Clickjacking

CSIRT PoP-MG
alison@csirt.pop-mg.rnp.br

Agenda

- Clickjacking
  - O que é e como funciona
  - Vídeos e Exemplos
- Técnicas "avançadas"
  - Métodos de posicionamento
  - Injeção de texto
- Como se proteger
- Clickjacking Tool

O que é Clickjacking

- Sequestro de Cliques entre domínios

- Foi identificado e publicado em 2008 por Jeremiah Grossman e Robert "Rsnake" Hansen

Processo de exploração

1. Vítima acessa (ou recebe) uma página falsa
2. Vítima clica em algum lugar da página falsa mas na verdade ela está clicando em algo invisível
3. Ação maliciosa é realizada

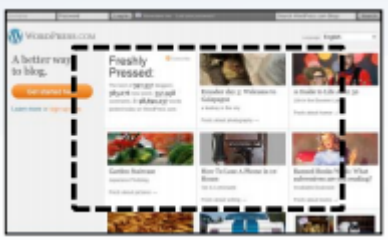
Como é possível?

- Iframes

- Opacidade

- Ordem de pilha (Z-Index)

- Stacking + Opacidade



Exemplo de código

```
<html>
<head>
<Title> Teste2 CJ</title>
</head>
<body>

<div>
<input type="button" style="position:absolute; left:470px; top:12px;" value="Clique">
<input type="button" style="position:absolute; left:550px; top:12px;" value="Clique">
</div>
<iframe style="opacity:0.3;" height="27" width="1000" scrolling="no" src="http://www.boardgamegeek.com/geekmail#messagelist"></iframe>
</body>
</html>
```

Vídeos

Macromedia Flash

- **Guya**

Vídeo: http://www.youtube.com/watch?v=gxyLbpldmuU

O jogo: http://guya.net/security/clickjacking/game.html

- Feross

http://www.youtube.com/watch?feature=player_embedded&v=-LbvglVj8Ho (0:45)

Técnicas "Avançadas"

- Fragmentos e âncoras
- Injeção de texto

Fragmentos e âncoras

- Fragmentos e âncoras
  - <a name="envio">
    - http://exemplo.com.br/index.html#envio
  - <input type="submit" value="Enviar" id="envio">
    - http://exemplo.com.br/index.php?title=CJ&action=edit#envio

Injeção de texto - Drag and Drop (Arrastar e soltar)

- Todos navegadores implementam Drag and Drop API
  - Inicialmente no Internet Explorer, depois, parte do HTML 5
  - Pode passar dados entre domínios

1. A vítima é induzida a arrastar um objeto visível de um ponto A a um ponto B.
2. Quando o arrastamento começa, um script define o texto que deve ser copiado para o campo de formulário de destino, o qual não fica visível para o usuário.
3. Quando a vítima solta o objeto, o dado é copiado para o campo alvo.
4. Deve ser feito para cada campo.
5. Normalmente o usuário deve clicar depois em algum botão de submit.

http://www.youtube.com/watch?v=2Q0ZS12R2hA&feature=related (7:15m)

Como se proteger

- Cliente (usuário)
  - Links
  - Noscript (firefox) - protege desde 2009

- Servidor (desenvolvedor)
  - X-Frame-Options header
  - Frame busting / Frame killing

X-Frame-Options

- Introduzido em 2009 no Internet Explorer 8
  - Internet Explorer, Safari, Firefox, Chrome

WORDPRESS 3.1.3

curl -i www.wordpress.org/wp-login.php

HTTP/1.1 200 OK

Server: nginx

Date: Mon, 12 Dec 2011 12:51:34 GMT

Content-Type: text/html; charset=UTF-8

Connection: close

Vary: Accept-Encoding

Expires: Wed, 11 Jan 1984 05:00:00 GMT

Last-Modified: Mon, 12 Dec 2011 12:51:34 GMT

Cache-Control: no-cache, must-revalidate, max-age=0

Pragma: no-cache

Set-Cookie: wordpress_test_cookie=WP+Cookie+check; path=/; domain=.wordpress.org

X-Frame-Options: SAMEORIGIN

Content-Length: 2251

Frame Busting

- Verifica por meio de scripts se a página está carregada em outro frame e em caso positivo, redireciona o frame para um nível ativo.

```
if (top.location != location)
    top.location = self.location;
```

  - Código pode ser quebrado por meio do atributo "sandbox" do iframe (desabilita o javascript)
  - Tratamento do evento "onBeforeUnload", disparado antes de uma página ser descarregada.
- Problemas com filtros de XSS

Frame Busting

- Melhor solução é por padrão exibir uma página em branco e somente mostrar o documento original, caso o código de proteção não esteja executando no contexto de um frame.

```
<style>
    html {display:none;}
</style>
<script>
if (self == top)  {
   document.documentElement.style.display=
"block";
} else {
    top.location = self.location;
}
</script>
```

Clickjacking Tool

Disponível em:

http://www.contextis.com/research/tools/clickjacking-tool/cjtool.zip

- Clickjacking básico
- Pegar ID's
- Injeção de texto

Para saber mais....

- Clickjacking (The Original Whitepaper)

By Jeremiah Grossman and Robert Hansen

http://www.sectheory.com/clickjacking.htm

- Next Generation Clickjacking

By Paul Stone, presented at BlackHat 2010

http://www.contextis.com/resources/white-papers/clickjacking

- Busting Frame Busting:

A study of clickjacking vulnerabilities on top sites

By Stanford Web Security Group

http://w2spconf.com/2010/papers/p27.pdf

- Clickjacking at OWASP

https://www.owasp.org/index.php/Clickjacking