

# TNeGA - Directorate of Medical and Rural Health Services

(20/02/2023)

## Web Application Penetration Testing Report



## DOCUMENT CONTROL

ITEM	DESCRIPTION
Document Title:	TNeGA - Directorate of Medical and Rural Health Services
Testing Approach:	Grey Box
Version No.:	V1.0
Assessment Date	10/02/2023 – 15/02/2023
Document Submission Date:	20/02/2023
Author	Sukar Anas IP
Analyst	Sukar Anas IP & Adam

## REVISION RECORD

VERSION	MODIFIED BY	SIGNATURE / DATE	NOTES	Review & Approve
V1.0	Sukar Anas IP	20/02/2023	Final Release	AuriseG Quality Team

## CONTACT

NAME	E-Mail	Contact no
PMO - AuriseG	pmo@auriseG.com	+91 99408 71528

# Table of Contents

<b>1</b>	<b>EXECUTIVE SUMMARY</b>	<b>3</b>
<b>1.1</b>	<b>PROJECT SCOPE</b>	<b>3</b>
<b>1.1.1</b>	<b>TARGET SYSTEMS</b>	<b>3</b>
<b>2</b>	<b>SUMMARY OF EVALUATION</b>	<b>3</b>
<b>2.1</b>	<b>APPROACH AND METHODOLOGY</b>	<b>3</b>
<b>2.2</b>	<b>OWASP TOP 10 CHECKLIST</b>	<b>4</b>
<b>2.3</b>	<b>RISK CATEGORIES</b>	<b>5</b>
<b>2.4</b>	<b>FINDINGS – PICTORIAL REPRESENTATION</b>	<b>6</b>
<b>3</b>	<b>DETAILED APPLICATION PENETRATION TESTING FINDINGS</b>	<b>6</b>
<b>3.1</b>	<b>BROKEN AUTHENTICATION</b>	<b>6</b>
<b>3.2</b>	<b>CAPTCHA BYPASS VIA NO VERIFICATION</b>	<b>8</b>
<b>3.3</b>	<b>HOST HEADER INJECTION</b>	<b>9</b>
<b>3.4</b>	<b>DOUBLE EXTENSION FILE UPLOAD</b>	<b>12</b>
<b>3.5</b>	<b>WEAK KEY EXCHANGE LEADS TO DECRYPT CREDENTIALS BASE 64</b>	<b>14</b>
<b>3.6</b>	<b>INFORMATION DISCLOSURE VIA DIRECTORY LISTING</b>	<b>16</b>
<b>3.7</b>	<b>PRIVATE IP DISCLOSED</b>	<b>18</b>
<b>3.8</b>	<b>VULNERABLE JQUERY</b>	<b>19</b>
<b>3.9</b>	<b>TLS COOKIE WITHOUT SECURE FLAG SET</b>	<b>20</b>
<b>3.10</b>	<b>CLICKJACKING</b>	<b>21</b>
<b>3.11</b>	<b>HSTS DISABLED</b>	<b>23</b>
<b>4</b>	<b>SUMMARY OF RECOMMENDATIONS</b>	<b>24</b>
<b>5</b>	<b>SECURITY BANNER</b>	<b>24</b>
<b>6</b>	<b>DISCLAIMER &amp; LIMITATIONS</b>	<b>25</b>
<b>7</b>	<b>ANNEXURE</b>	<b>26</b>
<b>8</b>	<b>LIST OF TOOLS USED</b>	<b>27</b>
<b>9</b>	<b>CONTACT US</b>	<b>27</b>

# 1 Executive Summary

AuriseG was contracted by TNeGA - Directorate of Medical and Rural Health Services to conduct a Web Application Penetration testing to determine its exposure to a targeted attack. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against TNeGA - Directorate of Medical and Rural Health Services with the goals of:

- ✓ Identifying if a remote attacker could penetrate TNeGA - Directorate of Medical and Rural Health Services.
- ✓ Determining the impact of a security breach on:
  - Confidentiality of the company's private data.
  - External infrastructure and availability of TNeGA - Directorate of Medical and Rural Health Services information systems.

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data.

## 1.1 Project Scope

The Penetration testing performed was focused on TNeGA - Directorate of Medical and Rural Health Services. This result is intended to be an overall assessment of TNeGA - Directorate of Medical and Rural Health Services that fall within the scope of this project.

Furthermore, the findings in this report reflect the conditions found during the testing and do not necessarily reflect current conditions.

### 1.1.1 Target Systems

The following table lists all Assets that were targeted during this assessment.

#### Assets in Scope

- <https://rtionline.tn.gov.in/nursec/nursecounsil-audit/>

# 2 Summary of Evaluation

## 2.1 Approach and Methodology

The attack methodology is straightforward, once the target is identified and information is gathered on the attack surface, all different attacks are planned and tested. If exploitation is successful, the target is compromised and all technical details that led to this situation are exposed in the report document. Unsuccessful attacks will not be represented in the final report, but vulnerabilities in the system will be documented.

Our penetration testing methodology is outlined below:

## Web Application Security Testing Methodology



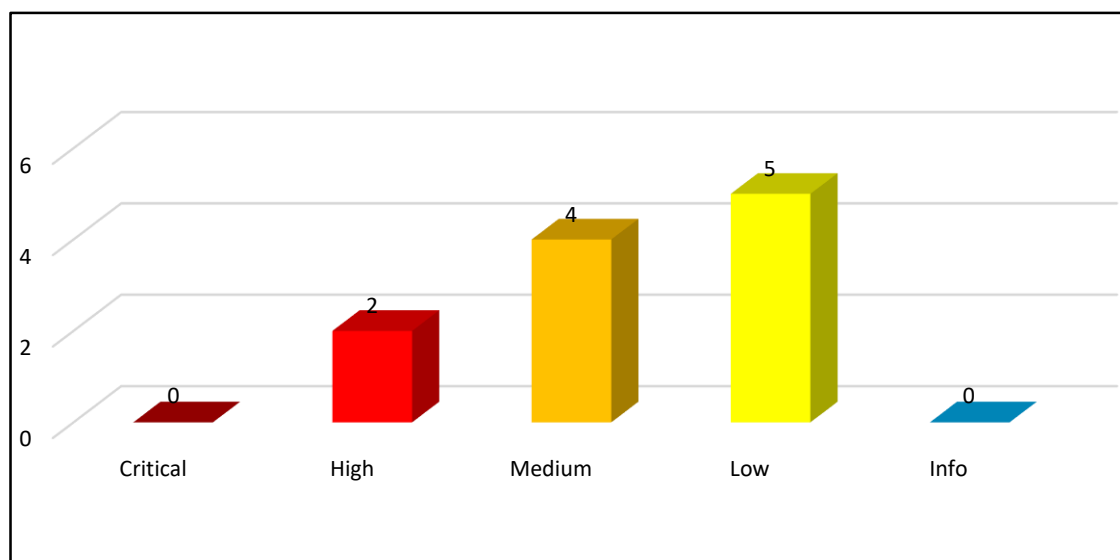
## 2.2 OWASP Top 10 Checklist

Web Application Vulnerability Assessment – OWASP top 10	
A01:2021-Broken Access Control	Scope URL
A02:2021-Cryptographic Failures	PASS
A03:2021-Injection	FAIL
A04:2021-Insecure Design	FAIL
A05:2021-Security Misconfiguration	PASS
A06:2021-Vulnerable and Outdated Components	FAIL
A07:2021-Identification and Authentication Failures	FAIL
A08:2021-Software and Data Integrity Failures	FAIL
A09:2021-Security Logging and Monitoring Failures	PASS
A10:2021-Server-Side Request Forgery	PASS
A01:2021-Broken Access Control	PASS

## 2.3 Risk Categories

VULNERABILITY RATING	LEVEL OF SEVERITY
Critical / High	<p><b>Impact:</b> Vulnerability noted on the affected IT asset can be exploited to obtain remote privileged or unprivileged access and cause severe impact on system operations.</p> <p><b>Ease of Exploit:</b> Exploit techniques are well known. The techniques can be easily obtained and executed by unskilled attackers. The circumstances under which the attack may occur are very common.</p>
Medium	<p><b>Impact:</b> Vulnerability noted on the affected IT asset can be exploited to obtain limited user privileges or network-level access.</p> <p><b>Ease of Exploit:</b> Exploit techniques are fairly well known. Techniques can be easily obtained and executed by persons with general computer security knowledge. The circumstances under which the attack may be successful are common.</p>
Low	<p><b>Impact:</b> Vulnerability noted on the affected IT asset provides little or no chance for exploitation.</p> <p><b>Ease of Exploit:</b> Exploit techniques are not widely known. Techniques are difficult to obtain and execute and require detailed computer security knowledge and experience. The circumstances under which the attack may be successful are rare.</p>

### Web Application Penetration Testing Findings



## 2.4 Findings – Pictorial Representation

Sr. No.	VULNERABILITIES	SEVERITY	OWASP - 2021	STATUS
1	Broken authentication	High	A7	Open
2	Captcha Bypass VIA No Verification	High	A7	Open
3	Host Header Injection	Medium	A3	Open
4	Double Extension File Upload	Medium	A5	Open
5	Weak key Exchange Leads to decrypting Credentials Base 64	Medium	A2	Open
6	Information disclosure via directory listing	Medium	A3	Open
7	Private IP Disclosed	Low	A5	Open
8	Vulnerable JQuery	Low	A6	Open
9	TLS Cookie Without Secure Flag Set	Low	A5	Open
10	Clickjacking	Low	A5	Open
11	HSTS disabled	Low	A5	Open

## 3 Detailed Application Penetration Testing Findings

### 3.1 Broken Authentication

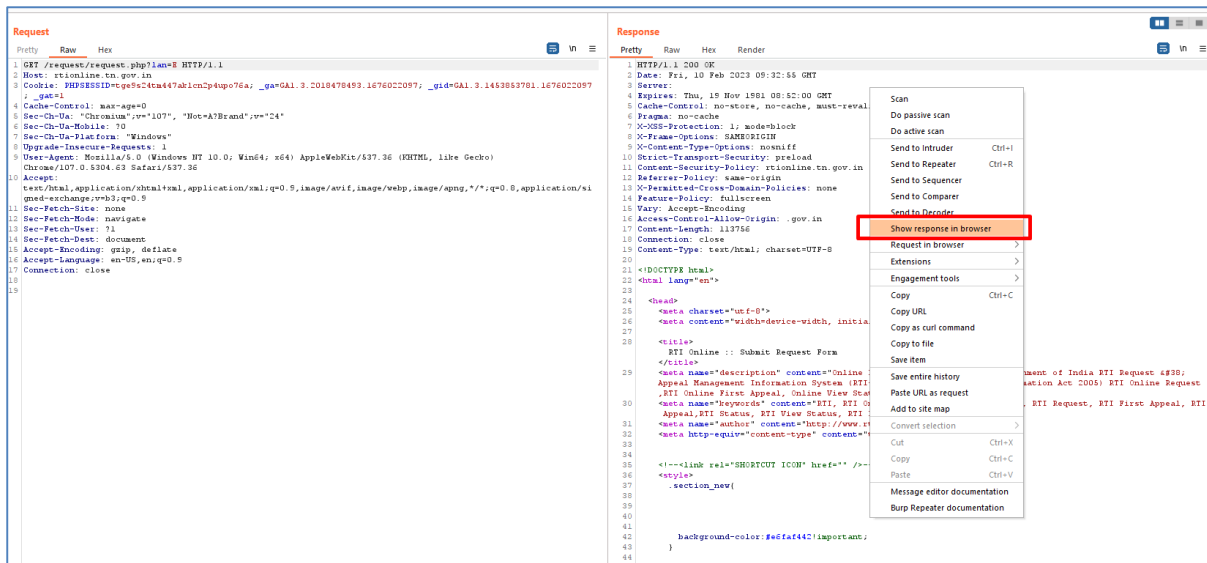
#### Threat Description: **High**

Authentication is “broken” when attackers are able to compromise passwords, keys or session tokens, user account information, and other details to assume user identities. Due to poor design and implementation of identity and access controls, the prevalence of broken authentication is widespread.

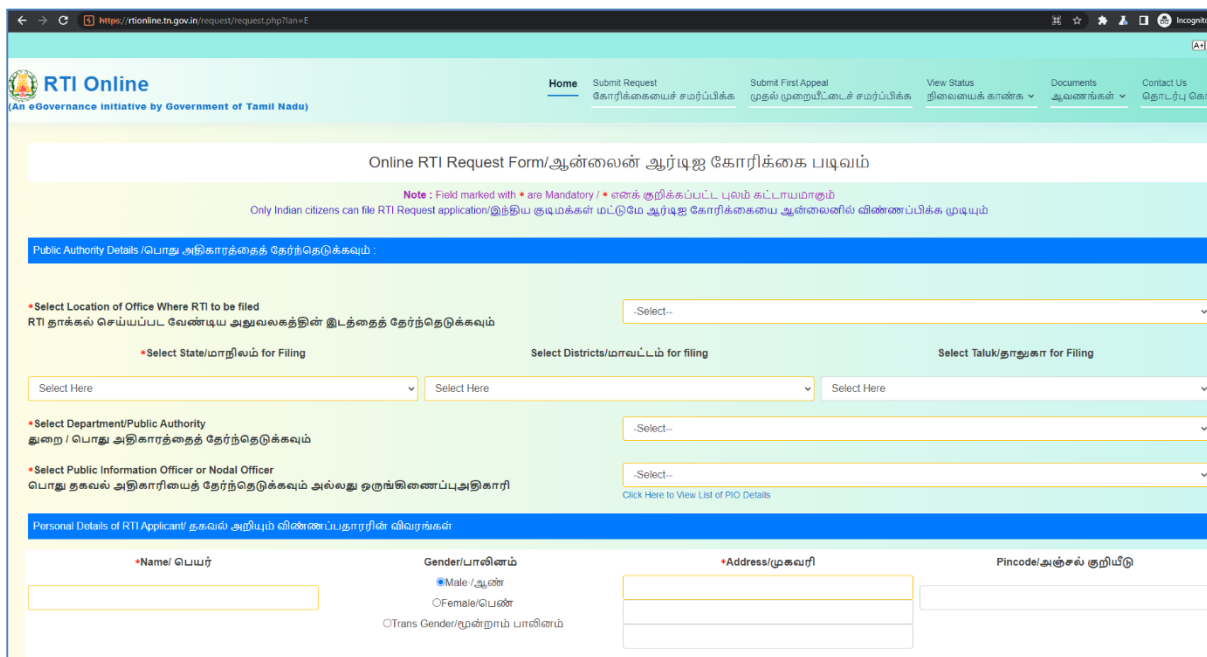
#### Methodology:

During the assessment, it was found that the application is vulnerable to broken authentication.

**Step 1:** Capture the request of the valid session and logout the session.



## Step 2: Use that session to log in the application.



## Impact:

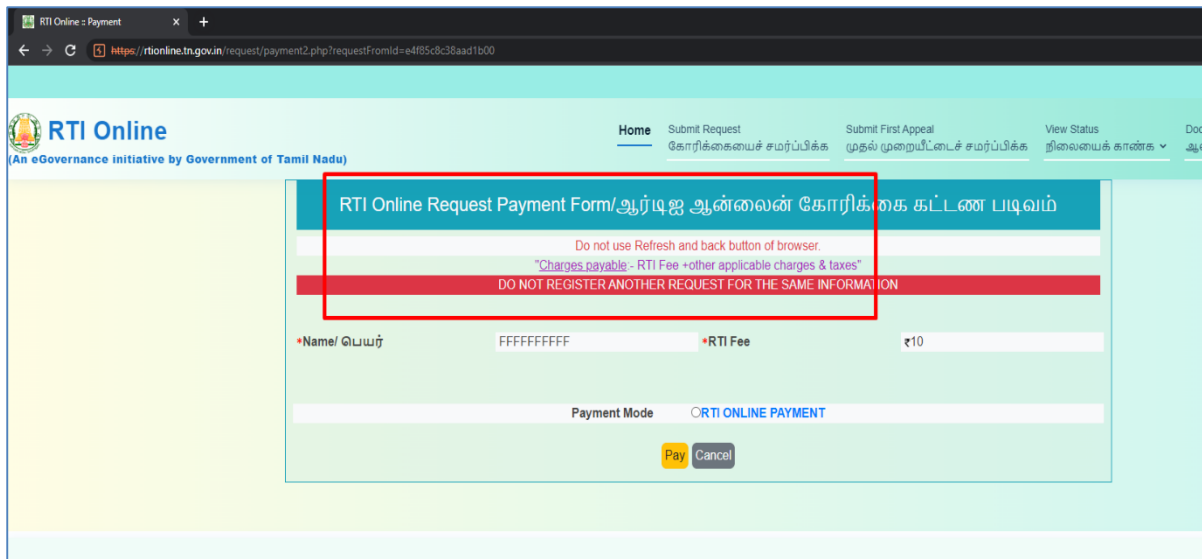
The goal of an attack is to take over one or more accounts, and for the attacker to get the same privileges as the attacked user. If the attacker successfully hijacks an admin account, the attacker could therefore do as much as an ordinary admin, which depending on the application could have a great impact. Other impact includes modification of data, adding and deleting new user, installing any backdoor application for continuous control over the application, etc.

## Affected Hosts:

Host	Proof
<a href="https://rtionline.tn.gov.in/request/request.php?lan=E">https://rtionline.tn.gov.in/request/request.php?lan=E</a>	Available







### Impact:

If the server or web host has a maximum limit of queries to be stored, this attack can exceed it and exploit the server/brute-forcing forcing the function request "limit+X" a number of times. If it is a web hosting, the hosted project will be deleted/banned by the providers leading to data loss of this admin panel users. If it's a server, the server might go down because of storage.

### Affected Hosts:

Host	Proof
<a href="https://rtionline.tn.gov.in/request/payment2.php?requestFromId=e4f85c8c38aad1b00">https://rtionline.tn.gov.in/request/payment2.php?requestFromId=e4f85c8c38aad1b00</a>	Available

### Recommendation:

We recommend the below methods to mitigate this vulnerability:

- Add Rate Limiting functionality to this function and other related functionalities as well.
- Implement a strong Re-CAPTCHA Functionality.
- User server rate limit technique to control the no on request.
- The server should be blacklisted for the source IP for a certain time to send a required period of time.

## 3.3 Host Header Injection

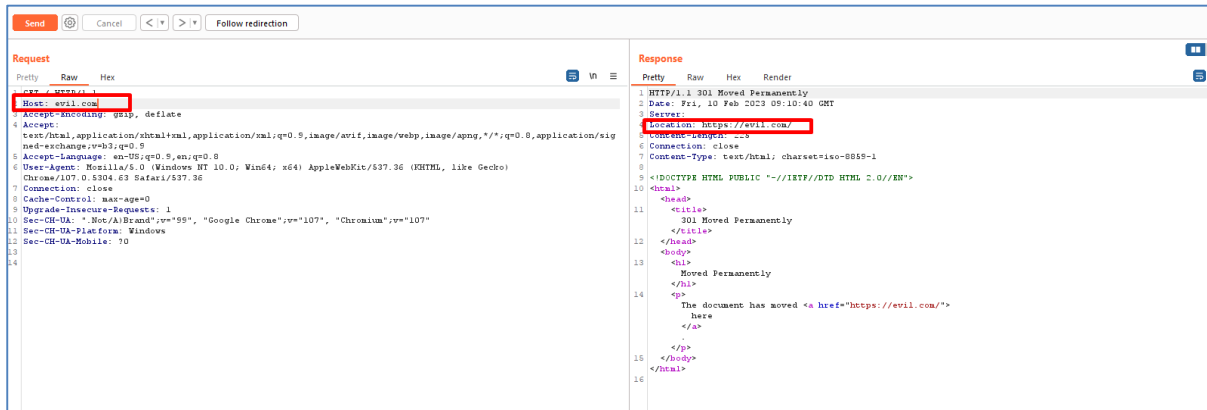
### Threat Description: **Medium**

The host header specifies which website or web application should process an incoming HTTP request. The web server uses the value of this header to dispatch the request to the specified website or web application. A website is prone to this attack if this header is dynamically generated based on user input.

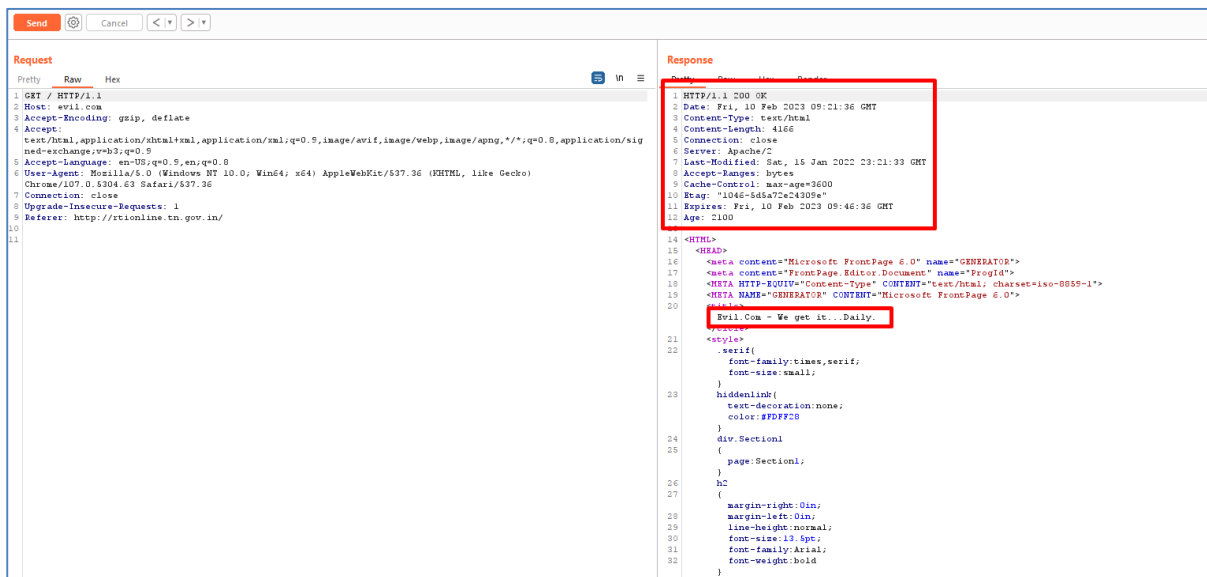
## Methodology:

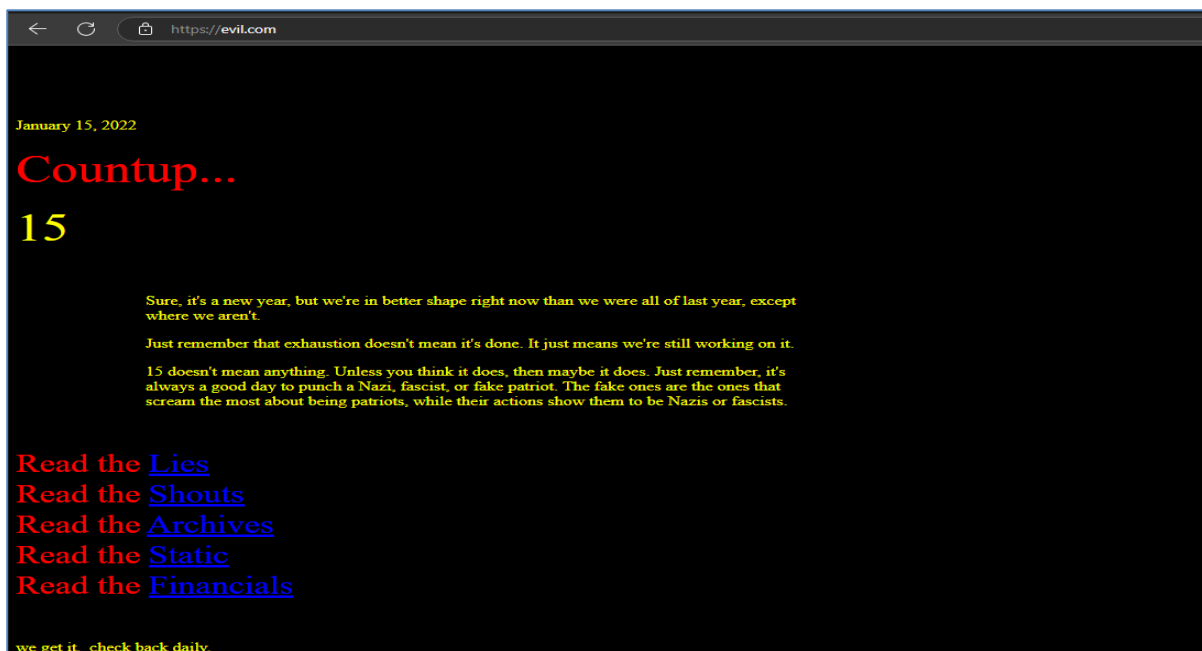
It was found that web application is vulnerable to host header injection. An attacker can manipulate the host header as seen by the web application and cause the application to behave in unexpected ways.

**Step 1:** Capture the page and edit the hostname into evil.com and click send button.



**Step 2:** The Response location changes into evil.com Website.





### Impact:

An attacker can use this vulnerability to redirect users to other malicious websites, which can be used for phishing web cache poisoning, and other similar attacks. The HTTP Host header can be controlled by an attacker. This can be exploited using a web cache.

### Affected Hosts:

Host	Proof
<a href="https://rtionline.tn.gov.in/nursec/nurseccouncil-audit/">https://rtionline.tn.gov.in/nursec/nurseccouncil-audit/</a>	Available

### Recommendation:

- The web application should not trust Host and X-Forwarded-Host and should use a secure SERVER\_NAME instead of these headers.
- We recommend using \$\_SERVER ['SERVER\_NAME'] instead of \_SERVER ['HTTP\_HOST'] and enforcing it at the HTTPD (Apache, Nginx, etc.) configuration level.
- The major difference between \$\_SERVER ['SERVER\_NAME'] is a server-controlled variable, while \$\_SERVER ['HTTP\_HOST'] is a user-controlled value.
- (What this means is that you should have an explicitly configured virtual host for each domain you serve. Or in other words, do not allow "catch-all" configurations.)
- Ensure that you only accept URLs that are located on accepted domains.
- \$domains = ['abc.example.com',' foo. bar. baz'];
- if ( ! in array(\$\_SERVER['SERVER\_NAME'], \$domains)) { // error }
- Whitelist all valid UR. Do not accept other URLs without validating them.

## 3.4 Double Extension File Upload

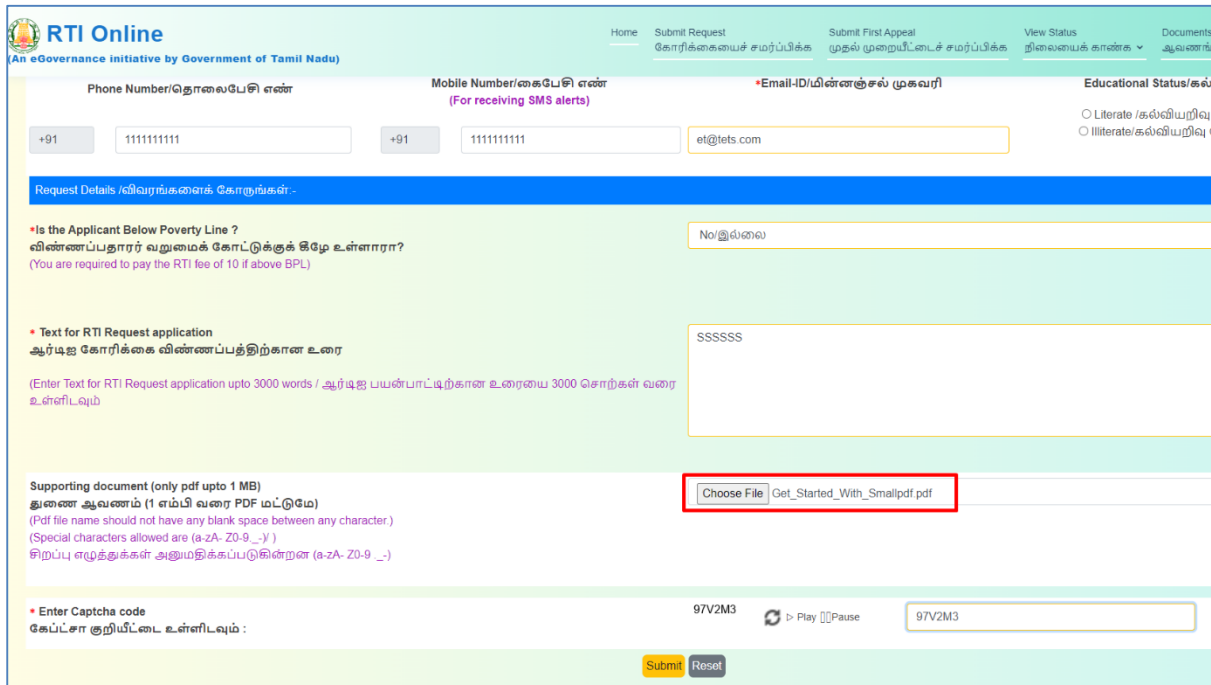
### Threat Description: **Medium**

File upload vulnerabilities are when a web server allows users to upload files to its file system without sufficiently validating things like their name, type, contents, or size. Failing to properly enforce restrictions on these could mean that even a basic image upload function can be used to upload arbitrary and potentially dangerous files instead. This could even include server-side script files that enable remote code execution.

### Methodology:

During the assessment, we observed that affected host is vulnerable to double extensions vulnerability.

**Step 1:** Enter the details and try to upload double extensions file and proceed to submit.



**RTI Online**  
(An eGovernance initiative by Government of Tamil Nadu)

Home Submit Request கோரிக்கையைச் சமர்ப்பிக்க Submit First Appeal முதல் முறையீட்டைச் சமர்ப்பிக்க View Status நிலைமையைக் காண்க Documents ஆவணம்

Phone Number/தொலைபேசி எண்: +91 1111111111  
Mobile Number/கைபேசி எண் (For receiving SMS alerts): +91 1111111111  
Email-ID/மின்னஞ்சல் முகவரி: et@tets.com  
Educational Status/கல்: ☐ Literate / கல்வியறிவு ☐ Illiterate / கல்வியறிவு

**Request Details / விவரங்களைக் கொடுங்கள்:-**

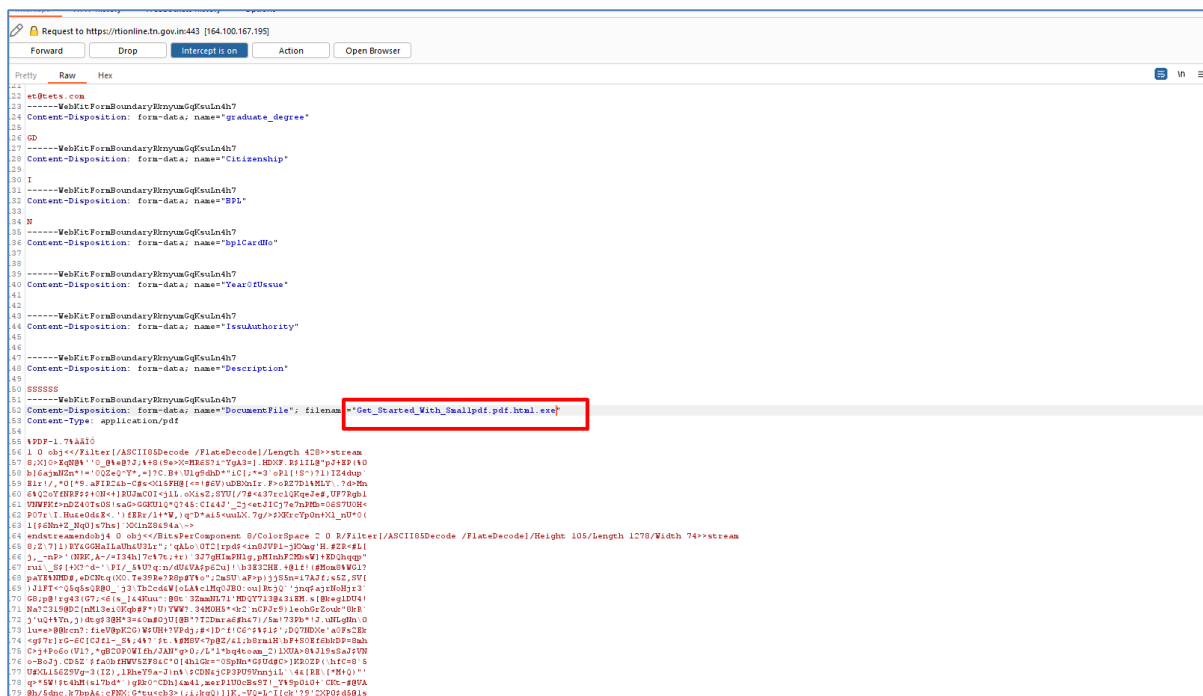
• Is the Applicant Below Poverty Line ?  
விண்ணப்பதாரர் வறுமைக் கோட்டுக்குக் கீழே உள்ளாரா?  
(You are required to pay the RTI fee of 10 if above BPL)  
No/இல்லை

• Text for RTI Request application  
ஆர்.டி. கோரிக்கை விண்ணப்பத்திற்கான உரை  
(Enter Text for RTI Request application upto 3000 words / ஆர்.டி. பயன்பாட்டிற்கான உரையை 3000 சொற்கள் வரை உள்ளிடவும்)  
SSSSSS

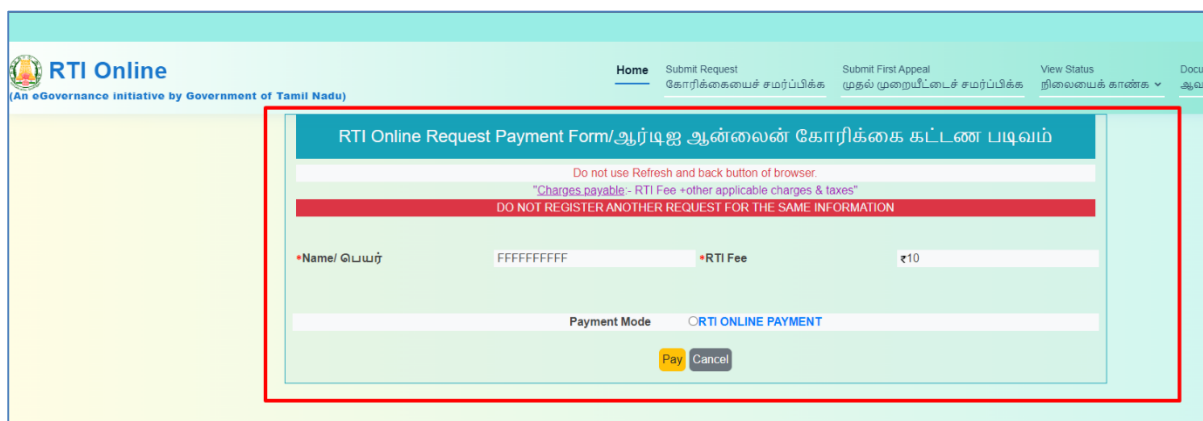
Supporting document (only pdf upto 1 MB)  
துணை ஆவணம் (1 எம்பி வரை PDF மட்டுமே)  
(Pdf file name should not have any blank space between any character.)  
(Special characters allowed are (a-zA-Z0-9\_-'))  
சிறப்பு எழுத்துக்கள் அனுமதிக்கப்படுகின்றன (a-zA-Z0-9\_-)  
Choose File Get\_Started\_With\_Smallpdf.pdf

• Enter Captcha code  
கேப்டசா குறியீட்டை உள்ளிடவும் : 97V2M3  
97V2M3  
Submit Reset

**Step 2:** Capture the request in burp and Add extension and forward the Request.



### Step 3: The page has redirecting to the next page.



### Impact:

The consequences of unrestricted file upload can vary, including complete system takeover, an overloaded file system or database, forwarding attacks to back-end systems, and simple defacement. It depends on what the application does with the uploaded file and especially where it is stored. Here is the list of attacks that the attacker might do:

- Compromise the web server by uploading and executing a web shell that can run commands, browse system files, browse local resources, attack other servers, exploit local vulnerabilities, and so forth.
- Put a phishing page on the website.
- Put a permanent XSS into the website.
- Bypass cross-origin resource sharing (CORS) policy and exfiltrate potentially sensitive data.
- Upload a file using a malicious path or name which overwrites critical files or personal data that other user's access. For example; the attacker might replace the. hatches file to allow him/her to execute specific scripts.

## Affected Hosts:

Host	Proof
<a href="https://rtionline.tn.gov.in/request/request.php?lan=E">https://rtionline.tn.gov.in/request/request.php?lan=E</a>	Available

## Recommendation:

Restrict file types accepted for upload: check the file extension and only allow certain files to be uploaded.

- Use a whitelist approach instead of a blacklist.
- Check for double extensions such as .php.png.
- Check for files without a filename like .hatches (on ASP.NET, check for configuration files like web. c config).
- Change the permissions on the upload folder so the files within it are not executable. If possible, rename the files that are uploaded.

## 3.5 Weak key Exchange Leads to Decrypt Credentials Base 64

### Threat Description: **Medium**

Applications sometimes Base64-encode parameters in an attempt to obfuscate them from users or facilitate the transport of binary data. The presence of Base64-encoded data may indicate security-sensitive information or functionality that is worthy of further investigation. The data should be reviewed to determine whether it contains any interesting information, or provides any additional entry points for malicious input.

### Methodology:

**Step 1:** Capture the request of login page and copy the credential.

```

Pretty Raw Hex
1 POST /nursec/nursecounsel-audit/User/loginauth_emp HTTP/1.1
2 Host: rtionline.tn.gov.in
3 Cookie: language=en; PHPSESSID=tge9s24tm447ak1cn2p4upo76a; _ga=
  GAL.3.2018478493.1676022097; _gid=GAL.3.1453853781.1676022097
4 Content-Length: 67
5 Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
6 Accept: */*
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Sec-Ch-Ua-Mobile: ?0
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/107.0.5304.63 Safari/537.36
11 Sec-Ch-Ua-Platform: "Windows"
12 Origin: https://rtionline.tn.gov.in
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://rtionline.tn.gov.in/nursec/nursecounsel-audit/user/login
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.9
19 Connection: close
20
21
22 email=ZXRAAdGV0cy5jb20%3D&password=YWFhYWFhYWFhYQ%3D%3D& aptcha=aaaa
  
```

**Step 2:** Decode credential with burp decoder.

ZXRAdGV0cy5jb20%3D
et@tets.cb20%3D

YWFnYWFnYWFnYQ%3D%3D
aaaaaaaaYQ%3D%3D

**Step 3:** Base64 Decoded credentials are disclosed.

The following parameters appear to contain Base64-encoded data:

- email = et@tets.com
- password = aaaaaaaaaa

### Impact:

The attacker can decrypt base 64 encryption very easily as base 64 is very easy to decrypt which allows the attacker to steal sensitive information like email and password.



**Affected Hosts:**

Host	Proof
<a href="https://rtionline.tn.gov.in/nursec/nursecouncil-audit/User/loginauth_emp">https://rtionline.tn.gov.in/nursec/nursecouncil-audit/User/loginauth_emp</a>	Available

**Recommendation:**

When it comes to key exchange, it's important to use a strong and secure algorithm to prevent attackers from eavesdropping or tampering with the communication. Here are some recommendations for secure key exchange algorithms:

1. **Diffie-Hellman Key Exchange:** Diffie-Hellman is a widely used algorithm for key exchange that allows two parties to securely exchange a secret key over an insecure communication channel. It provides a secure method for two parties to agree on a shared secret key without transmitting it directly over the communication channel.
2. **Elliptic Curve Diffie-Hellman Key Exchange:** Elliptic Curve Diffie-Hellman (ECDH) is similar to Diffie-Hellman, but uses elliptic curves instead of prime numbers. This makes ECDH more efficient and requires shorter key sizes, which can be an advantage in certain applications.
3. **RSA Key Exchange:** RSA is a well-known algorithm for public-key cryptography, and can also be used for key exchange. However, it is generally slower and requires larger key sizes than Diffie-Hellman or ECDH.
4. **Secure Sockets Layer (SSL) and Transport Layer Security (TLS):** SSL and TLS are protocols that use a combination of symmetric and asymmetric encryption for secure communication over the internet. They are widely used for secure web browsing, email communication, and other applications.

## 3.6 Information disclosure via directory listing

**Threat Description: Medium**

Directory listing vulnerability is a security issue that arises when a web server is configured to display the contents of a directory instead of a specific web page or resource. In such cases, if there is no default index page, the server may display a list of files and directories within that directory, which can be accessed by anyone who has the appropriate URL. Directory listing vulnerability can be exploited by attackers to obtain sensitive information about a website or application, such as usernames, passwords, source codes, and other confidential data. This can be done by scanning the server for directories that have directory listing enabled and then accessing the directory listings to view the contents.

**Methodology:**

During the assessment, we found that the application exposed Sensitive Information via Directory Listing vulnerability.

**Impact:**

1. **Data Breach:** If the directory contains sensitive or confidential data such as personally identifiable information (PII), financial data, or confidential business information, then the disclosure of this data can lead to a data breach. The consequences of a data breach can be severe, including financial losses, reputational damage, and legal repercussions.
2. **Loss of Confidentiality:** Directory listing disclosure can lead to the loss of confidentiality of sensitive data, which can result in the loss of trust from customers, partners, and other stakeholders. For example, if a directory listing exposes trade secrets or other confidential business information, this can harm a company's competitive advantage and market position.
3. **Regulatory Compliance Issues:** Depending on the type of data that is disclosed, directory listing disclosure can lead to violations of various regulatory requirements such as the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), or the Payment Card Industry Data Security Standard (PCI DSS). These violations can result in fines, penalties, and legal action.
4. **Damage to Reputation:** The disclosure of sensitive information via directory listing can damage a company's reputation and erode customer trust. This can result in loss of business and difficulty attracting new customers, partners, and investors.

Host	Proof
<a href="https://rtionline.tn.gov.in/de/images/">https://rtionline.tn.gov.in/de/images/</a>	Available

It's important to disable directory listing on web servers and ensure that all directories have a default index page. Additionally, organizations should implement robust security controls, including access controls, encryption, monitoring, and regular security audits.

## 3.7 Private IP Disclosed

### Threat Description: **LOW**

The host header specifies which website or web application should process an incoming HTTP request. The web server uses the value of this header to dispatch the request to the specified website or web application. A website is prone to this attack if this header is dynamically generated based on user input.

### Methodology:

During the assessment, we found that the application exposed private IP addresses via the .js File.

```

// var url="http://10.163.19.176/medical_transfer_council/";
// var url="<?php echo URL8007?>";
// function hi()
// {
// }
// Prevent from space at the begining of the textbox.
$('body').on('keypress', function(e)
{
    if (e.which == 32 && e.target.selectionStart == 0)
        return false;
});

$('body').bind('cut paste', function (e) {
    e.preventDefault();
});

// Allow Alphabets and Numbers
$('.alpha_numeric').on('keypress', function(event)
{
    if ((event.charCode > 64 && event.charCode < 91) || (event.charCode > 96 && event.charCode < 123) || (event.charCode >= 48 && event.charCode <= 57) || (event.charCode == 32) )
        return true; // let it happen, don't do anything
    else
        return false;
});

$('.address').on('keypress', function(event)
{
    if ((event.charCode > 64 && event.charCode < 91) || (event.charCode > 96 && event.charCode < 123) || (event.charCode >= 48 && event.charCode <= 57) || (event.charCode == 32) || (event.charCode == 44) || (event.charCode == 45) )
        return true; // let it happen, don't do anything
    else
        return false;
});

$('.alpha_numeric_wo_space_slash').on('keypress', function(event)
{
    if ((event.charCode > 64 && event.charCode < 91) || (event.charCode > 96 && event.charCode < 123) || (event.charCode >= 48 && event.charCode <= 57) || (event.charCode == 47) )
        return true; // let it happen, don't do anything
    else
        return false;
});

$('.reference_number').on('keypress', function(event)
{
    if ((event.charCode > 64 && event.charCode < 91) || (event.charCode > 96 && event.charCode < 123) || (event.charCode >= 48 && event.charCode <= 57) || (event.charCode == 47) || (event.charCode == 191) )
        return true; // let it happen, don't do anything
    else
        return false;
});

//Allow Alphabets and Numbers without space
$('.alpha_numeric_wo_space').on('keypress', function(event)
{
    if ((event.charCode > 64 && event.charCode < 91) || (event.charCode > 96 && event.charCode < 123) || (event.charCode >= 48 && event.charCode <= 57) )
        return true; // let it happen, don't do anything
    else
        return false;
});

```

### Impact:

Disclosure of Internal IP address can be used by an attacker to exploit the server, its hosting network, etc. This helps an attacker to chain multiple issues and launch specific attacks against internal environment of the application.

### Affected Hosts:

Host	Proof
<a href="https://rtionline.tn.gov.in/nursec/nursecouncil-audit/public/dash/js/custom_js.js">https://rtionline.tn.gov.in/nursec/nursecouncil-audit/public/dash/js/custom_js.js</a>	Available

There is not usually any good reason to disclose the internal IP addresses used within an Organization's infrastructure. If these are being returned in service banners or debug messages, then the relevant services should be configured to mask the private addresses. If they are being used to track back-end servers for load-balancing purposes, then the addresses should be rewritten with innocuous identifiers from which an attacker cannot infer any useful information about the infrastructure.

An outdated JQuery vulnerability refers to a security flaw in an older version of the JQuery library that has been identified and patched in newer versions, but may still be present in websites or applications that are using the older version. Since JQuery is widely used for web development, many websites and applications may still be using older versions of the library that is no longer supported. If these older versions contain known vulnerabilities, they can be exploited by attackers to compromise the security of a website or application.

[illegible]

Affected versions of this package are vulnerable to Cross-site Scripting (XSS). Passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `.html()`, `.append()`, and others) may execute untrusted code.

## Affected Hosts:

Host	Proof
<a href="https://rtionline.tn.gov.in/javascripts/additional-methods.min.js">https://rtionline.tn.gov.in/javascripts/additional-methods.min.js</a>	Available

## Recommendation:

We recommend the below methods to mitigate this vulnerability.

- We strongly recommend upgrading the affected JavaScript library to the latest version as suggested by the vendor or the OEM. The latest known jQuery Version is 3.6.3 which can be used for better security.
- The code for including new updated jQuery is `<script src="https://code.jquery.com/jquery-3.6.0.js"></script>`.
- It is recommended to download and test with an uncompressed version of the latest jQuery in a development environment.

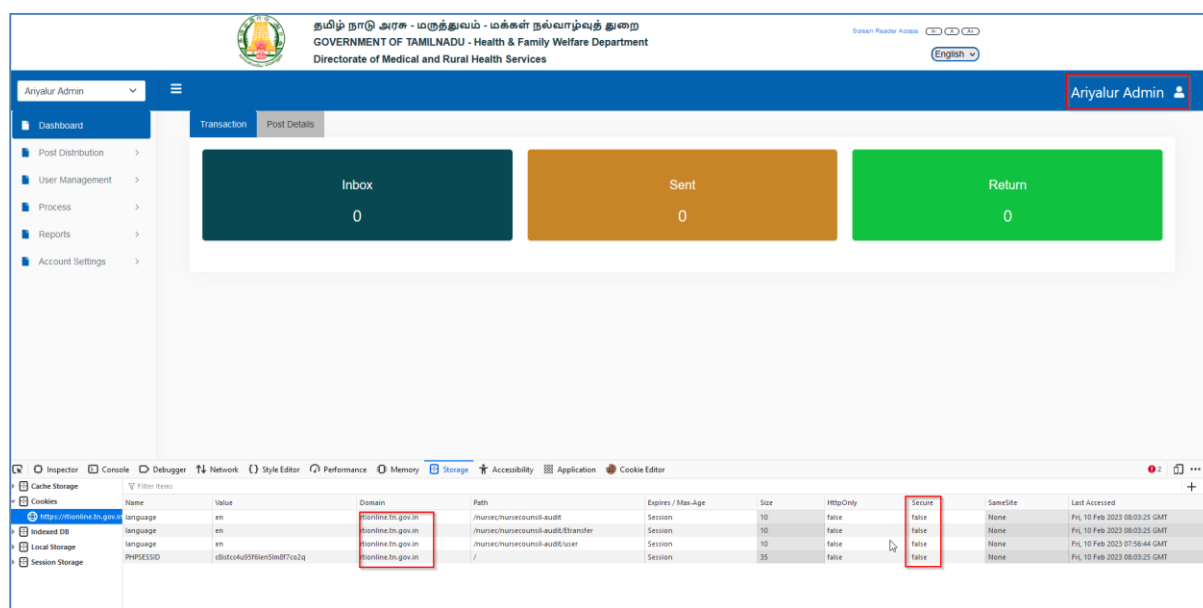
## 3.9 TLS Cookie without Secure Flag Set

### Threat Description: **LOW**

If the secure flag is set on a cookie, then browsers will not submit the cookie in any requests that use an unencrypted HTTP connection, thereby preventing the cookie from being trivially intercepted by an attacker monitoring network traffic. If the secure flag is not set, then the cookie will be transmitted in clear text.

### Methodology:

During the assessment, we found secure cookie not set be true, As below POC shown.



The screenshot shows the website interface with a sidebar menu and a main content area. The main content area displays three boxes: 'Inbox' (0), 'Sent' (0), and 'Return' (0). Below the interface, the browser's developer tools are open, showing the 'Cookies' tab. The table below lists the cookies found on the page.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
language	en	rtionline.tn.gov.in	/marsec/humsec/audit	Session	10	false	false	None	Fri, 10 Feb 2023 08:03:25 GMT
language	en	rtionline.tn.gov.in	/marsec/humsec/audit/Etransfer	Session	10	false	false	None	Fri, 10 Feb 2023 08:03:25 GMT
language	en	rtionline.tn.gov.in	/marsec/humsec/audit/user	Session	10	false	false	None	Fri, 10 Feb 2023 07:56:44 GMT
PHPSESSID	cd5tccu89f6ierd5m87Tos2q	rtionline.tn.gov.in	/	Session	35	false	false	None	Fri, 10 Feb 2023 08:03:25 GMT

### Impact:

If the secure flag is not set, then the cookie will be transmitted in clear text if the user visits any HTTP URLs within the cookie's scope. An attacker may be able to induce this event by feeding a user suitable links, either directly or via another website. Even if the domain that issued the cookie does not host any content that is accessed over HTTP, an attacker may be able to use links of the form ("http://example.com:443/") to perform the same attack. Once the attacker has gained the plaintext Cookies or session, it will lead to a Session Hijacking attack.

#### Affected Hosts:

Host	Proof
<a href="https://rtionline.tn.gov.in/nursec/nursecounsel-audit/Etransfer/dashboard">https://rtionline.tn.gov.in/nursec/nursecounsel-audit/Etransfer/dashboard</a>	Available

#### Recommendation:

- The secure flag is an option that can be set by the application server when sending a new cookie to the user within an HTTP Response.
- The secure flag should be set on all cookies that are used for transmitting sensitive data when accessing content over HTTPS.
- As the host mentioned in the affected section is not protected with a secure flag it is useful for an attacker to eavesdrop on the communication. Setting up secure cookies depends upon the technology in use. We recommend some of the sample code or syntax to set the secure cookie flag.

- **In Apache:**

Go to Apache2.conf file and set the secure cookie flag as follows:

Load Module headers module /usr/lib/apache2/modules/mod\_headers.so

Header edit Set-Cookie ^ (.\* ) \$ \$1; HttpOnly; Secure

- **Java:**

Servlet 3.0 (Java EE 6) introduced a standard way to configure secure attributes for the session cookie, this can be done by applying the following configuration in web.xml.

```
<Session-config>
<Cookie-config>
  <Secure>true</secure>
</cookie-config>
</session-config>
```

- **Asp.net**

In web. Config uses the following code <httpCookies requires="true" /> for setting up a secure cookie flag.

## 3.10 Clickjacking

#### Threat Description: **LOW**

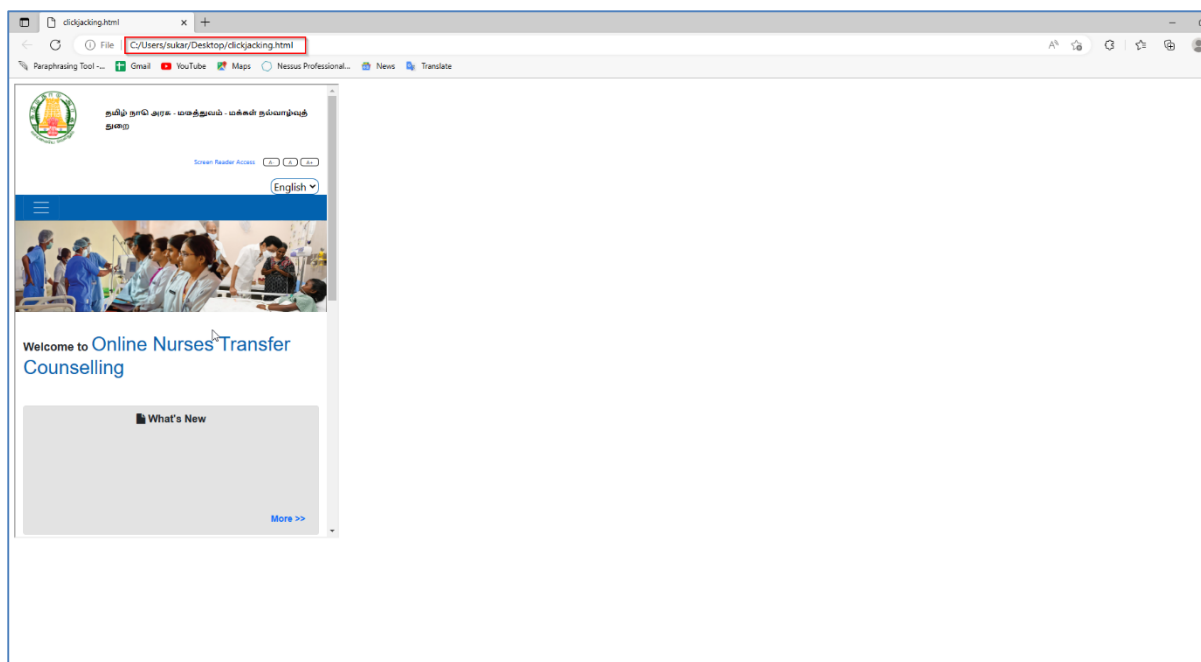
During the assessment, it was found that the hosts listed in the "Affected Hosts" section were vulnerable to Clickjacking (User Interface redress attack), which is a malicious technique of tricking a



Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

## Methodology:

During the assessment, we observed that the given application is vulnerable to clickjacking.



## Impact:

The potential risks exposed by clickjacking and its inherent impact render it a medium risk issue in most sensitive applications, such as financial or sensitive data handling apps. The reason why it is a medium risk and not a high-risk issue is down to the delivery method of attack and its execution vectors. This vulnerability requires user interaction and an element of social engineering as victims must voluntarily interact with the malicious page. The overall risk may only be a medium rating; however, the impact is high. This vulnerability can be linked to a multitude of attacks including keylogging and stealing user credentials.

## Affected Hosts:

Host	Proof
<a href="https://rtionline.tn.gov.in/nursec/nursecounsel-audit">https://rtionline.tn.gov.in/nursec/nursecounsel-audit</a>	Available

## Recommendation:

The following techniques can be used to aid in the prevention of clickjacking:

- X-Frame-Options: Same Origin.
- Frame Busting JavaScript.
- Unique URL request.
- Use CAPTCHAs.
- Element Randomization.

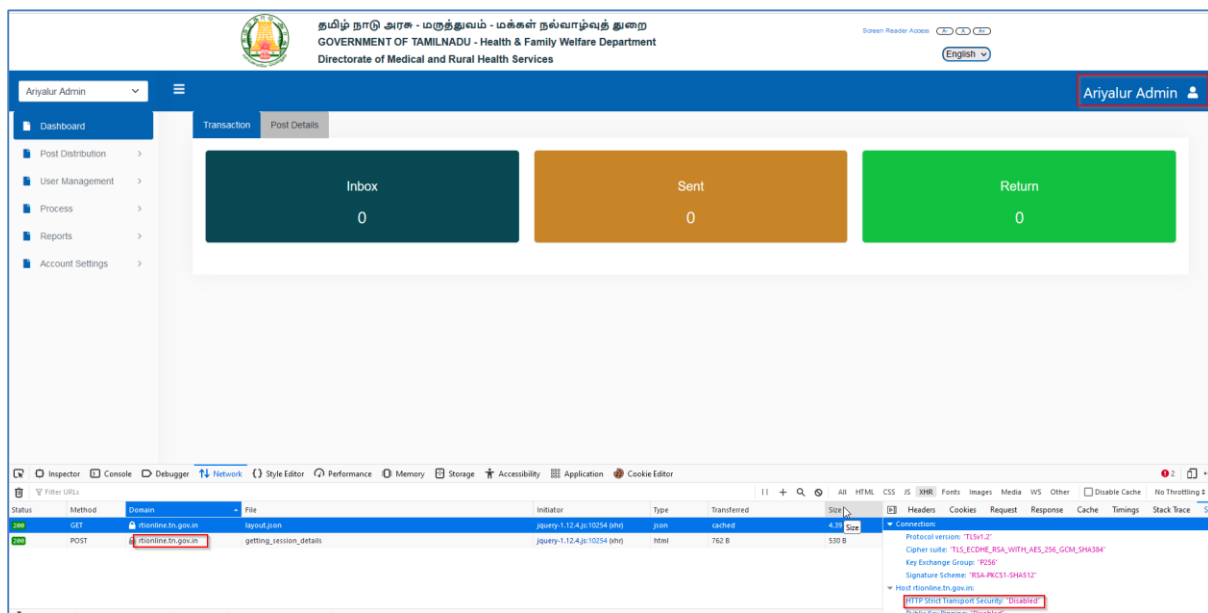
### 3.11 HSTS disabled

#### Threat Description: **Low**

HTTP Strict Transport Security (HSTS) tells a browser that a website is only accessible using HTTPS. It is detected that the web application does not implement HTTP Strict Transport Security (HSTS) as the Strict Transport Security header is missing from the response.

#### Methodology:

During the assessment, it was observed that the application has not implemented HSTS.



#### Impact:

As the communication is done via HTTP, the site will be vulnerable to Man in the Middle Attack (MITM).

#### Affected Hosts:

Host	Proof
<a href="https://rtionline.tn.gov.in/nursec/nursecounsel-audit">https://rtionline.tn.gov.in/nursec/nursecounsel-audit</a>	Available

#### Recommendation:

- It's recommended to implement HTTP Strict Transport Security (HSTS) into our web application.



## 4 Summary of Recommendations

The Recommendations to close these vulnerabilities are:-

- Generate a Unique session or access token for different users.
- Access token should be valid only for one-time login.
- Add Rate Limiting functionality to this function and other related functionalities as well.
- Implement a strong Re-CAPTCHA Functionality.
- Avoid the usage of certain deprecated software protocols like HTTP.
- Ensure that you only accept URLs that are located on accepted domains.
- Whitelist all valid UR. Do not accept other URLs without validating them.
- Use a whitelist approach instead of a blacklist.
- Check for double extensions such as. php.png.
- Diffie-Hellman Key Exchange: Diffie-Hellman is a widely used algorithm for key exchange that allows two parties to securely exchange a secret key over an insecure communication channel. It provides a secure method for two parties to agree on a shared secret key without transmitting it directly over the communication channel.
- Damage to Reputation: The disclosure of sensitive information via directory listing can damage a company's reputation and erode customer trust. This can result in loss of business and difficulty attracting new customers, partners, and investors.
- The secure flag is an option that can be set by the application server when sending a new cookie to the user within an HTTP Response.
- X-Frame-Options: Same Origin.
- It's recommended to implement HTTP Strict Transport Security (HSTS) into our web application.

## 5 Security Banner

It is a well-known fact that no organization can claim 100 % security due to ever-changing threat and vulnerability scenarios. New vulnerabilities surface on a daily basis and both seasoned and casual Hackers can exploit these vulnerabilities to cause serious harm to the organization. We conclude that, The Vulnerability Status of the in-scope items for the TNeGA - Directorate of Medical and Rural Health Services are:-

URL	Security Posture	Comments
<a href="https://rtionline.tn.gov.in/request/request.php?lan=E">https://rtionline.tn.gov.in/request/request.php?lan=E</a>	High	Generate a Unique session or access token for different users.

<a href="https://rtionline.tn.gov.in/request/payment2.php?requestFromId=e4f85c8c38aad1b00">https://rtionline.tn.gov.in/request/payment2.php? requestFromId=e4f85c8c38aad1b00</a>	High	Implement a strong Re-CAPTCHA Functionality.
--	------	--

The vulnerabilities identified by an attacker can exploit and this may cause:

- Data Loss
- Reputational loss
- Information Leakage

We recommend that TNeGA - Directorate of Medical and Rural Health Services create a detailed plan for the closure of the gaps found during this penetration test as soon as possible. The closure plan should address the highly severe vulnerabilities followed by the medium and low-level vulnerabilities. The closure plan should be tested before making any changes to the production environment. We also recommend that the TNeGA - Directorate of Medical and Rural Health Services adopt a program-based approach that ensures that all new vulnerabilities are identified in a timely manner and closed before they are exploited by an attacker.

Thus, the security posture of the External Infrastructure of the TNeGA - Directorate of Medical and Rural Health Services can be maintained at a high level. This will assist in securing the information, IT infrastructure, and image of the TNeGA - Directorate of Medical and Rural Health Services.

We thank TNeGA - DIRECTORATE OF MEDICAL AND RURAL HEALTH SERVICES for giving us this opportunity and we assure you full assistance in securing information and IT infrastructure in the long run.

## 6 Disclaimer & Limitations

This report is solely for use by the management and relevant information technology (IT) department of the TNeGA - Directorate of Medical and Rural Health Services. Recipients of this report should not circulate, quote or reproduce this report in any form, without the prior written consent of the management of the TNeGA - Directorate of Medical and Rural Health Services.

The specific IP addresses and domain names were provided by the TNeGA - Directorate of Medical and Rural Health Services. Our subsequent testing, the study of issues in detail, and the developing of action plans are directed toward the identified issues. The vulnerabilities identified were limited to the time period of the test.

The scope of the engagement was limited to the IP Address as stated in section 1.1.1 (Scope).

The assessment was performed:

- Without any detailed knowledge of the target TNeGA - Directorate of Medical and Rural Health Services technical and architecture details.
- Without any access to the design/source code of various applications hosted on the target assets.

## 7 Annexure

### Open Web Application Security Project Framework (OWASP)

The Open Web Application Security Project (OWASP) is a worldwide not-for-profit charitable Organization. The OWASP Web Application Penetration Testing method is based on the black box approach. The tester knows nothing or very little information about the application to be tested. The test is divided into 2 phases:

**Passive mode:** where the tester tries to understand the application's logic and plays with the application. Tools can be used for information gathering, for example, an HTTP proxy to observe all the HTTP requests and responses. At the end of this phase, the tester should understand all the access points (gates) of the application.

**Active mode:** In this phase, the tester begins to test using the following set of active tests in 9 sub-categories for a total of 66 controls:

Testing Sub Categories	
Configuration Management Testing	Authorization Testing
Business Logic Testing	Data Validation Testing
Authentication Testing	Denial of Service Testing
Session Management Testing	Web Services Testing
Ajax Testing	

### The Open Source Security Testing Methodology Manual (OSSTMM)

Open Source Security Testing Methodology Manual (OSSTMM) was written by Pete Herzog and is being distributed by Institute for Security and Open Methodologies (ISECOM). It gives a road description of categories of testing, and it includes step-by-step process description and information on penetration testing tools.

### National Institute of Standards and Technology (NIST)

The United States National Institute of Standards and Technology (NIST) has released a document called as Technical Guide to Information Security Testing and Assessment which addresses and covers network penetration testing methodologies at a high level.

### CVE - Common Vulnerabilities and Exposure

Common Vulnerabilities and Exposures is a dictionary of common names (i.e., CVE Identifiers) for publicly known information security vulnerabilities. CVE's common identifiers make it easier to share data across the separate network, security databases, and tools and provide a baseline for evaluating the coverage of an organization's security tools. The process of creating a CVE Identifier begins with the discovery of potential security vulnerabilities.

## 8 List of tools used

No	Tool Name	Description
1	NESSUS Vulnerability assessment tool.	Key features include remote and local (authenticated) security checks, a client/server architecture with a GTK graphical interface, and an embedded scripting language for writing your plugins or understanding the existing ones.
2	Web Vulnerability Scanner	Web Vulnerability Scanner automatically checks applications for vulnerabilities specific to the web applications such as SQL Injection, cross-site scripting, Weak session management secure authentication, etc.
3	Burp Suite	Allows an attacker to combine manual and automated techniques to enumerate, analyze, attack, and exploit web applications. The various burp tools work together effectively to share information and allow findings identified within one tool to form the basis of an attack using another.
4	Metasploit Framework	It is an advanced open-source platform for developing, testing & using exploit code. It ships with hundreds of exploits. This makes writing your exploits easier, and it certainly beats scouring the darkest corners of the Internet for illicit shell code of dubious quality.
5	Nmap	Nmap ("Network Mapper") is an open-source (license) utility for network exploration or security auditing. System and network administrators find it useful for tasks such as OS fingerprinting

## 9 Contact Us



Auriseq Consulting Private Limited

Email: [info@auriseq.com](mailto:info@auriseq.com)

India: +91 99408 71528

Head Office:

#17 / 22, Valliyammai Street,  
 Vijayalakshmi Nagar, Chromepet  
 CHENNAI, TAMIL NADU 600044  
 India