Application Security Assessment: Scoping Form

1. Application Information

Application Name:	
Application URL(s):	
Point of Contact (with email):	

2. Technical Details

Please describe the functionality of the app:
What are the components (i.e., customer portal, Admin/config app, WebAPI):
Describe the architecture:
Backend platform details (i.e., ASP.NET, SQL Server, IIS7, etc.):
Describe any secure data and how obtained and stored (i.e., HIPAA, PII, SSN and other Sensitive Data):
Is Credit Card data obtained or processed? Does the app interface with a Credit Card Payment processor?

3. Application Users

Who are the intended users of each application (i.e., Gov Agency, Public Citizens, Granicus Only):
Are there different levels of access control (i.e., Super Admin, Admin, Power User, User):
What applications, pages, areas are open without a login:

Any special requirements to setting up a user (i.e., self-serve public account, admin activation, etc):

4. Authentication

Question	Yes	No	NA	Comments
Is SSO supported? If yes, indicate the mechanism in comments.	☐	☐	☐	
Is MFA Supported? If yes, indicate the mechanism in the comments.	☐	☐	☐	
Does the application force “new” users to change their password upon first login into the application?	☐	☐	☐	
Does the application support complex passwords?	☐	☐	☐	
Can the application force password expiration and prevent users from reusing a password?	☐	☐	☐	
Are passwords HASHED (not encrypted) in storage? If yes, what is the hash algorithm.	☐	☐	☐	
Are encryption keys stored in a secure location, separate for the application (i.e., Azure Key Vault)? If yes, indicate the storage mechanism.	☐	☐	☐	
Are passwords ever returned to the client in away way, include password reset email, temp password, etc.?	☐	☐	☐	
Does the application support account lock on failed login? If yes, indicate the number of unsuccessful attempts.	☐	☐	☐	
Does the application prohibit users from logging into the application on more than one workstation at the same time with the same user ID?	☐	☐	☐	
Can an administrator lock/disable a user’s account?	☐	☐	☐	

What is your authentication design? Basic Authentication, Forms Auth?
Do you have any backdoors, maintenance hooks, or other mechanisms/designs that do not follow your standard authentication process (i.e., Anonymous Users)?

Question	Highly	Mod	Low	Very Low	Comments
How confident are you in the app's Authentication mechanisms?	☒	☒	☒	☒	
Are there areas of the app or pages you are concerned about Authentication? Areas we should "target"?					

5. Sessions

How does the app implement Session IDs? In URLs, cookies, form data? Sequential Numbers or GUIDs?
Do sessions expire? If so, hard expire or on inactivity? What is the default time out?
How are sessions terminated (i.e., Log out button on every page)?

Question	Highly	Mod	Low	Very Low	Comments
How confident are you in the app's Session Handling?	☐	☐	☐	☐	
How confident are you in the app's AntiCSRF Defense?	☐	☐	☐	☐	
Are there areas of the app or pages you are concerned about Sessions? Stealing sessions? Exposed JWTs? Areas we should "target"?					

6. Authorization

Question	Highly	Mod	Low	Very Low	Comments
How confident are you that AuthZ is checked on every single request?	☐	☐	☐	☐	
How do you prevent against Insecure Direct Object Reference (IDOR), changing sequential IDs in the query string, or form data, where a user gets access to an object they should not?					
Are there areas of the app or pages you are concerned about Authorization? Areas we should "target"?					

7. Cross Site Scripting (XSS)

Please explain the app's XSS defenses?
Does the app validate input/detect XSS from all user input controls including the query string?
Does the app encode all user output?
Does the app allow for an administrator to enter and store javascript (i.e., Private Labeling)?

Question	Highly	Mod	Low	Very Low	Comments
How confident are you with the app's XSS Defenses?	☐	☐	☐	☐	
Are there areas of the app or pages you are concerned about XSS? Areas we should "target"?					

8. SQL Injection (SQLi)

Please explain your SQLi defenses? Does the application only use parameterized queries and/or stored procedures? Is all user input validated?

Does the application allow for building dynamic SQL, such as for complex reports (i.e., string sql = "select " + userinput + " from sometable where " + userInputFilters;)?
What set of database permissions is the app running under?

Question	**Highly**	**Mod**	**Low**	**Very Low**	**Comments**
How confident are you with the app's SQLi defenses?	☐	☐	☐	☐	
Are there areas of the app or pages you are concerned about SQLi? Areas we should "target":					

9. Did we miss anything?

Do you have any areas, pages, or functionality of concern? What keeps you up at night? If given dev time, what vulnerable code would you go back and change?