Vulnerability Assessment

November 2021

Source: https://wilsoncgrp.com/vulnerability-assessment

Note: Any sensitive data such as the client company name and client employee names have been removed or replaced by fake names.

Executive Summary

The team has identified a total of 5 high risk and 1 medium risk vulnerabilities. These vulnerabilities have been discovered by conducting research on people working in ABC company, on abc.com.sg (WordPress website) and on abc.dyndns.org (Firewall).

Most of the vulnerabilities found pertain to the abc.com.sg domain. We could not find any vulnerabilities found for abc.dyndns.org and no actions are needed for it.

Major Findings

1. **People:** Credentials owned by two ABC people have been leaked and are publicly available.

2. **abc.com.sg:** 5 vulnerabilities exist for the WordPress website due to misconfiguration on the WordPress website as well as misconfiguration on the server that hosts the abc.com.sg domain.

Key Recommendations

Website administrator(s) for abc.com.sg should quickly remediate any vulnerabilities found below by installing relevant plugins and upgrading software versions to the latest versions. ABC accounts with leaked credentials should have their passwords changed on all websites and services that use the leaked credentials.

Methodology

The team was given the *https://abc.dyndns.org/* domain to work with and was tasked with finding any other vulnerabilities that may exist. We searched the web for any other websites and servers that may be linked to ABC Company. We found three key websites that would serve as our focuses for the vulnerability assessment.

linkedin.com: Employee Information

To understand more about the people working in the company, we referred to ABC group's LinkedIn (*https://www.linkedin.com/company/abcgroup/*). We used tools that are publicly available to find any leaked credentials for the people listed in the link above. (See Appendix A)

abc.com.sg: Front-facing website

abc.com.sg appears to be the "front-face" of ABC Company. We used scanning tools to check if there are any vulnerabilities related to the WordPress website, and the server that is hosting the website. (See Appendix A)

abc.dyndns.org: Firewall to access Virtual Office

abc.dyndns.org seems to be the gateway to access IT resources for ABC Company. Like abc.com.sg, we used scanning tools to check if there are any vulnerabilities related to the login page, and the server that is hosting the firewall login page. (See Appendix A)

Risk Assessment

The team has identified a total of 6 vulnerabilities. They are categorised into high, medium and low risk as below.

Risk Level	Count
High	5
Medium	1
Low	0

fig. 1 Number of vulnerabilities categorised by risk category

High risk vulnerabilities cause severe damage to ABC Company. ABC Company may lose access to important resources as the server is not well configured. Sensitive information has also been leaked.

Medium risk vulnerabilities may cause considerable damage to ABC Company. Usernames can be enumerated that allows hackers to potentially gain access to ABC's resources when used with other methods.

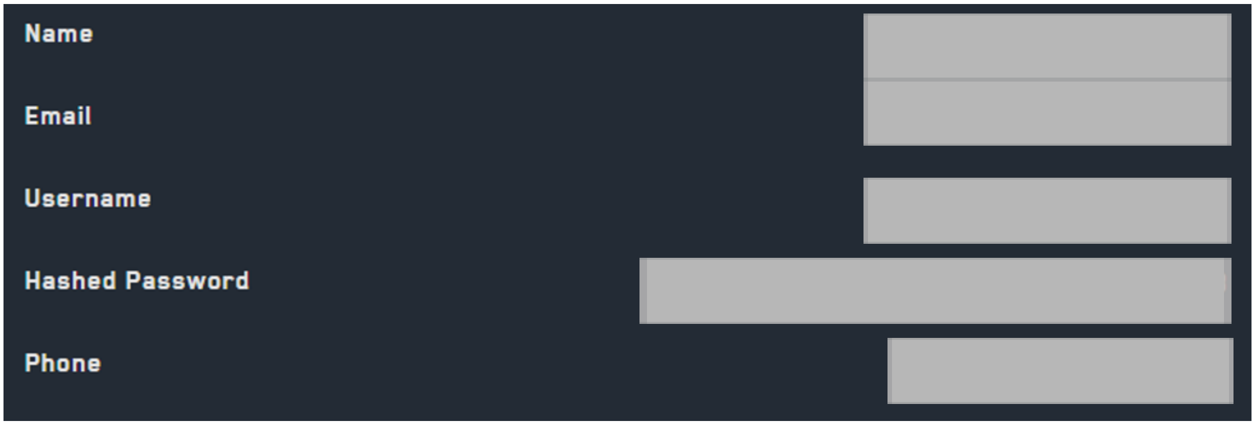
Low risk vulnerabilities may cause damage to ABC Company. No vulnerabilities have been found that are low risk.

High Risk

1. Employee Credentials leaked

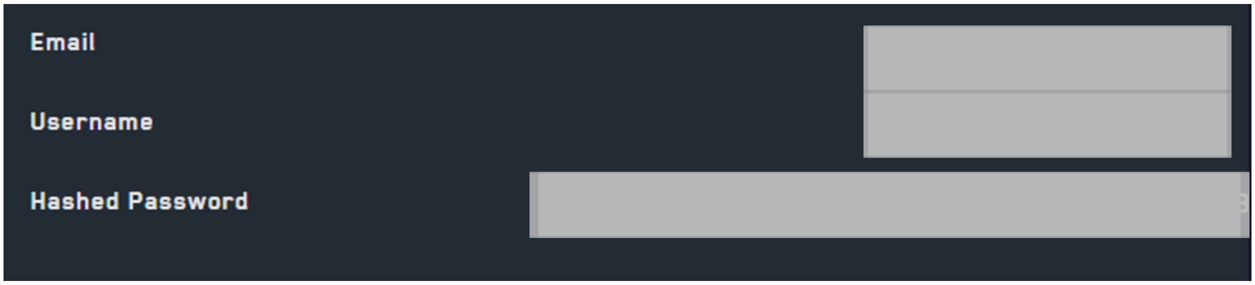
Impact

John ABC and Jane ABC's credentials have been leaked and are publicly available. Hackers may use their credentials to access services owned by John and Jane if they have not changed their password since the leak.



Name	[redacted]
Email	[redacted]
Username	[redacted]
Hashed Password	[redacted]
Phone	[redacted]

fig. 2 John's leaked credentials



Email	[redacted]
Username	[redacted]
Hashed Password	[redacted]

fig. 3 Jane's leaked credentials

Recommendations

On any services that are using the credentials highlighted above, change your password to a secure password (At least 12 characters long; Use a mix of characters; Avoid personal information[1]) and if possible, add two factor authentication.

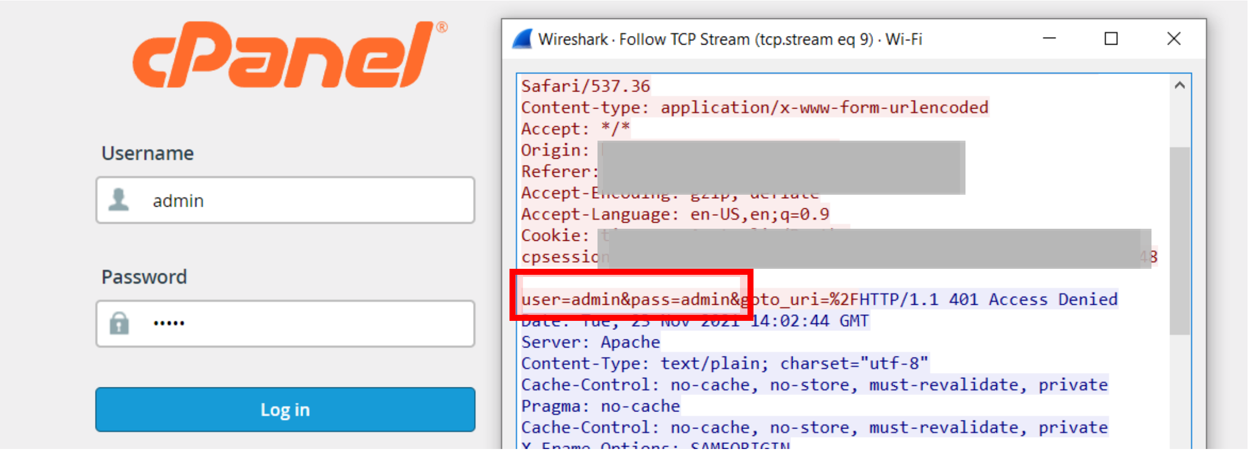
[1] https://support.google.com/accounts/answer/32040

High Risk

2. Credentials inputted on WordPress login pages in clear text

Impact

Hackers can obtain credentials to both ***http://cpanel.abc.com.sg/*** and ***http://webmail.abc.com.sg/*** if hackers are in the same network as ABC people through an attack called the Man in the Middle attack. This means that if a ABC personnel accesses *http://cpanel.abc.com.sg/* in Starbucks and a hacker happens to be running an attack on the Starbucks network, the hacker can obtain the credentials that the personnel inputted. An example of such an attack is shown below using a set of mock username and password.



Username

admin

Password

•••••

```
Safari/537.36
Content-type: application/x-www-form-urlencoded
Accept: */*
Origin: [redacted]
Referer:
Accept-E
Accept-Language: en-US,en;q=0.9
Cookie: [redacted]
cpsessio

user=admin&pass=admin&goto_uri=%2FHTTP/1.1 401 Access Denied
Date: Tue, 23 Nov 2021 14:02:44 GMT
Server: Apache
Content-Type: text/plain; charset="utf-8"
Cache-Control: no-cache, no-store, must-revalidate, private
Pragma: no-cache
Cache-Control: no-cache, no-store, must-revalidate, private
X-Frame-Options: SAMEORIGIN
```

fig. 4 Network traffic can be captured using Wireshark to capture credentials

Areas Affected

- *http://abc.com.sg/*
- *http://cpanel.abc.com.sg/*
- *http://webmail.abc.com.sg/*

Recommendations

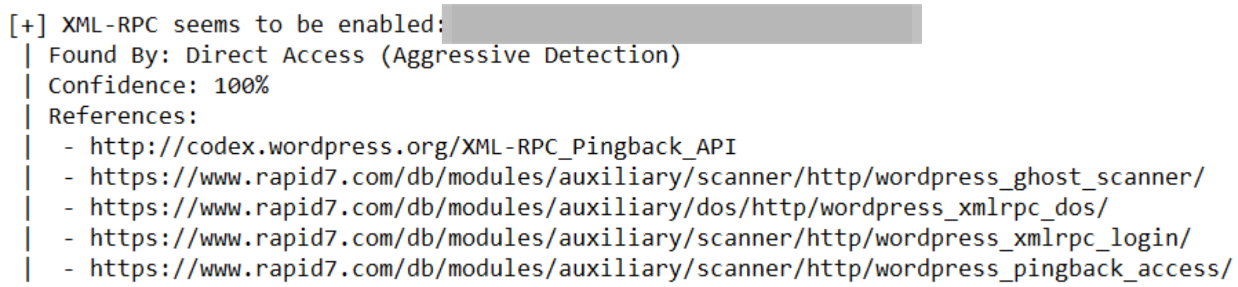
Apply for an AlphaSSL Certificate from HostSG to encrypt traffic through the affected websites[2]. This ensures that all information sent and received is encrypted and undecipherable by hackers conducting a Man in the Middle attack.

[2] Link: http://www.hostsg.com/solutions/ssl-certificate.php

High Risk

3. Brute Force attack possible to login to WordPress website

We ran a WordPress scan and found that the XML-RPC feature is enabled. This feature is vulnerable to CVE-2020-28035[3] (Common Vulnerabilities and Exposures).



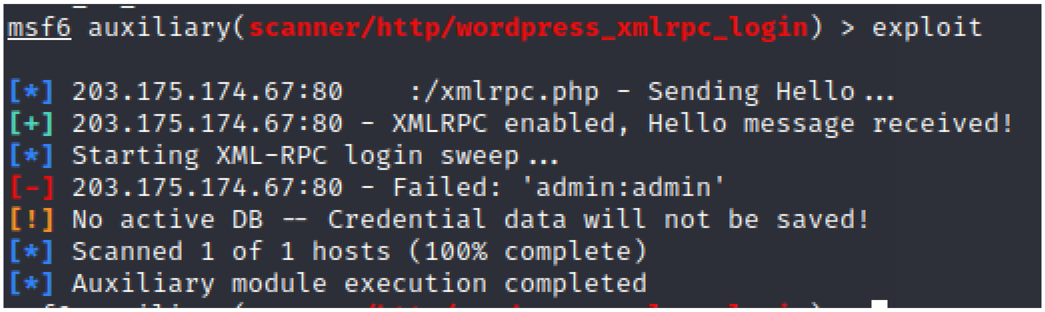
```
[+] XML-RPC seems to be enabled: [redacted]
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
```

fig. 5 XML-RPC is enabled

Impact

Hackers can run a brute force attack on ***http://abc.com.sg/xmlrpc.php*** to determine login credentials to access the abc.com.sg WordPress website. Additionally, if any credentials that were leaked are used as the login to the WordPress website, the brute force attack will be easier to conduct for hackers. This may lead to defacement of the website and even loss of access to the WordPress website. This attack is possible as the link above is publicly available.

The example below shows a mock brute force attack using only one username and one password.



```
msf6 auxiliary(scanner/http/wordpress_xmlrpc_login) > exploit

[*] 203.175.174.67:80    :/xmlrpc.php - Sending Hello ...
[+] 203.175.174.67:80 - XMLRPC enabled, Hello message received!
[*] Starting XML-RPC login sweep ...
[-] 203.175.174.67:80 - Failed: 'admin:admin'
[!] No active DB -- Credential data will not be saved!
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

fig. 6 Brute Force attack example

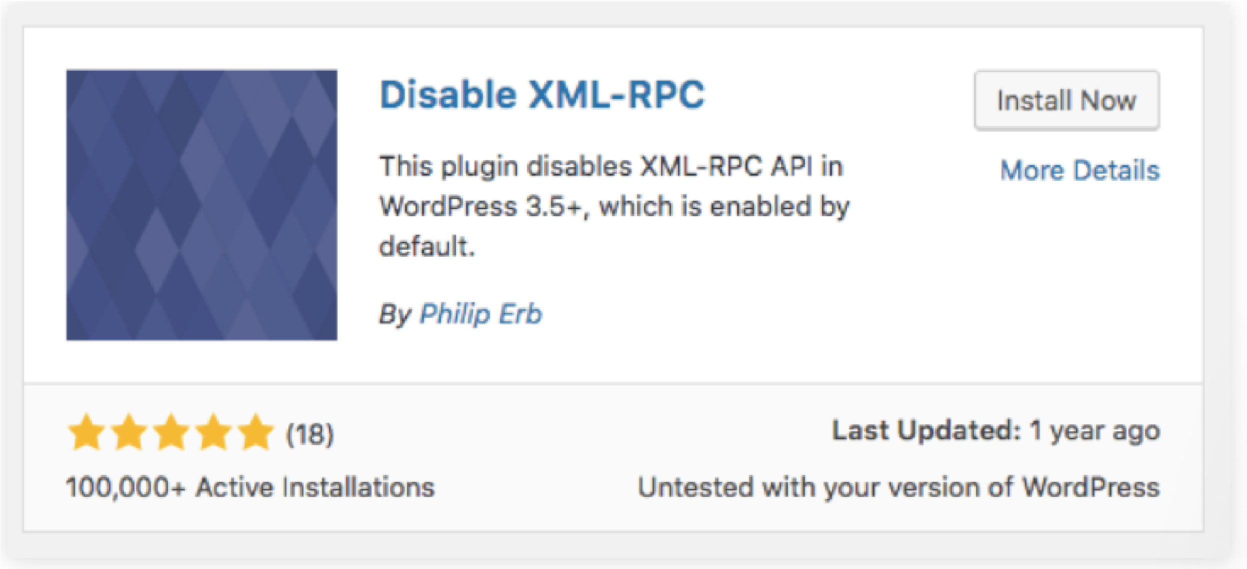
[3] Link to CVE: https://nvd.nist.gov/vuln/detail/CVE-2020-28035

Areas Affected

- *http://abc.com.sg/*
- *http://cpanel.abc.com.sg/*
- *http://webmail.abc.com.sg/*

Recommendations

Navigate to Plugins > Add New section from your WordPress dashboard. Search for, and install the **Disable XML-RPC** plugin[4]**.** This disables the XML-RPC plugin and prevents hackers from exploiting the vulnerable XML-RPC feature.



Disable XML-RPC

This plugin disables XML-RPC API in WordPress 3.5+, which is enabled by default.

By Philip Erb

★★★★★ (18)

100,000+ Active Installations

Last Updated: 1 year ago

Untested with your version of WordPress

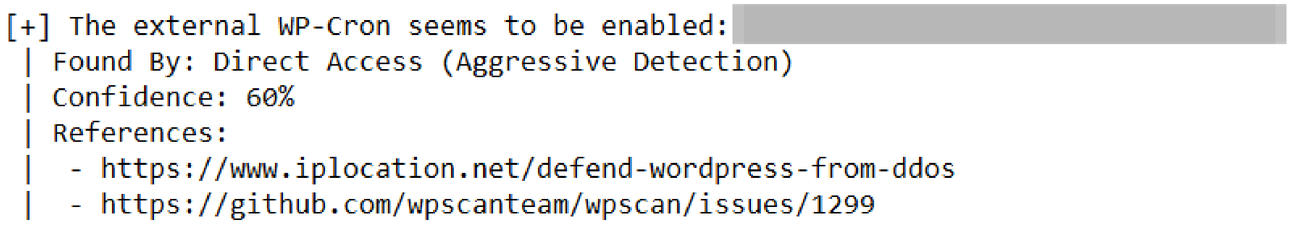
fig. 7 Disable XML-RPC plugin[5]

[4] Source: https://www.hostinger.com/tutorials/xmlrpc-wordpress

High Risk

4. Distributed Denial of Service (DDOS)

As above, from the WordPress scan we found that the XML-RPC feature and the WP-Cron feature is enabled. This causes the WordPress website to be vulnerable to DDOS.



```
[+] The external WP-Cron seems to be enabled: [redacted]
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299
```

fig. 8 WP-Cron is enabled

Impact

Hackers can run a Distributed Denial of Service attack on ***http://abc.com.sg/xmlrpc.php*** and ***http://abc.com.sg/wp-cron.php*** to slow down and potentially, bring down the WordPress website. This attack leverages on the same principles as the brute force attack above. The key difference is that for a DDOS attack, instead of using a list of credentials, the attacker will use multiple servers to send requests to the links above. If the server is not able to process all the requests, it will crash.

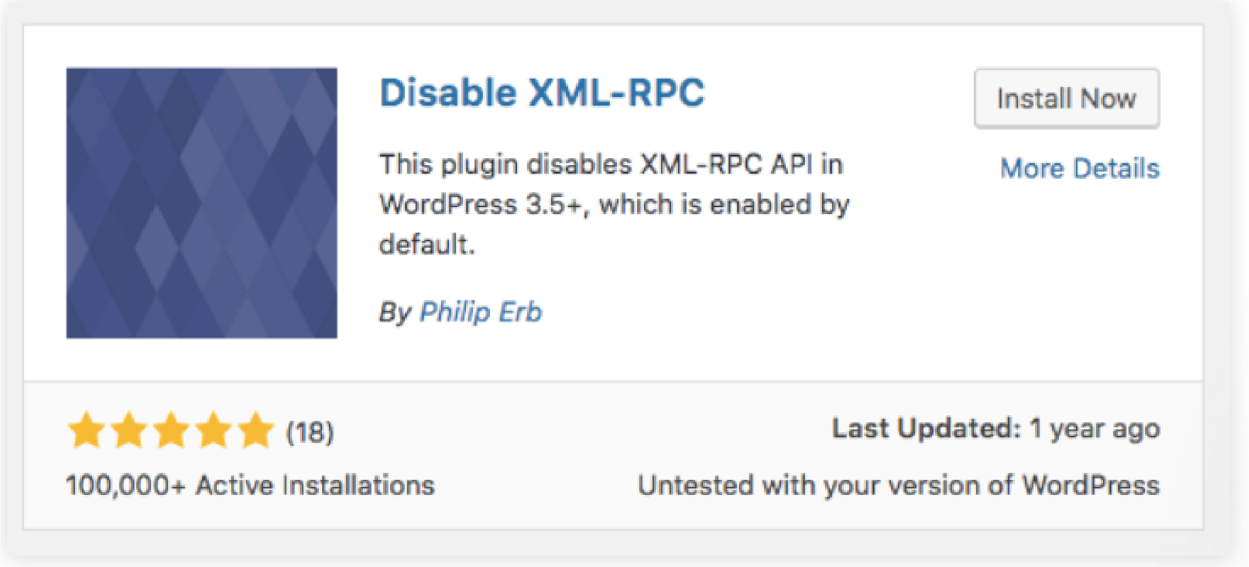
Areas Affected

- *http://abc.com.sg/*
- *http://cpanel.abc.com.sg/*
- *http://webmail.abc.com.sg/*

Recommendations

To disable XML-RPC:

Navigate to Plugins > Add New section from your WordPress dashboard. Search and install the **Disable XML-RPC** plugin[5]**.** This disables the XML-RPC plugin and prevents hackers from exploiting the vulnerable XML-RPC feature.



Disable XML-RPC

This plugin disables XML-RPC API in WordPress 3.5+, which is enabled by default.

By Philip Erb

100,000+ Active Installations

Last Updated: 1 year ago

Untested with your version of WordPress

fig. 9 Disable XML-RPC plugin[6]

To disable WP-Cron:

Update your wp-cronfig.php file to include `define('DISABLE_WP_CRON', true);` following the line `define('DB_COLLATE', '');` (This is typically found in public_html)[6].

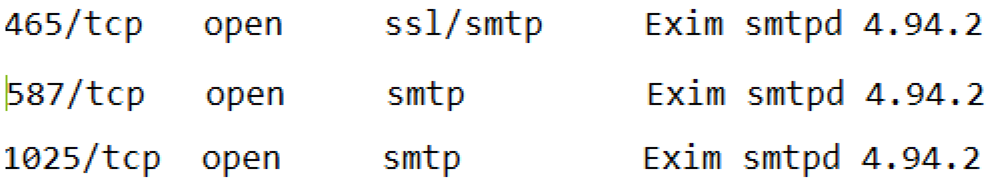
If you are currently relying on cron jobs, please refer to the following link: https://blog.cpanel.com/how-to-configure-a-cron-job/

[5] Source: https://www.hostinger.com/tutorials/xmlrpc-wordpress
[6] Link: https://medium.com/@thecpanelguy/the-nightmare-that-is-wpcron-php-ae31c1d3ae30

High Risk

5. Email interception

We ran an nmap scan on 203.175.174.67 and found that The SMTP service uses Exim smtpd 4.94.2 and is vulnerable to CVE-2021-38371[7].



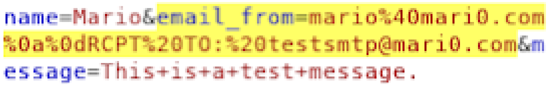
```
465/tcp    open     ssl/smtp     Exim smtpd 4.94.2
587/tcp    open     smtp         Exim smtpd 4.94.2
1025/tcp   open     smtp         Exim smtpd 4.94.2
```

fig. 10 SMTP service uses Exim smtpd 4.94.2

Impact

Hackers can intercept emails sent through the webmail server and change the contents of the email, including the recipients receiving the email, the body of the email. This means that hackers can use the abc.com.sg domain to send phishing emails to unsuspecting parties and also block any emails from being sent to intended parties.

An example of such an attack is shown in the image below. Note that hackers are able to intercept any emails sent and change the recipients who will receive them.



```
name=Mario&email_from=mario%40mari0.com
%0a%0dRCPT%20TO:%20testsmtp@mari0.com&m
essage=This+is+a+test+message.
```

fig. 11 Example of email interception[8]

Areas Affected

- *http://webmail.abc.com.sg/*

Recommendations

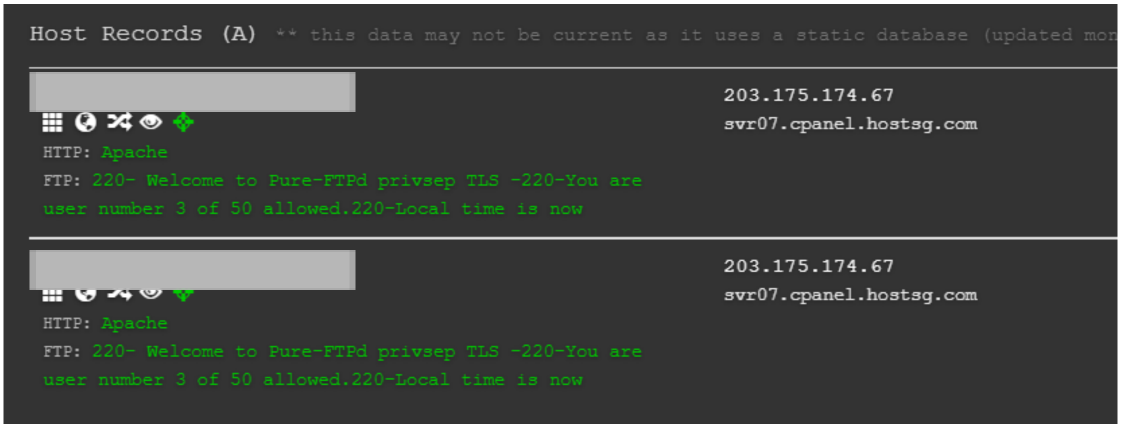
As this attack can only be done by hackers in your local network, only send emails when in a trusted network, such as at your office[9].

[7] Link to CVE: https://nvd.nist.gov/vuln/detail/CVE-2021-38371
[8] Source: https://jagskap.blogspot.com/2019/06/smtp-injection.html
[9] Additional information on vulnerability: https://vuldb.com/?id.180505

Medium Risk

1. Hostsg server hosts multiple WordPress domains with similar vulnerabilities

We conducted a DNS lookup on abc.com.sg and found the IP address linked to it. Based on the domain name of the server, we concluded that abc.com.sg is hosted on a hostsg server.



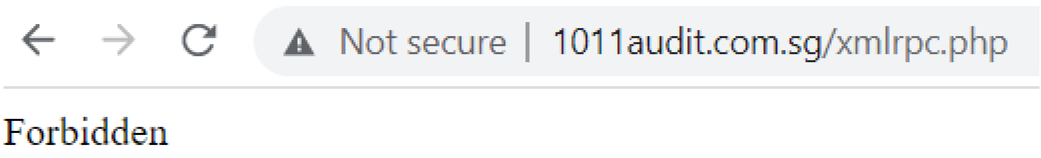
```
Host Records (A) ** this data may not be current as it uses a static database (updated mon

[redacted]                                                    203.175.174.67
                                                              svr07.cpanel.hostsg.com
HTTP: Apache
FTP: 220- Welcome to Pure-FTPd privsep TLS -220-You are
user number 3 of 50 allowed.220-Local time is now

[redacted]                                                    203.175.174.67
                                                              svr07.cpanel.hostsg.com
HTTP: Apache
FTP: 220- Welcome to Pure-FTPd privsep TLS -220-You are
user number 3 of 50 allowed.220-Local time is now
```

fig. 12 DNS lookup result on abc.com.sg

Impact

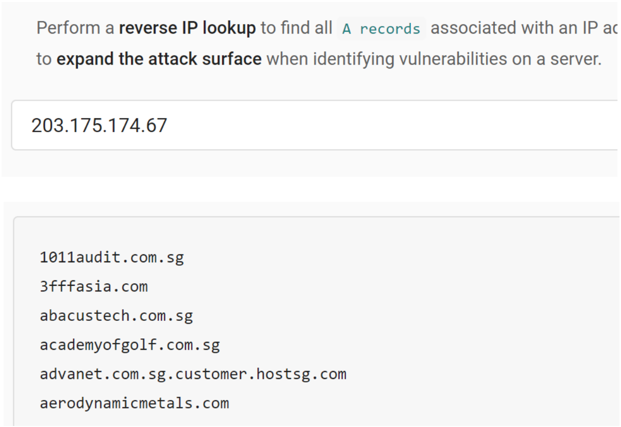
The server that hosts abc.com.sg hosts 213 other WordPress websites[10], all with similar vulnerabilities to the vulnerabilities highlighted above. This presents more opportunities for hackers to access and/or crash the server. For example, a hacker would not need to target ***http://abc.com.sg/xmlrpc.php*** to run a DDOS attack. Instead, they can target ***http://1011audit.com.sg/xmlrpc.php***, and potentially, 212 more links to run a DDOS attack to bring down the server.

[10] Source: https://hackertarget.com/reverse-ip-lookup/



Forbidden

fig. 13 XML-RPC is enabled on other WordPress websites hosted on hostsg



Perform a **reverse IP lookup** to find all `A records` associated with an IP ac
to **expand the attack surface** when identifying vulnerabilities on a server.

203.175.174.67

```
1011audit.com.sg
3fffasia.com
abacustech.com.sg
academyofgolf.com.sg
advanet.com.sg.customer.hostsg.com
aerodynamicmetals.com
```

fig. 14 Sample list of domains that are hosted on the same server that hosts abc.com.sg

Areas Affected

- *http://abc.com.sg/*
- *http://cpanel.abc.com.sg/*
- *http://webmail.abc.com.sg/*

Recommendations

Consider other hosting services to host the WordPress website.

Summary

abc.com.sg is vulnerable due to misconfiguration on both the WordPress website and the hosting server. In the short term, website administrators can quickly remediate vulnerabilities that are accessible on the WordPress administrator's dashboard. In the long term, we recommend ABC Company to consider other hosting sites as its default configuration for WordPress websites are insecure.

abc.dyndns.org is secure and we could not find any vulnerabilities associated with the firewall.

Overall, all risks are associated with ABC Company's public profile. In comparison, ABC Company's key IT resources are secure.

Appendix

Appendix A: Tools used for Vulnerability Assessment

Tools to find any leaked credentials for people in ABC

- LinkedIn: https://www.linkedin.com/company/abcgroup/
- have I been pwned: https://haveibeenpwned.com/
- dehashed: https://dehashed.com/
    - Full results can be found in included file “Dehashed.docx”
- pwndb (dark web website): www.pwndb2am4tzkvold.onion

Tools to scan WordPress website

- nmap: https://nmap.org/
    - Full results can be found in included file “website_nmap.txt”
- WPscan: https://wpscan.com/
    - Full results can be found in included file “website_wpscan.txt”

Tools to scan firewall

- nmap: https://nmap.org/
    - Full results can be found in included file “firewall_nmap.txt”

Appendix B: Analysis on OSINT conducted on ABC employees

OSINT on LinkedIn

The team first conducted Open Source Intelligence (OSINT) on ABC employees found from LinkedIn[11]. Even though the company listed 9 employees, we found that 6 of these employees work in a separate ABC company that is based in India.

For example, the Managing Director for ABC Company lives in Gurugram/Gurgaon, India, the same city that the Indian ABC Group is based in. We thus focused our research on James ABC, John ABC and Jane ABC.

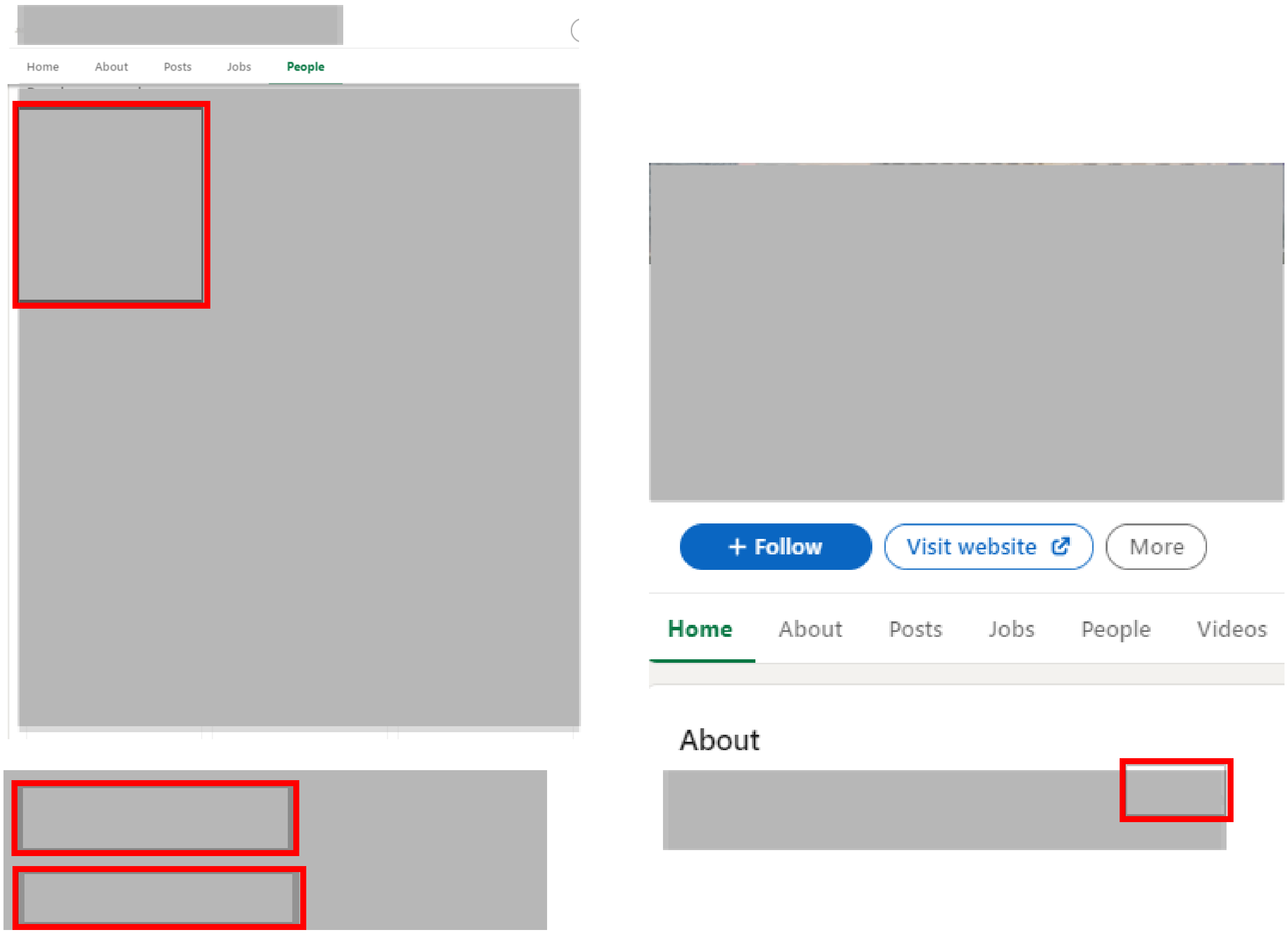
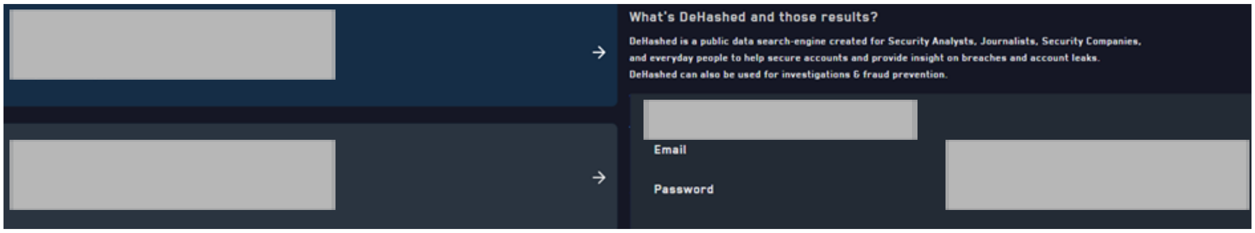


fig. 15 Not all people listed actually work in ABC

[11] https://www.linkedin.com/company/abcgroup/

Finding leaked credentials (*Related vulnerability: Employee Credentials leaked*)

We used pwndb[12] to find any leaked credentials associated with abc.com.sg and found that there are no leaked credentials on pwndb. We then turned to dehashed[13] and found leaked credentials for John and Jane. All credentials found can be found in the file Dehashed.docx.



[redacted] →

[redacted] →

What's DeHashed and those results?

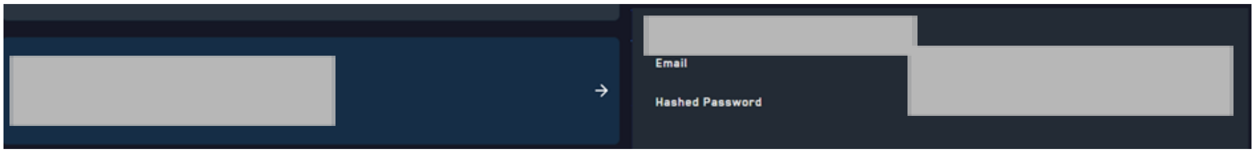
DeHashed is a public data search-engine created for Security Analysts, Journalists, Security Companies, and everyday people to help secure accounts and provide insight on breaches and account leaks. DeHashed can also be used for investigations & fraud prevention.

[redacted]

Email

Password

[redacted]



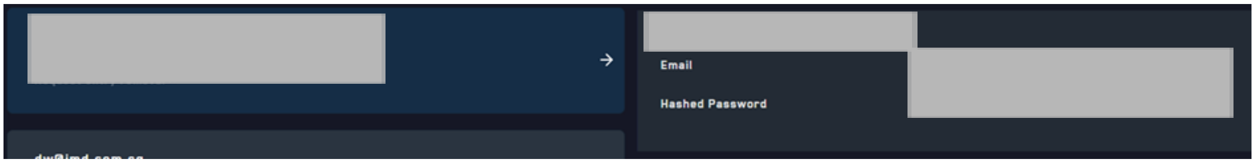
[redacted] →

[redacted]

Email

Hashed Password

[redacted]



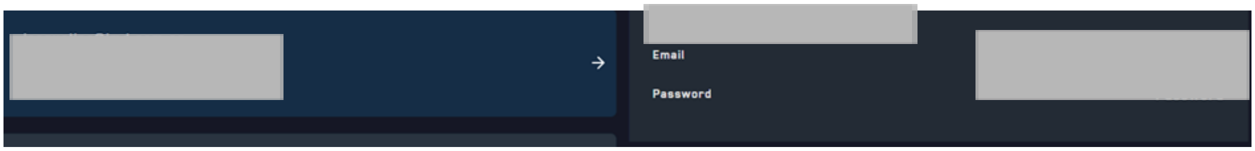
[redacted] →

[redacted]

Email

Hashed Password

[redacted]



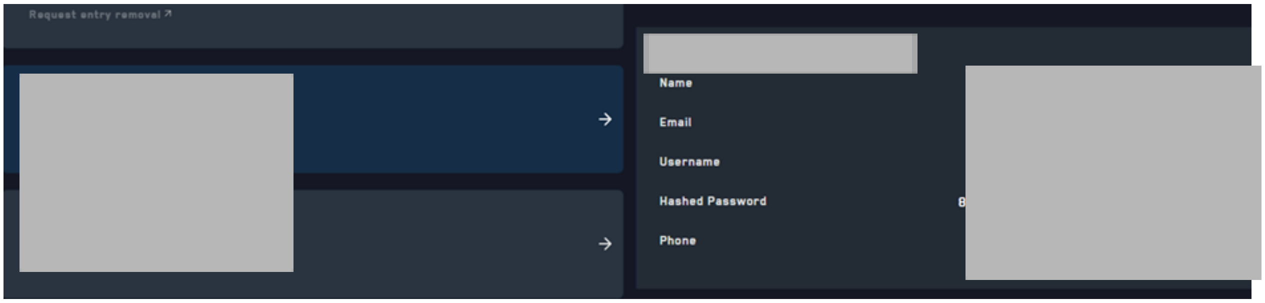
[redacted] →

[redacted]

Email

Password

[redacted]



Request entry removal ↗

[redacted] →

→

[redacted]

Name

Email

Username

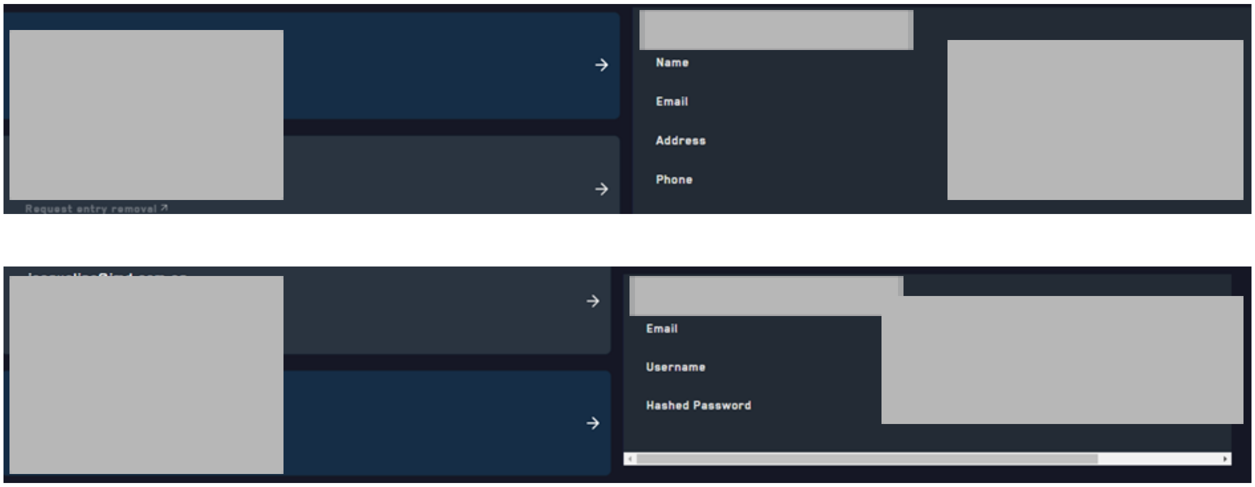
Hashed Password

Phone

[redacted]

[12] Link: www.pwndb2am4tzkvold.onion

[13] Link: https://dehashed.com/

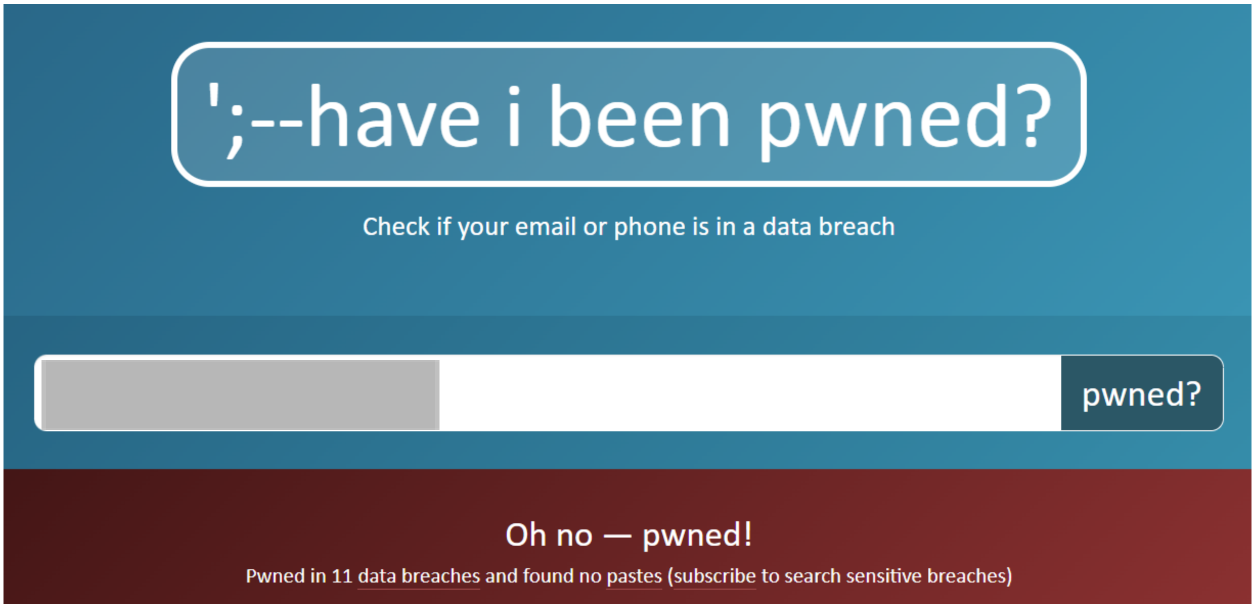


[redacted] [redacted] [redacted]

[redacted] [redacted] [redacted]

fig. 16 Leaked credentials for John and Jane

This is also verified by https://haveibeenpwned.com/ for john@abc.com.sg whose email has been pwned in 11 data breaches .



';--have i been pwned?

Check if your email or phone is in a data breach

[redacted]

Oh no — pwned!

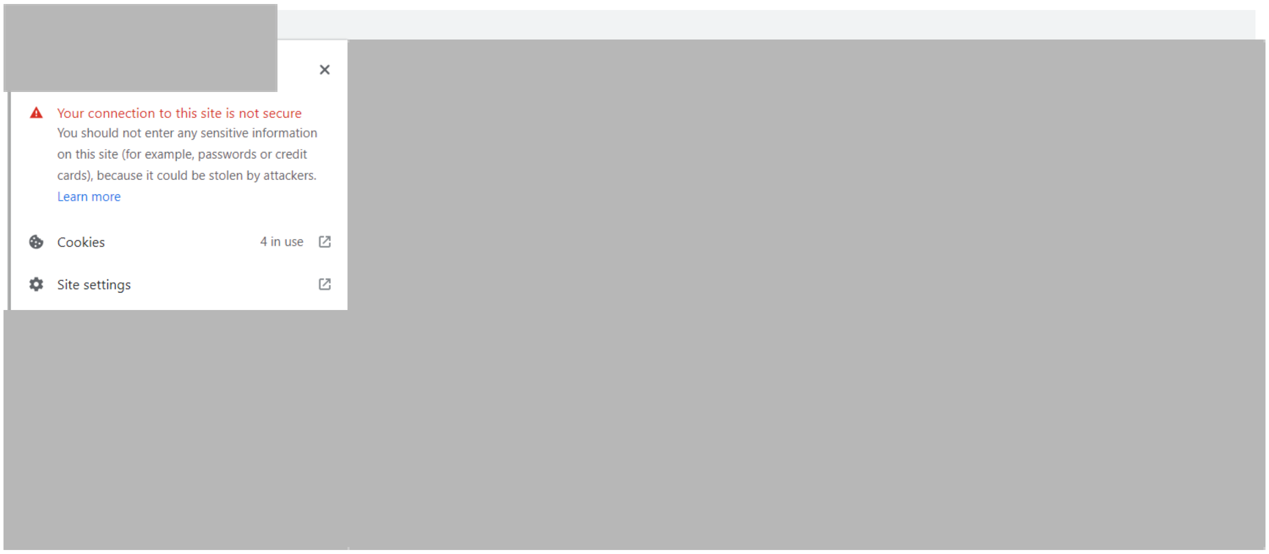
Pwned in 11 data breaches and found no pastes (subscribe to search sensitive breaches)

fig. 17 john@abc.com.sg has been pwned

Appendix C: Analysis on abc.com.sg

WordPress website uses http protocol

On first entering the website, we immediately noticed that the website uses the http protocol which means that information sent and received on the website is in clear text.



[redacted]

Your connection to this site is not secure
You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers.
Learn more

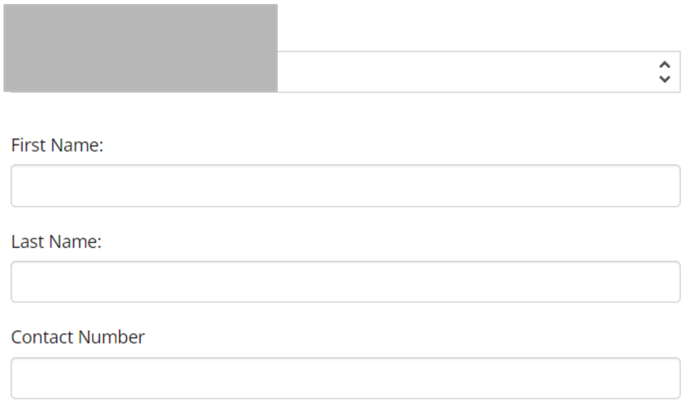
Cookies 4 in use

Site settings

[redacted]

fig. 18 abc.com.sg uses http protocol

Key information that hackers may obtain on this website are leasing enquiries and emails who subscribe to their newsletter.



[redacted]

First Name:

Last Name:

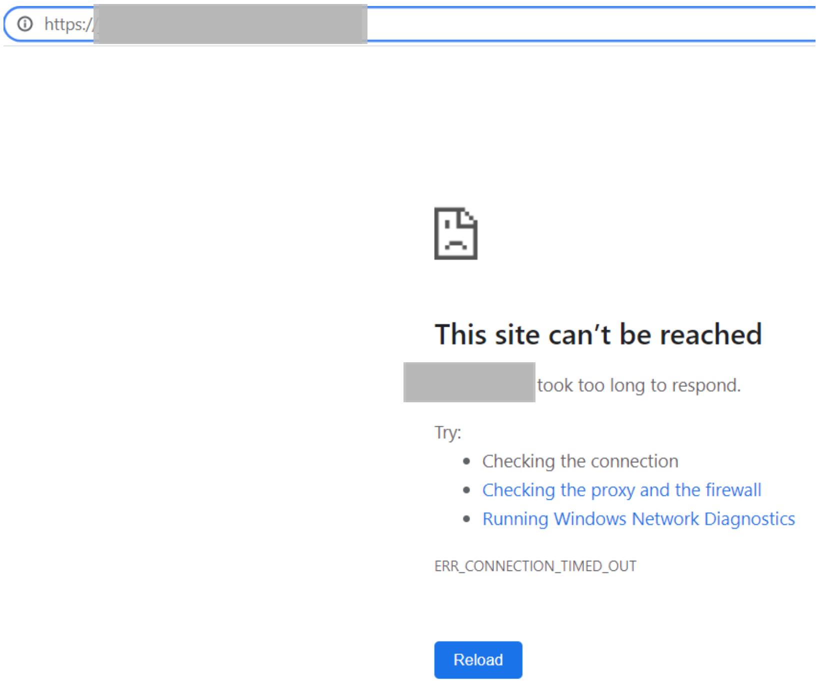
Contact Number

fig. 19 leasing enquiries may be intercepted

[redacted]

fig. 20 Emails may be intercepted

This issue is made even more glaring as abc.com.sg does not support https.



https:/[redacted]

This site can’t be reached

[redacted] took too long to respond.

Try:

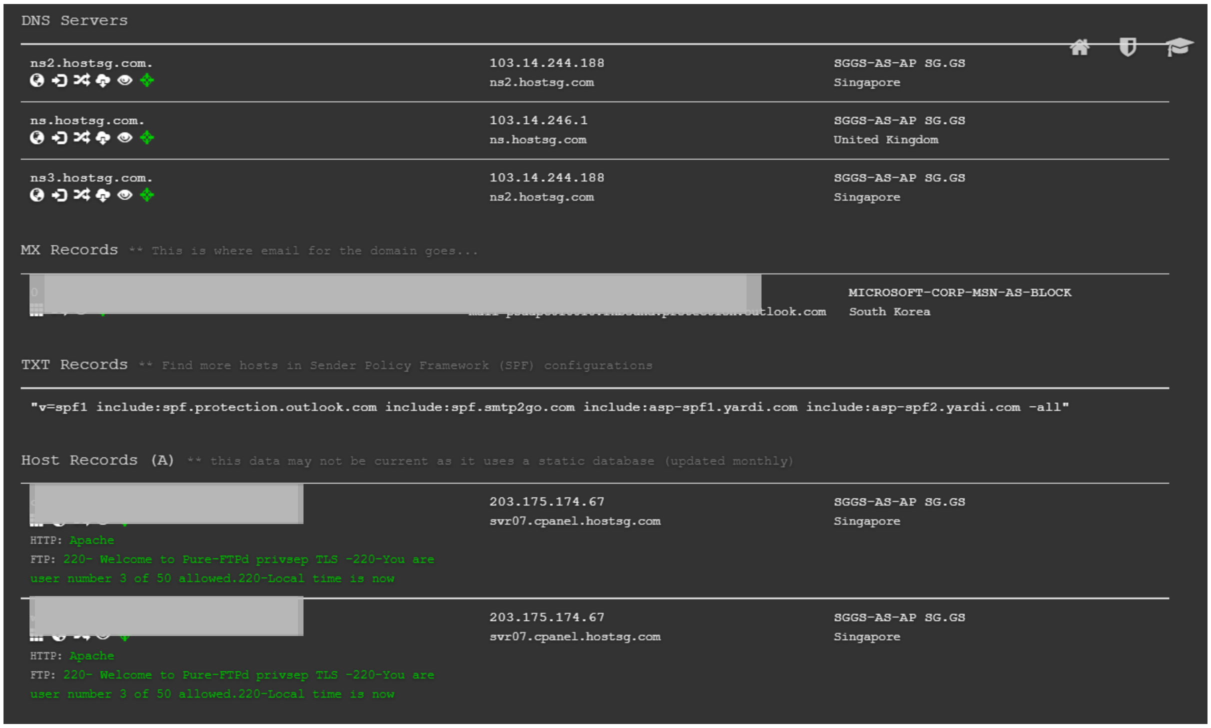
- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

fig. 21 abc.com.sg does not support https protocol

Subdomains also use http protocol (*Related vulnerability: Credentials inputted on WordPress login pages in clear text*)

To find subdomains related to abc.com.sg, we conducted a DNS lookup[14] as well as a certificate search[15]. The key subdomains found are cpanel.abc.com.sg and webmail.abc.com.sg. Through this search, we also found that abc.com.sg is hosted on hostsg.com, at IP address 203.175.174.67. This IP address would later be used for an nmap scan.

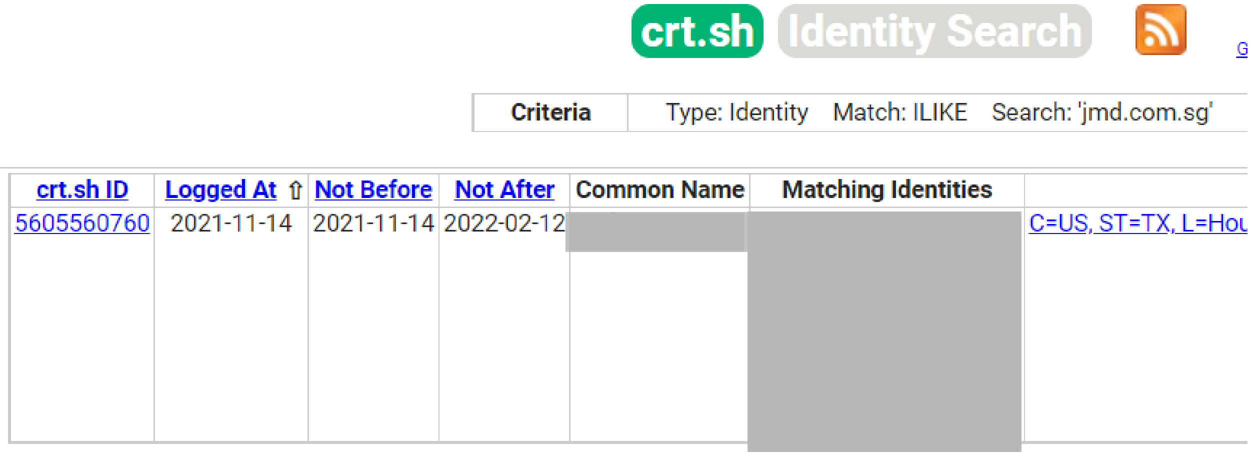


```
DNS Servers

ns2.hostsg.com.              103.14.244.188            SGGS-AS-AP SG.GS
                             ns2.hostsg.com            Singapore

ns.hostsg.com.               103.14.246.1              SGGS-AS-AP SG.GS
                             ns.hostsg.com             United Kingdom

ns3.hostsg.com.              103.14.244.188            SGGS-AS-AP SG.GS
                             ns2.hostsg.com            Singapore

MX Records ** This is where email for the domain goes...

[redacted]                                              MICROSOFT-CORP-MSN-AS-BLOCK
                                                        South Korea

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

"v=spf1 include:spf.protection.outlook.com include:spf.smtp2go.com include:asp-spf1.yardi.com include:asp-spf2.yardi.com -all"

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

[redacted]                   203.175.174.67            SGGS-AS-AP SG.GS
                             svr07.cpanel.hostsg.com   Singapore
HTTP: Apache
FTP: 220- Welcome to Pure-FTPd privsep TLS -220-You are
user number 3 of 50 allowed.220-Local time is now

[redacted]                   203.175.174.67            SGGS-AS-AP SG.GS
                             svr07.cpanel.hostsg.com   Singapore
HTTP: Apache
FTP: 220- Welcome to Pure-FTPd privsep TLS -220-You are
user number 3 of 50 allowed.220-Local time is now
```

fig. 22 DNS lookup result from dnsdumpster

[14] Link: https://dnsdumpster.com/

[15] Link: https://crt.sh/?q=abc.com.sg

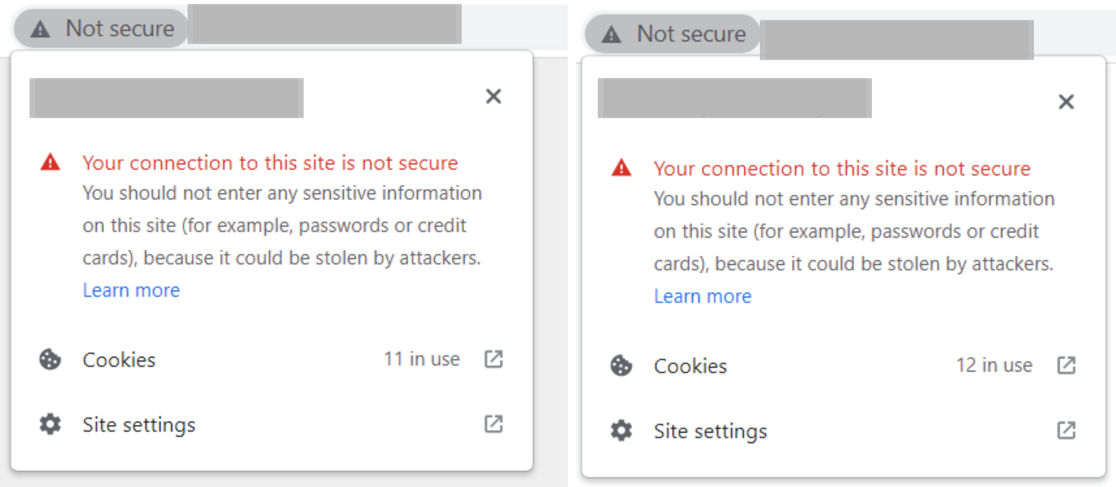


Criteria	Type: Identity Match: ILIKE Search: 'jmd.com.sg'

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities	
5605560760	2021-11-14	2021-11-14	2022-02-12	[redacted]	[redacted]	C=US, ST=TX, L=Hou

fig. 23 Certificate search from crt.sh

Both cpanel.abc.com.sg and webmail.abc.com.sg use the http protocol. This presents a severe vulnerability as all credentials inputted will be shown in clear text and hackers can easily extract these credentials through a Man in the Middle attack.



Not secure [redacted]

[redacted] ✕

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

Cookies 11 in use

Site settings

Not secure [redacted]

[redacted] ✕

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

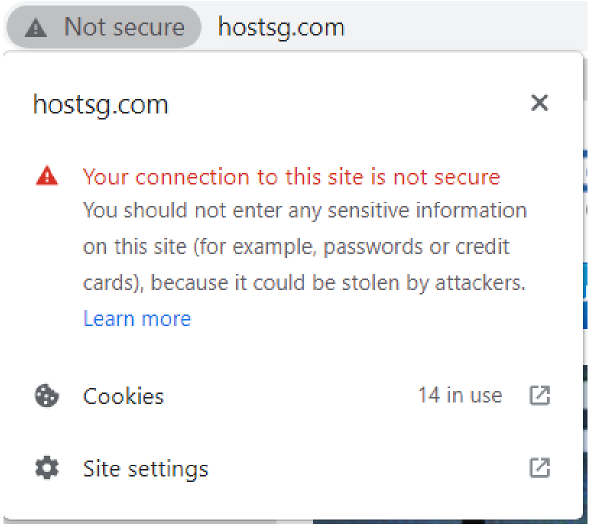
Cookies 12 in use

Site settings

fig. 24 cpanel and webmail uses http protocol

Hosting server hosts 214 vulnerable WordPress websites (*Related vulnerability: Hostsg server hosts multiple WordPress domains with similar vulnerabilities*)

We further conducted research on hostsg.com and found that their main website also uses the http protocol. This does not inspire confidence on the security hostsg brings to the domains that are hosted on their servers.

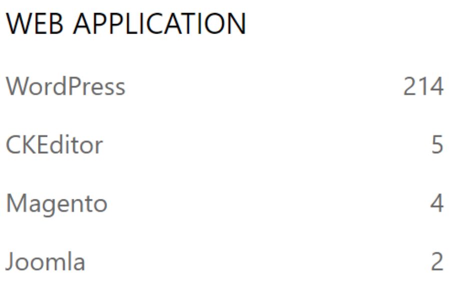


▲ Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

fig. 25 hostsg uses http protocol

Using a reverse IP lookup[16], we found that 214 WordPress websites are hosted on the same server as abc.com.sg. All the WordPress websites have the same vulnerabilities abc.com.sg and this presents more attack surfaces that hackers can target to access the server.



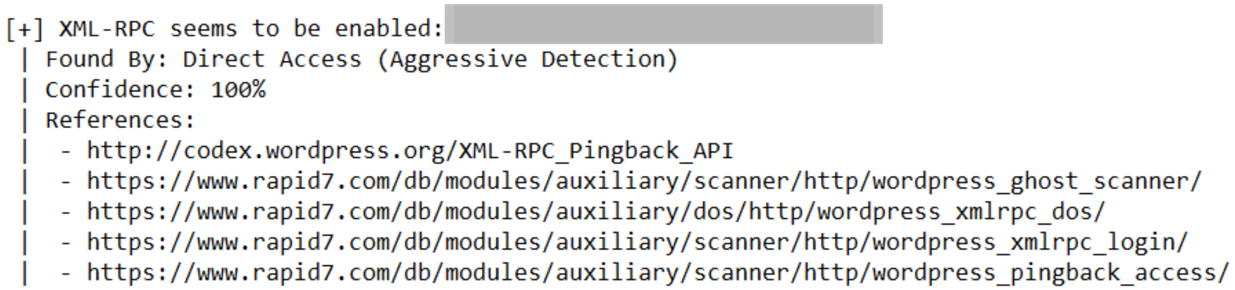
WEB APPLICATION	
WordPress	214
CKEditor	5
Magento	4
Joomla	2

fig. 26 hostsg server hosts 214 WordPress websites

[16] Links: https://hackertarget.com/reverse-ip-lookup/ & https://www.zoomeye.org/searchResult/report?q=203.175.174.67&t=web

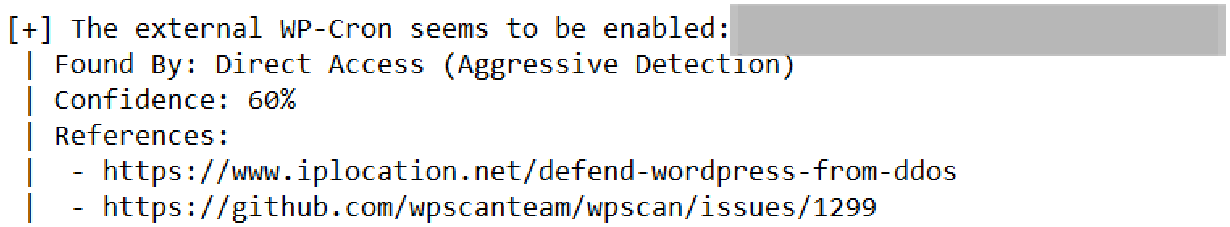
WordPress scan on abc.com.sg overview

After enumerating potential attack surfaces, we scanned for vulnerabilities. We first used WordPress scan[17] to scan for any WordPress related vulnerabilities. Through the scan, we found two vulnerable services, XML-RPC and WP-Cron are enabled.



```
[+] XML-RPC seems to be enabled: [redacted]
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/
```

fig. 27 XML-RPC is enabled



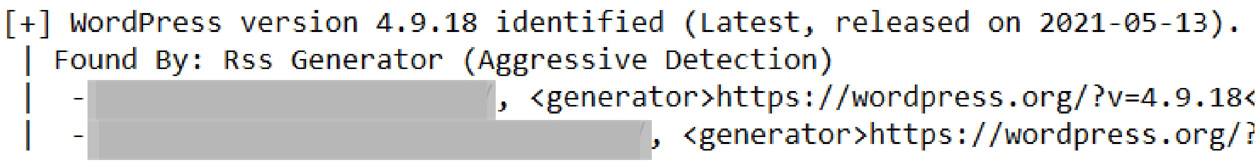
```
[+] The external WP-Cron seems to be enabled: [redacted]
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299
```

fig. 28 WP-Cron is enabled

[17] https://wpscan.com/wordpress-security-scanner

Privilege Escalation through XML-RPC (*Related vulnerability: Brute Force attack possible to login to WordPress website*)

The first vulnerability that is relevant to the features enabled is privilege escalation through XML-RPC (CVE-2020-28035[18]). This vulnerability is present for WordPress versions before 5.5.2 and the current version installed on abc.com.sg is 4.9.18.



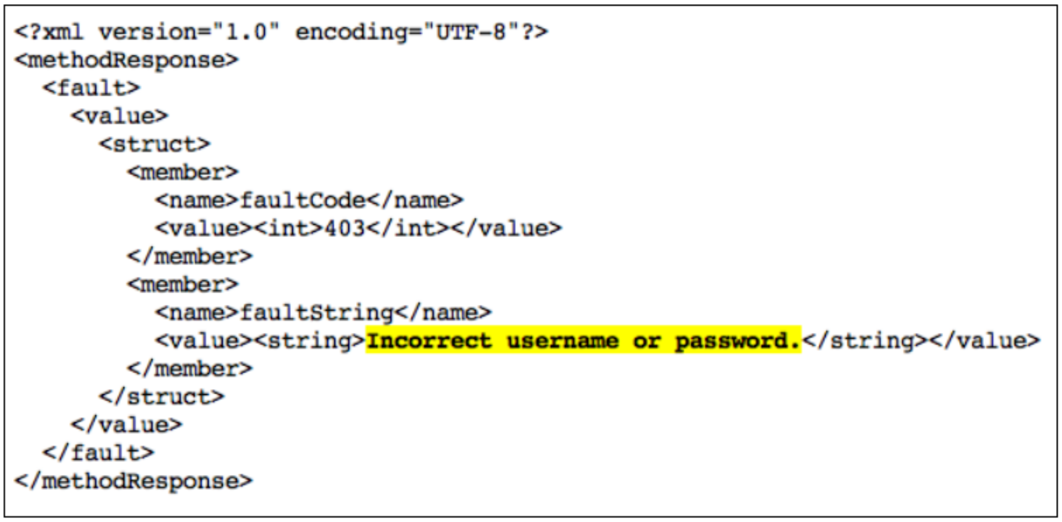
```
[+] WordPress version 4.9.18 identified (Latest, released on 2021-05-13).
 | Found By: Rss Generator (Aggressive Detection)
 |  - [redacted], <generator>https://wordpress.org/?v=4.9.18<
 |  - [redacted], <generator>https://wordpress.org/?
```

fig. 29 WordPress version 4.9.18 < 5.5.2

This feature enables POST requests to be made to the endpoint. If correct credentials are provided, data will be given back in response, else, the endpoint will respond with “Incorrect username or password”. This allows brute force attacks to test for the correct credentials through this endpoint. The following examples show example responses from the endpoint when correct and incorrect credentials are provided[19].

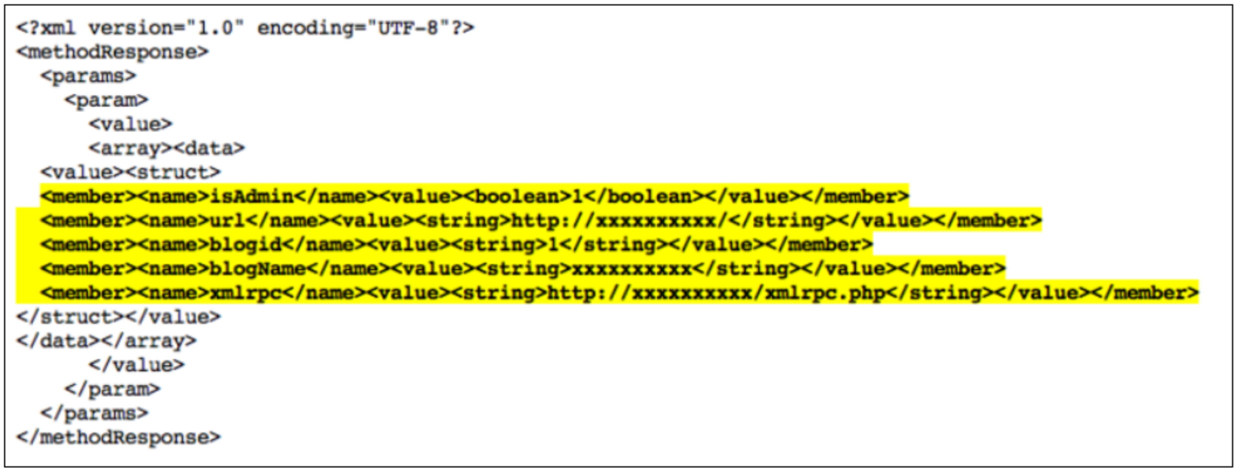
[18] https://nvd.nist.gov/vuln/detail/CVE-2020-28035

[19] Source: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/honeypot-alert-wordpress-xml-rpc-brute-force-scanning/



```
<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
  <fault>
    <value>
      <struct>
        <member>
          <name>faultCode</name>
          <value><int>403</int></value>
        </member>
        <member>
          <name>faultString</name>
          <value><string>Incorrect username or password.</string></value>
        </member>
      </struct>
    </value>
  </fault>
</methodResponse>
```

fig. 30 Incorrect username/password given



```
<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
  <params>
    <param>
      <value>
      <array><data>
  <value><struct>
  <member><name>isAdmin</name><value><boolean>1</boolean></value></member>
  <member><name>url</name><value><string>http://xxxxxxxxx/</string></value></member>
  <member><name>blogid</name><value><string>1</string></value></member>
  <member><name>blogName</name><value><string>xxxxxxxxx</string></value></member>
  <member><name>xmlrpc</name><value><string>http://xxxxxxxxx/xmlrpc.php</string></value></member>
</struct></value>
</data></array>
      </value>
    </param>
  </params>
</methodResponse>
```

fig. 31 Correct username/password given

Distributed Denial of Service through XML-RPC and WP-Cron (*Related vulnerability: Distributed Denial of Service (DDOS)*)

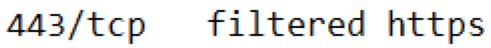
The second vulnerability that is relevant to the features enabled is Distributed Denial of Service (DDOS) through XML-RPC and WP-Cron. As mentioned above, the endpoint allows for POST requests to be sent to an endpoint. Hackers may use multiple servers to send POST requests simultaneously to the same endpoint, putting stress on the server. Additionally, this vulnerability is made worse as 214 vulnerable WordPress websites are hosted on the hostsg server, increasing the likelihood of a DDOS attack.

Additionally, wp-cron.php does not actually function like a typical cron job. Its default behaviour is to piggyback on incoming requests. Thus, WordPress generates an additional request from itself to the wp-cron file, doubling the number of requests to the server[20].

[20] https://medium.com/@thecpanelguy/the-nightmare-that-is-wpcron-php-ae31c1d3ae30

Nmap scan on hosting server overview

Finally, we ran an nmap scan on 203.175.174.67 that is the IP address of the server hosting abc.com.sg. While there are many open ports, the SMTP service was the only service that was vulnerable. An additional point of interest is that the https port is filtered, that explains why we could access http://abc.com.sg but not https://abc.com.sg.

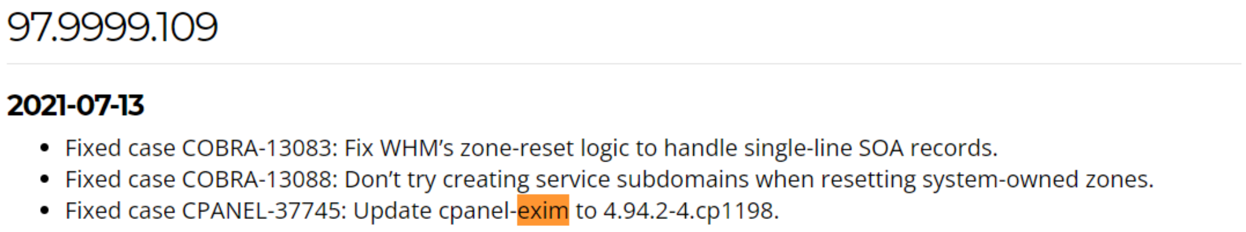


```
443/tcp   filtered https
```

fig. 32 port 443 (https) is filtered

Vulnerable SMTP service (*Related vulnerability: Email interception*)
The SMTP service uses Exim smtpd 4.94.2 and is open on ports 465, 587 and 1025. This version is vulnerable to response injection (buffering) during MTA SMTP sending (CVE-2021-38371[21]). Thankfully, the attack needs to be done on a local network and neither technical details nor an exploit are publicly available[22].

Additionally, the SMTP service is linked to the webmail.abc.com.sg domain. After searching through the cpanel changelogs, the latest version of cpanel is still using Exim smtpd 4.94.2[23]. This means that updating cpanel will not make a difference and users will have to ensure that they only send emails from the domain on trusted networks.



97.9999.109

2021-07-13

- Fixed case COBRA-13083: Fix WHM's zone-reset logic to handle single-line SOA records.
- Fixed case COBRA-13088: Don't try creating service subdomains when resetting system-owned zones.
- Fixed case CPANEL-37745: Update cpanel-exim to 4.94.2-4.cp1198.

fig. 33 cpanel still usesExim smtpd 4.94.2

[21] Link: https://nvd.nist.gov/vuln/detail/CVE-2021-38371
[22] Source: https://vuldb.com/?id.180505
[23] Source: https://docs.cpanel.net/changelogs/