CyberSecurityWorks Pvt. Ltd

E-3, Third Floor, 599 Anna Salai,
Chennai - 600 006. Tamil Nadu, India.
Tel : +91 44 4208 9337, 2825 5242
Fax : +91 44 2825 5242
info@cybersecurityworks.com
www.cybersecurityworks.com

Security Certificate

(**Unique Ref No: CSW-SC-05-072019**)

Audit Performed by: Cyber Security Works Pvt. Ltd.

Application Name: National Assessment and Accreditation Council (NAAC) Web Application

Staging URL on which the audit has been performed: http://218.248.45.210/naacvapt/public/index.php

Production URL of the web application: https://assessmentonline.naac.gov.in/

Audit Details:

Name	Lourdhuraj P
Email	lourdhuraj@cybersecurityworks.com
Telephone	+91-44-42089337
Level - 01 Assessment date	01-10-2018 to 05-10-2018
Level - 02 Assessment date	05-11-2018 to 09-11-2018
Level - 03 Assessment date	30-01-2019 to 04-02-2019
Level - 04 Assessment date	01-04-2019 to 04-04-2019
Level - 05 Assessment date	28-05-2019 to 30-05-2019
Issue Date	25-07-2019
Validity	Till no modification or until 24-07-2020 (whichever is earlier)
Unique Reference No.	CSW- SC- 05 – 072019

Audit for the National Assessment and Accreditation Council (NAAC) web application was completed on the staging server URL http://218.248.45.210/naacvapt/public/index.php from CSW office, Chennai. During the initial assessment of the web application, following vulnerabilities were discovered in the application.

CYBER SECURITY WORKS PVT. LTD. CHENNAI 600 006

CyberSecurityWorks Pvt. Ltd
E-3, Third Floor, 599 Anna Salai,
Chennai - 600 006. Tamil Nadu, India.
Tel : +91 44 4208 9337, 2825 5242
Fax : +91 44 2825 5242
info@cybersecurityworks.com
www.cybersecurityworks.com

Some of the issues were fixed by the development team, except **#5 Sensitive Data Exposure, #8 Weak Ciphers, #9 Malicious File Upload, #13 Host Header Attack, #16 Vulnerable jQuery version Found and #18 Response Headers. These 6 issues have to be fixed on the production server before going live.**

1. SQL Injection
2. Cross Site Scripting
3. Session Management
4. HTML Injection
5. Sensitive Data Exposure *
6. Cross Site Request Forgery
7. External Service Interaction (DNS & HTTP)
8. Weak Ciphers *
9. Malicious File Upload *
10. Missing Input Validation
11. URL Rewrite Vulnerability
12. Security Misconfiguration
13. Host Header Attack *
14. Automation Attack
15. Password Field Autocomplete Enabled
16. Vulnerable jQuery version Found *
17. User Enumeration
18. Response Headers *

*** Vulnerability should be fixed on the production server before going live.**

CONCLUSION:

Audit for National Assessment and Accreditation Council (NAAC) web application was conducted between **October 01, 2019 to October 05, 2018** on the staging server URL http://218.248.45.210/naacvapt/public/index.php by Cyber security Works Pvt. Ltd. The follow-up audits were conducted November 05, 2018 – November 09, 2018, January 30, 2019 – February 04, 2019, April 01, 2019 – April 04, 2019 and May 28, 2019 – May 30, 2019.

There is pending nonconformity w.r.t OWASP Top 10, 2017 as on May 30, 2019 as the following issues - Sensitive Data Exposure, Weak Ciphers, Malicious File Upload, Host Header Attack and Vulnerable jQuery Version Found and Response headers have not been resolved on the environment that was tested. **These 6 issues have to be fixed on the production server before going live along with the recommendations listed below.**

CYBER SECURITY WORKS PVT. LTD. CHENNAI 600 006

CyberSecurityWorks Pvt. Ltd
E-3, Third Floor, 599 Anna Salai,
Chennai - 600 006. Tamil Nadu, India.
Tel : +91 44 4208 9337, 2825 5242
Fax : +91 44 2825 5242
info@cybersecurityworks.com
www.cybersecurityworks.com

Recommendations:

a) The entire application should be hosted with read permission only.

b) The database user mentioned in the connection string of the application should be with low level privilege and the database user password should be in encrypted format.

c) Any folder in which files are uploaded through the web application should have only read and write permission. No execute permission should be given.

d) SSL should be enabled on production server. HttpOnly and secure flags should be enabled on all session ids and cookies.

e) Web server/framework and OS level hardening must be completed on the production servers.

f) The 6 pending issues (Sensitive Data Exposure, Weak Ciphers, Malicious File Upload, Host Header Attack, Vulnerable jQuery Version Found and Response headers) have to be fixed on the production server before going live.

CYBER SECURITY WORKS PVT. LTD. CHENNAI 600 006

Ravi Pandey
(Lead- Technical)
For Cyber Security Works Pvt. Ltd.

Date : 02-08-2019

Place : Chennai