por R\$580,00. Parcele em até 10 vezes! de ~~R\$ 1.200,00~~ por R\$ 580,00 (Desconto de 52%)

### Quer Mais Mel?



75% OFF Netbook HD 7" com Google Android 2,2 e 2GB de memória, de R\$799,00 por R\$199,00. Frete grátis para todo Brasil! de ~~R\$ 799,00~~ por R\$ 199,00 (Desconto de 75%)

# O que aconteceu?!

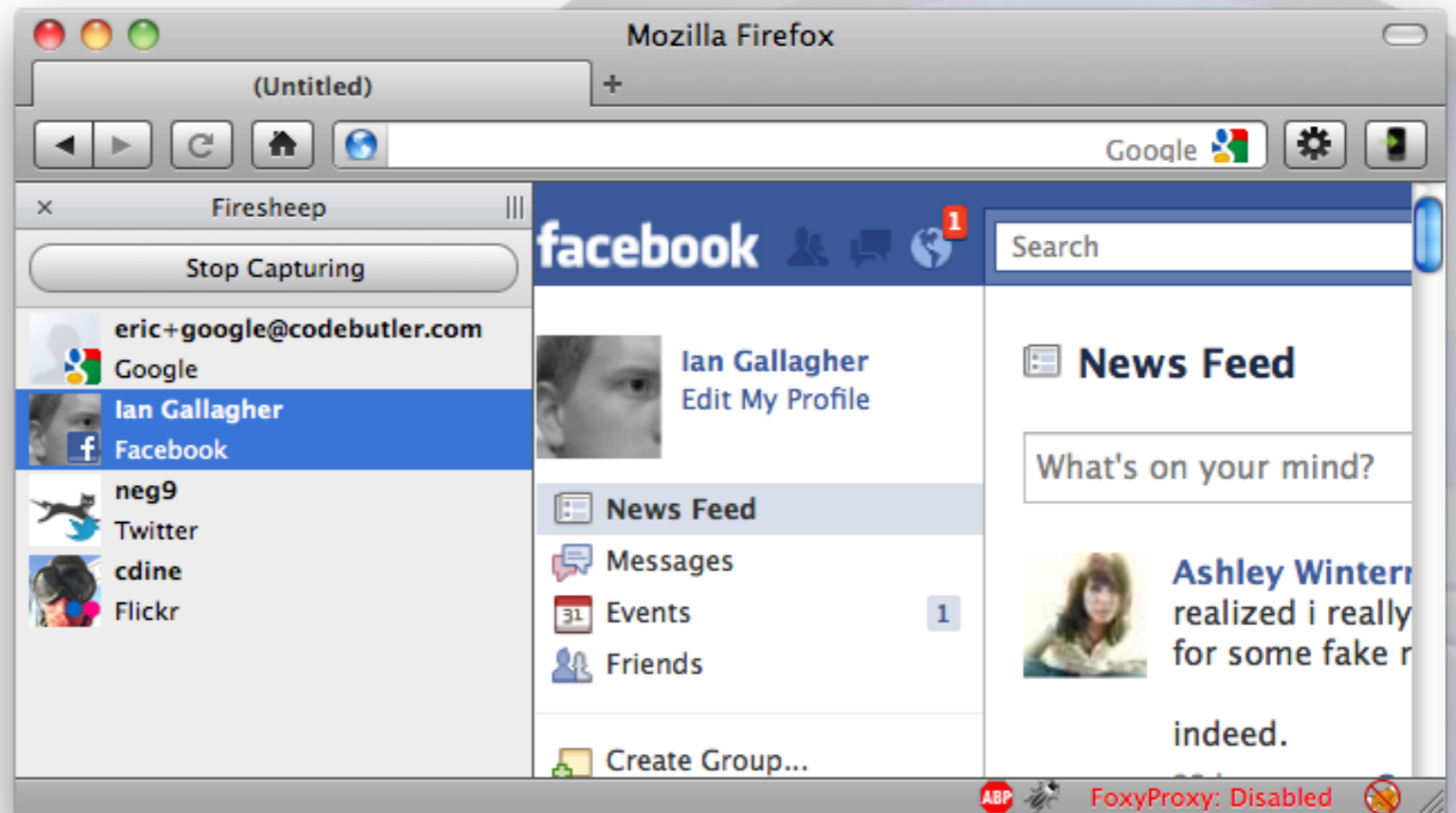
- Provavelmente SQL Injection...
- Afetou a imagem e a confiança do site
- Clientes provavelmente deixaram de comprar lá
- Site diz que tomou medidas para se proteger...
- Mas ainda está vulnerável a SQLi!!!



# Captura de Sessões

- Facilmente realizado em redes sem fio
- Utilizando o Firesheep
- Captura as sessões do usuários
- Imprime os cupons e pronto!
- Sites permitem a mudança no nome do cupom

# Ainda não usa SSL?



# Como fazer?

- Firesheep + TamperData
- Escolher um alvo
- Obter o nome do cookie de sessão
- Criar o script para o Firesheep
- Começar a capturar!

# Modelo de Script

```
register({  
  name: "Site Alvo",  
  url: "http://sitealvo.com/login",  
  domains: [ "sitealvo.com" ],  
  sessionCookieNames: [ "JSESSIONID" ],  
  identifyUser: function () {  
    var resp = this.httpGet(this.siteUrl);  
  }  
});
```

# Versões Mobile



## DROIDSHEEP

- Já existem “cópias” do Firesheep para Android
- Droidsheep e Faceniff
- Permitem a captura de sessões até em redes protegidas com WPA2
- Mais difícil de perceber se alguém está utilizando...



- Se você acessou ou está acessando algum serviço sem criptografia através da rede do evento...



# Site Falsos

57 mil sites falsos  
criados por semana

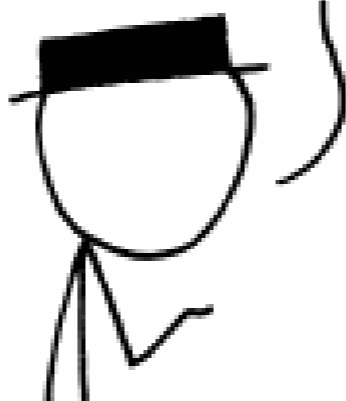


- Criar um site de compra coletiva falso
- Obter as senhas dos usuários
- Testar em outros sites (senhas iguais?)
- Obter os emails dos cadastrados
- Enviar spam ou malware
- Quantos cadastros você tem?

PASSWORD ENTROPY IS RARELY RELEVANT. THE REAL MODERN DANGER IS PASSWORD REUSE.



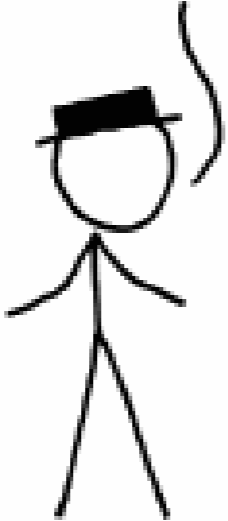
SET UP A WEB SERVICE TO DO SOMETHING SIMPLE, LIKE IMAGE HOSTING OR TWEET SYNDICATION, SO A FEW MILLION PEOPLE SET UP FREE ACCOUNTS.



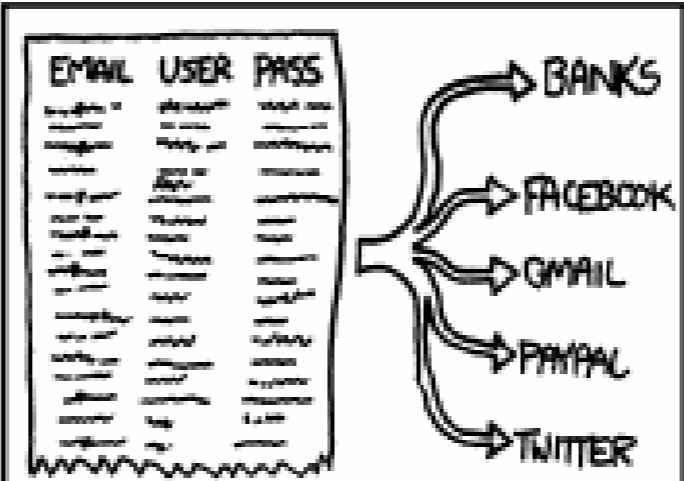
BAM, YOU'VE GOT A FEW MILLION EMAILS, DEFAULT USERNAMES, AND PASSWORDS.



TONS OF PEOPLE USE ONE PASSWORD, STRONG OR NOT, FOR MOST ACCOUNTS.



USE THE LIST AND SOME PROXIES TO TRY AUTOMATED LOGINS TO THE 20 OR 30 MOST POPULAR SITES, PLUS BANKS AND PAYPAL AND SUCH.



YOU'VE NOW GOT A FEW HUNDRED THOUSAND REAL IDENTITIES ON A FEW DOZEN SERVICES, AND NOBODY SUSPECTS A THING.





# Contrameditadas



# E agora?

- Não acesse esses sites através de redes sem fio públicas
- Não faça cadastro em sites que ainda não tem promoções
- Utilize HTTPS sempre que o site permitir



# Lembre-se disto!

- Não salvar os dados do cartão de crédito
  - E utilizar um cartão específico (baixo limite)
- Não informar dados pessoais:
  - CPF, RG, Data de Nasc, Endereço, Tel
- Não clicar em ofertas recebidas por email
  - São facilmente forjáveis!

# Sugestões de Proteção

- Add-ons Firefox ou Chrome





# Perguntas?

Special thanks to:  
Sarah Baso  
Gustavo Barbato

# Referências

[http://www.owasp.org/index.php/Top\\_10\\_2010-Main](http://www.owasp.org/index.php/Top_10_2010-Main)

<http://www.baixaki.com.br/tecnologia/5995-como-funcionam-os-sites-de-compras-coletivas-e-quais-cuidados-devemos-tomar.htm>

<http://www.higorjorge.com.br/258/comercio-eletronico-crimes-ciberneticos-e-procedimentos-preventivos>

<http://miguelalmeida.pt/2010/12/comprar-na-internet-com-seguran%C3%A7a.html>

<http://safeandsavvy.f-secure.com/2010/09/29/shop-savvy-7-practices-to-shop-safely-online>