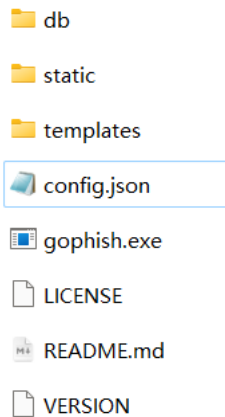


# build a phishing website by gophish

## Gophish: Open-Source Phishing Toolkit

[Gophish](#) is an open-source phishing toolkit designed for businesses and penetration testers. It provides the ability to quickly and easily setup and execute phishing engagements and security awareness training. Gophish can be obtained from [gophish/gophish: Open-Source Phishing Toolkit \(github.com\)](https://github.com/gophish/gophish).

### before start gophish



After downloading gophish-v0.12.1-windows-64bit, you should check the config.json file, which contains information about the listen url for administrator server and phish server. If your port 80 or 3333 is occupied, you need to consider changing the port number.

```
{
  "admin_server": {
    "listen_url": "127.0.0.1:3333",
    "use_tls": true,
    "cert_path": "gophish_admin.crt",
    "key_path": "gophish_admin.key",
    "trusted_origins": []
  },
  "phish_server": {
    "listen_url": "0.0.0.0:80",
    "use_tls": false,
    "cert_path": "example.crt",
    "key_path": "example.key"
  },
  "db_name": "sqlite3",
  "db_path": "gophish.db",
  "migrations_prefix": "db/db_",
  "contact_address": "",
  "logging": {
    "filename": "",
    "level": ""
  }
}
```

### Run gophish.exe and login into admin page

Double-click to run gophish.exe, and the terminal information shown below will pop up.

```
D:\tools\gophish-v0.12.1-windows-64bit\gophish.exe
time="2024-05-28T20:41:06+09:00" level=warning msg="No contact address has been configured."
time="2024-05-28T20:41:06+09:00" level=warning msg="Please consider adding a contact address entry in your config.json"
goose: migrating db environment 'production', current version: 0, target: 20220321133237
OK 20160118194630_init.sql
OK 20160131153104_0.1.2_add_event_details.sql
OK 20160211211220_0.1.2_add_ignore_cert_errors.sql
OK 20160217211342_0.1.2_create_from_col_results.sql
OK 20160225173824_0.1.2_capture_credentials.sql
OK 20160227180335_0.1.2_store_smtp_settings.sql
OK 20160317214457_0.2_redirect_url.sql
OK 20160605210903_0.2_campaign_scheduling.sql
OK 20170104220731_0.2_result_statuses.sql
OK 20170219122503_0.2.1_email_headers.sql
OK 20170827141312_0.4_utc_dates.sql
OK 20171027213457_0.4.1_maillogs.sql
OK 20171208201932_0.4.1_next_send_date.sql
OK 20180223101813_0.5.1_user_reporting.sql
OK 20180524203752_0.7.0_result_last_modified.sql
OK 20180527213648_0.7.0_store_email_request.sql
OK 20180830215615_0.7.0_send_by_date.sql
OK 20190105192341_0.8.0_rbac.sql
OK 2019104103306_0.9.0_create_webhooks.sql
OK 20200116000000_0.9.0_imap.sql
OK 20200619000000_0.11.0_password_policy.sql
OK 20200730000000_0.11.0_imap_ignore_cert_errors.sql
OK 20200914000000_0.11.0_last_login.sql
OK 20201201000000_0.11.0_account_locked.sql
OK 20220321133237_0.4.1_envelope_sender.sql
time="2024-05-28T20:41:12+09:00" level=info msg="Please login with the username admin and the password 0cf33a81e43a3aba" time="2024-05-28T20:41:12+09:00" level=info msg="Starting phishing se
ver at http://0.0.0.0:80"
time="2024-05-28T20:41:12+09:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2024-05-28T20:41:12+09:00" level=info msg="Creating new self-signed certificates for administration interface"
time="2024-05-28T20:41:12+09:00" level=info msg="Starting IMAP monitor manager"
time="2024-05-28T20:41:12+09:00" level=info msg="Starting new IMAP monitor for user admin"
time="2024-05-28T20:41:12+09:00" level=info msg="TLS Certificate Generation complete"
time="2024-05-28T20:41:12+09:00" level=info msg="Starting admin server at https://127.0.0.1:3333"
```


Log in to the admin server using the username and password displayed in the terminal



# Please sign in

Sign in

Enter the administrator page

 **gophish**

Dashboard

Campaigns

Users & Groups

Email Templates

Landing Pages

Sending Profiles

Account Settings

User Management Admin

Webhooks Admin

User Guide

API Documentation

# Dashboard

No campaigns created yet. Let's create one!

# Configuration

To send a phishing email containing a phishing website, you need to configure the following four modules: user & groups, email templates, landing pages, sending profiles. There is no requirement for the order of configuration.

## Sending Profiles

In this section, the mailbox for sending phishing emails will be configured

### New Sending Profile

Name:

Profile name

Interface Type:

SMTP

SMTP From: ?

First Last <test@example.com>

Host:

smtp.example.com:25

Username:

Username

Password:

Password

☒ Ignore Certificate Errors ?

Email Headers:

X-Custom-Header

{{.URL}}-gophish

+ Add Custom Header

Show 10 entries

Search:

Header

Value

No data available in table

Showing 0 to 0 of 0 entries

Previous

Next

Send Test Email

Cancel

Save Profile

The configuration information about SMTP can be obtained from the SMTP settings of the mail website used. If you use SSL connection, the SMTP HOST port needs to be filled in 465, otherwise it is 25

When the configuration is complete, you can click send test email to check whether the configuration is successful.

## email templates

You can configure the template for phishing emails here

## New Template

Name:

Template name

✉ Import Email

Envelope Sender: ⓘ

First Last <test@example.com>

Subject:

Email Subject

Text

HTML

Plaintext

☒ Add Tracking Image

✚ Add Files

Show 10 entries

Search:

Name

No data available in table

Showing 0 to 0 of 0 entries

Previous

Next

Cancel

Save Template

Users can first design a phishing email in their own mailbox system, and then send it to themselves or other partners. After receiving the designed email, open it and choose to export it as an eml file or display the original email, and then copy the content into gophish's Import Email to import the designed phishing email into. Don't forget to include a hyperlink in your email, as it will be replaced with a phishing link.

## Users & Groups

You can configure the users to whom phishing emails will be sent here

## New Group

Name:

### + Bulk Import Users

[Download CSV Template](#)

First Nam

Last Name

+ Add

Show 10 entries

Search:

First Name

Last Name Email Position 

No data available  
in table

Showing 0 to 0 of 0 entries

[Previous](#)

Next

Save changes

Loading the phishing page is the most important part of the entire phishing process. You need to build a phishing page that is exactly the same as the original login page.

## New Landing Page

Name:

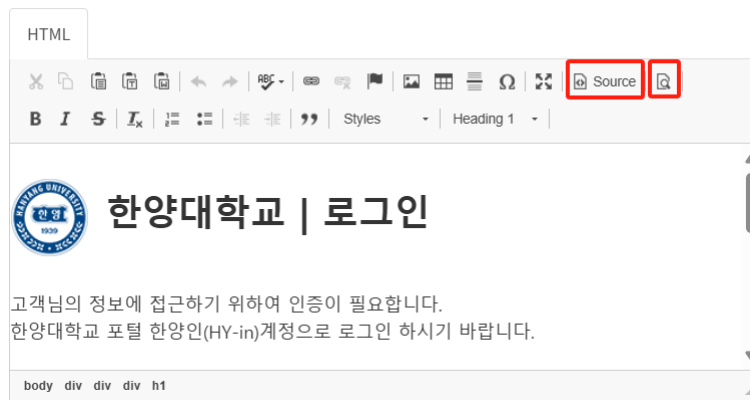
 Import Site

HTML

☐ Capture Submitted Data ?

Save Page

Click import site and enter the page you want to emulate, for example [https://api.hanyang.ac.kr/o\\_auth/login](https://api.hanyang.ac.kr/o_auth/login). The source code of the web page will be automatically crawled, but this is not the end.



These two buttons are very important. One button can make necessary edits to the web page source code, and the other button can preview the page.

The imported front-end source code must strictly contain the `<form method="post" ...><input name="aaa" ... /> ... <input type="submit" ... />` structure. If it is not satisfied, the submitted data cannot be captured.

Although we do not have the necessary network editing knowledge, all of this can be done through ChatGPT. This will solve most or all of your problems.



To add the specified form structure to your existing HTML page source, we'll wrap the existing input elements for the user ID and password inside a form tag with the `method="post"`. This will ensure the form data is sent via a POST request when the submit button is clicked.

Here is the edited version of the provided HTML:

```
html
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1"
<html lang="ko" xml:lang="ko" xmlns="http://www.w3.org/1999/xhtml">
<head>
  <base href="https://api.hanyang.ac.kr/oauth/login" /><meta http-equiv="content-type" c
  <title>한양대학교 인증센터</title>
  <link href="/resources/css/oauth_css.css" rel="stylesheet" type="text/css" /><script t
  var _submit = true;
  var _complete = false;
  var contextPath = '';
  $( document ).ready(function() {
```



给“ChatGPT”发送消息



```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html lang="ko" xml:lang="ko" xmlns="http://www.w3.org/1999/xhtml">
<head>
  <base href="https://api.hanyang.ac.kr/oauth/login"/>
  <meta http-equiv="content-type" content="text/html; charset=euc-kr"/>
  <meta name="viewport" content="width=device-width, initial-scale=1.0, user-
scalable=no, minimum-scale=1.0, maximum-scale=1.0"/>
  <meta http-equiv="X-UA-Compatible" content="IE=edge"/>
  <title>한양대학교 인증센터</title>
  <link href="/resources/css/oauth_css.css" rel="stylesheet" type="text/css"/>
  <script type="text/javascript" src="/resources/js/core/jquery-2.1.0.min.js">
</script>
  <script type="text/javascript" src="/resources/js/enc_base64.js"></script>
  <script type="text/javascript" src="/resources/js/enc_core.js"></script>
```

```

<script type="text/javascript">
    // Your existing JavaScript code remains here.
</script>
</head>
<body>
<div id="wrap">
    <div id="header">
        <div class="box">
            <h1 class="logo"><span class="title">한양대학교 | 로그인
</span></h1>
            <h2 class="title_txt mt30">고객님의 정보에 접근하기 위하여 인증이 필요합니다.
<br/>
            한양대학교 포털 한양인(HY-in)계정으로 로그인 하시기 바랍니다.</h2>
        </div>
    </div>
    <div id="container">
        <div class="box">
            <div class="c_b mt30"> </div>
            <div class="login">
                <div class="login_con">
                    <p class="login_tit">Portal Login</p>
                    <form method="post" action="/oauth/login_submit.json">
                        <dl>
                            <dt><label for="userId">ID</label></dt>
                            <dd><input name="userId" id="uid" placeholder="아이디
를 입력하세요" type="text" value=""/></dd>
                            <dt><label for="userPassword">Password</label></dt>
                            <dd><input name="userPassword" id="upw"
placeholder="비밀번호를 입력하세요" type="password" value=""/></dd>
                        </dl>
                        <div class="btn"><button type="submit" id="login_btn">로그
인</button></div>
                    </form>
                </div>
            </div>
            <div class="c_b mt50"> </div>
        </div>
    </div>
    <div id="bottom">
        <div class="box">
            <h2><span>한양대학교API 개발자센터</span></h2>
            <address><span>우)133-791 서울특별시 성동구 왕십리로 222</span></address>
            <p class="copyright">Copyright 2014 Hanyang University. All Rights
Reserved.</p>
        </div>
    </div>
</div>
</body>
</html>

```

Click the preview button, they look exactly the same



Don't forget to check these two buttons, it will record all the information entered by the phishing user, including the password. And redirect to the normal interface, the user will not notice and log in again, as if the website just froze for a while.

☒ Capture Submitted Data ?

☒ Capture Passwords

**⚠ Warning:** Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to: ?

<http://example.com>

## Create New Campaigns

Now, fill in the name configured during the configuration phase. Send phishing emails and wait for users to take the bait.



New Campaign

Name:

Campaign name

Email Template:

midterm exam

Landing Page:

api hanyang

URL: ?

http://192.168.1.1

Launch Date

May 28th 2024, 9:37 pm

Send Emails By (Optional) ?

Sending Profile:

163.com

Send Test Email

Groups:

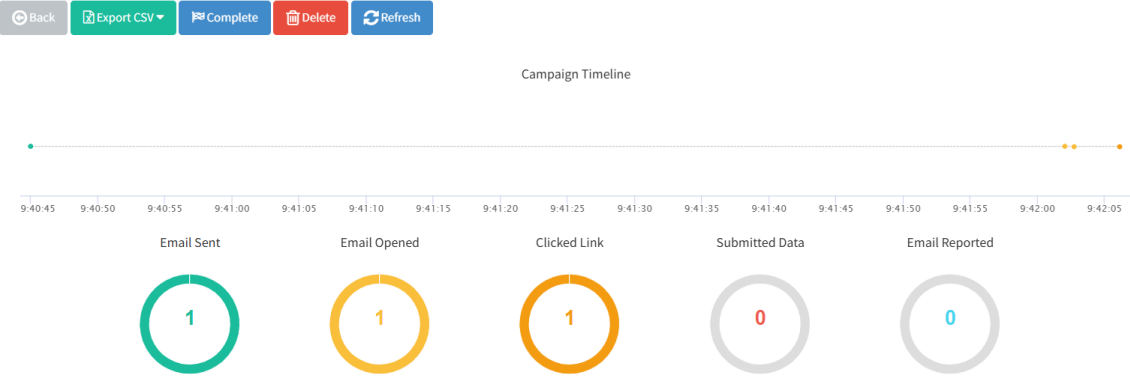
Select Group

Close

Launch Campaign

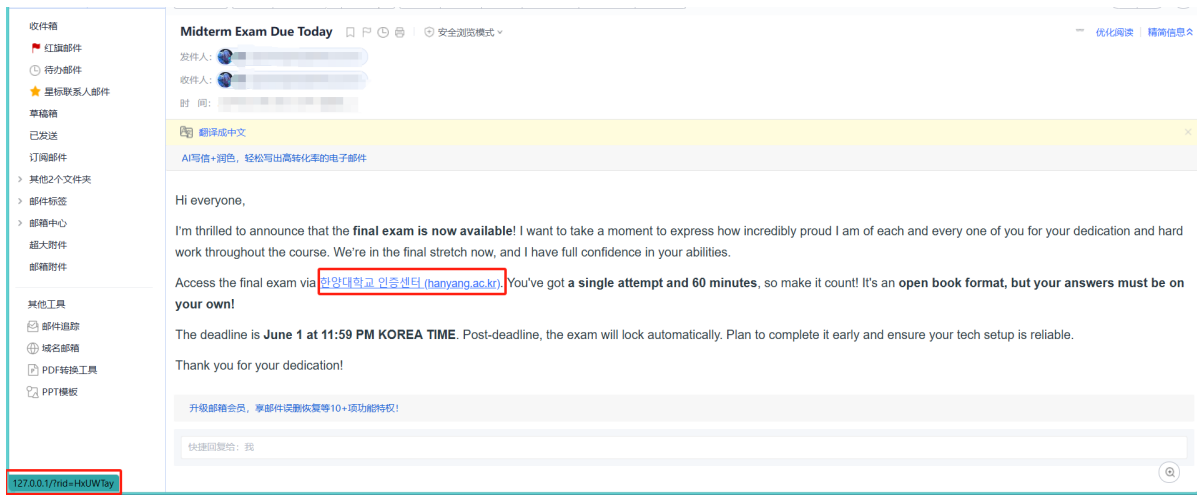
You can monitor the results of phishing link feedback in real time here

# Results for test2

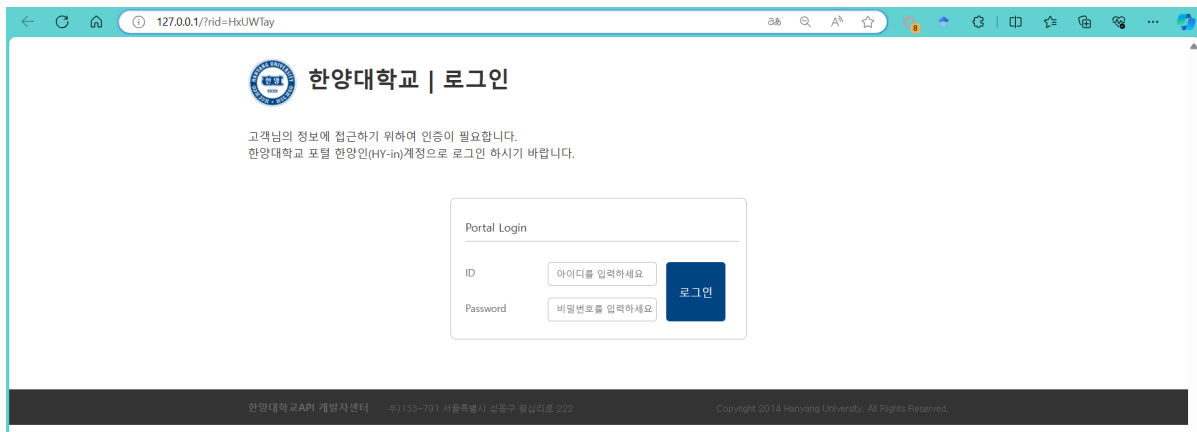


## Victims' perspective

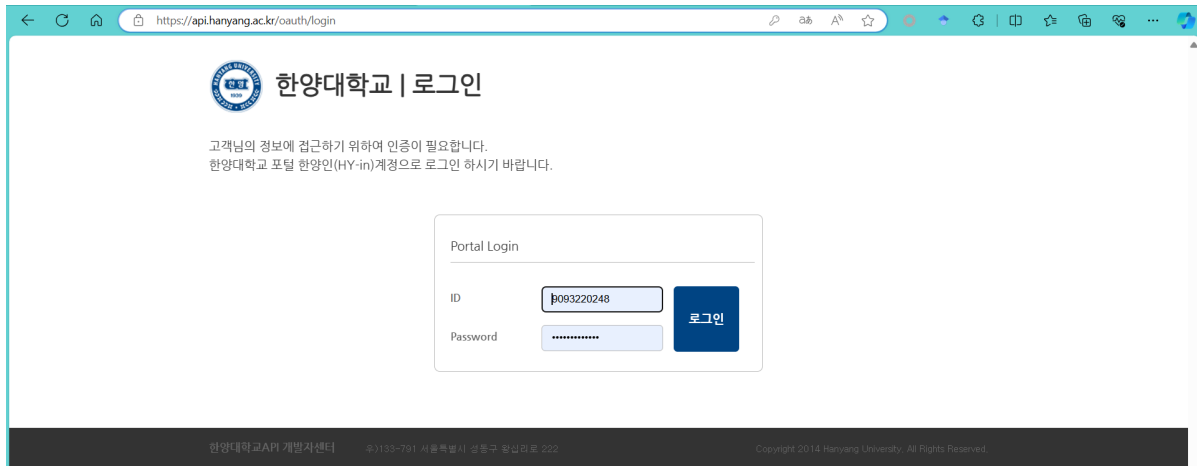
Seeing that the midterm exam was about to end, I immediately clicked on the link in the email without considering the fake link in the lower left corner.



This page is not much different from the normal login page, so I feel comfortable entering my account password and clicking Login.



After entering the password, I was redirected to the exact same web page. I didn't care and thought it was just an error caused by network fluctuations. And this time I logged in successfully




In some dark corner of the Internet, my account and password were stolen. One day later, the hacker deliberately handed in a blank paper in my important exam.

## Timeline for

Email: jszmqw2022@163.com

Result ID: HxUWTay

-  Campaign Created May 28th 2024 9:40:43 pm
-  Email Sent May 28th 2024 9:40:45 pm
-  Email Opened May 28th 2024 9:42:02 pm
-  Email Opened May 28th 2024 9:42:02 pm
-  Clicked Link May 28th 2024 9:42:06 pm
  -  Windows (OS Version: 10)
  -  Chrome (Version: 125.0.0.0)
-  Submitted Data May 28th 2024 9:48:13 pm
  -  Windows (OS Version: 10)
  -  Chrome (Version: 125.0.0.0)

 Replay Credentials

▼ View Details

Parameter	Value(s)
password	fake_password
userId	9093220248

## reference link:

[钓鱼工具gophish史上最详细教程（附实例）——手把手教你成为“捕鱼人”-CSDN博客](#)