

- [1 背景](#)
- [2 Gophish搭建钓鱼平台](#)
- [3 Gophish功能介绍](#)
 - [2.1 Groups](#)
 - [2.2 Email Templates](#)
 - [2.3 Landing Pages](#)
 - [2.4 Sending Profiles](#)
 - [2.5 Campaigns](#)
- [4 邮件服务器搭建](#)
- [5 问题点](#)

1 背景







近期需要组织个应急演练，其中有个科目就是邮件钓鱼，为了这个科目进行相关环境搭建，主要利用Gophish搭建钓鱼平台，由于是使用ubuntu所以使用Postfix+mailutils搭建邮件服务器（如果vps是centos，有更好用的平台EwoMail搭建，参考官方文档进行一步步搭<http://doc.ewomail.com/docs/ewomail/install>），具体搭建过程如下：

2 Gophish搭建钓鱼平台

Gophish 是一个功能强大的开源网络钓鱼框架。Github 地址:<https://github.com/gophish/gophish>

在github上查找合适的版本，本次的搭建的vps是ubuntu，Gophish版本为gophish-v0.11.0

f1af96033c946ed2fe757b9b3a7aefc3ec3548f0ab21f01c44d70a58410ffbe	gophish-v0.11.0-osx-64bit.zip
f5083bc084715319a4e671bc58dc28f66828fec78a43bd41456373fcc024703c	gophish-v0.11.0-windows-64bit.zip

▼ Assets 6		
 gophish-v0.11.0-linux-32bit.zip	30.9 MB	29 Aug 2020
 gophish-v0.11.0-linux-64bit.zip	31.3 MB	29 Aug 2020
 gophish-v0.11.0-osx-64bit.zip	33.2 MB	29 Aug 2020
 gophish-v0.11.0-windows-64bit.zip	31.7 MB	29 Aug 2020
 Source code (zip)		29 Aug 2020
 Source code (tar.gz)		29 Aug 2020

解压并启动

```
wget https://github.com/gophish/gophish/releases/download/v0.11.0/gophish-
```

```
v0.11.0-linux-64bit.zip
unzip gophish-v0.11.0-linux-64bit.zip
```

修改config.json,

后台管理页面开放的端口: admin_server 把 127.0.0.1 改为 0.0.0.0,外网直接访问就要0.0.0.0

钓鱼网站开放的端口: listen_url也要是0.0.0.0:89, 由于默认80端口被占用了, 所以修改为89
修改之后的配置文件如下:

```
root@easy-echo-2:~/tool/diaoyu# cat config.json
{
  "admin_server": {
    "listen_url": "0.0.0.0:3333",
    "use_tls": true,
    "cert_path": "gophish_admin.crt",
    "key_path": "gophish_admin.key"
  },
  "phish_server": {
    "listen_url": "0.0.0.0:89",
    "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": ""
  }
}
```

配置完成后直接运行

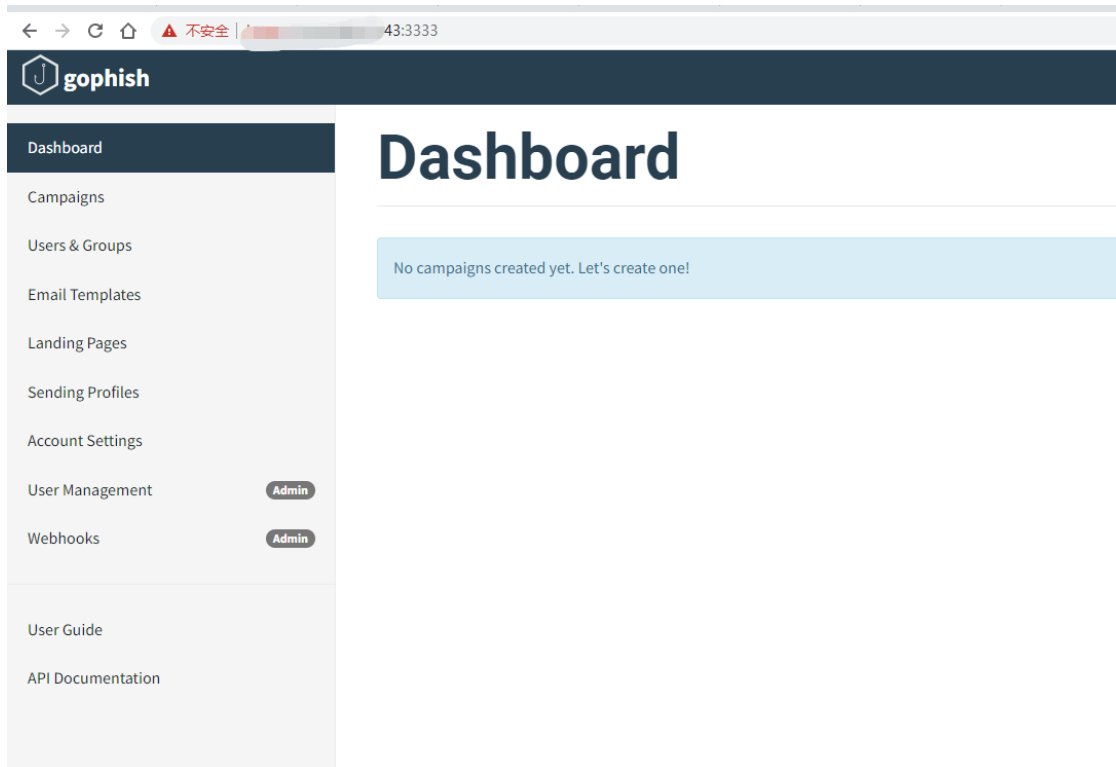
```
chmod 777 gophish
```

```
./gophish
```

开启后admin密码会在启动信息中显示 2a1774145a66fbfc

```
0.11.0_imap_ignore_cert_errors.sql
6:15Z" level=info msg="Please login with the username admin and the password 2a1774145a66fbfc"
6:15Z" level=info msg="Creating new self-signed certificates for administration interface"
6:15Z" level=info msg="Starting IMAP monitor manager"
6:15Z" level=info msg="Starting new IMAP monitor for user admin"
6:15Z" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
6:15Z" level=info msg="Starting phishing server at http://0.0.0.0:89"
6:15Z" level=info msg="TLS Certificate Generation complete"
6:15Z" level=info msg="Starting admin server at https://0.0.0.0:3333"
```

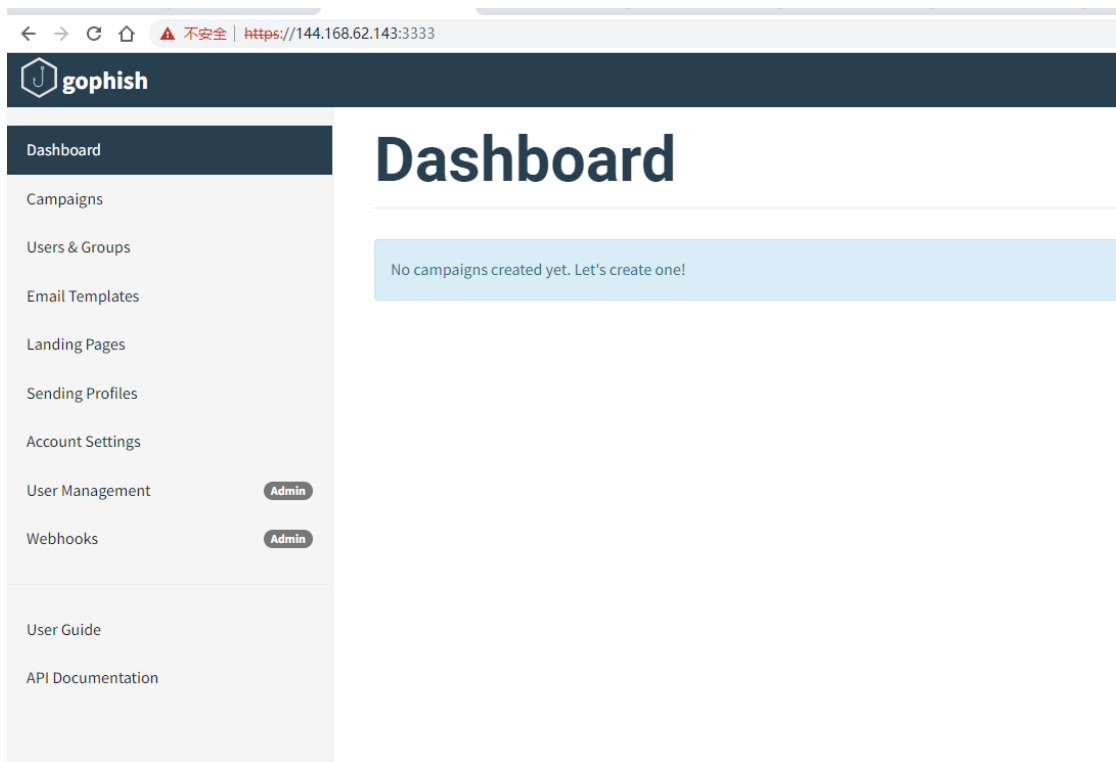
登录管理后台地址，端口为3333，利用获取的登录账号密码，admin,2a1774145a66fbfc



到此钓鱼平台搭建完成。

3 Gophish功能介绍

安装完成后页面如下：



官方指导手册地址：<https://docs.getgophish.com/user-guide/>

2.1 Groups

该功能主要是设置要进行钓鱼攻击的邮箱地址，可进行单个添加

New Group

Name:

[+ Bulk Import Users](#)

[Download CSV Template](#)

[+ Add](#)

Show entries

Search:

First Name

Last Name

Email

Position

No data available
in table

Showing 0 to 0 of 0 entries

[Previous](#)

[Next](#)

[Close](#)

[Save changes](#)

也支持表格导入，下载模板，

The screenshot shows the 'New Group' form with a red rectangular box highlighting the 'Download CSV Template' link. The form includes a 'Name' field, a '+ Bulk Import Users' button, and a 'Download CSV Template' link. Below these are input fields for 'First Name', 'Last Name', 'Email', and 'Position', followed by a '+ Add' button. There is also a 'Show' dropdown set to '10' and a 'Search' field. The table below the form shows 'No data available in table' and 'Showing 0 to 0 of 0 entries'. At the bottom right, there are 'Previous' and 'Next' navigation buttons, and at the very bottom, 'Close' and 'Save changes' buttons.

	A	B	C	D	E	F
1	First Name	Last Name	Email	Position		
2	11	11	11@163.com	Systems Administrator		
3	11		11@164.com			
4	11		11@165.com			
5	11		11@166.com			
6	11		11@167.com			
7						
8						
9						
10						

批量导入

+ Bulk Import Users
Download CSV Template

+ Add

Show entries
 Search:

First Name	Last Name	Email	Position
11	11	11@163.com	Systems Administrator
11	11	11@164.com	
11	11	11@165.com	
11	11	11@166.com	
11	11	11@167.com	

Showing 1 to 5 of 5 entries

Previous
1
Next

Close
Save changes

2.2 Email Templates

“模板”是发送到目标的电子邮件的内容。它们可以从现有电子邮件中导入，也可以从头开始创建。他们还支持发送附件。

New Template



Name:

Template name

Import Email

Subject:

Email Subject

TextHTML

Plaintext

☒ Add Tracking Image

+ Add Files

Show10entriesSearch:

Name

No data available in table

Showing 0 to 0 of 0 entries

PreviousNext

此处尝试导入现有电子邮件，将要保存的邮件另存为eml格式，然后粘贴导入

×

```
OyB3aG10ZS1zcGFjZTpub3dyYXA7IGZvbncQ6MTVweCBjb3VyaWVyOyBjb2xvcjojZmZmZmZmOyI+LSAtIC0gLSAtIC0gLSAtIC0gLSAtIC0gLSAtIC0gLSAtIC0gLSAtIC0gLSAtIC08L2Rp  
dj4KICAgIDwvdGQ+CIAgPC90cj4KICAgIS0tIGNsb3NlIGlwaG9uZSBnbWFpbCBmaXggLS0+CIAgPHRyPgogICAgPHRkPgogICAgICAgIDxpbgwcgc3JjPSJodHRwczovL2FwcC55aW54aWFuZy5jb20vZXRwYS83NTM2OTAyNC1oDRjLTQON2QtYmExMC0wZWMM4YWVhOGVjZTkilHN0eWxlPSJoZWlnaHQ6IDFweDsgd2lkdgG6IDFweDsiIC8+CgogICAgPC90ZD4KICA8L3RyPgo8L3RhYmxlPgoKICAgICAgICAgICAgICA8L3RkPgogICAgICAgICAgICA8L3RyPgo8ICAgICAgICAgPC90YWJsZT4KICAgICAgICAgIDwhLS0gZW5kIGJhY2tncm9lbmdqdgGfIBGUgLS0+CIAgICAgICAgPC90ZD4KICAgICAgPC90cj4KICAgIDwvdGFIbGU+CIAgPC9ib2R5Pgo8L2h0bWw+Cg==  
-----_Part_80_1790905162.1649808715729--
```

Cancel Import

2.3 Landing Pages

X

! Page name already in use

<http://ti>

为了防止怀疑。为了防止用户在输入凭据后变得可疑，您可能希望将他们重定向到原始

URL。

Gophish 可以在用户提交凭据后轻松重定向用户。要重定向用户，请在选中“捕获提交的数据”复选框后出现的“重定向到：”文本字段中输入 URL。

2.4 Sending Profiles

要发送电子邮件，Gophish 要求您配置称为“发送配置文件”的 SMTP 中继详细信息。

要设置发送配置文件，请单击侧栏中的“发送配置文件”导航条目，然后单击“新建配置文件”按钮。我的邮件服务器和钓鱼网站部署在一台机器上，所以设置127.0.0.1

New Sending Profile

×

Name:

Profile

Interface Type:

SMTP

From:

admin@test.com

Host:

127.0.0.1

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

Name: Name字段是为新建的发件策略进行命名，不会影响到钓鱼的实施，建议以发件邮箱为名字，例如使用qq邮箱来发送钓鱼邮件，则Name字段可以写 xxxxxx@qq.com。

Interface Type: Interface Type 是接口类型，默认为 SMTP类型 且不可修改，因此需要发件邮箱开启SMTP服务From: From 是发件人，即钓鱼邮件所显示的发件人。（在实际使用中，一般需要进行近似域名伪造）这里为了容易理解，就暂时以qq邮箱为例，所以From字段可以写: testxxxxxx@qq.com。

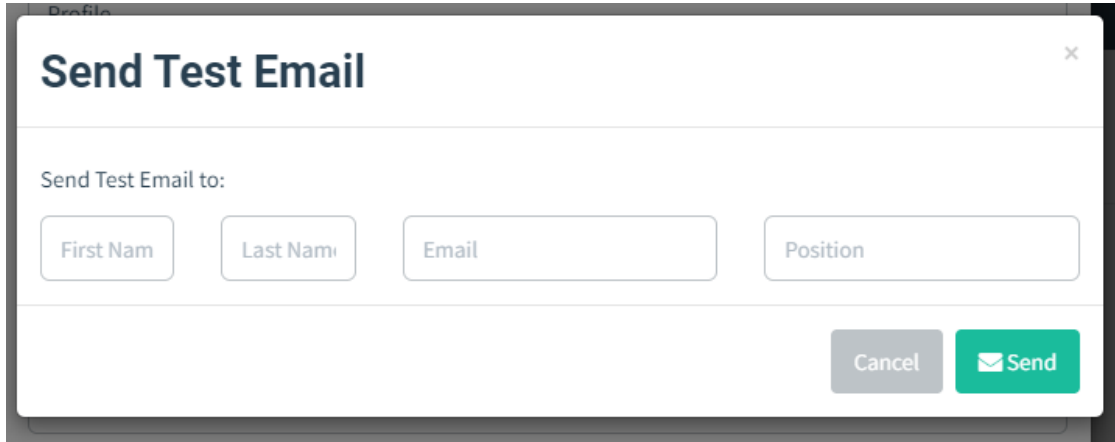
Host: Host 是SMTP服务器的地址，格式是 smtp.example.com:25，例如qq邮箱的smtp服务器地址为 smtp.qq.com。但这里要注意，如果搭建Gophish平台用的vps是阿里云的话，是不能使用25端口的，因为阿里云禁用25端口，你可以通过提工单解封，但申请通过的难度很大。所以，我们这里可以把25端口改为465端口，即填写 smtp.qq.com:465，这样就可以成功发送邮件了。

Username: Username 是SMTP服务认证的用户名，如果是qq邮箱，Username则是自己的qq邮箱号 xxxx@qq.com。

Password: Password 是SMTP服务认证的密码，例如qq邮箱，需要在登录qq邮箱后，依次点击“设置” —> “账户” —> “开启SMTP服务” —> “生成授权码” 来获取SMTP服务授权码，Password的值则填写我们收到的授权码。

由于本次测试是用的我的vps搭建的邮件服务器，所以host地址写127.0.0.1，username和password为空。

配置完成后可进行邮件发送测试

A screenshot of a 'Send Test Email' dialog box. The dialog has a title bar with a close button (X). Below the title, it says 'Send Test Email to:'. There are four input fields: 'First Name', 'Last Name', 'Email', and 'Position'. At the bottom right, there are two buttons: 'Cancel' (grey) and 'Send' (green with a white envelope icon).

2.5 Campaigns

开始钓鱼

Campaigns 的作用是将上述四个功能Sending Profiles、Email Templates、Landing Pages、Users & Groups联系起来，并创建钓鱼事件。在Campaigns中，可以新建钓鱼事件，并选择编辑好的钓鱼邮件模板，钓鱼页面，通过配置好的发件邮箱，将钓鱼邮件发送给目标用户组内的所有用户。点击“New Campaign”新建一个钓鱼事件：

New Campaign

Name: 111

Email Template: ceshi

Landing Page: xuezhe

URL: http://143:89

Launch Date: June 16th 2022, 4:10 pm

Send Emails By (Optional):

Sending Profile: Profile [Send Test Email](#)

Groups: ceshi

[Close](#) [Launch Campaign](#)

Name: Name 是为新建的钓鱼事件进行命名。

Email Template: Email Template 即钓鱼邮件模板。

Landing Page: Landing Page 即钓鱼页面。

URL (重点): URL 是用来替换选定钓鱼邮件模板中超链接的值, 该值指向部署了选定钓鱼页面的url地址。简单来说, 这里的URL需要填写当前运行Gophish脚本主机的IP。因为启动Gophish后, Gophish默认监听了3333端口和80端口(我们这配置的是81端口), 其中3333端口是后台管理系统, 而89端口就是用来部署钓鱼页面的。当URL填写了http://主机IP/, 并成功创建了当前的钓鱼事件后, Gophish会在主机的81端口部署当前钓鱼事件所选定的钓鱼页面, 并在发送的钓鱼邮件里, 将其中所有的超链接都替换成部署在81端口的钓鱼页面的url。所以, 这里的URL填写我本地当前运行Gophish的vps主机IP和端口, 即我这里是http://47.xxx.xxx.72:81/。

Launch Date: Launch Date 即钓鱼事件的实施日期, 通常如果仅发送少量的邮箱, 该项不需要修改。如果需要发送大量的邮箱, 则配合旁边的“Send Emails By”效果更佳。

Send Emails By (可选): Send Emails By 配合Launch Date使用, 可以理解为当前钓鱼事件下所有钓鱼邮件发送完成的时间。Launch Date作为起始发件时间, Send Emails By 作为完成发件时间, 而它们之间的时间将被所有邮件以分钟为单位平分。例如, Launch Date的值为2020.07.22,09:00, Send Emails By的值为 2020.07.22,09:04, 该钓鱼事件需要发送50封钓鱼邮件。那么经过以上设定, 从9:00到9:04共有5个发件点, 这5个发件点被50封邮件平分, 即每个发件点将发送10封, 也就是每分钟仅发送10封。这样的好处在于, 当需要发送大量的钓鱼邮件, 而发件邮箱服务器并未限制每分钟的发件数, 那么通过该设定可以限制钓鱼邮件不受约束的发出, 从而防止因短时间大量邮件抵达目标邮箱而导致的垃圾邮件检测, 甚至

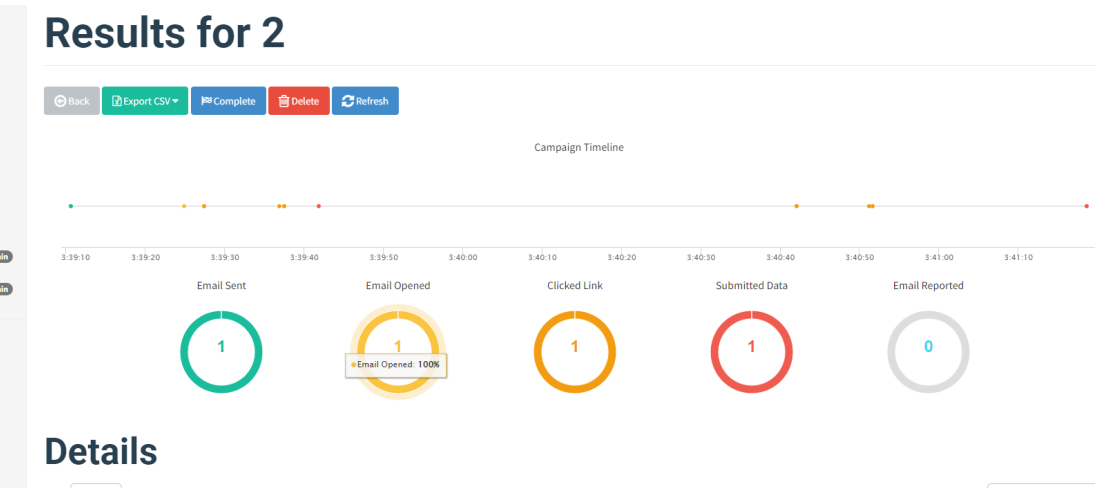
发件邮箱服务器IP被目标邮箱服务器封禁。

Sending Profile：Sending Profile 即上文中我们配置的发件邮箱策略，这里选择刚刚编辑好的名为 发件策略profile。

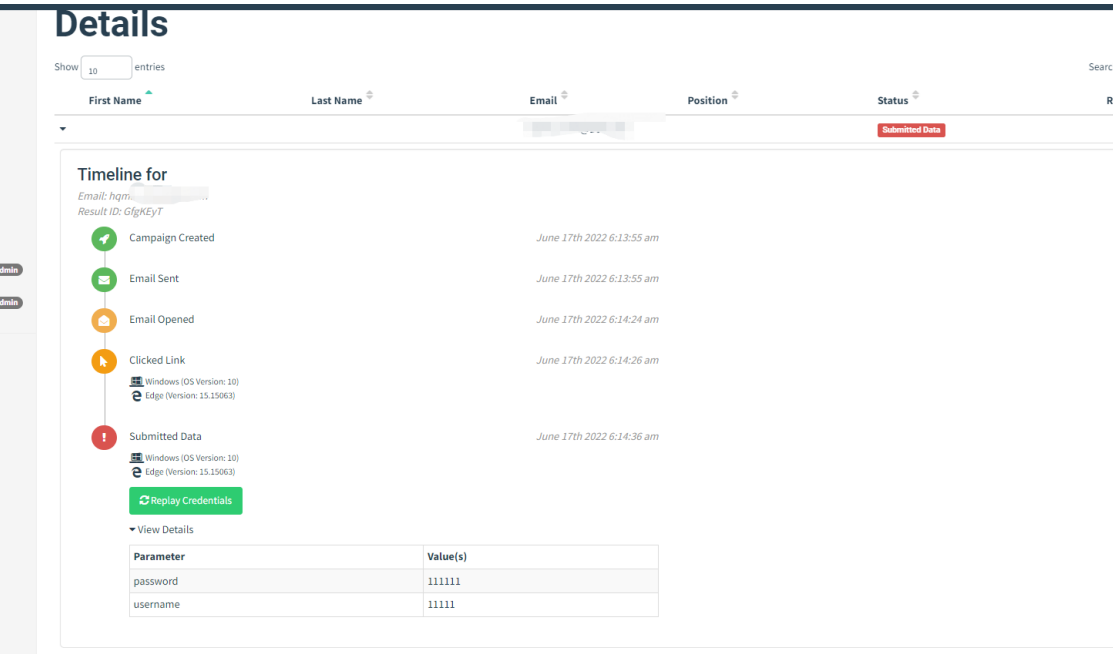
Groups：Groups 即接收钓鱼邮件的目标用户组，这里选择刚刚编辑好的名为ceshi。

填写完以上字段，点击“Launch Campaign”后将会创建本次钓鱼事件（注意：如果未修改“Launch Date”，则默认在创建钓鱼事件后就立即开始发送钓鱼邮件）：

钓鱼成功



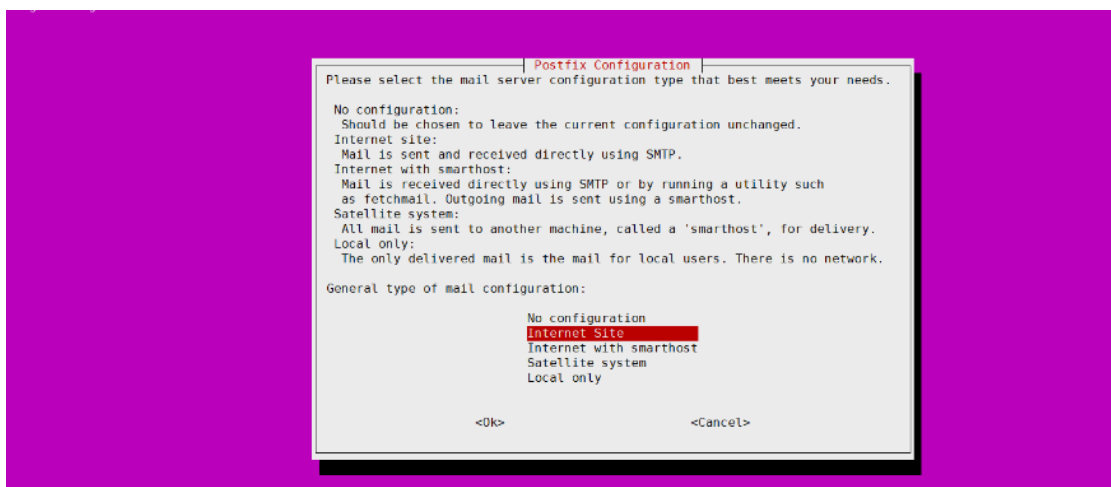
钓鱼成功过后可查看钓鱼详情：



4 邮件服务器搭建

1、安装 postfix

apt-get install postfix，安装过程只需对这一步进行配置，internet site填写注册的域名



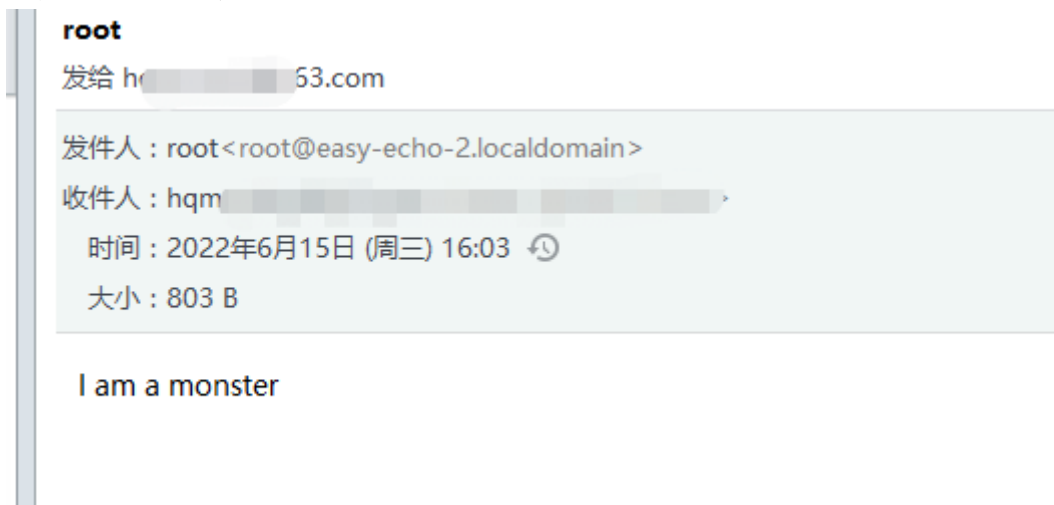
开启 postfix

service postfix start

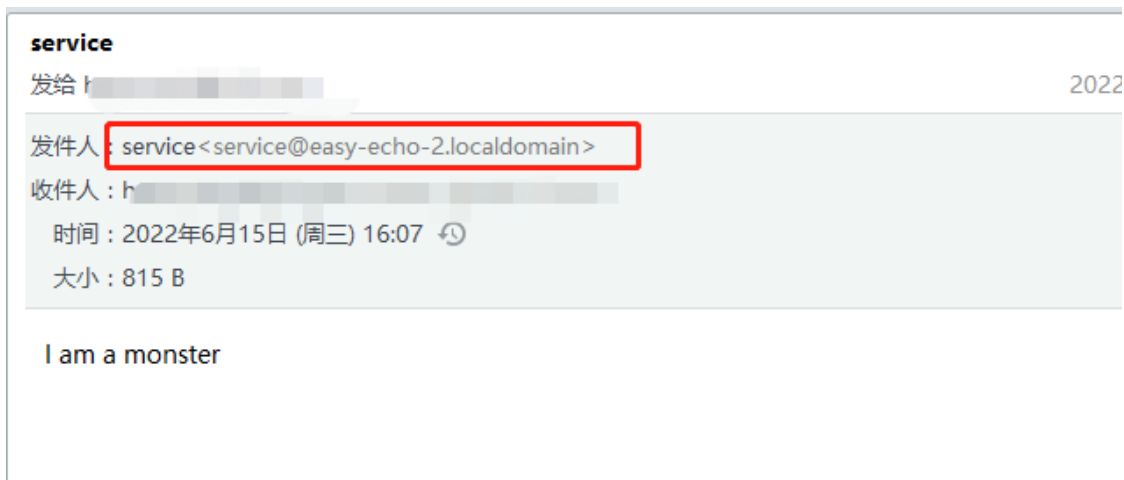
2、安装 mailx

apt-get install mailutils

安装完成后，利用echo "I am a monster" | mail -s "test" xx@163.com 进行测试，进行邮件发送，可成功收到邮件



我们需要尝试伪造发件人信息，在ubuntu新建service账户，adduser service，切换到该账户再次进行发送，可改变发件人信息



5 问题点

简单记录下搭建过程中遇到的问题，网上的搭建资料已经很多了，参考他人的搭建过程，从gophish搭建到邮箱服务器搭建都比较顺利，最后出现的两个问题都在Landing Pages搭建钓鱼页面，第一、无法获取受害者输入的数据；第二、无法点击登录按钮，这里确实很坑，找了很多资料才发现导入网站的数据必须要有form表单，需要自己修改，顿时觉得为啥别人知道我不知道，继续翻它的官方文档才发现人家的Q&A给出了答案

Q Search

Submitted Form Data Isn't Being Captured

To capture data submitted through a landing page, you need to create an HTML `<form>` element on your landing page that has a few specific properties:

Here is a minimal example `<form>` element which captures data:

```
1 <form action="" method="POST">
2   <input name="username" type="text" placeholder="username" />
3   <input name="password" type="password" placeholder="password" />
4   <input type="submit" value="Submit" />
5 </form>
```

There are a few things to note about this form:

- The action is `""` so that form submissions are directed to your phishing page and, therefore, to your Gophish server
- The form submission method is `POST`
- Each input which you expect to see in Gophish has a `name` attribute

Each of these should be checked when troubleshooting HTML forms that don't appear to be sending data correctly.

If you still aren't seeing your form submitted correctly, you may need to review and remove any Javascript on the page interfering with the form submission.

Finally, ensure that when saving the landing page that you have both the "Capture Submitted Data" and "Capture Passwords" (if appropriate) options checked. Otherwise, Gophish will remove the `name` attributes from your inputs so they aren't submitted with the form.

Copy link

CONTENT

Unable to Re:

How to Bypa:

Events Aren't

Submitted Fc

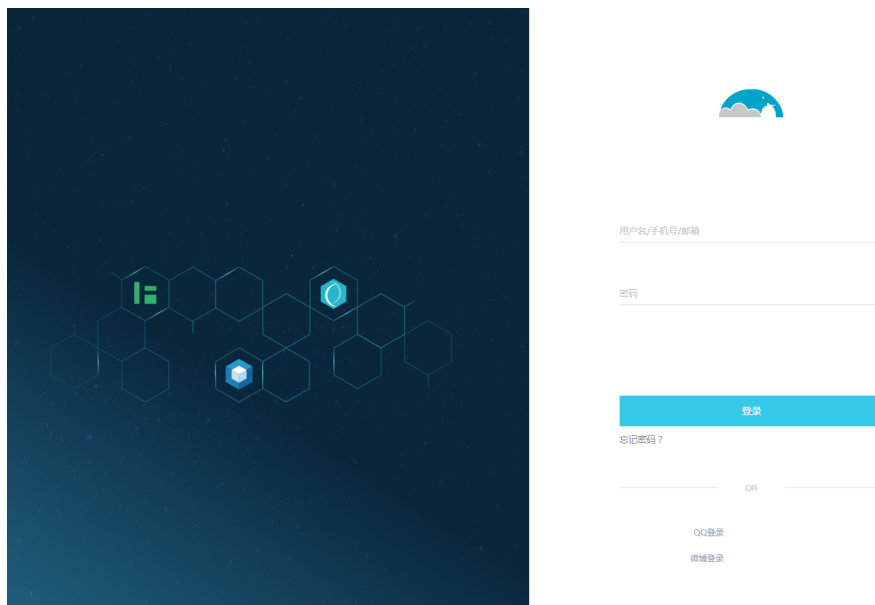
上面也提到过了Landing Pages有个比较方便的功能就是直接克隆目标url地址，所以需要在修改source中修改源码，修改为form结构，其实也比较好修改，直接调用该代码本身就能生成一个登录框如下图

```
<form action="" method="POST">
  <input name="username" type="text" placeholder="username" />
  <input name="password" type="password" placeholder="password" />
  <input type="submit" value="Submit" />
</form>
```

← → ↻ 🏠 ⓘ about:blank

username password Submit

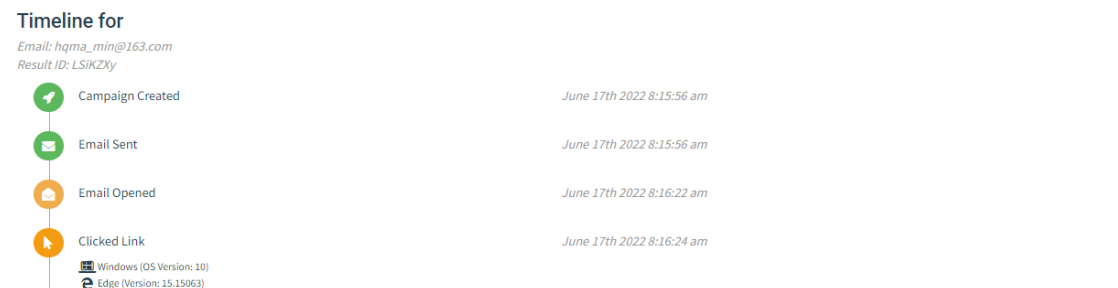
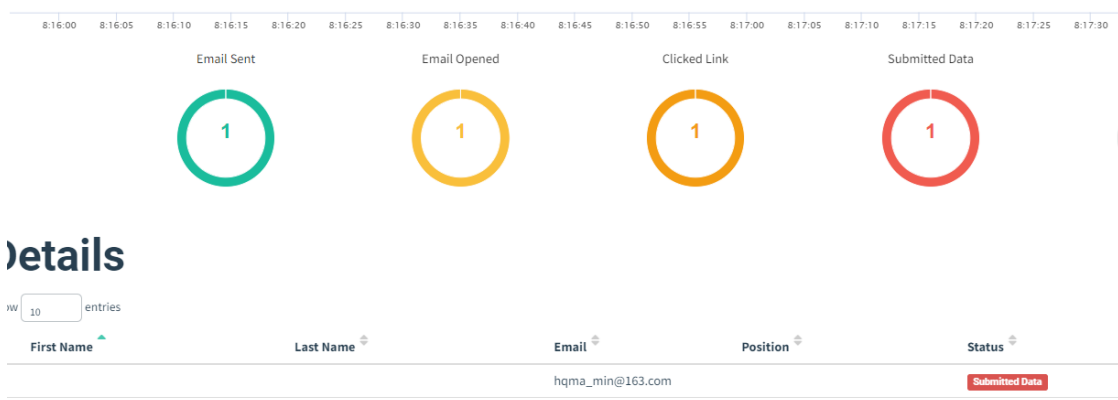
该登录框是最原始的登录框，在该基础上加入原有页面的<head>、div标签就能成功展示，如下是克隆的freebuf的登录页面



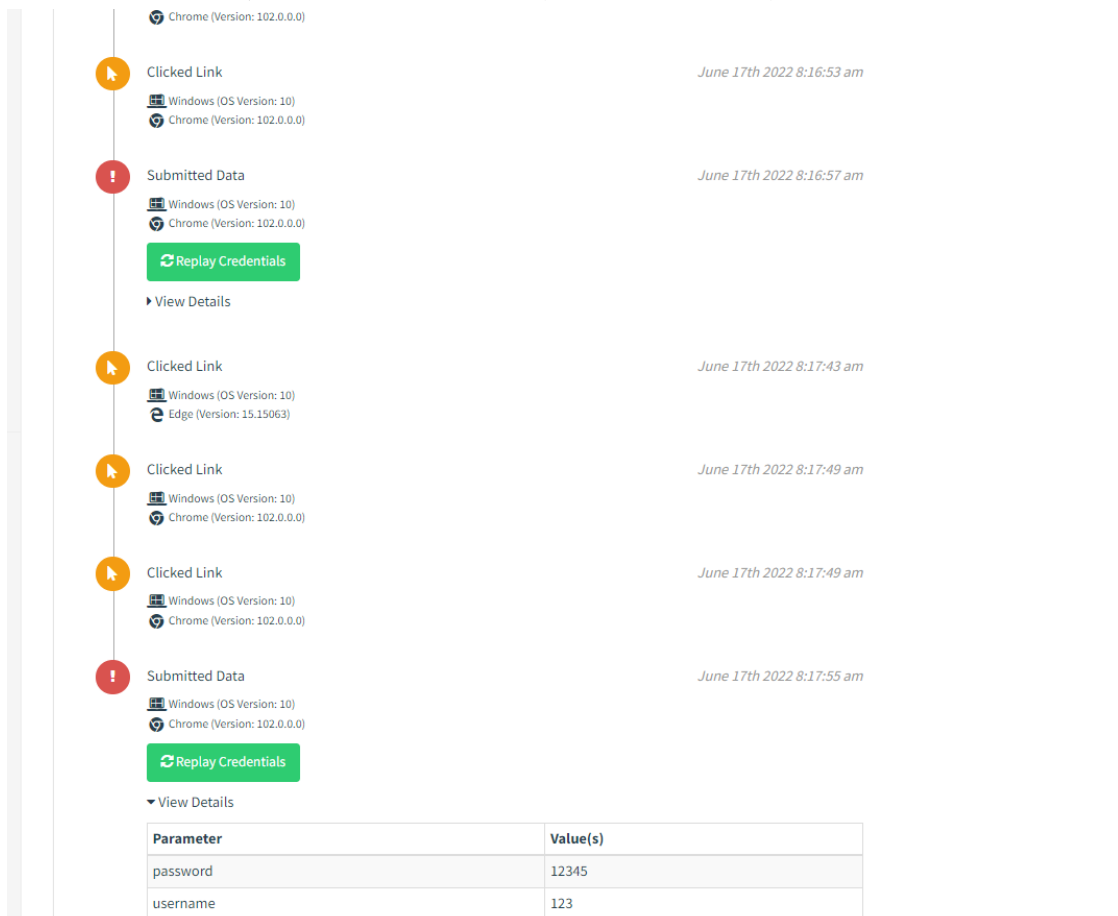
受害者收到邮件后点击相关链接调转到登录页面



受害点击后能获取到输入的相关信息



另外还发现除了以邮件形式发送该钓鱼地址，还可进行url群发，这样也能记录登录的信息



尝试了克隆了几个不同的网站，基本都需要进行源码修改，在保留原有网页情况下删除不必要的一些函数或js加载，图中标记处为需要修改的地方，有时候网页调用js脚本进行加密，但是我们需要的是明文的密码，在我们克隆的页面中可找到加密js文件，并删除调用。


```

<form class="form-horizontal" id="form_login" method="post" style="margin: inherit;" action="">
<div class="form-group">
<div class="col-sm-11"><input class="form-control" id="emp_no" name="emp_no" type="text"
placeholder="帐号"/></div>
</div>
<div class="form-group">
<div class="col-sm-11"><input class="form-control" id="password" name="password" type="password"
placeholder="密码" type="password"/></div>
</div>
<div class="form-group">
<div class="col-sm-11 row">
<div class="col-xs-8"><input class="form-control" id="verify" name="verify" placeholder="验证码"/></di
<div class="col-xs-4" style="margin-top: 2%;"><!-- </
</div>
</div>
<div class="form-group">
<div class="col-sm-12" style=""><input class="btn btn-sm btn-primary col-40" id="deng" onclick="login(
style="text-align: center;
border: none;
background: #32d37a;
color: #fff;
cursor: pointer;
font-size: 18px;
font-weight: bold;
width: 90%;
height: 40px;" type="submit" value="登 录"/></div>

```

也有时候会存在网页克隆后，页面资源打不开，这时候可把页面资源全部打包下载，放在自己的vps上，新建一个网站，然后再利用Landing Pages进行导入。

下面列举几个收集邮箱的网站：

<https://intelx.io>

<https://phonebook.cz/>

<https://hunter.io/>

<http://www.skymem.info/>

参考文章：

<https://mp.weixin.qq.com/s/ZU8LrUENEnCSX9Q9ZxiyyA>

<https://security.tencent.com/index.php/blog/msg/165>

<https://xz.aliyun.com/t/11400>