Cybersecurity Essentials

Basic knowledge and CTF's

Prabhas Bhat
1RVU22BSC069

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING (SoCSE)
RV University
Bengaluru.

OCTOBER-2024

Cybersecurity Essentials

Basic knowledge and CTF's

Submitted by

Prabhas Bhat

1RVU22BSC069

Under the guidance of

Dr. Phani Kumar Pullela

Center for Innovation and Entrepreneurship

Submitted in partial fulfillment of the requirements for the summer internship conducted during July-August 2024, as part of the BSC (Hons) program at the School of Computer Science and Engineering.

RV UNIVERSITY

Go, change the world

an initiative of RV EDUCATIONAL INSTITUTIONS

CERTIFICATE

This is to certify that the work presented in this report, entitled "***CYBERSECURITY ESSENTIALS: BASIC KNOWLEDGE & CTF's***," has been carried out by ***PRABHAS BHAT (USN NO: 1RVU22BSC069)*** as part of the summer internship during July-August 2024. The work was completed under my supervision and guidance at the School of Computer Science and Engineering, RV University, Bengaluru, India.

I confirm that the content of this report is the student's original work and has not been submitted elsewhere for the award of any degree or diploma.

Prof. Suresh
School of Computer Science and Engineering,
RV University, Bengaluru.

(Signature)

Center Head

Dr. Phani Kumar Pullela
School of Computer Science
and Engineering, (SoCSE)
RV University, Bengaluru.

(Signature)

Program Head

Vidya M J
School of Computer Science
and Engineering, (SoCSE)
RV University, Bengaluru.

(Signature)

Bengaluru,
October, 2024

CERTIFICATE

I hereby certify that the work presented in this report, entitled "***CYBERSECURITY ESSENTIALS: BASIC KNOWLEDGE & CTF'S***," has been carried out by me during my summer internship in July-August 2024. This work was conducted under the supervision of Dr. Phani Kumar Pullela & Suresh, School of Computer Science and Engineering, RV University, Bengaluru, India.

I confirm that the work embodied in this report is my own and has not been submitted for the award of any degree or diploma.

Prabhas Bhat
1RVU22BSC069
School of Computer Science and Engineering,
RV University, Bengaluru.

Bengaluru,

October, 2024

Acknowledgement

I would like to express my heartfelt gratitude to the Center for Innovation & Entrepreneurship for providing me with the opportunity to undertake this internship and for their unwavering support throughout the program.

I am especially thankful to Prof. Suresh and Dr. Phani Kumar for their valuable guidance, mentorship, and encouragement, which played a pivotal role in enhancing my learning experience and helping me build a strong foundation in cybersecurity.

Introduction:

The internship provided a valuable opportunity to explore the evolving field of cybersecurity through theoretical learning, hands-on training, and practical challenges. It enhanced my understanding of core cybersecurity concepts, tools, and techniques critical to protecting digital assets and mitigating threats.

The coursework covered phishing attacks, recent cyber threats, the CIA triad, secure design principles, firewalls, IDS, encryption, data loss prevention, and incident response. Specialized modules included OWASP Top 10: A1 Injection, focusing on injection attack mitigation using tools like OWASP ZAP, and CompTIA Cybersecurity Analyst: Malware, which explored malware detection and countermeasures.

A key highlight was solving Capture The Flag (CTF) challenges, where I applied theoretical knowledge to real-world scenarios, improving problem-solving skills and vulnerability assessment techniques.

Overall, the internship provided a solid foundation in cybersecurity and hands-on experience with essential tools and practices for securing digital systems.

Objectives:

In the course of the internship the 5 courses and CTF challenges covered a variety of objectives.

- Develop foundational knowledge of core cybersecurity concepts, including the CIA triad, secure design principles, and OWASP Top 10 vulnerabilities.
- Understand various cyber threats such as phishing, malware, and injection attacks, and explore defense mechanisms like firewalls, IDS, and data encryption.
- Enhance ethical hacking skills through hands-on experience with reconnaissance tools and hacker tactics to identify and mitigate vulnerabilities.
- Learn techniques for securing applications and networks, including vulnerability assessment, patching, and incident response.
- Gain practical experience with tools like OWASP ZAP for vulnerability assessment and injection attack mitigation.
- Explore malware types, delivery methods, detection techniques, and mitigation strategies.
- Strengthen problem-solving skills by participating in Capture The Flag (CTF) challenges to apply theoretical knowledge in real-world scenarios.
- Foster awareness of compliance scanning and social engineering techniques to protect users and systems.
- Build real-world expertise to tackle cybersecurity challenges and enhance the security posture of organizations.

Methodology:

The approach included structured coursework, practical demonstrations, and interactive activities such as Capture The Flag (CTF) challenges. The key components of the methodology are outlined below:

1. Structured Coursework and Knowledge Acquisition

Each course emphasized essential concepts such as foundational concepts, defense mechanisms, ethical hacking, malware analysis, and vulnerability mitigation, the CIA triad, OWASP Top 10 vulnerabilities, data classification, and secure design principles. This theoretical foundation was crucial for understanding the cybersecurity landscape.

2. Practical Demonstrations and Tool Usage

The courses had pre-recorded demos on how to implement SQL injection attacks, command injections, and malware detection on test operating systems. Industry -standard tools like OWASP ZAP were used to simulate application vulnerability assessments, enabling a practical understanding of security threats and mitigation techniques.

3. Capture The Flag (CTF) Challenges

Participated in CTF challenges of HTB (Hack the Box) and Pico CTF which required the application of acquired knowledge to identify vulnerabilities, exploit systems, and secure data in controlled environments. The challenges enhanced critical thinking and problem-solving skills.

4. Documentation and Reporting

Regular documentation of activities in the internship journal ensured systematic tracking of progress and learning outcomes.

Implementation:

As part of the internship, I engaged in various CTF challenges to apply theoretical cybersecurity knowledge in practical, problem-solving scenarios.

PicoCTF Challenges

1. Verify: Utilized sha256sum to compute file hashes and grep to validate legitimate flags. A provided decrypt script was used to identify the correct flag, demonstrating proficiency with command-line tools and hashing.

2.Heap3 (Binary Exploitation): Exploited a use-after-free vulnerability by reallocating memory and modifying variables to call the check_win function and retrieve the flag.

3.Binary Search: Solved a number-guessing game using the binary search algorithm to identify the correct flag within a limited number of guesses. This reinforced the fundamentals of efficient data search and processing.

4.Unminify (Web Exploitation):Examined the minified website source code to locate the flag, enhancing my ability to analyze and reverse-engineer obfuscated code.

Hack The Box (HTB) CTF Challenges

1.Cyber Apocalypse 2024 (Dimensional Escape Quest):

Solved a series of narrative-driven puzzles by issuing precise commands to progress through an enchanted maze and retrieve the flag.

2.Flag Command:

Exploited the /api/options endpoint and identified the flag by analyzing server responses and outputs.

3.TimeKORP:

Discovered and exploited a command injection vulnerability in a PHP-based application. By injecting a payload (?format='; cat ../flag %23) into the format parameter, the flag was retrieved. This demonstrated a practical understanding of command injection and URL encoding.

- Binary Exploitation: Identified and leveraged memory mismanagement vulnerabilities to achieve specific objectives.
- Command Injection: Exploited server-side vulnerabilities to gain unauthorized access to sensitive data.
- Web Exploitation: Analyzed web pages and backend logic to identify vulnerabilities and extract sensitive information.
- Problem-Solving: Applied algorithms like binary search to efficiently solve challenges.
- Tool Proficiency: Gained hands-on experience with tools and scripting for practical cybersecurity tasks.

Results:

The internship provided invaluable learning experiences, enabling me to apply theoretical cybersecurity concepts to practical challenges. I gained a solid understanding of core topics such as the CIA triad, OWASP Top 10 vulnerabilities, and defense mechanisms like firewalls and IDS. Hands-on training with tools like OWASP ZAP and practical scenarios, including CTF challenges on platforms like PicoCTF and Hack The Box, allowed me to exploit vulnerabilities such as command injection and memory mismanagement, while honing my problem-solving and ethical hacking skills. These experiences enhanced my proficiency in scripting, debugging, and secure practices, preparing me to tackle real-world cybersecurity challenges with confidence and expertise.

Conclusion & Future Work:

The internship provided a comprehensive understanding of core cybersecurity concepts, tools, and techniques while offering hands-on experience through CTF challenges and practical problem-solving scenarios. This blend of theoretical knowledge and practical application has enhanced my skills in identifying and mitigating cyber threats, equipping me with the expertise to address real-world cybersecurity challenges effectively.

Annexure:

MOOC certificates:

Infosys
Navigate your next

COURSE COMPLETION CERTIFICATE

The certificate is awarded to

Prabhas Bhat

for successfully completing the course

Introduction to Cyber Security

on July 1, 2024

Infosys | Springboard

Congratulations! You make us proud!

Thirumala Arohi
Executive Vice President and Global Head
Education, Training & Assessment (ETA)
Infosys Limited

Issued on: Monday, July 1, 2024
To verify, scan the QR code at https://verify.onwingspan.com

Infosys
Navigate your next

COURSE COMPLETION CERTIFICATE

The certificate is awarded to

Prabhas Bhat

for successfully completing the course

Cyber Security: Endpoint Defense

on July 1, 2024

Infosys | Springboard

Congratulations! You make us proud!

Thirumala Arohi
Executive Vice President and Global Head
Education, Training & Assessment (ETA)
Infosys Limited

Issued on: Tuesday, July 2, 2024
To verify, scan the QR code at https://verify.onwingspan.com

Infosys
Navigate your next

COURSE COMPLETION CERTIFICATE

The certificate is awarded to

Prabhas Bhat

for successfully completing the course

Cyber Security and Hacker Tactics Awareness Training

on July 2, 2024

Infosys | Springboard

Congratulations! You make us proud!

Thirumala Arohi
Executive Vice President and Global Head
Education, Training & Assessment (ETA)
Infosys Limited

Issued on: Wednesday, July 3, 2024
To verify, scan the QR code at https://verify.onwingspan.com

PB

Prabhas Bhat

5 Credentials | 1 Issuer

Wallet | Transcript

CompTIA Cybersecurity Analyst+: Malware
9 July 2024
Skillsoft

OWASP Top 10: A1 - Injection
3 July 2024
Skillsoft

Capture the flag challenges:

Verify

Easy | Forensics | picoCTF 2024 | grep | browser_webshell_solvable | checksum

AUTHOR: JEFFERY JOHN

Description

People keep trying to trick my players with imitation flags. I want to make sure they get the real thing! I'm going to provide the SHA-256 hash and a decrypt script to help you know that my flags are legitimate.

You can download the challenge files here:

- `challenge.zip`

The same files are accessible via SSH here:

`ssh -p 58038 ctf-player@rhea.picoctf.net`

Using the password `f3b61b38`. Accept the fingerprint with `yes`, and `ls` once connected to begin. Remember, in a shell, passwords are hidden!

- Checksum: fba9f49bf22aa7188a155768ab0dfdc1f9b86c47976cd0f7c9003af2e20598f7
- To decrypt the file once you've verified the hash, run `./decrypt.sh files/<file>`.

This challenge launches an instance on demand.

Its current status is: RUNNING

Instance Time Remaining: 26:31

Restart Instance

Hints

1 2 3

```
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

ctf-player@pico-chall$ ls
checksum.txt  decrypt.sh  files
ctf-player@pico-chall$ history
    1  ls
    2  history
ctf-player@pico-chall$ sha256sum files/* | grep `cat checksum.txt`
fba9f49bf22aa7188a155768ab0dfdc1f9b86c47976cd0f7c9003af2e20598f7  files/87590c24
ctf-player@pico-chall$ ./decrypt.sh files/87590c24
picoCTF{trust_but_verify_87590c24}
ctf-player@pico-chall$
```

Binary Search

Easy | General Skills | picoCTF 2024 | shell | browser_webshell_solvable | ls

AUTHOR: JEFFERY JOHN

Description

Want to play a game? As you use more of the shell, you might be interested in how they work! Binary search is a classic algorithm used to quickly find an item in a sorted list. Can you find the flag? You'll have 1000 possibilities and only 10 guesses.

Cyber security often has a huge amount of data to look through - from logs, vulnerability reports, and forensics. Practicing the fundamentals manually might help you in the future when you have to write your own tools!

You can download the challenge files here:

- challenge.zip

Additional details will be available after launching your challenge instance.

This challenge launches an instance on demand.

Its current status is: ERROR

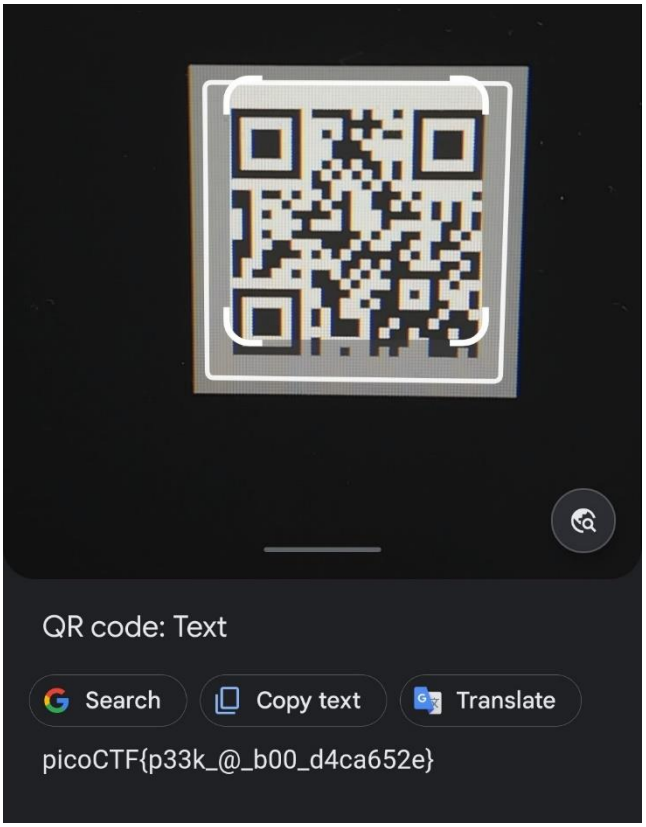
Instance error. Restart?

Hints

1 2 3

The program will randomly choose a new number each time you connect. You can always try again, but you should start your binary search over from the beginning - try around 500. Can you think of why?

```
prab_rvu-picoctf@webshell:~/home/ctf-player/drop-in$ ./guessing_game.sh
Welcome to the Binary Search Game!
I'm thinking of a number between 1 and 1000.
Enter your guess: 500
Lower! Try again.
Enter your guess: 250
Higher! Try again.
Enter your guess: 375
Lower! Try again.
Enter your guess: 313
Higher! Try again.
Enter your guess: 344
Lower! Try again.
Enter your guess: 328
Lower! Try again.
Enter your guess: 320
Lower! Try again.
Enter your guess: 323
Lower! Try again.
Enter your guess: 316
Higher! Try again.
Enter your guess: 318
Congratulations! You guessed the correct number: 318
cat: /challenge/metadata.json: No such file or directory
Here's your flag:
prab_rvu-picoctf@webshell:~/home/ctf-player/drop-in$
```



Unminify

Easy | Web Exploitation | picoCTF 2024 | obfuscation | browser_webshell_solvable | minification

AUTHOR: JEFFERY JOHN

Description

I don't like scrolling down to read the code of my website, so I've squished it. As a bonus, my pages load faster!

Browse here, and find the flag!

This challenge launches an instance on demand.

Its current status is: RUNNING

Instance Time Remaining: 29:48

Restart Instance

re view-source:titan.picoctf.net:54660

```
>If you're reading this, your browser has succesfully received the flag.</p><p class="picoCTF{pr3tty_c0d3_d9c45a0b}"></p><p
```

heap 3

Medium | Binary Exploitation | picoCTF 2024 | browser_webshell_solvable | heap

AUTHOR: ABRXS

Description

This program mishandles memory. Can you exploit it to get the flag?

Download the binary here.

Download the source here.

Connect with the challenge instance here:

`nc tethys.picoctf.net 51837`

This challenge launches an instance on demand.

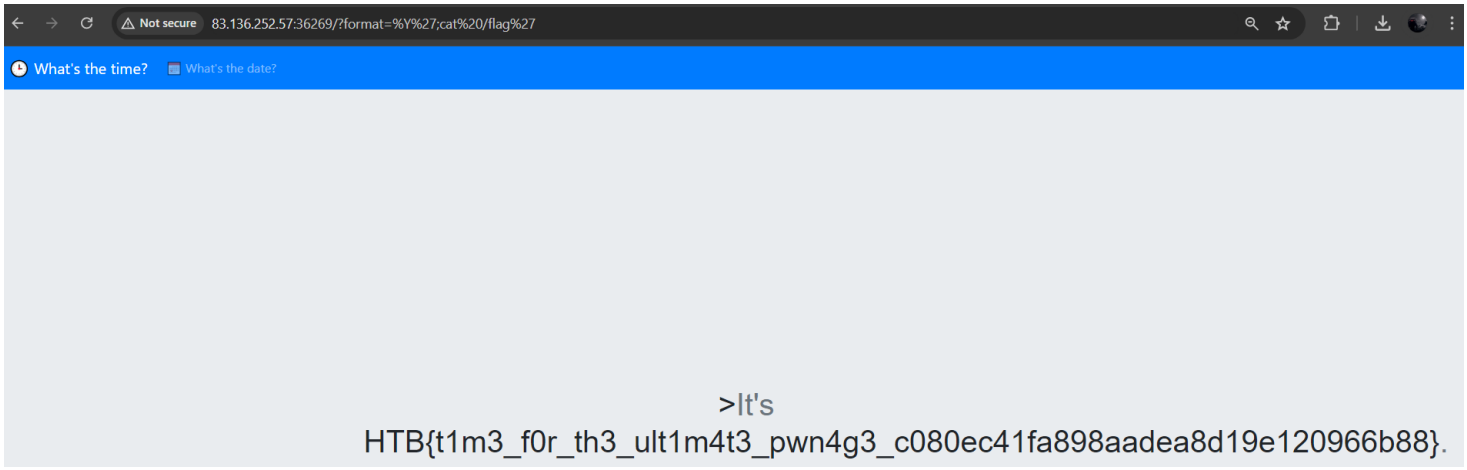
Its current status is: RUNNING

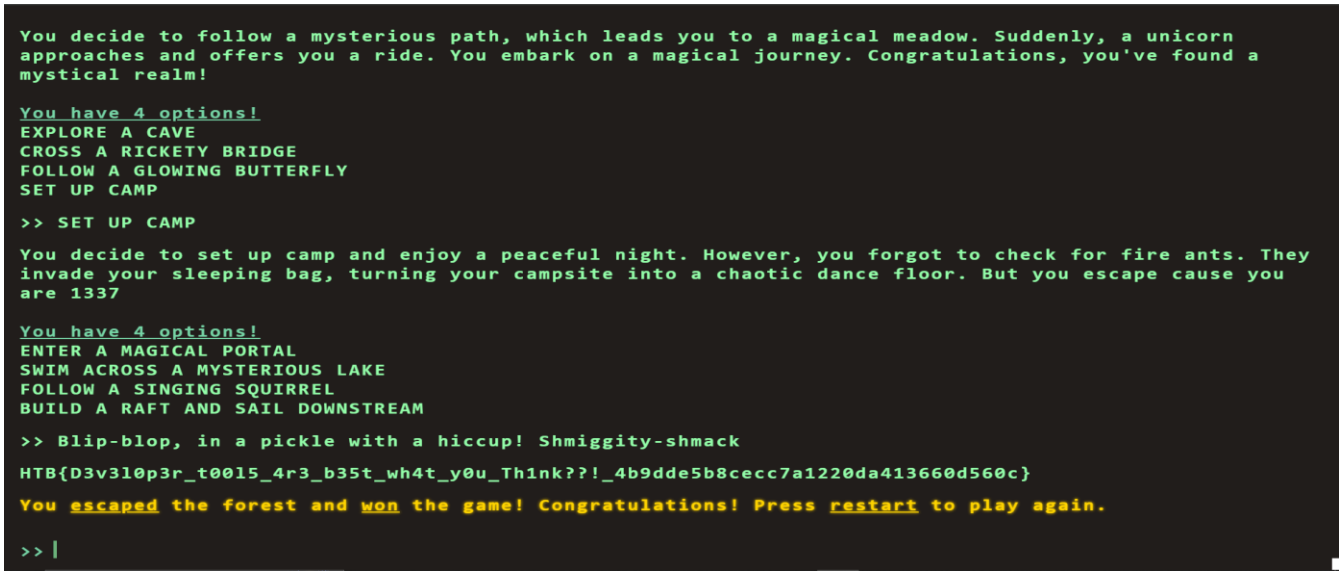
Instance Time Remaining: 29:50

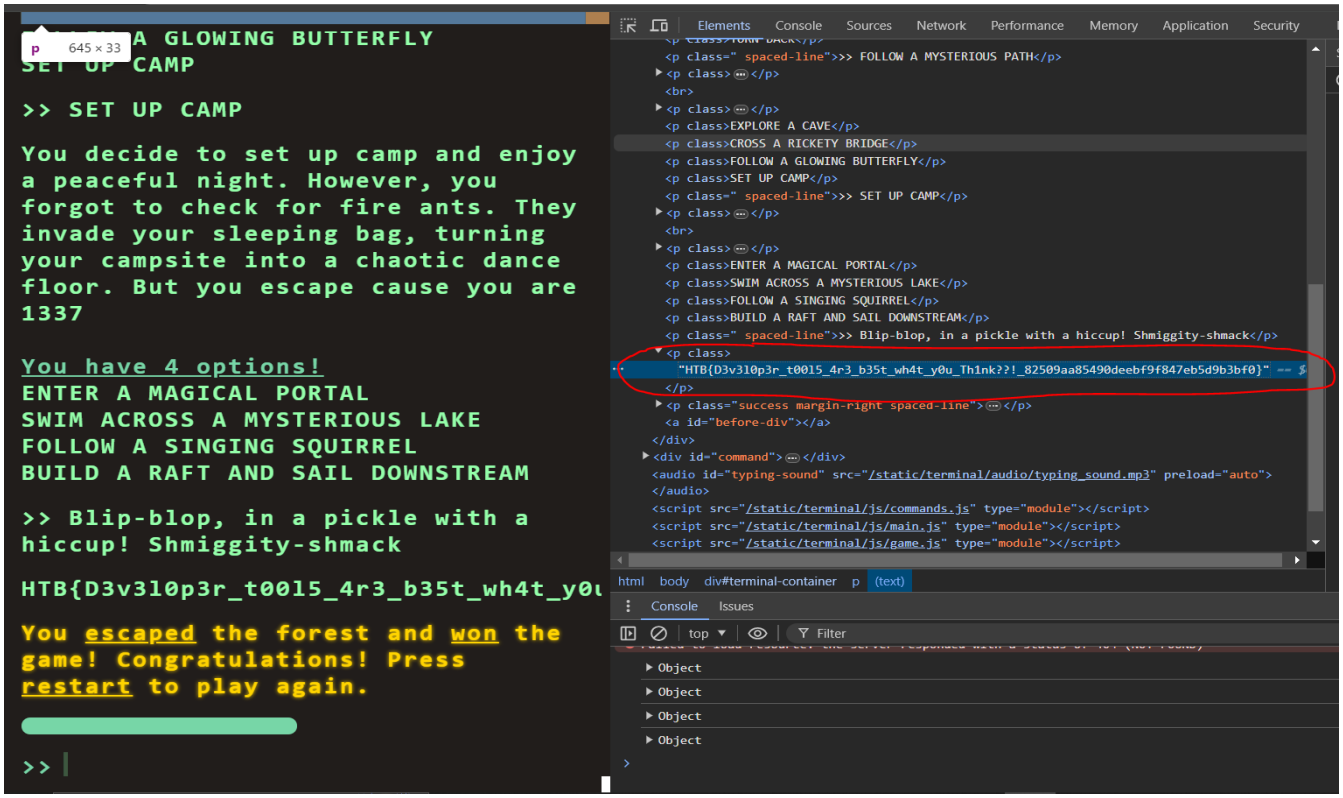
Restart Instance

Hints

```
[*]   0x9592ce  ->   12pico
+-------------+-----------+

1. Print Heap
2. Allocate object
3. Print x->flag
4. Check for win
5. Free x
6. Exit

Enter your choice: 2
Size of object allocation: 36
Data for flag: qwertyuiopasdfghjklzxcvbnm1234pico

1. Print Heap
2. Allocate object
3. Print x->flag
4. Check for win
5. Free x
6. Exit

Enter your choice: 1
[*]   Address   ->   Value
+-------------+-----------+
[*]   0x9592ce  ->   pico
+-------------+-----------+

1. Print Heap
2. Allocate object
3. Print x->flag
4. Check for win
5. Free x
6. Exit

Enter your choice: 4
YOU WIN!!11!!
picoCTF{now_thats_free_real_estate_f8fb9f96}
```


Not secure
83.136.252.57:36269/?format=%Y%27;cat%20/flag%27
What's the time?
What's the date?
>It's
HTB{t1m3_f0r_th3_ult1m4t3_pwn4g3_c080ec41fa898aadea8d19e120966b88}.


You decide to follow a mysterious path, which leads you to a magical meadow. Suddenly, a unicorn approaches and offers you a ride. You embark on a magical journey. Congratulations, you've found a mystical realm!
You have 4 options!
EXPLORE A CAVE
CROSS A RICKETY BRIDGE
FOLLOW A GLOWING BUTTERFLY
SET UP CAMP
>> SET UP CAMP
You decide to set up camp and enjoy a peaceful night. However, you forgot to check for fire ants. They invade your sleeping bag, turning your campsite into a chaotic dance floor. But you escape cause you are 1337
You have 4 options!
ENTER A MAGICAL PORTAL
SWIM ACROSS A MYSTERIOUS LAKE
FOLLOW A SINGING SQUIRREL
BUILD A RAFT AND SAIL DOWNSTREAM
>> Blip-blop, in a pickle with a hiccup! Shmiggity-shmack
HTB{D3v310p3r_t0015_4r3_b35t_wh4t_y0u_Th1nk??!_4b9dde5b8cecc7a1220da413660d560c}
You escaped the forest and won the game! Congratulations! Press restart to play again.
>>


p 645 × 33
A GLOWING BUTTERFLY
CAMP
>> SET UP CAMP
You decide to set up camp and enjoy a peaceful night. However, you forgot to check for fire ants. They invade your sleeping bag, turning your campsite into a chaotic dance floor. But you escape cause you are 1337
You have 4 options!
ENTER A MAGICAL PORTAL
SWIM ACROSS A MYSTERIOUS LAKE
FOLLOW A SINGING SQUIRREL
BUILD A RAFT AND SAIL DOWNSTREAM
>> Blip-blop, in a pickle with a hiccup! Shmiggity-shmack
HTB{D3v310p3r_t0015_4r3_b35t_wh4t_y0u
You escaped the forest and won the game! Congratulations! Press restart to play again.
>>
Elements
Console
Sources
Network
Performance
Memory
Application
Security
>>> FOLLOW A MYSTERIOUS PATH
<p class>EXPLORE A CAVE
<p class>CROSS A RICKETY BRIDGE
<p class>FOLLOW A GLOWING BUTTERFLY
<p class>SET UP CAMP
>>> SET UP CAMP
<p class>ENTER A MAGICAL PORTAL
<p class>SWIM ACROSS A MYSTERIOUS LAKE
<p class>FOLLOW A SINGING SQUIRREL
<p class>BUILD A RAFT AND SAIL DOWNSTREAM
>>> Blip-blop, in a pickle with a hiccup! Shmiggity-shmack
"HTB{D3v310p3r_t0015_4r3_b35t_wh4t_y0u_Th1nk??!_82509aa85490deebf9f847eb5d9b3bf0}"

<audio id="typing-sound" src="/static/terminal/audio/typing_sound.mp3" preload="auto">
<script src="/static/terminal/js/commands.js" type="module"></script>
<script src="/static/terminal/js/main.js" type="module"></script>
<script src="/static/terminal/js/game.js" type="module"></script>
html body div#terminal-container p (text)
Console
Issues
top
Filter
Object
Object
Object
Object

Internship Journal

Sl.No	Date	Content learned
1.	**28-06-2024**	**Started Beginner course-1** Intro to cyber security
2.	**29-06**	Course-1
3.	**30-06**	Course-1
4.	**1-07**	**Completed Beginner course-1** **Started Beginner course-2** Cyber security: Endpoint defense
5.	**2-07**	**Started Beginner course-3** Cyber security and hacker tactics awareness course
6.	**3-07**	**Completed Intermediate course-1** OWASP Top 10: A1 Injection
7.	**4-07**	Course-3 (continuation). Installed kali linux on USB live boot option.
8.	**5-07**	Course-3 (continuation).
9.	**6-07**	Completed course-3
10.	**8-07**	**Started Intermediate course-2** CompTIA Cybersecurity Analyst+: Malware
11.	**9-07**	**Completed Intermediate course-3** Capture the flag preparation.
12.	**10-07**	**Youtube videos for CTF:** tryhackme RootMe Walkthrough, RootMe CTF | TryHackMe | Nmap, Gobuster & Reverse Shell Guide
13.	**11-07**	Started CTF's at **hackthebox.com** **TimeKORP CTF** captured
14.	**12-07**	**Flagcommand** CTF captured. Attempted **Labyrinth linguist.** Too difficult.

15.	**13-07**	Started Picoctf challenges and Tutorials. More research on CTF's.
16.	**14-07**	Picoctf easy challenge: Verify, Heap 0.
17.	**15-07**	Picoctf easy challenges: QR ctf, Binary search
18.	**17-07**	Pico ctf medium: Heap1, Heap 2 CTFs
19.	**20-07**	Pico CTF Medium CTFs: Heap 3, Weirdsnake