5verflow (Team 5) Security Requirements

Category	Security Requirements ID	Security Requirements	TID [1]	Threat	Mitigation
Input Validation for Client Application	SR 1-1	Client Application must check if the format of input IP address is in valid format	170	attacker can TAMPER the IP address input to extremly long characters that might causes buffer overflow. This attack might break the system or simply leads to DENIAL OF SERVICE	Addressing malformed User Input of IP address. This SR does not address an malicious IP address within a valid range. We categorized that kind of attack into Spoofing, and thus can be handled by secure authentication (SR 3-1).
	SR 1-2	Server and Client should check respectively whether the input for Username field on the Register mode is valid as a filename.	170	An attacker can cause buffer overflow using a very long filename as the input or inability to save a file using special characters	Even on the non-secure mode, the input validation check for filename should be conducted.
	SR 1-3	Client should check if the input of the Port field is within the valid port number range.	170	An attacker can write a very large number or string text at the input of Port field and it can cause buffer overflow.	We need to check whether the input is a type of integer and is within the valid port number to mitigate the risk of wrong inputs.
	SR 1-4	Server and client should check input validation respectively whether the input for video file name field on the Playback mode has video file format such as . mp4.	170	An attacker can cause buffer overflow using a very long filename as the input, and can write a file name which is not a video file format to excute or store malicious binary file.	Even on the non-secure mode, the input validation check for filename should be conducted.
	SR 1-5	Client should check whether the image recevied from server is format of jpeg before displaying it.	N/A	An attacker can modify data which is transmitted from server. A header of jpeg format can be compromised.	If a jpeg header is attacked, the image cannot be displayed using openCV or even any other libraries. Simply, we can check SOI (start of image) byte for jpeg format.
	SR 1-6	Client should compare the number of detected face and the number of its information, which are received from server, and they should be same.	N/A	By tempering of an attacker, the number of detected face cannot be matched to the number of face information.	We will send a face information for an image at server as follows: - Number of detected faces - Face area and username for each deetected faces
Secure Data Transmission	SR 2-1	After connection establishment all the data transferred between server and client must be securely encrypted	N/A	INFORMATION DISCLOSURE of data over the network	Mitigation strategy: TLS Applied only when the application is running on Secure Mode
	SR 2-2	Must check integrity of all the transmitted data between server and client	N/A	TAMPERING of the data over the network	Mitigation strategy: TLS Applied only when the application is running on Secure Mode
Secure Authentication	SR 3-1	Server and Client must mutually authenticate each other with X.509 certificates	98, 105	Server or client might be spoofed by an attacker (SPOOFING) for an unauthorized access	Mitigation strategy: X.509 certificates (TLS)
Secure Data Store	SR 4-1	Images and name of registered users must be stored in secure storage to prevent access from unauthorized users	20, 22	DS1. Face Data Storage may be spoofed by an attacker	Mitigation strategy: Secure Storage (cryptfs or cryptomount) Assume the data is encrypted and not accessible to unauthorized users. This requirement covers all the threats of the data flows between '2.2 Face Recognition' and 'DS1. Face Data Storage'.
			21	Denial of Service by resource consumption attack	
			23	An attacker may read information not inteded for disclosure	
			10, 12	DS2. Certificate Data Storage may be spoofed by an attacker	Mitigation strategy: Secure Storage (cryptfs or cryptomount) Assume the data is encrypted and not accessible to

		SR 4-2	Root and CA certificates must be stored in secure storage	11	Denial of Service by resource consumption attack	Assume the data is encrypted and not accessible to unauthorized users. This requirement covers all the threats of the data flows between '2.1 Server' and 'DS2. Certificate Data Storage'.
				13	An attacker may read information not inteded for disclosure	
		SR 4-3	Client certificates must be stored in secure storage	6,7,8,9	Spoofing, DoS, Information Disclosure attacks on DS3. Certificate Data Storage	Assume APIs for secure stroage is used
	Logging	SR 5-1	Server and client should leave the message about the connection status as a log, respectively.	99, 106	Server and client can claim that they didn't receive the message.	We decided to log only connection history because log size becomes too big if we log every transaction.
	Policy	SR 6-1	Client Application should run on legitimate Windows with firewall and surveillance enabled.	173, 174	DoS Attack of App (Crash, Stop, Input interruptions)	Let OS do it
				175, 176	Elevation of Privilege Attack	

Quality Attribute Requirement Scenario

	Desc.	
Stimulus	Write invalid form of IP address (ex. 123.456.789)	Input validation
Source	User input for IP address	
Environment	Before connecting to JetsonNano server	
Artifacts	Configuration data	
Response	Check whether the input IP address is on the valid range	
Response Measure	100 percent of detecting invalid IP address	
	Desc.	
Stimulus	Sniffing data on network between JetsonNano and user laptop	Data Encryption
Source	Attacker connected on the same network	
Environment	Secure mode operation with connection	
Artifacts	Data on transmission	
Response	Encrypting data during transmission	
Response Measure	100 percent of transmitted data is encrypted	
	Desc.	
Stimulus	connection from unknown client	Authentication
Source	unidentified user	
Environment	Server is listening to connection request	
Artifacts	Server system	
Response	authenticated with 2 factor method	
Response Measure	always deny for authentication failed	

						Likelihood Factors										Impact Factors									
						Threat Agent Factors					Vulnerability Factors					Technical Impact Factors					Business Impact Factors					
Id	Title	Category	Interaction	Description	Final Risk Level	Skill Level	Motive	Opportunity	Size	Ease of Discovery	Ease of Exploit	Awareness	IntrusionDetection	Overall Likelihood	Likelihood Level	Loss of Confidentiality	Loss of Integrity	Loss af Availability	Loss of Accountability	Finalcial Damage	Reputation Damage	Non-compliance	Privacy Violation	Overall Impact	Impact Level
179	Data Flow 16. Display Result Is Potentially Interrupted	Denial Of Service	16. Display Result	An external agent interrupts data flowing across a trust boundary in either direction.	#REF!									#DIV/0!	#REF!									#DIV/0!	#REF!
2	Elevation Using Impersonation	Elevation Of Privilege	2. Request Transmission	1.2 Client may be able to impersonate the context of 1.1 Setting Manager (Special Face ID) in order to gain additional privilege.	#REF!									#DIV/0!	#REF!									#DIV/0!	#REF!
3	Elevation Using Impersonation	Elevation Of Privilege	15. Return Data	1.1 Setting Manager (Special Face ID) may be able to impersonate the context of 1.2 Client in order to gain additional privilege.	#REF!									#DIV/0!	#REF!									#DIV/0!	#REF!
14	Elevation Using Impersonation	Elevation Of Privilege	8. Send Command for Mode	2.2 Face Recognition may be able to impersonate the context of 2.1 Server in order to gain additional privilege.	#REF!									#DIV/0!	#REF!									#DIV/0!	#REF!
15	Elevation Using Impersonation	Elevation Of Privilege	13. Return Image Frame and Analysis Information	2.1 Server may be able to impersonate the context of 2.2 Face Recognition in order to gain additional privilege.	#REF!									#DIV/0!	#REF!									#DIV/0!	#REF!
25	Elevation Using Impersonation	Elevation Of Privilege	10. Return Image Frame	2.2 Face Recognition may be able to impersonate the context of E2. Camera in order to gain additional privilege.	#REF!									#DIV/0!	#REF!									#DIV/0!	#REF!
111	Cross Site Request Forgery	Elevation Of Privilege	14. Send Response	Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting. The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.	#REF!									#DIV/0!	#REF!									#DIV/0!	#REF!
104	Cross Site Request Forgery	Elevation Of Privilege	5. Send Request	Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting. The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.	#REF!									#DIV/0!	#REF!									#DIV/0!	#REF!
121	2.2 Face Recognition May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	10. Return Image Frame	E2. Camera may be able to remotely execute code for 2.2 Face Recognition.	#REF!									#DIV/0!	#REF!									#DIV/0!	#REF!
172	Data Flow Sniffing	Information Disclosure	1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode	Data flowing across 1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.	#REF!									#DIV/0!	#REF!									#DIV/0!	#REF!
178	External Entity E1. User Potentially Denies Receiving Data	Repudiation	16. Display Result	E1. User claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	#REF!									#DIV/0!	#REF!									#DIV/0!	#REF!

						Likelihood Factors										Impact Factors									
						Threat Agent Factors				Vulnerability Factors						Technical Impact Factors				Business Impact Factors					
Id	Title	Category	Interaction	Description	Final Risk Level	Skill Level	Motive	Oppertunity	Size	Ease of Discovery	Ease of Exploit	Awareness	IntrusionDetection	Overall Likelihood	Likelihood Level	Loss of Confidentiality	Loss of Integrity	Loss af Availability	Loss of Accountability	Finalcial Damage	Reputation Damage	Non-compliance	Privacy Violation	Overall Impact	Impact Level
171	Potential Data Repudiation by 1.1 Setting Manager (Special Face ID)	Repudiation	1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode	1.1 Setting Manager (Special Face ID) claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	#REF!									#DIV/0!	#REF!									#DIV/0!	#REF!
177	Spoofing of the E1. User External Destination Entity	Spoofing	16. Display Result	E1. User may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of E1. User. Consider using a standard authentication mechanism to identify the external entity.	#REF!	5	9	7	9	3	5	9	3	6.25	#REF!	9	3	5	7	7	9	2	3	5.625	#REF!
112	Spoofing of the E2. Camera External Destination Entity	Spoofing	9. Request Image Frame	E2. Camera may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of E2. Camera. Consider using a standard authentication mechanism to identify the external entity.	#REF!									#DIV/0!	#REF!									#DIV/0!	#REF!
7	Potential Excessive Resource Consumption for 1.2 Client or DS3. Certificate Data Storage	Denial Of Service	3. Request Certificate	Does 1.2 Client or DS3. Certificate Data Storage take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.	High	5	4	9	4	9	9	6	3	6.13	High	2	1	9	7	1	9	2	3	4.25	Midium
11	Potential Excessive Resource Consumption for 2.1 Server or DS2. Certificate Data Storage	Denial Of Service	6. Request Certificate	Does 2.1 Server or DS2. Certificate Data Storage take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.	High	5	4	9	4	9	9	6	3	6.125	High	2	1	9	7	1	9	2	3	4.25	Midium
21	Potential Excessive Resource Consumption for 2.2 Face Recognition or DS1. Face Data Storage	Denial Of Service	11. Request Image	Does 2.2 Face Recognition or DS1. Face Data Storage take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.	High	5	4	9	4	9	9	6	3	6.125	High	2	1	9	7	1	9	2	3	4.25	Midium
108	Data Flow 14. Send Response Is Potentially Interrupted	Denial Of Service	14. Send Response	An external agent interrupts data flowing across a trust boundary in either direction.	High	5	4	9	4	9	9	6	3	6.125	High	2	9	9	7	1	9	2	3	5.25	Midium
107	Potential Process Crash or Stop for 1.2 Client	Denial Of Service	14. Send Response	1.2 Client crashes, halts, stops or runs slowly; in all cases violating an availability metric.	High	5	4	9	4	9	9	6	3	6.125	High	2	9	9	7	1	9	2	3	5.25	Midium
101	Data Flow 5. Send Request Is Potentially Interrupted	Denial Of Service	5. Send Request	An external agent interrupts data flowing across a trust boundary in either direction.	High	5	4	9	4	9	9	6	3	6.125	High	2	9	9	7	1	9	2	3	5.25	Midium
100	Potential Process Crash or Stop for 2.1 Server	Denial Of Service	5. Send Request	2.1 Server crashes, halts, stops or runs slowly; in all cases violating an availability metric.	High	5	4	9	4	9	9	6	3	6.125	High	2	9	9	7	1	9	2	3	5.25	Midium
120	Data Flow 10. Return Image Frame Is Potentially Interrupted	Denial Of Service	10. Return Image Frame	An external agent interrupts data flowing across a trust boundary in either direction.	Midium	5	1	7	2	3	3	4	1	3.25	Midium	2	1	7	7	1	1	2	3	3	Midium
119	Potential Process Crash or Stop for 2.2 Face Recognition	Denial Of Service	10. Return Image Frame	2.2 Face Recognition crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Midium	5	1	7	2	3	3	4	1	3.25	Midium	2	1	7	7	1	1	2	3	3	Midium
114	Data Flow 9. Request Image Frame Is Potentially Interrupted	Denial Of Service	9. Request Image Frame	An external agent interrupts data flowing across a trust boundary in either direction.	Midium	5	1	7	2	3	3	4	1	3.25	Midium	2	1	7	7	1	1	2	3	3	Midium
174	Data Flow 1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode Is Potentially Interrupted	Denial Of Service	1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode	An external agent interrupts data flowing across a trust boundary in either direction.	High	5	4	9	4	9	9	6	3	6.125	High	2	9	9	7	1	9	2	3	5.25	Midium
173	Potential Process Crash or Stop for 1.1 Setting Manager (Special Face ID)	Denial Of Service	1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode	1.1 Setting Manager (Special Face ID) crashes, halts, stops or runs slowly; in all cases violating an availability metric.	High	5	4	9	4	9	9	6	3	6.125	High	2	9	9	7	1	9	2	3	5.25	Midium
97	Elevation Using Impersonation	Elevation Of Privilege	5. Send Request	2.1 Server may be able to impersonate the context of 1.2 Client in order to gain additional privilege.	Low	1	4	4	2	3	3	4	3	3	Midium	2	1	5	7	1	1	2	3	2.75	Low
1	Elevation Using Impersonation	Elevation Of Privilege	14. Send Response	1.2 Client may be able to impersonate the context of 2.1 Server in order to gain additional privilege.	Low	1	4	4	2	3	3	4	3	3	Midium	2	1	5	7	1	1	2	3	2.75	Low
5	Elevation Using Impersonation	Elevation Of Privilege	1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode	1.1 Setting Manager (Special Face ID) may be able to impersonate the context of E1. User in order to gain additional privilege.	Low	1	4	4	2	3	3	4	3	3	Midium	2	1	5	7	1	1	2	3	2.75	Low
110	Elevation by Changing the Execution Flow in 1.2 Client	Elevation Of Privilege	14. Send Response	An attacker may pass data into 1.2 Client in order to change the flow of program execution within 1.2 Client to the attacker's choosing.	Low	1	4	4	2	3	3	4	3	3	Midium	2	1	5	7	1	1	2	3	2.75	Low
109	1.2 Client May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	14. Send Response	2.1 Server may be able to remotely execute code for 1.2 Client.	Low	1	4	4	2	3	3	4	3	3	Midium	2	1	5	7	1	1	2	3	2.75	Low
103	Elevation by Changing the Execution Flow in 2.1 Server	Elevation Of Privilege	5. Send Request	An attacker may pass data into 2.1 Server in order to change the flow of program execution within 2.1 Server to the attacker's choosing.	Low	1	4	4	2	3	3	4	3	3	Midium	2	1	5	7	1	1	2	3	2.75	Low
102	2.1 Server May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	5. Send Request	1.2 Client may be able to remotely execute code for 2.1 Server.	Low	1	4	4	2	3	3	4	3	3	Midium	2	1	5	7	1	1	2	3	2.75	Low

						Likelihood Factors											Impact Factors									
						Threat Agent Factors				Vulnerability Factors							Technical Impact Factors				Business Impact Factors					
Id	Title	Category	Interaction	Description	Final Risk Level	Skill Level	Motive	Oppertunity	Size	Ease of Discovery	Ease of Exploit	Awareness	IntrusionDetection	Overall Likelihood	Likelihood Level	Loss of Confidentiality	Loss of Integrity	Loss af Availability	Loss of Accountability	Finalcial Damage	Reputation Damage	Non-compliance	Privacy Violation	Overall Impact	Impact Level
122	Elevation by Changing the Execution Flow in 2.2 Face Recognition	Elevation Of Privilege	10. Return Image Frame	An attacker may pass data into 2.2 Face Recognition in order to change the flow of program execution within 2.2 Face Recognition to the attacker's choosing.	Low	1	4	4	2	3	3	4	3	3	Midium	2	1	5	7	1	1	2	3	2.75	Low
176	Elevation by Changing the Execution Flow in 1.1 Setting Manager (Special Face ID)	Elevation Of Privilege	1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode	An attacker may pass data into 1.1 Setting Manager (Special Face ID) in order to change the flow of program execution within 1.1 Setting Manager (Special Face ID) to the attacker's choosing.	Low	1	4	4	2	3	3	4	3	3	Midium	2	1	5	7	1	1	2	3	2.75	Low
175	1.1 Setting Manager (Special Face ID) May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode	E1. User may be able to remotely execute code for 1.1 Setting Manager (Special Face ID).	Low	1	4	4	2	3	3	4	3	3	Midium	2	1	5	7	1	1	2	3	2.75	Low
9	Weak Access Control for a Resource	Information Disclosure	4. Return Certificate	Improper data protection of DS3. Certificate Data Storage can allow an attacker to read information not intended for disclosure. Review authorization settings.	High	3	9	4	4	7	5	6	3	5.125	Midium	9	7	1	7	7	9	5	9	6.75	High
13	Weak Access Control for a Resource	Information Disclosure	7. Return Certificate	Improper data protection of DS2. Certificate Data Storage can allow an attacker to read information not intended for disclosure. Review authorization settings.	High	3	9	4	4	7	5	6	3	5.125	Midium	9	7	1	7	7	9	5	9	6.75	High
23	Weak Access Control for a Resource	Information Disclosure	12. Return Image	Improper data protection of DS1. Face Data Storage can allow an attacker to read information not intended for disclosure. Review authorization settings.	High	3	9	4	4	7	5	6	3	5.125	Midium	9	7	1	7	7	9	5	9	6.75	High
118	Data Flow Sniffing	Information Disclosure	10. Return Image Frame	Data flowing across 10. Return Image Frame may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.	High	1	4	4	2	3	3	6	3	3.25	Midium	7	3	1	7	7	9	5	9	6	High
106	Potential Data Repudiation by 1.2 Client	Repudiation	14. Send Response	1.2 Client claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Midium	3	1	7	6	7	5	9	8	5.75	Midium	2	1	5	7	1	1	5	3	3.125	Midium
99	Potential Data Repudiation by 2.1 Server	Repudiation	5. Send Request	2.1 Server claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Midium	3	1	7	6	7	5	9	8	5.75	Midium	2	1	5	7	1	1	5	3	3.125	Midium
117	Potential Data Repudiation by 2.2 Face Recognition	Repudiation	10. Return Image Frame	2.2 Face Recognition claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Midium	3	1	7	6	7	5	9	8	5.75	Midium	2	1	5	7	1	1	5	3	3.125	Midium
113	External Entity E2. Camera Potentially Denies Receiving Data	Repudiation	9. Request Image Frame	E2. Camera claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Midium	3	1	7	6	7	5	9	8	5.75	Midium	2	1	5	7	1	1	5	3	3.125	Midium
4	Spoofing the E1. User External Entity	Spoofing	1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode	E1. User may be spoofed by an attacker and this may lead to unauthorized access to 1.1 Setting Manager (Special Face ID). Consider using a standard authentication mechanism to identify the external entity.	High	5	9	7	9	3	5	9	3	6.25	High	9	3	5	7	7	9	2	3	5.625	Midium
6	Spoofing of Destination Data Store DS3. Certificate Data Storage	Spoofing	3. Request Certificate	DS3. Certificate Data Storage may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of DS3. Certificate Data Storage. Consider using a standard authentication mechanism to identify the destination data store.	High	5	9	7	9	3	5	9	3	6.25	High	9	3	5	7	7	9	2	3	5.625	Midium
8	Spoofing of Source Data Store DS3. Certificate Data Storage	Spoofing	4. Return Certificate	DS3. Certificate Data Storage may be spoofed by an attacker and this may lead to incorrect data delivered to 1.2 Client. Consider using a standard authentication mechanism to identify the source data store.	High	5	9	7	9	3	5	9	3	6.25	High	9	3	5	7	7	9	2	3	5.625	Midium
10	Spoofing of Destination Data Store DS2. Certificate Data Storage	Spoofing	6. Request Certificate	DS2. Certificate Data Storage may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of DS2. Certificate Data Storage. Consider using a standard authentication mechanism to identify the destination data store.	High	5	9	7	9	3	5	9	3	6.25	High	9	3	5	7	7	9	2	3	5.625	Midium
12	Spoofing of Source Data Store DS2. Certificate Data Storage	Spoofing	7. Return Certificate	DS2. Certificate Data Storage may be spoofed by an attacker and this may lead to incorrect data delivered to 2.1 Server. Consider using a standard authentication mechanism to identify the source data store.	High	5	9	7	9	3	5	9	3	6.25	High	9	3	5	7	7	9	2	3	5.625	Midium
20	Spoofing of Destination Data Store DS1. Face Data Storage	Spoofing	11. Request Image	DS1. Face Data Storage may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of DS1. Face Data Storage. Consider using a standard authentication mechanism to identify the destination data store.	High	5	9	7	9	3	5	9	3	6.25	High	9	3	5	7	7	9	2	3	5.625	Midium
22	Spoofing of Source Data Store DS1. Face Data Storage	Spoofing	12. Return Image	DS1. Face Data Storage may be spoofed by an attacker and this may lead to incorrect data delivered to 2.2 Face Recognition. Consider using a standard authentication mechanism to identify the source data store.	High	5	9	7	9	3	5	9	3	6.25	High	9	3	5	7	7	9	2	3	5.625	Midium
24	Spoofing the E2. Camera External Entity	Spoofing	10. Return Image Frame	E2. Camera may be spoofed by an attacker and this may lead to unauthorized access to 2.2 Face Recognition. Consider using a standard authentication mechanism to identify the external entity.	High	5	9	7	9	3	5	9	3	6.25	High	9	3	5	7	7	9	2	3	5.625	Midium

						Likelihood Factors										Impact Factors									
						Threat Agent Factors				Vulnerability Factors						Technical Impact Factors				Business Impact Factors					
Id	Title	Category	Interaction	Description	Final Risk Level	Skill Level	Motive	Oppertunity	Size	Ease of Discovery	Ease of Exploit	Awareness	IntrusionDetection	Overall Likelihood	Likelihood Level	Loss of Confidentiality	Loss of Integrity	Loss af Availability	Loss of Accountability	Finalcial Damage	Reputation Damage	Non-compliance	Privacy Violation	Overall Impact	Impact Level
105	Spoofing the 2.1 Server Process	Spoofing	14. Send Response	2.1 Server may be spoofed by an attacker and this may lead to unauthorized access to 1.2 Client. Consider using a standard authentication mechanism to identify the source process.	High	5	9	7	9	3	5	9	3	6.25	High	9	3	5	7	7	9	2	3	5.625	Midium
98	Spoofing the 1.2 Client Process	Spoofing	5. Send Request	1.2 Client may be spoofed by an attacker and this may lead to unauthorized access to 2.1 Server. Consider using a standard authentication mechanism to identify the source process.	High	5	9	7	9	3	5	9	3	6.25	High	9	3	5	7	7	9	2	3	5.625	Midium
115	Spoofing the 2.2 Face Recognition Process	Spoofing	10. Return Image Frame	2.2 Face Recognition may be spoofed by an attacker and this may lead to information disclosure by E2. Camera. Consider using a standard authentication mechanism to identify the destination process.	High	5	9	7	9	3	5	9	3	6.25	High	9	3	5	7	7	9	2	3	5.625	Midium
169	Spoofing the 1.1 Setting Manager (Special Face ID) Process	Spoofing	1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode	1.1 Setting Manager (Special Face ID) may be spoofed by an attacker and this may lead to information disclosure by E1. User. Consider using a standard authentication mechanism to identify the destination process.	High	5	9	7	9	3	5	9	3	6.25	High	9	3	5	7	7	9	2	3	5.625	Midium
116	Potential Lack of Input Validation for 2.2 Face Recognition	Tampering	10. Return Image Frame	Data flowing across 10. Return Image Frame may be tampered with by an attacker. This may lead to a denial of service attack against 2.2 Face Recognition or an elevation of privilege attack against 2.2 Face Recognition or an information disclosure by 2.2 Face Recognition. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.	Low	1	1	0	2	1	1	4	1	1.375	Low	7	7	1	7	7	5	2	3	4.875	Midium
170	Potential Lack of Input Validation for 1.1 Setting Manager (Special Face ID)	Tampering	1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode	Data flowing across 1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode may be tampered with by an attacker. This may lead to a denial of service attack against 1.1 Setting Manager (Special Face ID) or an elevation of privilege attack against 1.1 Setting Manager (Special Face ID) or an information disclosure by 1.1 Setting Manager (Special Face ID). Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.	Critical	5	9	7	9	3	5	9	3	6.25	High	9	9	5	7	7	9	2	3	6.375	High

Id	Title	Category	Diagram	Interaction	Priority	State	Description	Last Modified
97	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	5. Send Request	High	Not Started	**"2.1 Server"** may be able to impersonate the context of "1.2 Client" in order to gain additional privilege.	Generated
1	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	14. Send Response	High	Not Started	**"1.2 Client"** may be able to impersonate the context of "2.1 Server" in order to gain additional privilege.	Generated
2	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	2. Request Transmission	High	Not Started	**"1.2 Client"** may be able to impersonate the context of "1.1 Setting Manager (Special Face ID)" in order to gain additional privilege.	Generated
3	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	15. Return Data	High	Not Started	**"1.1 Setting Manager (Special Face ID)"** may be able to impersonate the context of **"1.2 Client"** in order to gain additional privilege.	Generated
4	Spoofing the E1. User External Entity	Spoofing	Diagram 1	1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode	High	Not Started	**"E1. User"** may be spoofed by an attacker and this may lead to unauthorized access to **"1.1 Setting Manager (Special Face ID)"**. Consider using a standard authentication mechanism to identify the external entity."	Generated
5	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode	High	Not Started	**"1.1 Setting Manager (Special Face ID)"** may be able to impersonate the context of **"E1. User"** in order to gain additional privilege.	Generated
6	Spoofing of Destination Data Store DS3. Certificate Data Storage	Spoofing	Diagram 1	3. Request Certificate	High	Not Started	**"DS3. Certificate Data Storage"** may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of **"DS3. Certificate Data Storage"**. Consider using a standard authentication mechanism to identify the destination data store.	Generated
7	Potential Excessive Resource Consumption for 1.2 Client or DS3. Certificate Data Storage	Denial Of Service	Diagram 1	3. Request Certificate	High	Not Started	Does **"1.2 Client"** or **"DS3. Certificate Data Storage"** take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.	Generated
8	Spoofing of Source Data Store DS3. Certificate Data Storage	Spoofing	Diagram 1	4. Return Certificate	High	Not Started	**"DS3. Certificate Data Storage"** may be spoofed by an attacker and this may lead to incorrect data delivered to **"1.2 Client"**. Consider using a standard authentication mechanism to identify the source data store.	Generated
9	Weak Access Control for a Resource	Information Disclosure	Diagram 1	4. Return Certificate	High	Not Started	Improper data protection of **"DS3. Certificate Data Storage"** can allow an attacker to read information not intended for disclosure. Review authorization settings.	Generated
10	Spoofing of Destination Data Store DS2. Certificate Data Storage	Spoofing	Diagram 1	6. Request Certificate	High	Not Started	**"DS2. Certificate Data Storage"** may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of **"DS2. Certificate Data Storage"**. Consider using a standard authentication mechanism to identify the destination data store.	Generated
11	Potential Excessive Resource Consumption for 2.1 Server or DS2. Certificate Data Storage	Denial Of Service	Diagram 1	6. Request Certificate	High	Not Started	Does **"2.1 Server"** or **"DS2. Certificate Data Storage"** take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.	Generated

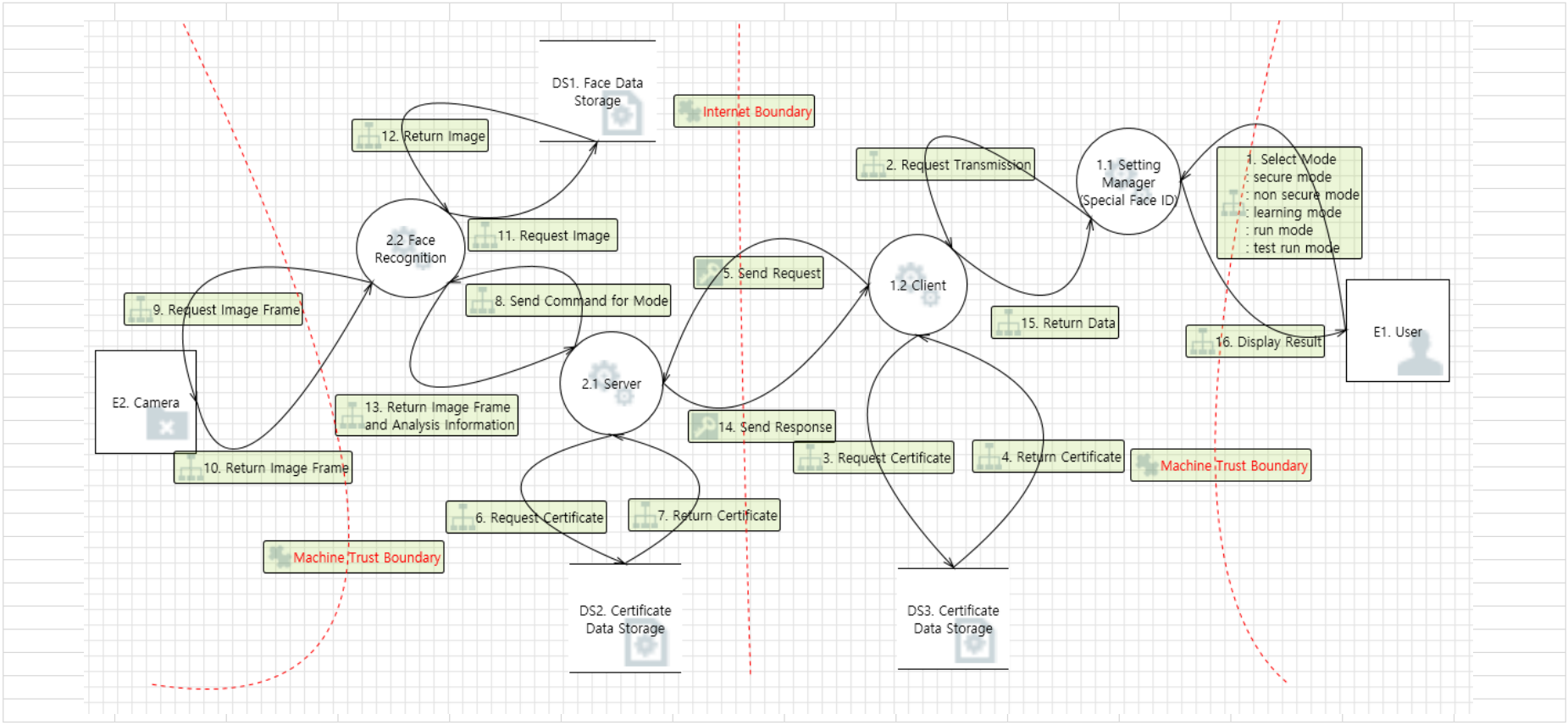
Id	Title	Category	Diagram	Interaction	Priority	State	Description	Last Modified
12	Spoofing of Source Data Store DS2. Certificate Data Storage	Spoofing	Diagram 1	7. Return Certificate	High	Not Started	**"DS2. Certificate Data Storage"** may be spoofed by an attacker and this may lead to incorrect data delivered to "2.1 Server". Consider using a standard authentication mechanism to identify the source data store.	Generated
13	Weak Access Control for a Resource	Information Disclosure	Diagram 1	7. Return Certificate	High	Not Started	Improper data protection of **"DS2. Certificate Data Storage"** can allow an attacker to read information not intended for disclosure. Review authorization settings.	Generated
14	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	8. Send Command for Mode	High	Not Started	**"2.2 Face Recognition"** may be able to impersonate the context of **"2.1 Server"** in order to gain additional privilege.	Generated
15	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	13. Return Image Frame and Analysis Information	High	Not Started	**"2.1 Server"** may be able to impersonate the context of **"2.2 Face Recognition"** in order to gain additional privilege.	Generated
20	Spoofing of Destination Data Store DS1. Face Data Storage	Spoofing	Diagram 1	11. Request Image	High	Not Started	**"DS1. Face Data Storage"** may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of **"DS1. Face Data Storage**". Consider using a standard authentication mechanism to identify the destination data store.	Generated
21	Potential Excessive Resource Consumption for 2.2 Face Recognition or DS1. Face Data Storage	Denial Of Service	Diagram 1	11. Request Image	High	Not Started	Does **"2.2 Face Recognition"** or **"DS1. Face Data Storage"** take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.	Generated
22	Spoofing of Source Data Store DS1. Face Data Storage	Spoofing	Diagram 1	12. Return Image	High	Not Started	**"DS1. Face Data Storage"** may be spoofed by an attacker and this may lead to incorrect data delivered to **"2.2 Face Recognition"**. Consider using a standard authentication mechanism to identify the source data store.	Generated
23	Weak Access Control for a Resource	Information Disclosure	Diagram 1	12. Return Image	High	Not Started	Improper data protection of **"DS1. Face Data Storage"** can allow an attacker to read information not intended for disclosure. Review authorization settings.	Generated
24	Spoofing the E2. Camera External Entity	Spoofing	Diagram 1	10. Return Image Frame	High	Not Started	**"E2. Camera"** may be spoofed by an attacker and this may lead to unauthorized access to **"2.2 Face Recognition"**. Consider using a standard authentication mechanism to identify the external entity.	Generated
25	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	10. Return Image Frame	High	Not Started	**"2.2 Face Recognition"** may be able to impersonate the context of **"E2. Camera"** in order to gain additional privilege.	Generated

Id	Title	Category	Diagram	Interaction	Priority	State	Description	Last Modified
111	Cross Site Request Forgery	Elevation Of Privilege	Diagram 1	14. Send Response	High	Not Started	Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting. The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.	Generated
110	Elevation by Changing the Execution Flow in 1.2 Client	Elevation Of Privilege	Diagram 1	14. Send Response	High	Not Started	An attacker may pass data into **"1.2 Client"** in order to change the flow of program execution within **"1.2 Client"** to the attacker's choosing.	Generated
109	1.2 Client May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	Diagram 1	14. Send Response	High	Not Started	**"2.1 Server"** may be able to remotely execute code for **"1.2 Client"**.	Generated
108	Data Flow 14. Send Response Is Potentially Interrupted	Denial Of Service	Diagram 1	14. Send Response	High	Not Started	An external agent interrupts data flowing across a trust boundary in either direction.	Generated
107	Potential Process Crash or Stop for 1.2 Client	Denial Of Service	Diagram 1	14. Send Response	High	Not Started	**"1.2 Client"** crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Generated
106	Potential Data Repudiation by 1.2 Client	Repudiation	Diagram 1	14. Send Response	High	Not Started	**"1.2 Client"** claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Generated
105	Spoofing the 2.1 Server Process	Spoofing	Diagram 1	14. Send Response	High	Not Started	**"2.1 Server"** may be spoofed by an attacker and this may lead to unauthorized access to **"1.2 Client"**. Consider using a standard authentication mechanism to identify the source process.	Generated

Id	Title	Category	Diagram	Interaction	Priority	State	Description	Last Modified
104	Cross Site Request Forgery	Elevation Of Privilege	Diagram 1	5. Send Request	High	Not Started	Cross-site request forgery (CSRF or XSRF) is a type of attack in which an attacker forces a user's browser to make a forged request to a vulnerable site by exploiting an existing trust relationship between the browser and the vulnerable web site. In a simple scenario, a user is logged in to web site A using a cookie as a credential. The other browses to web site B. Web site B returns a page with a hidden form that posts to web site A. Since the browser will carry the user's cookie to web site A, web site B now can take any action on web site A, for example, adding an admin to an account. The attack can be used to exploit any requests that the browser automatically authenticates, e.g. by session cookie, integrated authentication, IP whitelisting. The attack can be carried out in many ways such as by luring the victim to a site under control of the attacker, getting the user to click a link in a phishing email, or hacking a reputable web site that the victim will visit. The issue can only be resolved on the server side by requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. See the Forgery Protection property on the flow stencil for a list of mitigations.	Generated
103	Elevation by Changing the Execution Flow in 2.1 Server	Elevation Of Privilege	Diagram 1	5. Send Request	High	Not Started	An attacker may pass data into **"2.1 Server"** in order to change the flow of program execution within **"2.1 Server"** to the attacker's choosing.	Generated
102	2.1 Server May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	Diagram 1	5. Send Request	High	Not Started	**"1.2 Client"** may be able to remotely execute code for "2.1 Server".	Generated
101	Data Flow 5. Send Request Is Potentially Interrupted	Denial Of Service	Diagram 1	5. Send Request	High	Not Started	An external agent interrupts data flowing across a trust boundary in either direction.	Generated
100	Potential Process Crash or Stop for 2.1 Server	Denial Of Service	Diagram 1	5. Send Request	High	Not Started	**"2.1 Server"** crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Generated
99	Potential Data Repudiation by 2.1 Server	Repudiation	Diagram 1	5. Send Request	High	Not Started	**"2.1 Server"** claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Generated
98	Spoofing the 1.2 Client Process	Spoofing	Diagram 1	5. Send Request	High	Not Started	**"1.2 Client"** may be spoofed by an attacker and this may lead to unauthorized access to **"2.1 Server"**. Consider using a standard authentication mechanism to identify the source process.	Generated
122	Elevation by Changing the Execution Flow in 2.2 Face Recognition	Elevation Of Privilege	Diagram 1	10. Return Image Frame	High	Not Started	An attacker may pass data into **"2.2 Face Recognition"** in order to change the flow of program execution within **"2.2 Face Recognition"** to the attacker's choosing.	Generated
121	2.2 Face Recognition May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	Diagram 1	10. Return Image Frame	High	Not Started	**"E2. Camera"** may be able to remotely execute code for "2.2 Face Recognition".	Generated
120	Data Flow 10. Return Image Frame Is Potentially Interrupted	Denial Of Service	Diagram 1	10. Return Image Frame	High	Not Started	An external agent interrupts data flowing across a trust boundary in either direction.	Generated
119	Potential Process Crash or Stop for 2.2 Face Recognition	Denial Of Service	Diagram 1	10. Return Image Frame	High	Not Started	**"2.2 Face Recognition"** crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Generated

Id	Title	Category	Diagram	Interaction	Priority	State	Description	Last Modified
118	Data Flow Sniffing	Information Disclosure	Diagram 1	10. Return Image Frame	High	Not Started	Data flowing across **"10. Return Image Frame"** may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.	Generated
117	Potential Data Repudiation by 2.2 Face Recognition	Repudiation	Diagram 1	10. Return Image Frame	High	Not Started	**"2.2 Face Recognition"** claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Generated
116	Potential Lack of Input Validation for 2.2 Face Recognition	Tampering	Diagram 1	10. Return Image Frame	High	Not Started	Data flowing across **"10. Return Image Frame"** may be tampered with by an attacker. This may lead to a denial of service attack against **"2.2 Face Recognition"** or an elevation of privilege attack against **"2.2 Face Recognition"** or an information disclosure by **"2.2 Face Recognition"**. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.	Generated
115	Spoofing the 2.2 Face Recognition Process	Spoofing	Diagram 1	10. Return Image Frame	High	Not Started	**"2.2 Face Recognition"** may be spoofed by an attacker and this may lead to information disclosure by **"E2. Camera"**. Consider using a standard authentication mechanism to identify the destination process.	Generated
114	Data Flow 9. Request Image Frame Is Potentially Interrupted	Denial Of Service	Diagram 1	9. Request Image Frame	High	Not Started	An external agent interrupts data flowing across a trust boundary in either direction.	Generated
113	External Entity E2. Camera Potentially Denies Receiving Data	Repudiation	Diagram 1	9. Request Image Frame	High	Not Started	**"E2. Camera"** claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Generated
112	Spoofing of the E2. Camera External Destination Entity	Spoofing	Diagram 1	9. Request Image Frame	High	Not Started	**"E2. Camera"** may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of **"E2. Camera"**. Consider using a standard authentication mechanism to identify the external entity.	Generated
179	Data Flow 16. Display Result Is Potentially Interrupted	Denial Of Service	Diagram 1	16. Display Result	High	Not Started	An external agent interrupts data flowing across a trust boundary in either direction.	Generated
178	External Entity E1. User Potentially Denies Receiving Data	Repudiation	Diagram 1	16. Display Result	High	Not Started	**"E1. User"** claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Generated
177	Spoofing of the E1. User External Destination Entity	Spoofing	Diagram 1	16. Display Result	High	Not Started	**"E1. User"** may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of **"E1. User"**. Consider using a standard authentication mechanism to identify the external entity.	Generated
176	Elevation by Changing the Execution Flow in 1.1 Setting Manager (Special Face ID)	Elevation Of Privilege	Diagram 1	1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode	High	Not Started	An attacker may pass data into **"1.1 Setting Manager (Special Face ID)"** in order to change the flow of program execution within **"1.1 Setting Manager (Special Face ID)"** to the attacker's choosing.	Generated

Id	Title	Category	Diagram	Interaction	Priority	State	Description	Last Modified
175	1.1 Setting Manager (Special Face ID) May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	Diagram 1	1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode	High	Not Started	E1. User may be able to remotely execute code for **"1.1 Setting Manager (Special Face ID)"**.	Generated
174	Data Flow 1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode Is Potentially Interrupted	Denial Of Service	Diagram 1	1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode	High	Not Started	An external agent interrupts data flowing across a trust boundary in either direction.	Generated
173	Potential Process Crash or Stop for 1.1 Setting Manager (Special Face ID)	Denial Of Service	Diagram 1	1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode	High	Not Started	**"1.1 Setting Manager (Special Face ID)"** crashes, halts, stops or runs slowly; in all cases violating an availability metric.	Generated
172	Data Flow Sniffing	Information Disclosure	Diagram 1	1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode	High	Not Started	Data flowing across **"1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode"** may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.	Generated
171	Potential Data Repudiation by 1.1 Setting Manager (Special Face ID)	Repudiation	Diagram 1	1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode	High	Not Started	**"1.1 Setting Manager (Special Face ID)"** claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	Generated
170	Potential Lack of Input Validation for 1.1 Setting Manager (Special Face ID)	Tampering	Diagram 1	1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode	High	Not Started	Data flowing across **"1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode"** may be tampered with by an attacker. This may lead to a denial of service attack against **"1.1 Setting Manager (Special Face ID)"** or an elevation of privilege attack against **"1.1 Setting Manager (Special Face ID)"** or an information disclosure by **"1.1 Setting Manager (Special Face ID)"**. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.	Generated
169	Spoofing the 1.1 Setting Manager (Special Face ID) Process	Spoofing	Diagram 1	1. Select Mode : secure mode : non secure mode : learning mode : run mode : test run mode	High	Not Started	**"1.1 Setting Manager (Special Face ID)"** may be spoofed by an attacker and this may lead to information disclosure by **"E1. User"**. Consider using a standard authentication mechanism to identify the destination process.	Generated


DS1. Face Data Storage
Internet Boundary
12. Return Image
2. Request Transmission
1.1 Setting Manager (Special Face ID)
1. Select Mode
: secure mode
: non secure mode
: learning mode
: run mode
: test run mode
2.2 Face Recognition
11. Request Image
5. Send Request
1.2 Client
9. Request Image Frame
8. Send Command for Mode
15. Return Data
16. Display Result
E1. User
E2. Camera
2.1 Server
13. Return Image Frame and Analysis Information
14. Send Response
3. Request Certificate
4. Return Certificate
Machine Trust Boundary
10. Return Image Frame
6. Request Certificate
7. Return Certificate
Machine Trust Boundary
DS2. Certificate Data Storage
DS3. Certificate Data Storage

https://owasp-risk-rating.com/

Likelihood Factors

Skill Level		Motive		Oppertunity		Size		Ease of Discovery		Ease of Exploit		Awareness		IntrusionDetection	
1	Security Penetration Skills	1	Low or No reward	0	Full access or expensive resource required	2	Developers Or system administrators	1	Practically impossible	1	Theoretical	1	Unknown	1	Active detection in application
3	Network Programming Skills	4	Possible reward	4	Special access or resources required	4	Intranet users	3	Difficult	3	Difficult	4	Hidden	3	Logged and reviewed
5	Advanced Computer User	9	High reward	7	Some access or resources required	5	Partners	7	Easy	5	Easy	6	Obvious	8	Logged without review
6	Some Technical Skills			9	No access or resources required	6	Authentication users	9	Automated tools available	9	Automated tools available	9	Public knowledge	9	Not logged
9	No Technical Skills					9	Anonymous Internet users								

Impact Factors

Loss of Confidentiality		Loss of Integrity		Loss af Availability		Loss of Accountability		Finalcial Damage		Reputation Damage		Non-compliance		Privacy Violation	
2	Minimal non-sensitive data disclosed	1	Minimal slightly corrupt data	1	Minimal secondary services interrupted	1	Fully traceable	1	Less than the cost to fix the vulnerability	1	Minimal damage	2	Minor violation	3	One individual
6	Minimal critical data or extensive non-sensitive data disclosed	3	Minimal seriously corrupt data	5	Minimal primary or extensive secondary services interrupted	7	Possibly traceable	3	Minor effect on annual profit	4	Loss of major accounts	5	Clear violation	5	Hundreds of people
7	Extensive critical data disclosed	5	Extensive slightly corrupt data	7	Extensive primary services interrupted	9	Completely anonymous	7	Significant effect on annual profit	5	Loss of goodwill	7	High profile violation	7	Thousands of people
9	All data disclosed	7	Extensive seriously corrupt data	9	All services completely lost			9	Bankruptcy	9	Brand damage			9	Millions of people
		9	All data totally corrupt												

From	To	Value
0	2	Low
3	5	Midium
6	9	High

Likelihood Factor	Impact Factor	Value
Low	Low	Note
Low	Midium	Low
Low	High	Midium
Midium	Low	Low
Midium	Midium	Midium
Midium	High	High
High	Low	Midium
High	Midium	High
High	High	Critical

Priority

High															
Medium															
Low															
Status															
Not Started															
Needs Investigation															
Not Applicable															
Mitigated															

[1] This ID is associated with an OWASP risk assessment. You can find it on the third tab of this article.