SCIENCE AND TECHNOLOGY COUNCIL
IIT (BHU) VARANASI

13th
INTER IIT
TECH MEET

IIT BOMBAY

- Cybersecurity
- Low-prep Event

13th
INTER IIT
TECH MEET

SCIENCE AND TECHNOLOGY COUNCIL
IIT (BHU) VARANASI

Cybersecurity Low-prep event

In this event you will be given known real life vulnerabilities and your task is to stimulate the environment and reproduce the vulnerability exploitation. The challenges presented will consist of CVE numbers and you are expected to read and understand the vulnerability before setting up an environment to test and develop a PoC exploit.

The event involves real life exploit development for various commonly used services and tools.

The second part of the event is a theoretical assessment. You are required to present a model for tackling a certain problem within a company.

PROBLEM STATEMENT

CVE-2024-32113 (100 Points)

Bug Overview: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Apache OFBiz.This issue affects Apache OFBiz: before 18.12.13.

13th
INTER IIT
TECH MEET

SCIENCE AND TECHNOLOGY COUNCIL
IIT (BHU) VARANASI

Cybersecurity Low-prep event

Aim:

- Write a working exploit for this CVE.
- Install vulnerable service in a VM/Docker and ensure to meet the conditions so that you can exploit it.
- Run your exploit on the vulnerable service and make a video of it
- Write a brief report about this bug including your exploit code and link for exploit and video proof.

CVE-2020-7245 (100 Points)

Bug Overview: Incorrect username validation in the registration process of CTFd v2.0.0 - v2.2.2 allows an attacker to take over an arbitrary account if the username is known and emails are enabled on the CTFd instance.

Aim:

- Write a working exploit for this CVE.
- Install vulnerable service in a VM and ensure to meet the conditions so that you can exploit it.
- Run your exploit on the vulnerable service and make a video of it
- Write a brief report about this bug including your exploit code and link for exploit and video proof.

13th
INTER IIT
TECH MEET

SCIENCE AND TECHNOLOGY COUNCIL
IIT (BHU) VARANASI

Cybersecurity Low-prep event

CVE-2019-0217 (100 Points)

Bug Overview: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

Aim:

- Write a working exploit for this CVE.
- Install vulnerable service in a VM/Docker and ensure to meet the conditions so that you can exploit it.
- Run your exploit on the vulnerable service and make a video of it
- Write a brief report about this bug including your exploit code and link for exploit and video proof.

CVE-2016-3841 (100 Points)

Bug Overview: The IPv6 stack in the Linux kernel before 4.3.3 mishandles options data, which allows local users to gain privileges or cause a denial of service (use-after-free and system crash) via a crafted sendmsg system call.

13th
INTER IIT
TECH MEET

SCIENCE AND TECHNOLOGY COUNCIL
IIT (BHU) VARANASI

Cybersecurity Low-prep event

- **Aim**:
  - Write a working exploit for this CVE.
  - Install vulnerable service in a VM and ensure to meet the conditions so that you can exploit it.
  - Run your exploit on the vulnerable service and make a video of it
  - Write a brief report about this bug including your exploit code and link for exploit and video proof.

CVE-2020-9484 (100 Points)

Bug Overview: Apache Tomcat versions 10.0.0-M1 to 10.0.0-M4, 9.0.0.M1 to 9.0.34, 8.5.0 to 8.5.54 and 7.0.0 to 7.0.103 are vulnerable to Remote Code Execution (RCE).

Aim:

- Write a working exploit for this CVE.
- Install vulnerable service in a VM/Docker and ensure to meet the conditions so that you can exploit it.
- Run your exploit on the vulnerable service and make a video of it
- Write a brief report about this bug including your exploit code and link for exploit and video proof.

13th
INTER IIT
TECH MEET

SCIENCE AND TECHNOLOGY COUNCIL
IIT (BHU) VARANASI

Cybersecurity Low-prep event

PART 2 – AUTOMATING CYBER SECURITY AUDITING (200 POINTS)

Design and architect a system to automate the task of cybersecurity auditing. Explicitly state the technical requirements for your model. Prepare a report and presentation for the same.

RULES

1. The participation is individual.
2. Sharing of solutions or clues is not allowed. Doing so will result in disqualification.
3. Participants are encouraged not to copy exploits from the internet but use them as a reference. More unique exploits will be scored more.
4. No solution will be accepted after the mentioned deadline.
5. The duration of the event is 10 days.

13th
INTER IIT
TECH MEET

SCIENCE AND TECHNOLOGY COUNCIL
IIT (BHU) VARANASI

Cybersecurity Low-prep event

SUBMISSION

The videos, report and exploit code should be stored in Google Drive and shareable link should be uploaded in this form

↗ SUBMIT HERE

CONTACT

Reach out for any queries!
Yuval Goyal - 9465973007

RESOURCES

1. Web Based Vulnerabilities - https://portswigger.net/web-security
2. Binary Exploitation - https://youtube.com/playlist?list=PLhixgUqwRTjxglIswKp9mpkfPNfHkzyeN
3. Exploit Development - https://pwn.college/