

# Cookie Parser by Using Network Hacking

쿠키 인증을 통한 로그인 세션 가로채기



CCIT 최종 발표회  
정보보안 S/W 융합  
장한빈

# 목차

- Cookie 란?
- Web Site의 Cookie 인증 방식
- Web Site의 취약점
- 취약점을 이용한 Cookie Parser 만들기
- 개선방안
- 향후계획
- Q&A

Cookie 란?

# Cookie 란?

- HTTP
  - HTTP는 Stateless 한 Protocol 로 Session이 끊어지면 현재 연결된 Login 정보 등을 상실
- Cookie
  - 따라서, HTTP 통신에서 로그인 정보 등을 저장하기 위해 사용되는 것이 Cookie로 인터넷 통신시 Cookie라는 특정한 값이 전송되어 특정한 사용자로 인증 되는 방식

# Web Site의 Cookie 인증 방식



The image shows a screenshot of the Naver login page. At the top, the word "NAVER" is displayed in a large, bold, blue font. Below the logo, there are two input fields: the first contains the text "espoir\_noa09" and the second contains ten black dots representing a password. A large blue button with the text "로그인" (Login) is positioned below the password field. At the bottom of the form, there are several options: a checked checkbox for "로그인 상태 유지" (Keep login state), "IP보안 OFF" (IP Security OFF), and a link for "일회용 로그인" (One-time login) with a question mark icon. A yellow warning box at the very bottom contains the text "개인정보 보호를 위해 개인 PC에서만 사용하세요. [도움말보기](#)" (For personal information protection, use only on a personal PC. [View help](#)).

# Web Site의 Cookie 인증 방식

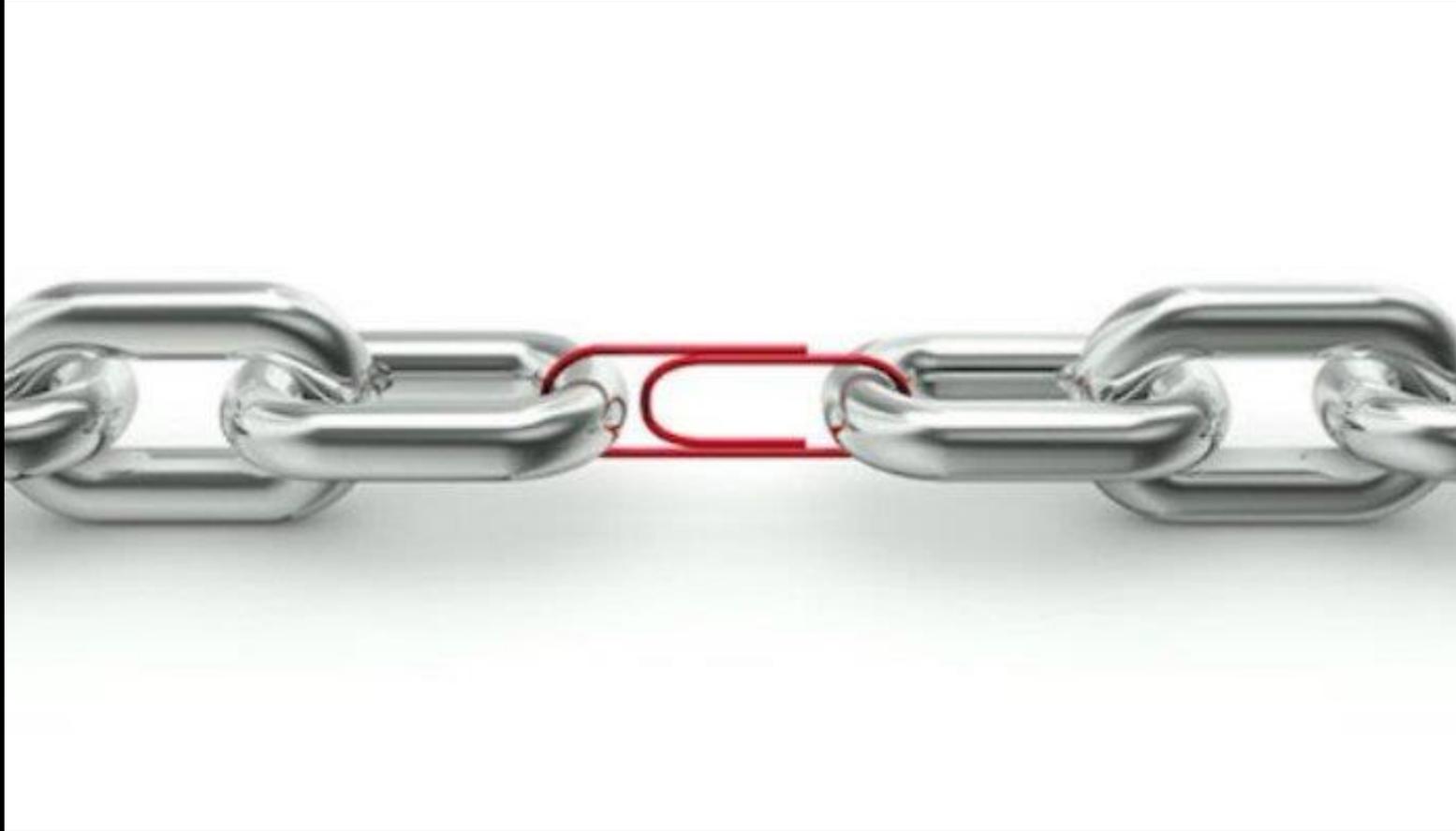
# Web Site의 Cookie 인증 방식

```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: ko-KR
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: www.naver.com
Connection: Keep-Alive
Cookie: NM_THEMECAST_NEW=tcc_bty%2Ctcc_fod%2Ctcc_lif; PM_CK_latestPanelDate=20170921; PM_CK_readNewPanel=ANIMAL%3BWEDDING%3BITTECH;
npic=7jff4tm4TLbQNIIm4EwTkP4DP/BG42oB2LY4tuWjjWrPdEavNLZNXLIg4kpE/nkrHCA==; NNB=DHOZCXYSVKEVO; ASID=b761a18c000001593ba61e3900000052;
_ga=GA1.2.1414891810.1493977526; nx_ssl=2; nid_inf=-785374642; NID_AUT=3Drr0UntMnlme5iN2rfQYcYCowZ8Xk/o2d+G9gUD49JJOLor8E7wIqkbez1onDJU;
NID_SES=AAABfKeJYiFArFJ7hFKq3MhIoB1PJC+uFm7IiRE3kCgwGJ539XGc41K/3UbM8vjgSvPzxaEutixn3Hj+hyq8y5JzYfnKrtcabwYOTY/1wFV5+2o9a9ehLnFLi
+vNZDuMMswCtWkVuc2nw6rzY325xAUOZJmNEMDcGaq1sqCxbSAtsvd1e1z0twIa7A8/11Jc2yBmI/qLMcpIs0g3sR1NsnDS+yTk1FuYr7NmQb61CFIszLIIn12Hh/BD196RocPUEJQ
+H4hq4XfS0fTm0Qmu9r-fBXV9n7gv1twSVEW5Mh5hkDXF7QGCfzHXIKgL827a0CKUqhpQdmlCKvwLGUS5D07eftTMD3Vzt93DtEfKZ5xA49XviZdDm270ikjY0xuiA5DhFGcFecWafS77xqB1izeJ06CvmvE
gGA6tgh0z0kjAkSmb1HQTEfDAQjH9NgC8u9YXCxsX/z5Idu5MJPCizKvt1YR5NdP1BilKUqCqSDVhe00h+F/e+dw0wi/cn4TPcHPKVw==
```

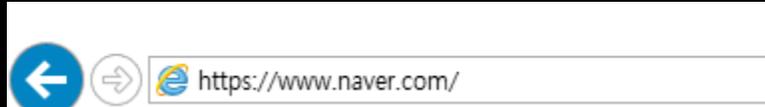
```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: ko-KR
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: daum.net
Connection: Keep-Alive
Cookie: TIARA=yt2jsGzABC1xsDpLnIb5XmwiW3E2mstYRBjNmiY7yzsli.V9SkYBSYc8Nyi_1hM_6MZmaG14XkITp_tvu3EG-5lpybn207cE;
webid=yJxkclrTZndMoaxJ007s7jpZipHEjo2Fv0CwaDsPrDBfCRWe0azmTpmc3jd4QI/X; webid_sync=1511058237138; AGEN=I4a95Q1G0bCDL1AwkjrNP4AaXJKnDGrrI9bpiM_lmMk;
SLEVEL=1; TS=1511058245; HTS=KUG1z.6xOPSjY3U5IwZ8bg00; HM_CU=58LJ6M8HDxA; PROF=0603012032024064024120UiQPJk7X-6w0mlxoempuaa-
JbjP0ym1sUo0a8X8AUpy.KuZP3z7wE12W4..NYhR74w00LYSA9A1_cGNLCyhCzrw0gyiAbNDcmXx31Vb26yxIdFExAQ9BjPTVjje18Lmp9GFfIauQ1o80TLnHHY.bHDTw005.D3F1Q7ttIGSDMyc2OZQZI
t5MtQdMNgRwKqd_7J.HUt61QfwCuqFc8f.._DCEM20D8V-.8.En9Aas1ATS5nrw_ToEHgBeukyAk8MXUQj3qhrIYsAISFQ00; LSID=d04d663b-a860-48db-8f34-b705bdacfbcb21511058245493
```

Web Site의 취약점

# 취약점



# Web Site의 취약점(일반 접속시)



```
.....Z9:.8..C....ng.)::\U*.4....z.....&.,+.0./.$#.(.'
.....=<.5./
...2.....
www.naver.com.....
.....
.....#..~.^."r.....p!D..J...iy..w.-..1.....7..{3....^..m..W.....}.c.[Uw.....~/..=...7.L.o.!.....g>...mCv.
...}.A.c.W.<.oMYp.C.x.f.N.+6...7p...
.B...$.../D(..k.^..o.b9.zLs...HW .x.m.....(.....h2.http/1.1.....
.....J...F...|.&.dd.B....%...Z!S.j...../.....#.....h2.....10...-0.....B...w.E.o.*...70
.....*..H..
.....0..1.0.....U....GB1.0...U...Greater Manchester1.0...U...Salford1.0...U.
..COMODO CA Limited1<0:...U...3COMODO RSA Organization Validation Secure Server CA0..
17041200000Z.
190501235959Z0...1.0.....U....KR1.0...U....135611.0...U...Gyeonggi-do1.0...U...Seongnam-si1#0!..U. ..6, Buljeong-ro, Bundang-gu1.0...U.
..NAVER Corp.1"0 ..U...Information Security Team1@0>..U...7Hosted by Korea Information Certificate Authority, Inc.1.0...U...SGC SSL
Wildcard1.0...U...*.www.naver.com0.."0
.....*..H..
.....0..
.....QR.OX.....vBp&.5.2YE.....=..C-...%...H0.7..0/\%hN+.lu.U....MD6..^..tD..f..7..r(.cJ;.TeGYgK.$.;
.H....d4z..B..7:.....^..G.2...M..x.&.....1....J=Z&|].....*...<WT.F.....H9.....B.....6h>z.....>...tDO....3.7...R;..#.:]_ze.'....d... =
%.....0...0...U.#.0.....+...0./.*HH*...B.$0...U.....C...t.X..P... ..H..0...U.....0...U.....0.0...U.%..0...+.....+.....0P..U.
.I0G0;..+.....1.....0+0)..+.....https://secure.comodo.com/CPS0...g.....0Z.U...S0Q00.M.K.Ihttp://crl.comodoca.com/
COMODORSAAOrganizationValidationSecureServerCA.crl0...+.....0}0U...+.....0..Ihttp://crt.comodoca.com/
COMODORSAAOrganizationValidationSecureServerCA.crt0$.+.....0..http://ocsp.comodoca.com0)..U..."0 ..*.www.naver.com.
www.naver.com0
.....*..H..
.....7..v.....3.....$...]-sz.....II,*......RL~3...3.B...r2s.o....dJ....v..$G'.soK.+d....].,eJ=..0..V(=7...Pu...R...wsW?].
G...J...e.W<3E...$+..L4.....NB5...d|.1..N.A...}.c.8d...~k...<..!x...{"%.....Z...[.#.GT\...-.....^.....GVon.a
.....0...0.....6.^.....~.sk.<0
```

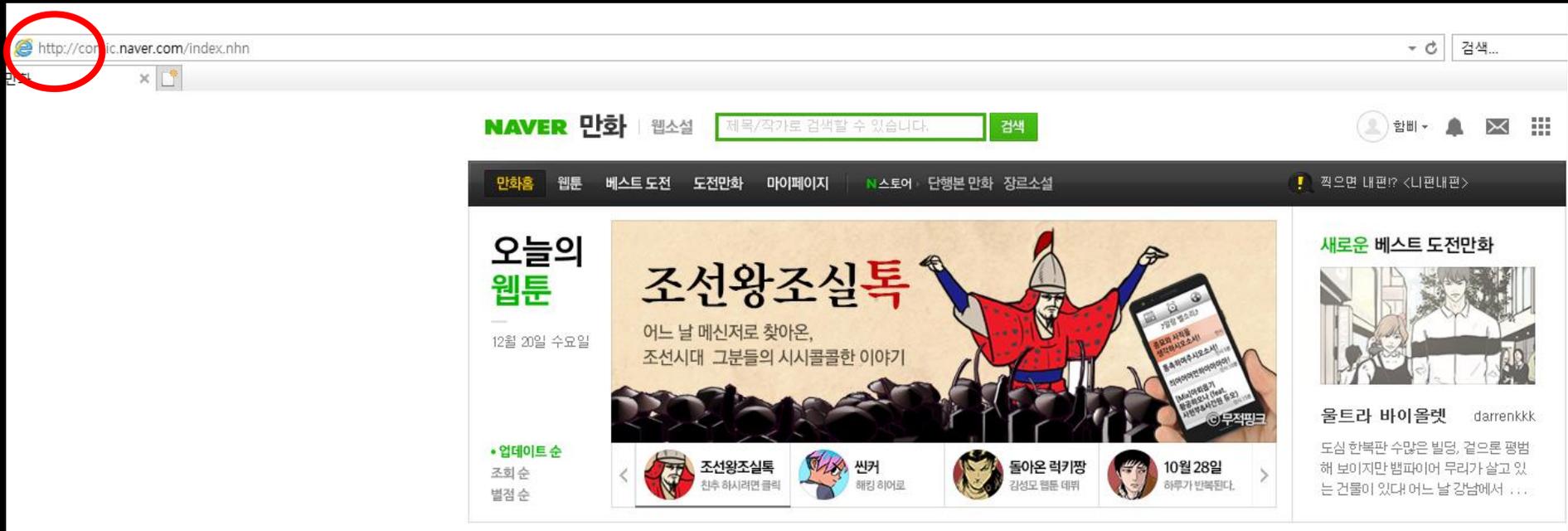
# Web Site의 취약점(일반 접속시)

- 코드가 암호화 되어 통신

```
a4 5a fc 2e 01 bb f8 cd 44 0e a1 dc 1f ca 50 18 .Z..... D.....P.
04 00 75 11 00 00 17 03 03 01 2b 00 00 00 00 00 ..u..... ..+.....
00 00 02 72 2c 0c 37 6d 37 54 90 c4 c4 a8 4b 4c ...r,..7m 7T....KL
87 17 d3 da d1 4d c4 4a 74 a5 90 d2 81 9c e7 a6 .....M.J t.....
0e 61 a8 d7 a2 81 c1 2b 92 0c 27 5e e6 08 54 7f .a.....+ ..'^..T.
4d 13 7f 20 57 77 d8 63 45 4c 85 c7 97 33 97 6d M.. Ww.c EL...3.m
78 60 ac e8 23 3f b0 18 63 72 2c ba 6f 08 56 a7 x`..#?.. cr,.o.V.
31 ff 7d 0f 52 1a e6 5d 31 60 ae 6f ef 69 eb af 1.}.R..] 1`.o.i..
57 5a c1 d0 f7 b0 76 52 d6 15 81 38 7f 96 4b 35 WZ....vR ...8..K5
4e e7 08 fe 62 9b 00 10 4d c6 32 cf a1 b4 a1 55 N...b... M.2....U
f6 75 f1 bf 1b dd 79 fd 65 21 85 45 8d 70 ab 55 .u....y. e!.E.p.U
f1 e2 d2 a5 ed 40 1d 2c 12 33 d3 08 12 13 89 56 .....@., .3.....V
77 9a b5 d7 91 29 da d3 62 a8 bb 0f 85 b2 39 c4 w....).. b.....9.
c0 a1 a1 67 d7 f6 6f 4a 12 9f e0 c9 33 e3 4a 50 ...g..oJ ....3.JP
a7 70 12 46 54 c5 c5 b2 89 40 f3 b2 a9 55 7e 9c .p.FT... .@...U~.
a7 05 32 46 33 f0 45 ff 68 3b 35 3d a4 74 aa 68 ..2F3.E. h;5=.t.h
94 94 04 d5 a5 41 13 ed bd 9f 0f 47 b9 33 1d eb .....A.. ...G.3..
8d 2b 3e fa 22 86 d7 61 b4 8c 12 66 19 c0 3e b5 .+>."..a ...f...>.
95 da 3f 9f 1c e0 c7 c8 12 26 f9 c5 00 b6 af 14 ..?..... .&.....
3f b5 68 23 77 c7 94 e8 75 8c 74 a9 1a b2 94 e5 ?.h#w... u.t.....
f2 65 8e fa a5 cf .e....
```

# Web Site의 취약점

- 네이버에서 웹툰 메뉴 클릭시(취약점)



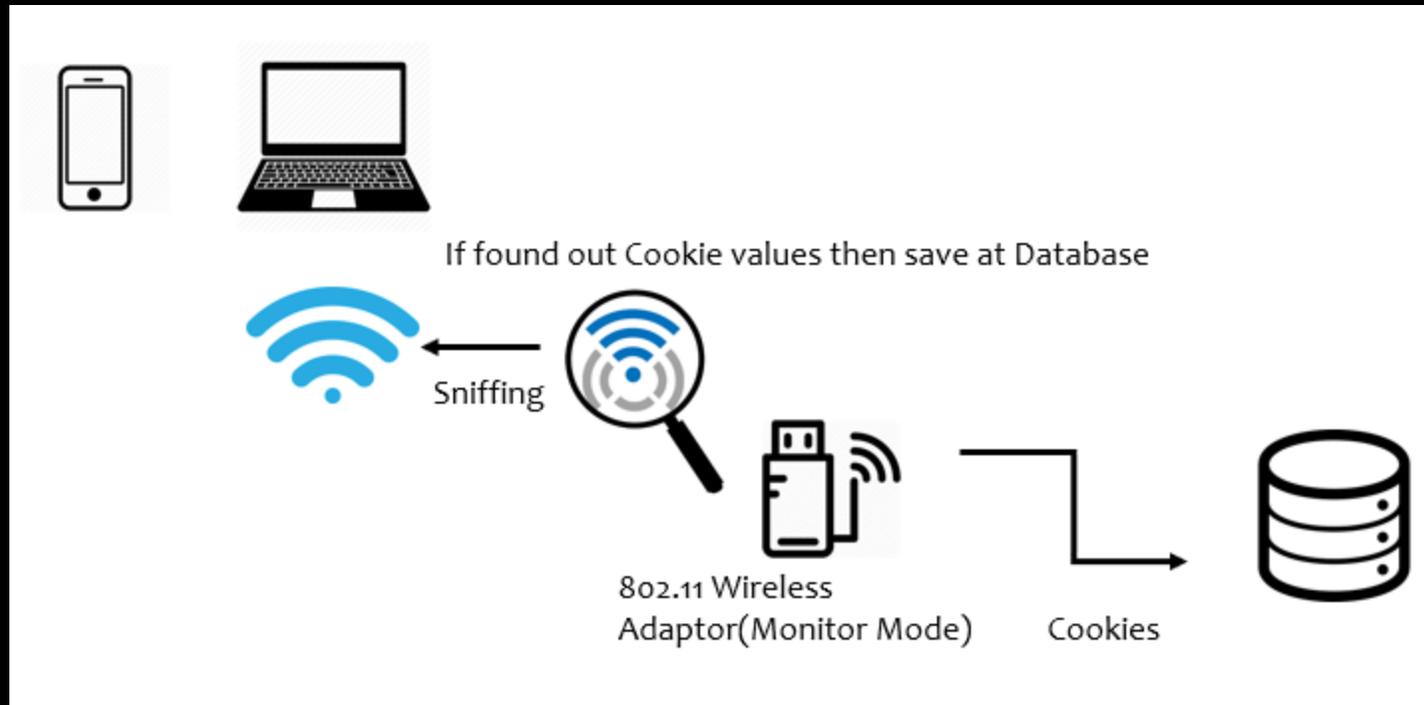
# Web Site의 취약점

- 네이버에서 웹툰 메뉴 클릭시(취약점)

```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: ko-KR
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: www.naver.com
Connection: Keep-Alive
Cookie: NM_THEMECAST_NEW=tcc_bty%2Ctcc_fod%2Ctcc_lif; PM_CK_latestPanelDate=20170921; PM_CK_readNewPanel=ANIMAL%3BWEDDING%3BITTECH;
npic=7jff4tm4TLbQNI4EwTkP4DP/BG42oB2LY4tuWjjWrPdEavNLZNXLiG4kpE/nkrHCA==; NNB=DHOZCXYSVKEVO; ASID=b761a18c000001593ba61e3900000052;
_ga=GA1.2.1414891810.1493977526; nx_ssl=2; nid_inf=-785374642; NID_AUT=3Drr0UntMnlme5iN2rfQYcYCowZ8Xk/o2d+G9gUD49JJOLor8E7wIqkbez1onDJU;
NID_SES=AAABfKeJYiFArFJ7hFKq3MhIoB1PJC+uFm7IiRE3kCgwGJ539XGc41K/3UbM8vjgSvPzxaEutixn3Hj+hyq8y5JzYfnKrtcabwYOTY/1wFV5+2o9a9ehLnFLi
+vNZDuMMswCtWKvuC2nw6rzY325xAUOZJmNEMDcGaqlsqCxbSAtsvd1e1z0twIa7A8/11Jc2yBmI/qLMcpIsOg3sRlNsnDS+yTk1FuYr7NmQb61CFIszLIIn12Hh/BD196RocPUEJQ
+H4hq44XFS0FtM0Qmu9rFBXV9n7gv1twSVEW5Mh5hkDXF7QGCfzHXIKgL827a0CKUqhpQdm1CKvwLGUS5D07eftTMD3Vzt93DtEfkZ5xA49XviZdDm270ikjY0xuiA5DhFGcFecWafS77xqB1izeJ06CvmvE
gGA6tgh0z0kjAkSmb1HQTEnFDAQjH9NgC8u9YXCxsX/z5Idu5MJPCizKvt1YR5NDP1Bi1KUqCqSDVhe00h+F/e+dwowi/cn4TPcHPKVw==
```

# 취약점을 이용한 Cookie Parser 만들기

# 동작 방식



# 프로그램 동작 화면

```
터미널
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
*****Detected AP Lists*****
1 BSSID : 90:9f:33:77:07:cc  SSID : HanBin

Choose number that add to Decrypt Info <Reload AP list : 0> : 1
Input " HanBin " Password : dorkdork
```

# 인증에 사용되는 Cookie Values

\*.naver.com

- NID\_SES
- NID\_AUT

\*.daum.net

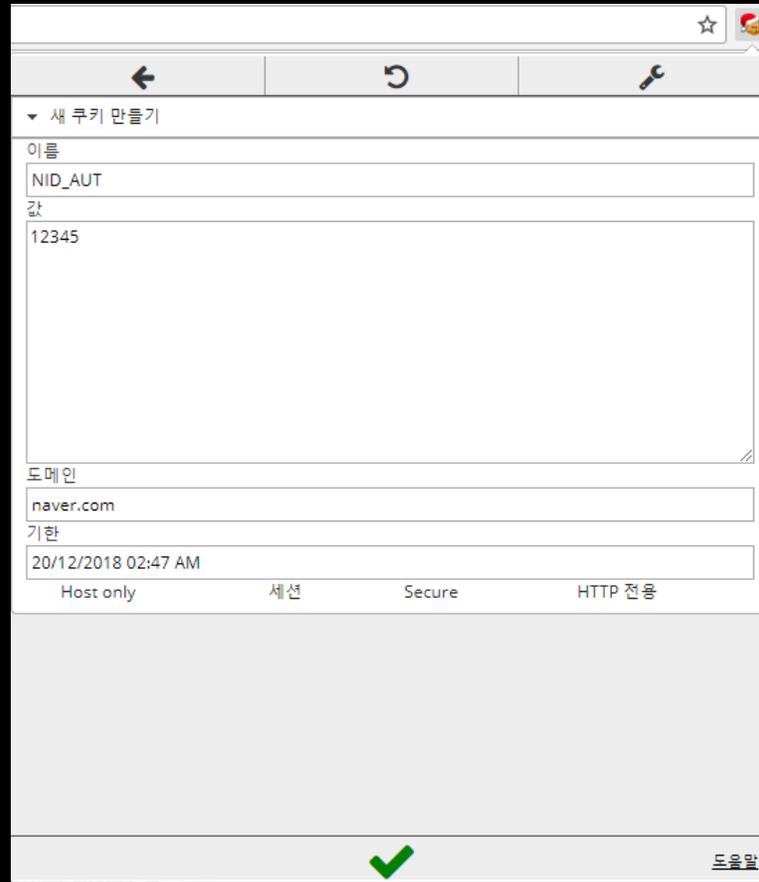
- TS
- PROF
- HTS
- HM\_CU

# 프로그램 동작 화면

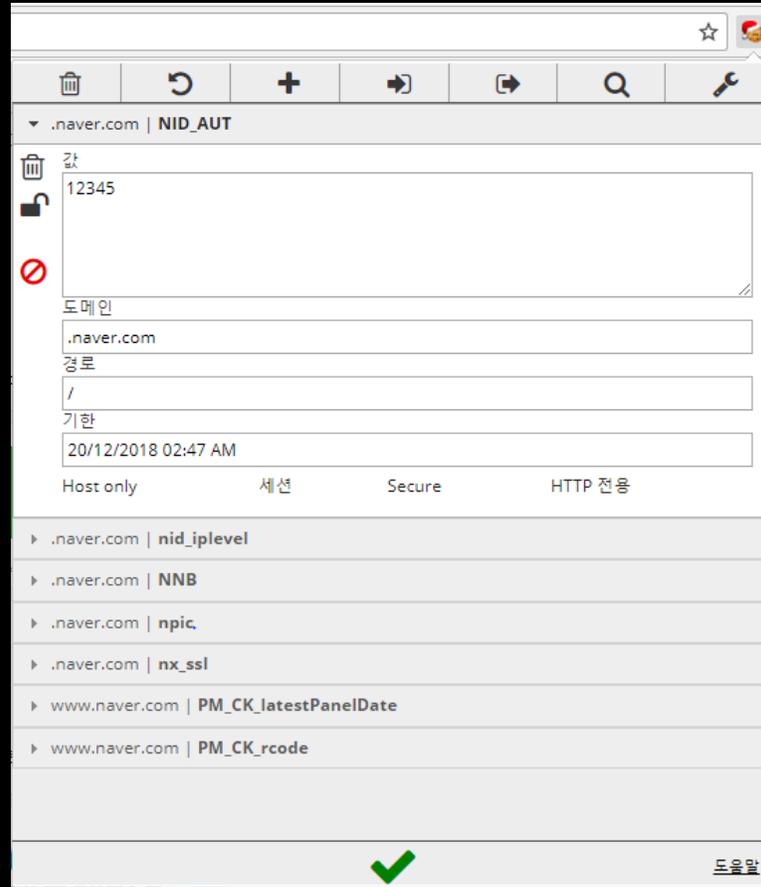
- Cookie가 탐지되면 자동으로 DB에 저장

```
root@kali: ~  
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)  
pQvodpb047YFL4GK+WpS0gW7orKPHKrjzdekd/abP; nid_inf=625166607; NID_AUT=gQ6s7qkDf7  
66TPEK5c8sIu248o+xTOKM7WTSg06YEKztENFiLU02t999Pw8K6Tq; NID_SES=AAABprVLawERAP4c  
efKHMVAfs/eFn6ml4GZJ/NNQqqUGhnf2tdUdMcm40b41JE5/qyXqzs7SmPFw/sk3e4bMW02t1MItLS6q  
L0i0V8oAa3oLTNYQCVGRiilTy0uCzLXw13S5cWl+9eB6Ne/2JRV2cBgx25kVZPpKAw31UU95y0NhVk7W  
80y6cLp+v+e2+lPYuqRnJ5fnFi/4bDPFoYluZg0alRJPArL0ygajuhl92hCJoAQm2B28x4eQGIWQLPDQ  
q0GvoyLSuNkQHXRLOFzoFiTFE78vL6qF00BXIFDcIAGDhVW5E01Bpkw1Dgz41H5lYxk2g644SKjlfIFA  
29eD1cjcMCSALJj6ru7vw7ZL11x+zF6kXeChovjC4mFvx3nk0Uyky6HOxGgnyJc1BV81Nr0+wcbeL7o  
7xnFshjko0GvnUfpmLKIQyLIkbDW8nTMwsYCq8FIqa+M/tnMrKVLuzpNgojPRT7MT0/j62i2vQwqtikk  
Jt6sVIxA1z6i4kSYWpJe35rCZxCjq+MHLX0HL4AJ40pZp9Xh+80nsBer7/BVWUfB+TQ0fR4d0aUB4kQj  
iv7tww==  
  
| lapi.live.navercorp.com | NNB=PA4SARK7FIIFU; nid_sec=rM0u2iAdBMs+Ikqjuz7TMBu  
pQvodpb047YFL4GK+WpS0gW7orKPHKrjzdekd/abP; nid_inf=625166607; NID_AUT=gQ6s7qkDf7  
66TPEK5c8sIu248o+xTOKM7WTSg06YEKztENFiLU02t999Pw8K6Tq; NID_SES=AAABprVLawERAP4c  
efKHMVAfs/eFn6ml4GZJ/NNQqqUGhnf2tdUdMcm40b41JE5/qyXqzs7SmPFw/sk3e4bMW02t1MItLS6q  
L0i0V8oAa3oLTNYQCVGRiilTy0uCzLXw13S5cWl+9eB6Ne/2JRV2cBgx25kVZPpKAw31UU95y0NhVk7W  
80y6cLp+v+e2+lPYuqRnJ5fnFi/4bDPFoYluZg0alRJPArL0ygajuhl92hCJoAQm2B28x4eQGIWQLPDQ  
q0GvoyLSuNkQHXRLOFzoFiTFE78vL6qF00BXIFDcIAGDhVW5E01Bpkw1Dgz41H5lYxk2g644SKjlfIFA  
29eD1cjcMCSALJj6ru7vw7ZL11x+zF6kXeChovjC4mFvx3nk0Uyky6HOxGgnyJc1BV81Nr0+wcbeL7o  
7xnFshjko0GvnUfpmLKIQyLIkbDW8nTMwsYCq8FIqa+M/tnMrKVLuzpNgojPRT7MT0/j62i2vQwqtikk  
Jt6sVIxA1z6i4kSYWpJe35rCZxCjq+MHLX0HL4AJ40pZp9Xh+80nsBer7/BVWUfB+TQ0fR4d0aUB4kQj  
iv7tww==
```

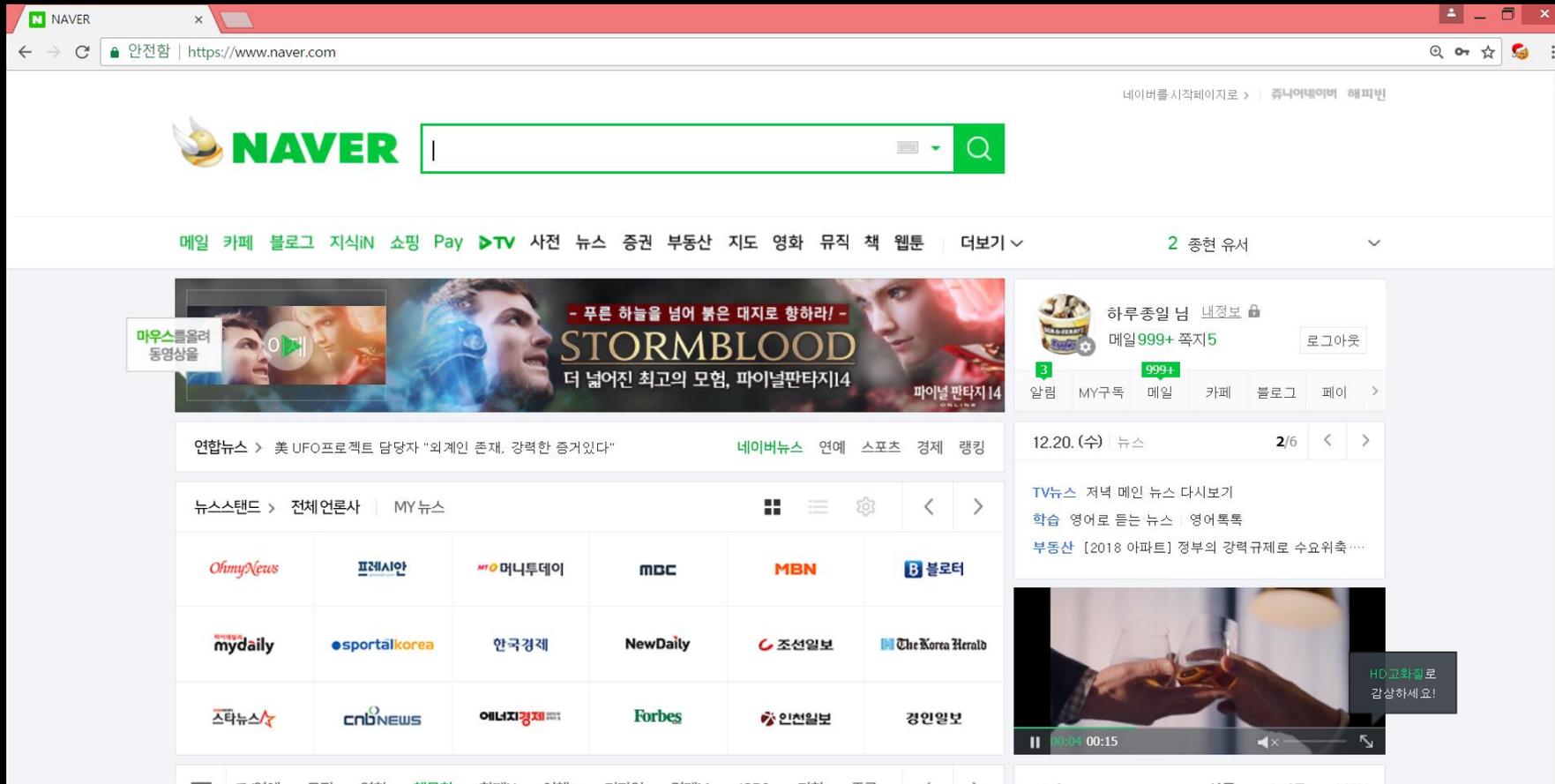
# EditCookie를 이용한 Cookie 조작



# EditCookie를 이용한 Cookie 조작



# Cookie 탈취를 통한 Login



개선방안

# 개선 방안

- Web Service 사용시 일부만 보안통신(SSL)을 이용하는 것이 아닌 **모두 보안 통신을 이용할 것**
  - 예) HSTS(HTTP Strict Transport Security)
- 쿠키 인증 정보를 **고정된 값으로 사용하는 것이 아닌** 난수화 시켜 해당 Cookie등의 정보를 Sniffing하더라도 사용할 수 없도록 개선
  - 예) RTA(Randomized Token Authentication)

향후 계획

# 향후 계획

- Wireless의 보안이 **아주 많이 취약**
  - Wireless(특히, WPA2방식)에서 보안을 높일 수 있는 연구 계획 중
  - WPA2의 Key-exchange를 **인증**을 통해 **저장한 Key를 사용**하도록 WPA2 인증방식을 수정
- EditThisCookie(Chrome Plugin)를 이용하는 것이 아닌 Web을 이용해 Database data를 정렬하고 Parsing한 Cookie 값을 통해 쉽게 인증이 가능하도록 웹의 형태로 서비스 구축
  - 일반 사용자가 쉽게 사용할 수 있게끔 제작하여 Cookie Parsing에 대한 심각성을 알림

Q&A

