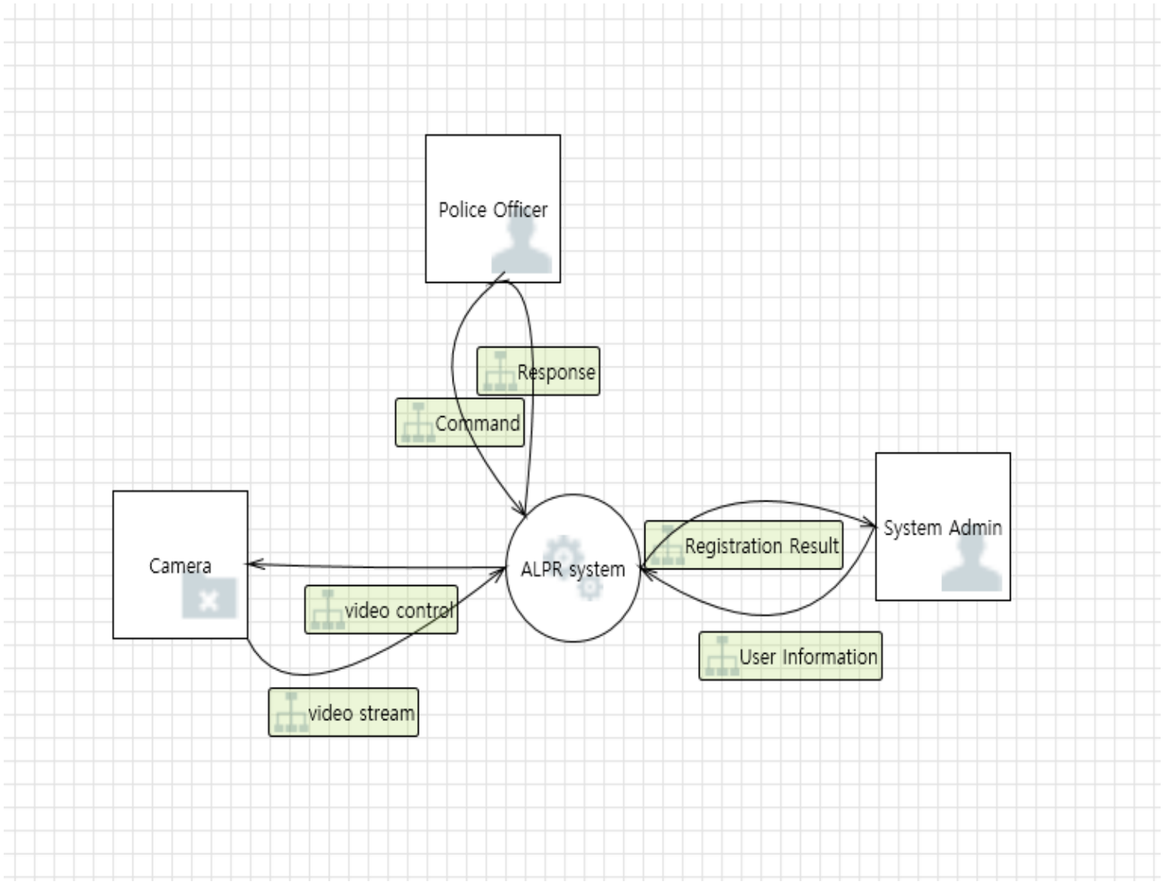
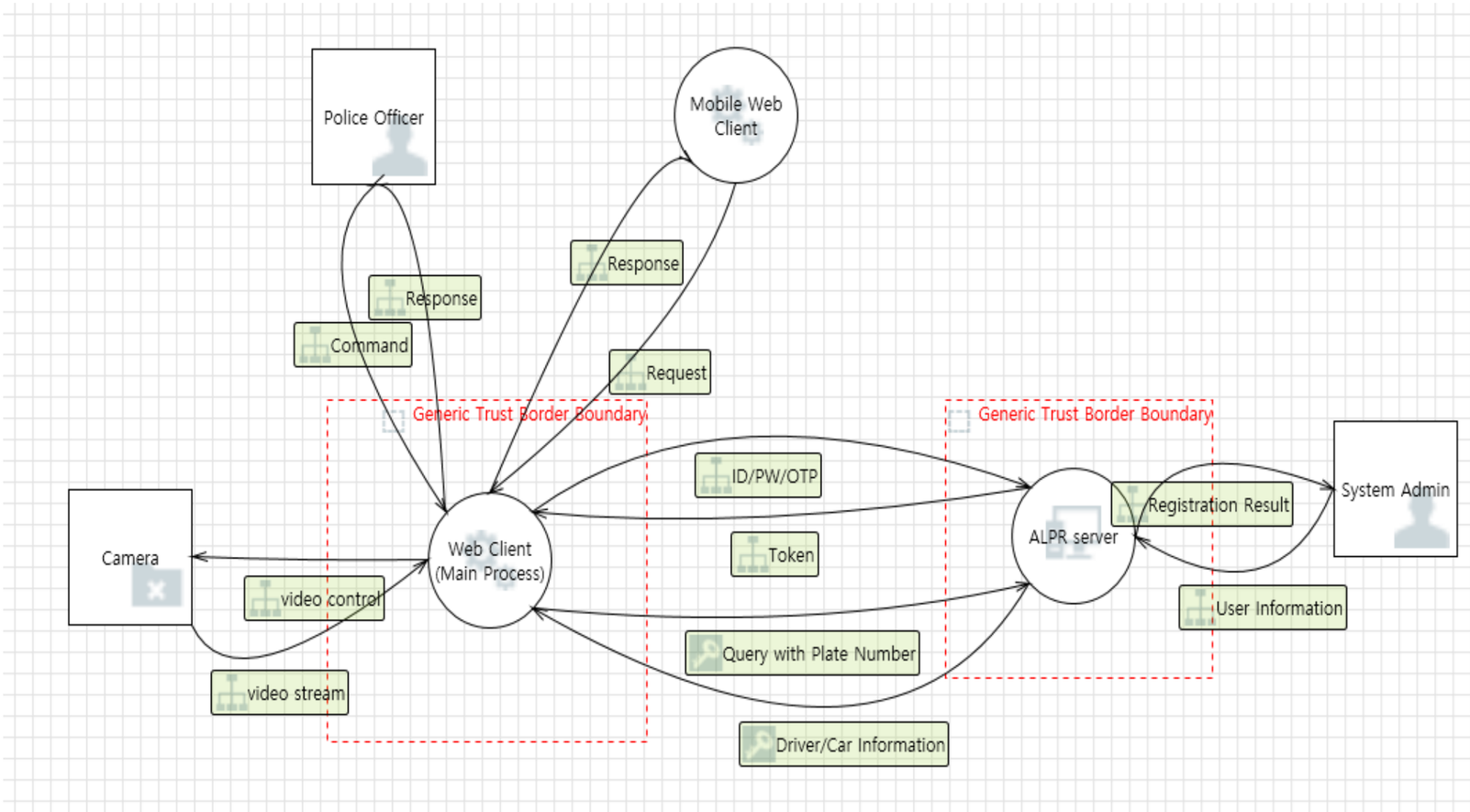
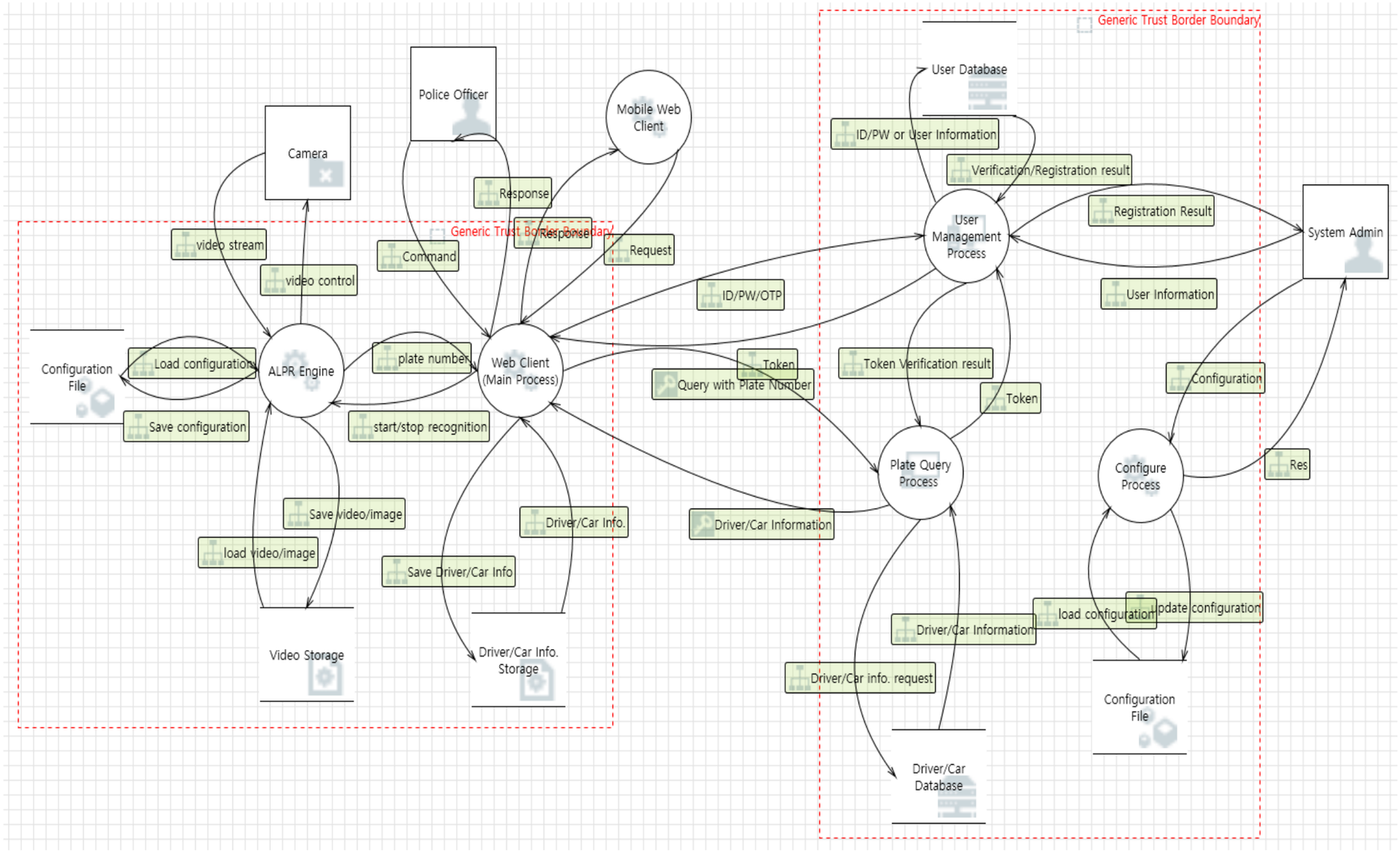
DFD0


Police Officer
Response
Command
Camera
ALPR system
Registration Result
System Admin
video control
User Information
video stream

DFD1


Police Officer
Mobile Web Client
Response
Response
Command
Request
Generic Trust Border Boundary
Generic Trust Border Boundary
ID/PW/OTP
System Admin
Registration Result
Camera
Web Client (Main Process)
ALPR server
Token
video control
User Information
Query with Plate Number
video stream
Driver/Car Information

DFD2


Generic Trust Border Boundary
Generic Trust Border Boundary
Police Officer
Camera
Mobile Web Client
User Database
ID/PW or User Information
Verification/Registration result
Response
Response
Request
Command
video stream
video control
User Management Process
Registration Result
System Admin
User Information
ID/PW/OTP
Configuration File
Load configuration
ALPR Engine
plate number
Web Client (Main Process)
Token
Query with Plate Number
Token Verification result
Token
Save configuration
start/stop recognition
Configuration
Plate Query Process
Configure Process
Res
Save video/image
Driver/Car Info.
load video/image
Save Driver/Car Info
Driver/Car Information
load configuration
update configuration
Driver/Car Information
Driver/Car info. request
Video Storage
Driver/Car Info. Storage
Configuration File
Driver/Car Database

All threats

threats derived from PnG methodology

Id	Title	Category	Description
1	login spoofing	Spoofing	Police Officer may be spoofed by an attacker and this may lead to unauthorized access to Web Client (Main Process). Consider using a standard authentication mechanism to identify the external entity.
2	user with root privileges	Repudiation	The administrator with root privileges can manipulate all information in the accessible DB and delete the log.

threats derived from Microsoft threat modeling tool

Id	Title	Category	Diagram	Interaction	Priority	State	Description
1	Spoofing of Destination Data Store Driver/Car Database	Spoofing	Diagram 1	Driver/Car info. request	High	Not Applicable	Driver/Car Database may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Driver/Car Database. Consider using a standard authentication mechanism to identify the destination data store.
2	Potential Excessive Resource Consumption for Plate Query Process or Driver/Car Database	Denial Of Service	Diagram 1	Driver/Car info. request	High	Needs Investigation	Does Plate Query Process or Driver/Car Database 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.
3	Spoofing of Source Data Store Driver/Car Database	Spoofing	Diagram 1	Driver/Car Information	High	Not Applicable	Driver/Car Database may be spoofed by an attacker and this may lead to incorrect data delivered to Plate Query Process . Consider using a standard authentication mechanism to identify the source data store.
4	Cross Site Scripting	Tampering	Diagram 1	Driver/Car Information	High	Not Started	The web server 'Plate Query Process ' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
5	Persistent Cross Site Scripting	Tampering	Diagram 1	Driver/Car Information	High	Not Applicable	The web server 'Plate Query Process ' could be a subject to a persistent cross-site scripting attack because it does not sanitize data store 'Driver/Car Database' inputs and output.
6	Weak Access Control for a Resource	Information Disclosure	Diagram 1	Driver/Car Information	High	Mitigated	Improper data protection of Driver/Car Database can allow an attacker to read information not intended for disclosure. Review authorization settings.
7	Potential Lack of Input Validation for Web Client (Main Process)	Tampering	Diagram 1	Command	High	Not Started	Data flowing across Command may be tampered with by an attacker. This may lead to a denial of service attack against Web Client (Main Process) or an elevation of privilege attack against Web Client (Main Process) or an information disclosure by Web Client (Main Process). 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.
8	Spoofing the Web Client (Main Process) Process	Spoofing	Diagram 1	Command	High	Not Started	Web Client (Main Process) may be spoofed by an attacker and this may lead to information disclosure by Police Officer. Consider using a standard authentication mechanism to identify the destination process.
9	Potential Data Repudiation by Web Client (Main Process)	Repudiation	Diagram 1	Command	High	Not Started	Web Client (Main Process) 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.
10	Spoofing the Police Officer External Entity	Spoofing	Diagram 1	Command	High	Not Started	Police Officer may be spoofed by an attacker and this may lead to unauthorized access to Web Client (Main Process). Consider using a standard authentication mechanism to identify the external entity.
11	Weak Access Control for a Resource	Information Disclosure	Diagram 1	load configuration	High	Not Started	Improper data protection of Configuration File can allow an attacker to read information not intended for disclosure. Review authorization settings.
12	Spoofing of Source Data Store Configuration File	Spoofing	Diagram 1	load configuration	High	Not Started	Configuration File may be spoofed by an attacker and this may lead to incorrect data delivered to Configure Process. Consider using a standard authentication mechanism to identify the source data store.
13	Spoofing of Source Data Store Video Storage	Spoofing	Diagram 1	load video/image	High	Not Started	Video Storage may be spoofed by an attacker and this may lead to incorrect data delivered to ALPR Engine. Consider using a standard authentication mechanism to identify the source data store.
14	Potential Excessive Resource Consumption for ALPR Engine or Video Storage	Denial Of Service	Diagram 1	Save video/image	High	Not Started	Does ALPR Engine or Video 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.
15	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	video stream	High	Not Started	ALPR Engine may be able to impersonate the context of Camera in order to gain additional privilege.
16	Spoofing the Camera External Entity	Spoofing	Diagram 1	video stream	High	Not Started	Camera may be spoofed by an attacker and this may lead to unauthorized access to ALPR Engine. Consider using a standard authentication mechanism to identify the external entity.
17	Spoofing of Destination Data Store Video Storage	Spoofing	Diagram 1	Save video/image	High	Not Started	Video Storage may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Video Storage. Consider using a standard authentication mechanism to identify the destination data store.

18	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	Driver/Car Information	High	Not Applicable	Web Client (Main Process) may be able to impersonate the context of Plate Query Process in order to gain additional privilege.
19	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	Query with Plate Number	High	Not Applicable	Plate Query Process may be able to impersonate the context of Web Client (Main Process) in order to gain additional privilege.
20	Cross Site Scripting	Tampering	Diagram 1	Query with Plate Number	High	Mitigated	The web server 'Plate Query Process ' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
21	Weak Access Control for a Resource	Information Disclosure	Diagram 1	load video/image	High	Not Started	Improper data protection of Video Storage can allow an attacker to read information not intended for disclosure. Review authorization settings.
22	Spoofing of Destination Data Store Driver/Car Info. Storage	Spoofing	Diagram 1	Save Driver/Car Info	High	Not Started	Driver/Car Info. Storage may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Driver/Car Info. Storage. Consider using a standard authentication mechanism to identify the destination data store.
23	Potential Excessive Resource Consumption for Web Client (Main Process) or Driver/Car Info. Storage	Denial Of Service	Diagram 1	Save Driver/Car Info	High	Not Started	Does Web Client (Main Process) or Driver/Car Info. 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.
24	Spoofing of Source Data Store Driver/Car Info. Storage	Spoofing	Diagram 1	Driver/Car Info.	High	Not Applicable	Driver/Car Info. Storage may be spoofed by an attacker and this may lead to incorrect data delivered to Web Client (Main Process). Consider using a standard authentication mechanism to identify the source data store.
25	Weak Access Control for a Resource	Information Disclosure	Diagram 1	Driver/Car Info.	High	Mitigated	Improper data protection of Driver/Car Info. Storage can allow an attacker to read information not intended for disclosure. Review authorization settings.
26	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	plate number	High	Not Started	Web Client (Main Process) may be able to impersonate the context of ALPR Engine in order to gain additional privilege.
27	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	start/stop recognition	High	Not Started	ALPR Engine may be able to impersonate the context of Web Client (Main Process) in order to gain additional privilege.
28	Cross Site Scripting	Tampering	Diagram 1	ID/PW/OTP	High	Not Started	The web server 'User Management Process' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
29	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	ID/PW/OTP	High	Not Started	User Management Process may be able to impersonate the context of Web Client (Main Process) in order to gain additional privilege.
30	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	Token	High	Not Started	Web Client (Main Process) may be able to impersonate the context of User Management Process in order to gain additional privilege.
31	Cross Site Scripting	Tampering	Diagram 1	Token Verification result	High	Not Started	The web server 'Plate Query Process ' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
32	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	Token Verification result	High	Not Started	Plate Query Process may be able to impersonate the context of User Management Process in order to gain additional privilege.
33	Cross Site Scripting	Tampering	Diagram 1	Token	High	Not Started	The web server 'User Management Process' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
34	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	Token	High	Not Started	User Management Process may be able to impersonate the context of Plate Query Process in order to gain additional privilege.
35	Spoofing of Destination Data Store User Database	Spoofing	Diagram 1	ID/PW or User Information	High	Not Applicable	User Database may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of User Database. Consider using a standard authentication mechanism to identify the destination data store.
36	Potential Excessive Resource Consumption for User Management Process or User Database	Denial Of Service	Diagram 1	ID/PW or User Information	High	Not Applicable	Does User Management Process or User Database 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.
37	Spoofing of Source Data Store User Database	Spoofing	Diagram 1	Verification/Registration result	High	Not Applicable	User Database may be spoofed by an attacker and this may lead to incorrect data delivered to User Management Process. Consider using a standard authentication mechanism to identify the source data store.
38	Cross Site Scripting	Tampering	Diagram 1	Verification/Registration result	High	Not Started	The web server 'User Management Process' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
39	Persistent Cross Site Scripting	Tampering	Diagram 1	Verification/Registration result	High	Not Applicable	The web server 'User Management Process' could be a subject to a persistent cross-site scripting attack because it does not sanitize data store 'User Database' inputs and output.
40	Weak Access Control for a Resource	Information Disclosure	Diagram 1	Verification/Registration result	High	Mitigated	Improper data protection of User Database can allow an attacker to read information not intended for disclosure. Review authorization settings.
41	Data Flow video control Is Potentially Interrupted	Denial Of Service	Diagram 1	video control	High	Not Started	An external agent interrupts data flowing across a trust boundary in either direction.
42	External Entity Camera Potentially Denies Receiving Data	Repudiation	Diagram 1	video control	High	Not Started	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.

43	Spoofing of the Camera External Destination Entity	Spoofing	Diagram 1	video control	High	Not Started	Camera may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Camera. Consider using a standard authentication mechanism to identify the external entity.
44	Cross Site Request Forgery	Elevation Of Privilege	Diagram 1	video stream	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.
45	Elevation by Changing the Execution Flow in ALPR Engine	Elevation Of Privilege	Diagram 1	video stream	High	Not Started	An attacker may pass data into ALPR Engine in order to change the flow of program execution within ALPR Engine to the attacker's choosing.
46	ALPR Engine May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	Diagram 1	video stream	High	Not Started	Camera may be able to remotely execute code for ALPR Engine.
47	Data Flow video stream Is Potentially Interrupted	Denial Of Service	Diagram 1	video stream	High	Not Started	An external agent interrupts data flowing across a trust boundary in either direction.
48	Elevation by Changing the Execution Flow in Web Client (Main Process)	Elevation Of Privilege	Diagram 1	Token	High	Not Started	An attacker may pass data into Web Client (Main Process) in order to change the flow of program execution within Web Client (Main Process) to the attacker's choosing.
49	Web Client (Main Process) May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	Diagram 1	Token	High	Not Started	User Management Process may be able to remotely execute code for Web Client (Main Process).
50	Data Flow Token Is Potentially Interrupted	Denial Of Service	Diagram 1	Token	High	Not Started	An external agent interrupts data flowing across a trust boundary in either direction.
51	Potential Process Crash or Stop for Web Client (Main Process)	Denial Of Service	Diagram 1	Token	High	Not Started	Web Client (Main Process) crashes, halts, stops or runs slowly; in all cases violating an availability metric.
52	Potential Data Repudiation by Web Client (Main Process)	Repudiation	Diagram 1	Token	High	Not Started	Web Client (Main Process) 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.
53	Spoofing the User Management Process Process	Spoofing	Diagram 1	Token	High	Not Started	User Management Process may be spoofed by an attacker and this may lead to unauthorized access to Web Client (Main Process). Consider using a standard authentication mechanism to identify the source process.
54	Cross Site Request Forgery	Elevation Of Privilege	Diagram 1	ID/PW/OTP	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.
55	Elevation by Changing the Execution Flow in User Management Process	Elevation Of Privilege	Diagram 1	ID/PW/OTP	High	Not Started	An attacker may pass data into User Management Process in order to change the flow of program execution within User Management Process to the attacker's choosing.

56	User Management Process May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	Diagram 1	ID/PW/OTP	High	Not Started	Web Client (Main Process) may be able to remotely execute code for User Management Process.
57	Data Flow ID/PW/OTP Is Potentially Interrupted	Denial Of Service	Diagram 1	ID/PW/OTP	High	Not Started	An external agent interrupts data flowing across a trust boundary in either direction.
58	Potential Process Crash or Stop for User Management Process	Denial Of Service	Diagram 1	ID/PW/OTP	High	Not Started	User Management Process crashes, halts, stops or runs slowly; in all cases violating an availability metric.
59	Potential Data Repudiation by User Management Process	Repudiation	Diagram 1	ID/PW/OTP	High	Not Started	User Management Process 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.
60	Spoofing the Web Client (Main Process) Process	Spoofing	Diagram 1	ID/PW/OTP	High	Not Started	Web Client (Main Process) may be spoofed by an attacker and this may lead to unauthorized access to User Management Process. Consider using a standard authentication mechanism to identify the source process.
61	Spoofing the Web Client (Main Process) Process	Spoofing	Diagram 1	Query with Plate Number	High	Mitigated	Web Client (Main Process) may be spoofed by an attacker and this may lead to unauthorized access to Plate Query Process . Consider using a standard authentication mechanism to identify the source process.
62	Potential Data Repudiation by Plate Query Process	Repudiation	Diagram 1	Query with Plate Number	High	Mitigated	Plate Query Process 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.
63	Potential Process Crash or Stop for Plate Query Process	Denial Of Service	Diagram 1	Query with Plate Number	High	Mitigated	Plate Query Process crashes, halts, stops or runs slowly; in all cases violating an availability metric.
64	Data Flow Query with Plate Number Is Potentially Interrupted	Denial Of Service	Diagram 1	Query with Plate Number	High	Not Applicable	An external agent interrupts data flowing across a trust boundary in either direction.
65	Plate Query Process May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	Diagram 1	Query with Plate Number	High	Not Applicable	Web Client (Main Process) may be able to remotely execute code for Plate Query Process .
66	Elevation by Changing the Execution Flow in Plate Query Process	Elevation Of Privilege	Diagram 1	Query with Plate Number	High	Not Applicable	An attacker may pass data into Plate Query Process in order to change the flow of program execution within Plate Query Process to the attacker's choosing.
67	Cross Site Request Forgery	Elevation Of Privilege	Diagram 1	Query with Plate Number	High	Not Applicable	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.
68	Spoofing the Plate Query Process Process	Spoofing	Diagram 1	Driver/Car Information	High	Not Applicable	Plate Query Process may be spoofed by an attacker and this may lead to unauthorized access to Web Client (Main Process). Consider using a standard authentication mechanism to identify the source process.
69	Potential Data Repudiation by Web Client (Main Process)	Repudiation	Diagram 1	Driver/Car Information	High	Mitigated	Web Client (Main Process) 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.
70	Potential Process Crash or Stop for Web Client (Main Process)	Denial Of Service	Diagram 1	Driver/Car Information	High	Not Applicable	Web Client (Main Process) crashes, halts, stops or runs slowly; in all cases violating an availability metric.
71	Data Flow Driver/Car Information Is Potentially Interrupted	Denial Of Service	Diagram 1	Driver/Car Information	High	Not Applicable	An external agent interrupts data flowing across a trust boundary in either direction.

72	Web Client (Main Process) May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	Diagram 1	Driver/Car Information	High	Not Applicable	Plate Query Process may be able to remotely execute code for Web Client (Main Process).
73	Elevation by Changing the Execution Flow in Web Client (Main Process)	Elevation Of Privilege	Diagram 1	Driver/Car Information	High	Not Applicable	An attacker may pass data into Web Client (Main Process) in order to change the flow of program execution within Web Client (Main Process) to the attacker's choosing.
74	Potential Process Crash or Stop for ALPR Engine	Denial Of Service	Diagram 1	video stream	High	Not Started	ALPR Engine crashes, halts, stops or runs slowly; in all cases violating an availability metric.
75	Data Flow Sniffing	Information Disclosure	Diagram 1	video stream	High	Not Started	Data flowing across video stream 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.
76	Potential Data Repudiation by ALPR Engine	Repudiation	Diagram 1	video stream	High	Not Started	ALPR Engine 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.
77	Potential Lack of Input Validation for ALPR Engine	Tampering	Diagram 1	video stream	High	Not Started	Data flowing across video stream may be tampered with by an attacker. This may lead to a denial of service attack against ALPR Engine or an elevation of privilege attack against ALPR Engine or an information disclosure by ALPR Engine. 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.
78	Spoofing the ALPR Engine Process	Spoofing	Diagram 1	video stream	High	Not Started	ALPR Engine may be spoofed by an attacker and this may lead to information disclosure by Camera. Consider using a standard authentication mechanism to identify the destination process.
79	Cross Site Request Forgery	Elevation Of Privilege	Diagram 1	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.
80	Elevation by Changing the Execution Flow in Web Client (Main Process)	Elevation Of Privilege	Diagram 1	Request	High	Not Started	An attacker may pass data into Web Client (Main Process) in order to change the flow of program execution within Web Client (Main Process) to the attacker's choosing.
81	Web Client (Main Process) May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	Diagram 1	Request	High	Not Started	Mobile Web Client may be able to remotely execute code for Web Client (Main Process).
82	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	Request	High	Not Started	Web Client (Main Process) may be able to impersonate the context of Mobile Web Client in order to gain additional privilege.
83	Data Flow Request Is Potentially Interrupted	Denial Of Service	Diagram 1	Request	High	Not Started	An external agent interrupts data flowing across a trust boundary in either direction.
84	Potential Process Crash or Stop for Web Client (Main Process)	Denial Of Service	Diagram 1	Request	High	Not Started	Web Client (Main Process) crashes, halts, stops or runs slowly; in all cases violating an availability metric.
85	Data Flow Sniffing	Information Disclosure	Diagram 1	Request	High	Not Started	Data flowing across Request 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.
86	Potential Process Crash or Stop for Web Client (Main Process)	Denial Of Service	Diagram 1	Command	High	Not Started	Web Client (Main Process) crashes, halts, stops or runs slowly; in all cases violating an availability metric.
87	Data Flow Sniffing	Information Disclosure	Diagram 1	Command	High	Not Started	Data flowing across Command 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.

88	Weak Access Control for a Resource	Information Disclosure	Diagram 1	Load configuration	High	Not Started	Improper data protection of Configuration File can allow an attacker to read information not intended for disclosure. Review authorization settings.
89	Potential Excessive Resource Consumption for Configure Process or Configuration File	Denial Of Service	Diagram 1	update configuration	High	Not Started	Does Configure Process or Configuration File 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.
90	Spoofing of Source Data Store Configuration File	Spoofing	Diagram 1	Load configuration	High	Not Started	Configuration File may be spoofed by an attacker and this may lead to incorrect data delivered to ALPR Engine. Consider using a standard authentication mechanism to identify the source data store.
91	Spoofing of Destination Data Store Configuration File	Spoofing	Diagram 1	update configuration	High	Not Started	Configuration File may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Configuration File. Consider using a standard authentication mechanism to identify the destination data store.
92	Potential Data Repudiation by Web Client (Main Process)	Repudiation	Diagram 1	Request	High	Not Started	Web Client (Main Process) 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.
93	Potential Lack of Input Validation for Web Client (Main Process)	Tampering	Diagram 1	Request	High	Not Started	Data flowing across Request may be tampered with by an attacker. This may lead to a denial of service attack against Web Client (Main Process) or an elevation of privilege attack against Web Client (Main Process) or an information disclosure by Web Client (Main Process). 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.
94	Spoofing the Web Client (Main Process) Process	Spoofing	Diagram 1	Request	High	Not Started	Web Client (Main Process) may be spoofed by an attacker and this may lead to information disclosure by Mobile Web Client. Consider using a standard authentication mechanism to identify the destination process.
95	Spoofing the Mobile Web Client Process	Spoofing	Diagram 1	Request	High	Not Started	Mobile Web Client may be spoofed by an attacker and this may lead to unauthorized access to Web Client (Main Process). Consider using a standard authentication mechanism to identify the source process.
96	Spoofing the Web Client (Main Process) Process	Spoofing	Diagram 1	Response	High	Not Started	Web Client (Main Process) may be spoofed by an attacker and this may lead to unauthorized access to Mobile Web Client. Consider using a standard authentication mechanism to identify the source process.
97	Spoofing the Mobile Web Client Process	Spoofing	Diagram 1	Response	High	Not Started	Mobile Web Client may be spoofed by an attacker and this may lead to information disclosure by Web Client (Main Process). Consider using a standard authentication mechanism to identify the destination process.
98	Potential Lack of Input Validation for Mobile Web Client	Tampering	Diagram 1	Response	High	Not Started	Data flowing across Response may be tampered with by an attacker. This may lead to a denial of service attack against Mobile Web Client or an elevation of privilege attack against Mobile Web Client or an information disclosure by Mobile Web Client. 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.
99	Potential Data Repudiation by Mobile Web Client	Repudiation	Diagram 1	Response	High	Not Started	Mobile Web 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.
100	Data Flow Sniffing	Information Disclosure	Diagram 1	Response	High	Not Started	Data flowing across Response 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.
101	Potential Process Crash or Stop for Mobile Web Client	Denial Of Service	Diagram 1	Response	High	Not Started	Mobile Web Client crashes, halts, stops or runs slowly; in all cases violating an availability metric.
102	Data Flow Response Is Potentially Interrupted	Denial Of Service	Diagram 1	Response	High	Not Started	An external agent interrupts data flowing across a trust boundary in either direction.
103	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	Response	High	Not Started	Mobile Web Client may be able to impersonate the context of Web Client (Main Process) in order to gain additional privilege.
104	Mobile Web Client May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	Diagram 1	Response	High	Not Started	Web Client (Main Process) may be able to remotely execute code for Mobile Web Client.
105	Elevation by Changing the Execution Flow in Mobile Web Client	Elevation Of Privilege	Diagram 1	Response	High	Not Started	An attacker may pass data into Mobile Web Client in order to change the flow of program execution within Mobile Web Client to the attacker's choosing.

106	Cross Site Request Forgery	Elevation Of Privilege	Diagram 1	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.
107	Cross Site Request Forgery	Elevation Of Privilege	Diagram 1	Configuration	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.
108	Elevation by Changing the Execution Flow in Configure Process	Elevation Of Privilege	Diagram 1	Configuration	High	Not Started	An attacker may pass data into Configure Process in order to change the flow of program execution within Configure Process to the attacker's choosing.
109	Configure Process May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	Diagram 1	Configuration	High	Not Started	System Admin may be able to remotely execute code for Configure Process.
110	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	Configuration	High	Not Started	Configure Process may be able to impersonate the context of System Admin in order to gain additional privilege.
111	Potential Excessive Resource Consumption for ALPR Engine or Configuration File	Denial Of Service	Diagram 1	Save configuration	High	Not Started	Does ALPR Engine or Configuration File 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.
112	Data Flow Configuration Is Potentially Interrupted	Denial Of Service	Diagram 1	Configuration	High	Not Started	An external agent interrupts data flowing across a trust boundary in either direction.
113	Spoofing the Configure Process Process	Spoofing	Diagram 1	Configuration	High	Not Started	Configure Process may be spoofed by an attacker and this may lead to information disclosure by System Admin. Consider using a standard authentication mechanism to identify the destination process.
114	Data Flow Res Is Potentially Interrupted	Denial Of Service	Diagram 1	Res	High	Not Started	An external agent interrupts data flowing across a trust boundary in either direction.
115	Spoofing of Destination Data Store Configuration File	Spoofing	Diagram 1	Save configuration	High	Not Started	Configuration File may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Configuration File. Consider using a standard authentication mechanism to identify the destination data store.
116	External Entity System Admin Potentially Denies Receiving Data	Repudiation	Diagram 1	Res	High	Not Started	System Admin 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.
117	Spoofing of the System Admin External Destination Entity	Spoofing	Diagram 1	Res	High	Not Started	System Admin may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of System Admin. Consider using a standard authentication mechanism to identify the external entity.
118	Potential Process Crash or Stop for Configure Process	Denial Of Service	Diagram 1	Configuration	High	Not Started	Configure Process crashes, halts, stops or runs slowly; in all cases violating an availability metric.
119	Data Flow Sniffing	Information Disclosure	Diagram 1	Configuration	High	Not Started	Data flowing across Configuration 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.

120	Potential Data Repudiation by Configure Process	Repudiation	Diagram 1	Configuration	High	Not Started	Configure Process 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.
121	Potential Lack of Input Validation for Configure Process	Tampering	Diagram 1	Configuration	High	Not Started	Data flowing across Configuration may be tampered with by an attacker. This may lead to a denial of service attack against Configure Process or an elevation of privilege attack against Configure Process or an information disclosure by Configure Process. 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.
122	Spoofing the System Admin External Entity	Spoofing	Diagram 1	Configuration	High	Not Started	System Admin may be spoofed by an attacker and this may lead to unauthorized access to Configure Process. Consider using a standard authentication mechanism to identify the external entity.
123	Spoofing of the System Admin External Destination Entity	Spoofing	Diagram 1	Registration Result	High	Not Started	System Admin may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of System Admin. Consider using a standard authentication mechanism to identify the external entity.
124	External Entity System Admin Potentially Denies Receiving Data	Repudiation	Diagram 1	Registration Result	High	Not Started	System Admin 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.
125	Data Flow Registration Result Is Potentially Interrupted	Denial Of Service	Diagram 1	Registration Result	High	Not Started	An external agent interrupts data flowing across a trust boundary in either direction.
126	Spoofing the User Management Process Process	Spoofing	Diagram 1	User Information	High	Not Started	User Management Process may be spoofed by an attacker and this may lead to information disclosure by System Admin. Consider using a standard authentication mechanism to identify the destination process.
127	Spoofing the System Admin External Entity	Spoofing	Diagram 1	User Information	High	Not Started	System Admin may be spoofed by an attacker and this may lead to unauthorized access to User Management Process. Consider using a standard authentication mechanism to identify the external entity.
128	Potential Lack of Input Validation for User Management Process	Tampering	Diagram 1	User Information	High	Not Started	Data flowing across User Information may be tampered with by an attacker. This may lead to a denial of service attack against User Management Process or an elevation of privilege attack against User Management Process or an information disclosure by User Management Process. 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.
129	Cross Site Scripting	Tampering	Diagram 1	User Information	High	Not Started	The web server 'User Management Process' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.
130	Potential Data Repudiation by User Management Process	Repudiation	Diagram 1	User Information	High	Not Started	User Management Process 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.
131	Data Flow Sniffing	Information Disclosure	Diagram 1	User Information	High	Not Started	Data flowing across User Information 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.
132	Potential Process Crash or Stop for User Management Process	Denial Of Service	Diagram 1	User Information	High	Not Started	User Management Process crashes, halts, stops or runs slowly; in all cases violating an availability metric.
133	Data Flow User Information Is Potentially Interrupted	Denial Of Service	Diagram 1	User Information	High	Not Started	An external agent interrupts data flowing across a trust boundary in either direction.
134	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	User Information	High	Not Started	User Management Process may be able to impersonate the context of System Admin in order to gain additional privilege.
135	User Management Process May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	Diagram 1	User Information	High	Not Started	System Admin may be able to remotely execute code for User Management Process.
136	Elevation by Changing the Execution Flow in User Management Process	Elevation Of Privilege	Diagram 1	User Information	High	Not Started	An attacker may pass data into User Management Process in order to change the flow of program execution within User Management Process to the attacker's choosing.

137	Cross Site Request Forgery	Elevation Of Privilege	Diagram 1	User Information	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.
138	Data Flow Command Is Potentially Interrupted	Denial Of Service	Diagram 1	Command	High	Not Started	An external agent interrupts data flowing across a trust boundary in either direction.
139	Elevation Using Impersonation	Elevation Of Privilege	Diagram 1	Command	High	Not Started	Web Client (Main Process) may be able to impersonate the context of Police Officer in order to gain additional privilege.
140	Web Client (Main Process) May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	Diagram 1	Command	High	Not Started	Police Officer may be able to remotely execute code for Web Client (Main Process).
141	Elevation by Changing the Execution Flow in Web Client (Main Process)	Elevation Of Privilege	Diagram 1	Command	High	Not Started	An attacker may pass data into Web Client (Main Process) in order to change the flow of program execution within Web Client (Main Process) to the attacker's choosing.
142	Cross Site Request Forgery	Elevation Of Privilege	Diagram 1	Command	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.
143	Spoofing of the Police Officer External Destination Entity	Spoofing	Diagram 1	Response	High	Not Started	Police Officer may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Police Officer. Consider using a standard authentication mechanism to identify the external entity.
144	External Entity Police Officer Potentially Denies Receiving Data	Repudiation	Diagram 1	Response	High	Not Started	Police Officer 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.
145	Data Flow Response Is Potentially Interrupted	Denial Of Service	Diagram 1	Response	High	Not Started	An external agent interrupts data flowing across a trust boundary in either direction.

Critical threats

Title	Category	Interaction	Weakness	Threat scenarios	Priority	security requirement	Mitigation
Weak Access Control for a Resource	Information Disclosure	Driver/Car Information	There are multiple users to retrieve DB records.	The attacker can use the police officer credential to obtain vehicle owner information (birthday, address) and vehicle information (manufacturer, year of production, model, color).	Critical	SR1 : All users accessing the DB of the system must be authenticated.	User authentication - Authentication in the context of web applications is commonly performed by submitting a username or ID and one or more items of private information that only a given user should know. - Implement Proper Password Strength Controls
			DB records are stored in plain text DB records contain private information of car owner.	The attacker can attack the server hosting company and take all DB data. At this time, if the DB data is stored in plain text, information leakage occurs.	Critical	SR2 : The DB of the system must be encrypted	Encrypt DB contents - Use strong encryption algorithms to encrypt data in the database - SQL Server allows administrators and developers to choose from among several algorithms, including DES, Triple DES, TRIPLE_DES_3KEY, RC2, RC4, 128-bit RC4, DESX, 128-bit AES, 192-bit AES, and 256-bit AES
					Critical	SR3 : User permissions to access DB should be classified and managed. (ACL, DAC)	only allow Read permission - Ensure that least-privileged accounts are used to connect to Database server - Sysadmin role should only have valid necessary users
Cross Site Scripting	Tampering	Query with Plate Number	No record of license plate inquiries No record of delivery of query results	The attacker can obtain the vehicle owner's information (vehicle number, name, date of birth, address) from the server upon triggering 'Partial Match' by incomplete plate numbers.	Critical	SR5 : Communication history management using communication channel between client and server should be performed.	Ensure that auditing and logging is enforced on the application
			No restrictions on the format and length of the license plate query string Web interface is vulnerable to XSS	The attacker can intercept communication and change the request or response. This could lower the reliability of the system by making the response come unconditionally as a criminal vehicle.	Critical	SR6 : The query statement through the communication channel between the client and the server must be verified.	Limit query string length & format Perform input validation and filtering on all string type Model properties All the input parameters must be validated before they are used in the application to ensure that the application is safeguarded against malicious user inputs. Validate the input values using regular expression validations on server side with a allowed list validation strategy. Unsanitized user inputs / parameters passed to the methods can cause code
					Critical	SR7 : The communication channel between the client and the server must be encrypted.	Enable HTTPS - Secure Transport channel The application configuration should ensure that HTTPS is used for all access to sensitive information.
Spoofing the Web Client (Main Process) Process	Spoofing	Query with Plate Number	User credential can be compromised.	The attacker can use the user credentials to query the license plate server.	Critical	SR8 : The client system can only use digitally signed queries.	Apply authentication token
			Weak password phrase	The attacker can guess user's id and password	Critical	SR9: The client user should use a strong password.	Support Proper Password Strength Controls.
			Authentication token can be compromised.	The attacker can use the key to create an authentication token.	Critical	SR10 : The server must manage the digital signature.	Change the token generation key periodically.
Potential Process Crash or Stop for Plate Query Process	Denial Of Service	Query with Plate Number	Excessive queries in a short time	After the attacker finds the port number used by the server, the attacker sends excessive queries to the extent that the service can be slowed down or stopped.	Critical	SR4 : The server must be capable of responding to a large number of queries.	Immediate recovery Deploy server as a container (fault tolerance)

Potential Data Repudiation by Plate Query Process	Repudiation	Query with Plate Number	No record of license plate inquiries No record of delivery of query results	The attacker can intercept the contents of query through a MITM attack and prevent it from being delivered to the server.	Critical	SR5 : Communication history management using communication channel between client and server should be performed.	logging (audit) Ensure that auditing and logging is enforced on the application