Mirox Cyber Security & Technology Pvt Ltd 4th Floor Nila Technopark 695581
Trivandrum Kerala India Ph: + 91-471- 4016888, 4000545. www.miroxindia.com
Mirox is Empanelled as an IT Security Auditor by CERT-In (Govt. of India)

SECURITY AUDIT CERTIFICATE

Ref : MI-CERT/IND-037/2021 Dated : 17-09-2021

This is hereby certified that Web Application/Site URL: **https://joinus-auto.iitpkd.ac.in/** , Static IP: **61.0.251.139 :443** is been Security Audited & Assessed as per CERT-IN Guideline & OWASP Standard. The Site & Web Application is fit and safe for hosting under continuous monitoring and observation by Authorized Authorities. The Application/Site is fulfilled the criteria as per CERT-IN Security norms.

The Security Audit and Penetration Test was conducted by Mirox Cyber Security's certified security engineers. We identified several Vulnerabilities and provided remediation advice to **Indian Institute of Technology, Palakkad** that all vulnerabilities had been Security Tested & verified. Mirox performed a verification security test on **24th May 2021** to **10th September 2021** and confirmed that all vulnerabilities identified were either fixed & rectified or had been adequately addressed through other controls.

While no application or system can be 100% secure, all of our security findings were rectified /corrected or addressed and it is our opinion that the applications tested are reasonably well written from a security perspective and the applications and supporting systems are deployed, configured and implemented in a secure manner. Application to remain secure, however, security posture must be evaluated and improved continuously.

S.No	Details	Details
1	Application Name	**IIT Palakkad Staff Recruitment Portal Web Application.**
2	Application URL name & IP	Application URL: **https://joinus-auto.iitpkd.ac.in/** Application IP – 61.0.251.139 :443
3	Applications Tested URL - IP Details	Tested IP: **61.0.251.139** Port: **443** Tested URL: **https://joinus-auto.iitpkd.ac.in/**
4	Testing Report Date	**24th MAY 2021** to **10th SEPTEMBER 2021**
5	Certification Validity	6 months to 1 Year Max from the issue date of the last audit report.

Sl. No.	OWASP 2017 Top 10 Vulnerabilities	No. of Vulnerabilities	Status			
A1	Injection	N/A	N/A			
A2	Broken Authentication	N/A	N/A			
A3	Sensitive Data Exposure	2	1 Fixed – High	1 Fixed - Medium		
A4	XML External Entities (XXE)	N/A	N/A			
A5	Broken Access Control	N/A				
A6	Security Misconfiguration	7	2 Fixed – High	1 Fixed – Medium	3 Fixed – Low	1 Fixed – Info
A7	Cross-Site Scripting (XSS)	1	1 Fixed – High			
A8	Insecure Deserialization	N/A	N/A			
A9	Using Components with Known Vulnerabilities	1	1 Fixed - Medium			
A10	Insufficient Logging & Monitoring	N/A	N/A			

Disclaimer

Mirox Cyber Security & Technology conducted this Audit/ Assessment/ VAPT on the applications and systems that existed as of **10th September 2021**. Information security threats are continually changing, with new vulnerabilities discovered on a daily basis, and no application can ever be 100% secure no matter how much Security Auditing, Assessment & Testing is conducted.

This report & certificate cannot and does not protect against personal or production loss as the result of use of the applications or systems described. Mirox offers no warranties, representations or legal certifications concerning the applications or systems it tests. All software includes defects: nothing in this document is intended to represent or warrant that security testing was complete and without error, nor does this document represent or warrant that the application tested is suitable to task, free of other defects than reported, fully compliant with any industry standards, or fully compatible with any operating system, hardware, or other application.

This is a computer-generated document. No signature is required. In case of any hard-copy required receive in any manner should be confirmed by Mirox through Sealing & Sign by Authorized Auditors.

This report contains sensitive information about the security state of IT systems and data assets. The data within this report must be treated with the same level of protection as the assets themselves, and should be classified as 'confidential' or 'restricted'. By accepting this document you agree to keep the contents in confidence and not copy, disclose, or distribute this without written request to and written confirmation from the Information Owners. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of the contents of this document is strictly prohibited.

Services Performed For:

Indian Institute of Technology Palakkad
Ahalia Integrated Campus,
Kozhippara P.O, Palakkad
Kerala , Pin: 678557

ValueMentor Consulting LLP
Chandanam, Infopark Thrissur,
Koratty, Kerala, India - 680 308

Cert No: VM/IND/2018/116 **Date of Issue: 16-03-2018**

Security Audit Certificate

ValueMentor Security Assessment Testing Program has tested and certified the following application.

Application Name	:	Website of IIT-Palakkad
Production URL	:	https://iitpkd.ac.in
URL Tested	:	https://iitpkd.ac.in
Testing Date	:	12th Febrauary, 2018 to 15th March, 2018
Auditing Performed By	:	ValueMentor Consulting LLP

Observation (in Details): The page hosted on production server was tested against OWASP Top 10 and other known vulnerabilities.

Conclusion: Application was found safe to host for its production usage.

Recommendations:

1. Web server and OS level hardening need to be in place for the production server.
2. Site may be hosted with the privileges of read only permission for the general public.
3. Write permission should be granted only on the folder where the files are to be uploaded.
4. It is recommended to deploy the site over TLS with recommended practices.

Jithu T George
Program Manager

Certificate Validity: The certificate is valid for a period of one year from the issue date or until a new version of the application is released, whichever date is earlier.

ValueMentor Consulting LLP
Chandanam, Infopark Thrissur,
Koratty, Kerala, India - 680 308

Appendix: Certification Status

The application was tested against the CERT-IN recommended certification standards and the table below shows the overall status of the application against the certification criteria. The different status that can be assigned to each criteria are "Meets Criteria", "Fails Criteria" or "Not Applicable" based on the vulnerabilities discovered in the application.

Security Requirement Criteria		
#	**Criteria Label**	**Status**
1	Injection	Meets Criteria
2	Broken Authentication	Meets Criteria
3	Sensitive Data Exposure	Meets Criteria
4	XML External Entities (XXE)	Meets Criteria
5	Broken Access Control	Meets Criteria
6	Security Misconfiguration	Meets Criteria
7	Cross-Site Scripting (XSS)	Meets Criteria
8	Insecure Deserialization	Meets Criteria
9	Using Components with Known Vulnerabilities	Meets Criteria
10	Insufficient Logging&Monitoring	Meets Criteria