



## 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](mailto:srini.mani@auriseg.com)

	Question	Response															
Background	Customer Contact: <ul style="list-style-type: none"> <li>■ Name &amp; title or role</li> <li>■ Name of company/division</li> <li>■ Mailing address</li> <li>■ Phone</li> <li>■ E-Mail address</li> </ul>	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 Develpoed in House	<table border="1"> <tr> <td>Purchased Application</td> <td>Y</td> <td>Developed in House</td> <td>Out-Sourced Development</td> </tr> </table>	Purchased Application	Y	Developed in House	Out-Sourced Development											
Purchased Application	Y	Developed in House	Out-Sourced Development														
Implementation	How is the Application Consumed: (Check all that apply)	<table border="1"> <tr> <td>Y</td> <td>Web Browser</td> <td>Thick Client</td> <td>Mobile Web App</td> </tr> <tr> <td></td> <td>Mobile Client</td> <td>Web Services</td> <td>Other</td> </tr> </table> Description:	Y	Web Browser	Thick Client	Mobile Web App		Mobile Client	Web Services	Other							
	Y	Web Browser	Thick Client	Mobile Web App													
		Mobile Client	Web Services	Other													
	Communication Protocols:	<table border="1"> <tr> <td></td> <td>HTTP</td> <td>Y</td> <td>HTTP(S)</td> <td>SOAP</td> </tr> <tr> <td></td> <td>SOAP(S)</td> <td>Y</td> <td>REST</td> <td>Serialized Objects</td> </tr> <tr> <td>Y</td> <td>TCP(S)</td> <td>Y</td> <td>WebSockets</td> <td>Custom</td> </tr> </table> Explain Custom:		HTTP	Y	HTTP(S)	SOAP		SOAP(S)	Y	REST	Serialized Objects	Y	TCP(S)	Y	WebSockets	Custom
		HTTP	Y	HTTP(S)	SOAP												
	SOAP(S)	Y	REST	Serialized Objects													
Y	TCP(S)	Y	WebSockets	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					Frontend: 36M Backend: 54M						
Screens/Pages	Fields	Files	Functions	Size													
				Frontend: 36M Backend: 54M													
How many users and roles does the application support?	<table border="1"> <tr> <td># of Roles</td> <td>2</td> <td>Admin, Users</td> </tr> <tr> <td># of Users</td> <td>17</td> <td>Admins: 3 Users: 14</td> </tr> </table> Briefly explain how authorization is implemented: JSON Web Token	# of Roles	2	Admin, Users	# of Users	17	Admins: 3 Users: 14										
# of Roles	2	Admin, Users															
# of Users	17	Admins: 3 Users: 14															

	Question	Response							
	Architectures and Frameworks	Y	<b>MVC</b> (e.g. JSF, Struts, Spring MVC, ASP.NET MVC, )	<b>Data Access</b> (e.g. Hibernate, EJB, JDBC, ODBC)	<b>Remoting</b> (CORBA, .Net Remoting, RMI)				
			<b>Dependency Injection</b> (e.g. Spring, AngularJS)	<b>AOP</b> (e.g. AspectJ, Groovy, PHP, Python, Ruby)	<b>RIA</b> (e.g. AngularJS, Flex, GWT, Cordova, Kendo UI, Sencha)				
			<b>SOA</b> (e.g. WCF, JAX-WS, CXF)	<b>Other</b>					
		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							
<b>Risk</b>	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				
<b>Project Information</b>	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?					