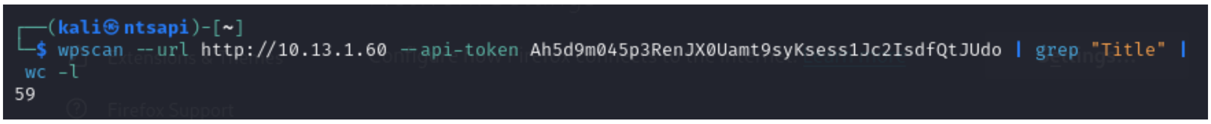
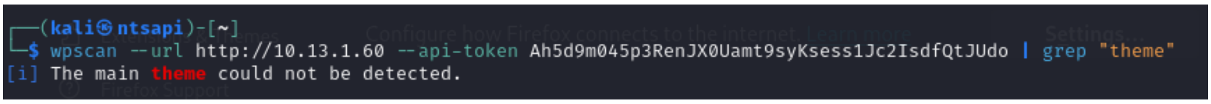
WPScan:

1. How many vulnerabilities have been discovered through the scan?
   Your answer: **59**



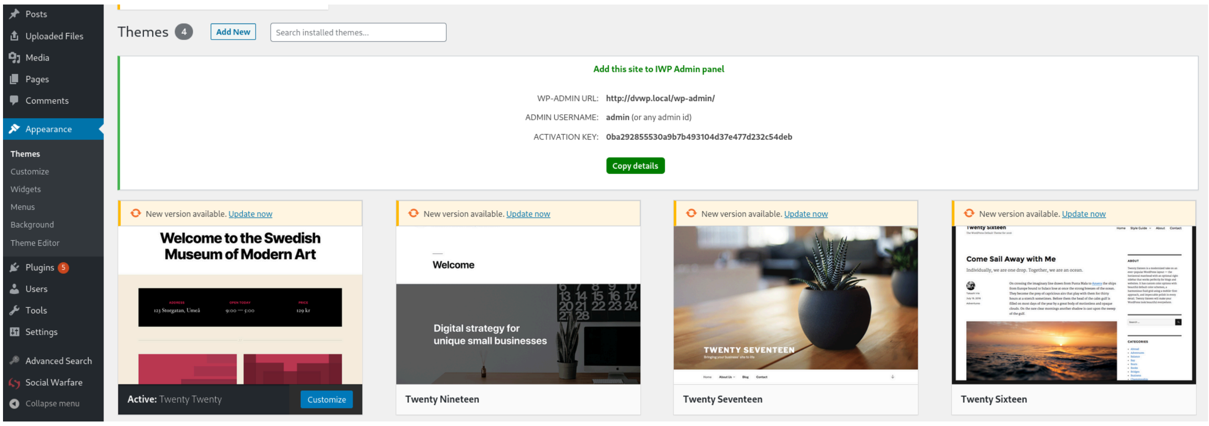
```
┌──(kali㉿ntsapi)-[~]
└─$ wpscan --url http://10.13.1.60 --api-token Ah5d9m045p3RenJX0Uamt9syKsess1Jc2IsdfQtJUdo | grep "Title" |
 wc -l
59
```

2. What is the theme found by wpscan?
   Your answer: Not found with command line



```
┌──(kali㉿ntsapi)-[~]
└─$ wpscan --url http://10.13.1.60 --api-token Ah5d9m045p3RenJX0Uamt9syKsess1Jc2IsdfQtJUdo | grep "theme"
[i] The main theme could not be detected.
```

Found on the Website



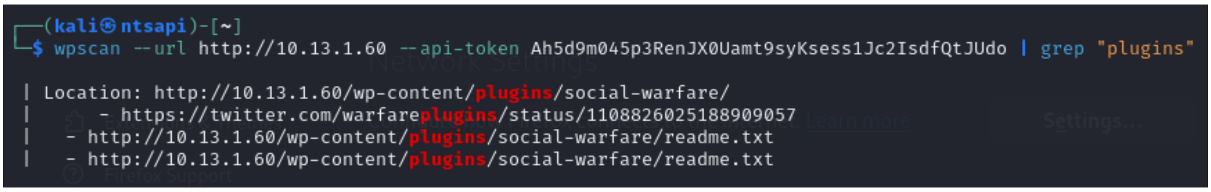
Add this site to IWP Admin panel

WP-ADMIN URL: http://dvwp.local/wp-admin/

ADMIN USERNAME: admin (or any admin id)

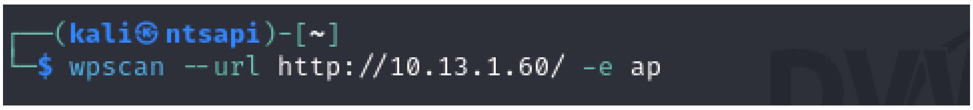
ACTIVATION KEY: 0ba292855530a9b7b493104d37e477d232c54deb

3. How many plug-ins did the scan find?
   Your answer: 4

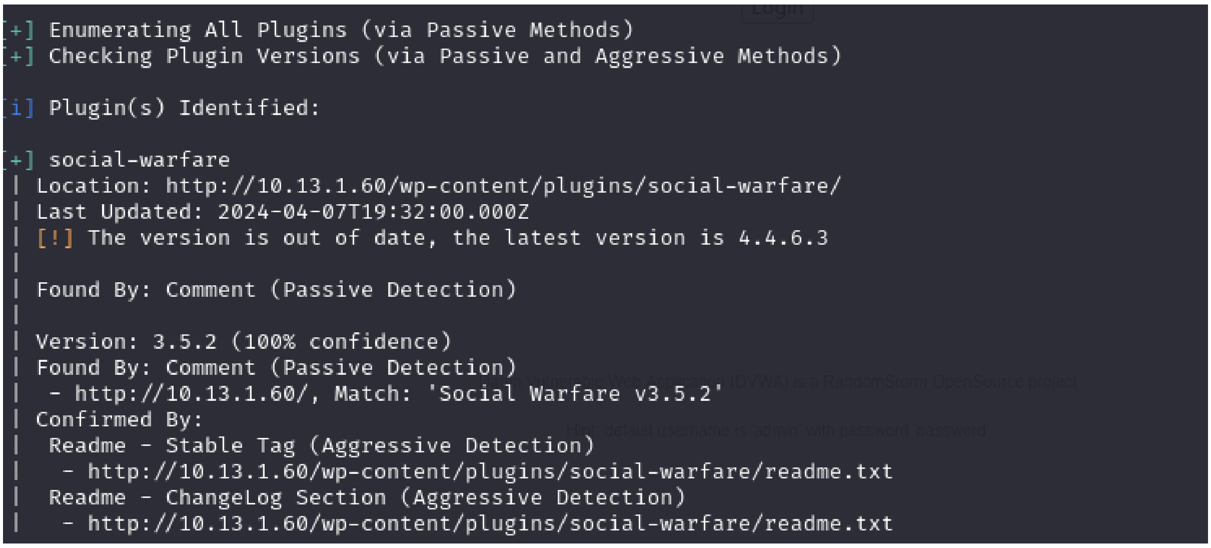


```
┌──(kali㉿ntsapi)-[~]
└─$ wpscan --url http://10.13.1.60 --api-token Ah5d9m045p3RenJX0Uamt9syKsess1Jc2IsdfQtJUdo | grep "plugins"

 | Location: http://10.13.1.60/wp-content/plugins/social-warfare/
 |     - https://twitter.com/warfareplugins/status/1108826025188909057
 |   - http://10.13.1.60/wp-content/plugins/social-warfare/readme.txt
 |   - http://10.13.1.60/wp-content/plugins/social-warfare/readme.txt
```

Alternative method

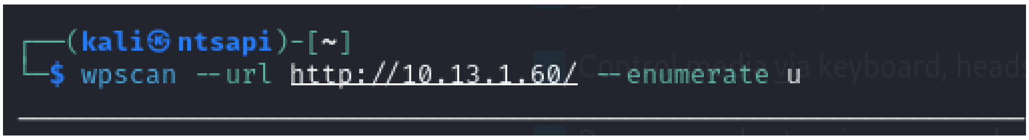


```
┌──(kali㉿ntsapi)-[~]
└─$ wpscan --url http://10.13.1.60/ -e ap
```

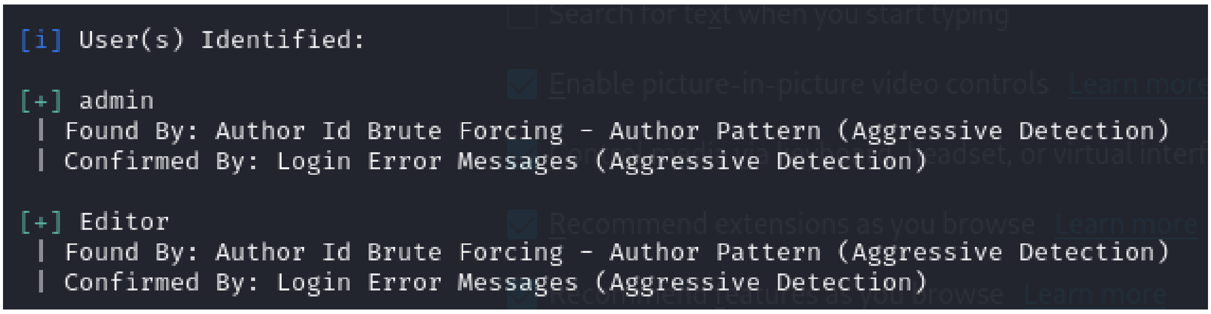


```
[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] social-warfare
 | Location: http://10.13.1.60/wp-content/plugins/social-warfare/
 | Last Updated: 2024-04-07T19:32:00.000Z
 | [!] The version is out of date, the latest version is 4.4.6.3
 |
 | Found By: Comment (Passive Detection)
 |
 | Version: 3.5.2 (100% confidence)
 | Found By: Comment (Passive Detection)
 |  - http://10.13.1.60/, Match: 'Social Warfare v3.5.2'
 | Confirmed By:
 |  Readme - Stable Tag (Aggressive Detection)
 |   - http://10.13.1.60/wp-content/plugins/social-warfare/readme.txt
 |  Readme - ChangeLog Section (Aggressive Detection)
 |   - http://10.13.1.60/wp-content/plugins/social-warfare/readme.txt
```

4. How many users did the scan find?
   Your answer: 2

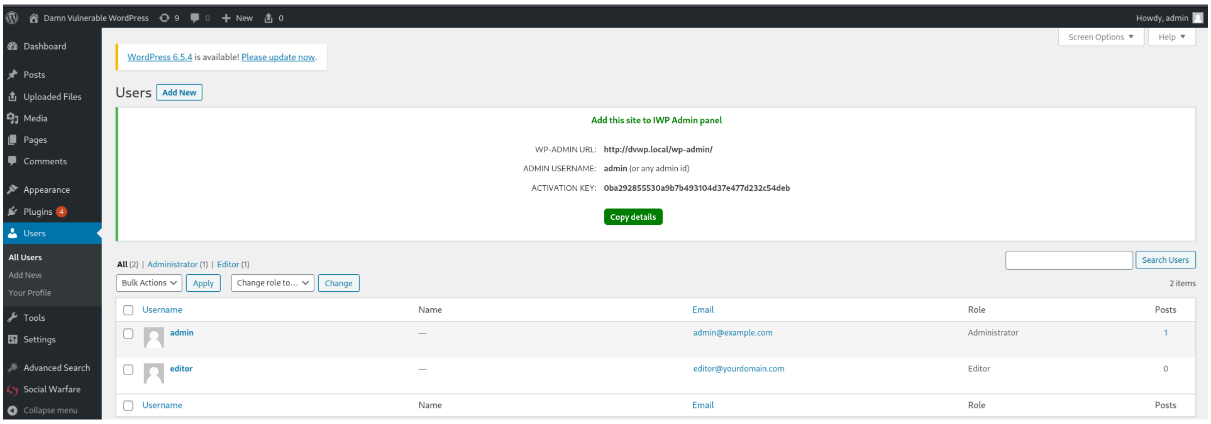


```
┌──(kali㉿ntsapi)-[~]
└─$ wpscan --url http://10.13.1.60/ --enumerate u
```



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

[+] admin
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] Editor
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

5. What is the password of the user starting with j ?
   Your answer: USER DON'T EXIST
6. What is the email of the user starting with j ?
   Your answer: EMAIL DO NOT EXIT



WordPress 6.5.4 is available! Please update now.

Users

Add this site to IWP Admin panel

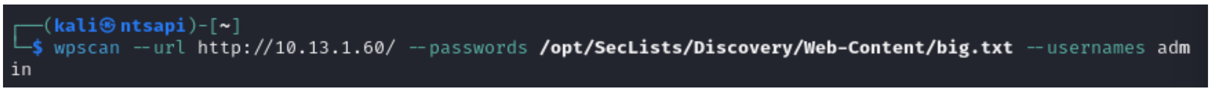
WP-ADMIN URL: http://dvwp.local/wp-admin/
ADMIN USERNAME: admin (or any admin id)
ACTIVATION KEY: 0ba292855530a9b7b493104d37e477d232c54deb

All (2) | Administrator (1) | Editor (1)

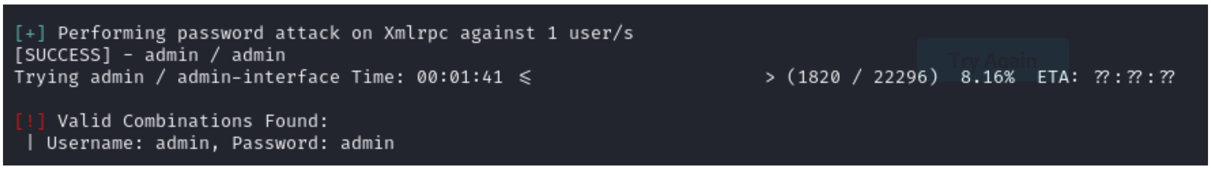
2 items

□ Username	Name	Email	Role	Posts
□ admin	—	admin@example.com	Administrator	1
□ editor	—	editor@yourdomain.com	Editor	0
□ Username	Name	Email	Role	Posts

7. What is the password of the user starting with a ?
   Your answer: **admin**



```
┌──(kali㉿ntsapi)-[~]
└─$ wpscan --url http://10.13.1.60/ --passwords /opt/SecLists/Discovery/Web-Content/big.txt --usernames adm
in
```

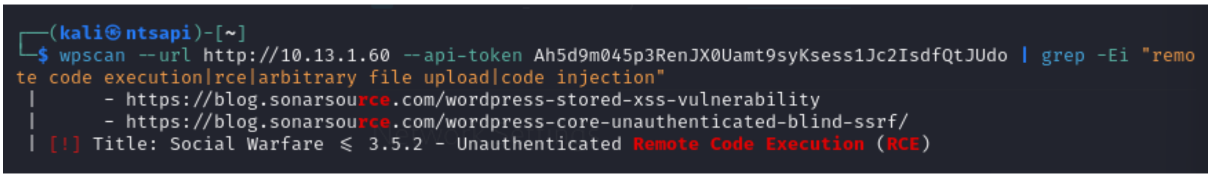


```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - admin / admin
Trying admin / admin-interface Time: 00:01:41 <                    > (1820 / 22296)  8.16%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: admin, Password: admin
```

8. What is the email of the user starting with a ?
   Your answer: admin@example.com

   After getting the password, I logged the details through http://10.13.1.60/wp-json/wp/v2/users/admin and got more information.

9. What vulnerability might be of interest to obtain an RCE?
   Your answer:



```
┌──(kali㉿ntsapi)-[~]
└─$ wpscan --url http://10.13.1.60 --api-token Ah5d9m045p3RenJX0Uamt9syKsess1Jc2IsdfQtJUdo | grep -Ei "remo
te code execution|rce|arbitrary file upload|code injection"
 |       - https://blog.sonarsource.com/wordpress-stored-xss-vulnerability
 |       - https://blog.sonarsource.com/wordpress-core-unauthenticated-blind-ssrf/
 | [!] Title: Social Warfare ≤ 3.5.2 - Unauthenticated Remote Code Execution (RCE)
```

10. If you are an admin, do you need an exploit for an RCE.
    Your answer: NO

As an admin, the concept of needing a Remote Code Execution (RCE) exploit should be approached with extreme caution and a strong adherence to ethical principles and legal boundaries. Here are important considerations regarding RCE exploits for admins:

1. **Understanding RCE**: RCE exploits allow an attacker to execute arbitrary code on a target system remotely, which can lead to complete compromise of the system. This is typically achieved by exploiting vulnerabilities in software or misconfigurations.
2. **Ethical and Legal Implications**:
   - **Ethics**: Using RCE exploits without proper authorization is unethical and can cause harm to individuals, organizations, and systems.
   - **Legality**: Unauthorized use of RCE exploits is illegal in many jurisdictions and can lead to severe legal consequences, including criminal charges.
3. **Admin Responsibilities**:
   - **Security**: Admins are responsible for maintaining the security and integrity of systems under their care. This includes patching vulnerabilities, configuring secure access controls, and monitoring for suspicious activities.
   - **Risk Management**: Rather than seeking out exploits, admins should focus on risk management, including vulnerability assessments, threat modeling, and proactive security measures.
4. **Handling Vulnerabilities**:
   - If you discover a vulnerability, the ethical approach is to report it to the relevant vendor or organization through responsible disclosure channels. This allows them to address the issue and protect their users.
   - Engaging in responsible disclosure helps maintain trust and promotes a safer digital environment.
5. **Security Best Practices**:
   - Stay informed about security best practices and industry standards.
   - Implement strong access controls, least privilege principles, and regular security audits.
   - Educate users and stakeholders about security risks and best practices.

In summary, as an admin, the focus should be on protecting systems and data rather than seeking out exploits like RCE. It's essential to prioritize ethical behavior, legal compliance, and responsible security practices in all aspects of system administration. If you encounter vulnerabilities, handle them responsibly by reporting them to the appropriate authorities for resolution.