UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

CCUEC

UNICAMP

nic.br | cert.br

4º Fórum Brasileiro de CSIRTs

17 e 18 de setembro de 2015

São Paulo, SP

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

CCUEC

Detectando vulnerabilidades e promovendo a segurança em aplicações Web

Gesiel Bernardes
gesielgb@unicamp.br

Agenda:

✔ CSIRT Unicamp

✔ Segurança Web na Unicamp

✔ Promovendo a segurança em Aplicações Web

✔ Resultados obtidos

Sobre o CSIRT Unicamp:

- Criado em 1999;
- Alocado no Centro de Computação da Unicamp (CCUEC);
- Trabalha em parceria com os Administradores de Redes e Sistemas das Unidades/Órgãos.
- 4 analistas / 91 unidades / 70 mil usuários

Sobre o CSIRT Unicamp:

Principais atividades:

- Resposta e tratamento de incidentes de segurança (análise de logs de firewalls, logs dos honeypots, análise de flows e notificações externas e internas)
- Emissão de Certificado Digital – Projeto Icpedu
- Palestras de conscientização para usuários finais
- Site: Publicações Técnicas e Informativas
- Testes de detecção de vulnerabilidades

Segurança Web na Unicamp

- ✔ Resolução interna (GR-052/2012) estabelece as normas para uso de TI:
  - ➔ Existem normas para o conteúdo dos sites;
  - ➔ Determina que seja realizada segurança preventiva;
- ✔ Unidades mantém sua própria Infraestrutura.

Segurança Web na Unicamp

Problemas:

- ✔ Manutenção do ambiente Web não era considerado crítico
- ✔ Aumento no número de casos de servidores Web comprometidos
- ✔ Maioria dos problemas ocasionados por falhas simples ou ausência de atualização.

Promovendo a Segurança em Aplicações Web

Incentivando a atualização das aplicações

- ✔ Divulgação de boletins de segurança das aplicações Web mais utilizadas:
  - → WordPress;
  - → Joomla;
  - → Drupal;
  - → Outros.

Promovendo a Segurança em Aplicações Web

Publicação de artigos para melhoria da Segurança e Hardening de Aplicações Web.

Dicas para manter seu ambiente Web seguro

Escrito por Gesiel Galvão Bernardes

Cada vez mais frequentes, os ataques á sites Web tiram o sono de qualquer Administrador. Abaixo listamos algumas dicas para melhorar a segurança de seu ambiente Web. Serão abordadas dicas para Servidores com Apache e Nginx.

Wordfence - Um plugin de segurança para Wordpress

Escrito por Vanderlei Busnardo Filho

Atualmente o uso de Gerenciadores de Conteúdo - CMS - é praticamente obrigatório, uma vez que oferece diversas posibilidades para administrar as publicações de um site.
Com um conteúdo cada vez mais dinâmico, instantâneo e interativo, o uso de uma ferramenta que faça o trabalho pesado é indispensável.

10 Dicas para manter seu Joomla seguro

Escrito por Gesiel Galvão Bernardes

O Joomla é o segundo CMS (Content Management System, ou Sistema de Gerenciamento de Conteúdo) mais utilizado no mundo. Porém alguns cuidados são necessários ao utilizar esta poderosa ferramenta. Neste artigo estão dez dicas para manter o Joomla mais seguro (sem precisar tornar-se um especialista em Joomla).

Promovendo a Segurança em Aplicações Web

Realizando Testes de Vulnerabilidades

- ✔ Antecipar problemas
- ✔ Meio de cobrar o cumprimento da Resolução Interna
- ✔ Chamar atenção dos Administradores para a Segurança do Ambiente

Promovendo a Segurança em Aplicações Web

Realizando Testes de Vulnerabilidades –> Divulgação

Divulgar que testes serão realizados em toda a rede.

- Abrangência
- Objetivos
- Benefícios
- Medidas

Promovendo a Segurança em Aplicações Web

Realizando Testes de Vulnerabilidades –> Criação da base de sites à serem testados

Base formada pelo *merge* de três listas:

- SEO Quake: extensão do Firefox, onde foi feita a pesquisa por “unicamp.br”, gerou lista csv;
- Consulta no DNS da Unicamp;
- Pedidos de inclusão.

Promovendo a Segurança em Aplicações Web

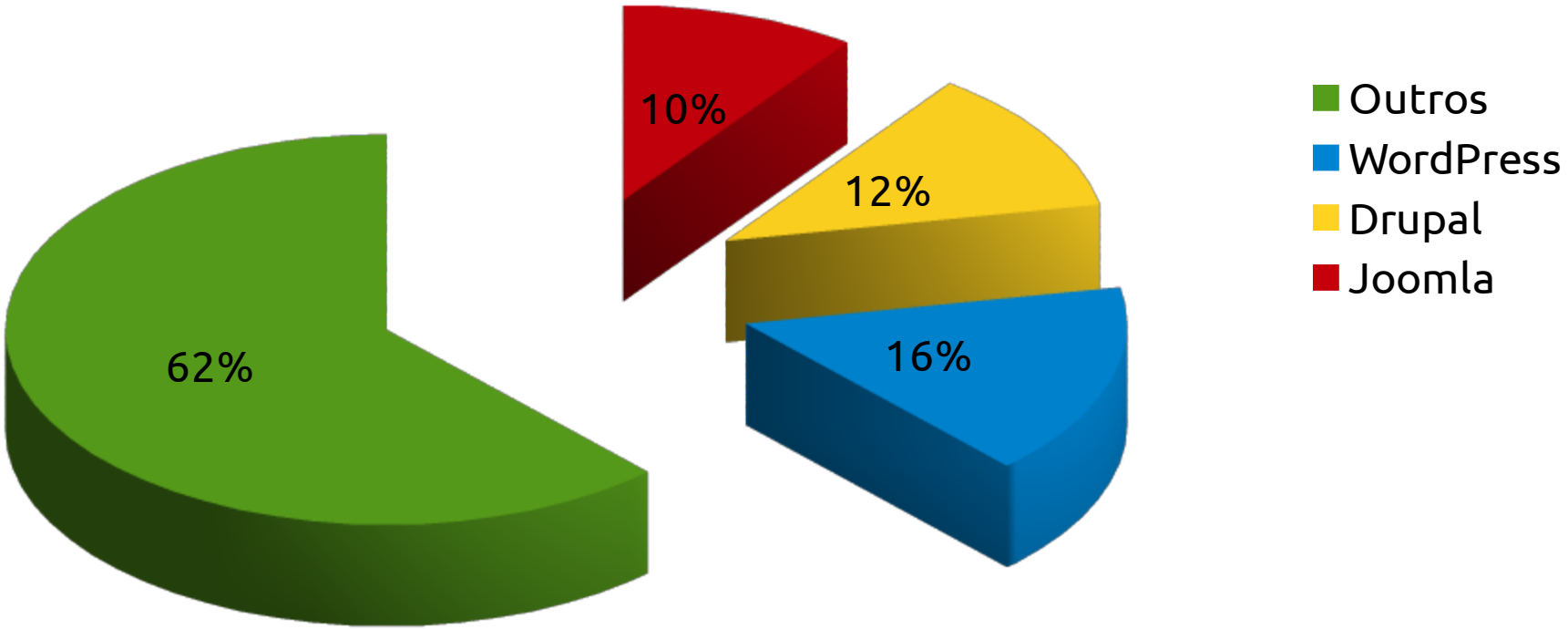
Realizando Testes de Vulnerabilidades –> Criação da base de sites à serem testados

- Número inicial de Sites: 745;
- Número final: 425 Sites;
- Números não incluem subsites (/site1, /site2...).

Identificar a aplicação utilizada pelo Site:

- Identificação utilizando Wappalyzer (Chrome/Firefox)
- Identificação automática via driver Python Wappalyzer

Identificação — Análise — Validação — Tratamento



Identificação — Análise — Validação — Tratamento

Realizar o teste de acordo com a aplicação:

- Wordpress: WPScan
- Wordpress + desenv. próprio: WPScan, Owasp Zap
- Joomla/Drupal: CMSmap
- Joomla/Drupal + desenv. próprio: CMSmap + Owasp ZAP
- Outros: Owasp ZAP

Identificação — Análise — Validação — Tratamento

- WordPress/Joomla/Drupal desatualizado (core): Envia notificação
- Plugins de CMS vulneráveis/desatualizados: Confirmar vulnerabilidade.
- Demais sites vulneráveis: Validação das vulnerabilidades (Sqlmap, testes manuais...)

Evitar falso positivo!

Identificação — Análise — Validação — Tratamento

Notificar o responsável:

- Registro dos incidentes;
- Acompanhar a solução;
- Reteste.

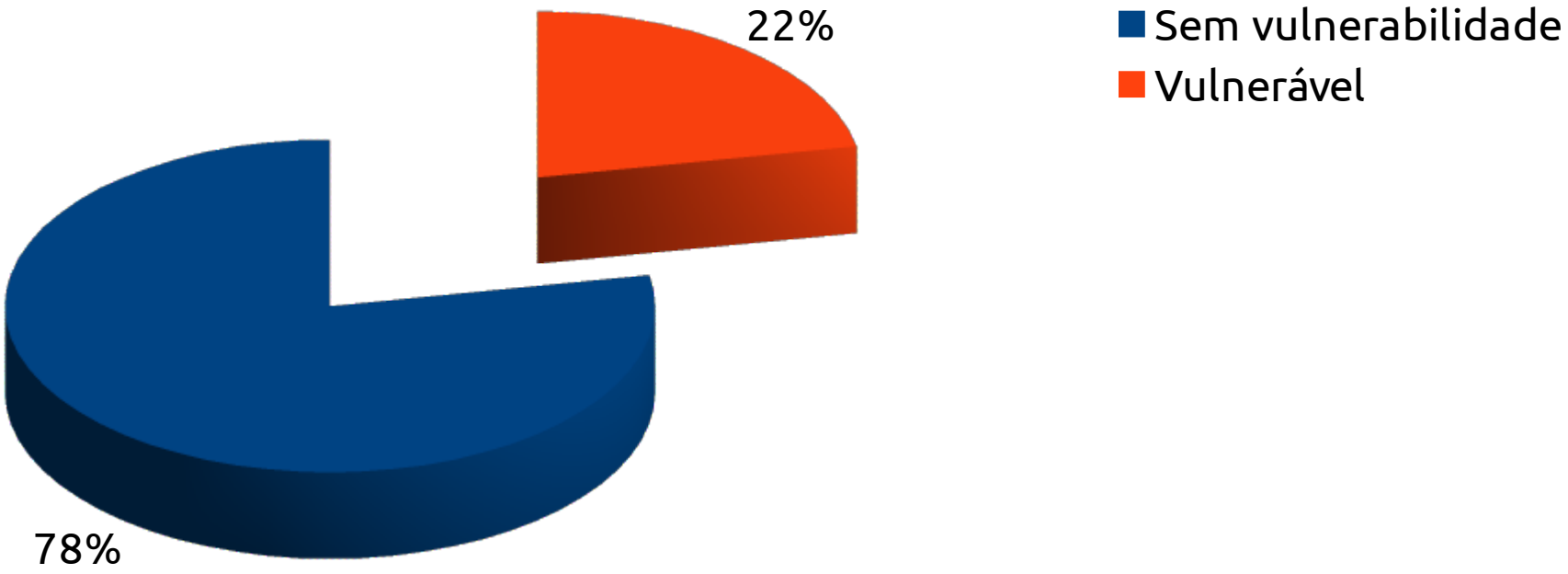
Casos especiais:

- Site comprometido
  - Identificar o problema
  - Resolver
  - Testar

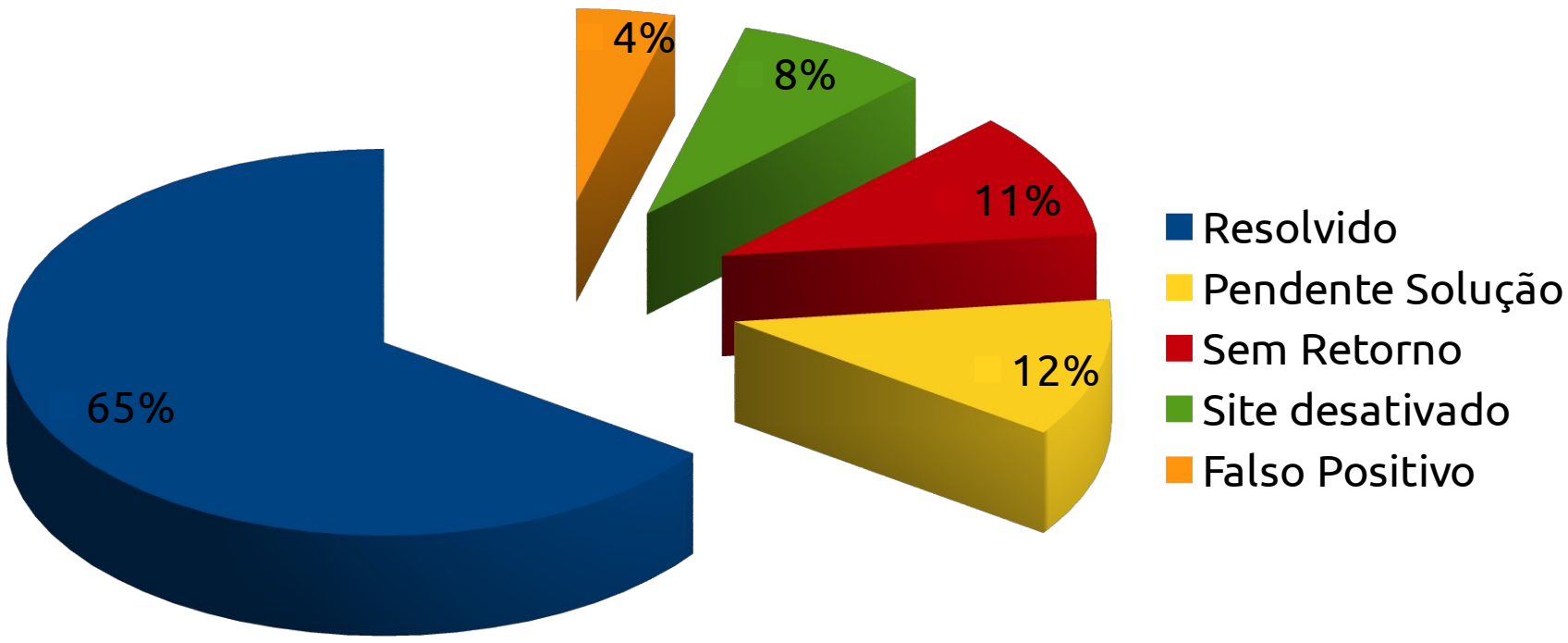
Resultados:

- 425 Sites testados;
- Cerca de 800 testes realizados;
- Aproximadamente 1200 vulnerabilidades graves corrigidas
- Redução de Sites comprometidos: De 5-10/mês para 1/mês.

Resultados:



Resultados:


4%
8%
11%
12%
65%
Resolvido
Pendente Solução
Sem Retorno
Site desativado
Falso Positivo

Desafios Encontrados:

- ✔ Escolha/ajustes das ferramentas a serem utilizadas;
- ✔ Validação das Vulnerabilidades encontradas;
- ✔ Unidades com site vulnerável sem recursos para resolução do problema;

Próximos Passos:

- ✔ Realimentar a base de sites a serem testados;
- ✔ Fazer testes mais específicos;
- ✔ Automatizar partes do processo;

UNICAMP

CSIRT UNICAMP
Computer Security Incident Response Team

CCUEC

Perguntas?

www.security.unicamp.br
security@unicamp.br

Apoio:

AFPU
Agência para a Formação Profissional da Unicamp