**NAME :** SHAIK.M.BILALDEEN

**COLLEGE :** ANNAMACHARYA INSTITUTE OF TECHNOLOGY AND SCIENCES, TIRUPATI.

**BRANCH :** E.C.E

**ASSIGNMENT-1**

**1**

**WEBSITE :** [testphp.vulnweb.com](http://www.google.com)

**IP ADDRES**

**IP V4 :** 44.228.249.3

**GENERAL INFORMATION**

**Hostname :** ec2-44-228-249-3.us-west-2.compute.amazonaws.com

**Domains :** AMAZONAWS.COM

**Cloud Provider :** Amazon

**Cloud Region :** us-west-2

**Cloud Service :** EC2

**Country :** United States

**City :** Boardman

**Organization :** Amazon.com, Inc.

**ISP :** Amazon.com, Inc.

**ASN :** AS16509

**SECURITY CONTACT**

**\*\*Didn’t provided\*\***

**PORTS OPENED**

**Port 80(HTTP) :** Hyper Text Transfer Protocol

Port 80 is the port number assigned to commonly used internet communication protocol, Hypertext Transfer Protocol (HTTP). It is the default [network port](https://www.techopedia.com/definition/24717/network-port) used to send and receive unencrypted web pages.

**Vulnerability**: there the transfer of data will be not in secure and it can be easily creates a security threat.

**Vulnerability for Ip Address** : 44.228.249.3

**A)** **CVE-2023-44487:** the http protocol can be used as a tool for the denial od service attack which can able to lead upto session hijacking scenario.

**B) CVE-2021-3618:** There might be chance of session hijacking, accessing resource via authentication, authorization, and availability of the resources by performing MitM attacks, session hijacking, DoS, DDos, etc. through the ALPCCA(Application Layer Protocol Control Confusion Attack) by accessing the TCP/IP layer.

**C) CVE-2021-23017:** refers to the overwrite of the information or instruction provided upto 1 Byte in order to broke in to the website and make it to be crash or other potential impact, by forging UDP packets from the DNS server.

**2**

**WEBSITE :** [www.google.com](http://www.google.com)

**IP ADDRESSES**

**IP V4 :** 142.251.46.228

**IP V6 :** 2607:f8b0:4005:811::2004

**GENERAL INFORMATION**

**Hostname :** sfo03s27-in-f4.1e100.net

**Domains :**1e100.NET

**Country :** United States

**City :** San Joe

**Organization :** Google LLC

**ISP :** Google LLC

**ASN :** AS15169

**SECURITY CONTACT**

**Contact :** security@google.com

**Encryption :** https://services.google.com/corporate/publickey.txt

**Policy :** https://g.co/vrp

**Hiring :** https://g.co/SecurityPrivacyEngJobs

**PORTS OPENED**

**Port 80(HTTP) :** Hyper Text Transfer Protocol

Port 80 is the port number assigned to commonly used internet communication protocol, Hypertext Transfer Protocol (HTTP). It is the default [network port](https://www.techopedia.com/definition/24717/network-port) used to send and receive unencrypted web pages.

**Vulnerability**: there the transfer of data will be not in secure

**Port 443(HTTPS)** : Hyper Text Transfer Protocol Secured

Port 443 is a virtual point ⁠through which data transmissions are sent and received. This communication endpoint is used by transport layer protocols, like the [Transmission Control Protocol (TCP)](https://nordvpn.com/blog/tcp-or-udp-which-is-better/), to divert different types of web traffic to its destination.

**Vulnerability**: there the files will be secure in the most of the case but if incase the protocol is hacked down then then the data will be stolen

**Vulnerability for google :** “NONE”

**Vulnerability for Ip Address** : 184.168.115.31

**A)** **CVE-2023-51385 :** Due to SQL Injection the data might me have a sub module and accesses the meta character of the host having the host name

**B) CVE-2023-51384 :** Its an SSH based vulnerability in which the private keys plays vital role

**C) CVE-2023-48795 :** The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted.

**D) CVE-2023-38408 :** has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system.

**E) CVE-2021-36368 :** Sniffing of the website been takes place and the password is being compromised and the credentials will used for further attacks.