The list of found vulnerabilities from team.2

Vuln. ID.	Summary	Location	Consequences/impact	CVSS Score	Proof of Concept	analysis technique	recommendation
ex)	A description of the vulnerability.	The location of the vulnerability in the project. This may be a component or source file.	The perceived impact of the vulnerability.	Use CVSS version 3.1 to compute the score	The specific test, technique step, or scenario that uncovered the vulnerability. This will depend on the technique selected.	The analysis technique that uncovered the vulnerability	

VID-1	If we can set request.session.error, then we have access to add a new user in the same privilege as super user.	C:\Users\user\source\repos\2022-security-specialist-team2\client\studio\webapp\templates\login\signup.html
		{% if user.is_superuser or request.session.error %}
		<button type="submit" class="btn btn-primary">생성하기
		</button>
		{% endif%}
		
		C:\Users\user\source\repos\2022-security-specialist-team2\client\studio\webapp\alpr\views.py > upload()
		try:
		video_path = settings.MEDIA_ROOT + '/..' + document.
		uploadedFile.url
		pic = Image.open(video_path)
		width, height = pic.size
		if (width*height <= 1):
		request.session['error'] = True
		comment = pic.app['COM'].decode('ascii')
			An attacker can have the same privilege as super user. He or she can add or delete an user.
			
			EOP
				High (8.7) CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N	We found that uploading an image with width and height less than or equal to 1 can set request.session.error.
					
					1) Make a small image with width and height less than or equal to 1
					
					2) Upload it
					
					3) Then we have access to add a new user in the same privilege as super user.
						Code Review
						- Looked closely at the code that seems to be seeded
							Fix improper error handling; Apply least privileged access control

VID-2	If the user id is '..' then a video or image file cannot be uploaded.	C:\Users\user\source\repos\2022-security-specialist-team2\client\studio\webapp\alpr\views.py > upload()	Path traversal allows unauthorized users to access files. DOS	Medium (6.5) CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	1) Make a small image with width and height less than or equal to 1 2) Upload it 3) Then we have access to add a new user in the same privilege as super user. 4) Add a new user - ID is '..' 5) Try to upload a video or image file 6) Get an error from Django framework ERROR:django.security.SuspiciousFileOperation:Detected path traversal attempt in 'media/../1.PNG' WARNING:django.request:Bad Request: /alpr/upload	Input Validation - File upload validation Refer to OWASP cheat sheet https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html	Recommend that you use user ID as user folder path.

VID-3	If you rename the sample video file to a long name and upload it, an internal error occurs the moment the license plate is recognized.	C:\Users\user\source\repos\2022-security-specialist-team2\client\studio\webapp\alpr\views.py > VideoUpstream > __del__
		
		def __del__(self):
		if self.video:
		self.video.release()
		print("video released")
		print("destroy............")
		
		def get_frame(self, frame=None):
		try:
		if frame is None:
		image = self.frame
		_, jpeg = cv2.imencode('.jpg', image)
		else :
		image = frame
		_, jpeg = cv2.imencode('.jpg', image)
		except:
		print("close connection")
			An attacker can trigger malfunction of various components by providing malformed data.
			
			DOS
				High (7.3) CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:H	1) Rename beaver1.avi to
					aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
					aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
					aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
					aaaaaaaaaaaaaa.avi
					
					2) Upload it
					
					3) An internal error occurs the moment the license plate is recognized for the first time and the recognition operation stops.
					
					update error: Storage can not find an available filename for "media/gord36k/aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
					aaaaaaaaaaaaaaa_OK0dS1s\261_099cwwv.jpg". Please make sure that the corresponding file field allows sufficient "max_length".
					video released
					destroy............
					end of update
					close connection
					video released
					destroy............
					video released
					destroy............
					[07/Jul/2022 17:58:31] "GET /alpr/playback?
					pid=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
					aaaaaaa_OK0dS1s.avi HTTP/1.1" 200 57362653
						Input Validation
						- Tried to input the longest file name the system can handle
							recommend limiting the file length in upload function.

The list of found vulnerabilities from team.2

Vuln. ID.	Summary	Location	Consequences/impact	CVSS Score	Proof of Concept	analysis technique	recommendation

VID-4	The key code value used for DB encryption in the Lookup server is the ASCII string '2Team_AhnLab' and it's hard-coded.	C:\Users\user\source\repos\2022-security-specialist-team2\server\plateServer\server\server.cpp
		const char code[12] = { 0x32, 0x54, 0x65, 0x61, 0x6d, 0x5f, 0x41, 0x68, 0x6e, 0x4c, 0x61, 0x62 };
		...
		ret = dbp->set_encrypt(dbp, code, flags);
			The use of a hard-coded cryptographic key significantly increases the possibility that encrypted data may be recovered.
			
			A weak encryption scheme can be subjected to brute force attacks that have a reasonable chance of succeeding using current attack methods and resources.
			
			INFORMATION-DISCLOSURE
			TAMPERING
				High (7.5) CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H	(INFORMATION-DISCLOSURE)
					We can read the encrypted DB using the hard-coded key.
					
					const char code[12] = { 0x32, 0x54, 0x65, 0x61, 0x6d, 0x5f, 0x41, 0x68, 0x6e, 0x4c, 0x61, 0x62 };
					
					ret = db_create(&dbp, NULL, 0);
					
					flags = DB_ENCRYPT_AES;
					ret = dbp->set_encrypt(dbp, code, flags);
					flags = DB_CREATE;
					ret = dbp->open(dbp, /* DB structure pointer */
					NULL, /* Transaction pointer */
					"licenseplate.db", /* On-disk file that holds the database. */
					NULL, /* Optional logical database name */
					DB_HASH, /* Database access method */
					flags, /* Open flags */
					0); /* File mode (using defaults) */
					ret = dbp->get(dbp, NULL, &key, &data, 0)
					
					(TAMPERING)
					1. read decryed DB and modify car's owner.
					2. make another DB by using same key {0x32, 0x54 ...}
					3. update DB file.
					4. plate server gets car information from the DB file that attacker changes.
						Code Review
						- Looked closely at the code that seems to be seeded
						
						tool
						- IDA, db_dump, Hex View
							Remove the hard-coded key value; Change to a stronger one and store it in a secure place

VID-5	If you upload an image file with comments as 'Ahnlab', it gives a shutdown command to the server.	C:\Users\user\source\repos\2022-security-specialist-team2\client\studio\webapp\alpr\views.py > upload() comment = pic.app['COM'].decode('ascii') if (comment.strip('\x00') == app_name): send_command()	An attacker can trigger malfunction of various components by providing malformed data. TAMPERING, DOS	High(7.6) CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:N/I:L/A:H	1) Add a comment into a sample JPEG file using ImageMagick convert tool $ convert target.jpg -set comment "Ahnlab" target.jpg 2) Upload it 3) The server stops because it receives 'shutdown' command	Code Review - Looked closely at the code that seems to be seeded	Remove unnecessary code through code review
VID-6	It is possible to delete files uploaded by another user.	C:\Users\user\source\repos\2022-security-specialist-team2\client\studio\webapp\alpr\views.py > remove() id = request.GET['id'] filepath = settings.BASE_DIR url = models.Document.objects.get(id=id).uploadedFile.url try: models.Document.objects.filter(id=id).delete() print(rootpath+'../'+url) os.remove(rootpath+'../'+url)	Uploaded contents can be deleted by anyone who logged in the system. TAMPERING	High (7.6) CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:N/I:H/A:L	1) Select one file 'id' (e.g. 54) in the DB 'alpr_document' table 2) Login to the client 3) Type https://ahnlab2.lge.com:8000/alpr/remove?id=54 in the browser 4) If the file deletion is successful, nothing is displayed. Otherwise, a 500 server error returns. 5) Check if the file 'id' has been removed in the DB 'alpr_document' table	Code Review Active Scan with OWASP ZAP	Apply access control so that users can only control their own data
VID-7	Using the user's session id, you can login without password or 2 factor authentication.	C:\Users\User\source\repos\2022-security-specialist-team2-main\2022-security-specialist-team2-main\team2\Lib\site-packages\django\contrib\sessions\backends\db.py > load() def load(self): s = self._get_session_from_db() return self.decode(s.session_data) if s else {}	An attacker can use another user's session ID to log in and use the system without a separate authentication process. Spoofing	Medium (5.8) CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:N/A:N	1) Access https://ahnlab2.lge.com:8000/ with a web browser 2) Open developer tools -> Application -> Cookies 3) Enter session id and value of other user session id in cookies 4) Access https://ahnlab2.lge.com:8000/alpr with a web browser	Tinker Check for known vulnerabilities	Set session validity period for user authentication In case of django, the session validity period can be set through the COOKIE_AGE value (default : 2 weeks)

VID-8	0 can be entered as the maximum user setting value in 'server.conf'. This causes the server to either return an internal error or hang.	C:\Users\user\source\repos\2022-security-specialist-team2\client\studio\webapp\alpr\views.py > send_configuration()
		
		conn_config.sendall("max".encode('utf-8')) #send Command
		
		value=int(max_user) # need to input value
		value=value.to_bytes(3, 'big')
		conn_config.sendall(value)
			An internal server error(500) occurs and the system is not work properly(hang).
			
			DOS
				High (7.9)
				CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:N/I:H/A:H
					1) Go to settings page
					2) Click update button without 2 values(maxuser, confidence)
					3) Check error message : Internal Server Error(500)
					4) Run the system again(restart each server)
					5) Check 'server.conf' file
						Input Validation
						Code Review
							Check setting input value whether it is within the normal range before use