|| 26- 28th March, 2021 ||

INTER IIT TECH MEET'21

IIT Guwahati

LOW PREP EVENT

(150 Points)

SAPTANG LAB'S NETWORK SECURITY HACKATHON

We are interested in offering the participants known real-world vulnerabilities and task them with working on the vulnerability to simulate the environment and reproduce the vulnerability exploitation. The challenges presented to the team of participants will consist of CVE numbers and the team is expected to read and understand the vulnerability before setting up an environment to test and develop a PoC exploit.

This is NOT a Capture the Flag event (CTF's). This event involves real-life exploit development for web services like Apache and Nginx.

SAPTANG LABS

PROBLEM STATEMENTS:

1. CVE-2014-0226 (100 points)

- **Bug Overview**: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

- **Aim**: Write a working exploit for this CVE.
- Install vulnerable service in a VM/Docker and ensure to meet the condition 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.

2. CVE-2017-12615 (100 points)

- **Bug Overview**: When running Apache Tomcat 7.0.0 to 7.0.79 on Windows with HTTP PUTs enabled (e.g. via setting the read-only initialisation parameter of the Default to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server. That could lead to remote code execution on the server.

- **Aim**: Write a working exploit for this CVE by which you can achieve RCE on local VM/Docker.
- Install vulnerable service in a VM/Docker and ensure to meet the condition 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.

SAPTANG
LABS

3. CVE-2020-0609 and CVE-2020-0610 (200 points)

- **Bug Overview**: Specially crafted requests lead to DoS/RCE without any user interaction on Windows RDP service.

- **Aim**: Setup a local Vm in which to install vulnerable windows RDP service and write an exploit that could lead to DoS/RCE on the local VM server.
- Write a brief report about this bug including your exploit code and link for exploit and Video proof.

4. CVE-2018-1335 (100 points)

- **Bug Overview**: This bug leads to command injection vulnerability in Apache Tika -server < 1.18 and uses Cscript.exe to execute Jscript or VBS code and run arbitrary commands.

- **Aim**: Write a working exploit for this CVE by which you can achieve RCE on the local VM.
- Install vulnerable service in a VM and ensure to meet the condition 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.

5. CVE-2019-0232 (100 points)

- **Bug Overview**: Apache Tomcat has a vulnerability in the CGI Servlet which can be exploited to achieve remote code execution (RCE). This is only exploitable when running on Windows in a non-default configuration in conjunction with batch files.

- **Aim**: Write a working exploit by which you can achieve RCE on the local VM.
- Install vulnerable service in a VM and ensure to meet the condition 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.

RULES:

1. The maximum number of participants allowed in a team is 5.
2. Sharing of solutions or clues is not allowed and any team indulging in such activity will be disqualified.
3. Participating teams are encouraged not to copy exploits from the internet but to use them as references.
4. No solutions will be accepted after the mentioned deadline.
5. Each of the challenges will carry 100 or 200 points based on the difficulty level.
6. The duration of the contest is 72 hours.

SUBMISSION:

The submission of a solution for a challenge should include a very brief report including links for exploit code hosted on Github/Bitbucket along with a short video demonstrating the triggering of the vulnerability and the PoC code.

EVENT TIMELINE:

1. Submission of Participant details by the Participating IITs: **23rd March 11:59 PM.**
2. Release of the Problem Statement: 24th March 12:01 AM
3. Deadline for the submission: 26th March 11:59 PM
4. Results Announcement: 28th March 3 PM

A maximum of 5 participants (per team) shall be awarded a participation /merit certificate.

SAPTANG
LABS