



Application Security Assessment Questionnaire

These questions are intended to help Auriseg scope the amount of effort that will be required to perform an application penetration testing. You can find additional information on our mobile application penetration testing, network security testing, code review and other services on our website at <https://auriseg.com> If you have any questions or would feel more comfortable discussing these questions with Auriseg VAPT Team, please contact us directly on +91-9940864275 or srini.mani@auriseg.com

	Question	Response									
Background	Customer Contact: <ul style="list-style-type: none"> ■ Name & title or role ■ Name of company/division ■ Mailing address ■ Phone ■ E-Mail address 	Name: Mr. Pankaj Dixit Company: Lata Dixit Tech Pvt. LTd. Phone: 9422044832 Email: Pankaj@latadixit.tech									
	Application Name	Sugarian									
	Business Functionality/Purpose	ERP Software									
	Purchased or Developed in House	<input type="checkbox"/> Purchased Application <input checked="" type="checkbox"/> Y <input type="checkbox"/> Developed in House <input type="checkbox"/> Out-Sourced Development									
Implementation	How is the Application Consumed: (Check all that apply)	<input checked="" type="checkbox"/> Y <input type="checkbox"/> Web Browser <input type="checkbox"/> Thick Client <input type="checkbox"/> Mobile Web App <input type="checkbox"/> Mobile Client <input type="checkbox"/> Web Services <input type="checkbox"/> Other									
	Description:										
	Communication Protocols:	<input type="checkbox"/> HTTP <input checked="" type="checkbox"/> Y <input type="checkbox"/> HTTP(S) <input type="checkbox"/> SOAP <input type="checkbox"/> SOAP(S) <input checked="" type="checkbox"/> Y <input type="checkbox"/> REST <input type="checkbox"/> Serialized Objects <input checked="" type="checkbox"/> Y <input type="checkbox"/> TCP(S) <input checked="" type="checkbox"/> Y <input type="checkbox"/> WebSockets <input type="checkbox"/> Custom									
	Explain Custom:										
	Number Screen, Fields, Files, Functions, Total Size (in MB) (estimation is ok)	<table border="1"> <thead> <tr> <th>Screens/Pages</th> <th>Fields</th> <th>Files</th> <th>Functions</th> <th>Size</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td>Frontend: 36M Backend: 54M</td> </tr> </tbody> </table>	Screens/Pages	Fields	Files	Functions	Size				
Screens/Pages	Fields	Files	Functions	Size							
				Frontend: 36M Backend: 54M							
How many users and roles does the application support?	<table border="1"> <thead> <tr> <th># of Roles</th> <th>2</th> <th>Admin, Users</th> </tr> </thead> <tbody> <tr> <th># of Users</th> <td>17</td> <td>Admins: 3 Users: 14</td> </tr> </tbody> </table>	# of Roles	2	Admin, Users	# of Users	17	Admins: 3 Users: 14				
# of Roles	2	Admin, Users									
# of Users	17	Admins: 3 Users: 14									
	Briefly explain how authorization is implemented: JSON Web Token										

	Question	Response							
	Architectures and Frameworks	Y	MVC (e.g. JSF, Struts, Spring MVC, ASP.NET MVC,)	Data Access (e.g. Hibernate, EJB, JDBC, ODBC)	Remoting (CORBA, .Net Remoting, RMI)				
			Dependency Injection (e.g. Spring, AngularJS)	AOP (e.g. AspectJ, Groovy, PHP, Python, Ruby)	RIA (e.g. AngularJS, Flex, GWT, Cordova, Kendo UI, Sencha)				
			SOA (e.g. WCF, JAX-WS, CXF)	Other					
		Explain Other: Backend in Flask, Frontend in Reactjs, MSSQL database							
	Briefly describe how authentication is implemented.	JSON Web Token							
	API's List and No of API's	More than 200 APIs							
Risk	How is application accessed?	Y	Internet		Intranet				
			Authenticated Internet		VPN				
	Assets	Y	Financial Information	Y	Ecommerce	Trade Secrets			
		Y	Financial transactions		Credit cards	Personally Identifiable Info (PII)			
			Health information		Passwords	Intellectual Property			
	Connectivity	Y	External Data Feeds		LDAP	Y	Other websites		
		Y	Web services	Y	Databases	Y	File Transfer/dump		
		Y	Email	Y	Messaging		Other		
Explain Other:									
What are your most important security concerns for the application?									
Are you aware of any vulnerabilities now?	We need to Security Testing against Internal/ Authentication Applications								
Specific regulations?		PCI		HIPAA		FISMA			
		SOX		COPA		NIST 800-53/800-30			
		GLB		DMCA		SOC			
Project Information	Lifecycle stage		Design		Development		QA	Y	Production

Question		Response				
	Tests being requested	Code Review	Y	Black Box Penetration Testing	Y	Grey Box Penetration Testing
		Architecture Review				
	Target Dates	Date available for review		03/11/2025		
		Date review must be complete				
	Test Logistics	Y	Can test system be accessed remotely?	Will mobile test devices be provided (If applicable)?	Can code and design / architecture documents be reviewed in Auriseg Labs?	
	Any additional information?					