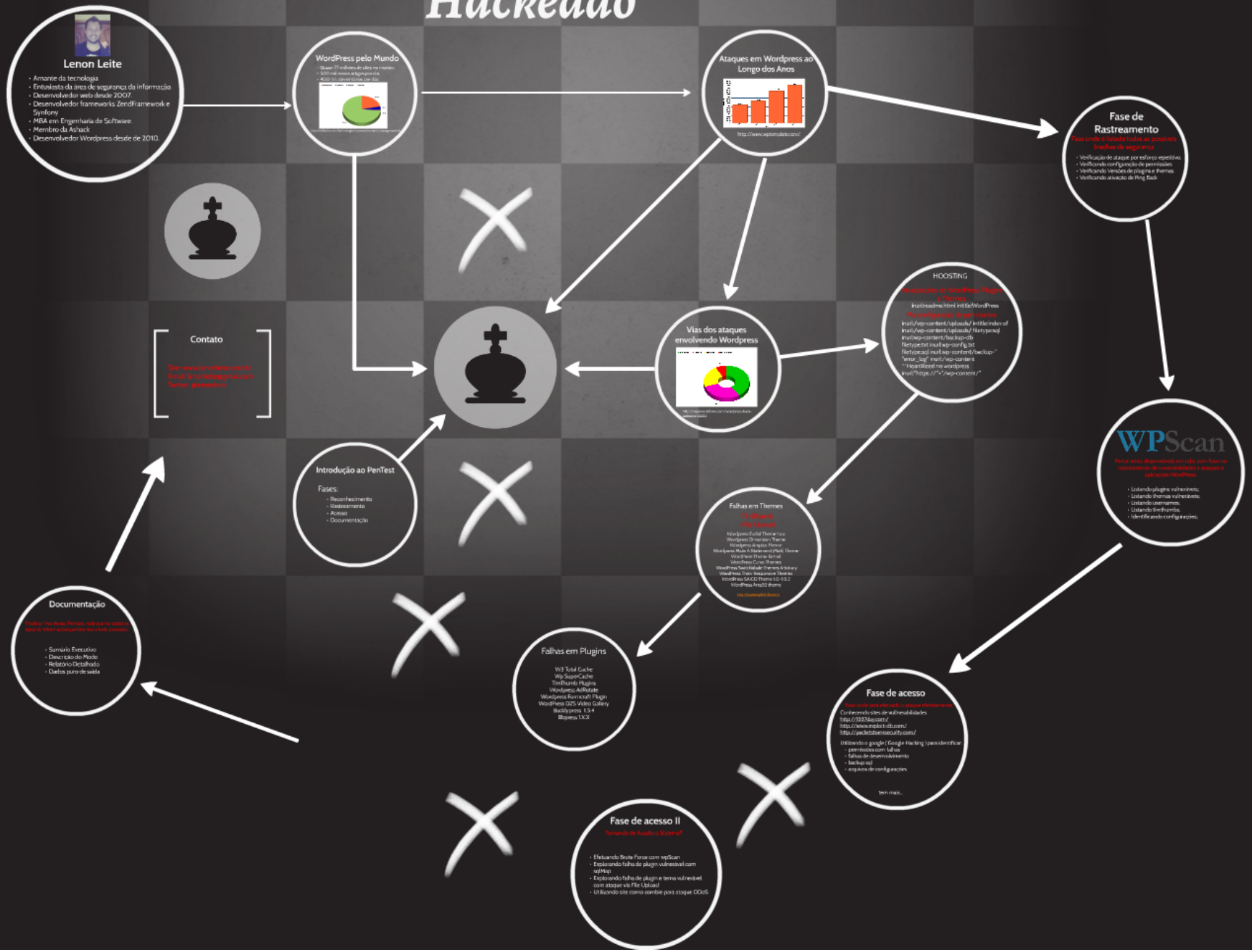
PenTest em WordPress.

Hackeando Para não ser Hackeado



Prezi

PenTest em WordPress.

Hackeando Para não ser Hackeado

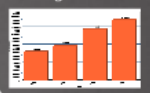
Lenon Leite

- Amante da tecnologia
- Entusiasta da área de segurança da informação.
- Desenvolvedor web desde 2007.
- Desenvolvedor frameworks ZendFramework e Synfony
- MBA em Engenharia de Software.
- Membro da Ashack
- Desenvolvedor Wordpress desde de 2010.

WordPress pelo Mundo

- Quase 77 milhões de sites no mundo;
- 500 mil novos artigos por dia
- 400 mil comentários por dia

Ataques em Wordpress ao Longo dos Anos



https://www.wpkeepalive.com/

Fase de Rastreamento

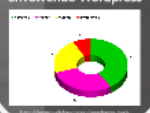
Fase onde é listado todas as possíveis brechas de segurança

- Verificação de ataque por esforço repetitivo.
- Verificando configuração de permissões
- Verificando Versões de plugins e themas.
- Verificando ativação de Ping Back

Contato

Site: www.lenonleite.com.br
Email: lenonleite@gmail.com
Twitter: @lenonleite

Vias dos ataques envolvendo Wordpress



HOOSTING

Atualizações do WordPress, Plugins e Temas

inurl:readme.html intitle:WordPress

Má configuração de permissões

inurl:/wp-content/uploads/ intitle:index of
inurl:/wp-content/uploads/ filetype:sql
inurl:wp-content/backup-db
filetype:txt inurl:wp-config.txt
filetype:sql inurl:wp-content/backup-*
"error_log" inurl:/wp-content
"Hosts/Bots" no wordpress
inurl:"https://"+"/wp-content/"

Introdução ao PenTest

Fases:

- Reconhecimento
- Rastreamento
- Acesso
- Documentação

WPSc

Ferramenta desenvolvida em rastreamento de vuneabilid aplicações Word

- Listando plugins vulne
- Listando themas vulne
- Listando usernames
- Listando timthumbs;
- Identificando configura

Falhas em Themes

RevPlumb
File Upload

Wordpress Basic Theme 1.0.x
Wordpress Dimension Theme
Wordpress Arrayus Theme
Wordpress Make A Statement [MaS] Theme
WordPress Theme Revel
WordPress Curio Themes
WordPress Switchblade Themes Arbitrary
WordPress Think Responsive Themes
WordPress SAICO Theme 1.0-1.0.2
WordPress Area51 theme

Falhas em Plugins

W3 Total Cache
Wp SuperCache
TimThumb Plugins
Wordpress AdRotate
Wordpress Formcraft Plugin
WordPress DZS Video Gallery

Documentação

Produto final do seu Pentest, nele que vai todos os tipos de informações pertinentes a todo processo

- Sumario Executivo
- Descrição do Modo
- Relatorio Detalhado
- Dados puro de saída

Fase de acesso

Prezi

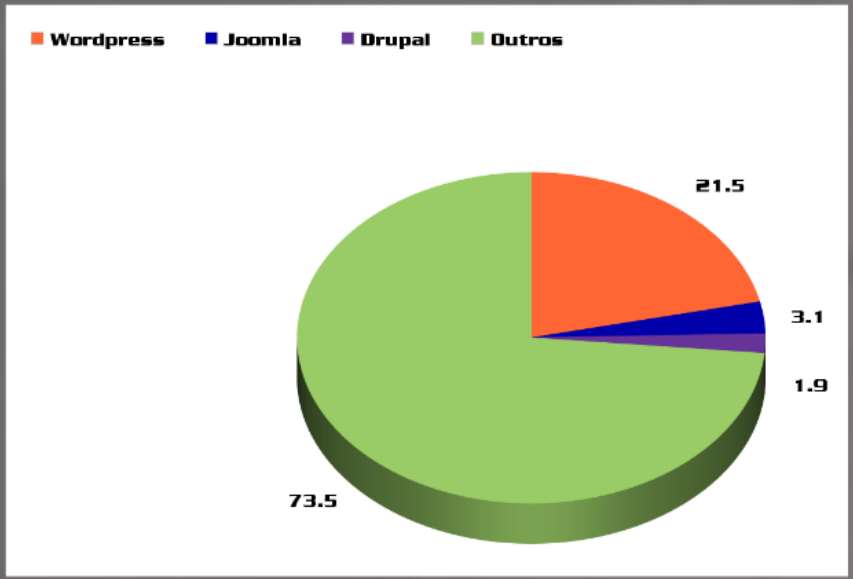
Lenon Leite

- Amante da tecnologia
- Entusiasta da área de segurança da informação.
- Desenvolvedor web desde 2007.
- Desenvolvedor frameworks ZendFramework e Synfony
- MBA em Engenharia de Software.
- Membro da Ashack
- Desenvolvedor Wordpress desde de 2010.

Prezi

WordPress pelo Mundo

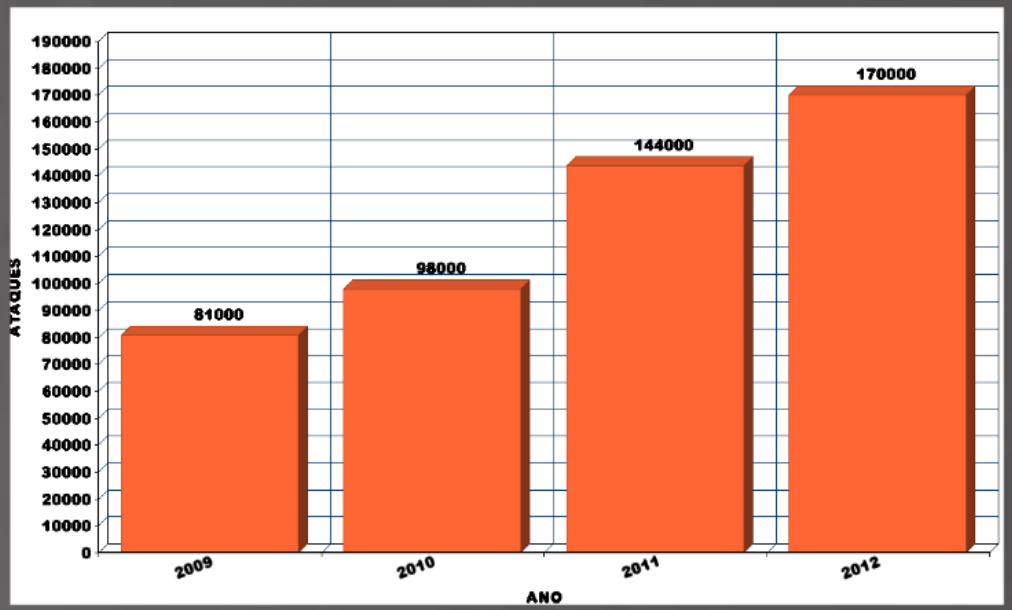
- Quase 77 milhões de sites no mundo;
- 500 mil novos artigos por dia;
- 400 mil comentários por dia;



http://w3techs.com/technologies/overview/content_management/all

Prezi

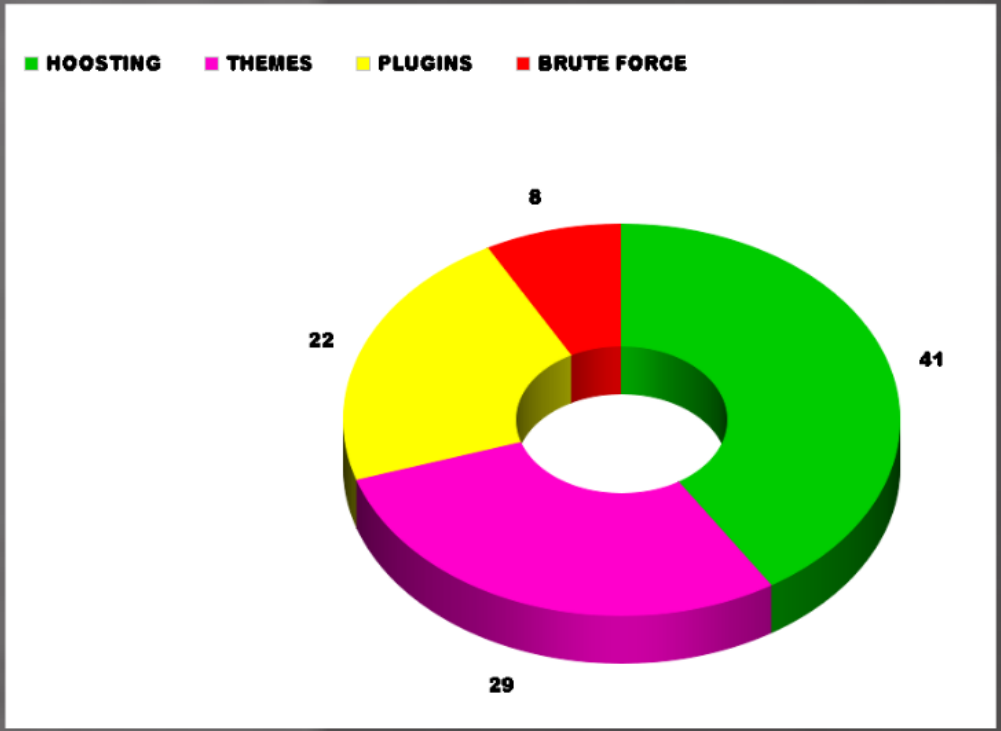
Ataques em Wordpress ao Longo dos Anos



http://www.wptemplate.com/

Prezi

Vias dos ataques envolvendo Wordpress



http://wpsmackdown.com/wordpress-hack-statistics-2013/

Prezi

HOOSTING

Atualizações do WordPress, Plugins e Themes.

inurl:readme.html intitle:WordPress

Má configuração de permissões.

inurl:/wp-content/uploads/ intitle:index of
inurl:/wp-content/uploads/ filetype:sql
inurl:wp-content/backup-db
filetype:txt inurl:wp-config.txt
filetype:sql inurl:wp-content/backup-*
"error_log" inurl:/wp-content
**HeartBleed no wordpress
inurl:"https://"+"/wp-content/"

Prezi

Falhas em Themes

-TimThumb
-File Upload

Wordpress Euclid Theme 1.x.x
Wordpress Dimension Theme
Wordpress Amplus Theme
Wordpress Make A Statement (MaS) Theme
WordPress Theme Kernel
WordPress Curvo Themes
WordPress Switchblade Themes Arbitrary
WordPress Think Responsive Themes
WordPress SAICO Theme 1.0-1.0.2
WordPress Area53 theme

http://www.exploit-db.com/

Prezi

Falhas em Plugins

W3 Total Cache
Wp SuperCache
TimThumb Plugins
Wordpress AdRotate
Wordpress Formcraft Plugin
WordPress DZS Video Gallery
Buddypress 1.5.4
Bbpress 1.X.X

Prezi

Introdução ao PenTest

Fases:

- Reconhecimento
- Rastreamento
- Acesso
- Documentação

Prezi

Fase de Rastreamento

Fase onde é listado todas as possíveis brechas de segurança

- Verificação de ataque por esforço repetitivo.
- Verificando configuração de permissões
- Verificando Versões de plugins e themas.
- Verificando ativação de Ping Back

Prezi

WPScan

Ferramenta desenvolvida em ruby com foco no rastreamento de vunerabilidades e ataques a aplicações WordPress.

- Listando plugins vulneráveis;
- Listando themas vulneráveis;
- Listando usernames;
- Listando timthumbs;
- Identificando configurações;

Prezi

Fase de acesso

Fase onde será efetuado o ataque efetivamente.

Conhecendo sites de vullnerabilidades
http://1337day.com/
http://www.exploit-db.com/
http://packetstormsecurity.com/

Utilizando o google (Google Hacking) para identificar:

- permissões com falhas
- falhas de desenvolvimento
- backup sql
- arquivos de configurações

tem mais...

Prezi

Fase de acesso II

Tomando de Assalto o Sistema!!

- Efetuando Brute Force com wpScan
- Explorando falha de plugin vulnerável com sqlMap
- Explorando falha de plugin e tema vulnerável com ataque via File Upload
- Utilizando site como zombie para ataque DDoS

Prezi

Documentação

Produto final do seu Pentest, nele que irá todos os tipos de informações pertinentes a todo processo.

- Sumário Executivo
- Descrição do Modo
- Relatório Detalhado
- Dados puro de saída

Prezi

Contato

Site: www.lenonleite.com.br
Email: lenonleite@gmail.com
Twitter: @lenonleite

Prezi

PenTest em WordPress.

Hackeando Para não ser Hackeado

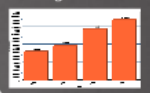
Lenon Leite

- Amante da tecnologia
- Entusiasta da área de segurança da informação.
- Desenvolvedor web desde 2007.
- Desenvolvedor frameworks ZendFramework e Synfony
- MBA em Engenharia de Software.
- Membro da Ashack
- Desenvolvedor Wordpress desde de 2010.

WordPress pelo Mundo

- Quase 77 milhões de sites no mundo;
- 500 mil novos artigos por dia
- 400 mil comentários por dia

Ataques em Wordpress ao Longo dos Anos



https://www.wpkeepalive.com/

Fase de Rastreamento

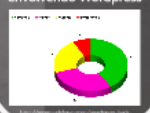
Fase onde é listado todas as possíveis brechas de segurança

- Verificação de ataque por esforço repetitivo.
- Verificando configuração de permissões
- Verificando Versões de plugins e themas.
- Verificando ativação de Ping Back

Contato

Site: www.lenonleite.com.br
Email: lenonleite@gmail.com
Twitter: @lenonleite

Vias dos ataques envolvendo Wordpress



HOOSTING

Atualizações do WordPress, Plugins e Temas

inurl:readme.html intitle:WordPress

Má configuração de permissões

inurl:/wp-content/uploads/ intitle:index of
inurl:/wp-content/uploads/ filetype:sql
inurl:wp-content/backup-db
filetype:txt inurl:wp-config.txt
filetype:sql inurl:wp-content/backup-*
"error_log" inurl:/wp-content
"Hosts/Bots" no wordpress
inurl:"https://"+"/wp-content/"

Introdução ao PenTest

Fases:

- Reconhecimento
- Rastreamento
- Acesso
- Documentação

WPSc

Ferramenta desenvolvida em rastreamento de vuneabilid aplicações Word

- Listando plugins vulne
- Listando themas vulne
- Listando usernames
- Listando timthumbs;
- Identificando configura

Falhas em Themes

RevPlumb
File Upload

Wordpress Basic Theme 1.0.x
Wordpress Dimension Theme
Wordpress Arrayus Theme
Wordpress Make A Statement [MaS] Theme
WordPress Theme Revel
WordPress Curio Themes
WordPress Switchblade Themes Arbitrary
WordPress Think Responsive Themes
WordPress SAICO Theme 1.0-1.0.2
WordPress Area51 theme

Falhas em Plugins

W3 Total Cache
Wp SuperCache
TimThumb Plugins
Wordpress AdRotate
Wordpress Formcraft Plugin
WordPress DZS Video Gallery

Documentação

Produto final do seu Pentest, nele que vai todos os tipos de informações pertinentes a todo processo

- Sumario Executivo
- Descrição do Modo
- Relatorio Detalhado
- Dados puro de saída

Fase de acesso

Prezi