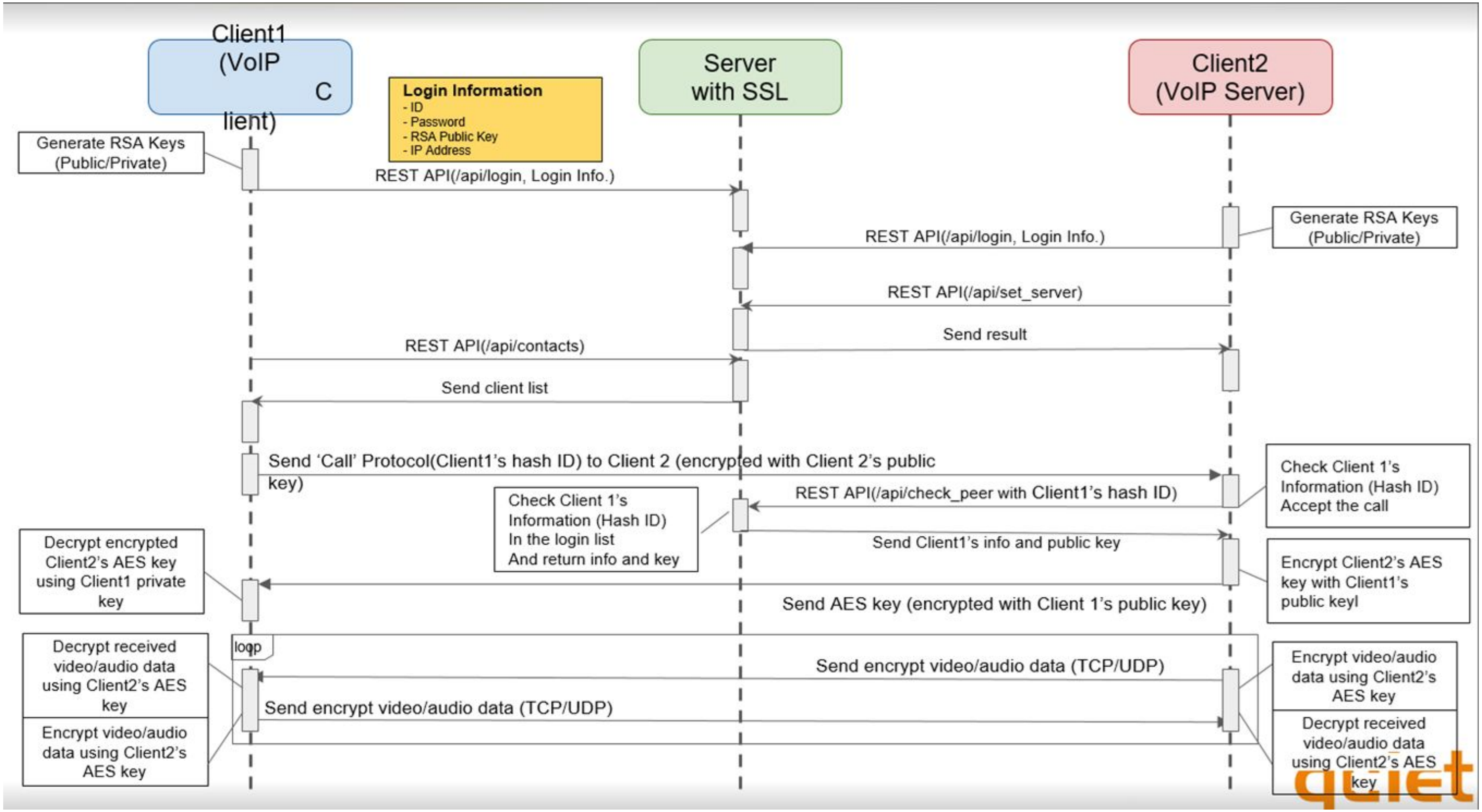
VideoChat

3조 보안연대
Team David
Belasco

Architecture(team1 project)

call CALL_STATUS_PORT :10002
VOIP_LOCAL_PORT :10001
VIDEO_PORT :10000



Demo

Project Members and Role

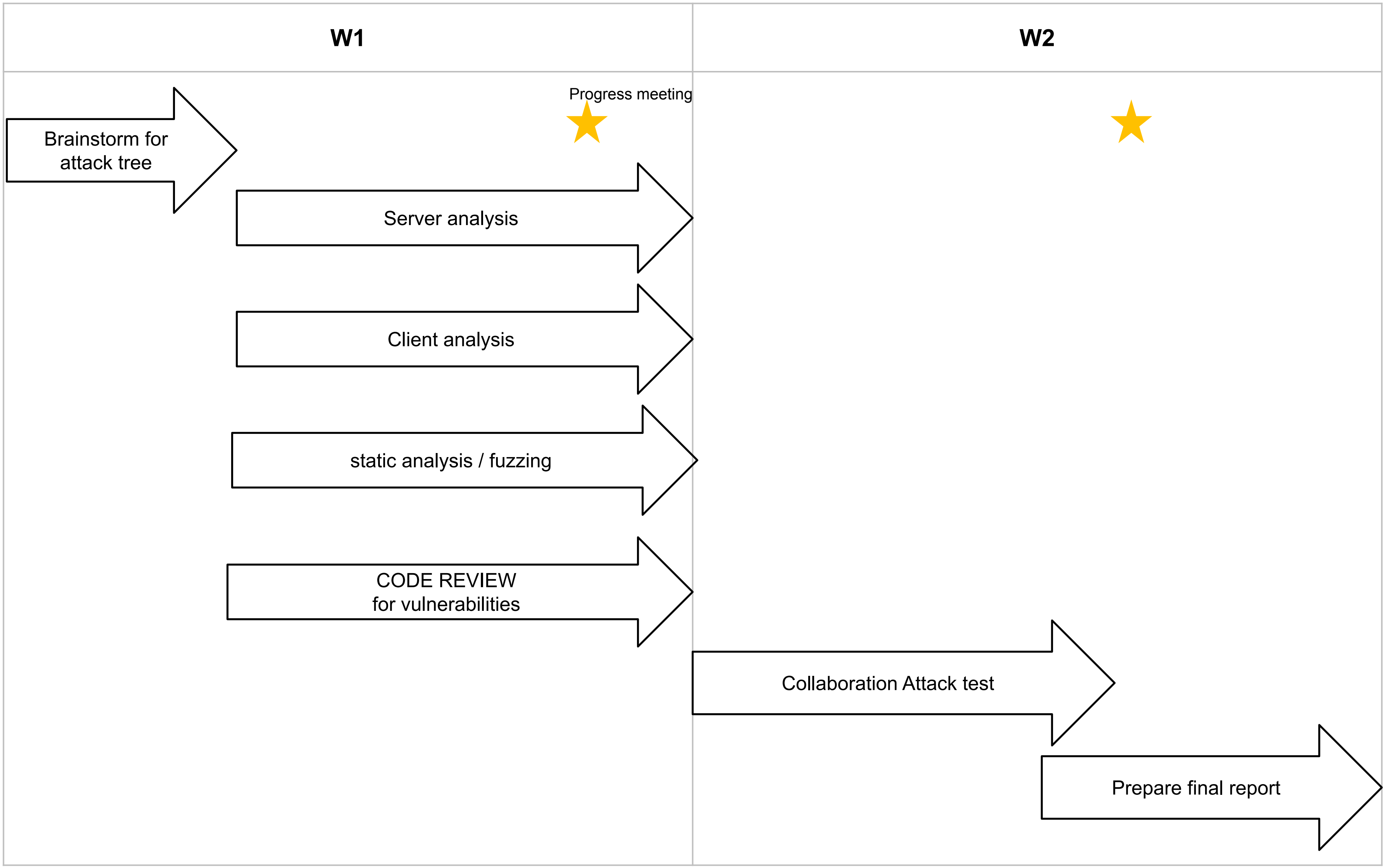
- Server vulnerability analysis
  Robin Kim(김성준), SeKi Park(박세기)

- Client vulnerability analysis
  SungMin Kim(김성민), DongHoon Shin(신동훈)

- Static analysis and fuzzing
  JiYoung Yoon(윤지영)

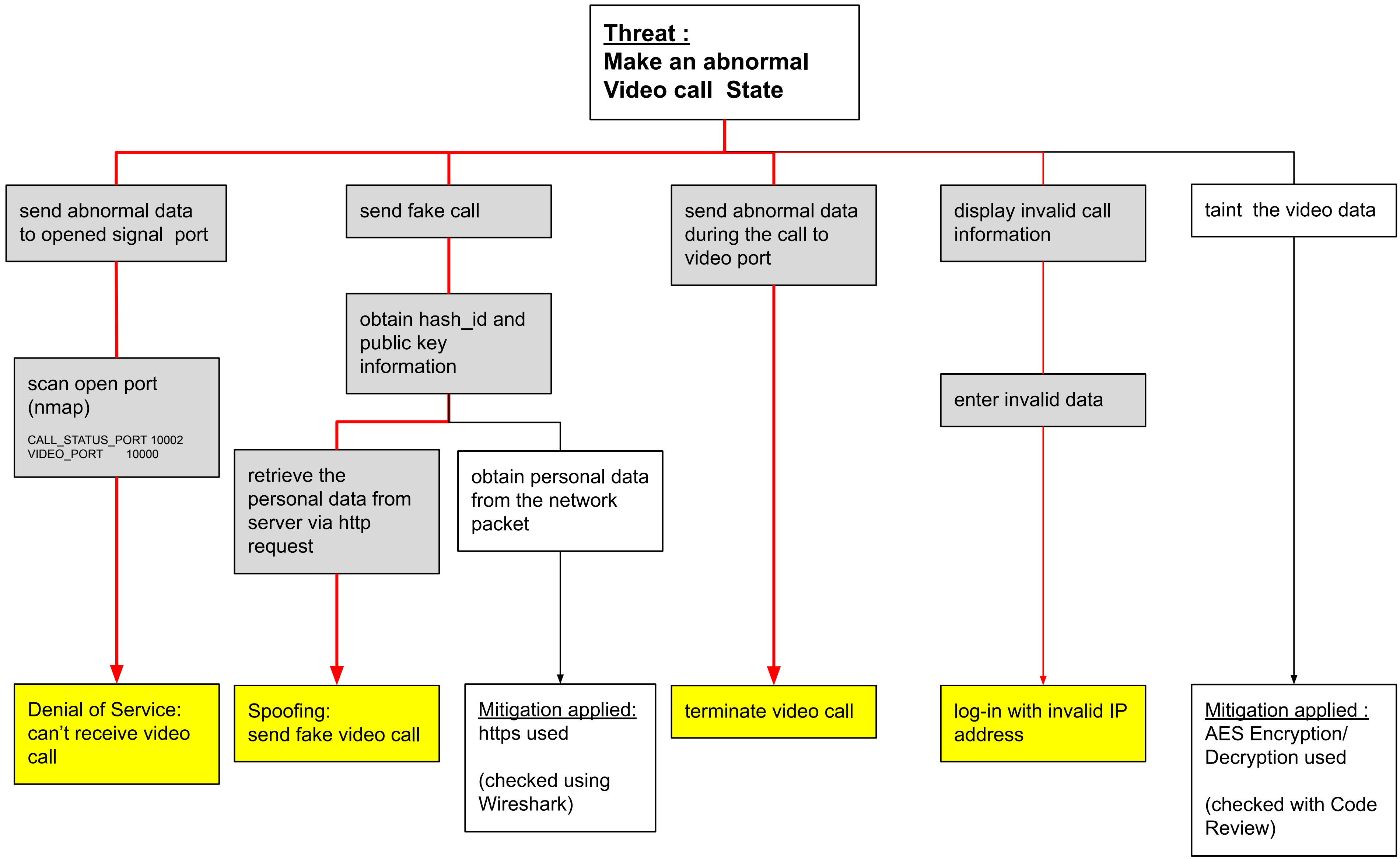
- Mentor / Support
  David Belasco

Schedule



W1
W2
Progress meeting
Brainstorm for attack tree
Server analysis
Client analysis
static analysis / fuzzing
CODE REVIEW for vulnerabilities
Collaboration Attack test
Prepare final report

Attack Tree


Threat :
Make an abnormal
Video call State
send abnormal data to opened signal port
send fake call
send abnormal data during the call to video port
display invalid call information
taint the video data
scan open port (nmap)
CALL_STATUS_PORT 10002
VIDEO_PORT 10000
obtain hash_id and public key information
enter invalid data
retrieve the personal data from server via http request
obtain personal data from the network packet
Denial of Service: can't receive video call
Spoofing: send fake video call
Mitigation applied: https used
(checked using Wireshark)
terminate video call
log-in with invalid IP address
Mitigation applied : AES Encryption/ Decryption used
(checked with Code Review)

Executive Summary

- Top 5 vulnerabilities listed out of 12

Priority	Vulnerability	Impact	Recommendation
High (CVSS 7.5) Appendix-22	If hash_id and public key is known, it is possible to make fake call. (Spoofing)	Attacker can make a fake call with hash_id and public_key.	- Check and validate the caller's IP address. - Compare real IP and IP registered in server
High (CVSS 7.5)	Any call request can be allowed. (Denial of Service)	Attacker can make a fake call infinitely	- Check and validate the caller's IP address - Limit request count within some duration
High (CVSS 7.5)	Anyone can send the call end request. (Denial of Service)	Attacker can make a request call end infinitely Attacker can make call end during a call	- Open video port only call is received
Mid (CVSS 5.4)	All REST api is exposed. (Information disclosure)	An attacker can retrieve the personal data via http request	Remove REST api document page
Low (CVSS 3.1)	Need IP address sanitizer	Possible to log-in with invalid IP address	IP address input validation

Evaluation Constraints - Mitigating Factors

Mitigating Factors	**Descriptions**
Data Encryption	Video call data should be secured in transit.
	Sensitive data should be stored securely.
Authentication / Authorization	All users should be authenticated correctly and securely.
	Network communications should use TLS or an equivalent encryption protocol.
	Each user should only have the capabilities they are explicitly granted permitted to use
Secure Coding	Secure coding practices are applied to avoid common security flaws like SQL injection and buffer overflow.

Evaluation Constraints - Assumptions

Assumptions	**Descriptions**
Cryptography	Crypto APIs used are assumed to be secure. ex) RAND_bytes()
	Crypto library providing APIs is assumed to be safe. ex) OpenSSL
Storage Security	Due to hardware constraints, credentials are assumed to be securely stored in trusted location.
	Credentials are not left in system memory.
	The inherent stability and security specific to currently used database are not taken into consideration.

Evaluation Narrative

Analysis Technique	Using Tool	Result	Vulnerability
Static Analysis X Code Review O	SonarCloud, Cppcheck	No meaningful issue	Vul-5 Appendix-11~13
Web Fuzzing O	DirBuster, DIRB	Detected critical page (docs, redoc) REST api is exposed and possible to get user data.	Vul-1 Appendix-1~4
Client Fuzzing X	SPIKE	Run a fuzzing test on the socket communication and found no issues.	None Appendix-23
Input Validation O	Code Review	Need IP address validation. (Any data is acceptable in IP addr)	Vul-5 Appendix-10
Use Exploit Tools O	Postman, Wireshark, nmap, Kali, scapy, checksec	Postman - http request Kali - ARP spoofing checksec - CFG,RFG not present User info. is exposed with REST api.	Vul-2, Vul-3, Vul-4 Vul-6 Appendix-5~9 Appendix-17~21
Research Vulnerability DB X	https://www.cvedetails.com	No issue : There's no vulnerabilities. (openssl 3.1.1, opus 1.3.1)	None Appendix-14
Dependency check X	Owasp dependency-check	No meaningful issue	None Appendix-15

** Vul : It's defined vulnerability issue.

Vulnerability Reporting(1)

Num.	Summary	Location	Consequences/ Impact	CVSS Score	Proof of Concept(POC)
Vul-1	REST api is exposed. **/ Network Attack**	FastAPI expose REST api in docs, redoc	Attacker can retrieve user information / **Information disclosure**	CVSS 5.4	https://ip:8000/docs https://ip:8000/redoc
Vul-2	Make fake call **/ Client exploit**	If hash_id, public_key and IP is known, it is possible to make fake call	Attacker can make the fake call / **Spoofing**	CVSS 7.5	C++/Python exploit code can be made
Vul-3	Make fake call infinitely **/ Client exploit**	same as Vul-2	Attacker can make the fake call infinitely / **Denial of Service**	CVSS 7.5	C++/Python exploit code can be made

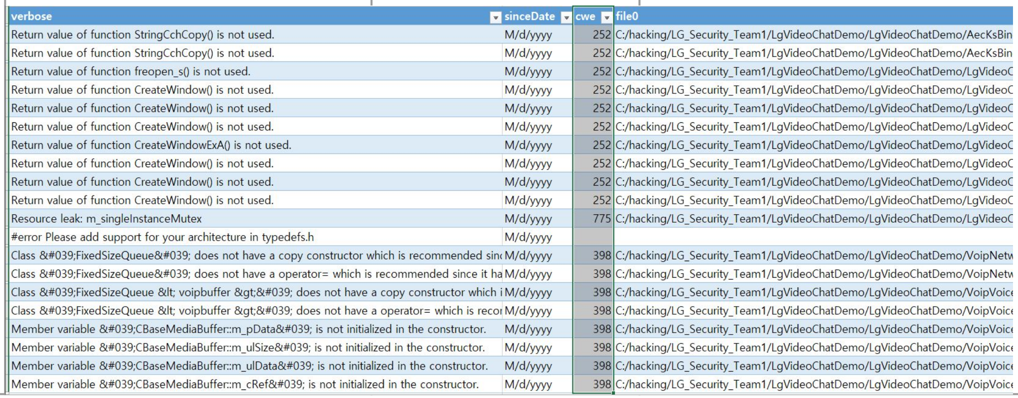
```
peer_hash_id = 'WOYXCNFRXYCVFO66'
rsa_key = 'LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0 … <snippet> ’

my_socket.connect(host, port)
encrypt_msg = my_socket.encrypt_message(rsa_key, peer_hash_id)
my_socket.send(encrypt_msg)
```

Vulnerability Reporting(2)

Num.	Summary	Location	Consequences/ Impact	CVSS Score	Proof of Concept(POC)
Vul-4	Make fake call end infinitely **/ Client exploit**	video port 10000 is always ready	Attacker can make the fake call end infinitely / **Denial of Service**	CVSS 7.5	C++/Python exploit code can be made
Vul-5	IP address input validation **/ Client attack**	No IP address validation check	Can not use video call if invalid IP address entered /	CVSS 3.1	Executable with invalid IP address
Vul-6	Spoof Voip Server **/ MITM, Network Attack** * Exploit not complete	Voip client does not have the process of authenticating Voip server.	Attacker can send AES keys Voip client/ Incorrect call connection or exposure of image data	CVSS 5.4	ARP Spoofing IP Spoofing

Weakness Reporting(1) - Client

Num.	Summary	Location	Consequences/ Impact	CWE number	Proof of Concept(POC)
Weak-1	Unchecked Return Value	LgVideoChatDemo/LgVideoChatDemo/AecKsBinder.cpp line 202,203 LgVideoChatDemo/LgVideoChatDemo.cpp line 175,705, 713	N/A	CWE-252	If error returns, malfunction
Weak-2	Indicator of Poor Code Quality	LgVideoChatDemo\LgVideoChatDemo\FixedSizeQueue.h line 18 LgVideoChatDemo\LgVideoChatDemo\mediabuf.h line 20	N/A	CWE-398	N/A
Weak-3	Missing Release of File Descriptor Handle after Effective Lifetime	LgVideoChatDemo/LgVideoChatDemo.cpp line 925	N/A	CWE-775	Memory leak



verbose	sinceDate	cwe	file0
Return value of function StringCchCopy() is not used.	M/d/yyyy	252	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/AecKsBin
Return value of function StringCchCopy() is not used.	M/d/yyyy	252	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/AecKsBin
Return value of function freopen_s() is not used.	M/d/yyyy	252	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/LgVideoC
Return value of function CreateWindow() is not used.	M/d/yyyy	252	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/LgVideoC
Return value of function CreateWindow() is not used.	M/d/yyyy	252	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/LgVideoC
Return value of function CreateWindow() is not used.	M/d/yyyy	252	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/LgVideoC
Return value of function CreateWindowExA() is not used.	M/d/yyyy	252	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/LgVideoC
Return value of function CreateWindow() is not used.	M/d/yyyy	252	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/LgVideoC
Return value of function CreateWindow() is not used.	M/d/yyyy	252	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/LgVideoC
Return value of function CreateWindow() is not used.	M/d/yyyy	252	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/LgVideoC
Resource leak: m_singleInstanceMutex	M/d/yyyy	775	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/LgVideoC
#error Please add support for your architecture in typedefs.h	M/d/yyyy		
Class 'FixedSizeQueue' does not have a copy constructor which is recommended sin	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/VoipNetw
Class 'FixedSizeQueue' does not have a operator= which is recommended since it ha	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/VoipNetw
Class 'FixedSizeQueue < voipbuffer >' does not have a copy constructor which i	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/VoipVoice
Class 'FixedSizeQueue < voipbuffer >' does not have a operator= which is recor	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/VoipVoice
Member variable 'CBaseMediaBuffer::m_pData' is not initialized in the constructor.	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/VoipVoice
Member variable 'CBaseMediaBuffer::m_ulSize' is not initialized in the constructor.	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/VoipVoice
Member variable 'CBaseMediaBuffer::m_ulData' is not initialized in the constructor.	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/VoipVoice
Member variable 'CBaseMediaBuffer::m_cRef' is not initialized in the constructor.	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideoChatDemo/LgVideoChatDemo/VoipVoice

Weakness Reporting(2) - OpenCV

OpenCV has 8 CWEs, Major 3 are below

CWE - 190 : Integer Overflow or Wraparound

CWE Definition	http://cwe.mitre.org/data/definitions/190.html
Number of vulnerabilities:	1879
Description	The software performs a calculation that can produce an integer overflow or wraparound, when the logic assumes that the resulting value will always be larger than the original value. This can introduce other weaknesses when the calculation is used for resource management or execution control.An integer overflow or wraparound occurs when an integer value is incremented to a value that is too large to store in the associated representation. When this occurs, the value may wrap to become a very small or negative number. While this may be intended behavior in circumstances that rely on wrapping, it can have security consequences if the wrap is unexpected. This is especially the case if the integer overflow can be triggered using user-supplied inputs. This becomes security-critical when the result is used to control looping, make a security decision, or determine the offset or size in behaviors such as memory allocation, copying, concatenation, etc.

CWE - 476 : NULL Pointer Dereference

CWE Definition	http://cwe.mitre.org/data/definitions/476.html
Number of vulnerabilities:	2131
Description	A NULL pointer dereference occurs when the application dereferences a pointer that it expects to be valid, but is NULL, typically causing a crash or exit.
Background Details	
Other Notes	

CWE - 457 : Use of Uninitialized Variable

CWE Definition	http://cwe.mitre.org/data/definitions/457.html
Number of vulnerabilities:	10
Description	The code uses a variable that has not been initialized, leading to unpredictable or unintended results.In some languages, such as C, an uninitialized variable contains contents of previously-used memory. An attacker can sometimes control or read these contents.
Background Details	
Other Notes	Before variables are initialized, they generally contain junk data of what was left in the memory that the variable takes up. This data is very rarely useful, and it is generally advised to pre-initialize variables or set them to their first values early. If one forgets -- in the C language -- to initialize, for example a char *, many of the simple string libraries may often return incorrect results as they expect the null termination to be at the end of a string.

Conclusions and Recommendations

- REST API document page must be *NOT* exposed publicly.
- Authenticate and validate all requests on server-side (eg. IP check)
- Rate Limiting
  - Set limits on number of requests per user or IP in certain time
- Recommend implementing logging system
- IP Reputation Lists : Blocking known malicious IPs
- Least Privilege Principle to SQLite db
  - No password and no setting of privilege in SQLite db
- Setup IDS(Intrusion Detection Systems)
  - monitor and alert system to detect any unusual activities

Reflection and Lessons Learned

- Gained critical insights into security vulnerabilities, types of attacks, and the potential for exploitation
- Required more experience to apply the attack techniques we have practiced in the course

What Worked Well?

- All requirements are satisfied in time
- Collaborated very well with each other during the project

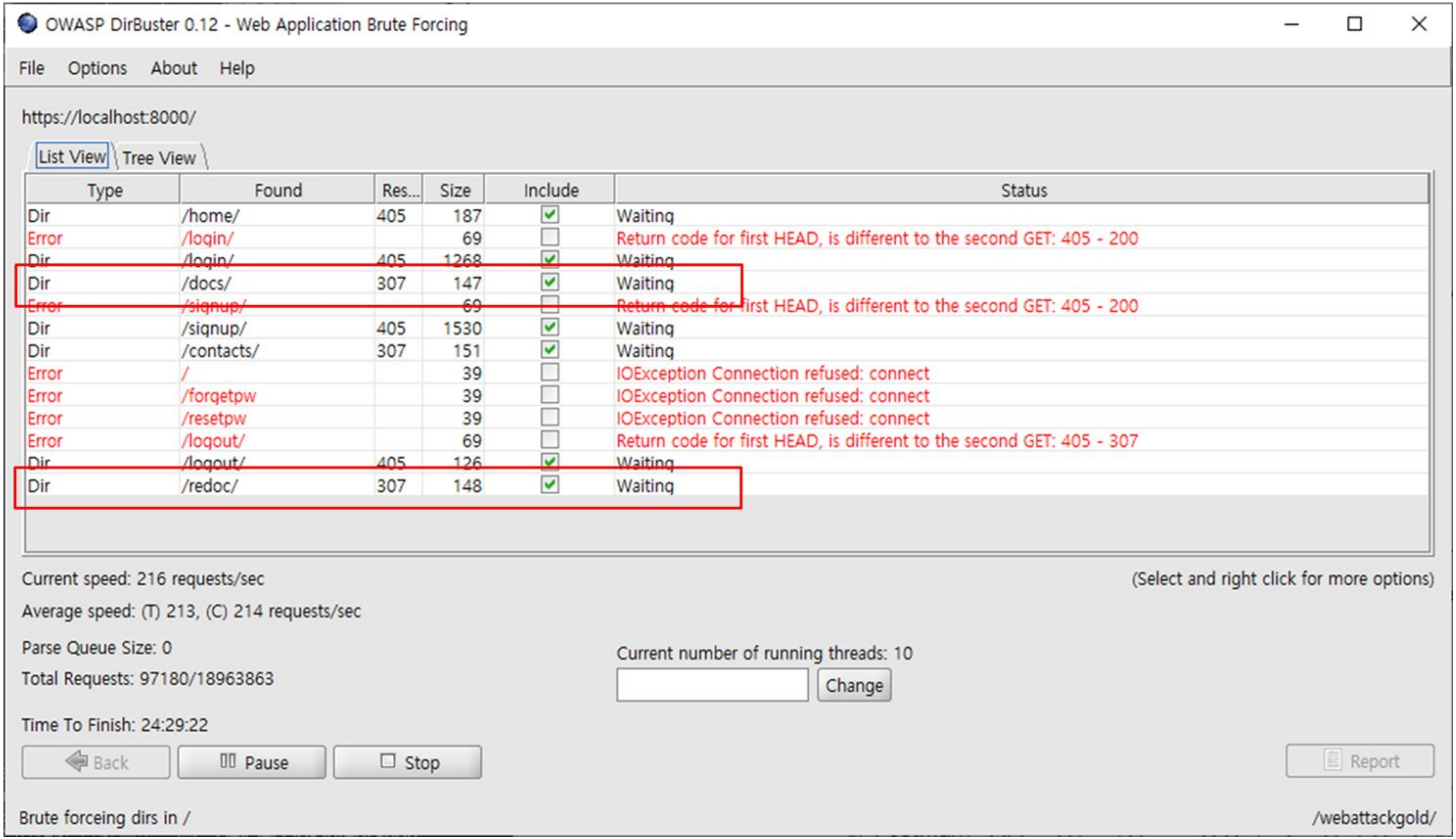
What Didn't Work Well?

- Does NOT execute GUI based Client Fuzzing (winAFL…)

Appendix

Appendix-1) DirBuster

Web Fuzzing Tool (DirBuster)

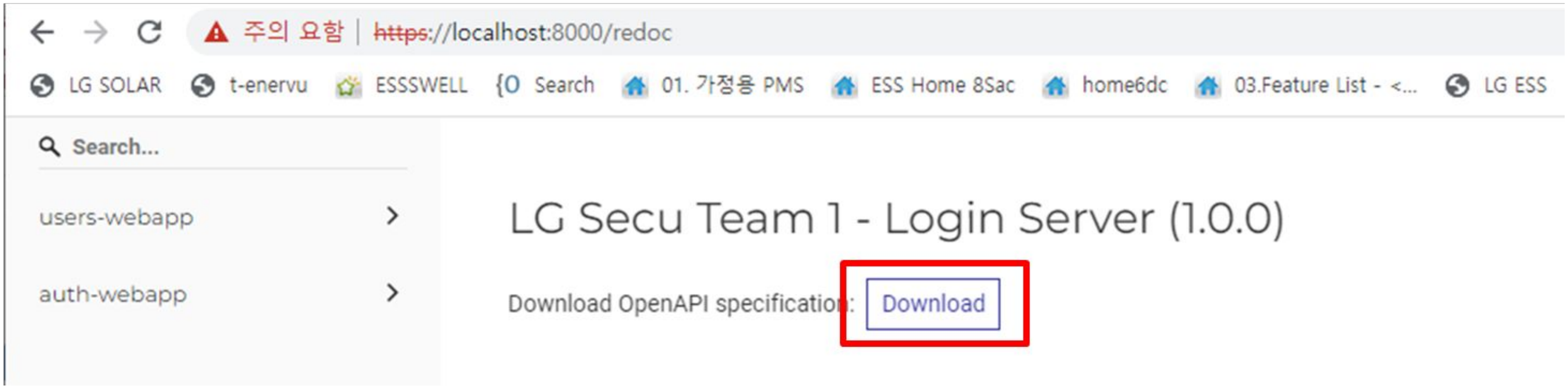


Appendix-2) DIRB(1)

```
$ dirb https://127.0.0.1:8000
-----------------
DIRB v2.22
By The Dark Raver
-----------------
START_TIME: Tue Jun 27 22:31:01 2023
URL_BASE: https://127.0.0.1:8000/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----------------
GENERATED WORDS: 4612
---- Scanning URL: https://127.0.0.1:8000/ ----
+ https://127.0.0.1:8000/contacts (CODE:422|SIZE:175)
+ https://127.0.0.1:8000/docs (CODE:200|SIZE:953)
+ https://127.0.0.1:8000/home (CODE:307|SIZE:0)
+ https://127.0.0.1:8000/login (CODE:307|SIZE:0)
+ https://127.0.0.1:8000/logout (CODE:307|SIZE:0)
+ https://127.0.0.1:8000/signup (CODE:307|SIZE:0)
+ https://127.0.0.1:8000/static (CODE:307|SIZE:0)
-----------------
END_TIME: Tue Jun 27 22:31:08 2023
DOWNLOADED: 4612 - FOUND: 7
```

Appendix-3) DIRB(2)

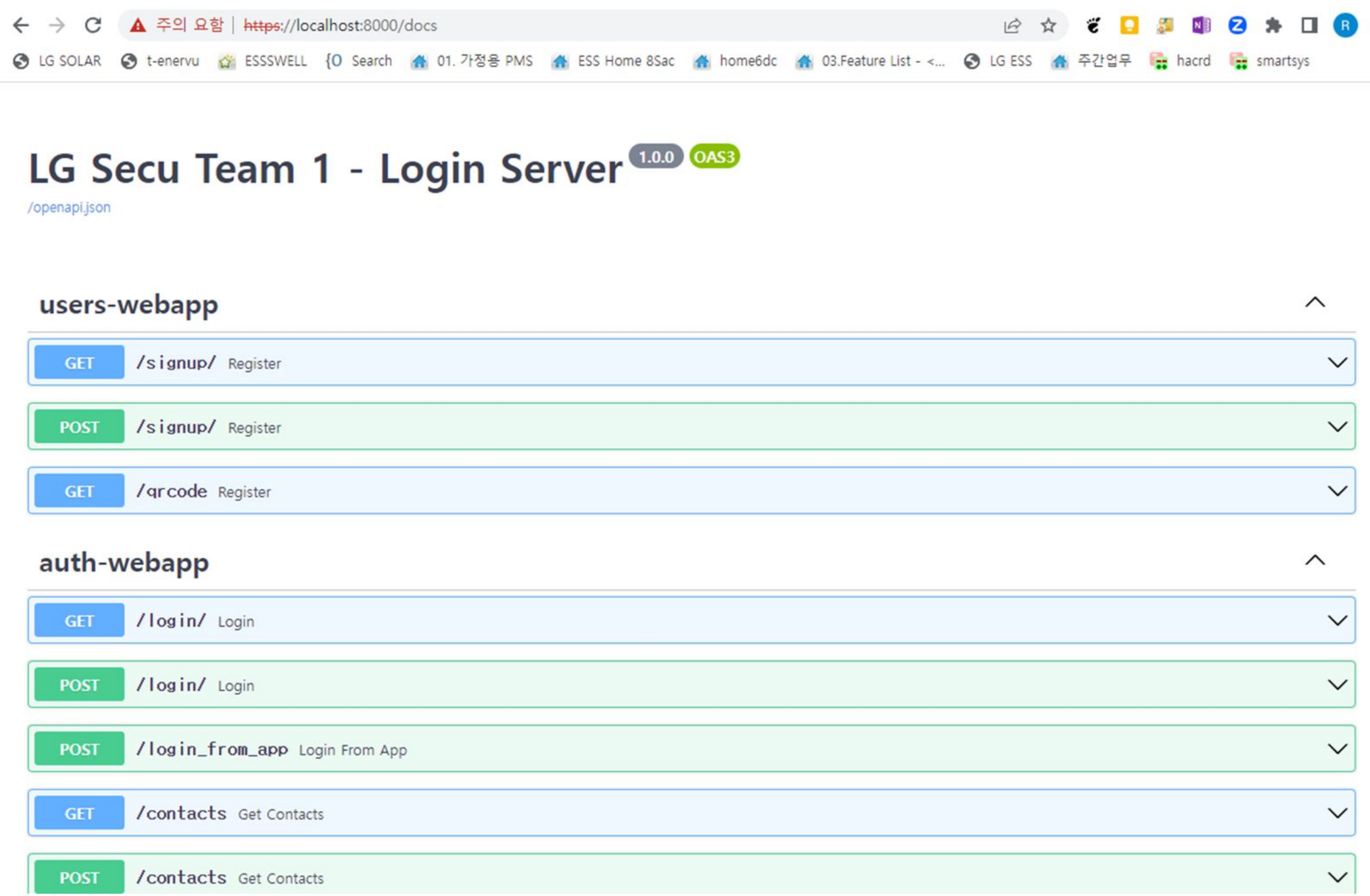
https://localhost:8000/redoc



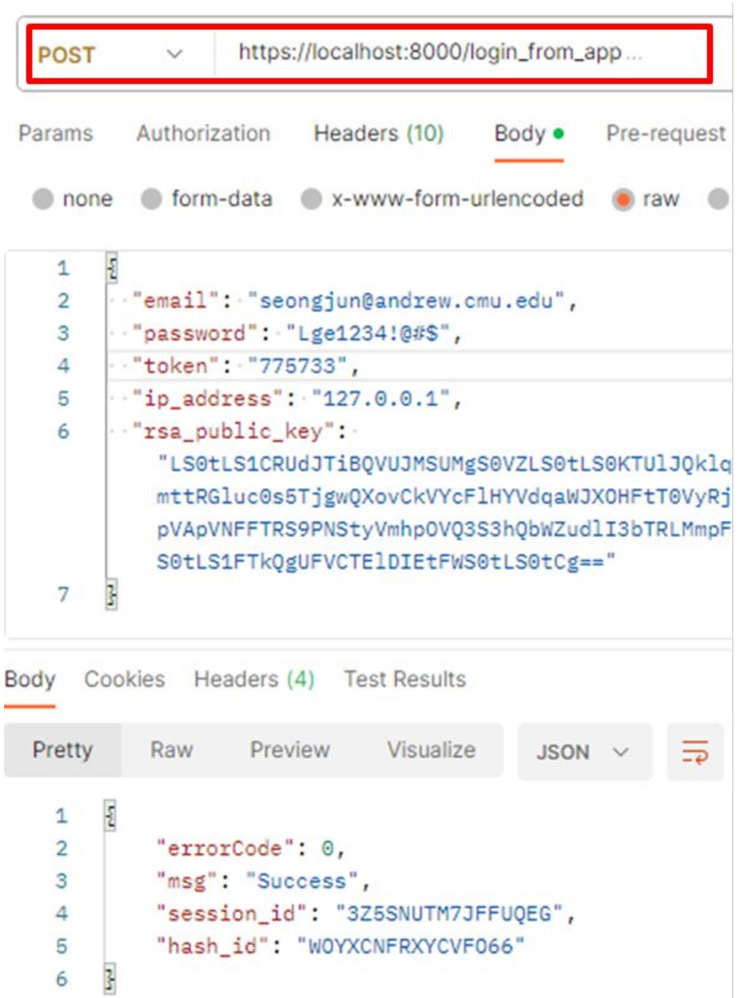
openapi.json

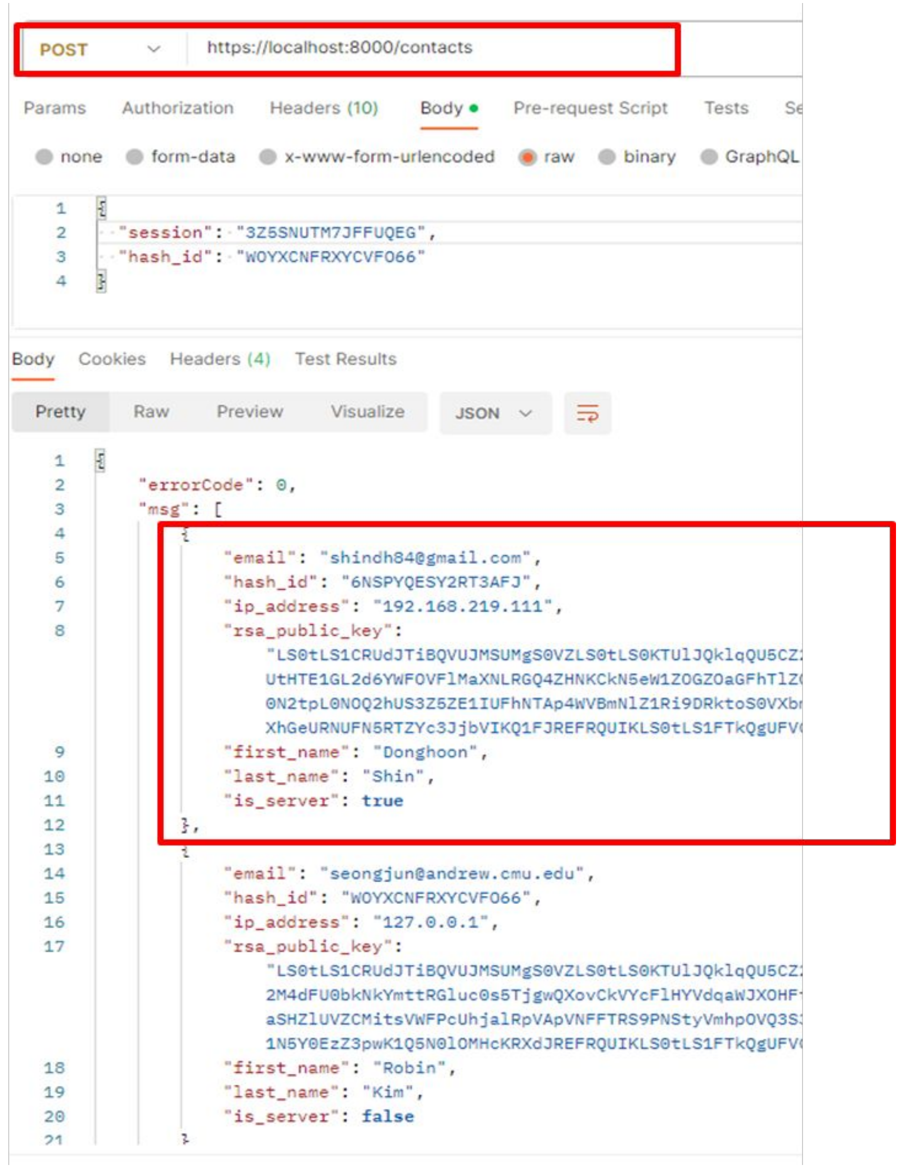
{"openapi":"3.0.2","info":{"title":"LG Secu Team 1 - Login Server","version":"1.0.0"},"paths":{"/signup/":{"get":{"tags":["users-
webapp"],"summary":"Register","operationId":"register_signup__get","responses":{"200":{"description":"Successful
Response","content":{"application/json":{"schema":{}}}}}},"post":{"tags":["users-
webapp"],"summary":"Register","operationId":"register_signup__post","responses":{"200":{"description":"Successful
Response","content":{"application/json":{"schema":{}}}}}}},"/qrcode":{"get":{"tags":["users-
webapp"],"summary":"Register","operationId":"register_qrcode_get","parameters":[{"required":true,"schema":{"title":"Email"},"name":"email","in":"query"}],"responses"
:{"200":{"description":"Successful Response","content":{"application/json":{"schema":{}}}},"422":{"description":"Validation
Error","content":{"application/json":{"schema":{"$ref":"#/components/schemas/HTTPValidationError"}}}}}}}},"/login/":{"get":{"tags":["auth-
webapp"],"summary":"Login","operationId":"login_login__get","responses":{"200":{"description":"Successful
Response","content":{"application/json":{"schema":{}}}}}},"post":{"tags":["auth-
webapp"],"summary":"Login","operationId":"login_login__post","responses":{"200":{"description":"Successful
Response","content":{"application/json":{"schema":{}}}}}}},"/login_from_app":{"post":{"tags":["auth-webapp"],"summary":"Login From
App","operationId":"login_from_app_login_from_app_post","requestBody":{"content":{"application/json":{"schema":{"$ref":"#/components/schemas/AppLoginData"}}},
"required":true},"responses":{"200":{"description":"Successful Response","content":{"application/json":{"schema":{}}}},"422":{"description":"Validation
Error","content":{"application/json":{"schema":{"$ref":"#/components/schemas/HTTPValidationError"}}}}}}}},"/contacts":{"get":{"tags":["auth-webapp"],"summary":"Get
Contacts","operationId":"get_contacts_contacts_get","parameters":[{"required":true,"schema":{"title":"Hash
Id"},"name":"hash_id","in":"query"},{"required":true,"schema":{"title":"Session Id"},"name":"session_id","in":"query"}],"responses":{"200":{"description":"Successful
Response","content":{"application/json":{"schema":{}}}},"422":{"description":"Validation
Error","content":{"application/json":{"schema":{"$ref":"#/components/schemas/HTTPValidationError"}}}}}}},"post":{"tags":["auth-webapp"],"summary":"Get
Contacts","operationId":"get_contacts_contacts_post","requestBody":{"content":{"application/json":{"schema":{"$ref":"#/components/schemas/AppSessionData"}}},"re
quired":true},"responses":{"200":{"description":"Successful Response","content":{"application/json":{"schema":{}}}},"422":{"description":"Validation
Error","content":{"application/json":{"schema":{"$ref":"#/components/schemas/HTTPValidationError"}}}}}}}},"/set_server":{"post":{"tags":["auth-
webapp"],"summary":"Turn On Server

Appendix-4) DIRB(3)



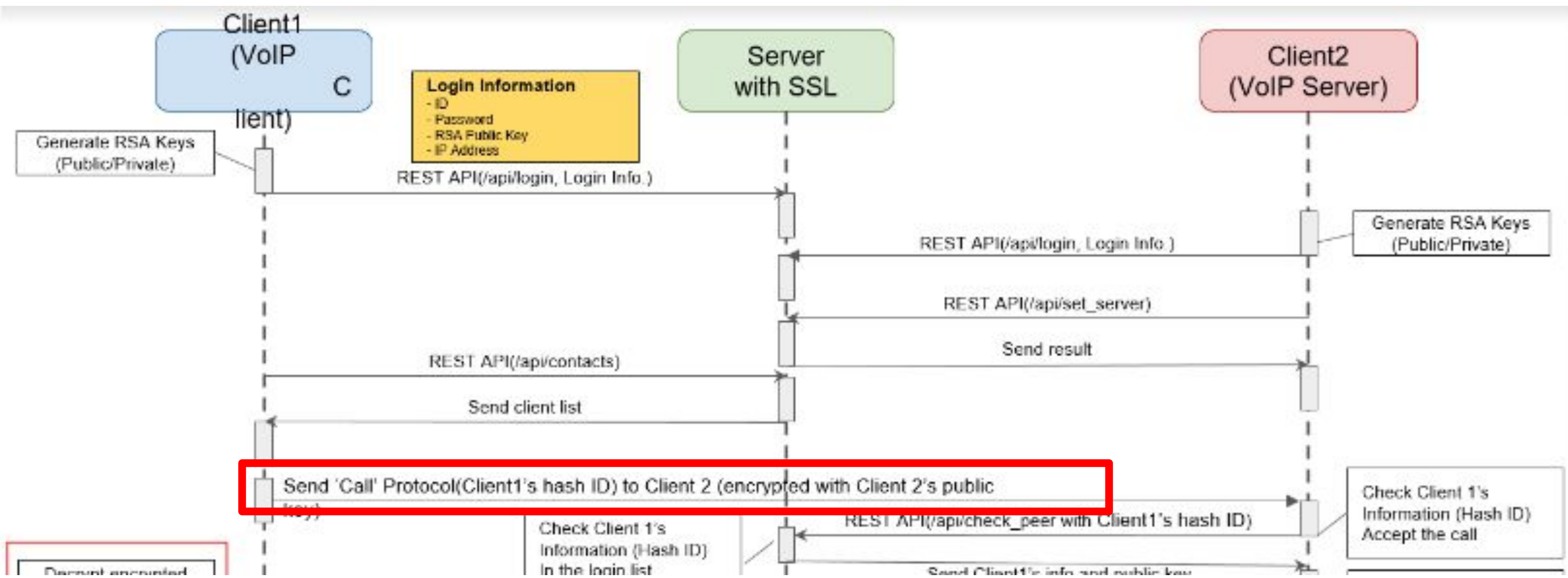
Appendix-5) Information Disclosure(Postman) - Exploit





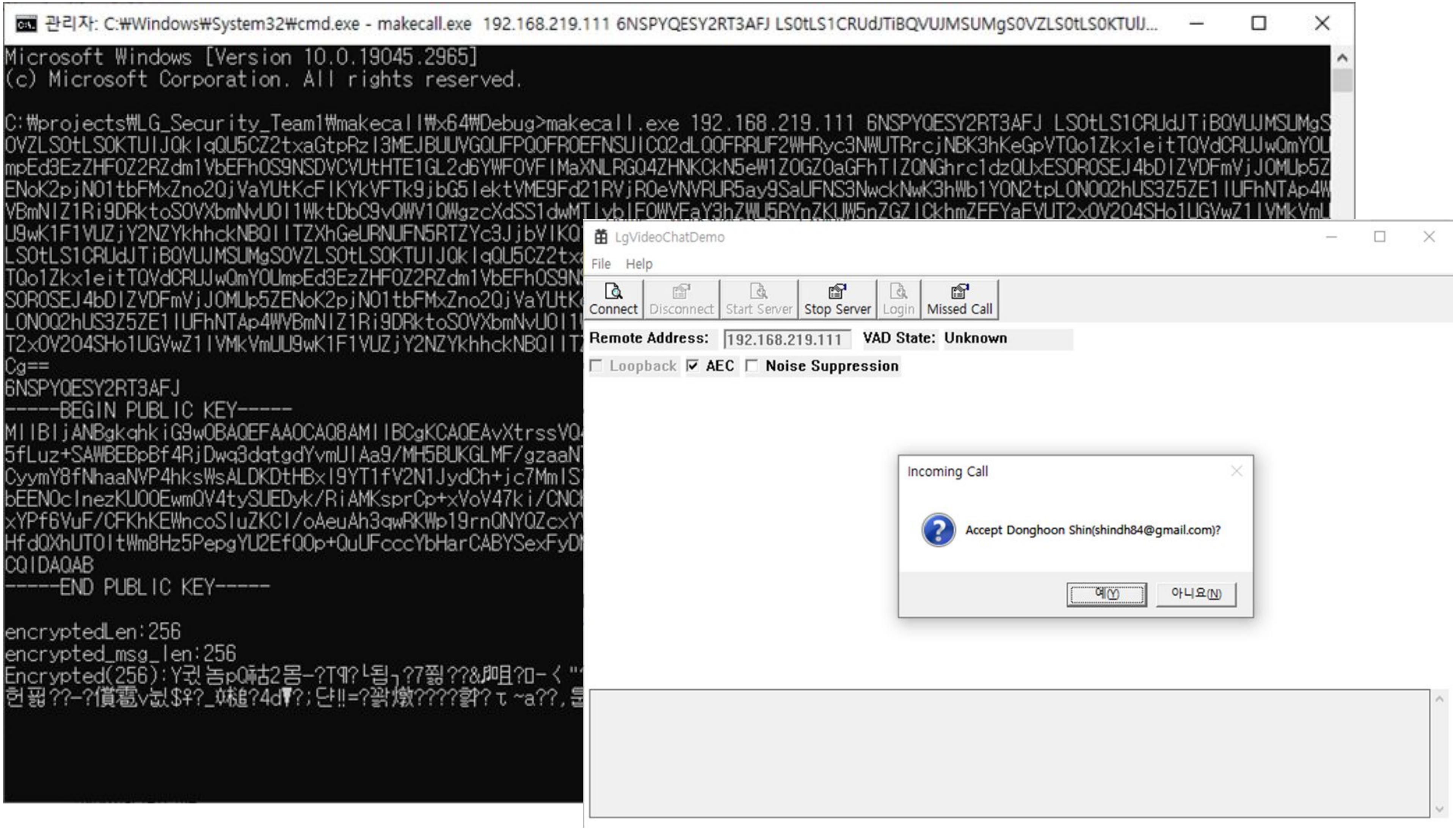
Appendix-6) Spoofing - Vulnerability

We can pretend to be someone else on the contact list with hash_id and rsa_public_key and make a call



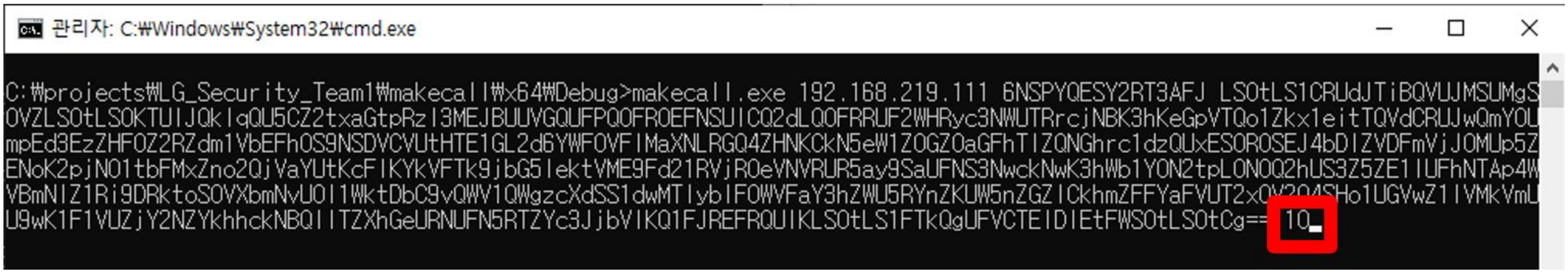
Appendix-7) Spoofing - Exploit

Exploit with hash_id and rsa_public_key for making a call

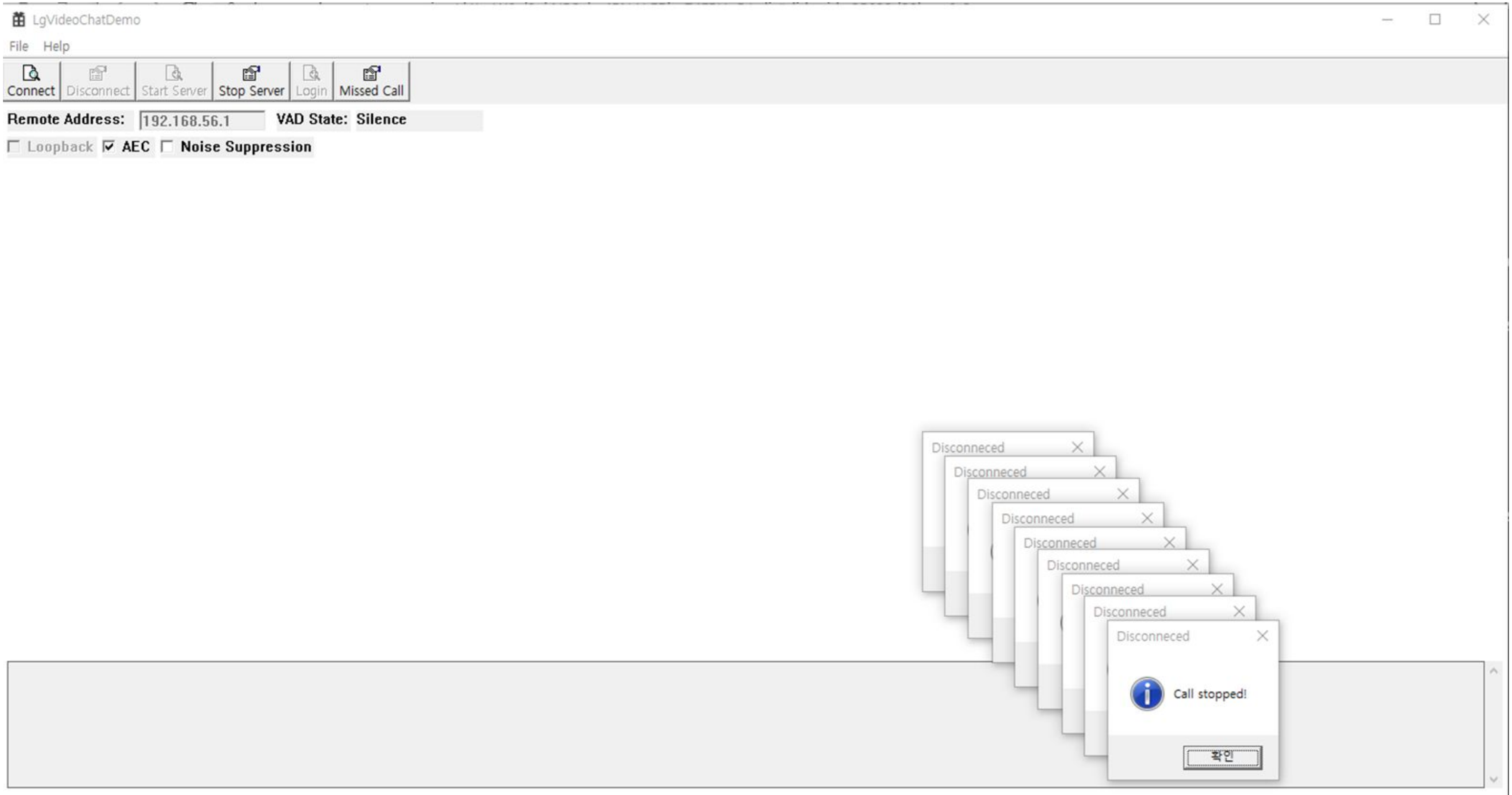


Appendix-8) Denial of Service - Vulnerability

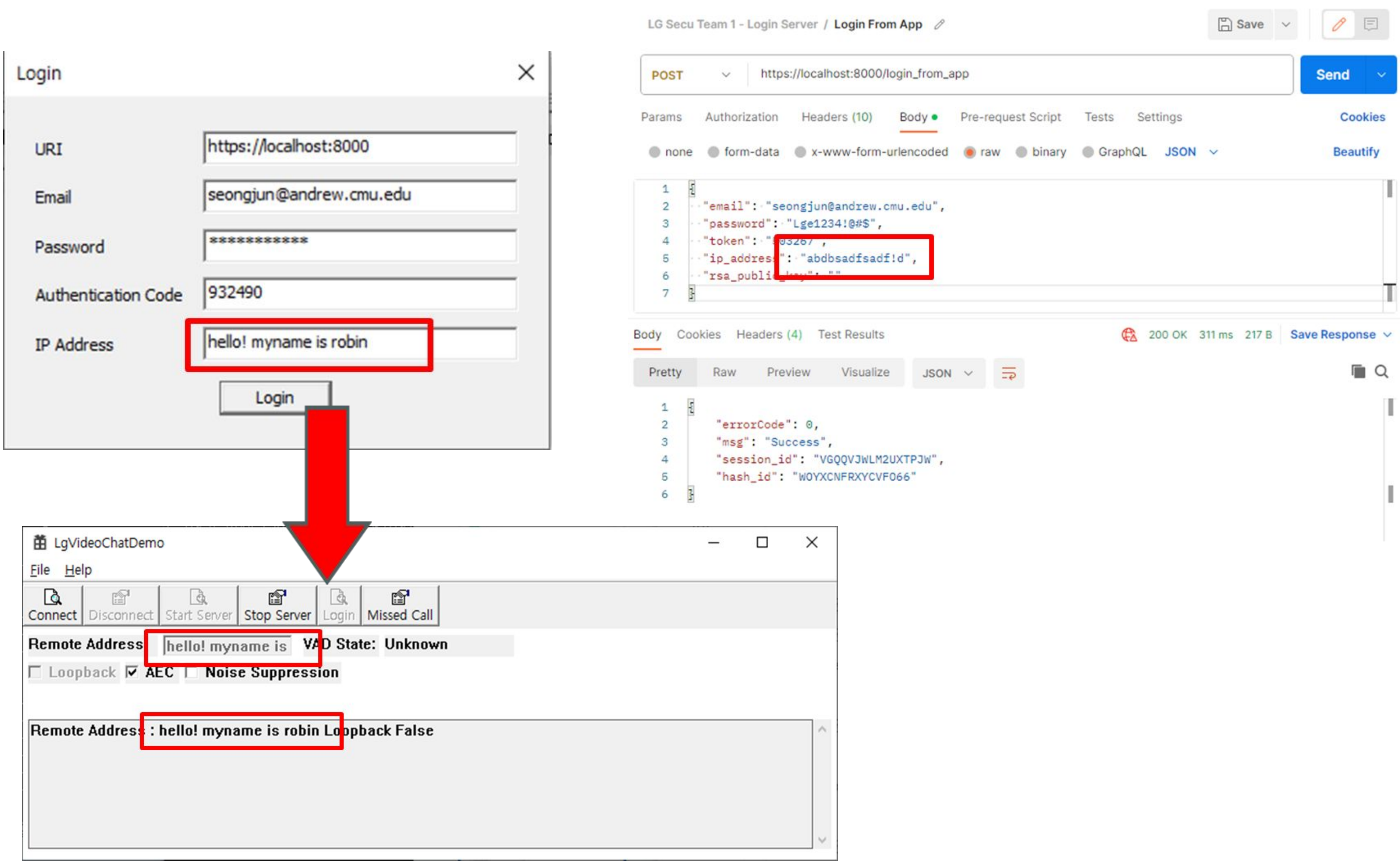
Exploit with hash_id and rsa_public_key for making a call
Last option is count and if we keep make a call, app invoke notice popup infinitely



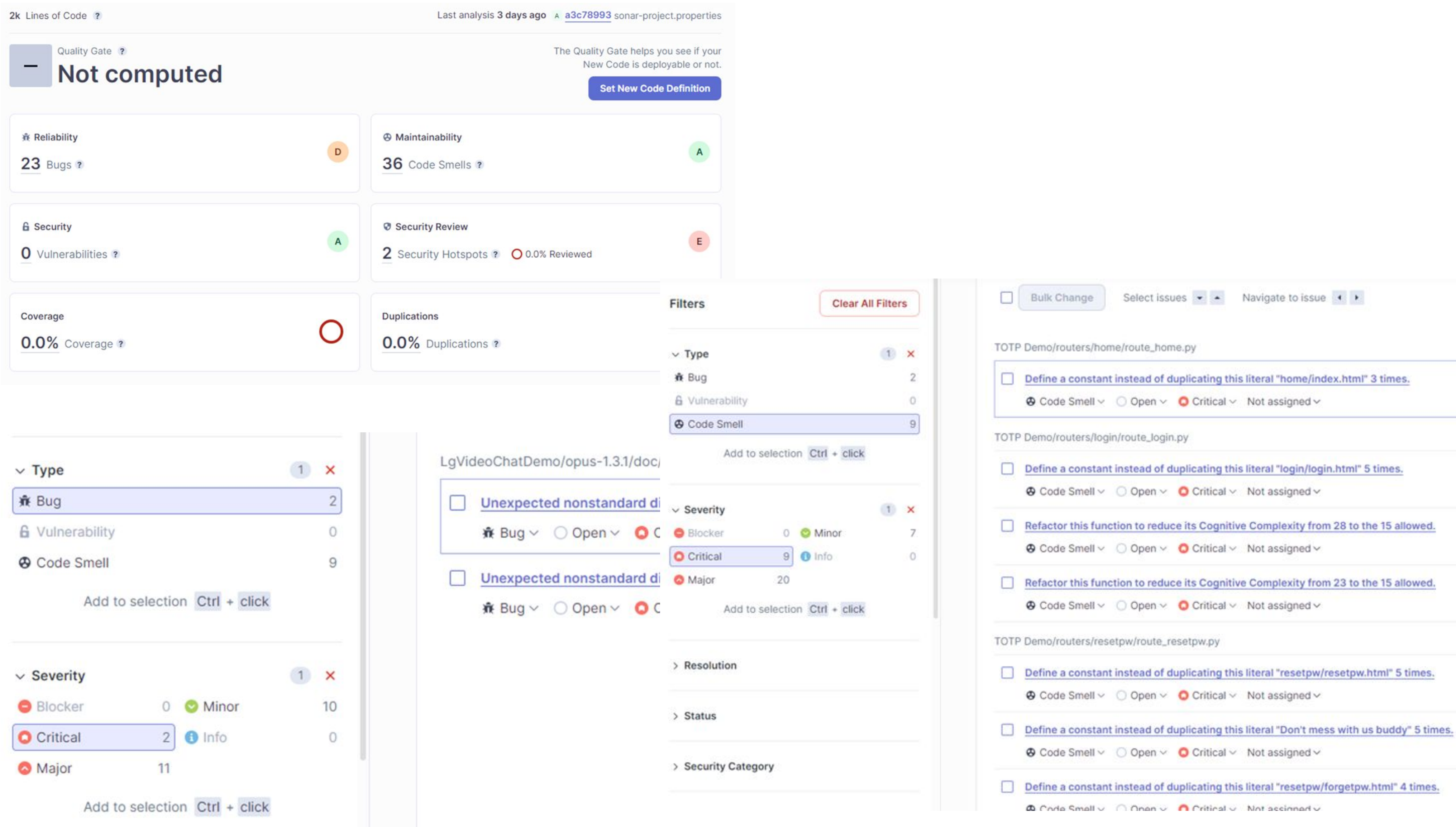
Appendix-9) Denial of Service - Exploit



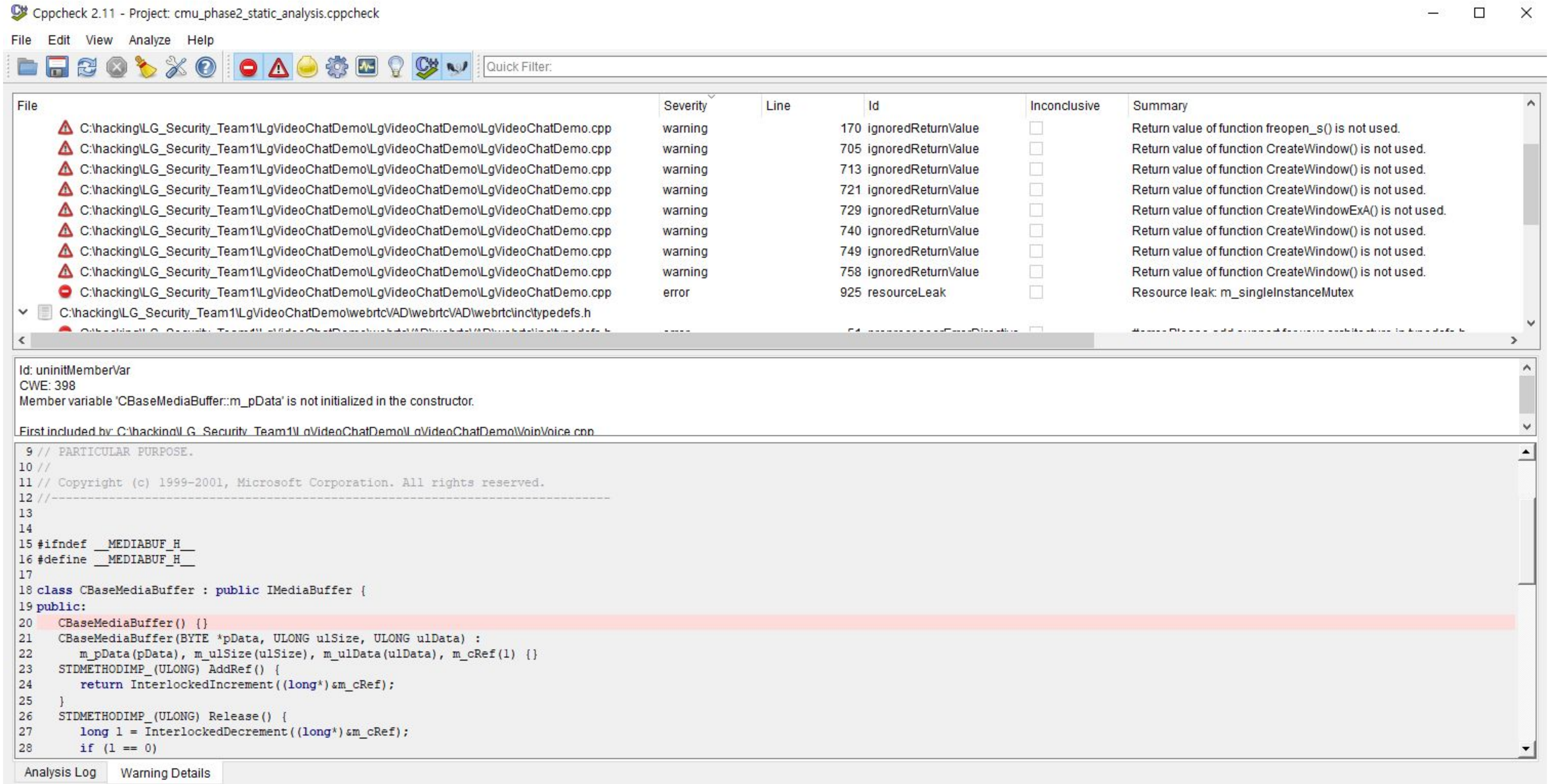
Appendix-10) Input Validation



Appendix-11) Code Review- Server



Appendix-12) Code Review- Client



Appendix-13) Code Review(OpenCV - CWEs)

8 CWEs

id	severity	msg	verbose	sinceDate	cwe	file0
integerOverflow	error	Signed integer overflow for expression &#0	Signed integer overflow for expression '(	M/d/yyyy	190	C:/hacking/LG_Security_Team1/LgVideo
integerOverflow	error	Signed integer overflow for expression &#0	Signed integer overflow for expression '(	M/d/yyyy	190	C:/hacking/LG_Security_Team1/LgVideo
nullPointer	error	Null pointer dereference: reinterpret_cast&lt	Null pointer dereference: reinterpret_cast<_T	M/d/yyyy	476	C:/hacking/LG_Security_Team1/LgVideo
uninitMemberVar	warning	Member variable 'UntypedMatrix::type	Member variable 'UntypedMatrix::type&	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideo
uninitMemberVar	warning	Member variable 'KNNSimpleResultSe	Member variable 'KNNSimpleResultSet::i	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideo
uninitMemberVar	warning	Member variable 'KNNSimpleResultSe	Member variable 'KNNSimpleResultSet::c	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideo
duplInheritedMember	warning	The class 'KNNRadiusUniqueResultSe	The class 'KNNRadiusUniqueResultSet&#	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideo
duplInheritedMember	warning	The class 'KNNRadiusUniqueResultSe	The class 'KNNRadiusUniqueResultSet&#	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideo
uninitvar	warning	Uninitialized variable: topind	Uninitialized variable: topind	M/d/yyyy	457	C:/hacking/LG_Security_Team1/LgVideo
uninitvar	warning	Uninitialized variable: topind	Uninitialized variable: topind	M/d/yyyy	457	C:/hacking/LG_Security_Team1/LgVideo
incorrectStringBooleanError	warning	Conversion of string literal "vectors siz	Conversion of string literal "vectors size n	M/d/yyyy	571	C:/hacking/LG_Security_Team1/LgVideo
incorrectStringBooleanError	warning	Conversion of string literal "vectors siz	Conversion of string literal "vectors size n	M/d/yyyy	571	C:/hacking/LG_Security_Team1/LgVideo
incorrectStringBooleanError	warning	Conversion of string literal "vectors siz	Conversion of string literal "vectors size n	M/d/yyyy	571	C:/hacking/LG_Security_Team1/LgVideo
incorrectStringBooleanError	warning	Conversion of string literal "vectors siz	Conversion of string literal "vectors size n	M/d/yyyy	571	C:/hacking/LG_Security_Team1/LgVideo
operatorEqVarError	warning	Member variable 'KMeansDistanceCo	Member variable 'KMeansDistanceComp	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideo
operatorEqVarError	warning	Member variable 'KMeansDistanceCo	Member variable 'KMeansDistanceComp	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideo
operatorEqVarError	warning	Member variable 'KMeansDistanceCo	Member variable 'KMeansDistanceComp	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideo
operatorEqVarError	warning	Member variable 'KMeansDistanceCo	Member variable 'KMeansDistanceComp	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideo
uninitvar	error	Uninitialized variable: centers_length	Uninitialized variable: centers_length	M/d/yyyy	457	C:/hacking/LG_Security_Team1/LgVideo
uninitvar	error	Uninitialized variable: centers_length	Uninitialized variable: centers_length	M/d/yyyy	457	C:/hacking/LG_Security_Team1/LgVideo
uninitMemberVar	warning	Member variable 'LshTable < unsig	Member variable 'LshTable < unsigned	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideo
uninitMemberVar	warning	Member variable 'LshTable < unsig	Member variable 'LshTable < unsigned	M/d/yyyy	398	C:/hacking/LG_Security_Team1/LgVideo
uninitvar	error	Uninitialized variable: stats.bucket_size_std_d	Uninitialized variable: stats.bucket_size_std_dev	M/d/yyyy	457	C:/hacking/LG_Security_Team1/LgVideo

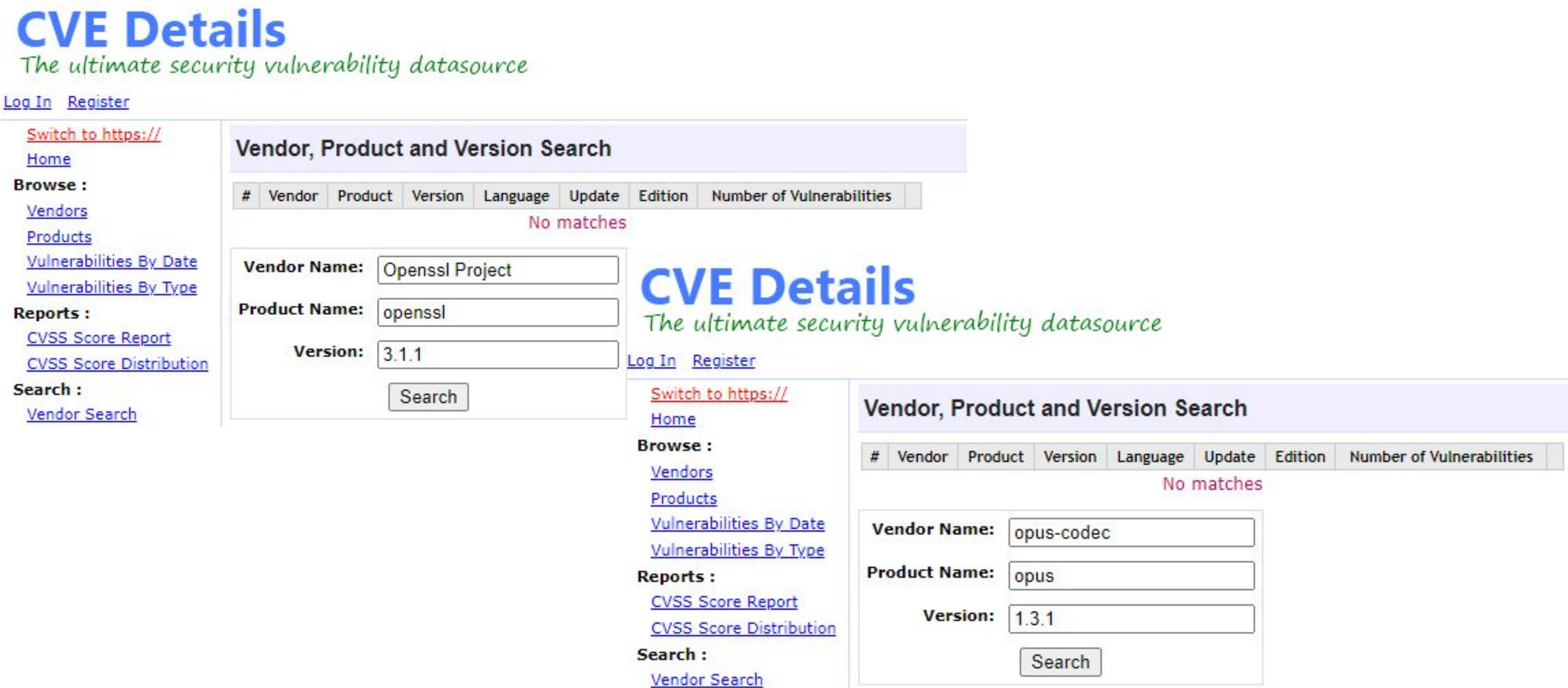
Sheet1

2150개 중 68개의 레코드가 있습니다. 평균: 371.5223881 개수: 68 합계: 24892

Appendix-14) Research Vulnerability DB

https://www.cvedetails.com

There's no vulnerability



Appendix-15) Dependency-check

There's no vulnerability

DEPENDENCY-CHECK

Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes a
analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the ana

How to read the report | Suppressing false positives | Getting Help: github issues

Sponsor

Project: .

Scan Information (show less):

- *dependency-check version*: 8.2.1
- *Report Generated On*: Tue, 4 Jul 2023 10:18:18 +0900
- *Dependencies Scanned*: 54 (44 unique)
- *Vulnerable Dependencies*: 0
- *Vulnerabilities Found*: 0
- *Vulnerabilities Suppressed*: 0
- *NVD CVE Checked*: 2023-07-04T10:17:59
- *NVD CVE Modified*: 2023-07-04T09:00:02
- *VersionCheckOn*: 2023-06-12T15:21:01
- *kev.checked*: 1688397902

Summary

Display: Showing Vulnerable Dependencies (click to show all)

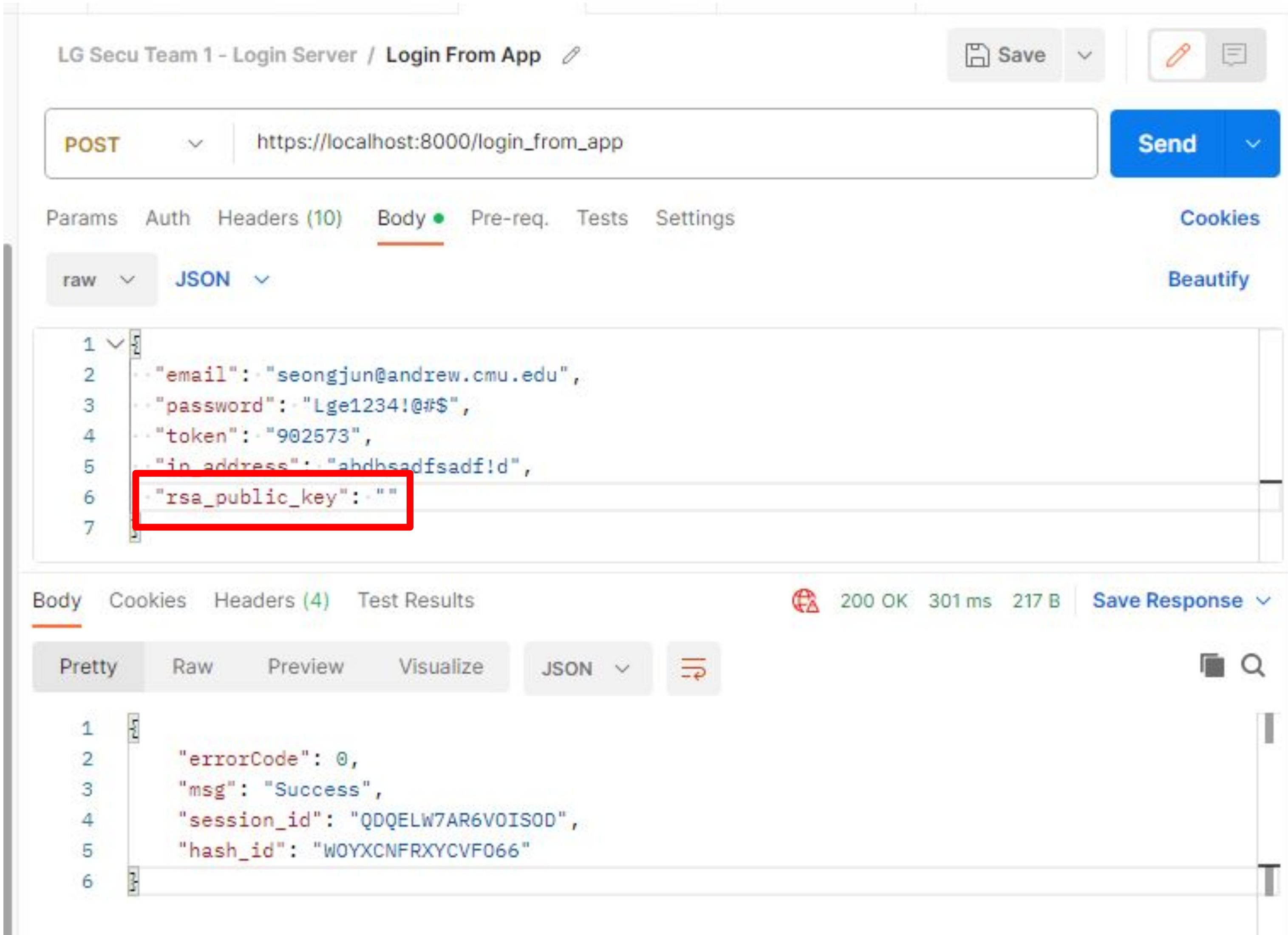
Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count

Dependencies

Attack Scenario (idea)

Appendix-16) Attack scenario

Login success with blank rsa_public_key -> Bob can send not encrypted AES key(?)
Not sure if we can get AES key which is not encrypted



Appendix-17) Client Side attack

test checksec : CFG/RFG disable → ROP Possibile (???)

```
D:₩pg₩c++>winchecksec.exe LgVideoChatDemo.exe C:₩Windows₩notepad.exe
Warn: large load config, probably contains undocumented fields
Results for: LgVideoChatDemo.exe
Dynamic Base      : "Present"
ASLR              : "Present"
High Entropy VA   : "Present"
Force Integrity   : "NotPresent"
Isolation         : "Present"
NX                : "Present"
SEH               : "Present"
CFG               : "NotPresent"
RFG               : "NotPresent"
SafeSEH           : "NotApplicable"
GS                : "Present"
Authenticode      : "NotPresent"
.NET              : "NotPresent"
CET Compatible    : "NotPresent"
```

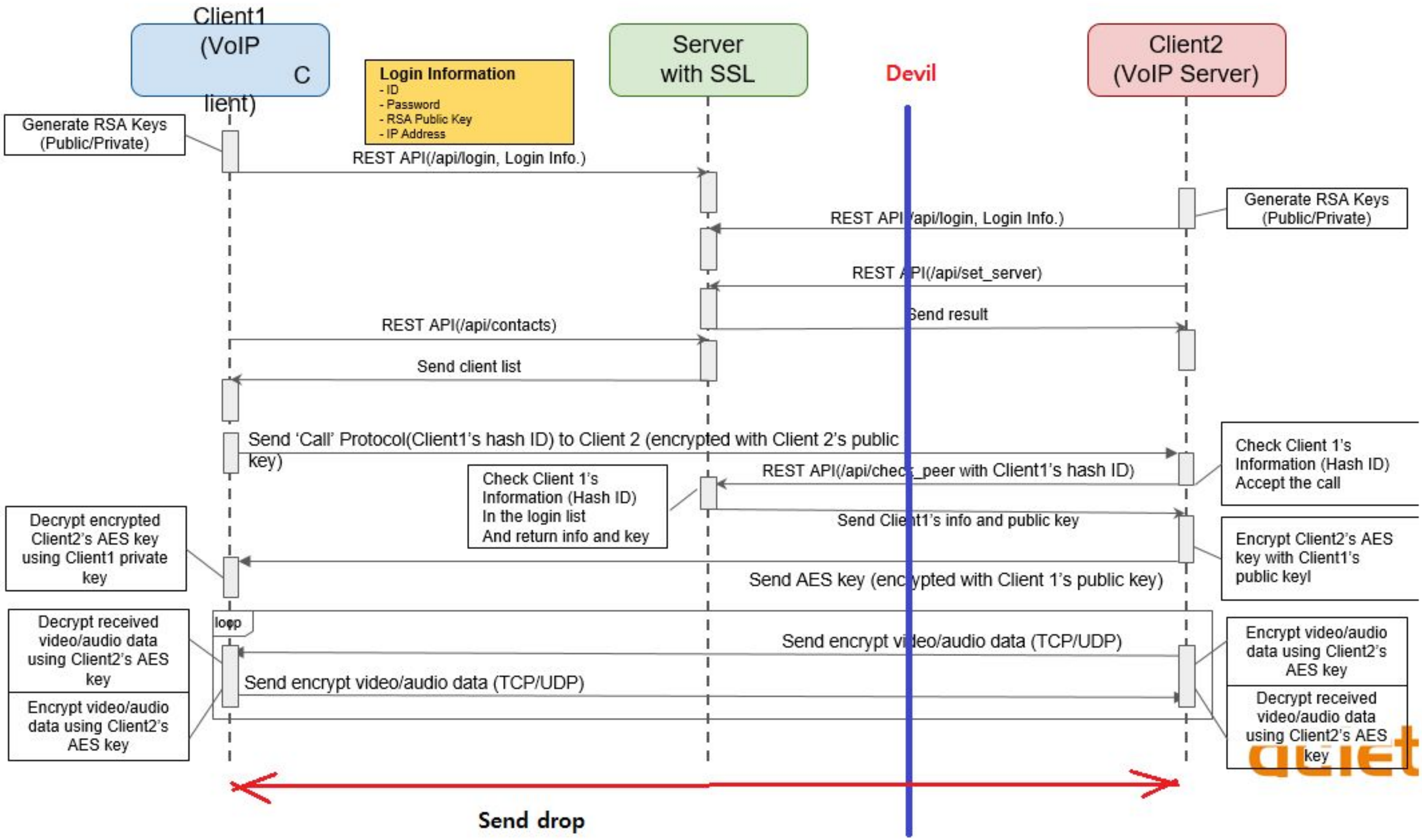
Scenario 1 :

1. OpenCV within project source has some critical vulnerabilities (integer overflow, NULL dereference, use of uninitialized variable)
2. code injection using step1's vulnerability
3. the shell code is to send private key or AES to attacker's server.
4. the attacker be able to sniff Video call using the victim's AES key

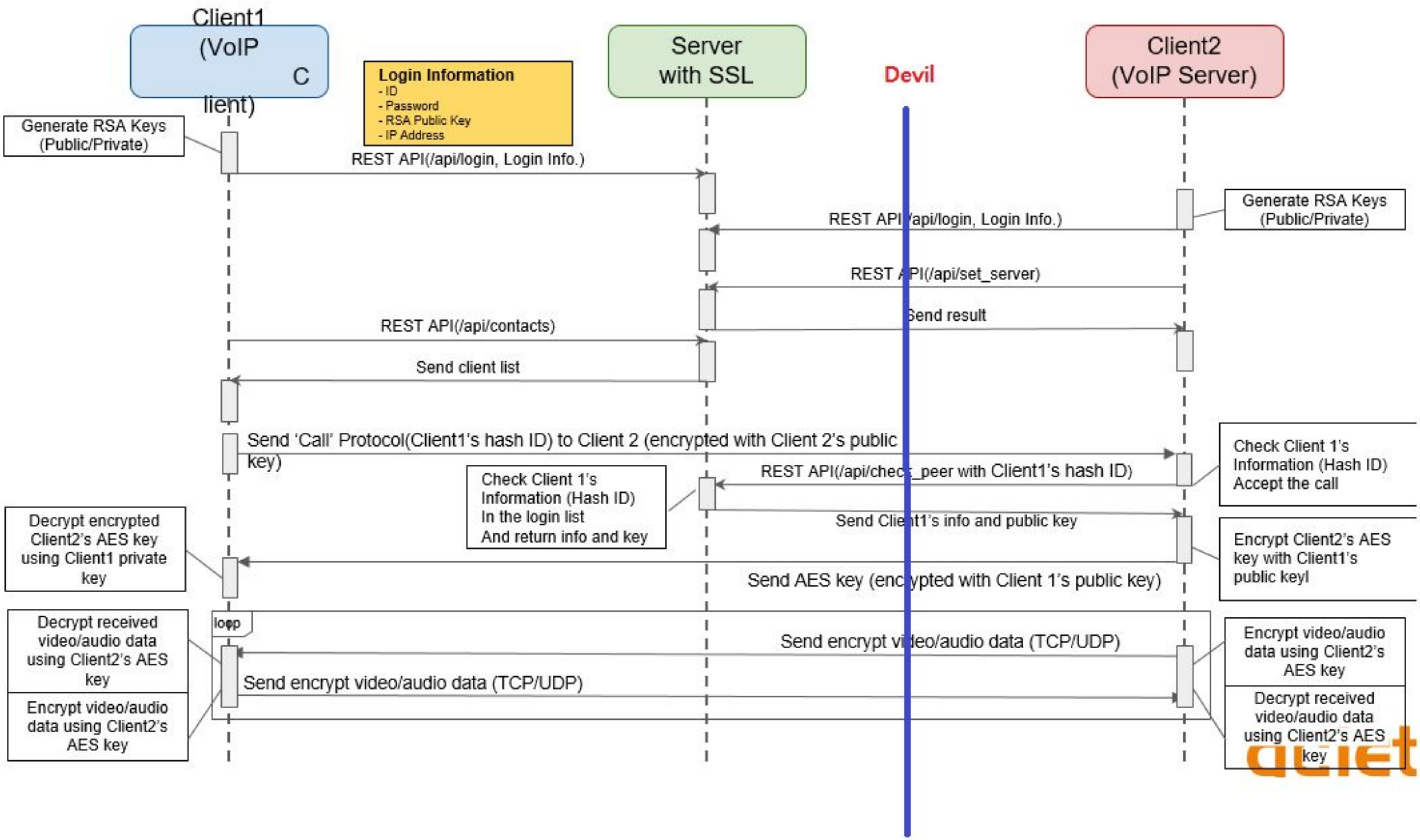
Scenario 2:

1. OpenCV within project source has some critical vulnerabilities (integer overflow, NULL dereference, use of uninitialized variable)
2. code injection using step1's vulnerability
3. the shell code is to exploit the client's host system (ex.. to execute powershell with privilege mode)

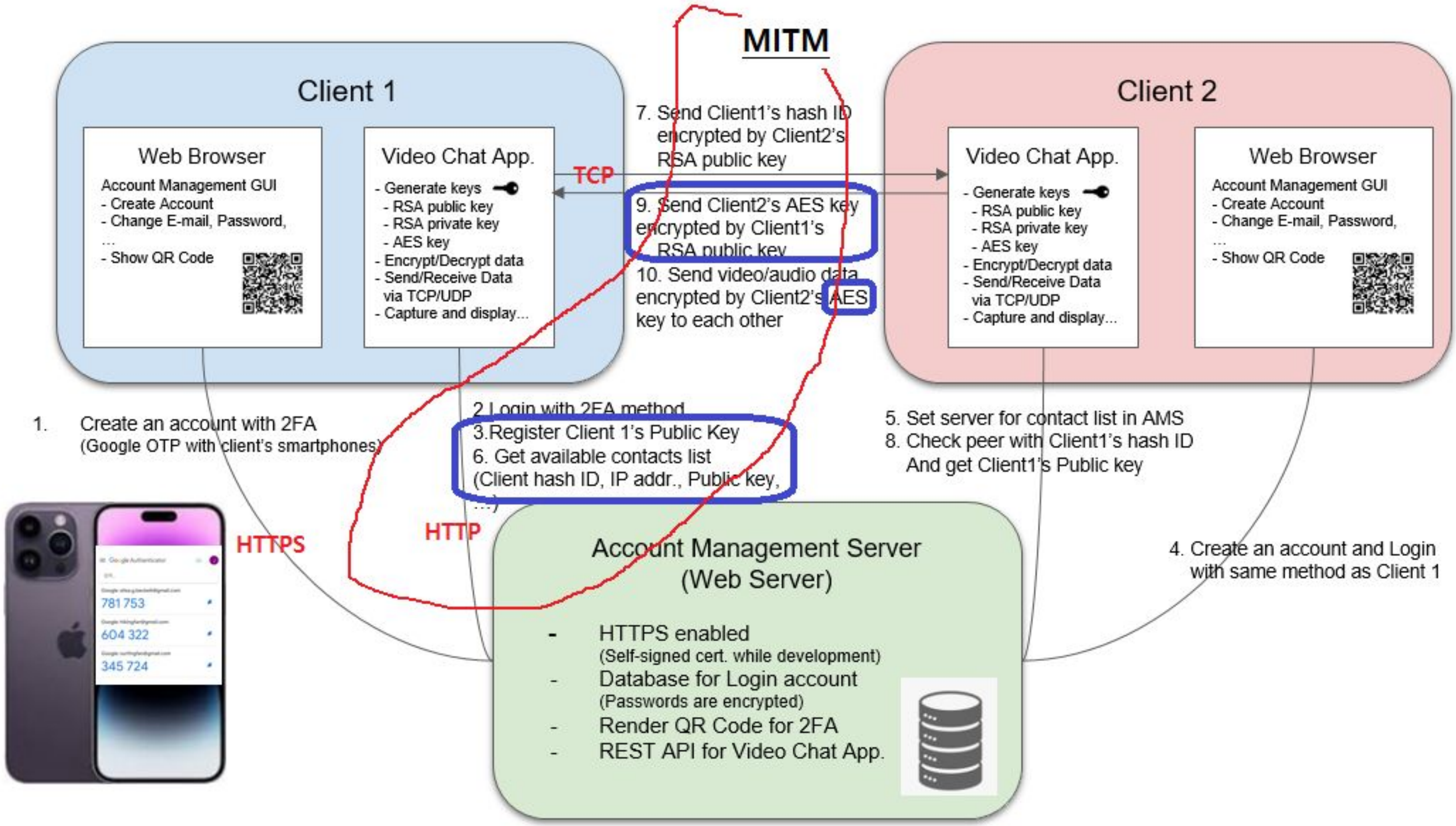
Appendix-18) Unwanted Call Drop via MITM or spoofing



Appendix-19) Sniffing video call via MITM(1)



Appendix-20) Sniffing video call via MITM(2)



IF Protocol HTTPS, HTTP, TCP more check needed!!

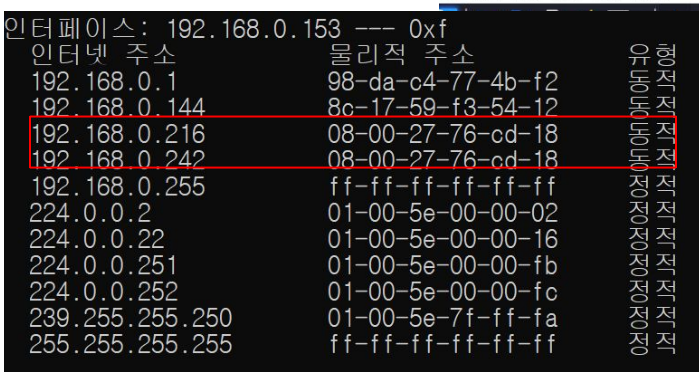
Appendix-21) ARP Spoofing

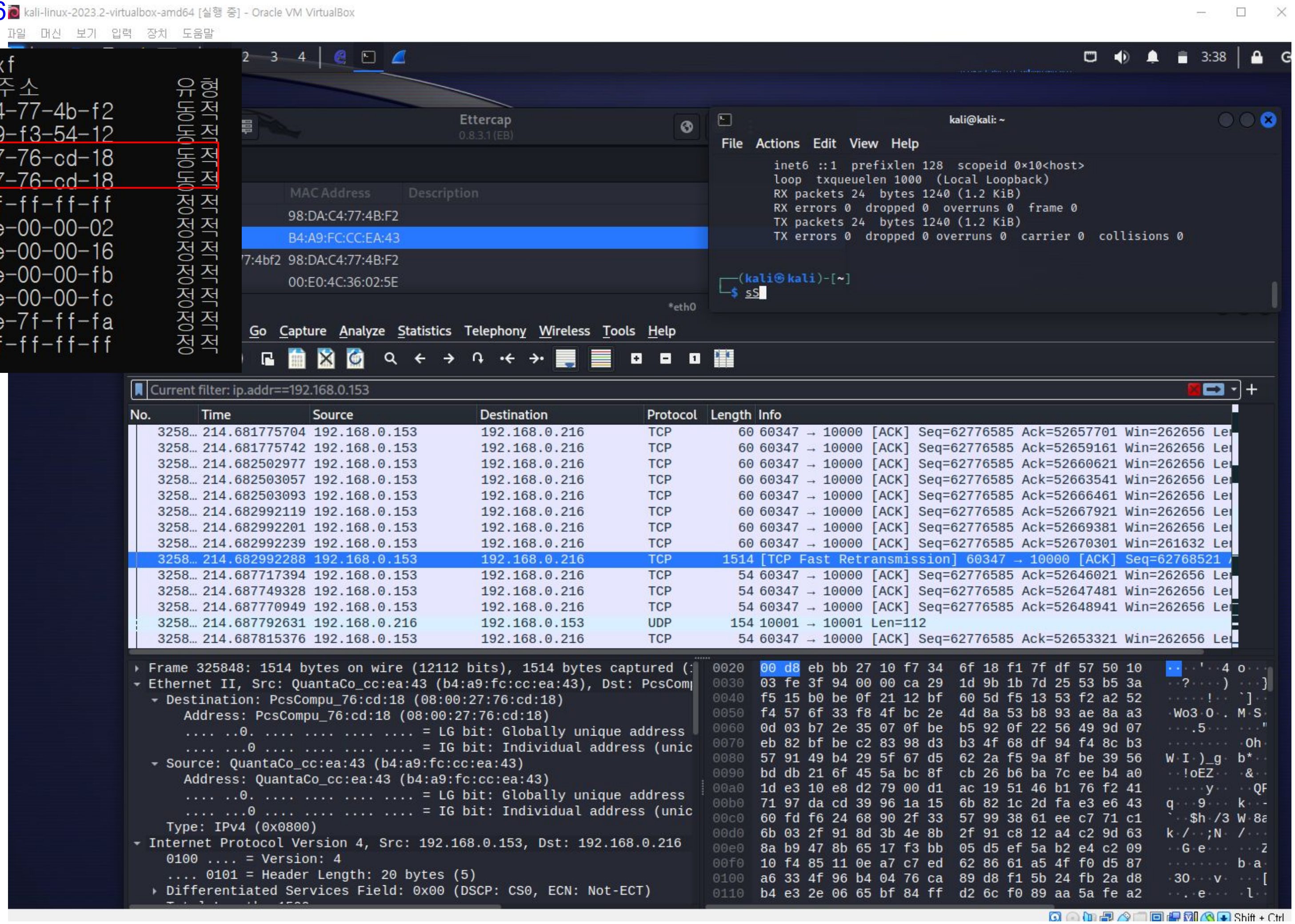
Attacker changed target's arp table

- Attacker : 192.168.0.242
- Target 1: 192.168.0.153
- Target 2: 192.168.0.216

Attacker try to sniff packets

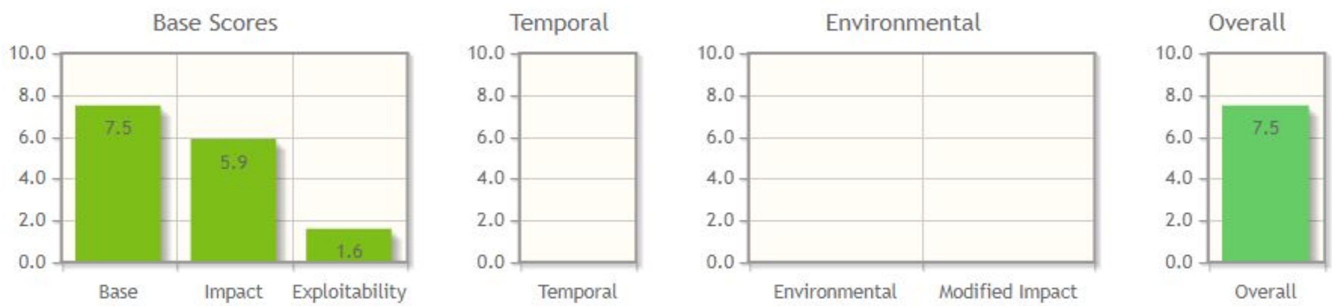
- Target 1: 192.168.0.153 <-> Target 2: 192.168.0.216





Appendix-22) Common Vulnerability Scoring System

Vulnerability :If hash_id and public key is known, it is possible to make fake call.



CVSS Base Score: 7.5
Impact Subscore: 5.9
Exploitability Subscore: 1.6
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 7.5

Show Equations

CVSS v3.1 Vector
AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*
Low (AC:L) | **High (AC:H)**

Privileges Required (PR)*
None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*
None (UI:N) | **Required (UI:R)**

Scope (S)*
Unchanged (S:U) | Changed (S:C)

Impact Metrics

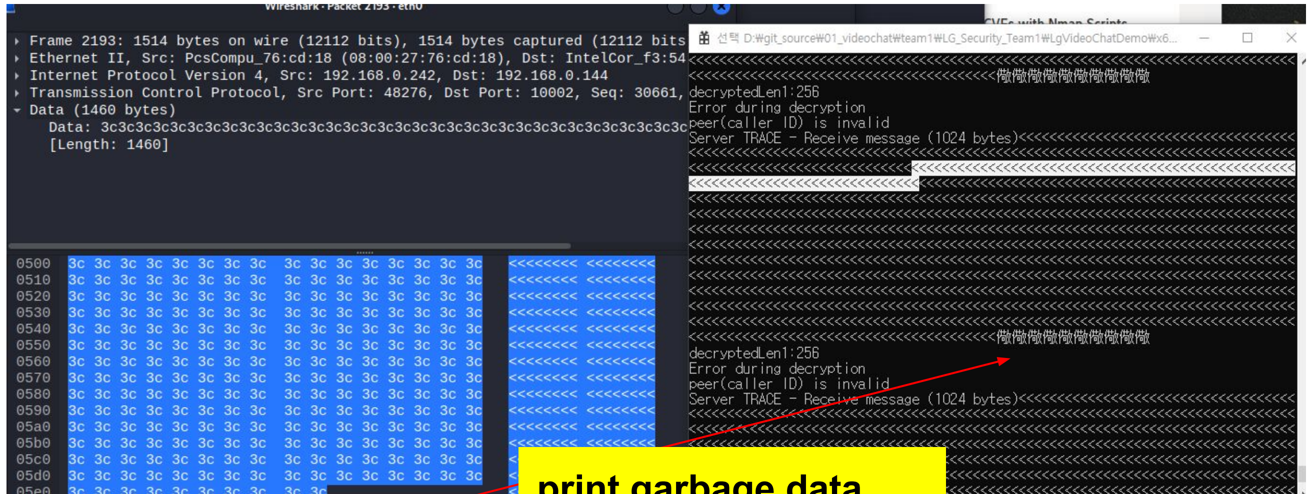
Confidentiality Impact (C)*
None (C:N) | Low (C:L) | **High (C:H)**

Integrity Impact (I)*
None (I:N) | Low (I:L) | **High (I:H)**

Availability Impact (A)*
None (A:N) | Low (A:L) | **High (A:H)**

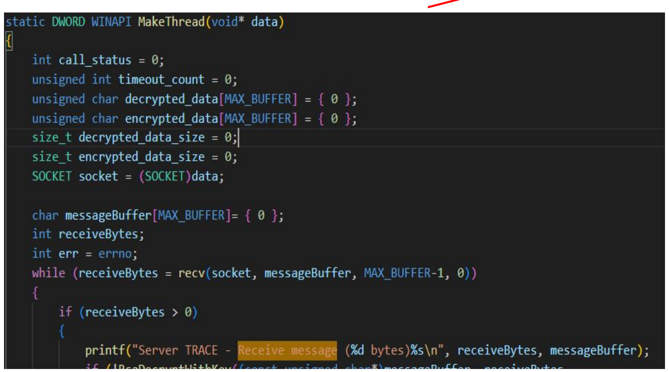
- https://www.first.org/cvss/specification-document
- https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Appendix-23) SPIKE Fuzzing



print garbage data

mesageBuffer is not NULL terminated



Recommend:
messageBuffer initialization
Change receive size