



Scan With NMAP:

Comandos `nmap -sV 192.168.1.33` (IP DEBIAN) --> comando utilizado para escaneo de puertos y versiones.

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)

CVE-2023-38408 es una vulnerabilidad de seguridad que afecta a SSH, relacionada con la ejecución remota de código(RCE)

<https://vulners.com/cve/CVE-2023-38408>

21/tcp open FTP ProFTPD 1.3.1

CVE-2019-19270-esta vulnerabilidad permite a un atacante realizar un ataque de cross-site scripting(XSS) , un atacante puede inyectar código malicioso JavaScript en ciertos campos de entrada, como el campo de nombre de usuario, este código se ejecutará en el navegador de otros usuarios cuando visualicen los datos comprometidos, lo que puede permitir el robo de cookies, la suplantación de identidad o la ejecución de acciones maliciosas.

8443/tcp open ssl/http nginx 1.4.0

CVE-2017-20005 es una vulnerabilidad que afecta a wordpress, CROSS-SITE SCRIPTING (XSS), permite a un atacante inyectar código javascript en ciertos campos de entrada de wordpress, el código se almacena en la base de datos y se ejecuta en el navegador de otros usuarios cuando visualizan el contenido afectadoo, robo de cookies, suplantación de identidad o la ejecución de acciones maliciosas en nombre de la víctima.