

**Dynamic Vulnerability Assessment**

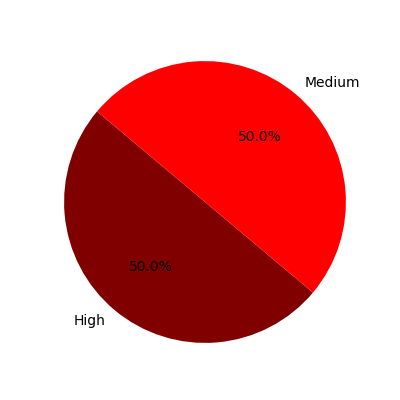
**Ratihngs Xpress DVA\_Broad**

**Requested by:** Jayaram Yalla

## Version Information

|  |  |  |
| --- | --- | --- |
| Date | Application Version | Reviewer |
| 02-May-2025 | Initial Draft | Bhanu Mudigonda |
| 02-May-2025 | Peer Review |  |
| 02-May-2025 | Approved |  |

**Vulnerability Severity Distribution**



## Summary Table

|  |  |  |  |
| --- | --- | --- | --- |
| Sl. No. | Security Observation | Risk Rating | Page No. |
| **High Severity** | | | |
| 1 | Insecure Transport: Weak SSL Ciphers | High | 4 |
| **Medium Severity** | | | |
| 2 | HTML5: Overly Permissive CORS Policy | Medium | 5 |

## URLs and Scope

URLs: https;//zero.webappsecurity.com

Scope: Entire applciation is in scope except adding new users

## Vulnerability Details

### 1. Insecure Transport: Weak SSL Ciphers

**Severity: High**

CVSS Score: 8.9

CVSS Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:H/A:H

#### Description

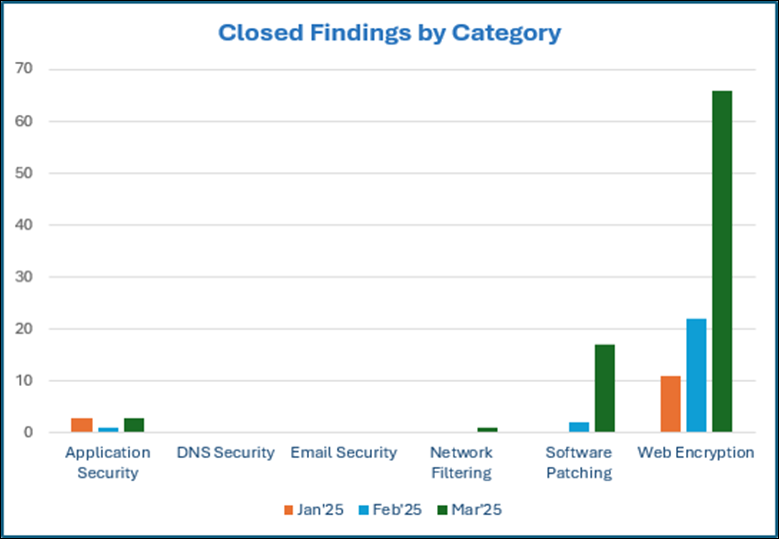
Improper The Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols provide a  
mechanism to help protect authenticity, confidentiality and integrity of the data transmitted between a  
client and web server. The strength of this protection mechanism is determined by the authentication,  
encryption and hashing algorithms. These are collectively known as a cipher suite chosen for the  
transmission of sensitive information over the TLS/SSL channel. Most web servers support a range of such  
cipher suites of varying strengths. Using a weak cipher or an encryption key of insufficient length, for  
example, could enable an attacker to defeat the protection mechanism and steal or modify sensitive  
information. If misconfigured, a web server could be manipulated into choosing weak cipher suites. A  
weak encryption scheme can be subjected to brute force attacks that have a reasonable chance of  
succeeding using current methods and resources. An attacker could possibly execute a man in the middle  
attack which would allow them to intercept, monitor and tamper with sensitive data. Each weak cipher  
was enumerated by establishing an SSL connection with the target host and specifying the cipher to test  
in the Client Hello message of the SSL handshake.

#### Evidence

Step 1: This is a test to upload text and images



Step 2: This is a test to upload text and images



#### Recommendation

It is recommended not to use RC4, CBC,SHA, SHA1, MD5 etc ciphers

#### Reference

https://www.acunetix.com/blog/articles/tls-ssl-cipher-hardening/  
http://zero.webappsecurity.com

### 2. HTML5: Overly Permissive CORS Policy

**Severity: Medium**

CVSS Score: 6.5

CVSS Vector: CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L

#### Description

Cross-Origin Resource Sharing, commonly referred to as CORS, is a technology that allows a domain to  
define a policy for its resources to be accessed by a web page hosted on a different domain using cross  
domain XML HTTP Requests (XHR). Historically, the browser restricts cross domain XHR requests to abide  
by the same origin policy. These restrictions are managed by access policies typically included in  
specialized response headers, such as: Access-Control-Allow-Origin, Access Control-Allow-Headers,  
Access-Control-Allow-Methods. A domain includes a list of domains that can make cross domain requests  
to shared resources in Access Control-Allow-Origin header. This header can have either list of domains or  
a wildcard character (“\*”) to allow all access. Having a wildcard is considered overly permissive policy.

#### Evidence

Step 1: This is a test to upload text and images



#### Recommendation

Review the Cross-Origin-Resource-Sharing policy and consider restricting access to only trusted domains.  
Never use wildcard open-access permissions (e.g. “\*”) in the Access-Control-Allow-Origin header.  
Additionally, do not automatically include Access-Control-Allow-Origin headers in the response unless the  
request is cross-domain. Alternatively, implement a whitelist of known domains that can access this  
domain and only include domains that tried to access the resource. Otherwise, reject the request and  
reply with only host domain not exposing all allowed domains. Please note that this needs to be  
implemented throughout the application as a best practice.

#### Reference

https://en.wikipedia.org/wiki/Cross-origin\_resource\_sharing