[redacted]

Vulnerability Assessment

[redacted]

30th Nov 2021

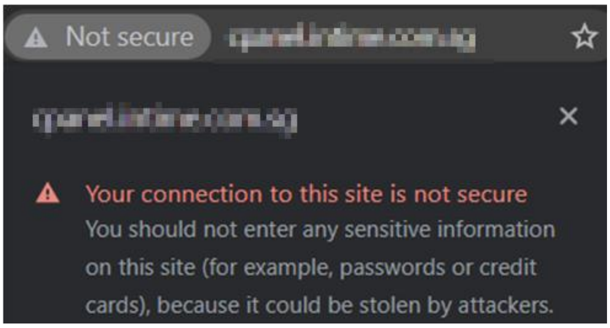
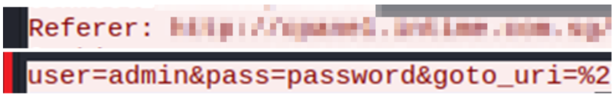
Content Page

Executive Summary

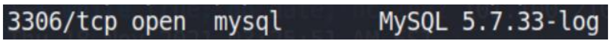
This report covers the results of a vulnerability assessment of ____________________’s website and the Company’s intranet firewall through the internet. In the assessment, a total of **five (5)** major vulnerabilities were discovered. The goal of this report is to explain these vulnerabilities, the impact of them (Table 1) and to provide recommendations on how to mitigate the issues. Further elaborations for consideration will be presented in our Appendix.

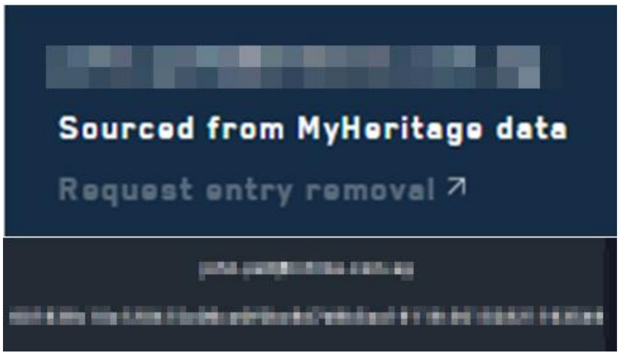
Table 1: Vulnerability & Potential Impact(s)

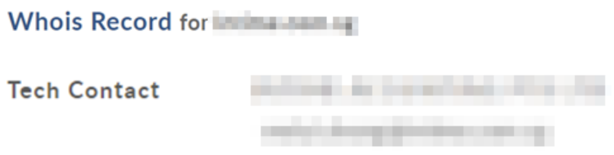
1	**Risk Level:** HIGH	
	Vulnerability: **cPanel vulnerable configuration**	
	Description	**Potential Impact(s)**

	Redirection of cPanel login page to Hypertext Transfer Protocol Secure (HTTPS) was not enabled
	
	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.
	We were able to capture the login credentials of a failed attempt in plain text format
	
	`Referer: [redacted]`
	`user=admin&pass=password&goto_uri=%2`
		Hackers may use the login username and password to access the Company’s website hosting server and intranet firewall to create, alter or remove crucial information.
		This can compromise both the strength of the firewall and the data within the Company’s website hosting server.

2	**Risk Level:** HIGH	
	Vulnerability:	**Wordpress site outdated plugin versions**
	Description	**Potential Impact(s)**
	(a) Unrestricted File Upload ● <u>Contact-form-7 (v 5.1.1)</u> Latest Version: 5.3.2 CVE: 2020-35489 (b) Authenticated Stored Cross-Site Scripting (XSS) ● <u>WPBakery Page Builder (v 4.3.5)</u> Latest Version: 6.4.1 CVE: 2020-28650 ● <u>Yoast SEO (Ver 11)</u> Latest Version: 11.6 CVE: 2019-13478 (c) Version Out-of-Date ● <u>Revslider (v 4.6.5)</u> Latest Version: 6.5.10	(a) Hackers can upload unlimited files onto the Company's Wordpress site to overload and crash the site. (b) Hackers can use Cross-Site Scripting (XSS) technique to inject malicious code to retrieve login usernames or passwords. (c) Hackers can edit the site database in plain sight.

3	**Risk Level:** HIGH	
	Vulnerability:	**Outdated MySQL, vulnerable unpatched version**
	Description	**Potential Impact(s)**
	 `3306/tcp open  mysql        MySQL 5.7.33-log` Current Version: 5.7.33 Latest Version: 8.0 CVE: 2021-3449, 2021-2384 & 2021-2307	The Company currently uses an outdated version of MySQL that contains an easily exploitable vulnerability. This allows unauthorised attackers to login into the Company's website hosting server to access and download confidential and/or restricted access data.

4	**Risk Level:** MEDIUM	
	Vulnerability:	**Employee’s company email address and password used on external website that was compromised in data breach**
	Description	**Potential Impact(s)**
	 [redacted] Sourced from MyHeritage data Request entry removal ↗ [redacted]	If this employee had subscribed to MyHeritage with the same email address and password as with the Company’s intranet server, it would be much easier for a hacker to use the same credentials to login and access the classified data. In future, if there are any similar incidents, it may cause other potential sources of compromise.

5	**Risk Level:** LOW	
	Vulnerability:	**Employee’s company email address used to register for website domain**
	Description	**Potential Impact(s)**
	 Whois Record for [redacted] Tech Contact [redacted] Our research found this user’s particulars, including her full company’s email address, listed in a publicly available IP-searching tool online.	Hackers may use this email to send spam or phishing emails (e.g. slightly altering their email address and sending emails to the firm’s clients or other key stakeholders) which may lead to more data breaches.

We recommend that the Company continuously update and patch their softwares (Wordpress plugins / mySQL version) to the next available stable versions so as to mitigate cybersecurity risks. In addition, enhanced cybersecurity training and regular briefings can be conducted to update employees on the latest market vulnerabilities. Subscriptions to relevant news forums to keep abreast of the latest cybersecurity threat, with quarterly quizzes to educate employees on how to safeguard against such vulnerabilities are beneficial as well. Our detailed recommendations will be elaborated under “Risk Assessment & Recommendations”.

Risk Assessment

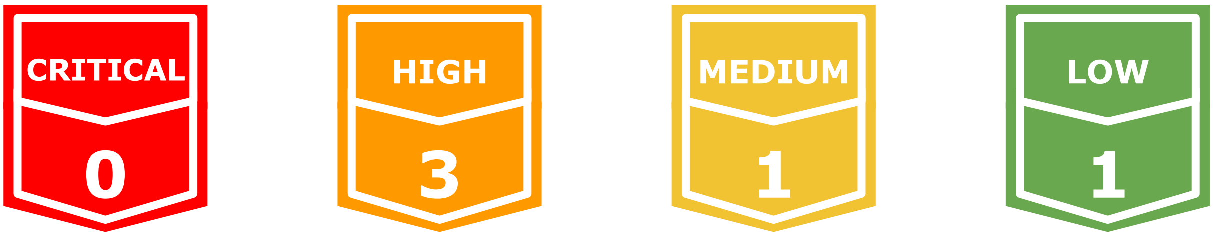
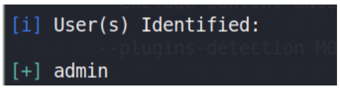


Diagram 1: Vulnerability risk level summary

We conducted the following assessments to find the Company’s vulnerability risk profile:

Category	**Type**
Reconnaissance	● Active scanning ● Gather victim host information ● Gather victim identity information ● Gather victim network information ● Gather victim organisation information ● Search open technical databases ● Search open websites/domains

Initial access	● Eg. admin username for Company's Wordpress site
	
	`[i] User(s) Identified:`
	`[+] admin`

Execution	● Command and scripting interpreter ● Exploitation for Client Execution (attempted)
Defense evasion	● Eg. slow scan to prevent detection
Credential Access	-

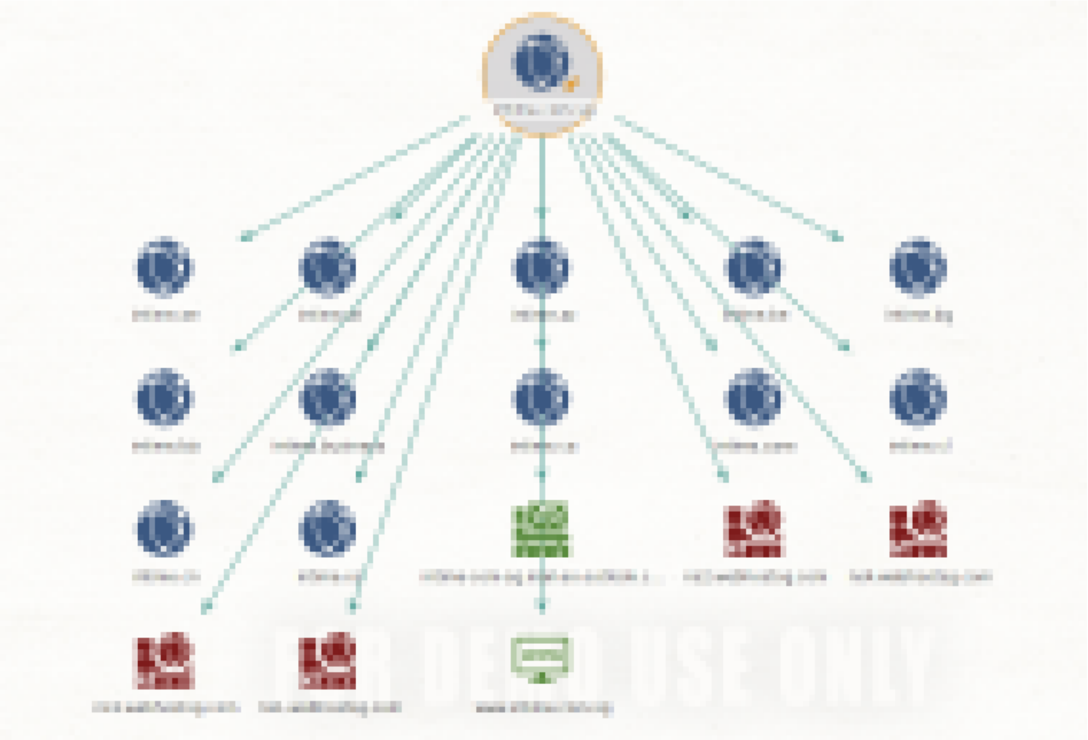
Recommendations

In this section, we will elaborate on the respective recommendations of each vulnerability.

No.	Vulnerability	Recommendation
1	HIGH **cPanel: Vulnerable configuration**	● Enable Force HTTPS Redirection from the insecure version (HTTP) to the secure version (HTTPS) with a toggle switch. (https://blog.cpanel.com/force-https-redirection/) The data transferred back and forth between the end-user and the site will be encrypted and not be in plain text. Encryption improves security by making it more difficult for hackers to decode and access information. Websites using HTTPS would get a slight ranking factor boost in searches using the search engine. (Google Analytics) Additionally, the newer HTTP/2 protocol has proven to perform faster than the standard HTTP but requires HTTPS for browser support.
2	HIGH **Wordpress site: Outdated plugin versions**	● Regularly check for the latest patch updates and install latest plugin versions. New patch(es) usually negates vulnerabilities in past versions and this can better safeguard the data on the Wordpress site because most web developers will consistently improve their plugins by adding new features, improving code quality, and keeping plugins secure. Users are advised to keep their Wordpress plugins up to date to ensure that those changes are applied on their site immediately. This improves Wordpress security and performance of their website. ● To perform manual patch updates instead of automatic updates to ensure that new patch/versions are compatible with existing systems to avoid system failures.
3	HIGH **MySQL: Outdated, vulnerable unpatched version**	● Constant monitoring of third-party access to data with regular checks for the latest patch updates Softwares are regularly updated to prevent hackers from utilizing its flaws and weaknesses. Not only do updates make software function better, they also strive to be more secure. Thus, updating to the next stable version can save users from future troubles. ● Conducting regular backups to your data management systems. Loss of data can lead to high recovery costs. Conducting regular backups can minimise the extent of data that needs to be retrieved if data is lost in a breach.

		- Save duplicate backup copies on different systems. The rapid evolvements in cybersecurity means that updated patch versions may potentially be jeopardized in the future. Having additional backup copies can reduce the impact of such data loss because if one of the systems is compromised, you have alternatives to fall back on and the extent of data recovery loss is ameliorated
4	MEDIUM **Employee's company email address and passwords used on external website that was compromised in data breach**	- Reset Password. We would advise the employee to reset the MyHeritage account password to a more secure password (e.g. with 2FA) or one that is unique (use different passwords across sites) and complex (a mix of numbers, symbols, uppercase and lowercase letters). - Use Password Manager. If there is a tendency to reuse passwords, a password manager can help to create a unique password for each site on which the employee is subscribed. - Check email spam settings. As exposed emails can be more susceptible to malware or phishing spam, a good cautionary practice is for employees to check their email settings and see if there is anything amiss.
5	LOW **Employee's company email address used to register for website domain**	- Employees can be more discreet when registering for a domain by using an email alias (e.g. it@______). This separates their own email from the domain registered email, making it difficult for hackers to ascertain all their personal/professional information.

Company Network Profile



__________________ is a multinational corporation with many subdirectories in each country it operates in. For the purpose of this vulnerability assessment, only the Singapore branch is analysed.

Conclusion

In conclusion, the Company's current security posture is relatively good. Our assessment found only two email addresses that were compromised. This shows that most employees have an adequate amount of cybersecurity awareness. We also attempted to access their firewall, which is hosted on SonicWall, but was unsuccessful. With an organised effort, however, a dedicated penetration testing team may be able to access it.

As an accounting firm, a data leak can lead to immense liability where clients' confidential information may be compromised, exposed or stolen for unethical uses. With these vulnerabilities identified in the Company, attackers can infiltrate the Company's servers using leaked employee account IDs, emails and passwords to access customers' confidential data (eg. financial statements, excel sheets, invoices) and create, amend or delete such data. While loss of data can be mitigated with backup copies, the loss of clients' confidence will potentially result in a loss of reputation, sales and revenue for _______________. Besides incurring monetary costs to reinstate lost, destroyed or doctored data, the firm may also incur additional costs to strengthen its existing cyber security policies and infrastructure. Consequently, crucial daily operations may be stymied during a data breach and the time taken to resume normal operations may inconvenience many employees and clients that need to abide by accounting timelines set by MAS.

Taking into consideration the Company's security profile, we propose the adoption of various strategies, as put forward in the Recommendations section, to counter the threat of cyber attacks. We are cognizant that every company is different and therefore, these recommendations have been tailored to suit the specific security needs of the Company. These will help the Company improve and take preventive measures to avoid detrimental outcomes of vulnerabilities found in our assessment.

Appendix

Our Appendix will include the following:-

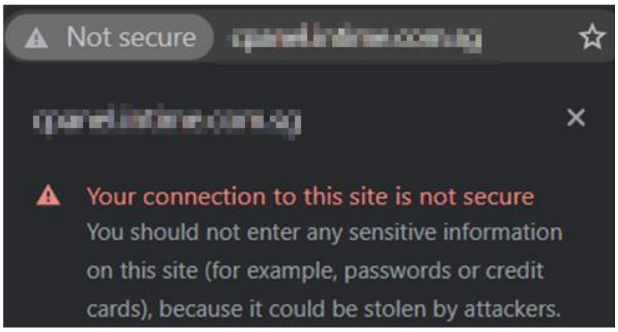
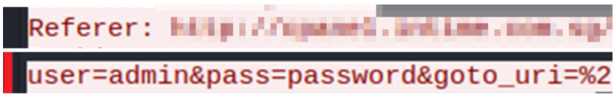
1. Screenshots showing the results of the scans we conducted on the Company's website and Company's intranet firewall through the internet; and
2. Other information that we found through methods of Reconnaissance, Initial access, Execution, Defense evasion and Credential Access.

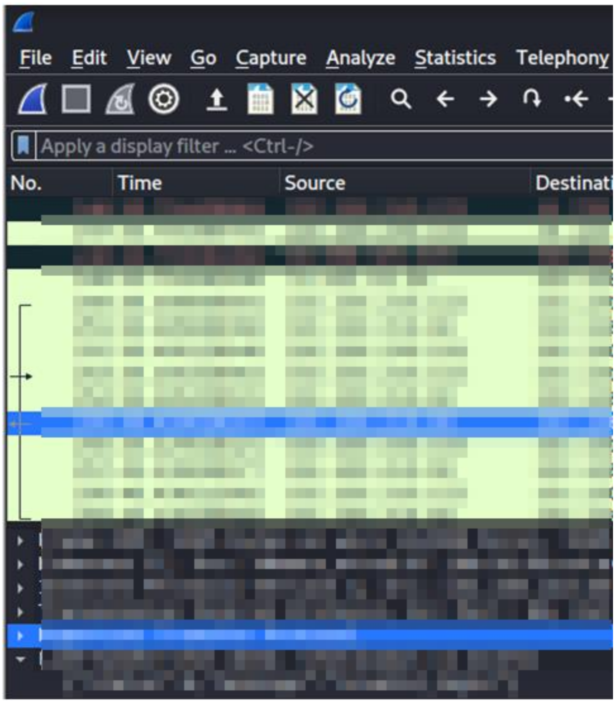
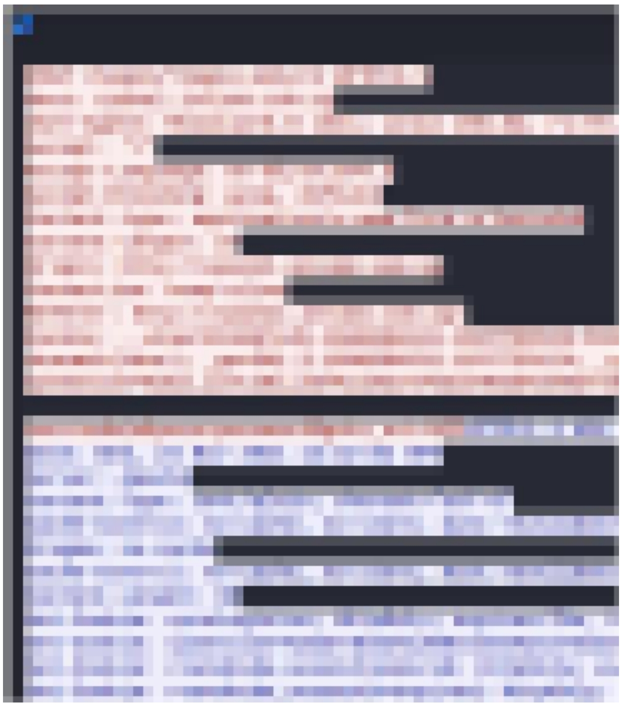
Appendix 1: cPanel

We accessed cpanel.____________ and discovered that it does not redirect to HTTPS.

HIGH

A vulnerable cPanel configuration

Vulnerability	Description
 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.	Redirection of cPanel login page to Hypertext transfer protocol secure (HTTPS) was not enabled.
 Referer: [redacted] user=admin&pass=password&goto_uri=%2	We were able to capture the login credentials of a failed attempt in plain text format.

 File Edit View Go Capture Analyze Statistics Telephony Apply a display filter ... <Ctrl-/> No. Time Source Destinati [redacted]	 [redacted]

Appendix 2: wpscan

We managed to retrieve the existing plugins used on the Company's Wordpress site that were vulnerable. (code: wpscan --url https://__________ -e u vps)

Hackers may also masquerade as the victim user and carry out any action that the user is able to perform. They may perform virtual defacement of the website and even inject trojan functionality into the web site, rendering the website to more vulnerabilities and viruses.

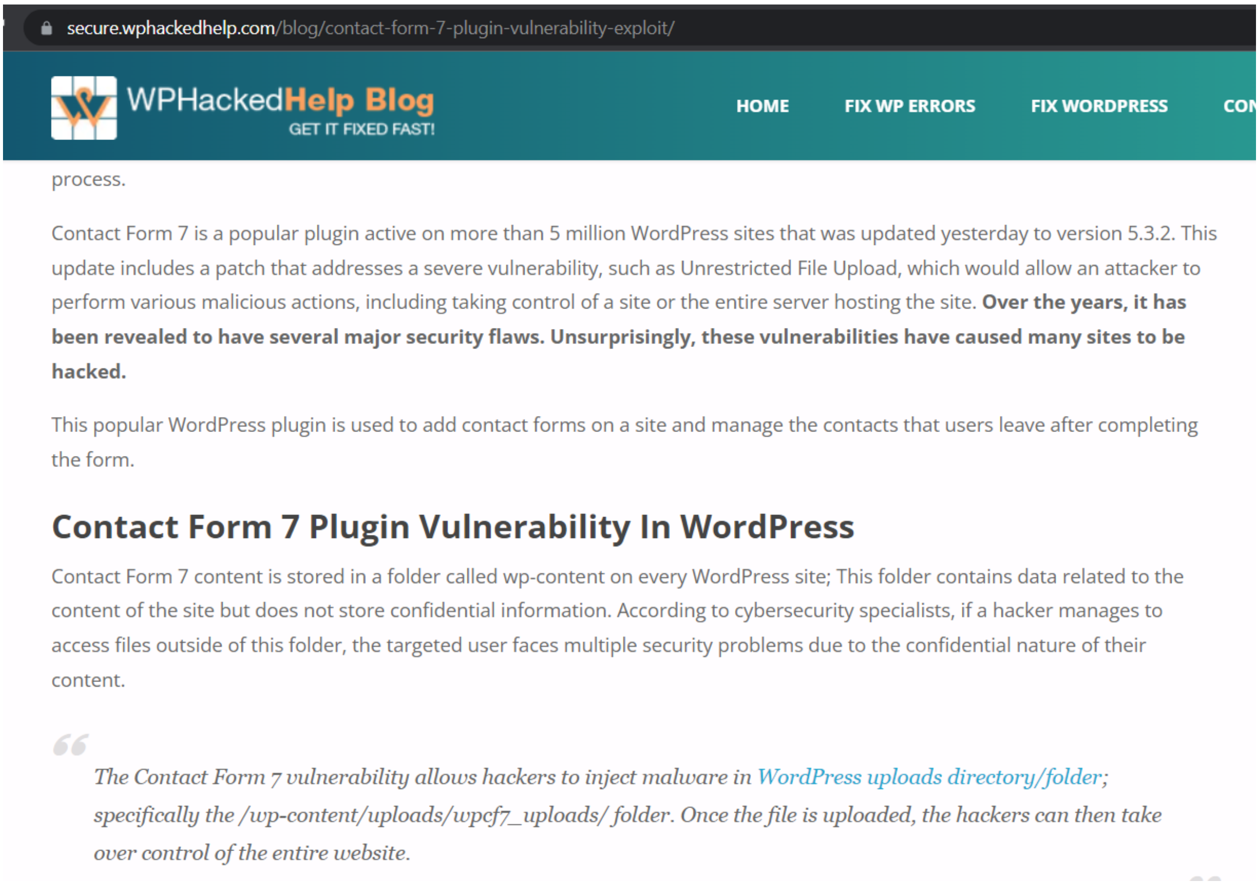
HIGH Outdated plugins on the Company's Wordpress site

No.	Vulnerability	Plugin / Version	Latest Version	CVE
1	Unrestricted File Upload	Contact-form-7 / 5.1.1	5.3.2	CVE-2020-35489
2	Authenticated Stored Cross-Site Scripting (XSS)	WPBakery Page Builder / 4.3.5	6.4.1	CVE-2020-28650
3	Authenticated Stored Cross-Site Scripting (XSS)	Yoast SEO / 11	11.6	CVE-2019-13478
4	Version Out-of-Date	Revslider / 4.6.5	6.5.10	Nil

Detailed list of the Wordpress plugin(s) Identified:-

```
[+] contact-form-7
 | Location: https://__________/wp-content/plugins/contact-form-7/
 | Last Updated: 2021-10-25T04:38:00.000Z
 | [!] The version is out of date, the latest version is 5.5.2
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: Contact Form 7 < 5.3.2 - Unrestricted File Upload
 |     Fixed in: 5.3.2
 |     References:
 |      - https://wpscan.com/vulnerability/7391118e-eef5-4ff8-a8ea-f6b65f442c63
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-35489
 |      - https://www.getastra.com/blog/911/plugin-exploit/contact-form-7-unrestricted-file-upload-vulnerability/
 |      - https://www.jinsonvarghese.com/unrestricted-file-upload-in-contact-form-7/
 |      - https://contactform7.com/2020/12/17/contact-form-7-532/#more-38314
 |

 | Version: 5.1.1 (20% confidence)
 | Found By: Query Parameter (Passive Detection)
 |  - https://_________/wp-content/plugins/contact-form-7/includes/css/styles.css?ver=5.1.1
 |  - https://_________/wp-content/plugins/contact-form-7/includes/js/scripts.js?ver=5.1.1

[+] js_composer
 | Location: https://__________/wp-content/plugins/js_composer/
 | Last Updated: 2021-07-07T11:50:24.000Z
 | [!] The version is out of date, the latest version is 6.7.0
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By:
 |  Meta Generator (Passive Detection)
 |  Body Tag (Passive Detection)
 |
 | [!] 2 vulnerabilities identified:
 |
 | [!] Title: WPBakery Page Builder < 4.7.4 - Multiple Unspecified Cross-Site Scripting (XSS)
 |     Fixed in: 4.7.4
 |     References:
 |      - https://wpscan.com/vulnerability/8c8bff1c-6d45-4673-bdbc-1ea199a43c4b
 |      - https://codecanyon.net/item/visual-composer-page-builder-for-wordpress/242431
 |      - https://forums.envato.com/t/visual-composer-security-vulnerability-fix/10494/7
 |
 | [!] Title: WPBakery Page Builder < 6.4.1 - Authenticated Stored Cross-Site Scripting (XSS)
 |     Fixed in: 6.4.1
 |     References:
 |      - https://wpscan.com/vulnerability/11285589-1b22-4ec0-adfc-f2add70db4d7
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28650
 |      - https://www.wordfence.com/blog/2020/10/vulnerability-exposes-over-4-million-sites-using-wpbakery/
 |
 | Version: 4.3.5 (60% confidence)
 | Found By: Body Tag (Passive Detection)
 |  - https://__________/, Match: 'js-comp-ver-4.3.5'

[+] revslider
 | Location: https//_________/wp-content/plugins/revslider/
 | Last Updated: 2021-11-16T14:31:25.000Z
 | [!] The version is out of date, the latest version is 6.5.10
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Comment (Passive Detection)
 |
 | Version: 4.6.5 (60% confidence)
 | Found By: Comment (Passive Detection)
 |  - https://__________/, Match: 'START REVOLUTION SLIDER 4.6.5'

[+] wordpress-seo
 | Location: https://__________/wp-content/plugins/wordpress-seo/
 | Last Updated: 2021-11-16T09:01:00.000Z
 | [!] The version is out of date, the latest version is 17.6
 |
 | Found By: Comment (Passive Detection)
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title:  Yoast SEO 1.2.0-11.5 - Authenticated Stored XSS
 |     Fixed in: 11.6
 |     References:
 |      - https://wpscan.com/vulnerability/8bc4cf95-79f7-4d92-b320-a841ab7e6a6f
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13478
 |      - https://gist.github.com/sybrew/2f53625104ee013d2f599ac254f635ee
 |      - https://github.com/Yoast/wordpress-seo/pull/13221
 |      - https://yoast.com/yoast-seo-11.6/
 |
 |      Version: 11.0 (60% confidence)
 |      Found By: Comment (Passive Detection)
 |      - https://_______________/, Match: 'optimized with the Yoast SEO plugin v11.0 -'
```

Evidences of exploited plugins:


secure.wphackedhelp.com/blog/contact-form-7-plugin-vulnerability-exploit/
WPHackedHelp Blog
GET IT FIXED FAST!
HOME
FIX WP ERRORS
FIX WORDPRESS
CON

process.

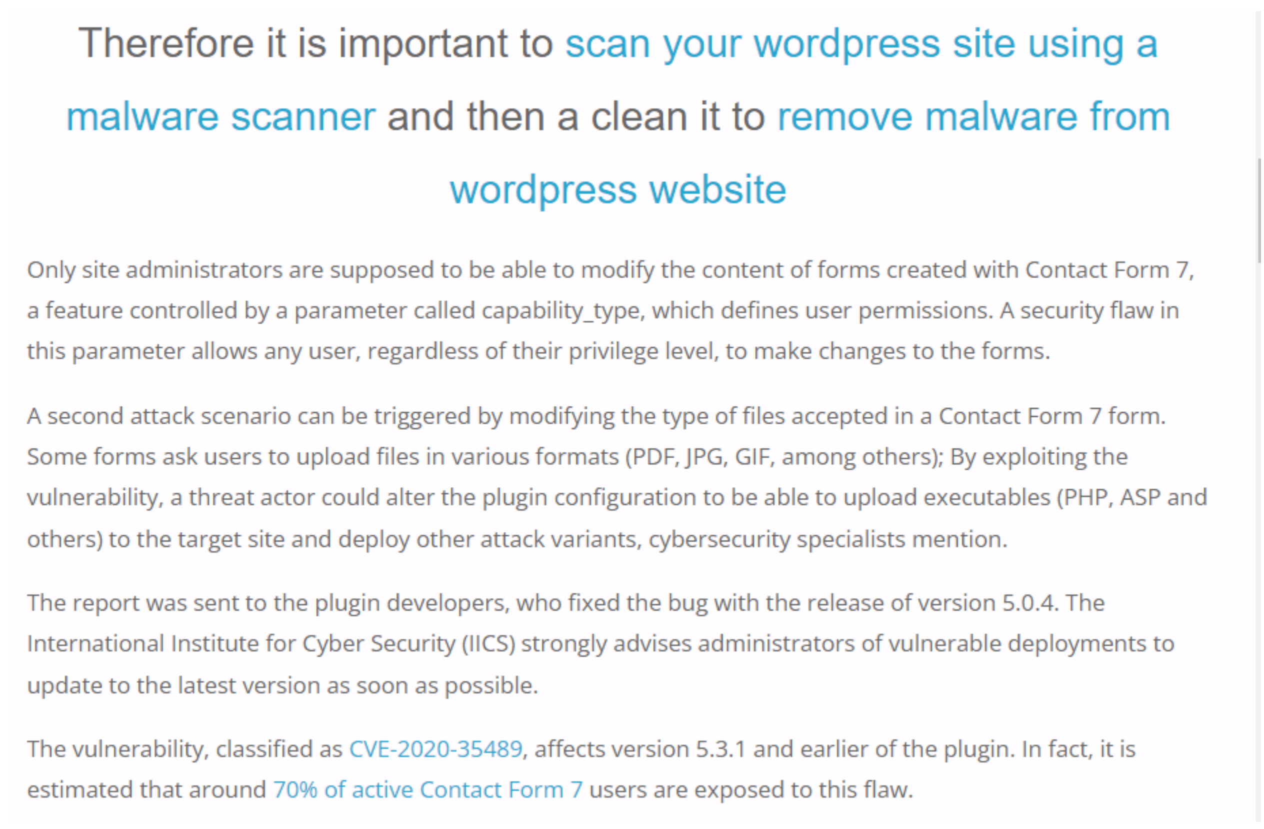
Contact Form 7 is a popular plugin active on more than 5 million WordPress sites that was updated yesterday to version 5.3.2. This update includes a patch that addresses a severe vulnerability, such as Unrestricted File Upload, which would allow an attacker to perform various malicious actions, including taking control of a site or the entire server hosting the site. **Over the years, it has been revealed to have several major security flaws. Unsurprisingly, these vulnerabilities have caused many sites to be hacked.**

This popular WordPress plugin is used to add contact forms on a site and manage the contacts that users leave after completing the form.

Contact Form 7 Plugin Vulnerability In WordPress

Contact Form 7 content is stored in a folder called wp-content on every WordPress site; This folder contains data related to the content of the site but does not store confidential information. According to cybersecurity specialists, if a hacker manages to access files outside of this folder, the targeted user faces multiple security problems due to the confidential nature of their content.

> *The Contact Form 7 vulnerability allows hackers to inject malware in WordPress uploads directory/folder; specifically the /wp-content/uploads/wpcf7_uploads/ folder. Once the file is uploaded, the hackers can then take over control of the entire website.*



Therefore it is important to scan your wordpress site using a malware scanner and then a clean it to remove malware from wordpress website

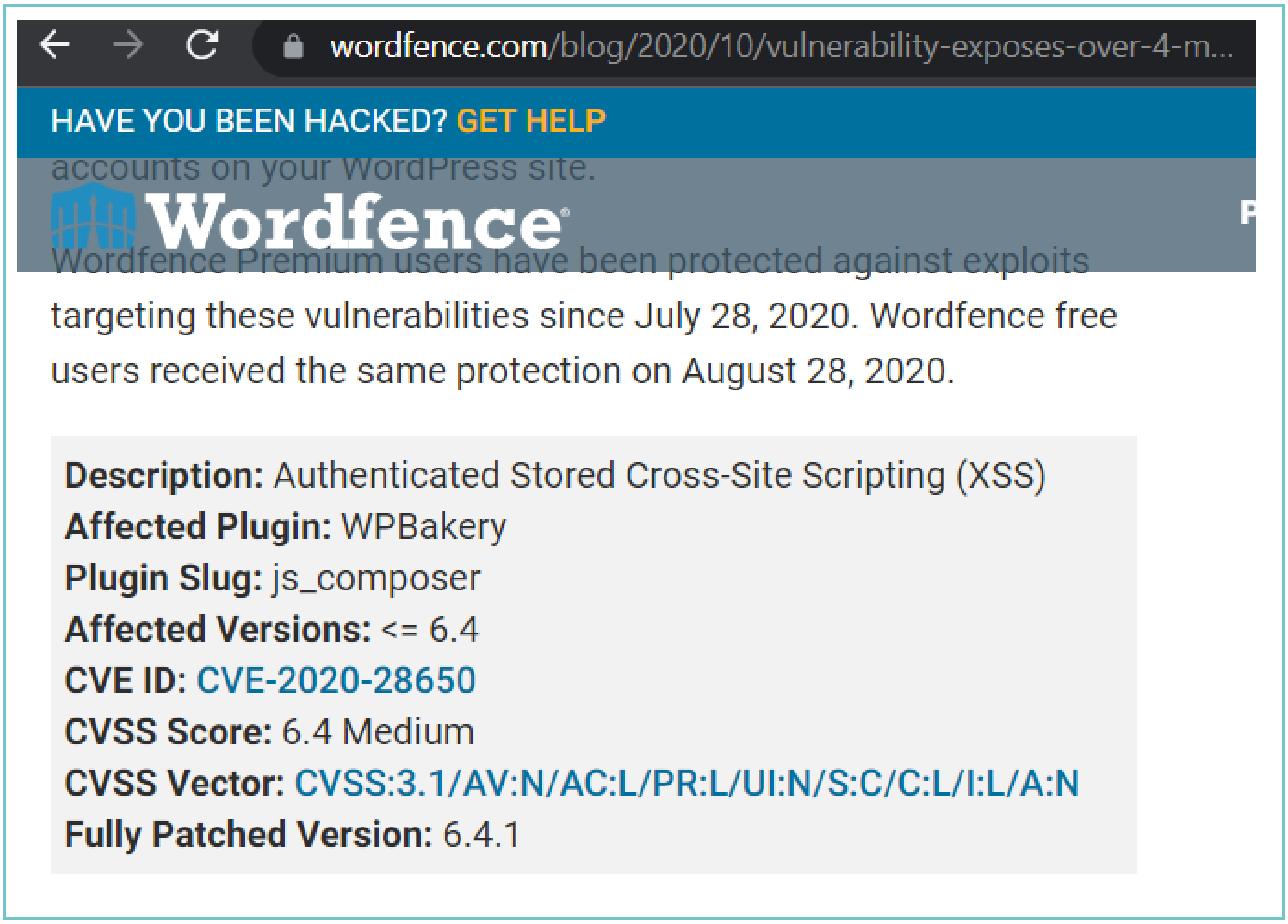
Only site administrators are supposed to be able to modify the content of forms created with Contact Form 7, a feature controlled by a parameter called capability_type, which defines user permissions. A security flaw in this parameter allows any user, regardless of their privilege level, to make changes to the forms.

A second attack scenario can be triggered by modifying the type of files accepted in a Contact Form 7 form. Some forms ask users to upload files in various formats (PDF, JPG, GIF, among others); By exploiting the vulnerability, a threat actor could alter the plugin configuration to be able to upload executables (PHP, ASP and others) to the target site and deploy other attack variants, cybersecurity specialists mention.

The report was sent to the plugin developers, who fixed the bug with the release of version 5.0.4. The International Institute for Cyber Security (IICS) strongly advises administrators of vulnerable deployments to update to the latest version as soon as possible.

The vulnerability, classified as CVE-2020-35489, affects version 5.3.1 and earlier of the plugin. In fact, it is estimated that around 70% of active Contact Form 7 users are exposed to this flaw.

https://secure.wphackedhelp.com/blog/contact-form-7-plugin-vulnerability-exploit/



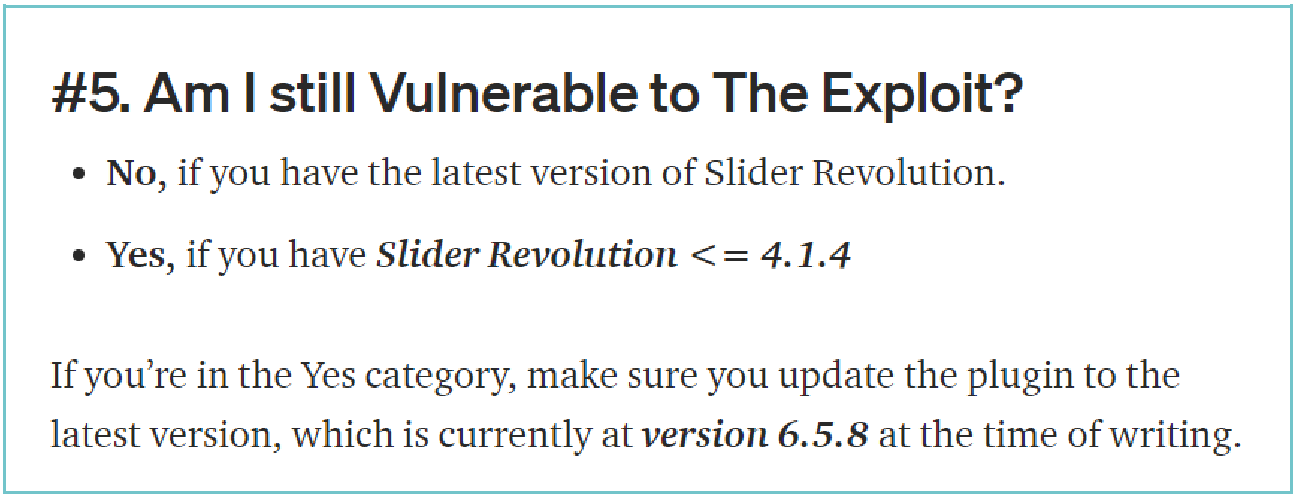
wordfence.com/blog/2020/10/vulnerability-exposes-over-4-m...
HAVE YOU BEEN HACKED? GET HELP
Wordfence

accounts on your WordPress site.

Wordfence Premium users have been protected against exploits targeting these vulnerabilities since July 28, 2020. Wordfence free users received the same protection on August 28, 2020.

Description: Authenticated Stored Cross-Site Scripting (XSS)
Affected Plugin: WPBakery
Plugin Slug: js_composer
Affected Versions: <= 6.4
CVE ID: CVE-2020-28650
CVSS Score: 6.4 Medium
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
Fully Patched Version: 6.4.1

https://www.wordfence.com/blog/2020/10/vulnerability-exposes-over-4-million-sites-using-wpbakery/

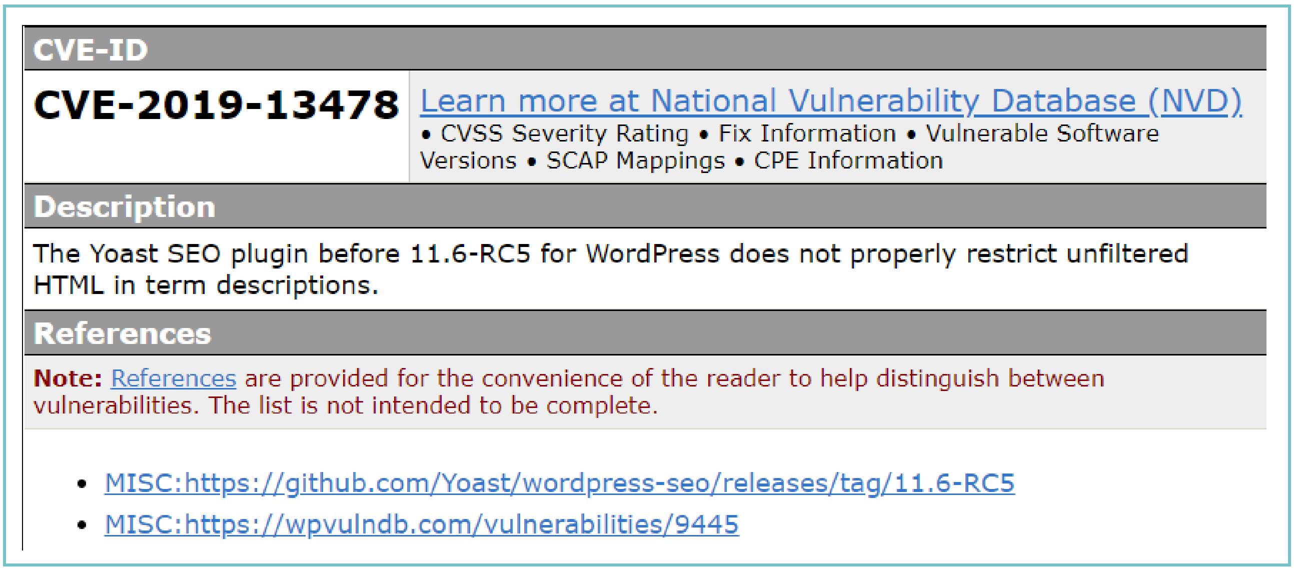


#5. Am I still Vulnerable to The Exploit?

- **No,** if you have the latest version of Slider Revolution.
- **Yes,** if you have ***Slider Revolution <= 4.1.4***

If you're in the Yes category, make sure you update the plugin to the latest version, which is currently at ***version 6.5.8*** at the time of writing.

https://stevemats.medium.com/revslider-plugin-exploit-the-imperceptible-earthquake-that-shook-wp-kingdom-2ca1289b5865



CVE-ID	
CVE-2019-13478	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

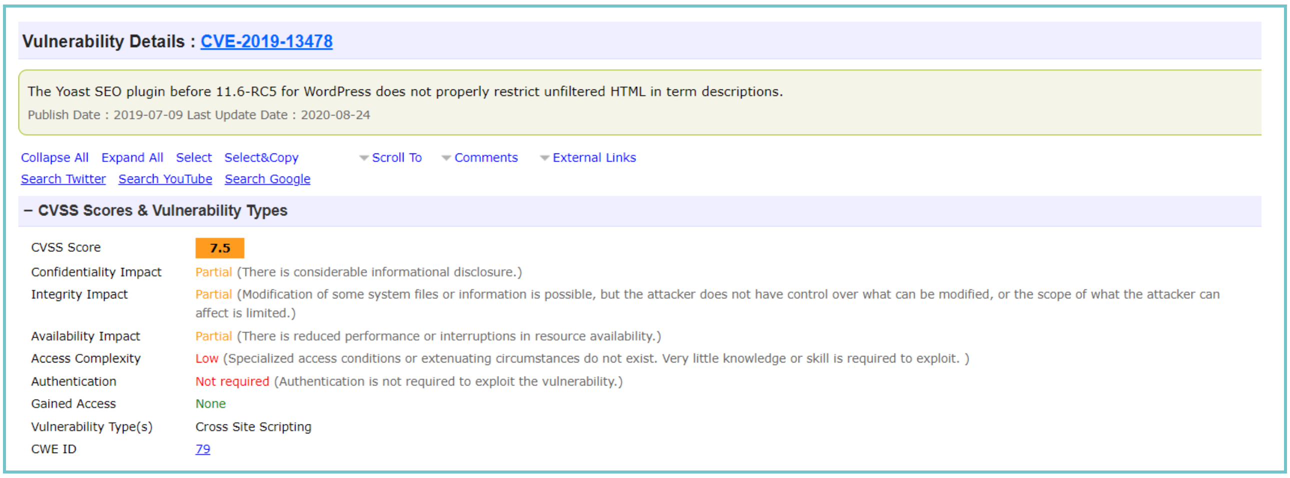
The Yoast SEO plugin before 11.6-RC5 for WordPress does not properly restrict unfiltered HTML in term descriptions.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://github.com/Yoast/wordpress-seo/releases/tag/11.6-RC5
- MISC:https://wpvulndb.com/vulnerabilities/9445

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13478



Vulnerability Details : CVE-2019-13478

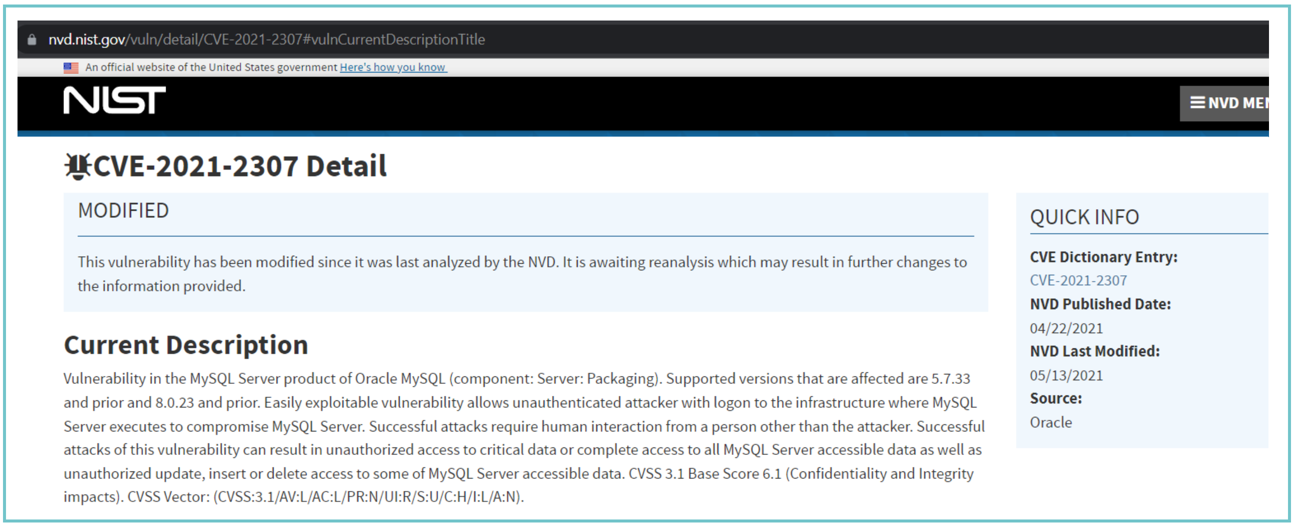
The Yoast SEO plugin before 11.6-RC5 for WordPress does not properly restrict unfiltered HTML in term descriptions.

Publish Date : 2019-07-09 Last Update Date : 2020-08-24

− CVSS Scores & Vulnerability Types

CVSS Score	7.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Cross Site Scripting
CWE ID	79

https://www.cvedetails.com/cve/CVE-2019-13478/



nvd.nist.gov/vuln/detail/CVE-2021-2307#vulnCurrentDescriptionTitle
An official website of the United States government Here's how you know
NIST
≡ NVD MEI

CVE-2021-2307 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Packaging). Supported versions that are affected are 5.7.33 and prior and 8.0.23 and prior. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N).

QUICK INFO

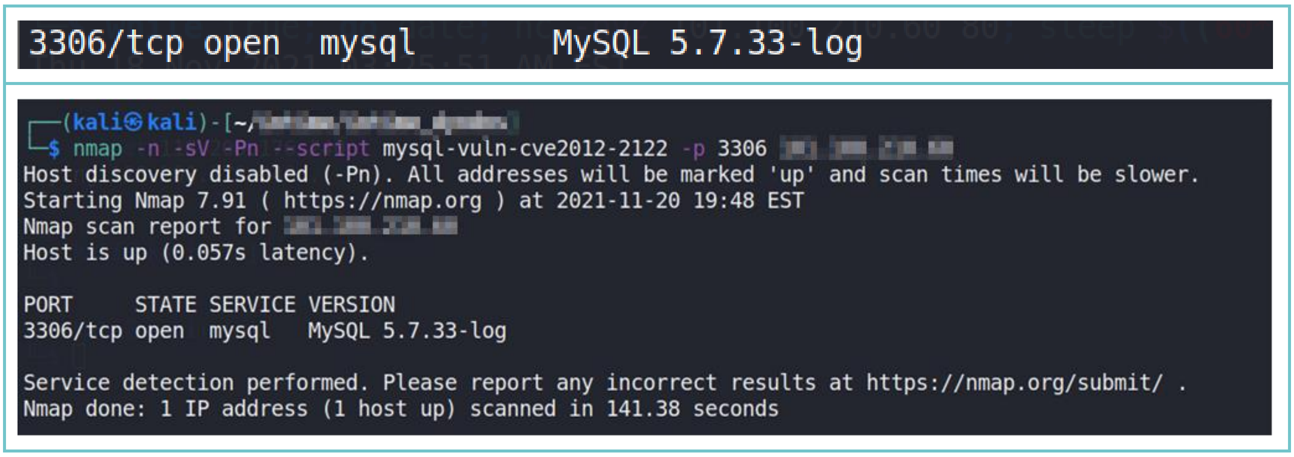
CVE Dictionary Entry:
CVE-2021-2307
NVD Published Date:
04/22/2021
NVD Last Modified:
05/13/2021
Source:
Oracle

https://nvd.nist.gov/vuln/detail/CVE-2021-2307#vulnCurrentDescriptionTitle

Appendix 3: Nmap scan showing MySQL port number and version details

We managed to identify that the Company’s website hosting server is currently using MySQL service. (code: nmap -n -sV -Pn --script mysql-vuln-cve2012-2122 -p 3306 _____________)

We discovered that TCP port 3306 is used for MySQL and the version is 5.7.33-log (screenshot below)



```
3306/tcp open  mysql      MySQL 5.7.33-log
```

```
┌──(kali㉿kali)-[~/[redacted]]
└─$ nmap -n -sV -Pn --script mysql-vuln-cve2012-2122 -p 3306 [redacted]
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-20 19:48 EST
Nmap scan report for [redacted]
Host is up (0.057s latency).

PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.7.33-log

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 141.38 seconds
```

HIGH

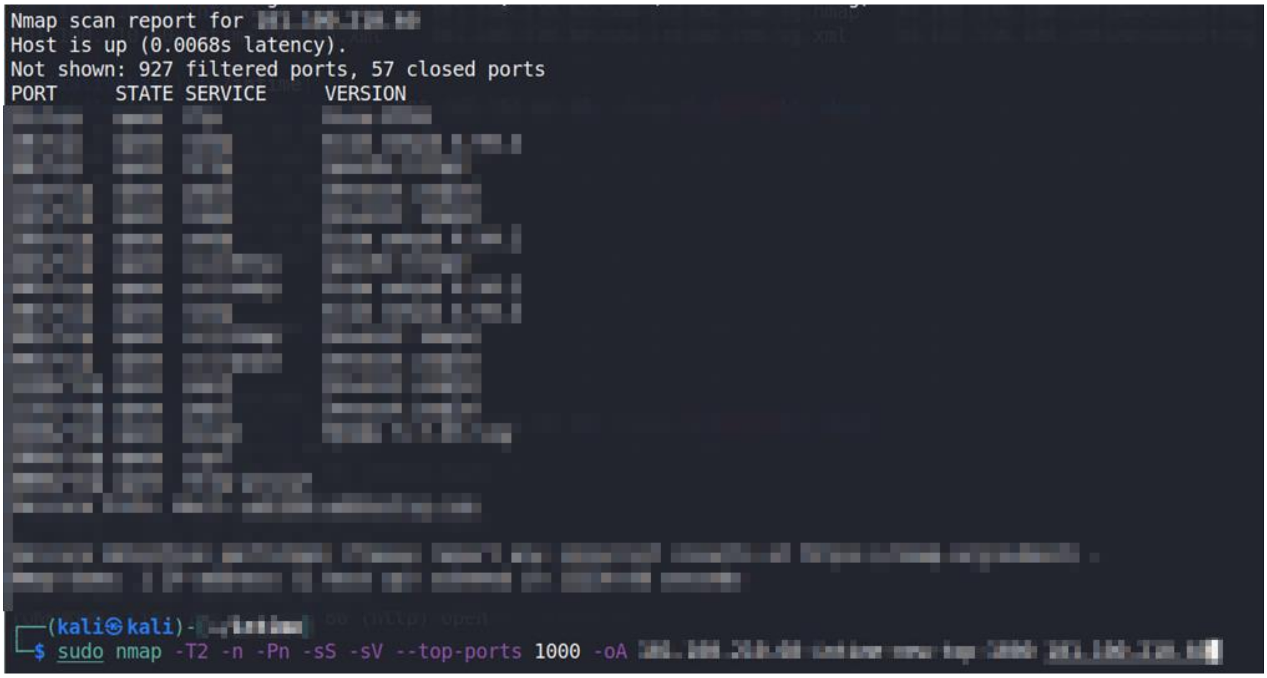
Utilization of an older, vulnerable version of MySQL

Vulnerability	Current Version	Latest Update	CVE
Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. Supported versions that are affected are 5.7.33 and prior.	5.7.33	April 2021 Critical Patch Update	CVE-2021-3449 CVE-2021-2384 CVE-2021-2307

Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data as well as unauthorized update, insert or delete access to some of MySQL Server accessible data

The link at **https://www.oracle.com/security-alerts/cpuapr2021.html** can be used to read and understand more about the vulnerabilities in this version.

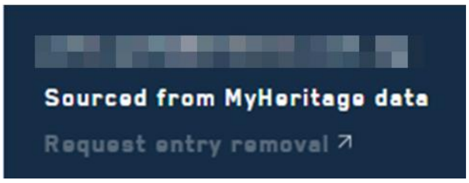
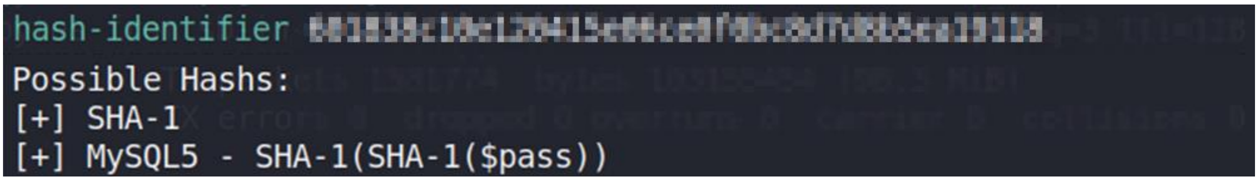
Appendix 4: Nmap scan report showing all the open Ports with respective services & versions (code: nmap -T2 -n -Pn -sS -sV --top-ports 1000 ___________)



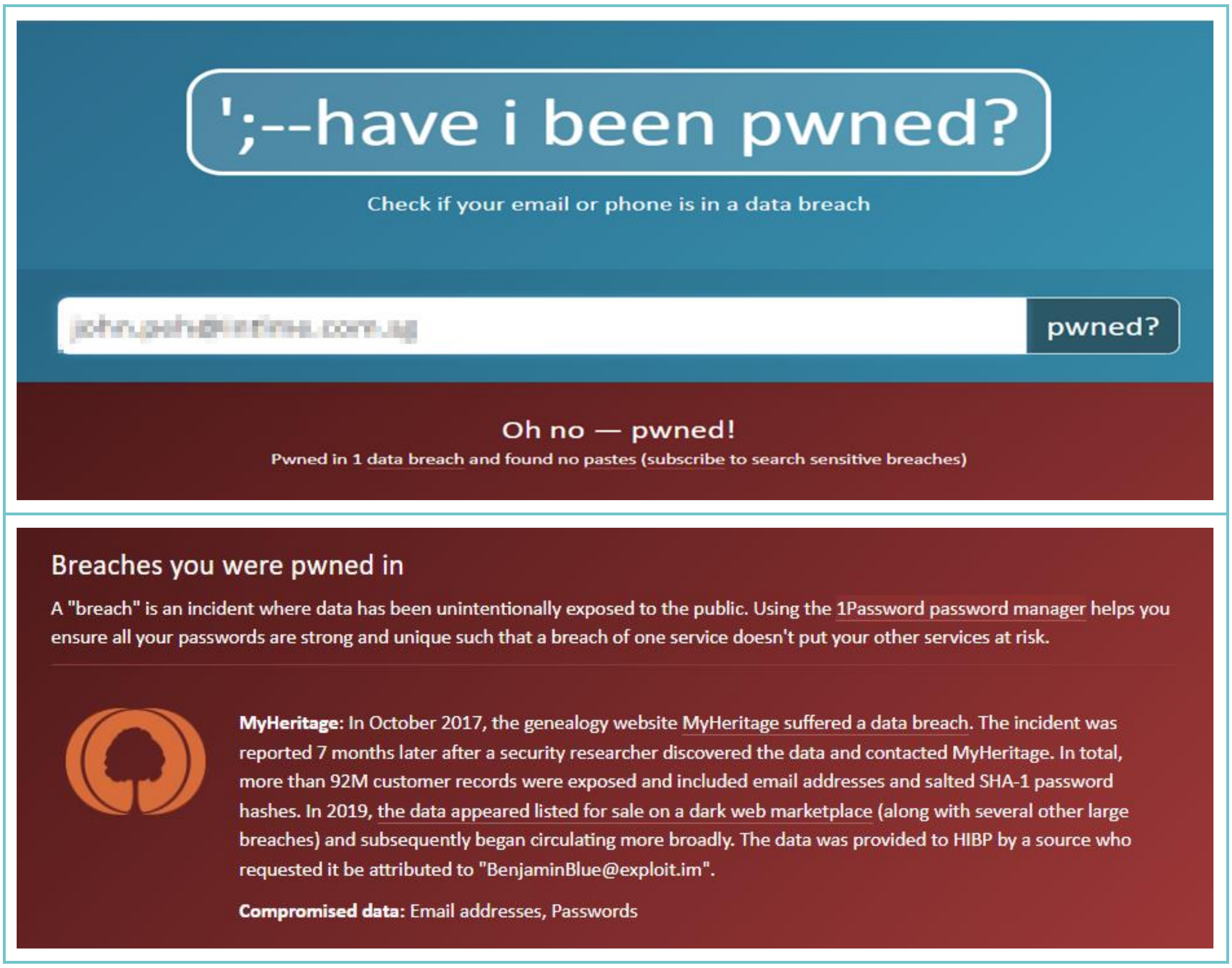
```
Nmap scan report for [redacted]
Host is up (0.0068s latency).
Not shown: 927 filtered ports, 57 closed ports
PORT     STATE SERVICE     VERSION
[redacted]

┌──(kali㉿kali)-[redacted]
└─$ sudo nmap -T2 -n -Pn -sS -sV --top-ports 1000 -oA [redacted]
```

Appendix 5: To check email leaks

MEDIUM **An employee's company email address being used by an external website that was compromised in a data breach**

MyHeritage	Leaked Hashed Password
 [redacted] Sourced from MyHeritage data Request entry removal ↗	 [redacted] [redacted]
 hash-identifier [redacted] Possible Hashs: [+] SHA-1 [+] MySQL5 - SHA-1(SHA-1($pass))	

Result #__________	
Email	___________@____________
Hashed Password	____



[redacted]

Oh no — pwned!
Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)

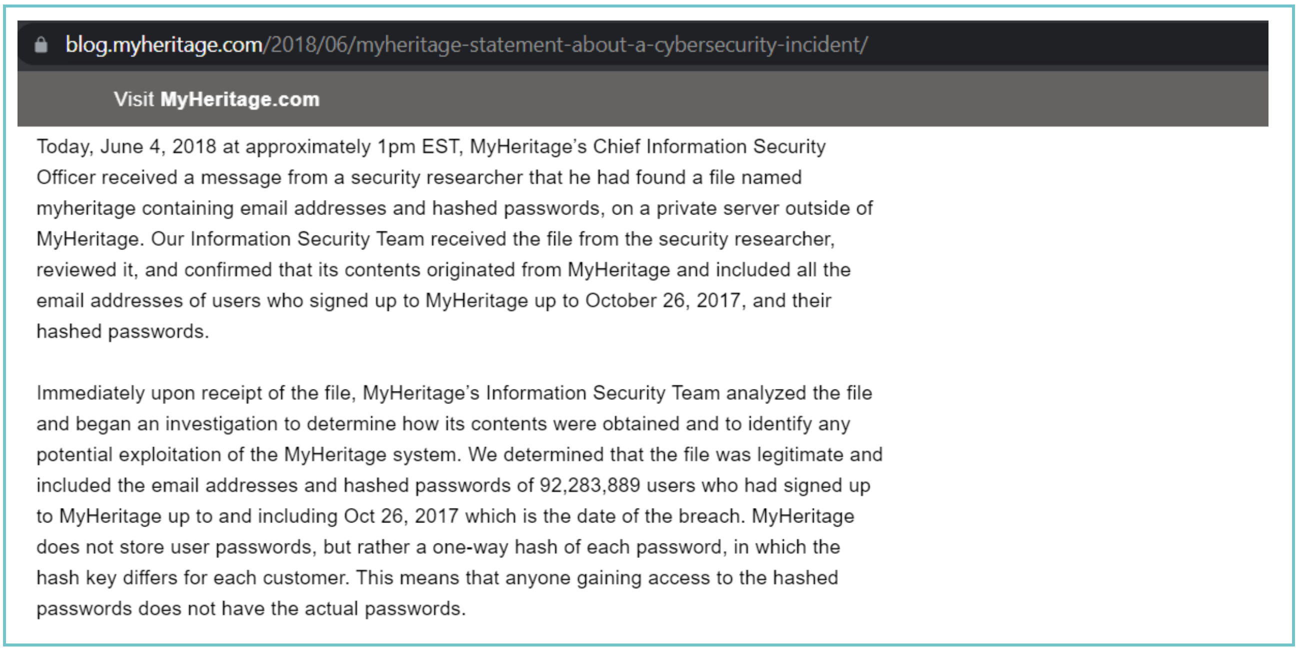
Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

MyHeritage: In October 2017, the genealogy website MyHeritage suffered a data breach. The incident was reported 7 months later after a security researcher discovered the data and contacted MyHeritage. In total, more than 92M customer records were exposed and included email addresses and salted SHA-1 password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it be attributed to "BenjaminBlue@exploit.im".

Compromised data: Email addresses, Passwords

An employee's email was used on MyHeritage, an external website providing lineage tracing services. This website suffered a data breach in October 2017 and in their blog's official statement via https://blog.myheritage.com/2018/06/myheritage-statement-about-a-cybersecurity-incident/ states that this breach included leaked email addresses and hashed passwords of users who signed up prior to 26 October 2017.

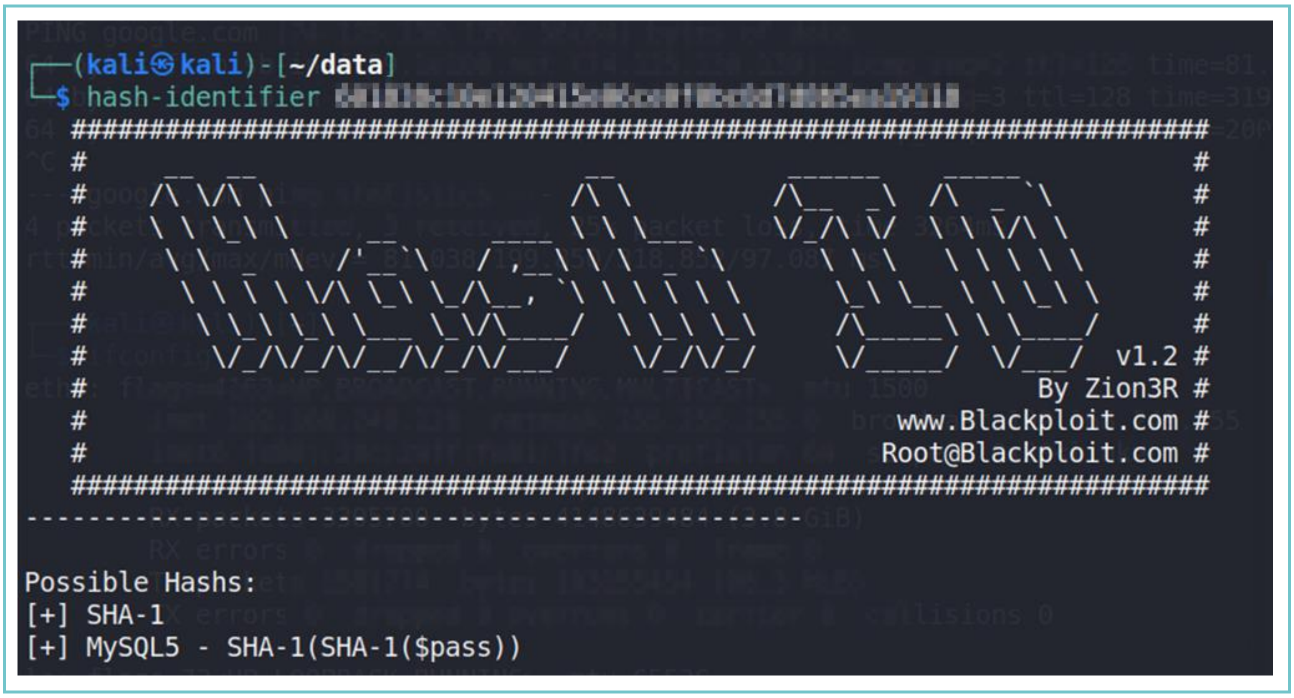


blog.myheritage.com/2018/06/myheritage-statement-about-a-cybersecurity-incident/
Visit **MyHeritage.com**

Today, June 4, 2018 at approximately 1pm EST, MyHeritage's Chief Information Security Officer received a message from a security researcher that he had found a file named myheritage containing email addresses and hashed passwords, on a private server outside of MyHeritage. Our Information Security Team received the file from the security researcher, reviewed it, and confirmed that its contents originated from MyHeritage and included all the email addresses of users who signed up to MyHeritage up to October 26, 2017, and their hashed passwords.

Immediately upon receipt of the file, MyHeritage's Information Security Team analyzed the file and began an investigation to determine how its contents were obtained and to identify any potential exploitation of the MyHeritage system. We determined that the file was legitimate and included the email addresses and hashed passwords of 92,283,889 users who had signed up to MyHeritage up to and including Oct 26, 2017 which is the date of the breach. MyHeritage does not store user passwords, but rather a one-way hash of each password, in which the hash key differs for each customer. This means that anyone gaining access to the hashed passwords does not have the actual passwords.

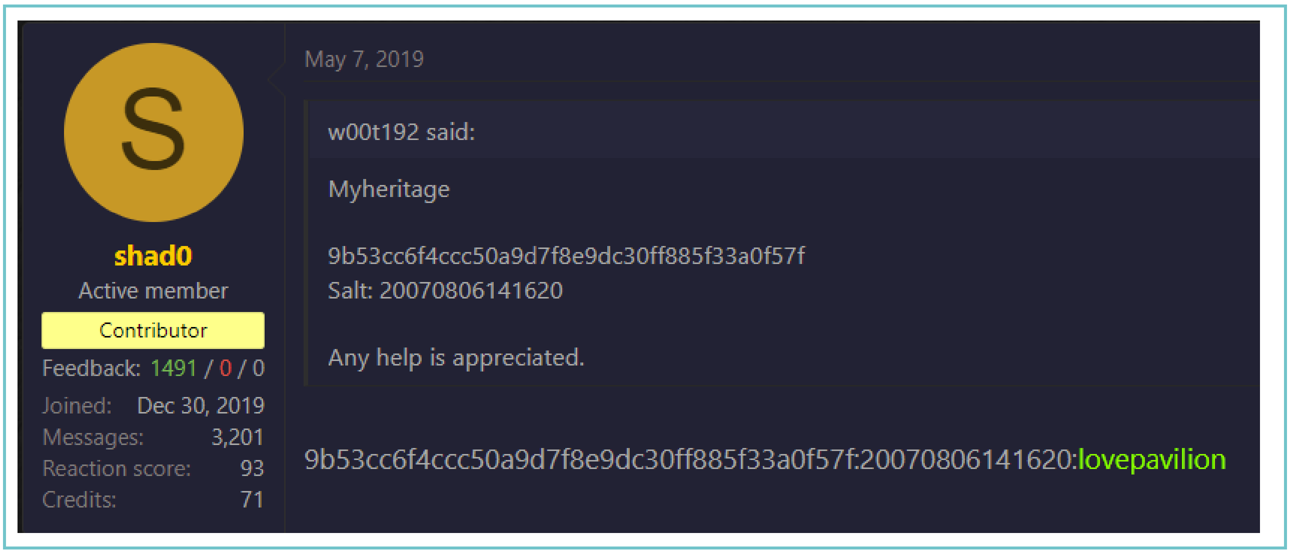
A search on https://www.dehashed.com/ revealed the hashed password used for the myHeritage account created under ____________@______________



```
┌──(kali㉿kali)-[~/data]
└─$ hash-identifier [redacted]
   #########################################################################
   #     __  __                     __           ______    _____           #
   #    /\ \/\ \                   /\ \         /\__  _\  /\  _ `\         #
   #    \ \ \_\ \     __      ____ \ \ \___     \/_/\ \/  \ \ \/\ \        #
   #     \ \  _  \  /'__`\   / ,__\ \ \  _ `\      \ \ \   \ \ \ \ \       #
   #      \ \ \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \      \_\ \__ \ \ \_\ \      #
   #       \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/      #
   #        \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                                             By Zion3R #
   #                                                    www.Blackploit.com #
   #                                                   Root@Blackploit.com #
   #########################################################################
--------------------------------------------------

Possible Hashs:
[+] SHA-1
[+] MySQL5 - SHA-1(SHA-1($pass))
```

In an organised attempt with the right tools and expertise, the hashed passwords can be decrypted to find the original passwords linked to the account.

https://forum.hashkiller.io/index.php?threads/25-hashes-or-less-requests-std-archived.28404/page-62



S

shad0

Active member

Contributor

Feedback: 1491 / 0 / 0

Joined: Dec 30, 2019

Messages: 3,201

Reaction score: 93

Credits: 71

May 7, 2019

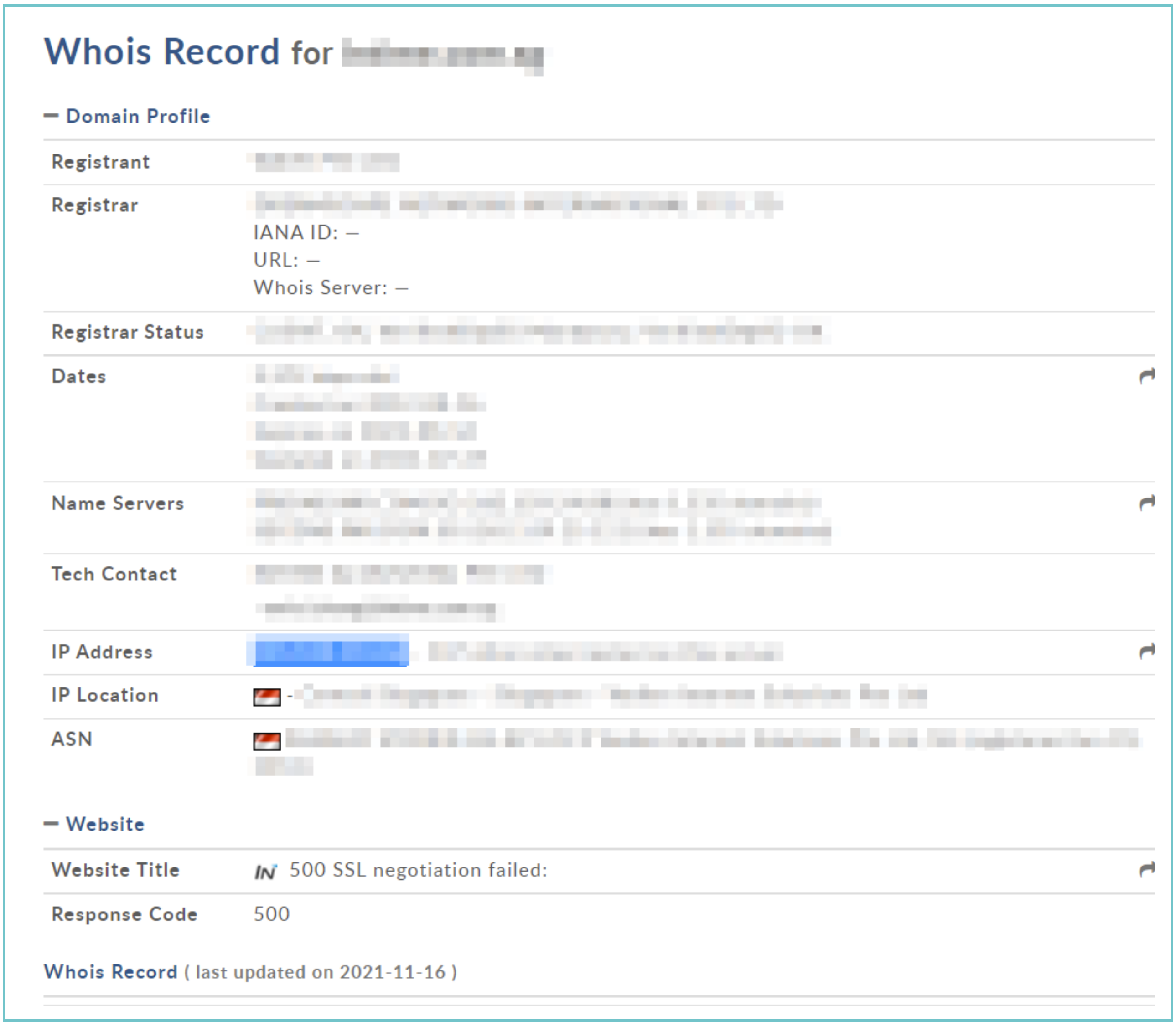
> w00t192 said:
>
> Myheritage
>
> 9b53cc6f4ccc50a9d7f8e9dc30ff885f33a0f57f
> Salt: 20070806141620
>
> Any help is appreciated.

9b53cc6f4ccc50a9d7f8e9dc30ff885f33a0f57f:20070806141620:lovepavilion

Appendix 6: To search domain information with Whois Tool

LOW

An employee’s office email being used to register for the Company's domain name



Whois Record for [redacted]

– Domain Profile

Registrant	[redacted]
Registrar	[redacted] IANA ID: – URL: – Whois Server: –
Registrar Status	[redacted]
Dates	[redacted]
Name Servers	[redacted]
Tech Contact	[redacted]
IP Address	[redacted]
IP Location	[redacted]
ASN	[redacted]

– Website

Website Title	500 SSL negotiation failed:
Response Code	500

Whois Record (last updated on 2021-11-16)

We searched on https://whois.domaintools.com/ for the Company's web server ______________ (https://whois.domaintools.com/__________) and found that the Company's managing director used her own email address to purchase the website domain.

Registrant Name:	______
Registrant Organization:	__________________
Registrant Street:	__________________
Registrant City	SG
Registrant State/Province:	SG
Registrant Postal Code:	__________________
Registrant Country:	SG
Registrant Phone:	______________

Appendix 7: List of Publicly available employee emails and Company information

This is all the open source information that we can find. If a phishing campaign is done, then they can refer to all these emails that we have found.

Company Profile:	Name: _________________
Contact details:	1. Tel: (+65) _____________
	2. Fax: (+65) ____________
	3.(from whois domain search) (+65) ___________

Nos.	Type(s)	Weblink(s)
1	Global	https://__________________
2	Local	https://__________________
3	Wordpress Login Page (Global)	https://__________________
4	Webmail (Global)	https://__________________
5	cPanel (Global)	https://__________________
6	Wordpress Login Page (Local)	https://__________________
7	Webmail (Local)	https://__________________
8	Cpanel (Local)	https://__________________

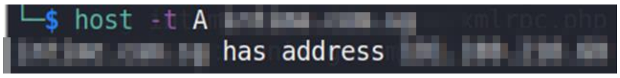
These are the employee emails publicly listed on domain which we have ran by the haveibeenpwned website:-

Email	pwned
_____@__________	X
_____@__________	X
________@__________	✓
_____@__________	X
_____@__________	X
_____@__________	X
_____@__________	X
_____@__________	X
_____@__________	X
_____@__________	X
_____@__________	X
_____@__________	X

Email	pwned
_____@__________	X
_____@__________	X
_____@__________	X
_____@__________	X
_____@__________	X
_____@__________	X
_____@__________	X
_____@__________	X
_____@__________	X
_____@__________	X
_____@__________	X
_____@__________	X

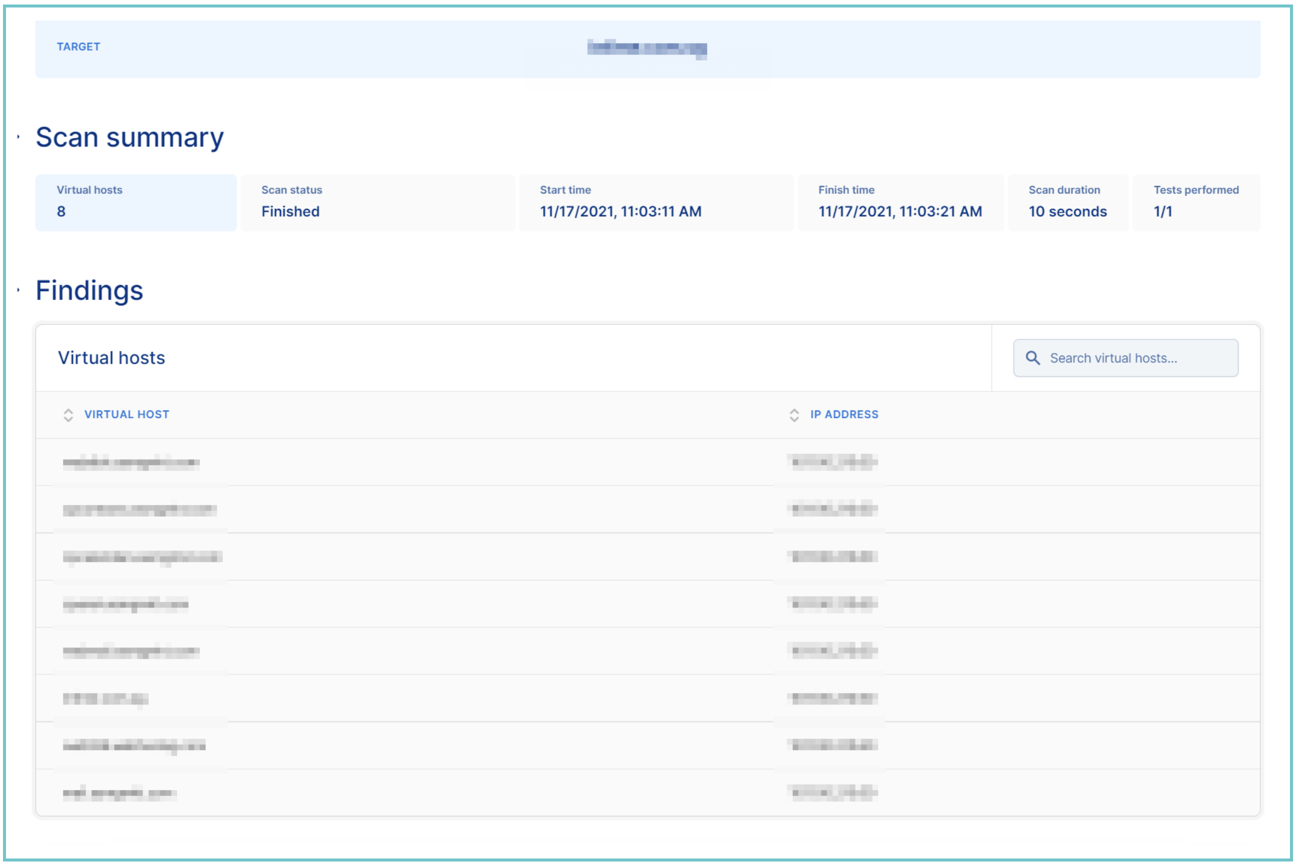
Appendix 8: IP address of Company's website

We managed to detect the Company's IP address to be ___________

 └─$ host -t A [redacted] [redacted] has address [redacted]	(code: $ host -t A ________)

Appendix 9: Ascertaining that Company's IP is valid and not hiding behind another provider

We ran a scan on https://pentest-tools.com/information-gathering/find-virtual-hosts for _____________ to detect the virtual hosts. (screenshot below).



TARGET [redacted]

Scan summary

Virtual hosts	Scan status	Start time	Finish time	Scan duration	Tests performed
8	Finished	11/17/2021, 11:03:11 AM	11/17/2021, 11:03:21 AM	10 seconds	1/1

Findings

Virtual hosts

VIRTUAL HOST	IP ADDRESS
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

We then used Nmap to double check. (code: nmap --script dns-brute -sn _____________)

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-17 05:17 EST
Nmap scan report for ___________ (__________)
Host is up (0.31s latency).
rDNS record for _________: _____________
Service Info: Host: _________: _____________
```

= **END** =