NEW FRONTIERS. NEW DREAMS

Web Application Security Assessment Report

1. Project Information

Organization	BEML
Application Name	BEML
Scope URL	https://bemlproto.crm-doctor.com/
Application type	UAT
Testing Start Date & End Date	5th July 2022
Testing Team Information	Yashil

Table of Contents

1. Project Information 1
2. Executive Summery 2
3. Summary of Vulnerability 3
4. Detailed Observations and Recommendations 5

Appendix A: OWASP Category 7

Appendix B: Definitions 8

2. Executive Summery

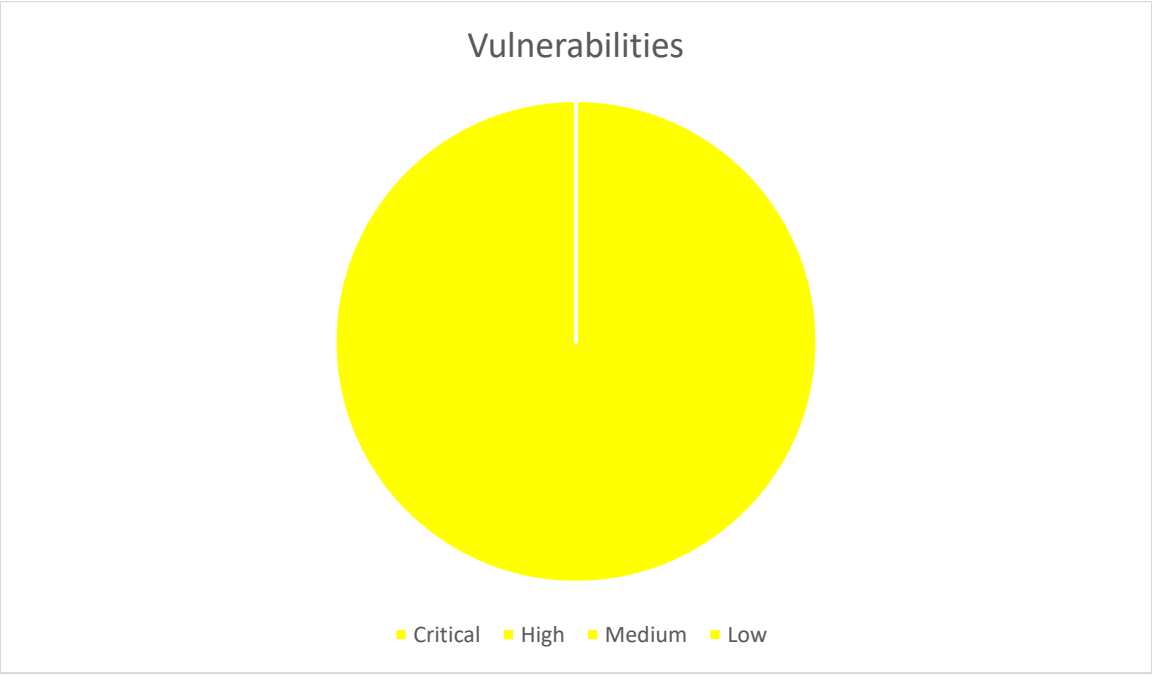
Biztechnosys performed the revalidation test on BEML web application belonging to BEML on 5th July 2022. This report presents the results of the penetration test that was conducted with no prior knowledge of the web application.

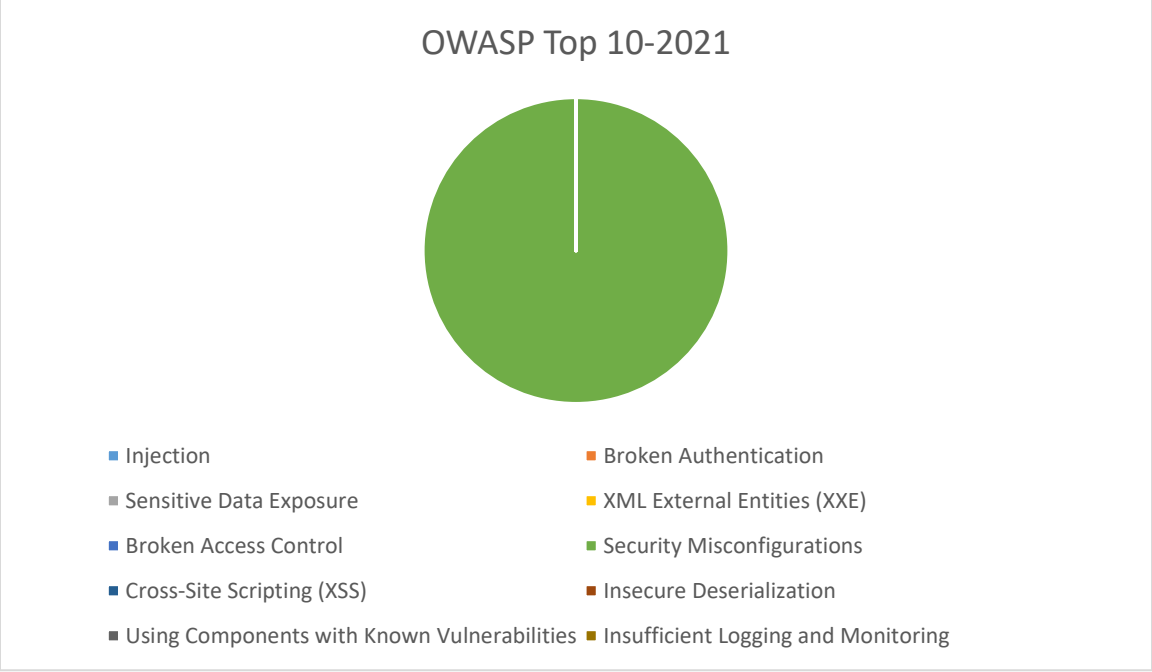
Scope URL: https://bemlproto.crm-doctor.com/ (UAT)

3. Summary of Vulnerability

The re-test found the 1 Low Risk vulnerability. There were the summarized below

The risk ratings used in this report are explained in the “Definitions” Section.





Sr. No	Title	Risk	Revalidation Status	Remediation comments
1	WordPress XML-RPC authentication brute force	Medium	Closed	
2	An attacker can access the sensitive API without any authentication.	Medium	Closed	
3	Attacker can spam the user by sending multiple requests using public forms.	Low	Open	Malcare WordPress Security Premium Plugin will be enabled on Production server to implement the Rate limit.

Application Strength:

It was observed that user inputs are properly sanitized and WordPress security plugins like Mod_Securty is installed properly.

4. Detailed Observations and Recommendations

1. WordPress XML-RPC authentication brute force

Status: Closed

Observation:
The vulnerability has been fixed.

Impact:
An attacker can access the System information or can perform the Brute force attack.

Risk: Medium

Solution:
It is possible to disable the XML-RPC script if you do not want to use it. Consult references for a WordPress plugin that does that. If you don't want to disable XML-RPC you can monitor for XML-RPC authentication failures with a Web Application Firewall like ModSecurity.

Reference:
https://wordpress.org/plugins/prevent-xmlrpc/
https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/honeypot-alert-wordpress-xml-rpc-brute-force-scanning/

Proof of concept:

The following screenshot shows the XMLRPC page is not accessible

2. An attacker can access the sensitive API without any authentication.

   Status: Closed

   Observation:
   The vulnerability has been fixed.

   Impact:
   An attacker can utilize this information to perform bruteforce attack.

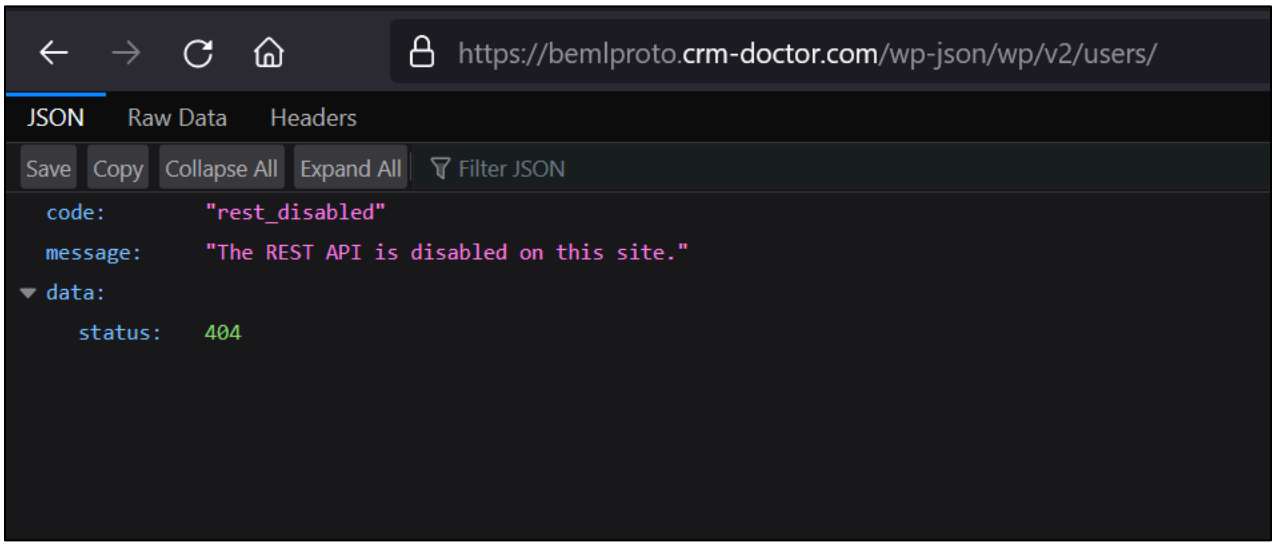
   Risk: Medium

   Solution:
   Restrict the API access.

   Reference:
   https://www.jinsonvarghese.com/prevent-wordpress-username-enumeration/

   Proof of concept:

   The REST-API is not accessible



3. Attacker can spam the user by sending multiple requests using public forms.

   Status: Open

   Observation:
   It was observed that the application has multiple public forms where user can enter and submit the values. The later respective owner can revert on the query.

   However, the forms do not have CAPTCHA or rate limiting which allow attacker to spam the email box.

   Impact: An attacker can spam the email box.

   Risk: Low

   Solution:
   Implement the CAPTCHA
   Implement the Rate limiting

   Reference:
   https://code.tutsplus.com/tutorials/how-to-build-rate-limiting-into-your-web-app-login--cms-22133

   Proof of concept:
   The following URL does not have CAPTCHA implemented.
   - https://bemlproto.crm-doctor.com/feedback/
   - https://bemlproto.crm-doctor.com/online-investor-complaints/
   - https://bemlproto.crm-doctor.com/online-vigilance-complaints/
   - https://bemlproto.crm-doctor.com/online-complaint-status/
   - https://bemlproto.crm-doctor.com/contact/
   - https://bemlproto.crm-doctor.com/careers/

Appendix A: OWASP Category

OWASP Top 10- 2021	Status
Injection	Safe
Broken Authentication	Safe
Sensitive Data Exposure	Safe
XML External Entities (XXE)	Safe
Broken Access Control	Safe
Security Misconfigurations	Unsafe
Cross-Site Scripting (XSS)	Safe
Insecure Deserialization	Safe

Using Components with Known Vulnerabilities	Safe
Insufficient Logging and Monitoring	Safe

Appendix B: Definitions

Symbol	Definition
High	These are the findings that can be exploited easily and have high impact when exploited.
Medium	These are the findings that do not pose an immediate risk to your system, but may do so over time.
Low	Findings that are very difficult, special requirment or low impact.
Info	Findings that are very difficult to exploit in practice
N/A	Requirement is not applicable
Unconfirmed Vulnerabilities	A vulnerabilities reported based on the identified the version.