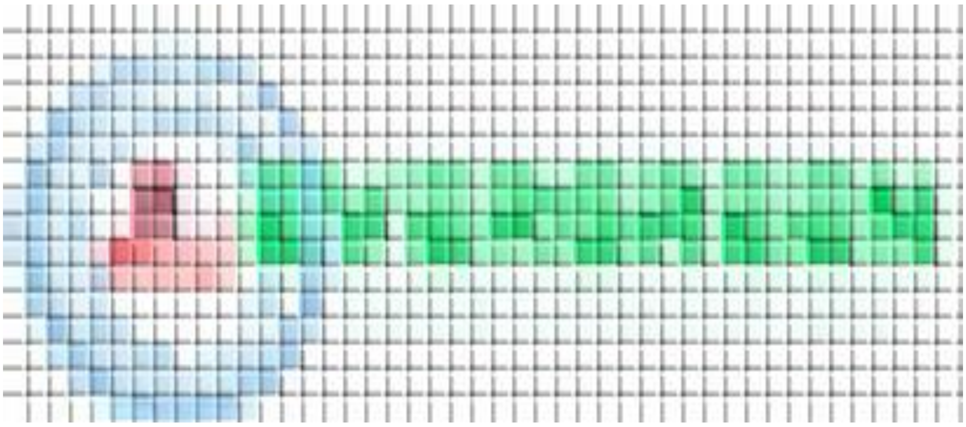
Client-Confidential

INDIAN CYBER SECURITY SOLUTIONS
INDIAN CYBER SECURITY SOLUTIONS

Project Web Application Pentest	Date 22/08/2022
Document Classification Client-Confidential	Version 1
Prepared By Indian Cyber Security Solutions	



Client’s Company logo

1. Document Control

1.1 Document Details

Document Reference	Property
Document Classification	Client-Confidential
Client Name	[redacted]
Document Title	Web Application Pentest Report
Author	Indian Cyber Security Solutions
Date	22/08/2022

1.2 Revision History

Version	Date	Issued By	Summary of Changes
1	22/08/2022	Indian Cyber Security Solutions	Initial Draft

1.3 Document Distribution List

Name	Organization	Role
Abhishek Mitra	Indian Cyber Security Solutions	CEO & Founder
[redacted]	[redacted]	[redacted]

1.4 Testing Team

Name	Role
Sourav Saha	Cyber Security Analyst
Palyam Ajay	Cyber Security Analyst

Table of Contents

2. Company Accreditations

Indian Cyber Security Solutions, A unit of Green Fellow IT Security Solutions Pvt Ltd, Member of NASSCOM, DSCI, ICC and ATC of EC- Council. Indian Cyber Security Solutions is an organization which caters to the need of technology- based risk management & cyber security solution across the globe. ICSS was established in 2013 & by this time it has gathered a good deal of momentum and has reached a distinguished position out of the leading firms in this domain in the country.

Indian Cyber Security Solutions as a unit of Green Fellow IT Security Solutions Pvt Ltd aims to provide cyber security solutions to private and government organizations across the globe. With around 200+ clients across the globe ICSS aims at providing Vulnerability Assessment & Penetration Testing services making cyber security convenient for every organization.

3. Management Details

This area contains management and high-level issue summaries. Detailed technical information can be found within Technical Details section of this report.

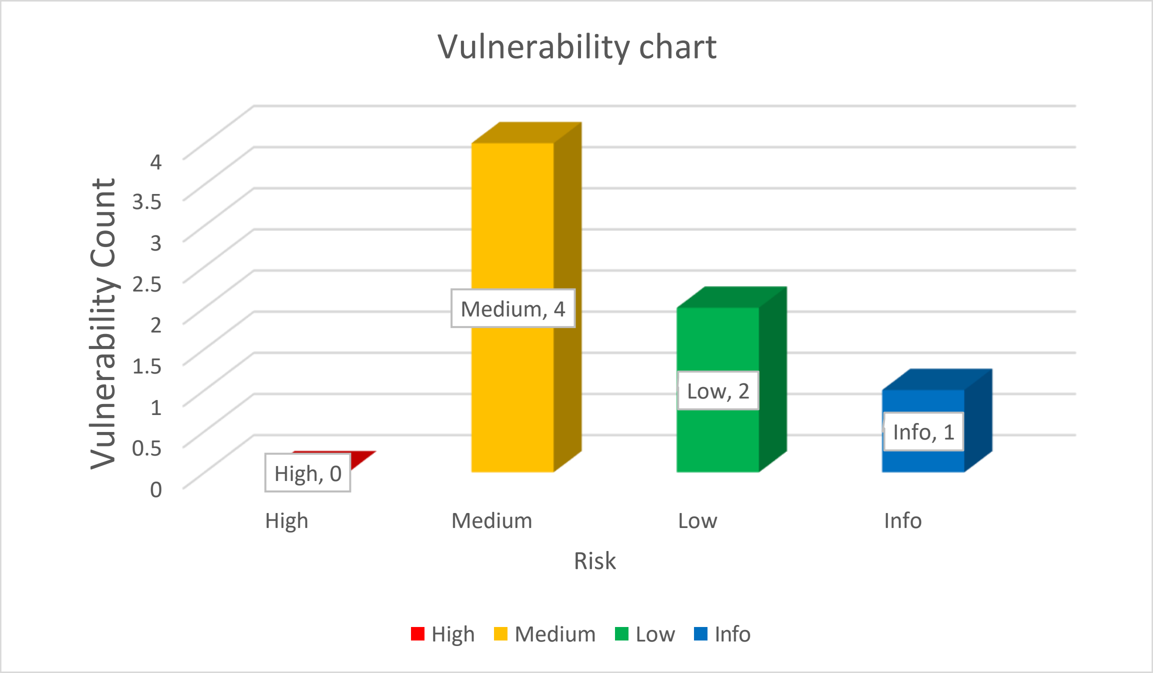
3.1 Risk Summary

Below are the issue ratings and scores used throughout the report. For a detailed explanation of how these risks are calculated, please refer to the Appendices section within this report.

Risk Rating	Overall Risk	CVSS Score	Description
Critical	20 - 25	9.0 – 10	Vulnerability was discovered that has been rated as critical and requires resolution as quickly as possible.
High Risk	12 - 16	7.0 – 8.9	Vulnerability was discovered that has been rated as important and requires resolution in the short term.
Medium	6 - 9	4.0 – 6.9	Vulnerability was discovered that has been rated as medium criticality and should be resolved as part of the ongoing security maintenance of the system.
Low	3 - 5	2.0 – 3.9	Vulnerability was discovered that has been rated as low criticality and should be addressed as part of routine maintenance tasks.
Very Low	1 - 2	1.0 – 1.9	Vulnerability was discovered that has been rated as very low criticality and should be addressed to meet with industry standard benchmarks.
Info	0	0 – 0.9	A finding was discovered that has been rated as informational and normally does not present a risk, but is included for information only.

3.2 Executive Summary

Indian Cyber Security Solutions were engaged by [redacted] to perform Web Application Penetration Testing. Testing was undertaken between 16th August 2022 and 19th August 2022 (First Round of testing) remotely.



The primary goal of this Web Application Penetration testing project was to identify any potential areas of concern associated with the application in its current state and determine the extent to which the system may be breached by an attacker. Using of different Web Application Scanning tools and using payloads, our Penetration Testers were using all the Black Hat techniques to penetrate into the web-based devices. All testing activities were performed on the URL provided in the scope by [redacted]. While performing the testing activities, **Indian Cyber Security Solutions** emulated an external attacker without prior knowledge of the environment.

Indian Cyber Security Solutions recommends [redacted] not to change the firewall policy.

The report summarizes what **Indian Cyber Security Solutions** believes are the most important issues to address in the application. Note the risk ratings were given to help assist in prioritizing remediation efforts. True risk can be calculated by an in-depth understanding of business process and data, as well as the likelihood of exploitation.

4. Introduction

Indian Cyber Security Solutions were engaged by [redacted] [redacted] to perform Web Application Penetration Testing. Testing was undertaken between 16ST August 2022 and 19th August 2022 (First Round of testing) remotely.

4.1 Approach

All testing was carried out using **Indian Cyber Security Solutions** standard testing methodology.

4.2 Scope

The scope of the engagement was as follows:

URL: https://[redacted].in/

5. Findings Summary

The following sections of the report contain technical information regarding the assessment that was conducted.
The findings table below contain a high-level summary of all issues, risk ratings and the status of the finding for each phase of the testing conducted.

5.1 Results of Web Application Penetration Test

All testing was carried out using Indian Cyber Security Solutions standard testing methodology.

Overall Risk Rating	CWE	Vulnerability Name	Status
Medium	87	Out-of-date Version (jQuery)	Open
Medium	1021	X-Frame Header Missing	Open
Low	757	TLSv1.0 and 1.1 enabled	Open
Low	1021	Content security policy	Open
Medium	327	Weak Ciphers Enabled	Open
Info	16	Referrer-Policy Not Implemented	Open

6. Results of Web Application Penetration Test

This section provides the detailed findings of the Web Application Penetration test that was performed between 16th August 2022 and 19th August 2022.

6.1. Vulnerability Name – JQuery Out Dated Version (Vulnerable to XSS)

Vulnerability:			
Overall Risk Rating	Medium	CWE Score	87
Issue Cause	WEB	Status	Open

Description:

Indian Cyber Security Solutions identified that the application has the Out-of-date version (jQuery) vulnerability.

Impact:

Since this is an old version of the software, it may be vulnerable to attacks.

Affected URL:

https://[redacted].in/

Proof of Concept:

Recommendation:

It is recommended to update the version JQuery to the latest version 3.6.0 as soon as possible.

6.2. Vulnerability Name – X-Frame Header Missing

Vulnerability:			
Overall Risk Rating	Medium	CWE	1021
Issue Cause	WEB	Status	Open

Description:

The server didn't return an `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack. The `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe.

Impact:

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top-level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.
Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

Affected URL:

https://[redacted].in/

Proof of Concept:

[redacted]

Recommendation:

- Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
    - X-Frame-Options: DENY It completely denies to be loaded in frame/iframe.
    - X-Frame-Options: SAMEORIGIN It allows only if the site which wants to load has a same origin.
    - X-Frame-Options: ALLOW-FROM URL It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.
- Employing defensive code in the UI to ensure that the current frame is the most top-level window.

6.3. Vulnerability Name – TLSv1.0 and 1.1 enabled

Vulnerability:			
Overall Risk Rating	LOW	CWE Score	326
Issue Cause	WEB	Status	Open

Description

Indian Cyber Security Solutions identified that the web server supports encryption through TLS 1.0. TLS 1.0 is not considered to be "strong cryptography" as defined and required by the PCI Data Security Standard 3.2(.1) when used to protect sensitive information transferred to or from web sites. According to PCI, "30 June 2018 is the deadline for disabling SSL/early TLS and implementing a more secure encryption protocol – TLS 1.1 or higher (TLS v1.2 is strongly encouraged) in order to meet the PCI Data Security Standard (PCI DSS) for safeguarding payment data.

Impact

An attacker may be able to exploit this problem to conduct man-in-the-middle attacks and decrypt communications between the affected service and clients.

Affected URL:

https://[redacted].in/

Proof of Concept

Recommendation

Indian Cyber Security Solutions recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher.

Steps -

1. open run and search regedit
2. Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols>TLS 1.0>Server>double click on Enabled>set value to 0
3. Restart-Computer

6.4 Vulnerability Name – Content security policy not implemented

Vulnerability:			
Overall Risk Rating	Low	CWE	1021
Issue Cause	WEB	Status	Open

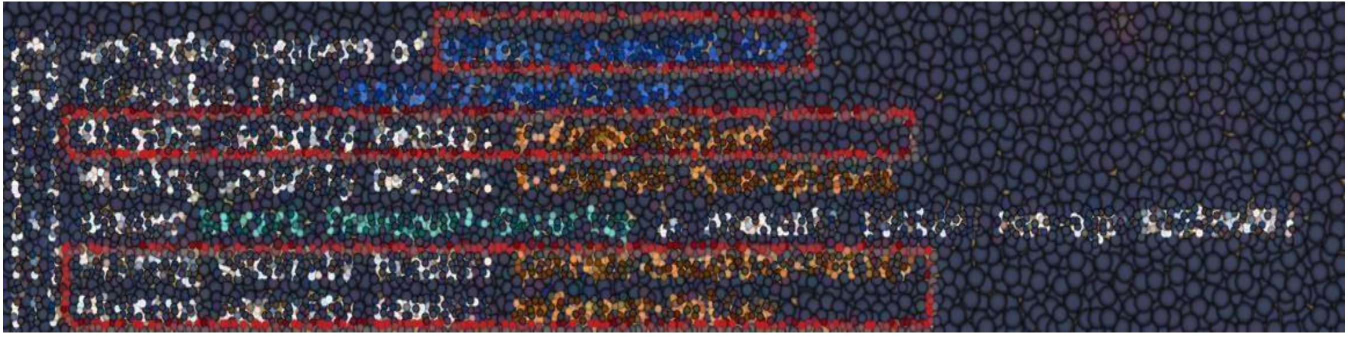
Description:

Indian Cyber Security Solutions identified that the application has the Content Security Policy (CSP) vulnerability. Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Impact:

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability. By not implementing CSP you'll be missing out on this extra layer of security.

Proof of concept:



Affected URL:

https://[redacted].in/

Recommendation: -

Indian Cyber Security Solutions It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the Content-Security-Policy HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

6.5 Vulnerability Name – Weak Ciphers Enabled

Vulnerability:			
Overall Risk Rating	**Medium**	**CWE**	**1021**
Issue Cause	WEB	**Status**	**Open**

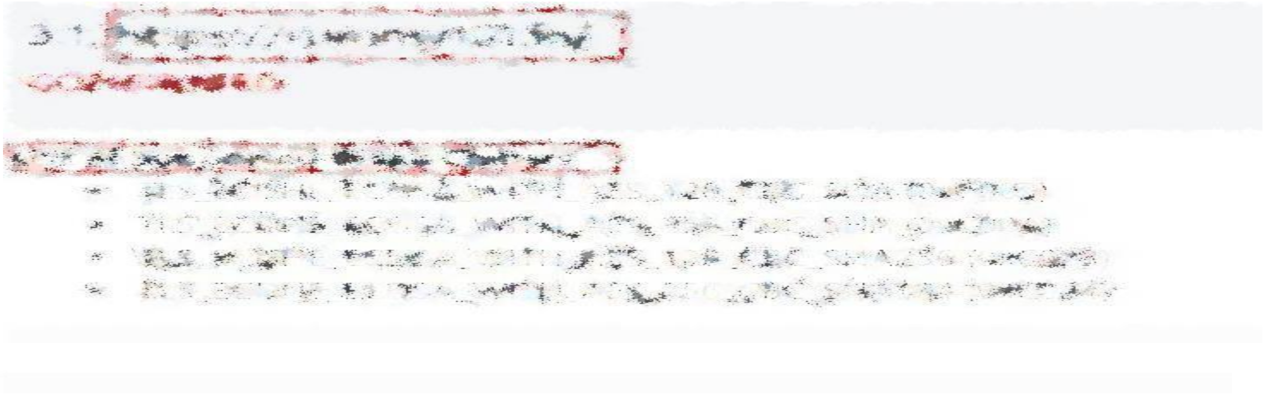
Description:

A weak cipher is defined as an encryption/decryption algorithm that uses a key of insufficient length. Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken. **Indian Cyber Security Solutions** detected that weak ciphers are enabled during secure communication (SSL). You should allow only strong ciphers on your web server to protect secure communication with your visitors

Impact:

Attackers might decrypt SSL traffic between your server and your visitors

Proof of concept:



Affected URL:

https://[redacted].in/

Recommendation

Transport Layer Security (TLS) and its predecessor, Secure Socket Layer (SSL), are widely used protocols. They were designed to secure the transfer of data between the client and the server through authentication, encryption, and integrity protection.

TLS/SSL technology is commonly used in websites and web applications together with the HTTP protocol. It is also used by several other services and protocols, for example, email (SMTP, POP, and IMAP protocols), FTP, chat (XMPP protocol), virtual private networks (TLS/SSL VPNs), and network appliances.

To secure the transfer of data, TLS/SSL uses one or more cipher suites. A cipher suite is a combination of authentication, encryption, and message authentication code (MAC) algorithms. They are used during the negotiation of security settings for a TLS/SSL connection as well as for the transfer of data.

The following are examples of what algorithms a cipher suite may use.

Function	Algorithm
Key Exchange	RSA, Diffie-Hellman, ECDH, SRP, PSK
Authentication	RSA, DSA, ECDSA
Bulk Ciphers	RC4, 3DES, AES
Message Authentication	HMAC-SHA256, HMAC-SHA1, HMAC-MD5

TLS is now a requirement in several regulatory standards. Major browsers mark sites as not secure in absence of TLS. It may therefore also be considered a requirement for serving websites and web applications. However, getting a correct TLS implementation may be difficult. Bad TLS configurations may provide a false sense of security and make websites and web applications vulnerable to attacks.

Many common TLS misconfigurations are caused by choosing the wrong cipher suites. Old or outdated cipher suites are often vulnerable to attacks. If you use them, the attacker may intercept or modify data in transit. Below is a list of recommendations for a secure SSL/TLS implementation.

6.6 Vulnerability Name – Referrer-Policy Not Implemented

Vulnerability:			
Overall Risk Rating	Info	CWE	16
Issue Cause	WEB	Status	Open

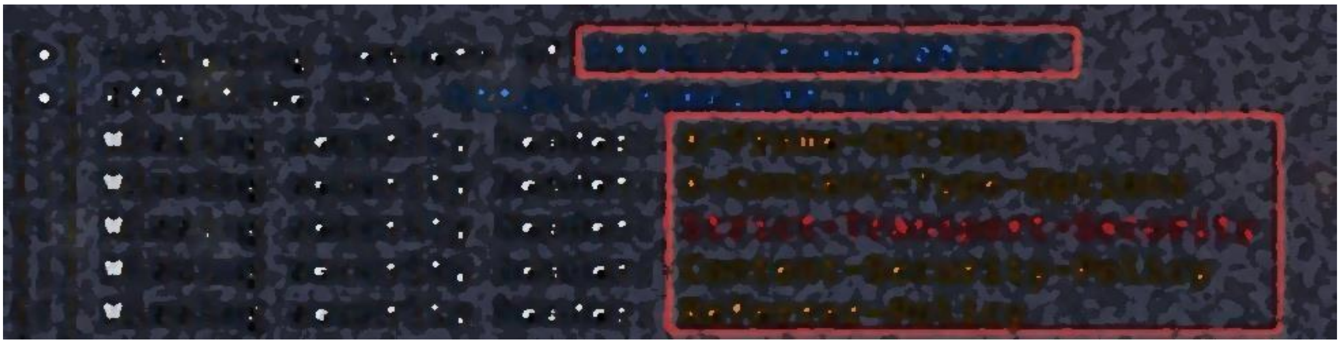
Description:

Indian Cyber Security Solutions identified that the application has the Referrer-Policy Not Implemented vulnerability. Referrer Policy controls behavior of the Referrer header, which indicates the origin or web page URL the request was made from. The web application uses insecure Referrer Policy configuration that may leak user's information to third-party sites.

Impact:

Referrer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site.

Proof of Concept:



Affected URLs:

https://[redacted].in/

Recommendation

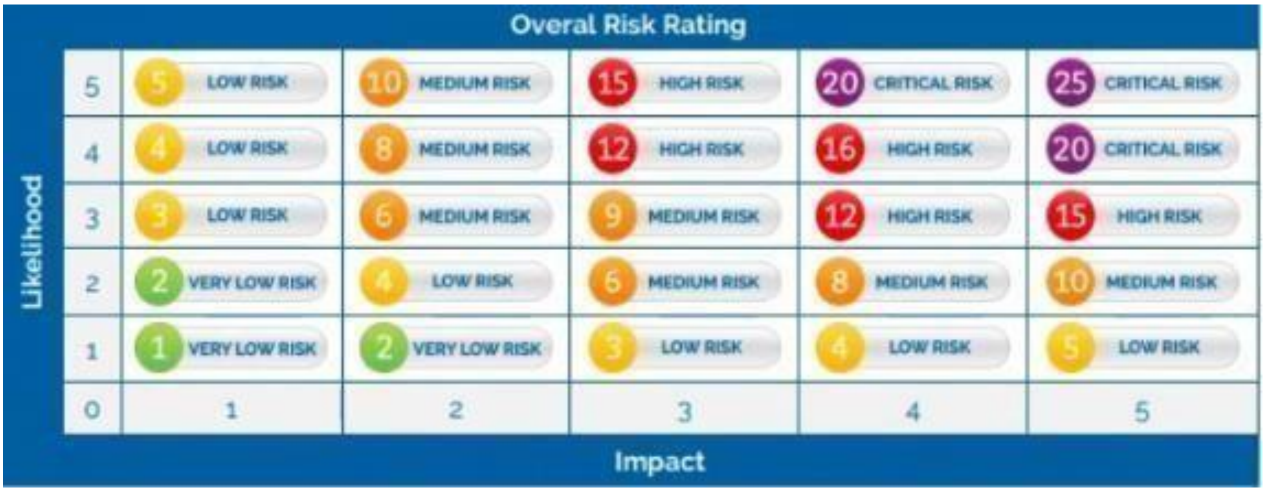
Indian Cyber Security Solutions recommends Please implement a Referrer-Policy by using the Referrer-Policy response header or by declaring it in the meta tags. It’s also possible to control referrer information over an HTML-element by using the real attribute.

Appendix A – Risk Ratings

To calculate the risk level of findings, a calculation is made by the impact/seriousness and likelihood of exploitation of the risk.

The overall risk rating is made up from the two values multiplied.

Overall Risk Rating = Impact X Likelihood

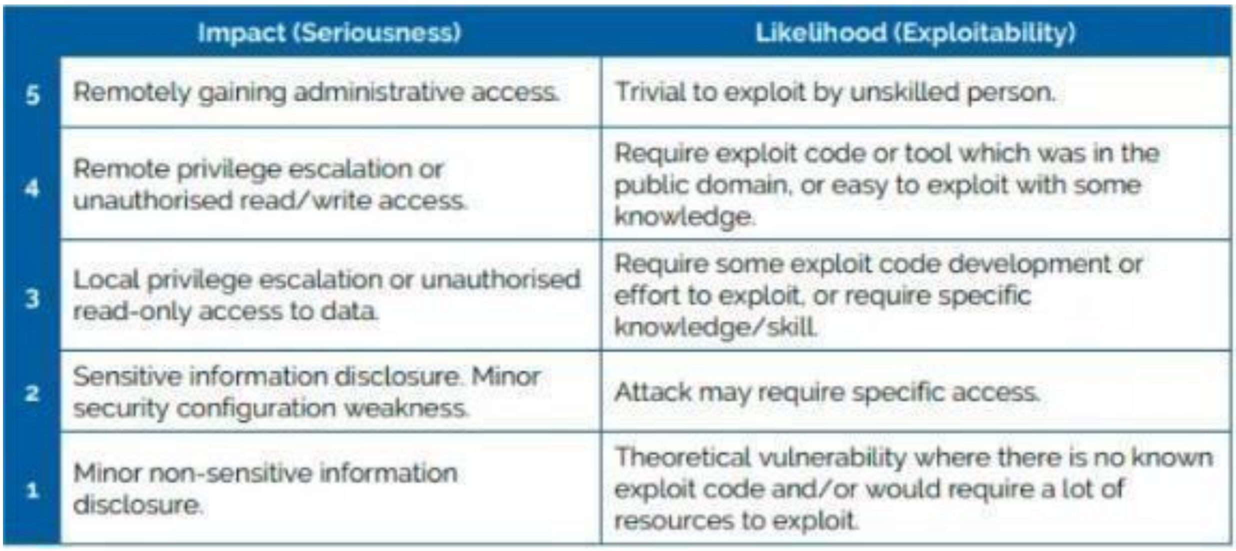


Overal Risk Rating

Likelihood					
5	5 LOW RISK	10 MEDIUM RISK	15 HIGH RISK	20 CRITICAL RISK	25 CRITICAL RISK
4	4 LOW RISK	8 MEDIUM RISK	12 HIGH RISK	16 HIGH RISK	20 CRITICAL RISK
3	3 LOW RISK	6 MEDIUM RISK	9 MEDIUM RISK	12 HIGH RISK	15 HIGH RISK
2	2 VERY LOW RISK	4 LOW RISK	6 MEDIUM RISK	8 MEDIUM RISK	10 MEDIUM RISK
1	1 VERY LOW RISK	2 VERY LOW RISK	3 LOW RISK	4 LOW RISK	5 LOW RISK
0	1	2	3	4	5

Impact

The explanation of the impact and likelihood can be found in the table below:



	Impact (Seriousness)	Likelihood (Exploitability)
5	Remotely gaining administrative access.	Trivial to exploit by unskilled person.
4	Remote privilege escalation or unauthorised read/write access.	Require exploit code or tool which was in the public domain, or easy to exploit with some knowledge.
3	Local privilege escalation or unauthorised read-only access to data.	Require some exploit code development or effort to exploit, or require specific knowledge/skill.
2	Sensitive information disclosure. Minor security configuration weakness.	Attack may require specific access.
1	Minor non-sensitive information disclosure.	Theoretical vulnerability where there is no known exploit code and/or would require a lot of resources to exploit.

Appendix B – Issue Status

Each finding has an assigned issue status that shows if this is a new issue, resolved issue or a retested issue that is unresolved.

Issue Status	Explanation
✗ Open	This is a new issue that has been identified during the assessment and is open and needs to be investigated by the client.
✓ Patched	A previously identified issue that has been addressed by the client and retested by Indian Cyber Security Solutions and found to be fully fixed.
✗ Unresolved	A previously identified issue that has been addressed by the client and retested by Indian Cyber Security Solutions and found yet to be resolved. This could be either the client has not attempted to fix, or the fixes applied have not resolved the issue.
✗ Partially Resolved	A previously identified issue that has been addressed by the client and retested by Indian Cyber Security Solutions and found yet to be fully resolved. This could be not all recommendations or hosts have been fully addressed, but attempts have been made to fix the issue.

Appendix C – Toolset Used

The following lists a selection of the tools used against the targets within scope of the security assessment.

Tool	Description	Date
Burp suite Professional	Integrated platform for performing security testing of web applications https://portswigger.net/	19th August 2022
Netsparker	Open-source tool to scan websites, web applications and services https://www.netsparker.com/	19th August 2022
OWASP ZAP	OWASP ZAP is an open-source web application security scanner. https://owasp.org/www-project-zap/	19th August 2022

Our Offices

KOLKATA
DN-36, Primarc Tower,
Unit no-1103, 11th floor,
College More,
Salt Lake Sector – 5,
Kolkata – 700091

BANGALORE
Chirush Mansion, 3478J
HAL 2nd Stage,13th A Main Road,
Indiranagar,
Bangalore – 560008

CANADA
Indian Cyber Security
Solutions Cyber Security
Research & Analytics
Center Vine Avenue
Moncton NB, Canada, PO
E1E 1J9

AUSTRALIA
Indian Cyber Security
Solutions Australia (Research
and Development Center)11
Darling Street, Hughesdale
Melbourne VIC. 3166

www.indiancybersecuritysolutions.com