ARENA SECURITY

EXECUTIVE SUMMARY

SYNOPSIS

Fahad Ahmed was asked to evaluate of the given IP address's (138.128.180.106) security by engaging in a 1-day penetration test that was conducted on September 26th, 2021. The goal of the "pentest" is to act as a threat-actor by performing cyber attacks against 138.128.180.106 corporate server. This will serve to discover any present vulnerabilities that could result in a breach and be leveraged to access to the given IP address's sensitive data by a real-world attacker. All issues discovered by me are achieved and verified through network evaluation, system vulnerability scanning and assessment, and both automated and manual exploitation (where applicable) of found vulnerabilities.

FINDING OVERVIEW

While conducting the external penetration test, there were several critical vulnerabilities discovered in the 138.128.180.106 network. I was able to gain full administrative privilege to the corporate server. This was possible due to a vulnerable web-application, which led to remote system access, then full administrative control was gained through improperly set permissions to a critical system file. A brief technical overview is listed below:

Target: performing a SQL Injection attack against indianfriedchicken, password was managed 'heera0518' found at URL: https://indianfriedchicken.net/products.php?cat=14 , granting me to access as an admin user Once access was established, privilege escalation was possible in other links using shell scripts; allowing the creation a new administrative user to the server.In other cases LFI (local file inclusion) was possible using "/etc/password" giving me the full root information.

RECOMMENDATION

To increase the security posture of 138.128.180.106, I recommend the following mitigations or remediations be performed:

Implement Prepared Statements with Parameterised Queries
Injection attacks remains the most common attacks leveraged against web applications. One of the most effective mitigation strategies for preventing SQL Injection attacks is the implementation of Prepared Statements with Parameterised Queries.

Implement User Input White listing
Another very useful mitigation against SQL Injection attacks is to validate the supplied user input. One should never trust that user input is safe and therefore should be checked for a set of disallowed characters.

Require Secure Coding Training for Developers
Developers are on the frontlines of security for any organisation and should be prepared to be the first line of defence. Training in secure coding techniques and practices will help ensure that your organisations applications are developed using the most secure code possible, thus reducing your attack surface and lowering your overall risk.

Implement Network Security Devices
Putting up a few fences can go along way to increasing your security posture and is a key piece of the Defense-in-Depth puzzle. By adding a Web Application Firewall (WAF), Next-Gen Firewall, and/or Intrusion Detection/Prevention System, you can significantly increase your ability to stop intruders from accessing your systems.

Perform Permissions Audit of System Files.
Permissions misconfigurations area common occurrence and can be leveraged to gain full administrative. Performing a baseline and then scheduled audits of the permissions to system files can ensure those files and their permissions are following security best-practices. Service accounts should not be owners of sensitive operating system files that control local user-accounts.

SEVERITY SCALE

CRITICAL Severity Issue: Poses immediate danger to systems, network, or data security and should be addressed as soon as possible.

HIGH Severity Issue: Poses significant danger to systems, network, and/or data security. Exploitation commonly requires some advanced knowledge, training, skill, and/or tools. Issue(s) should be addressed promptly.

MEDIUM Severity Issue: Vulnerabilities should be addressed in a timely manner. Exploitation is usually more dificult to achieve and requires special knowledge or access.

LOW Severity Issue: Danger of exploitation is unlikely as vulnerabilities offer little to no opportunity to compromise system, network, or data security. Can be handled as time permits.

INFORMATIONAL Issue: Meant to increase client's knowledge. Likely no actual threat.

FINAL REPORT

METHODOLOGY

My Testing methods that are widely adopted in the cyber security assessment industry. This includes 3 phases: **Information Gathering**, **Vulnerability Assessment**, **Exploitation**, and **Reporting**.

INFORMATION GATHERING

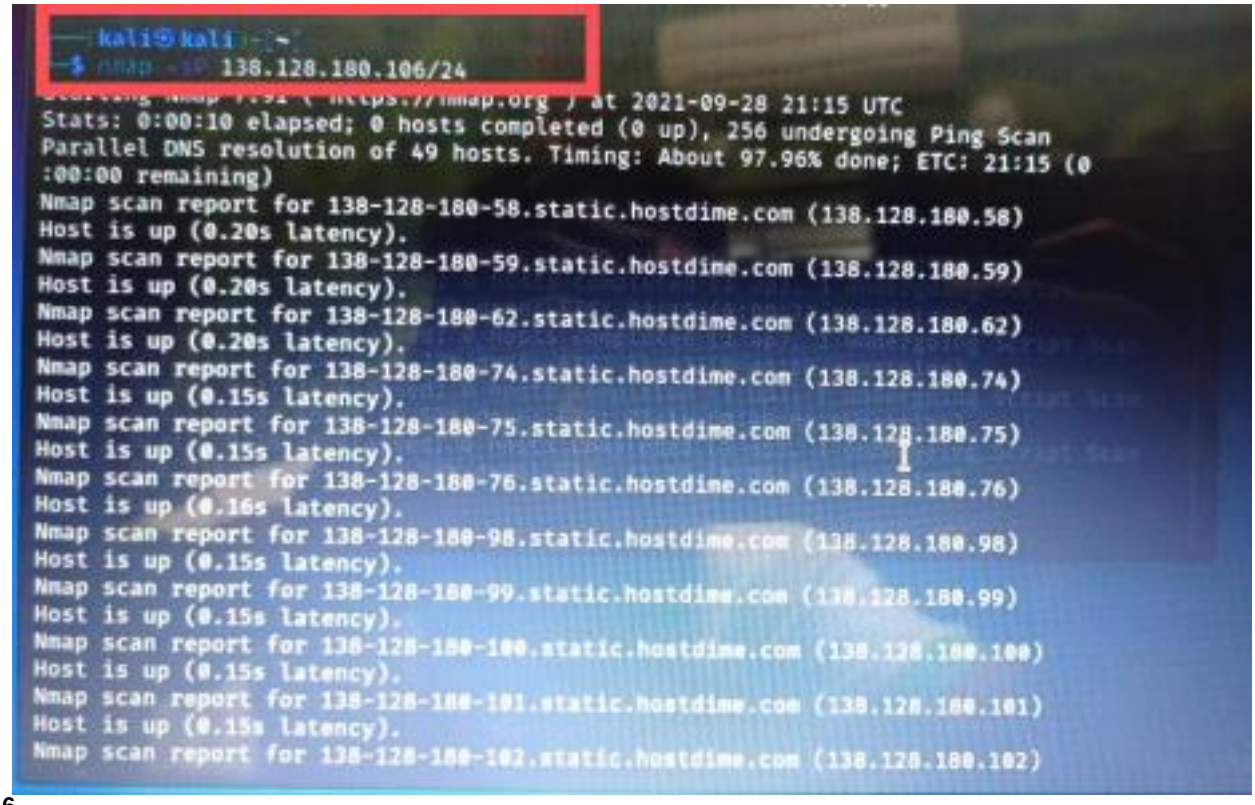
Hostname: ind.thecolourmoon.com
IP Address: 138.128.180.106

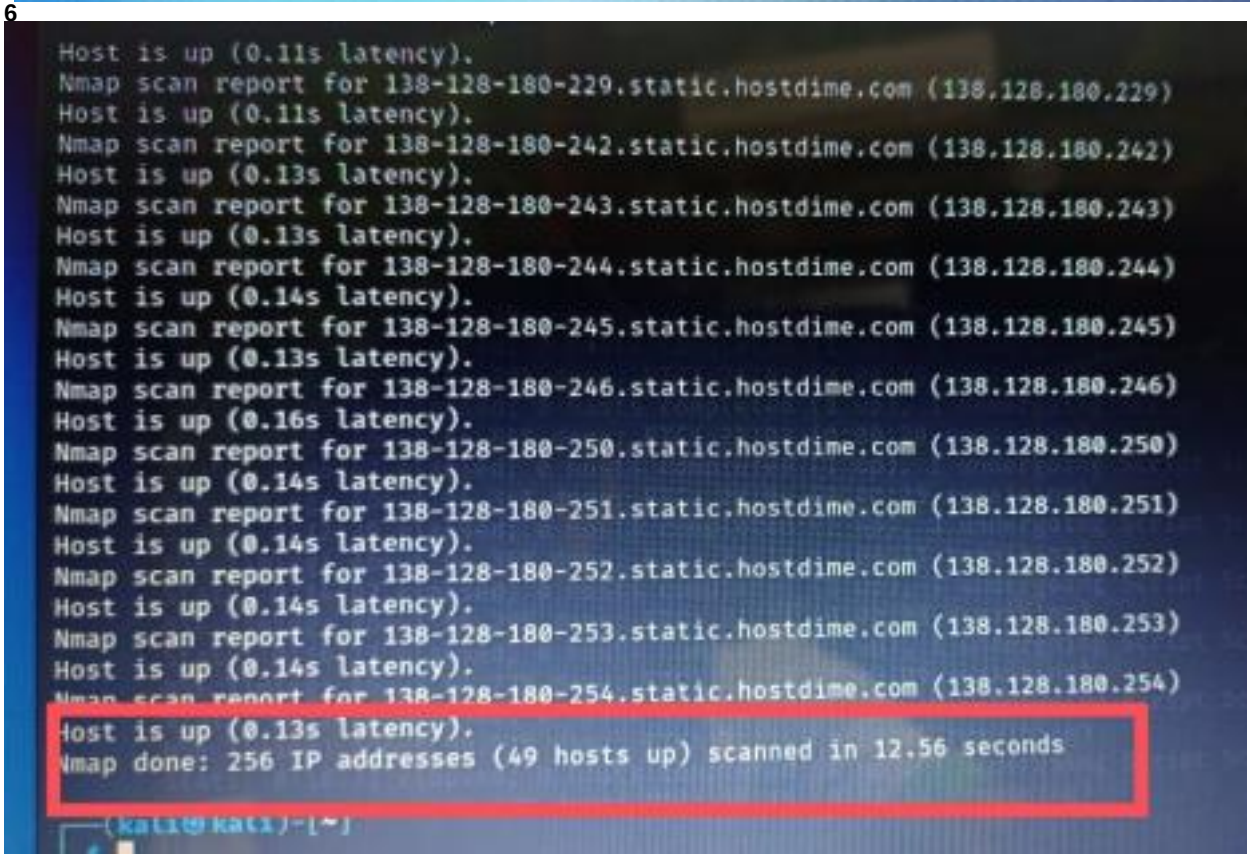
A total of 941 domains was hosted by the Given IP address shows on yougetsignal.com, Here are the Names:

Found **71** domains hosted on the same web server as indianfriedchicken.net (138.128.180.106).

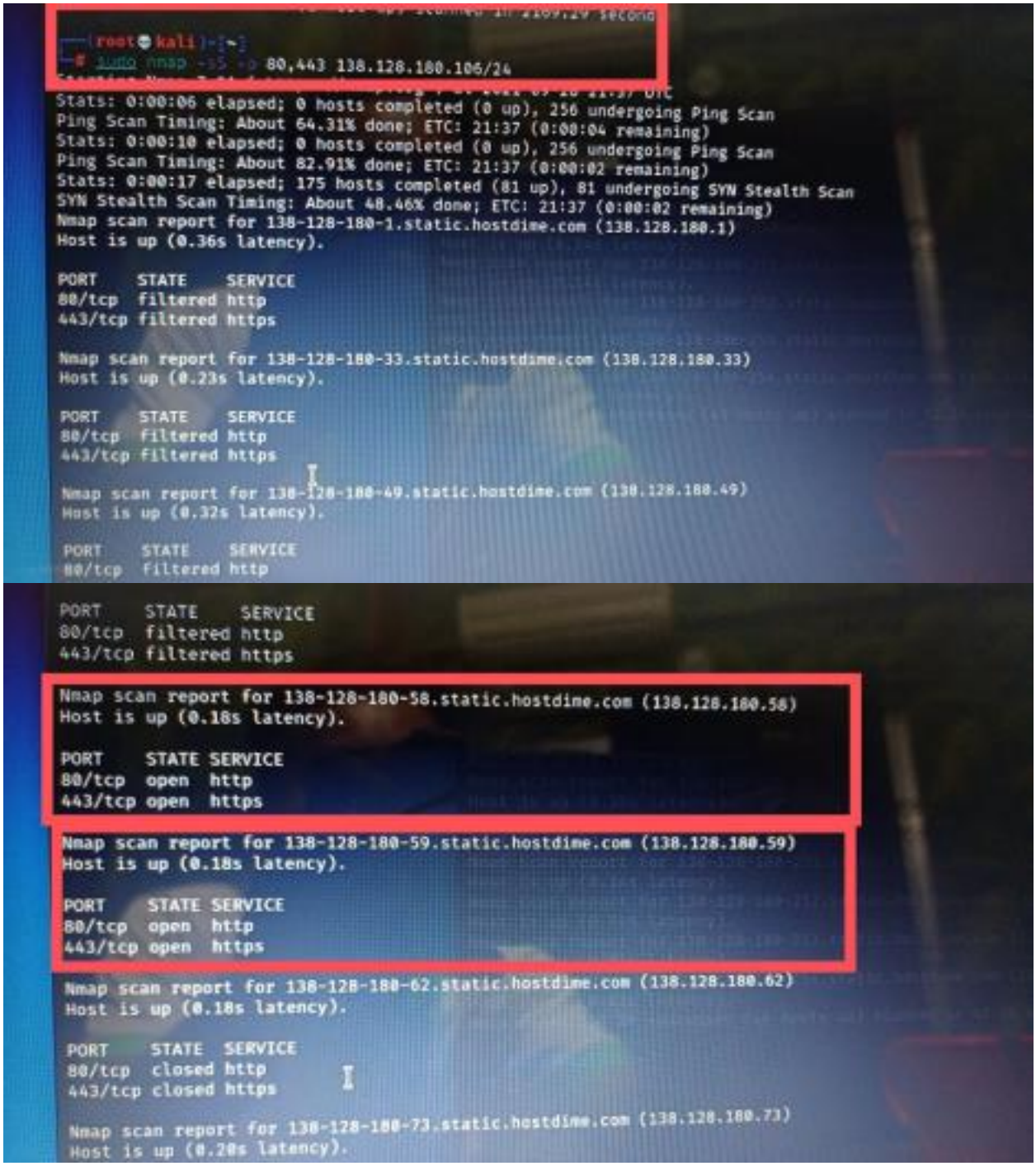
aarontech.in
agnikulakshathriya.com
andhrainfoservices.com
balajihighfields.in
bhavarajufoundation.org
colourmoon.in
doctorspages.in
dreamwardrobe.in
gecgudlavalleru.ac.in
hitechics.com
ind.thecolourmoon.com
indianfriedchicken.net
jpabs.org
leeleather.net
multiplystore.com
myairlinenews.com
payhub.uttamseva.com
ramanathsecondaryschool.com
reddysvaradhi.com
savetaxfiling.com
solutionvia.com
sunkristpublishing.com
thekeycorner.com
triparaku.com
viharifoods.com
visioncraft.in
weaverswardrobe.com
www.aaronindia.in
www.amigosfresh.com
www.ardeegroup.com
www.bhavarajufoundation.org
www.indiabix.com
www.jntc.in
www.musculoskeletalsociety.in
www.rcreddyiasstudycircle.com
www.thekeycorner.com
actimusbio.com
amigosfresh.com
appleischool.edu.in
bestnsetips.com
capitalhospitals.in
dhruvtax.com
doorstepgrocerys.com
edu.pharmadhunia.com
harshaenterprises.in
hplservices.in
indiabix.com
jeab.scienceresearchlibrary.com
kfresh.in
mail.indiabix.com
musculoskeletalsociety.in
niosrcvizag.ac.in
pcmbtimes.com
rcwing.in
saptestingguru.in
skillsnet.info
sske.in
thecolormoon.com
tonerandinkjetstore.com
tsrtbkcollege.com
visakhavalleyschool.com
vizagwaterpurifiers.com
wjpsonline.org
www.aarontech.in
www.appleischool.edu.in
www.bharatelevators.co.in
www.ijpda.com
www.indianfriedchicken.net
www.mightyperfect.in
www.myairlinenews.com
www.rvhc.in

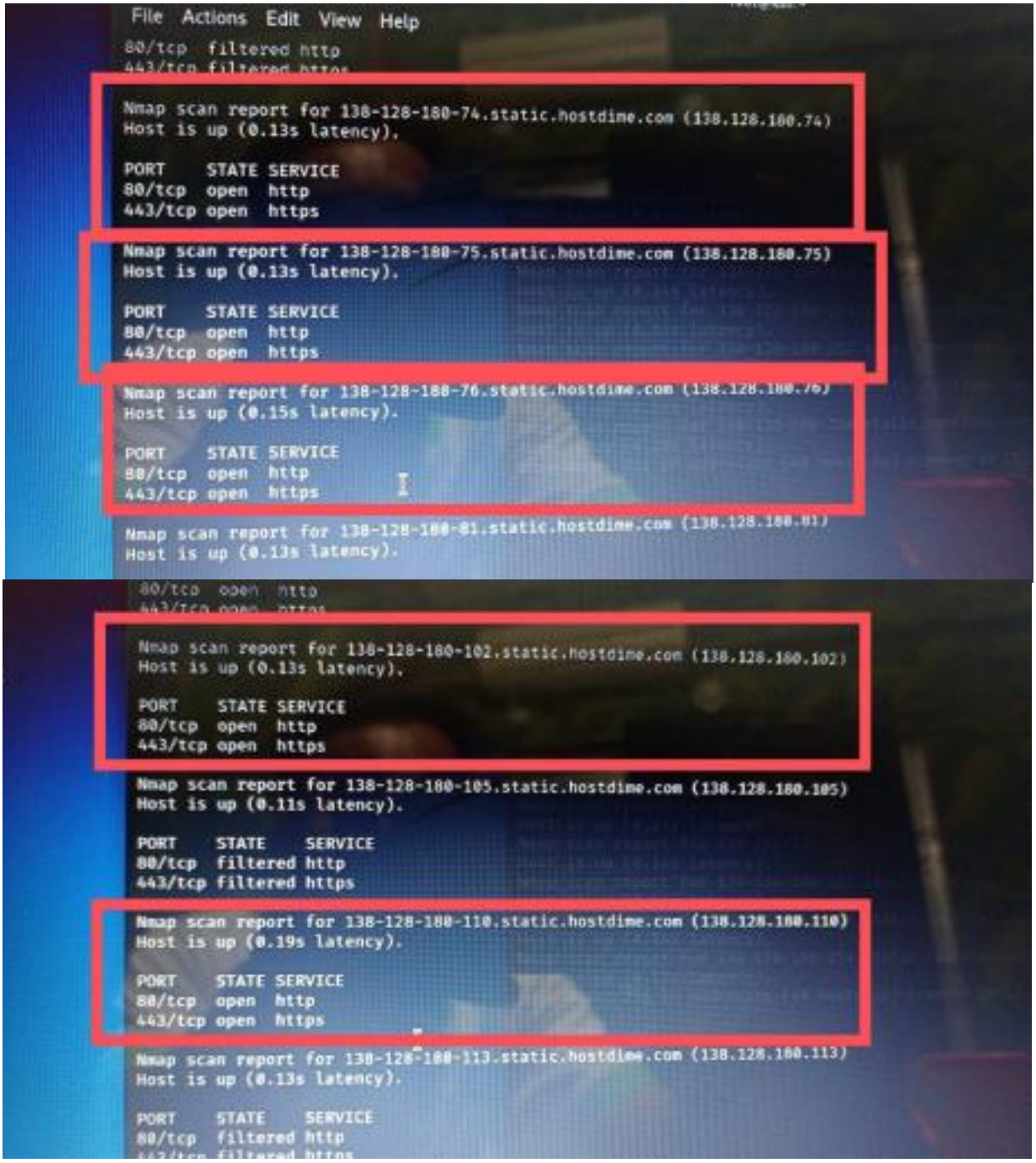
While using Nmap (used for finding network vulnerability and more), of cmd " nmap -sP 138.128.180.106/24 ", I found 256 IP addresses were their and 49hosts were up. Below is the screenshot of the scanned networks.





For Finding open ports I used nmap cmd like ‘sudo nmap -sS -p 80, 443 138.128.180.106/24’ (sS represents stealthy), below is the screenshot of open ports that are vulnerable for the server.





HIGH Severity Issue

VULNERABILITY ASSESSMENT

The vulnerability assessment is done in an attempt to verify that a vulnerability exists that may be exploitable by an attacker. I tested a variety of web application/sites vulnerability Testers/Scanner, such as ***Burp suit, nmap, yougetlink.com, cyberfox browser.*** which were successful at discovering an exploitable vulnerability (SQL Injection), (LFI attacks), (RCE attacks),(XSS), (SESSION HIJACKING), (ADMIN LOGIN BYPASS). In addition, the manual SQLI was successful with 57% of the domains This vulnerability was then leveraged by me to gain initial system access.

Vulnerability Exploited: SQL Injection

Vulnerability Explanation: SQL injection attacks occur when a web application does not perform any validation against the values received from objects like web forms, user input parameters, cookies, etc., before passing them to SQL queries that are to be executed on a database server. This facilitates a way for an attacker to manipulate the input so that the data is interpreted as a part of the code instead of user supplied data.

CRITICAL Severity Issue

Site link: https://indianfriedchicken.net/products.php?cat=14

HASH DECRYPTED= heera0518

Below is the Screenshot of SQLI using cyberfox browser.

SOME OTHER SITES THAT ARE VULNERABLE TO SQLI:

>>https://musculoskeletalsociety.in/page.php?id=2 **CRITICAL Severity Issue**

>>https://ramanathsecondaryschool.com/photos.php?id=12 **HIGH Severity Issue**

>>https://myairlinenews.com/news.php?id=MTK3 **HIGH Severity Issue**

>>https://aarontech.in/it/enquiry.php?id=1367 **CRITICAL Severity Issue**

>>http://rcwing.in/t-view.php?id=7 **HIGH Severity Issue**

>>https://samarthodisha.com/blockcontent.php?id=13. **MEDIUM Severity Issue** >>

http://leeleather.net/gifts-ideas.php?id=2 **CRITICAL Severity Issue**

>>https://bhavarajufoundation.org/photogallery.php?id=9 **CRITICAL Severity Issue**

>>https://bharatelevators.co.in/service_view.php?id=6 **MEDIUM Severity Issue**: 11

VULNERABILITY IN DETAILS:

>>http://aarontech.in **MEDIUM Severity Issue**

>>http://www.actimusbio.com **MEDIUM Severity Issue**

>>http://agnikulakshatriya.org **MEDIUM Severity Issue**

>>http://amigofresh.com/en/ **MEDIUM Severity Issue**

>>https://andhrainfoservices.com **MEDIUM Severity Issue**

Some of the major vulnerability is giving hacker full access of the server by uploading shell scripts, below are the links that shell scripts can be uploaded

Vulnerability Exploited: SHELL SCRIPTS

Vulnerability Explanation: A shell script is a list of commands in a computer program that is run by the Unix shell which is a command line interpreter. A shell script usually has comments that describe the steps. The different operations performed by shell scripts are program execution, file manipulation and text printing.

>>https://www.rrvhc.in/resume.php **HIGH Severity Issue**

>>https://ardeegroup.com/apply.php?apid=5 **CRITICAL**

Severity Issue >>http://tejahearingclinic.com/careers.php

CRITICAL Severity Issue

>>https://visioncraft.in/careers.php **HIGH Severity Issue**

>>http://www.genfobio.com/careers.php **HIGH Severity**

Issue >>https://www.medlinesmt.com/careers.php

CRITICAL Severity Issu >>

http://www.suryaalliedservices.com/careers **CRITICAL**

Severity Issu

HOUSE CLEANING

During a penetration testing engagement, tools, files, user accounts, etc., are created on the client's system(s) which would compromise the client's security.

Fahad Ahmed is diligent to ensure that no potential security issues are introduced to the given server environment through remnants left on their system(s) after the completion of the engagement, ind.thecolourmoon.com have had all tools, files, user accounts, etc. that were created by Fahad Ahmed testers during the engagement removed.