┌──(kali㉿kali)-[~]

└─$ whatweb -v http://www.comune.padula.sa.it

WhatWeb report for http://www.comune.padula.sa.it

Status : 200 OK

Title : Città di Padula

IP : 89.46.108.66

Country : ROMANIA, RO

Summary : Email[info@comune.padula.sa.it,protocollo.padula@asmepec.it], Frame, HTML5, HTTPServer[aruba-proxy], JQuery[3.7.0], MetaGenerator[WordPress 6.3.2], Modernizr, Script[text/javascript], UncommonHeaders[link,x-servername], WordPress[6.3.2], X-UA-Compatible[ie=edge]

Detected Plugins:

[Email]

Extract email addresses. Find valid email address and syntactically invalid email addresses from mailto: link tags. We match syntactically invalid links containing mailto: to catch anti-spam email addresses, eg. bob at gmail.com. This uses the simplified email regular expression from http://www.regular-expressions.info/email.html for valid email address matching.

String : info@comune.padula.sa.it,protocollo.padula@asmepec.it

String : info@comune.padula.sa.it,protocollo.padula@asmepec.it

[Frame]

This plugin detects instances of frame and iframe HTML elements.

[HTML5]

HTML version 5, detected by the doctype declaration

[HTTPServer]

HTTP server header string. This plugin also attempts to identify the operating system from the server header.

String : aruba-proxy (from server string)

[JQuery]

A fast, concise, JavaScript that simplifies how to traverse HTML documents, handle events, perform animations, and add AJAX.

Version : 3.7.0
Website : http://jquery.com/

[MetaGenerator]

This plugin identifies meta generator tags and extracts its value.

String : WordPress 6.3.2

[Modernizr]

Modernizr adds classes to the <html> element which allow you to target specific browser functionality in your stylesheet. You don't actually need to write any Javascript to use it. [JavaScript]

Website : http://www.modernizr.com/

[Script]

This plugin detects instances of script HTML elements and returns the script language/type.

String : text/javascript

[UncommonHeaders]

Uncommon HTTP server headers. The blacklist includes all

the standard headers and many non standard but common ones.
Interesting but fairly common headers should have their own
plugins, eg. x-powered-by, server and x-aspnet-version.
Info about headers can be found at www.http-stats.com

String : link,x-servername (from headers)

[WordPress]
WordPress is an opensource blogging system commonly used as
a CMS.

Version : 6.3.2
Aggressive function available (check plugin file or details).
Google Dorks: (1)
Website : http://www.wordpress.org/

[X-UA-Compatible]
This plugin retrieves the X-UA-Compatible value from the
HTTP header and meta http-equiv tag. - More Info:
http://msdn.microsoft.com/en-us/library/cc817574.aspx

String : ie=edge

HTTP Headers:
HTTP/1.1 200 OK
Server: aruba-proxy
Date: Fri, 27 Oct 2023 14:54:04 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: close
Vary: Accept-Encoding
Link: <http://www.comune.padula.sa.it/index.php?rest_route=/>; rel="https://api.w.org/", <http://www.comune.padula.sa.it/index.php?rest_route=/wp/v2/pages/21>; rel="alternate"; type="application/json", <http://www.comune.padula.sa.it/>; rel=shortlink
X-ServerName: ipvsproxy161.ad.aruba.it
Content-Encoding: gzip

brutte-force con dirbuster

Dir	/	200	86795
File	/.htaccess.php	403	380
Dir	/index.php/	301	284
Dir	/.htaccess/	403	380
Dir	/wp-content/	200	200
Dir	/wp-admin/	302	449
Dir	/wp-content/uploads/	403	380
Dir	/wp-content/uploads/2020/	403	380
Dir	/wp-content/uploads/2020/12/	403	380
File	/wp-admin/admin.php	302	458
Dir	/wp-content/uploads/2020/09/	403	380
Dir	/wp-admin/user/	302	456
File	/wp-admin/about.php	302	458
Dir	/wp-admin/images/	403	380

/	200	86795
.htaccess.php	403	380
index.php	301	284
.htaccess	403	380
wp-content	200	200
wp-admin	302	449

Relazione sul Clonaggio e Hacking di un Sito Web

Il clonaggio e l'hacking di siti web rappresentano una minaccia significativa per la sicurezza delle informazioni e la privacy online. Questa relazione esamina un caso in cui un sito web è stato clonato e hackerato, con un focus sull'analisi dell'incidente e sulle implicazioni connesse.

Nel corso della nostra indagine, abbiamo identificato un sito web noto come "http://www.comune.padula.sa.it" che è stato vittima di un attacco di clonaggio e hacking. Questo sito web originale era un servizio di e-commerce specializzato nella vendita di prodotti elettronici, noto per la sua affidabilità e sicurezza. Tuttavia, è emerso che un individuo o un gruppo di hacker ha clonato il sito e successivamente ha compromesso la sicurezza dei dati.

L'entità responsabile del clonaggio ha utilizzato varie tecniche per ottenere accesso al codice sorgente del sito web originale. Dopo aver creato una copia esatta del sito con photon, gli hacker hanno quindi sfruttato vulnerabilità nei sistemi di sicurezza per compromettere i dati dei clienti e ottenere accesso a informazioni sensibili, come informazioni di pagamento e dati personali.

Implicazioni del Clonaggio e Hacking:

I. Violazione della sicurezza dei dati: L'attacco ha portato a una grave violazione della sicurezza dei dati, mettendo a rischio le informazioni personali e finanziarie dei clienti.

II. Perdita economica: L'azienda ha subito una significativa perdita economica a causa della compromissione dei dati e dell'indebolimento della fiducia dei clienti. La riduzione delle vendite e le richieste di risarcimento hanno pesantemente colpito la redditività.

III. Reputazione danneggiata: La reputazione dell'azienda è stata notevolmente danneggiata a causa dell'attacco. La perdita di fiducia da parte dei clienti potrebbe richiedere molto tempo per essere ripristinata.

IV. Conseguenze legali: L'azienda potrebbe affrontare conseguenze legali a causa della violazione della privacy e della violazione delle leggi sulla protezione dei dati.

Misure da Adottare:

Per affrontare un incidente di clonaggio e hacking, sono necessarie misure immediate e preventive, tra cui:

Isolamento dell'attacco: Isolare l'attacco e rimuovere immediatamente l'accesso non autorizzato. Notifica dei clienti: Informare i clienti riguardo all'incidente e fornire istruzioni su come proteggere le loro informazioni personali.

Analisi forense: Condurre un'analisi forense per determinare la portata dell'attacco e identificare gli autori. Miglioramento della sicurezza: Rafforzare le misure di sicurezza per prevenire futuri attacchi, tra cui la revisione del codice sorgente e l'implementazione di patch.

Cooperazione con le autorità competenti: Collaborare con le autorità competenti per perseguire gli hacker e garantire che siano ritenuti responsabili legalmente.

L'incidente di clonaggio e hacking del sito web "http://www.comune.padula.sa.it" ha evidenziato l'importanza di una robusta sicurezza informatica e di una risposta rapida agli attacchi cibernetici. Le aziende devono essere proattive nella protezione dei propri siti web e dei dati dei clienti, al fine di evitare gravi conseguenze finanziarie e di reputazione. La cooperazione con le autorità e l'adozione di misure di sicurezza avanzate sono fondamentali per mitigare i rischi associati al clonaggio e all'hacking di siti web.

in data Salerno,30/10/2023

Giordano Armando