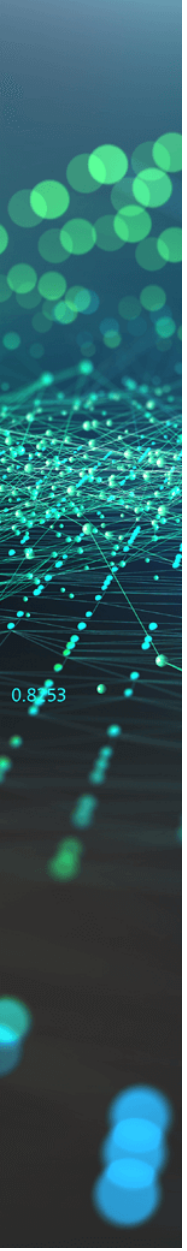

FCCN UNIDADE DA FCT
Tecnologia para o Conhecimento

CSIRT IN A BOX 2022

AUDITORIA

Louise Altvater

RCTS CERT

CERT RCTS

OBJECTIVO

- **Buscar vulnerabilidades num website que corre o WordPress e documentá-las no Template de Auditoria.**

- **Em grupo**

CONTEXTO

From: Sheila Souza <sheilasouza@pobreseguranca.tk>
Sent: 03 de Novembro de 2022 11:40
To: info@csirtfantasia.cf
Subject: URGENTE: Pedido de Auditoria – http://pobreseguranca.tk

Bom dia,

Estamos a lançar um novo site para a nossa empresa Pobre Segurança <pobreseguranca.tk> e por isso gostávamos de solicitar uma auditoria de segurança ao CSIRT Fantasia. Temos uma certa pressa pois iremos divulgar o site publicamente neste sábado, por isso esperamos que o relatório esteja pronto amanhã, se possível.

Sheila Souza

Segurança para Casas

Pobre Segurança

http://pobreseguranca.tk

INSTRUÇÕES

Instruções no ficheiro: [A14] Auditoria - INSTRUÇÕES PARA ACTIVIDADE

Ferramentas online que podem ser usadas:

- **WPScan**
- **Idyllum Labs**
- **Nikto (Através da Plataforma Onworks)**
- **HostedScan**

INSTRUÇÕES

```
__          _______ _____
\ \        / /  __ \ / ____|
 \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
  \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
   \  /\  /  | |     ____) | (__| (_| | | | |
    \/  \/   |_|    |_____/ \___|\__,_|_| |_|

WordPress Security Scanner by the WPScan Team
                Version 3.8.21
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
```

```
[+] URL: http://notreal.tk/ [199.255.181.99]
[+] Effective URL: http://notreal.tk/ru
[+] Started: Mon Mar 28 15:20:09 2022

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.6 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] http://notreal.tk/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] WooCommerce Help Scout
 | Location: https://notreal.tk/wp-content/plugins/woocommerce-help-scout/
 | Latest Version: 1.9.2 (up to date)
 | Last Updated: 2020-01-25T08:17:00.000Z
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 2.0 (100% confidence)
 | Found by: Readme - Changelog Section (Aggressive Detection)
 |
 | - http://notreal.tk/wp-content/plugins/woocommerce-help-scout/readme.txt
 | Confirmed By: Change Log (Aggressive Detection)
 | - http://notreal.tk/wp-content/plugins/woocommerce-help-scout/CHANGELOG.md,
Match '## v.2.0'
```

4 METODOLOGIA

4.1 TESTES AUTOMATIZADOS DE VULNERABILIDADES

Software	Resultados
WPScan (**EXEMPLO**):	**EXEMPLO:** A ferramenta WPScan encontrou os seguintes resultados: o Server: Apache/2.4.46 (Ubuntu) o Plugin(s) Identified: - WooCommerce Help Scout |Location: http://notreal.tk/wp-content/plugins/woocommerce-help-scout/ | Version: 2.0

4.2 TESTES MANUAIS

EXEMPLO:

- Através do que foi apontado pelo resultado da ferramenta WPScan, conseguimos confirmar que o website usa o plugin WooCommerce Help Scout, através do link : http://notreal.tk/wp-content/plugins/woocommerce-help-scout/readme.txt, mas que a versão utilizada é a 2.8.

FCCN UNIDADE DA FCT

Fundação para a Ciência e a Tecnologia

INSTRUÇÕES

5.2 Vulnerabilidades Detetadas

Serviços e Comunicações

Vulnerabilidades detetadas – 19X.XXX.XXX.XXX (pobreseguranca.tk)			
VulnID	Tipo de vulnerabilidade	Impacto (Alto, Médio ou Baixo)	Descrição
00	**EXEMPLO:** Unrestricted Upload of File with Dangerous Type	**Alto**	**EXEMPLO:** O website utiliza a versão 2.8 do plugin do WordPress WooCommerce Help Scout. As versões prévias à 2.9.1 deste plugin estão expostas à uma vulnerabilidade que permite que usuários não autenticados façam uploads de quaisquer ficheiros ao website que terminem com o padrão wp-content/uploads/hstmp (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24212)

6 Recomendações

Recomendamos as seguintes tomadas de ação, de forma a mitigar ou eliminar as falhas de segurança identificadas no capítulos anterior:

Vulnerabilidades	
VulnID	Recomendação
00	**EXEMPLO:** Houve um patch para tratar desta vulnerabilidade na versão 2.9.1 deste plugin. Recomendamos atualizar o plugin para uma versão igual ou superior à 2.9.1.

FCCN UNIDADE DA FCT

Fundação para a Ciência e a Tecnologia

INSTRUÇÕES

Vulnerabilidades NÃO devem ser exploradas

Tempo: 1h15

Breakout Rooms

RESULTADOS POSSÍVEIS

1 Informações Gerais

Auditoria	
Início:	04/11/2022 --:--
Final:	04/11/2022 --:--
Organização:	Pobre Segurança
Contactos:	Sheila Souza <sheilasouza@pobreseguranca.tk>

Documento	
Autor(es) :	

2 Introdução

2.1 Objetivos

Esta auditoria tem como principal objetivo identificar e documentar possíveis vulnerabilidades existentes no website da empresa Pobre Segurança (http://pobreseguranca.tk) passíveis de serem exploradas por atacantes externos.

2.2 Tipo de testes

A auditoria foi executada através de testes "black-box" e a informação previamente fornecida foi a seguinte:

- http://pobreseguranca.tk

4 Metodologia

4.1 Testes automatizados de vulnerabilidades

Software	Resultados
WPScan	A ferramenta WPScan encontrou os seguintes resultados: o Server: Apache/2.4.52 (Ubuntu) o http://pobreseguranca.tk/xmlrpc.php o http://pobreseguranca.tk/readme.html o http://pobreseguranca.tk/wp-cron.php o WordPress version 5.2 identified o WordPress theme in use: Neve - Version: 3.4.1 (80% confidence) < pode ser confirmado aqui http://pobreseguranca.tk/wp-content/themes/neve/style.css> o Plugin(s) Identified: • otter-blocks| Location: http://pobreseguranca.tk/wp-content/plugins/otter-blocks/ | Version: 1.3.1 (Versão certa 2.0.14 confirmável através de http://pobreseguranca.tk/wp-content/plugins/otter-blocks/readme.txt & http://pobreseguranca.tk/wp-content/plugins/otter-blocks/CHANGELOG.md)
Idyllum Labs	A ferramenta Idyllum Labs encontrou os seguintes resultados: o SSL Issues found. Traffic to site is not properly encrypted o IP: 193.136.2.58 o Open ports: 22 (tcp) – ssh o Port 80 (tcp) – http o CMS • Wordpress 6.0 o Other • Open-Graph-Protocol (website)

FCCN UNIDADE DA FCT

Fundação para a Ciência e a Tecnologia

RESULTADOS POSSÍVEIS

4.2 TESTES MANUAIS

- Foi possível fazer a enumeração de plugins usados através do seguinte link: http://pobreseguranca.tk/index.php?rest_route=/
- E, seguindo o padrão do WordPress de localizações de informações sobre plugins, foi possível encontrar a versão de alguns dos plugins através do link: https://pobreseguranca.tk/wp-content/plugins/nome-plugin/readme.txt

Plugins:

- oembed
- redux 4.3.19
- extendify-gutenberg-patterns-and-templates
- seopress 6.0.2
- nv
- elementor 3.6.0
- otter 2.0.14
- wp-site-health
- wp-block-editor

* Também foi possível encontrar a versão do plugin elementor através de link obtido por meio do scan feito pelo Idyllum Labs - http://pobreseguranca.tk/?p=174 .

- Existe divulgação de informação sensível em vários lugares:
  - No código fonte da página principal existe um comentário que divulga um endereço de email;
  - Existe um post de blog com o nome "Teste" onde há divulgação do que parece ser nomes de usuários do wordpress;

RESULTADOS POSSÍVEIS

5.2 Vulnerabilidades Detetadas

Serviços e Comunicações

VulnID	Vuln/Info	Impacto	Descrição
01	Divulgação de informação Sensível	Alto	É possível obter informação sensível através do código fonte da página principal e a enumeração dos usuários do WordPress através de post do blog. Estas informações facilitam um ataque de brute force.
02	Insufficient Access Control leading to Subscriber+ Remote Code Execution	Alto	Versão do plugin Elementor (3.6.0) utilizada pelo website está exposta a uma vulnerabilidade que, se explorada, permite a execução não autorizada de várias ações AJAX que tornam possível que um atacante modifique dados do site além de ser capaz de fazer o upload de ficheiros maliciosos que podem ser usados para obter remote code execution (RCE).
03	Uso do username 'admin'	Médio	Através da enumeração dos usuários do WordPress, que foi possível fazer por meio de descobrimento de divulgação de informação sensível, foi possível verificar que existe um usuário 'admin', o que facilita a execução de um ataque de brute force.
04	WordPress Admin Page	Médio	A página de login do WordPress está disponível
05	Missing Anti-clickjacking Header	Médio	O header X-Frame-Options não está presente, o que possibilita a execução de ataques do tipo "ClickJacking"
06	Porto 22 está aberto	Médio	Na enumeração de portos é possível verificar que o porto 22 (ssh) está aberto
07	Versão desatualizada do Wordpress 6.0	Médio	Vulnerabilidades desta versão: o SQLi via Link API o A Cross-Site Scripting (XSS) vulnerability on the Plugins screen o An output escaping issue within the_meta()
08	Versão desatualizada do Apache	Médio	Vulnerabilidades desta versão (só as moderadas): **mod_proxy_ajp: Possible request smuggling** **modulo Use of uninitialized value of in r:parsebody**
09	X-Content-Type-Options Header Missing	Baixo	O header Anti-Mime-Sniffing X-Content-Type-Options não está configurado como "nosniff", o que permite que alguns browsers façam MIME-sniffing através do response body, podendo fazer com que o response body seja interpretado e exibido como content type ao invés de um content type declarado. Isto pode, em algumas circunstâncias, ser usado para desempenhar ataques de Cross-Site Scripting.

RESULTADOS POSSÍVEIS

6 Recomendações

Recomendamos as seguintes tomadas de ação, por forma a mitigar ou eliminar as falhas de segurança identificadas no capítulos anterior:

Vulnerabilidades	
VulnID	**Recomendação**
01	Apagar qualquer informação sensível, esconder ou deletar post "Test".
02	Houve um patch para esta vulnerabilidade na versão 3.6.3 do plugin Elementor. Contudo, a versão mais atualizada do plugin é a 3.7.8. Recomendamos atualizar o plugin à versão mais recente sempre que possível, ou no mínimo à versão 3.6.3.
03	Evitar usar nomes de usuário como 'admin'. Mas como o nome dos usuários não pode ser mudado no WordPress, garantir que usa uma password segura de forma a diminuir as chances de haver uma intrusão através de brute-force.
04	A página de login da framework está acessível. A mesma deveria ser limitada ao host ou existir algum tipo de ACL de modo a restringir o acesso à mesma.
05	Implementar o Header X-Frame-options ou Content-Security-Policy, através das configurações do Apache, em todas as páginas web do website. Se for necessário que a página possa ser usada em frames por outras páginas dentro do mesmo servidor, então o header deve ser configurado como SAMEORIGIN, caso contrário, deve ser configurado como DENY. Se for implementada uma Content Security Policy, a diretiva "frame-ancestors" deve ser usada.
06	O porto ssh só deve estar aberto para IPs específicos dos administradores.
07	Atualizar o WordPress para a versão 6.1 (mais atual).
08	Atualizar o Apache para a versão 2.4.54 (mais atual).
09	Verificar as configurações do Apache para que use o header de Content-Type de forma apropriada, e configurar o header X-Content-Type-Options com a opção "nosniff" para todas as páginas do website.

Obrigada!