PenTest 1

ROOM A

GROUPNAME

Members

ID	Name	Role
XXX		Leader
YYY	Timothy Yap	Member
ZZZ	Ian Chai	Member
AAA	YPWong	Member

Steps: (example) Recon and Enumeration

You should divide your report into 4 sections in general:

1) **Recon and Enumeration (Where you gather data)**
2) **Initial Foothold (where you gain the first reverse shell)**
3) **Horizontal Privilege Escalation (If any, if you pivot to other users)**
4) **Root Privilege Escalation (final step, rooting)**

For each section do the following:

(frame your images with borders)

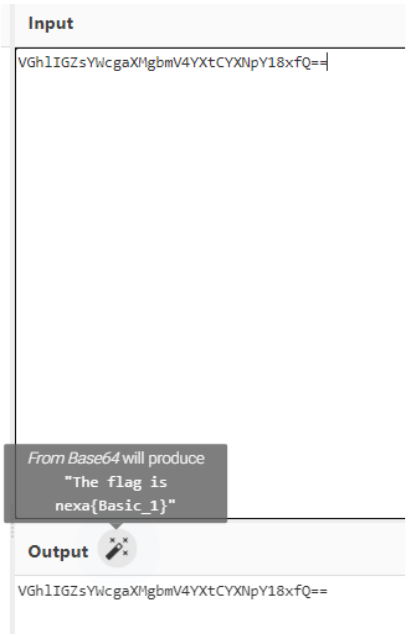
Members Involved: JJChin, Timothy

Tools used: **Nmap/Gobuster/WPScan etc**

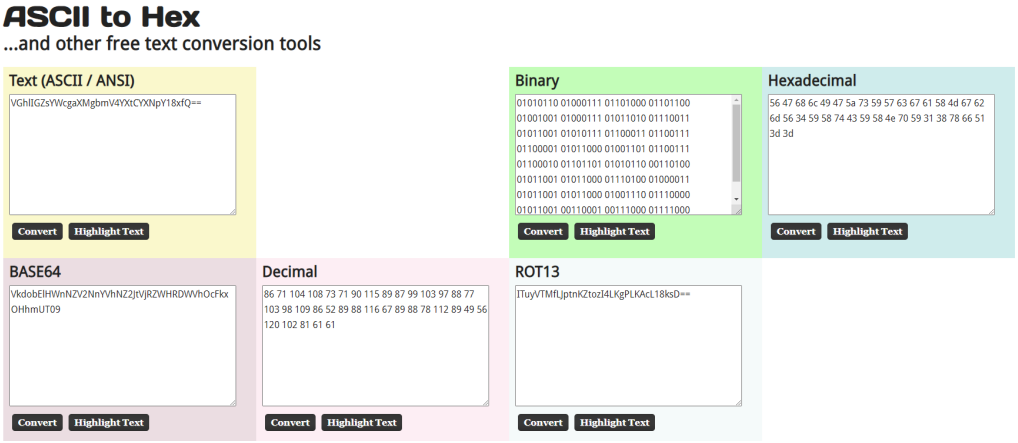
Thought Process and Methodology and Attempts:

JJChin recognised that the string is a base64 code with the '==' ending. Prior to the link being released, JJChin was already aware that Cyberchef could be used to decode base64 strings. Therefore he first attempted

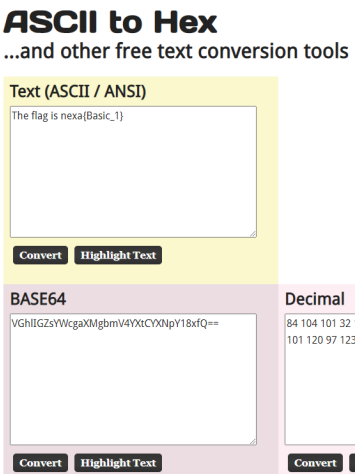
JJChin copied the string to Cyberchef, and the magic wand output revealed the flag.



Later Timothy verified the string was correct using the asciitohex alternative. However, he made a mistake of pasting to the wrong textbox which was the ASCII/ANSI textbox.

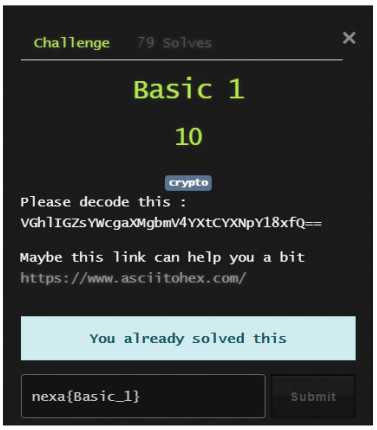


Upon double check, he repasted the string to Base64 textbox and managed to convert and verify the flag successfully.



Final Result: (if you did not manage to solve, just mention you moved on to other questions)

Upon verification of the flag, Timothy placed the flag into the TryHackMe site and got the confirmation.



Use a new page for a new Step

Category:

Question:

Contributions

At the end of the report, attach a table briefly mentioning each member's role and contribution:

ID	**Name**	Contribution	Signatures
XXX	JJChin	Did the recon. Discovered the exploit to root.	
YYY	Timothy Yap	Figured out the exploit for initial foothold.	
ZZZ	Ian Chai	Tried Exploit alternatives B and C but didn't work. Did most of the writing after compiling findings.	
AAA	YPWong	Pivoted from User A to User B. Coke and instant noodles supplier.	

NOTE: IT IS IMPORTANT EACH MEMBER CONTRIBUTES IN SOME WAY AND ALL MEMBERS MUST SIGN TO ACKNOWLEDGE THE CONTRIBUTIONS! DO NOT GIVE FREELOADERS THE FLAGS AS THEY DON'T DESERVE THE MARKS. DO NOT SHARE THE FLAGS WITH OTHER GROUPS AS WELL!

Attach the video link at the end of the report:

VIDEO LINK: https://www.youtube.com/asdkljaklsjdks