

# 중부대 OTP 통합로그인 자동화 프로그램 개발

---

중부대 SCP 정보보안 동아리  
92113566 1학년 부원 노무승

# 목차

1. 통합 로그인에 OTP 도입
2. 웹 사이트 분석
3. 개발 구상
4. 자동화 프로그램 개발
5. 시연 영상

# 1. 통합 로그인에 OTP 도입

# 1-1. OTP란?

두산백과

## OTP

[ One Time Password ]

**요약** 고정된 패스워드 대신 무작위로 생성되는 일회용 패스워드를 이용하는 사용자 인증 방식.

ID/PW 유출 사고를 대비한 인증 방식으로 **2팩터 인증**에 용이

# 1-2. OTP의 활용



중부대학교

★

45

2416 0933

NAVER

OTP 인증 번호 ?

2932 1373

유효시간 53초

유효시간 내에 인증 번호를 입력하세요.

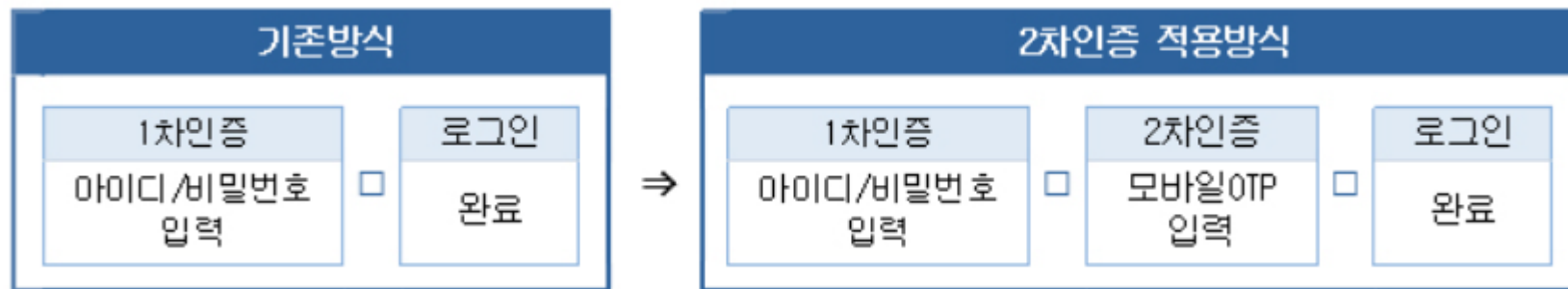
시간을 초과한 경우 새로 발급된 인증 번호를 다시 입력하셔야 합니다.

# 1-3. 중부대 통합로그인에 OTP 도입

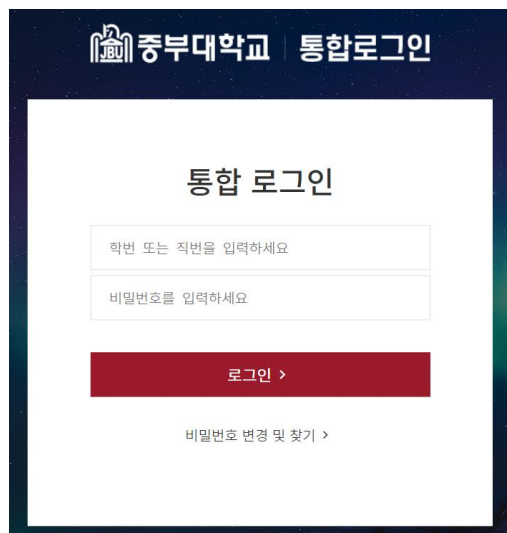
## 중요정보서비스의 2차인증(OTP) 적용 계획 안내

작성부서 전산정보원 | 작성일시 2021/08/09 | 분류 전체 | 조회수 26,333 | 공지기간 2021/08/09 ~ 2021/09/10

1. 관련 근거 : [교육부 정보보안 기본지침] 제74조(비밀번호 관리) 및  
고등교육법 시행령 제14조의2 일반대학의 원격수업 운영 기준



# 1-4. 로그인 절차



중부대학교 통합로그인

통합 로그인

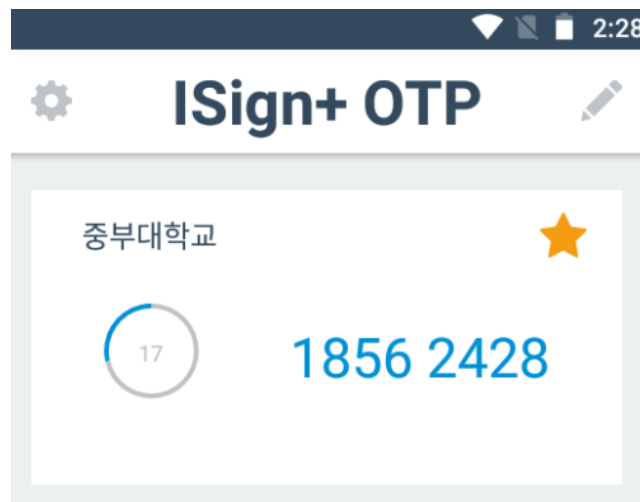
학번 또는 직번을 입력하세요

비밀번호를 입력하세요

로그인 >

비밀번호 변경 및 찾기 >

PC에서 ID/PW

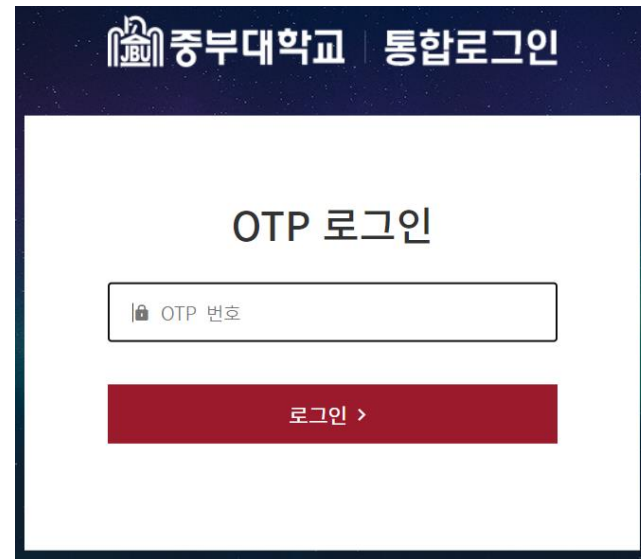
ISign+ OTP

중부대학교

17

1856 2428

모바일에서 OTP

중부대학교 통합로그인

OTP 로그인

OTP 번호

로그인 >

로그인 성공

기존 디폴트 아이디/패스워드 부여 방식에 찔렸는지

PC와 모바일을 오가는 **2채널 인증** 을 의도하여 로그인을 구성

## 2. 웹사이트 분석



## 2-1. OTP 우회방안

1. 사이트를 털어서 웹 취약점으로 OTP를 우회
2. OCR로 캡처를 인식해 OTP 자동 입력

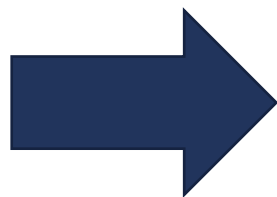
## 2-2. 웹사이트 분석 : ID/ PW 로그인 화면

POST https://sso.joongbu.ac.kr/authentication/idpw/loginProcess

agentId: "8"

id: "92113566"

pw: "██████████"



헤더 쿠키 요청 **응답** 타이밍 스택 추적 보안

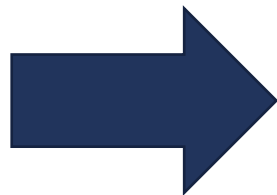
HTML

```
17 <input id="requestId" name="requestId" type="hidden" value="
18 <input id="isToken" name="isToken" type="hidden" value="Y" />
19 <input id="reTry" name="reTry" type="hidden" value="N" />
20 <input id="method" name="method" type="hidden" value="checkTo
21 </form>
22
23 <div>
24 <!-- backdrop template -->
25 <script id="tpl-backdrop" type="text/lodash-template">
26 <div class="backdrop">
27 <div class="backdrop-content">
28 <div>
29 <i class="fa fa-spin fa-refresh"></i> Loading
30 </div>
31 </div>
32 </div>
33 </script>
34 <script src="/webjars/adminlte/2.3.2/plugins/jquery/jquery-2.
35 <script src="/webjars/adminlte/2.3.2/bootstrap/js/bootstrap.m
36 <script src="/webjars/adminlte/2.3.2/dist/js/app.min.js"></sc
37 <script src="/webjars/adminlte/2.3.2/plugins/select2/select2.
38 <script src="/webjars/lodash/4.2.0/dist/lodash.min.js"></scri
39 <script src="/webjars/toastr/2.1.2/build/toastr.min.js"></scr
40 <script src="/resources/js/common/locale.ko.js"></script>
41 <script src="/resources/js/common/common.js"></script>
42 </div>
43 <script src="/resources/js/authentication/send.js"></script>
```

## 2-2. 웹사이트 분석 : 리다이렉트js

▶ GET <https://sso.joongbu.ac.kr/resources/js/authentication/send.js>

|        |                                 |
|--------|---------------------------------|
| 상태     | 200 ?                           |
| 버전     | HTTP/1.1                        |
| 전송됨    | 4.20 KB (3.95 KB 크기)            |
| 리퍼러 정책 | strict-origin-when-cross-origin |



```
if (resultCode != null && resultCode != "") {
    if (resultCode == "000000") {
        $('#form-send').submit();
    } else if (resultCode == "210010") {
        if(confirm(resultMessage) == true) {
            passwordChange(agentId, id);
            //window.history.back();
        } else {
            $('#resultCode').val("000000");
            $('#form-send').submit();
        }
    } else if (resultCode == "210002" || resultCode == "210011") {
        alert(resultMessage);
        passwordChange(agentId, id);
    } else if (resultCode == "270000") {
        alert(resultMessage);
    } else if (resultCode == "500001") {
        if(confirm(resultMessage) == true) {
            var action = "/duplicationLoginProcess";
            $('#form-send').attr('action', action);
            $('#form-send').submit();
            return;
        } else {
            var action = "/login.html?agentId=" + agentId;
            $('#form-send').attr('action', action);
            $('#form-send').submit();
            return;
        }
    } else if (resultCode == "200005") {
        // 첫번째 인증 받지 않은 경우
        alert(resultMessage);
        var action = "/login.html?agentId=" + agentId;
        $('#form-send').attr('action', action);
        $('#form-send').submit();
    } else if (resultCode == "280018" || resultCode == "280031") {
        // UAF 미등록
        if(confirm(L['UAF 로그인 인증 FIDO등록']) == true) {
            var action = "/authentication/uaf/uafRegister.html";
            $('#form-send').attr('action', action);
            $('#form-send').submit();
            return;
        }
    }
}
```

## 2-2. 웹사이트 분석 : 보안 세션 부여

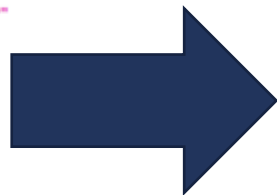
▶ POST <https://sso.joongbu.ac.kr/authentication/otp/otpLogin.html?agentId=8>

헤더 쿠키 요청 응답 타이밍 스택 추적 보안

요청 파라미터 거르기

양식 데이터 원시 ☐

```
resultCode: "000000"
resultMessage: "비밀번호+유효+기간이+지났습니다.+비밀번호+변경+화면으로+이동하시겠습니까?"
secureToken: ""
secureSessionId: "99C4900EC01749BE385755C0C0AD30A1"
userId: "92113566"
agentId: "8"
code: ""
requestId: ""
isToken: "Y"
reTry: "N"
method: "checkToken"
```



헤더 쿠키 요청 응답

HTML

중부대학교 통합로그인

**OTP 로그인**

- OTP 번호

로그인

## 2-2. 웹사이트 분석 : OTP 전송

▶ GET <https://sso.joongbu.ac.kr/resources/js/authentication/otp/otpLogin.js>

▶ POST <https://sso.joongbu.ac.kr/authentication/otp/loginProcess>

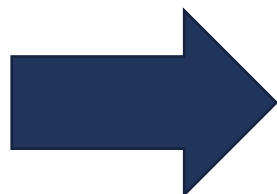
헤더 쿠키 요청 **응답** 타이밍 보안

응답 페이로드

```

1  $(function() {
2
3      // 토큰 정보들을 가지고 returnUrl로 forward 한다.
4      function sendToken(resultCode, resultMessage, secureToken, secureSe
5          returnUrl) {
6
7          var form = $('<form action="" + returnUrl + "" method="post">'
8              + '<input type="hidden" name="resultCode" value="" + re
9              + "" />' + '<input type="hidden" name="resultMessage" v
10             + resultMessage + "" />'
11             + '<input type="hidden" name="secureToken" value="" + s
12             + "" />' + '<input type="hidden" name="secureSessionId"
13             + secureSessionId + "" />' + '</form>');
14
15          $('body').append(form);
16          form.submit();
17      }
18
19      var props = {
20          constants : {},
21          elements : {
22              $formlogin : $('#form-login'),
23              $otpNumber : $('#otpNumber'),
24              $btnLogin : $('#btn-login'),
25              $linkTemporaryOtpNumber : $('#link-temporary-otp-number')
26          }
27      };
28
29      var LoginView = new ISP.View({
30          login : function() {
31
32              var otpNumber = $('#otpNumber').val();
33
34              //console.log(otpNumber);
35
36              if (otpNumber == undefined || otpNumber.length == 0) {
37                  alertErrorMessage(L[230007]);
38                  return;
39              }
40
41              var action = "/authentication/otp/loginProcess";
42              props.elements.$formlogin.attr('action', action);
43              props.elements.$formlogin.attr('method', 'post');
44              props.elements.$formlogin.submit();
45          }
46      });

```



헤더 쿠키 **요청**

요청 파라미터 거르기

양식 데이터

```

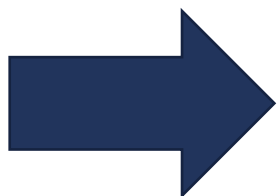
agentId: "8"
userId: "92113566"
otp: ""
otpNumber: "55914129"


```

## 2-2. 웹사이트 분석 : 보안 토큰 부여

▶ GET <https://sso.joongbu.ac.kr/resources/js/authentication/send.js>

POST <https://haksaweb.joongbu.ac.kr/sso/checkauth.jsp>



 헤더 쿠키 **요청** 응답 타이밍 스택 추적 보안

요청 파라미터 거르기

양식 데이터 원시 ☐

```
resultCode: "000000"
resultMessage: "성공"
secureToken: "wRbX8uRTQU8OCIfKNAQ1dTRDMelwq6Y3+JiPuHDfsBw4iTcdfylsmAEZnllwJGOUwdXG8WY
jwP2o1LRR7AJhyZJcmzH7hx3WLI6oCbW37OF6oQhIDOSbT388UVAI8SvPrmr2bSxgUw/EO59
50eECL3cpVHkrWERYuRybsGzZQ04="
secureSessionId: "DB2AB955E04A1C44C4DDB178ACF8E072"
userId: "92113566"
agentId: "8"
code: ""
requestId: ""
isToken: "Y"
reTry: "N"
method: "checkToken"
```

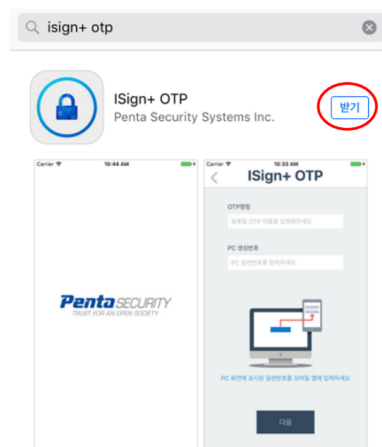
## 2-3. 느낀점

1. 서버단에서 보안 토큰과 보안 세션을 발급
2. 우리 대학교만 OTP가 적용된건 아닌듯..

### OTP 사용자 Manual

2020년  
경인여자대학교 전산정보원

#### OTP 프로그램 설치 (모바일)



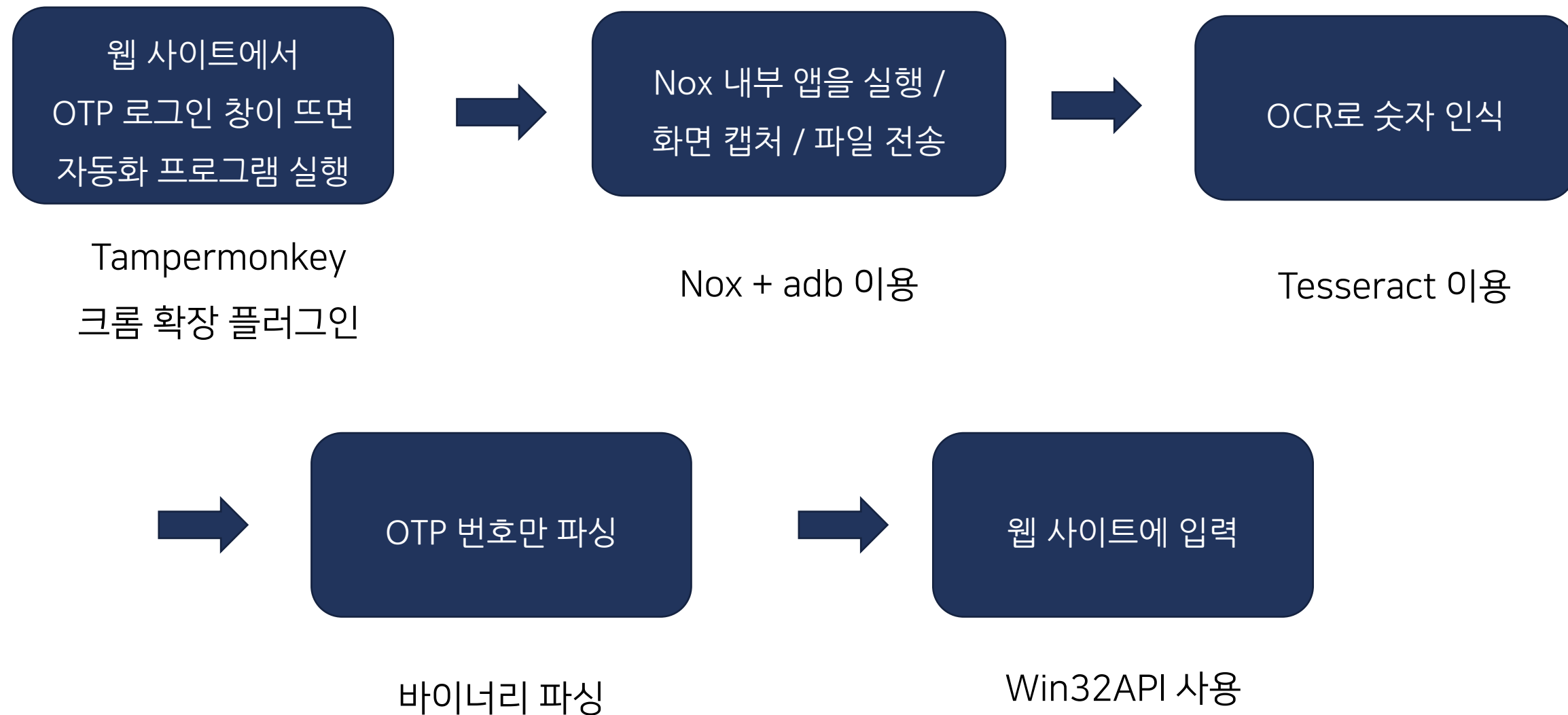
PlayStore 또는 AppStore에서

ISign+ OTP 를 검색하고, APP을  
설치합니다.

### 3. 개발 구상



## 3-1. 개발구상



## 4. 자동화 프로그램 개발

## 4-1. 웹사이트에서 프로그램 실행

```
1  |// ==UserScript==
2  |// @name      중부대 자동 로그인 JS
3  |// @namespace  http://tampermonkey.net/
4  |// @version    0.1
5  |// @description try to take over the world!
6  |// @author     You
7  |// @match      https://sso.joongbu.ac.kr/authentication/otp/otpLogin.html?*
8  |// @match      https://sso.joongbu.ac.kr/authentication/idpw/idPwLogin.html*
9  |// @match      https://sso.joongbu.ac.kr/authentication/idpw/loginProcess
10 |// @icon       https://www.google.com/s2/favicons?domain=ac.kr
11 |// @grant      none
12 |// ==/UserScript==
13 |
14 |(function() {
15 |   var url = document.location.href.split("?");
16 |   url = url[0].split(";");
17 |
18 |   if (url[0] === 'https://sso.joongbu.ac.kr/authentication/idpw/idPwLogin.html'){
19 |     document.getElementById('id').value = '92113566'
20 |     document.getElementById('pw').value = '
21 |     setTimeout(() => document.getElementById('btn-login').click(), 1000);
22 |
23 |
24 |   } else if (url[0] === 'https://sso.joongbu.ac.kr/authentication/otp/otpLogin.html'){
25 |     window.open("test://");
26 |
27 |   }
28 |}
```

Tampermonkey 크롬 확장 플러그인을 통해  
특정 URL에서 파일을 실행되게끔 구성

## 4-2. Custom URL Schemes

일반적으로 JS에서 로컬에 있는 특정 파일을  
실행시키는 것은 보안 상 차단되어 있음.



커스텀 브라우저 프로토콜을 사용하여 해결

## 4-2. Custom URL Schemes

레지스트리 편집기

파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H)

컴퓨터\HKEY\_CLASSES\_ROOT\test\shell\open\command

| 이름       | 종류     | 데이터                          |
|----------|--------|------------------------------|
| ab (기본값) | REG_SZ | "D:\Setup\otp auto.exe" "%1" |



test://

중부대학교 마이페이지 한국어 맞춤법/문법...

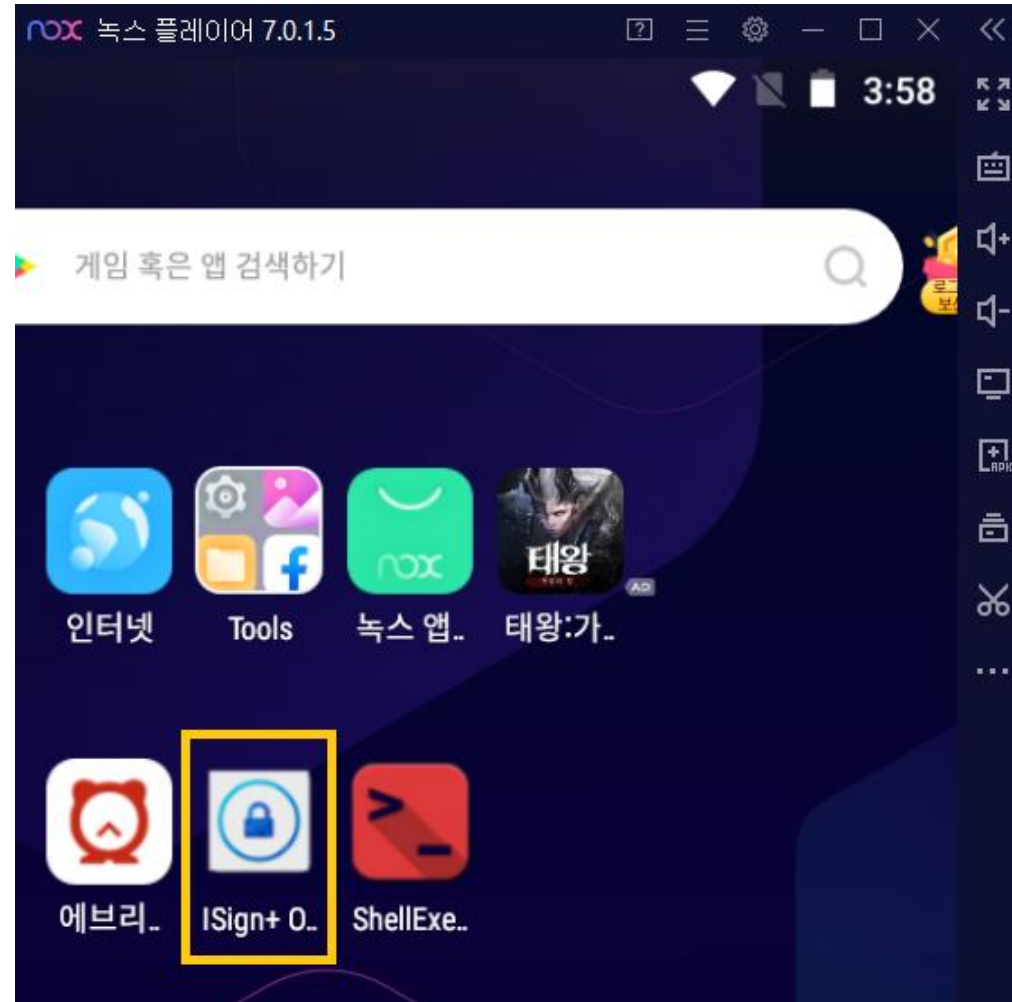
otp auto.exe을(를) 여시겠습니까?

웹사이트에서 이 애플리케이션을 열려고 합니다.

otp auto.exe 열기

취소

## 4-3. Nox 구성



## 4-4. adb를 이용한 Nox 컨트롤

```
Shell ("D:\Setup\Nox\bin\adb.exe connect 127.0.0.1:62001")  
Delay (1)
```

Nox와 adb를 연결시킴.

## 4-4. adb를 이용한 Nox 컨트롤

```
Shell ("D:\Setup\Nox\bin\adb.exe shell am start -n com.pentasecurity.isignplus.mobileotp/.ui.SplashActivity")  
Form1.Text = Form1.Text & "※ ISIGN+OTP 앱을 실행합니다." + vbNewLine  
Delay (4)
```

Adb를 이용해 ISIGN+OTP 앱을 실행함



## 4-4. adb를 이용한 Nox 컨트롤

```
d:##Setup##Nox##bin>adb shell pm list packages -f
package:/system/priv-app/CtsShimPrivPrebuilt/CtsShimPrivPrebuilt.apk=com.android.cts.priv.ctsshim
package:/system/priv-app/TelephonyProvider/TelephonyProvider.apk=com.android.providers.telephony
package:/system/priv-app/CalendarProvider/CalendarProvider.apk=com.android.providers.calendar
package:/system/priv-app/MediaProvider/MediaProvider.apk=com.android.providers.media
package:/system/priv-app/WallpaperCropper/WallpaperCropper.apk=com.android.wallpapercropper
package:/data/app/com.pentasecurity.isignplus.mobileotp-1/base.apk=com.pentasecurity.isignplus.mobileotp
package:/data/app/com.pentasecurity.isignplus.mobileotp-1/base.apk=com.pentasecurity.isignplus.mobileotp
```

```
d:##Setup##Nox##bin>adb shell pm dump com.pentasecurity.isignplus.mobileotp
DUMP OF SERVICE package:
  Activity Resolver Table:
    Schemes:
      isignplus:
        4755244 com.pentasecurity.isignplus.mobileotp/.ui.SplashActivity filter 9ab1e2b
          Action: "android.intent.action.VIEW"
          Category: "android.intent.category.DEFAULT"
          Category: "android.intent.category.BROWSABLE"
          Scheme: "isignplus"
          Authority: "otps": -1
          AutoVerify=false
```

## 4-4. adb를 이용한 Nox 컨트롤

```
Shell ("D:\Setup\Nox\bin\adb.exe shell screencap -p /sdcard/screen.png")  
Form1.Text = Form1.Text & "※ adb : NOX 스크린 샷을 찍습니다." + vbNewLine  
Delay (1)
```

```
Shell ("D:\Setup\Nox\bin\adb.exe pull /sdcard/screen.png D:\Setup\Nox\bin\screen.png")  
Form1.Text = Form1.Text & "※ adb : NOX 스크린 샷을 PC로 복사합니다." + vbNewLine
```

```
Do  
    If Len(Dir("D:\Setup\Nox\bin\screen.png")) Then  
        Delay (1)  
        Exit Do  
    End If  
    DoEvents  
Loop
```

adb를 이용해 Nox 스크린샷을 찍고  
스크린샷 파일을 PC로 복사함.

## 4-5. Tesseract를 이용한 OCR

```
Shell ("tesseract D:\Setup\Nox\bin\screen.png D:\Setup\Nox\bin\digits digits")
Form1.Text = Form1.Text & "※ OCR로 OTP 인식을 시작합니다." + vbNewLine
```

Tesseract를 이용해 스크린샷 파일을 OCR 돌리고

```
Do
If Len(Dir("D:\Setup\Nox\bin\digits.txt")) Then
Delay (1)
Dim Data(256) As Byte
Dim Count As Integer
Open "D:\Setup\Nox\bin\digits.txt" For Binary Access Read As #1
Get #1, , Data
For i = 0 To LOF(1) - 1
If ((Data(i) >= &H30) And (Data(i) <= &H39)) Then
Count = Count + 1
If (Count = 8) Then
otp = Chr(Data(i - 7)) & Chr(Data(i - 6)) & Chr(Data(i - 5)) & Chr(Data(i - 4)) & _
Chr(Data(i - 3)) & Chr(Data(i - 2)) & Chr(Data(i - 1)) & Chr(Data(i))
End If
Else
Count = 0
End If
Next i
Close #1
Exit Do
End If
DoEvents
Loop
```

OCR 결과에서 8자리 숫자만 파싱함.

## 4-6. 웹 브라우저에 OCR 번호 입력

```
Handle = FindWindow(vbNullString, "통합로그인 | 중부대학교 - Chrome")
```

```
Call SetForegroundWindow(Handle)
```

크롬 창 핸들 값을 구하고, 창의 포커스를 활성화 시킴

## 4-6. 웹 브라우저에 OCR 번호 입력

```

For i = 1 To Len(otp)
    Dim digit As Integer
    digit = Mid(otp, i, 1)
    Select Case (digit)
    Case 0
        Call PostMessage(Handle, WM_KEYDOWN, Asc(digit), KEYI_0)
        Call PostMessage(Handle, WM_KEYUP, Asc(digit), KEYI_0 + &HC00000000)
    Case 1
        Call PostMessage(Handle, WM_KEYDOWN, Asc(digit), KEYI_1)
        Call PostMessage(Handle, WM_KEYUP, Asc(digit), KEYI_1 + &HC00000000)
    Case 2
        Call PostMessage(Handle, WM_KEYDOWN, Asc(digit), KEYI_2)
        Call PostMessage(Handle, WM_KEYUP, Asc(digit), KEYI_2 + &HC00000000)
    Case 3
        Call PostMessage(Handle, WM_KEYDOWN, Asc(digit), KEYI_3)
        Call PostMessage(Handle, WM_KEYUP, Asc(digit), KEYI_3 + &HC00000000)
    Case 4
        Call PostMessage(Handle, WM_KEYDOWN, Asc(digit), KEYI_4)
        Call PostMessage(Handle, WM_KEYUP, Asc(digit), KEYI_4 + &HC00000000)

```

```

    Case 5
        Call PostMessage(Handle, WM_KEYDOWN, Asc(digit), KEYI_5)
        Call PostMessage(Handle, WM_KEYUP, Asc(digit), KEYI_5 + &HC00000000)
    Case 6
        Call PostMessage(Handle, WM_KEYDOWN, Asc(digit), KEYI_6)
        Call PostMessage(Handle, WM_KEYUP, Asc(digit), KEYI_6 + &HC00000000)
    Case 7
        Call PostMessage(Handle, WM_KEYDOWN, Asc(digit), KEYI_7)
        Call PostMessage(Handle, WM_KEYUP, Asc(digit), KEYI_7 + &HC00000000)
    Case 8
        Call PostMessage(Handle, WM_KEYDOWN, Asc(digit), KEYI_8)
        Call PostMessage(Handle, WM_KEYUP, Asc(digit), KEYI_8 + &HC00000000)
    Case 9
        Call PostMessage(Handle, WM_KEYDOWN, Asc(digit), KEYI_9)
        Call PostMessage(Handle, WM_KEYUP, Asc(digit), KEYI_9 + &HC00000000)
    End Select
Next i

```

각각의 OCR 번호를 Postmessage API에  
WM\_KEYDOWN 메시지와 WM\_KEYUP 메시지를 담아 전송

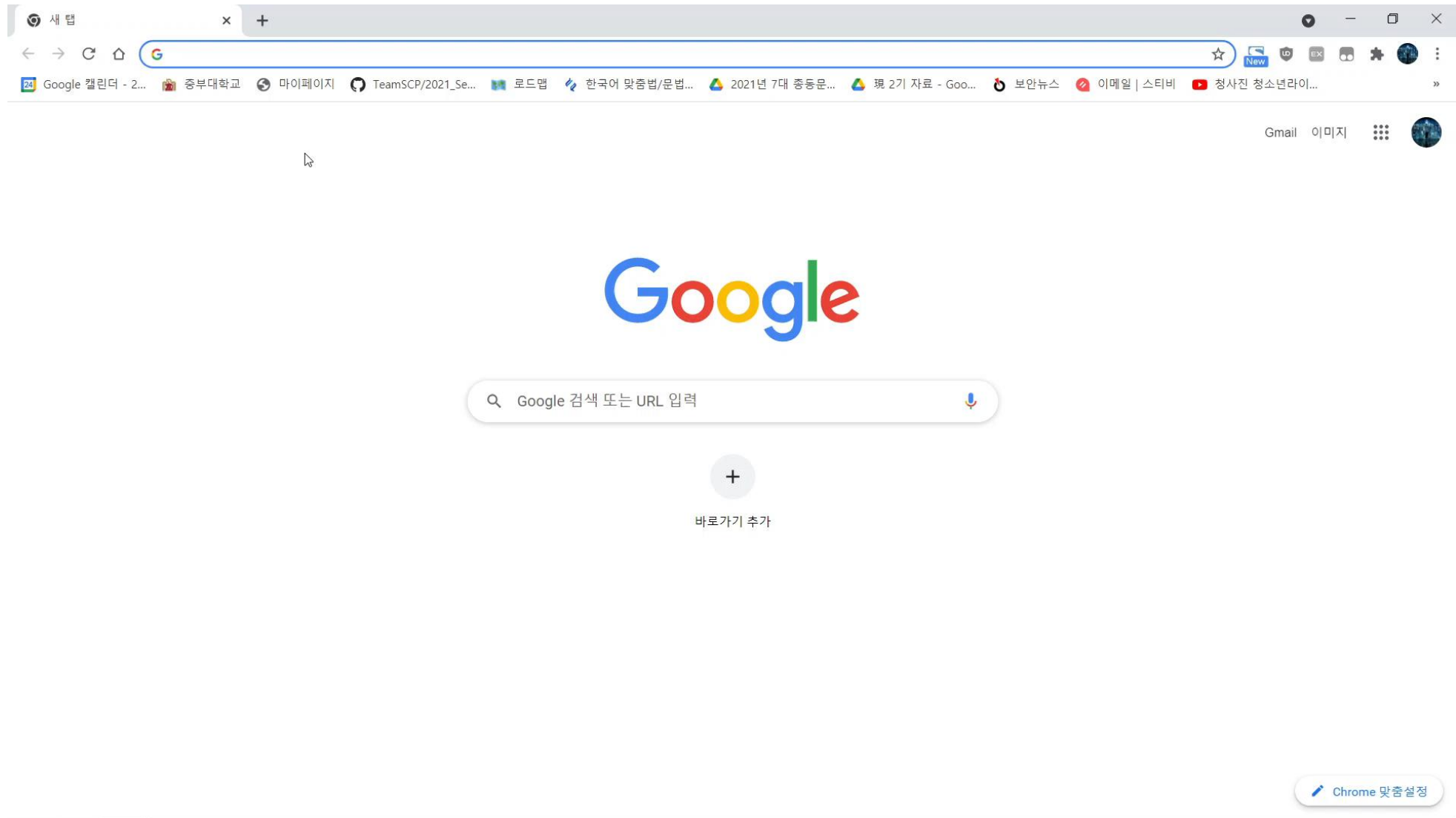
## 4-6. 웹 브라우저에 OCR 번호 입력

```
Delay (0.5)  
Call PostMessage(Handle, WM_KEYDOWN, &HD, &H1C0001)  
Call PostMessage(Handle, WM_KEYUP, &HD, KEYI_0 + &HC01C0001)  
Delay (2)  
End
```

마지막으로 브라우저 창에 엔터까지 입력하고  
프로그램을 종료

## 5. 시연 영상

# 5-1. 시연 영상





# Q & A

---

「

# 감사합니다

」