MADRE JANUS

BUSINESS PROPOSAL

www.madre-janus.com

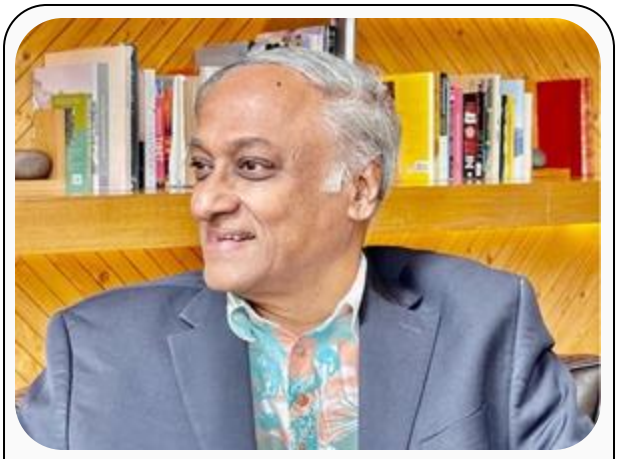
Presented to:

UNIFIED CREDIT SOLUTIONS

Table of Contents

About Us

Mr. Stijo Sebastian
CEO



Prof. Dr. Raghunath
Chairman of the Advisory Board

Vision

- To become the most trusted partner in delivering cutting edge cybersecurity solutions
- Empowering businesses to operate securely, efficiently and confidently in an increasingly digital world.

Mission

- To provide seamless proactive and scalable managed services that leverage Fortinet's industry.
- Leading cybersecurity technologies.
- To ensure organizations of all sizes achieve robust network security, data protection and compliance through tailored solutions and expert support.
- To foster trust and long-term relationships by delivering exceptional services, innovation and value to our clients.
- To continuously enhance our expertise and stay ahead of emerging threats to safeguard our clients digital ecosystem.

VULNERABILITIES IDENTIFIED

Unified Credit Solutions

Scope : group-ucs.com

Gathering Type : Passive (without directly interacting with the target's system)

HTTP Header Analysis

Description :

HTTP header analysis involves examining the metadata (key-value pairs) sent with HTTP requests and responses to understand how the client and server communicate, identify potential issues, and optimize website performance and security.

```
HTTP/1.1 302 Found
Date: Thu, 20 Mar 2025 05:56:29 GMT
Server: Apache
Upgrade: h2,h2c
Connection: Upgrade, Keep-Alive
Location: /404.html
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Content-Length: 0
Keep-Alive: timeout=5, max=75
Content-Type: text/html; charset=UTF-8

HTTP/1.1 200 OK
Date: Thu, 20 Mar 2025 05:56:30 GMT
Server: Apache
Last-Modified: Wed, 01 Jul 2020 09:24:23 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: no-cache, no-store, must-revalidate
Pragma: no-cache
Expires: 0
Content-Length: 4677
Keep-Alive: timeout=5, max=74
Connection: Keep-Alive
Content-Type: text/html
```

fig: 1. Http header details

VULNERABILITIES IDENTIFIED

Unified Credit Solutions

Findings:

Server name disclosure - Server name disclosure in HTTP headers, specifically the "Server" header, revealing information about the web server's software.

Mitigation:

Modify the HTTP headers of the webserver to not disclose detailed information about the underlying web server.

Missing HTTP Header

Description :

HTTP headers are key-value pairs that provide metadata about HTTP requests and responses, enabling communication between clients and servers on the web, including information about content type, caching, and authentication.

Missing Headers	Description	Recommended
Strict-Transport-Security (HSTS)	Ensures HTTPS enforcement and protects against man-in-the-middle (MITM) attacks	Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Content-Type-Options	Prevents MIME-sniffing attacks by enforcing the declared content type.	X-Content-Type-Options: nosniff
X-Frame-Options	Prevents clickjacking attacks by restricting iframe embedding.	X-Frame-Options: DENY
X-XSS-Protection	Helps mitigate reflected cross-site scripting (XSS) attacks.	X-XSS-Protection: 1; mode=block
Content-Security-Policy (CSP)	Prevents XSS and other injection attacks by restricting script execution.	Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'
Secure Flag	The Secure flag in a cookie ensures that the cookie is only sent over HTTPS connections	Ensure that the secure flag is set for cookies containing such sensitive information.

VULNERABILITIES IDENTIFIED

Unified Credit Solutions

Clickjacking or UI Redressing

Description :

Clickjacking is a cyberattack that tricks users into clicking on something other than what they intended.

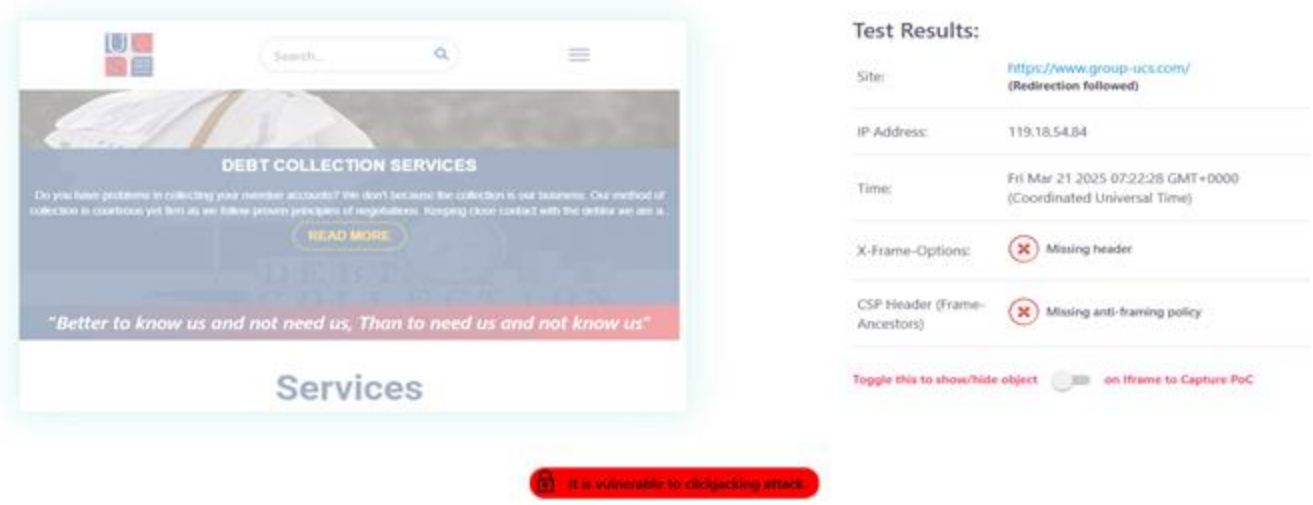


fig: 2. POC of clickjacking attack

URL: https://clickjacker.io/test?url=https://group-ucs.com

Mitigation:

Server-side methods – the most common is X-Frame-Options. Server-side methods are recommended by security experts as an effective way to defend against clickjacking.

VULNERABILITIES IDENTIFIED

Unified Credit Solutions

Domain Reputation

Description :
The domain reputation provides information about a domain's reputation, including whether it has been flagged as malicious by various sources.

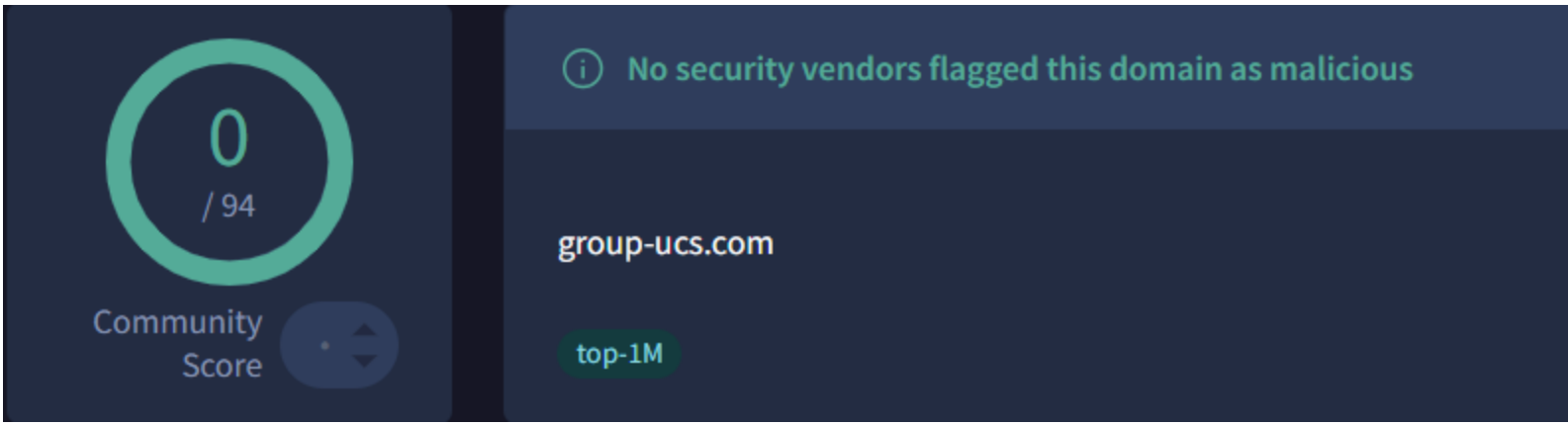


fig: 3. Domain reputation, not marked as suspicious

Findings:
The domain not flagged as malicious.

Subdomain

Description :
A subdomain is a distinct section or part of a website that appears before the main domain name in a URL, like "blog.example.com" where "blog" is the subdomain and "example.com" is the domain.

VULNERABILITIES IDENTIFIED

Unified Credit Solutions

Subdomains (7)

webservicenew.group-ucs.com	0 / 94	180.179.194.238		
cp.group-ucs.com	0 / 94	180.179.194.238		
uat.group-ucs.com	0 / 94	119.18.54.84		
group-ucs.com	0 / 94	119.18.54.84	13.248.196.204	180.179.194.238
webservice.group-ucs.com	0 / 94	180.179.194.238		
mail.group-ucs.com	0 / 94	67.227.236.173		
www.group-ucs.com	0 / 94	119.18.54.84	180.179.194.238	124.153.79.66

fig: 4. Subdomain enumeration

Server IP
119.18.54.84
13.248.196.204
180.179.194.238

Findings:

we were able to identify a subdomain that revealed an accessible UAT (User Acceptance Testing) website.

Mitigation:

it's crucial to restrict access to UAT environments using proper authentication mechanisms and ensure they aren't publicly accessible.

VULNERABILITIES IDENTIFIED

Unified Credit Solutions

fig: 5. Ip address reputation, marked as malicious

As shown in the image above, the IP address '119.18.54.84' associated with the domain has been flagged as malicious by one vendor.

Communicating Files (66)

Scanned	Detections	Type	Name
2025-03-20	28 / 64	PDF	0201b33abe13145f012861e4d0c38523e973888b2d0599f66e9fbdda3b302b83
2022-10-26	0 / 66	Android	046e31ba3bbc3320e609560d6065e6f93c82a45ca284c9f638220d5d6b6e94e7
2024-09-18	0 / 68	Android	22095d1f2121f14455aba53de62e11c840ef10b7c2984beada913fe424fa2cd6
2024-05-17	0 / 68	Android	e739f5f9339a4c3fea72685ac8584347a93a0cde.apk

fig: 6. Communicating files list

The image above illustrates the IP address interacting with multiple files, including APK and PDF files.

VULNERABILITIES IDENTIFIED

Unified Credit Solutions

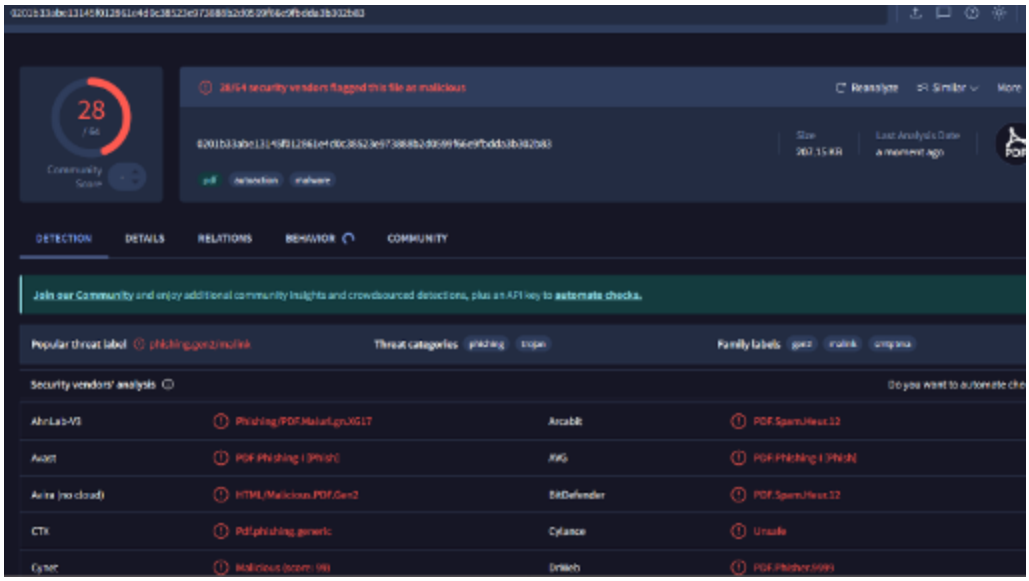


fig: 7. communicating file marked as malicious

As shown in the image above, the PDF file being communicated with has been flagged as malicious by 28 vendors.

Open Ports

An "open port" refers to a network port that is configured to accept incoming connections using protocols like TCP or UDP, allowing communication with services or applications running on that port.

VULNERABILITIES IDENTIFIED

Unified Credit Solutions

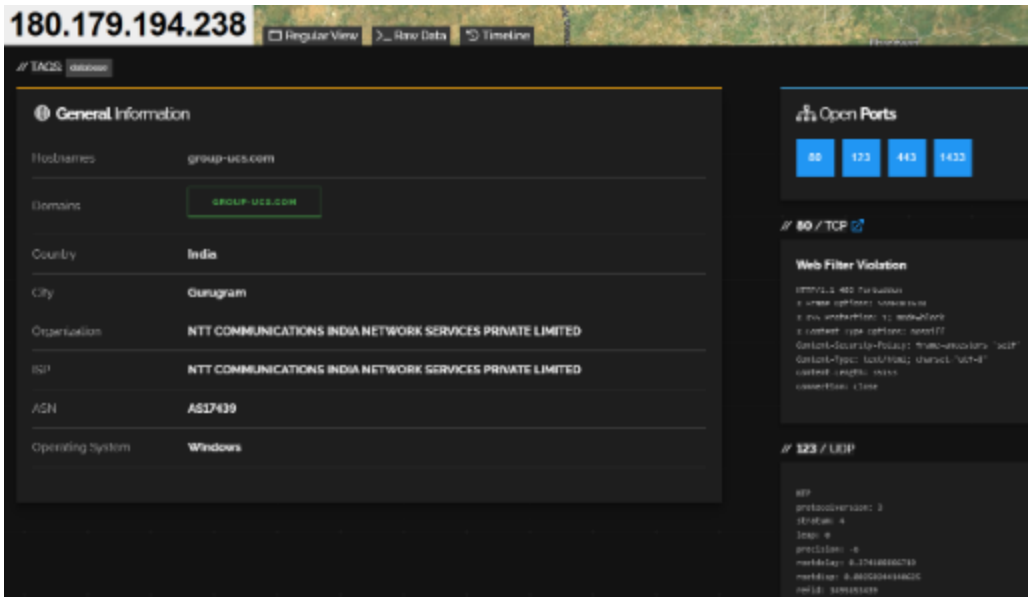


fig: 8. The open ports and it's service list

As shown in the image above, it is evident that ports 80, 123, 443, and 1433 are open.

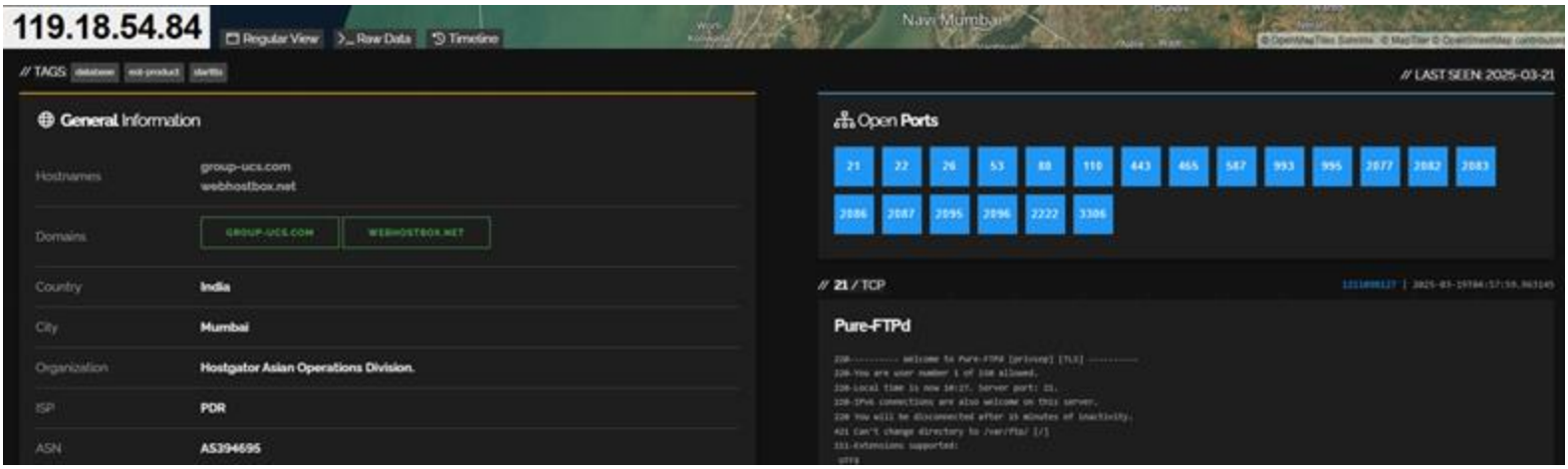


fig: 9. The open ports and its service list of another ip address

VULNERABILITIES IDENTIFIED

Unified Credit Solutions

Open Port	Service Running
21	FTP
22	OpenSSH
26	Exim Smtp
53	DNS
80	Apache Httpd
110	Dovecot POP3
443	Nginx 1.23.4
465	Exim Smtpd 4.98.1
587	Exim Smtpd 4.98.1
993	IMAP
995	Dovecot POP3
2077	CPanel service
2082	CPanel Login
2083	CPanel Login
2086	whm Login
2087	whm Login
2095	Webmail Login
2096	SSL connections to cPanel's webmail and WHM interfaces
2222	OpenSSH
3306	MySQL 5.7.23

The table above illustrates the open ports and their corresponding services.

VULNERABILITIES IDENTIFIED

Unified Credit Solutions

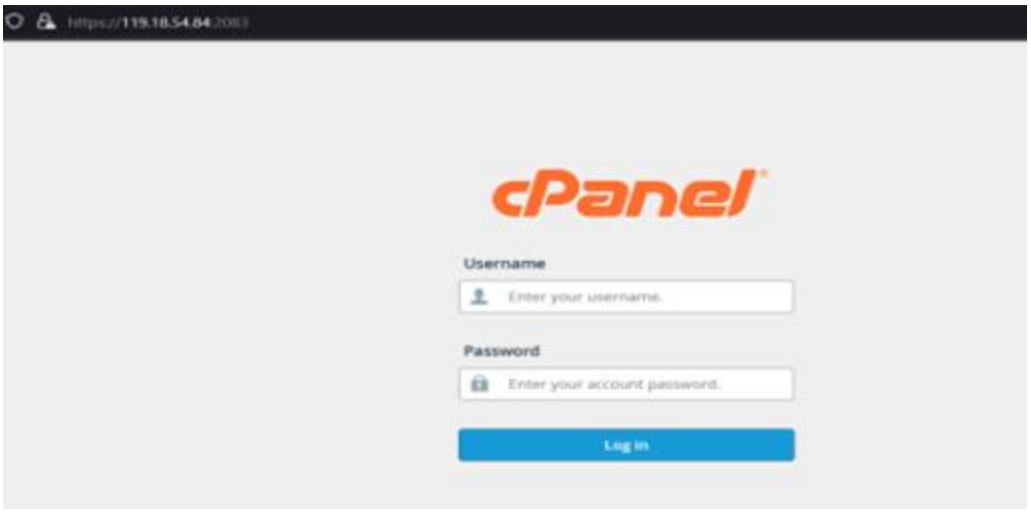


fig: 10. The Cpanel login page

The image above shows the Cpanel login page, which is accessible online.

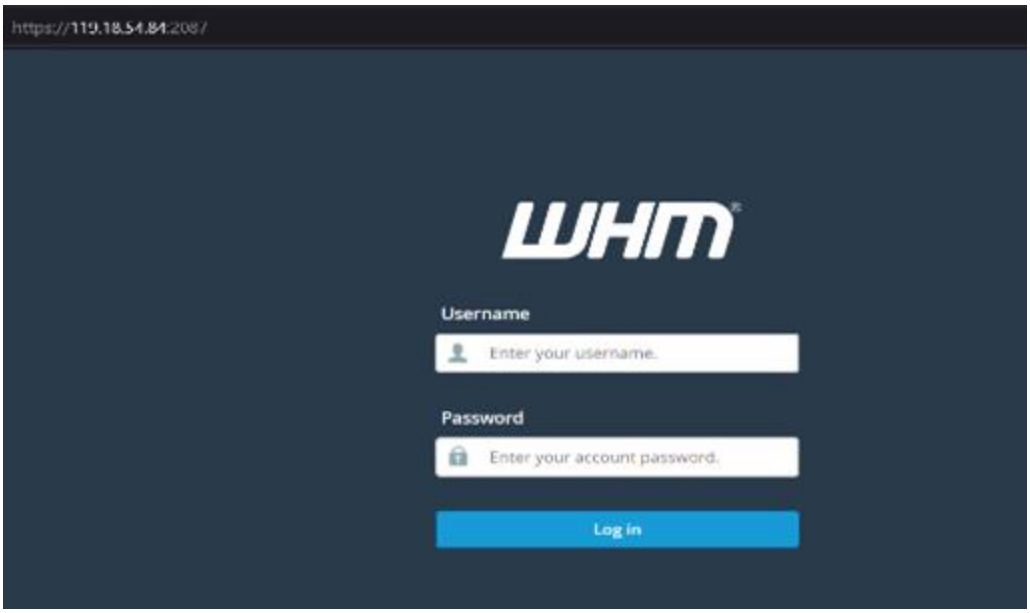


fig: 11. The WHM login page

The image above shows the WHM login page, which is accessible online.

VULNERABILITIES IDENTIFIED

Unified Credit Solutions

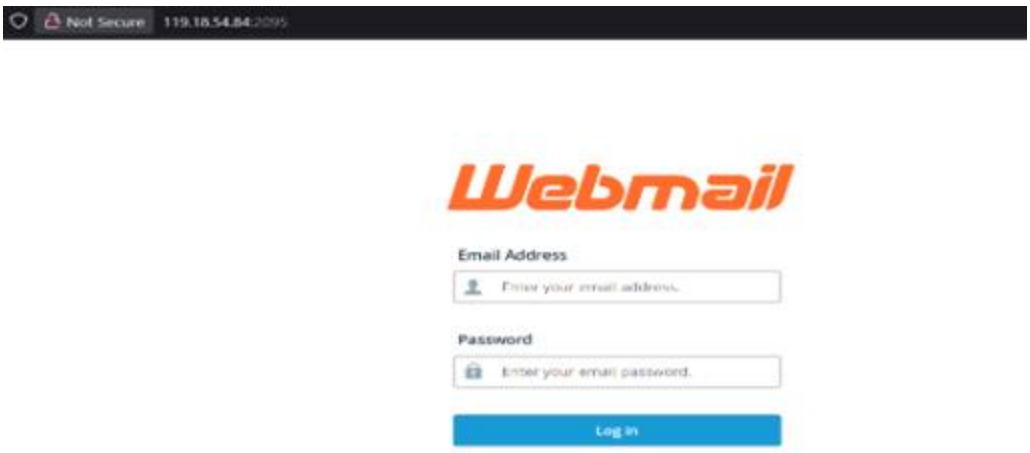


fig: 12. The Webmail login page

The image above shows the webmail login page, which is accessible online.

Findings:
We were able to identify the login pages for Cpanel, WHM, and Webmail, all of which are accessible online.

Mitigation:
To mitigate risks associated with open ports, close unnecessary ports, use firewalls to control traffic.

VULNERABILITIES IDENTIFIED

Unified Credit Solutions

Typosquatting

Description :

Typosquatting involves registering domains that closely resemble legitimate websites, but with slight variations that are common typing mistakes (e.g., "Gooogle.com" instead of "Google.com").

Typosquatting, also known as URL hijacking, is a cybercrime where malicious actors register domain names that are similar to legitimate websites, but with common typographical errors, to trick users into visiting fake sites.

Typosquatting URL
groupucs.com
group-ucs.cn
group-ucs.br
qroup-ucs.com
www-group-ucs.com
group-ucs.org
group-ucs.live
group-ucs.online
group-ucs.ltd
login-group-ucs.com

Mitigation:

Register the mentioned domain names and implement robust monitoring and security measures.

VULNERABILITIES IDENTIFIED

Unified Credit Solutions

Backup File Exposure

Description :

Sensitive files (backups, database dumps, or configs) are left publicly accessible, attackers can easily download and extract critical information.

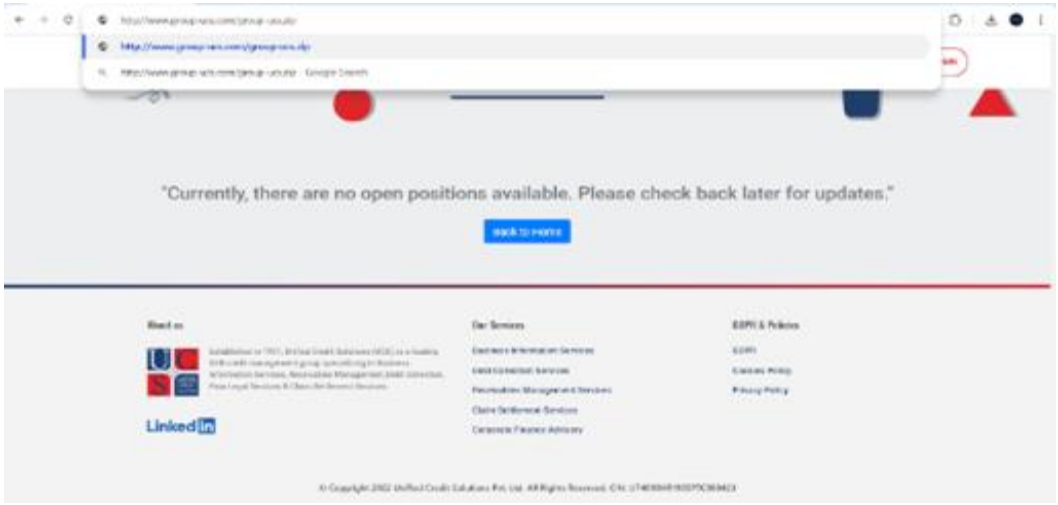


fig: 13. Changing URL as group-ucs.com.zip

CWE	CWE-530: Exposure of Backup File to an Unauthorized Control Sphere
	CWE-552: Files or Directories Accessible to External Parties
	CWE-200: Exposure of Sensitive Information

VULNERABILITIES IDENTIFIED

Unified Credit Solutions

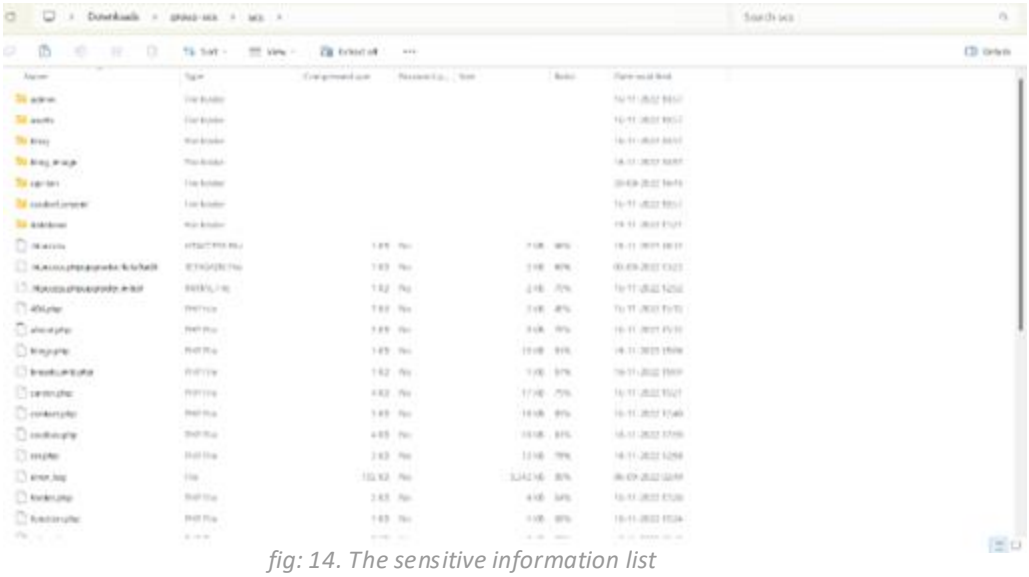


fig: 14. The sensitive information list

The sensitive file has been exposed online.

Recommendation	Block access via .htaccess (Apache)	<FilesMatch "\.(zip|sql|bak|tar|gz|7z)$"> Require all denied </FilesMatch>

MADRE JANUS

EMPOWERING BUSINESSES TO OPERATE SECURELY, EFFICIENTLY AND CONFIDENTLY IN AN INCREASINGLY DIGITAL WORLD

MADRE JANUS

Thank You

www.madre-janus.com