Now everyone talks about bitcoin and crypto-currencies. My acquaintance with crypto-currencies occurred about 5 months ago, that's when I started investing in bitcoin and ethereum, the rate at that time was $1900 for BTC and $89 for eth. In order for you to understand what profit I got, I will say that today bitcoin costs **$18 000**, and eth **$830** and continues to go into orbit along with the rest of the crypto-currencies. I thought that it would be great to see how safe the services are, where my savings are, whether I trade them or give them to trust management.

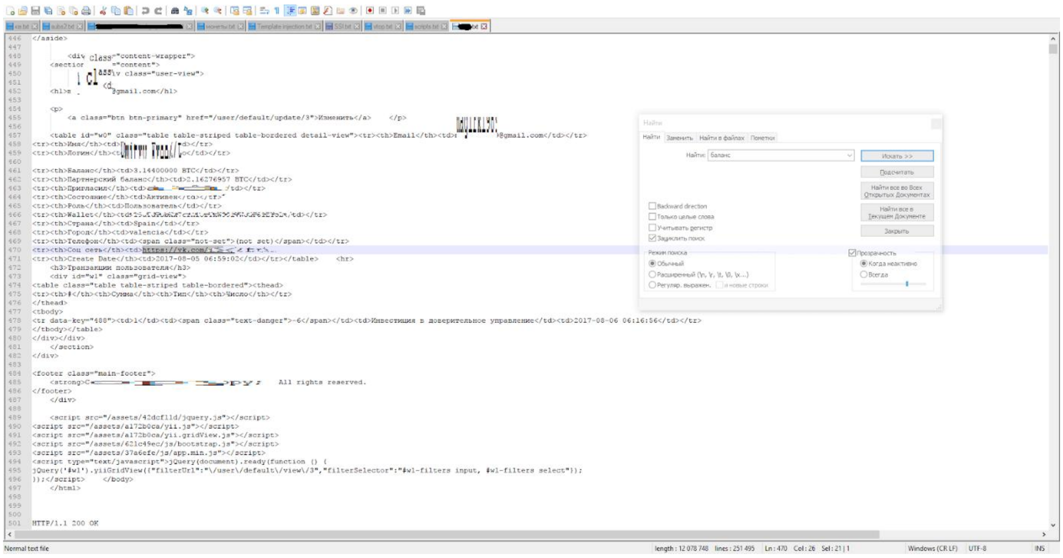
Back in the late spring, I bought access for $500 to insiders of one investment club. I bought more coins for my own, this is besides ether and bitcoin, and at the end of August I received a recommendation that one can give his bitcoins to traders at 15% per month, that was why I started my way from sites which were engaged in trust management (further in the article — TM).

The first company **example1.com** (they forbade disclosing the names associated with their websites) is very popular and is known for many investors. Before investing money there, I decided to check my account for vulnerabilities. Registered, but surprisingly — did not find anything, everywhere filtering, csrf tokens and so on. Then I registered another account, but instead of the name, I entered js sniffer. For a long time, nothing came to me, I already was reconciled to the fact that the project is doing well with security, there are no BLIND XSS and other things, but only until the logs came to me (source code, admin IP, local storage, etc.)

JS was executed when the admin checked the page with data about the user http://admin.example1.com/user/default/index?page=75. Similar vulnerabilities are increasingly encountered on hackerone, an example here https://hackerone.com/reports/251224.

Looking through the logs, I was upset because all the cookies with the httponly flag and could not get any, at the end — I would not be able to access the admin panel, but when I clicked the link http://admin.example1.com/user/default/index?page=75, I saw that **admin panel could be used without authorization**, this was a gross developer error (vulnerability Improper Access Control).

In total it was possible to view and change information about **2010** users (email, phone, links to the social network, bitcoin wallet address, login, balance, referrer). In the screenshot, one of the richest investors in my club, he has a large number of subscribers and I constantly follow his blog. He recommended all his subscribers to invest their money in this TM, of course on a referral link, but not more than 20% of the capital. After a short time, he managed to earn 20 bitcoins on this, which equals **$ 227 000 for today.**



```
</aside>

        <div class="content-wrapper">
    <section class="content">
        <div class="user-view">
    <h1>[redacted]@gmail.com</h1>

    <p>
        <a class="btn btn-primary" href="/user/default/update/3">Изменить</a>    </p>

    <table id="w0" class="table table-striped table-bordered detail-view"><tr><th>Email</th><td>[redacted]@gmail.com</td></tr>
<tr><th>Имя</th><td>[redacted]</td></tr>
<tr><th>Логин</th><td>[redacted]</td></tr>

<tr><th>Баланс</th><td>3.14400000 BTC</td></tr>
<tr><th>Партнерский баланс</th><td>2.16276957 BTC</td></tr>
<tr><th>Пригласил</th><td>[redacted]</td></tr>
<tr><th>Состояние</th><td>Активен</td></tr>
<tr><th>Роль</th><td>Пользователь</td></tr>
<tr><th>Wallet</th><td>[redacted]</td></tr>
<tr><th>Страна</th><td>Spain</td></tr>
<tr><th>Город</th><td>valencia</td></tr>
<tr><th>Телефон</th><td><span class="not-set">(not set)</span></td></tr>
<tr><th>Соц сеть</th><td>https://vk.com/[redacted]
<tr><th>Create Date</th><td>2017-08-05 06:59:02</td></tr></table>    <hr>
    <h3>Транзакции пользователя</h3>
    <div id="w1" class="grid-view">
<table class="table table-striped table-bordered"><thead>
<tr><th>#</th><th>Сумма</th><th>Тип</th><th>Число</th></tr>
</thead>
<tbody>
<tr data-key="488"><td>1</td><td><span class="text-danger">-6</span></td><td>Инвестиция в доверительное управление</td><td>2017-08-06 06:16:56</td></tr>
</tbody></table>
</div></div>
    </section>
</div>

<footer class="main-footer">
    <strong>C[redacted]    All rights reserved.
</footer>
    </div>

    <script src="/assets/42dcf11d/jquery.js"></script>
<script src="/assets/a172b0ca/yii.js"></script>
<script src="/assets/a172b0ca/yii.gridView.js"></script>
<script src="/assets/621c49ec/js/bootstrap.js"></script>
<script src="/assets/37a6efe/js/app.min.js"></script>
<script type="text/javascript">jQuery(document).ready(function () {
jQuery('#w1').yiiGridView({"filterUrl":"\/user\/default\/view\/3","filterSelector":"#w1-filters input, #w1-filters select"});
});</script>    </body>
    </html>



HTTP/1.1 200 OK
```

Найти

Найти | Заменить | Найти в файлах | Пометки

Найти: баланс

□ Backward direction
□ Только целые слова
□ Учитывать регистр
☑ Зациклить поиск

Режим поиска
● Обычный
○ Расширенный (\n, \r, \t, \0, \x...)
○ Регуляр. выражен. □ и новые строки

☑ Прозрачность
● Когда неактивно
○ Всегда

Искать >>
Подсчитать
Найти все во Всех Открытых Документах
Найти все в Текущем Документе
Закрыть

Normal text file    length : 12 078 748    lines : 251 495    Ln : 470    Col : 26    Sel : 21 | 1    Windows (CR LF)    UTF-8    INS

The attacker without any training or experience could easily go to the admin panel and change the email addresses of all the investors to their own (or simply change wallets for withdrawal, so as not to cause unnecessary suspicion when the victim decides to withdraw money for the wallet for some reason in deriving not displayed). Investors are large enough there, many of them have deposits >0.5btc. It is very strange that in the admin panel there are no passwords in the clear form.

I have a feeling that the developers of this TM are capable of anything at all in terms of deteriorating the security of their service.
After discovering the vulnerability, I sent a report to the developers, they contacted the creator and fixed the vulnerability. I was offered to charge the award on the account in their website, where I will receive % and in half a year I will be able to break into a breakeven, and in a year I will take the body itself. A month later, when I found a similar blind xss in their service and got another bounty for it, it was found out that the developers of the TM were fired (and they did not seem to have paid money for their work at that time), other people began to develop it.

A little later, after the first recommendation, the second has come (**example2.com**). This is also a top, popular service of trust management, he has 20 000 Alexa rank World and 3 000 Russia.

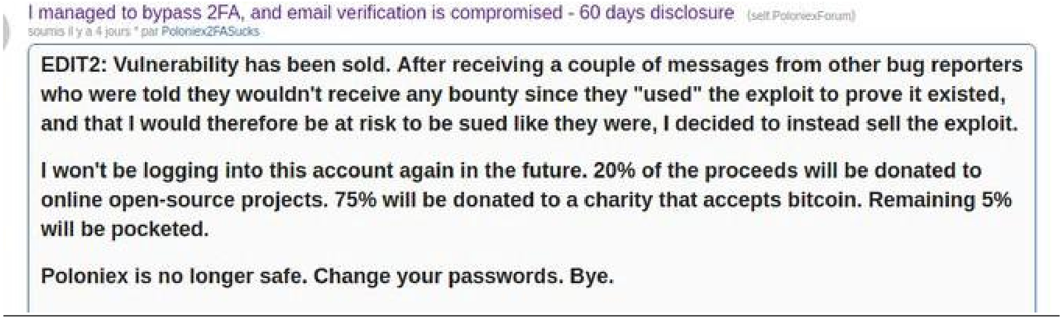
Thoroughly checking everything — nothing was found (even my favorite clickjacking ), except for two CSRF vulnerabilities in post requests. The first allowed to change the details for the withdrawal of funds, the user just had to click on the link to the CSRF exploit. The second allowed to withdraw the user's money to the already changed details. Thus, if a user simply goes through the link, he will lose all his money. How was the attack possible? An attacker could hire a specialist in social engineering, spam the participants of their chat in a telegram and get a good profit.

Immediately after the discovery, I wrote to the developers of the site, I also asked friends from the club to write to the owner. The developers responded that allegedly due to the fact that the user needed to go to the link — the vulnerability was absolutely not dangerous. It looked funny. After that, I wrote a couple more letters with the evidence that the bug was still worth attention and it must be fixed immediately, but I was ignored.

A little later, there were quite predictable things for projects of this kind — user details began to change in mass, I learned about it from their developer, who wrote to me just a couple of days ago (as I understood from his words — the users themselves made the withdrawal and the funds began to disappear). It is terrible to imagine losses in the event that hackers involved a vulnerability in the withdrawal of funds. The developer asked again to send a report on the vulnerability, then google recaptcha was added to the form of change of details and confirmation by SMS (for sure).

After that, I decided to look for vulnerabilities on **crypto-currency exchanges.**

Poloniex I decided not to touch, they do not pay for the vulnerability and capital I do not keep there, it is because of their ignoring of security problems — the vulnerability bypass two-factor authentication was sold in a darknet, the link is https://twitter.com/misterch0c/status/897756404093726720:



I managed to bypass 2FA, and email verification is compromised - 60 days disclosure (self.PoloniexForum)
soumis il y a 4 jours * par Poloniex2FASucks

**EDIT2: Vulnerability has been sold. After receiving a couple of messages from other bug reporters who were told they wouldn't receive any bounty since they "used" the exploit to prove it existed, and that I would therefore be at risk to be sued like they were, I decided to instead sell the exploit.**

**I won't be logging into this account again in the future. 20% of the proceeds will be donated to online open-source projects. 75% will be donated to a charity that accepts bitcoin. Remaining 5% will be pocketed.**

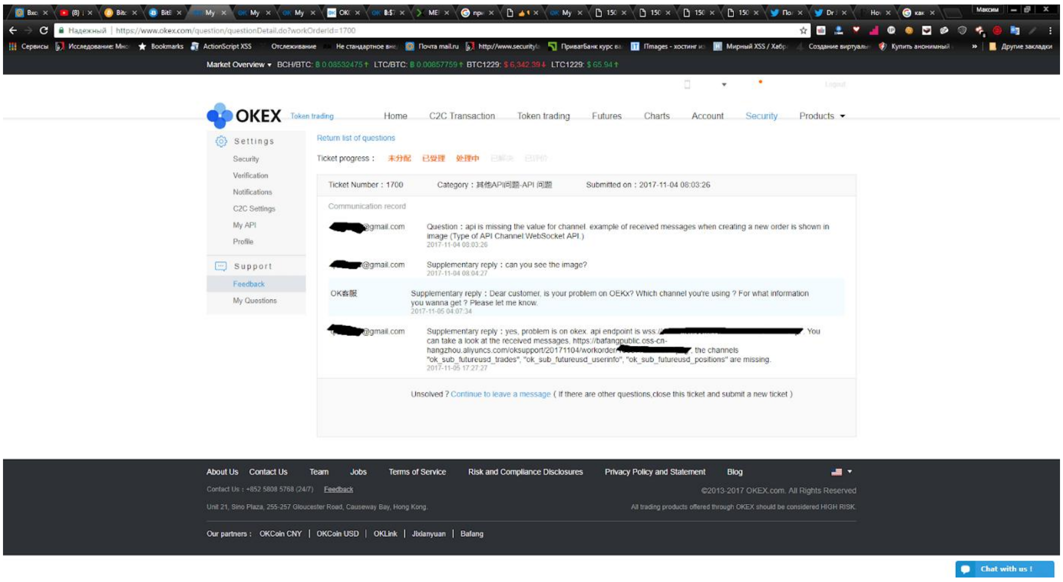
**Poloniex is no longer safe. Change your passwords. Bye.**

Earlier I had $ 6000 on my account, quite by accident I went to my account from vpn Moldova, as a result — my account was immediately blocked. I had to wait for a fortnight to unlock, after this case I brought out all my money from there. It was good that they hadn't taken it to themselves, as they did with many customers.

I decided to start with livecoin.net. The exchange proved to be well protected, found only low-impact **SELF XSS** vulnerability (it remained self, clickjacking on the site and csrf in the post request is not present). I was paid **$ 200 by fiat fund.**

Then I decided to go to okex.com. This exchange is very popular not only in China but all over the world. Some functionality is not fully translated into English, it is in Chinese, but it did not become a problem, the google translator extension helped me to quickly extract text and translate it without leaving the page. As in all other cases — I carefully checked security, including subdomains and directories. It turned out that https://www.okcoin.com/(6000 Alexa china), https://www.okcoin.cn/ (9000 worldwide, 2000 in China) have exactly the same design and functionality as okex. This means that if I find a vulnerability on one of their sites, then the rest will also be exposed to it. Later I've looked in the user support (a little fantasy about how I load the shell into the ticket and it is running) and I've found a lot of vulnerabilities. I'll talk about them below:

1. Vulnerability **iDOR** https://www.okex.com/question/questionDetail.do?workOrderId=2550, allowed to view all 2500 okex tickets for that time, today the number has increased to 4898, and these are only tickets on one exchange. The ticket displays the full phone number, email, real name, text of the correspondence between the user and the support and the full path to the attachment.



https://www.okex.com/question/questionDetail.do?workOrderId=1700

Market Overview ▾ BCH/BTC: B 0.08532475↑ LTC/BTC: B 0.00857759↑ BTC1229: $ 6,342.39↓ LTC1229: $ 65.94↑

Return list of questions

Ticket progress： 未分配 已受理 处理中 已解决 已评价

Ticket Number：1700 Category：其他API问题-API 问题 Submitted on：2017-11-04 08:03:26

Communication record

[redacted]@gmail.com Question：api is missing the value for channel. example of received messages when creating a new order is shown in image (Type of API Channel:WebSocket API.)
2017-11-04 08:03:26

[redacted]@gmail.com Supplementary reply：can you see the image?
2017-11-04 08:04:27

OK客服 Supplementary reply：Dear customer, is your problem on OEKx? Which channel you're using？For what information you wanna get？Please let me know.
2017-11-05 04:07:34

[redacted]@gmail.com Supplementary reply：yes, problem is on okex. api endpoint is wss://[redacted]. You can take a look at the received messages. https://bafangpublic.oss-cn-hangzhou.aliyuncs.com/oksupport/20171104/workorder[redacted], the channels "ok_sub_futureusd_trades", "ok_sub_futureusd_userinfo", "ok_sub_futureusd_positions" are missing.
2017-11-05 17:27:27

Unsolved？Continue to leave a message（If there are other questions,close this ticket and submit a new ticket）

About Us Contact Us Team Jobs Terms of Service Risk and Compliance Disclosures Privacy Policy and Statement Blog

Contact Us：+852 5808 5768 (24/7) Feedback

©2013-2017 OKEX.com. All Rights Reserved

Unit 21, Sino Plaza, 255-257 Gloucester Road, Causeway Bay, Hong Kong.

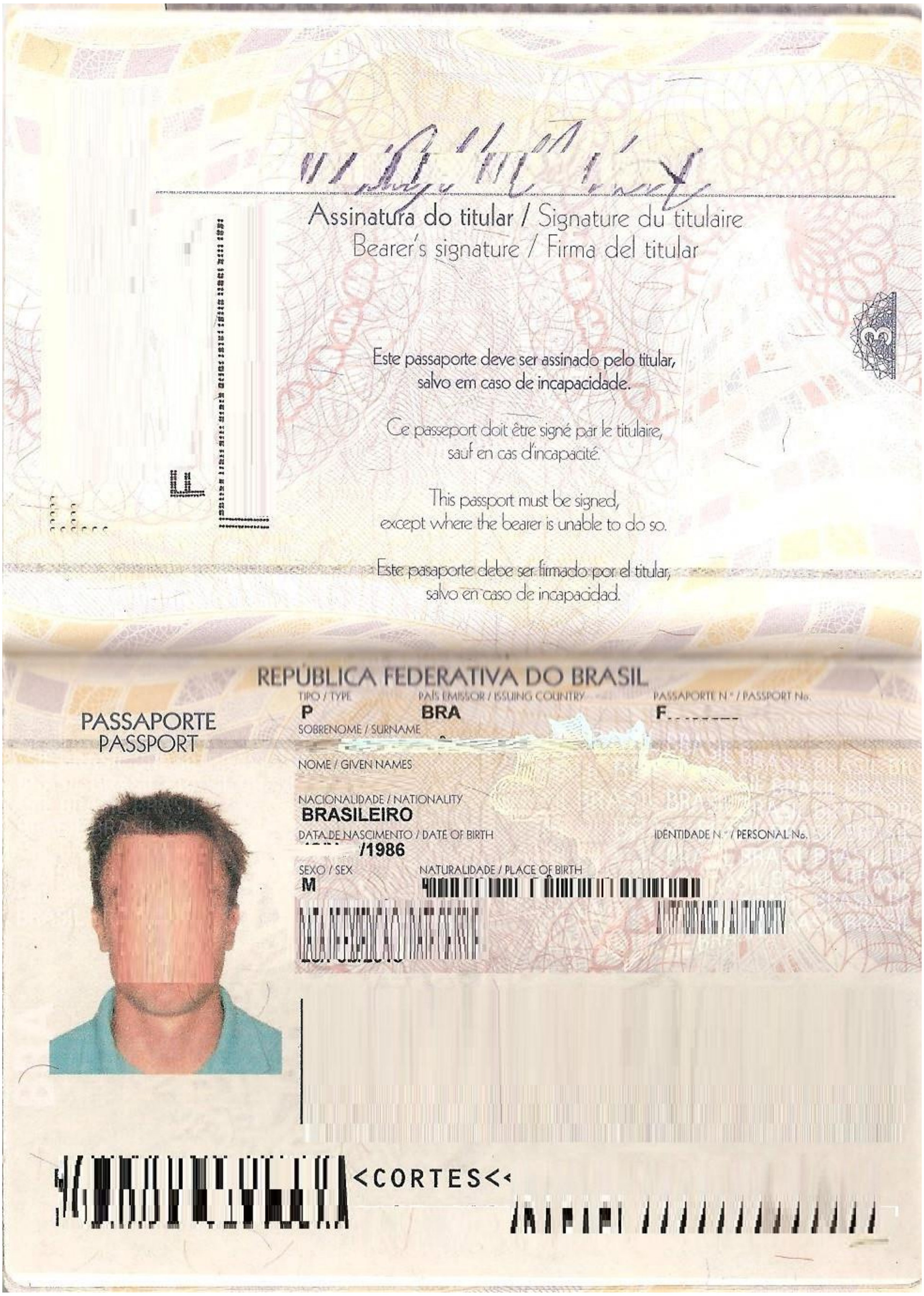
All trading products offered through OKEX should be considered HIGH RISK.

Our partners： OKCoin CNY | OKCoin USD | OKLink | Jixianyuan | Bafang

Chat with us！

As it turned out later, many users undergo the verification procedure in the support service in order to increase their withdrawal limit. It is necessary to attach the person with the passport, or simply a photo of the passport.

Here are some of these photos (Data is hidden):



[redacted]

Assinatura do titular / Signature du titulaire
Bearer's signature / Firma del titular

Este passaporte deve ser assinado pelo titular, salvo em caso de incapacidade.

Ce passeport doit être signé par le titulaire, sauf en cas d'incapacité.

This passport must be signed, except where the bearer is unable to do so.

Este pasaporte debe ser firmado por el titular, salvo en caso de incapacidad.

REPÚBLICA FEDERATIVA DO BRASIL

PASSAPORTE
PASSPORT

TIPO / TYPE
P

PAÍS EMISSOR / ISSUING COUNTRY
BRA

PASSAPORTE N.º / PASSPORT No.
F[redacted]

SOBRENOME / SURNAME
[redacted]

NOME / GIVEN NAMES
[redacted]

NACIONALIDADE / NATIONALITY
BRASILEIRO

DATA DE NASCIMENTO / DATE OF BIRTH
[redacted]/1986

IDENTIDADE N.º / PERSONAL No.

SEXO / SEX
M

NATURALIDADE / PLACE OF BIRTH
[redacted]

DATA DE EXPEDIÇÃO / DATE OF ISSUE
[redacted]

AUTORIDADE / AUTHORITY
[redacted]

[redacted]<CORTES<<
[redacted]

姓名 赵[redacted]

[redacted]

出生 1982 [redacted]

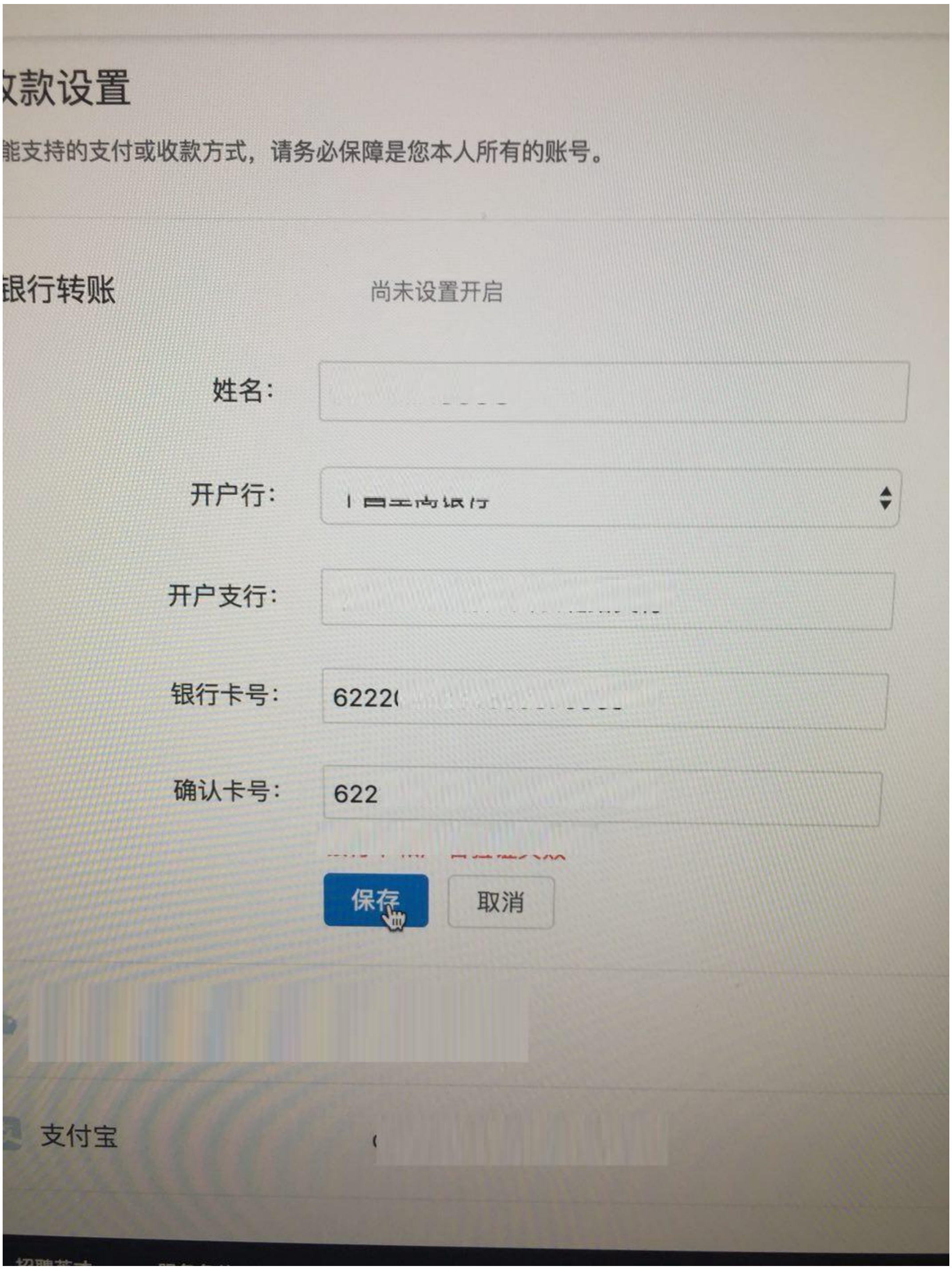
住址 [redacted]

公民身份号码 22[redacted]

姓名 赵[redacted]
性别 民族
出生 1994 年 [redacted]
住址 [redacted]
头布外屯23号
公民身份号码 45[redacted]

姓名 昊昊
性别 男 民族 汉
出生 1981 [redacted]
住址 [redacted]
公民身份号码 51[redacted]

In addition to passports, there are also a lot of photos and screenshots from the device screens.



收款设置

能支持的支付或收款方式，请务必保障是您本人所有的账号。

银行转账 尚未设置开启

姓名：[redacted]

开户行：[redacted]

开户支行：[redacted]

银行卡号：6222[redacted]

确认卡号：622[redacted]

[redacted]

[redacted]

支付宝 [redacted]

I proceeded to download all the tickets (used as evidence of the criticality of this problem). I used Burp Intruder, launched and put from 1 to 2549 to url /question/questionDetail.do?workOrderId=2550. Found that no information was downloaded. I decided to go back to the support and still intercept the requests. At that time I found out that the page loading was done via get https://www.okex.com/v2/support/cs/work-order/2550/replies. I threw this request into the intruder and downloaded all the tickets, now they could be freely sent to the developers of exchanges.

2. **Stored** **XSS** in api. Our js is not displayed in the ticket itself /question/questionDetail.do?workOrderId=2550, apparently, there was a filtering on forbidden characters. But in api /question/questionDetail.do? workOrderId=2550 everything worked fine, even js from third-party domains was loaded.

If you combine 1 and 2 vulnerabilities, you can successfully steal a lot of money. The attack was supposed to proceed according to this scenario:

1) We collect all email addresses.

2) On our page, we embed a js / html redirect to the phishing site of theexchange itself (in this case there are several exchanges and for each one will need to make a form), Myetherwallet, blockchain.info, etc.

Some attackers have come to the point that immediately after entering the login and password on poloniex.com / bittrex.com / blockchain.info, the victim is asked for her 2FA code (from google authenticator) every 15 seconds (to log in to the account, to withdraw funds), to respond to the 2FA input is necessary very quickly, because its validity expires after a short period of time. Thus, using unicode characters, replacing some letters, for example i on L (BITTREX.com, POIONIEX.COm), registering the exchange on a different domain (for example, poloniex.com.ua), creating applications on android and advertising in search engines, in 2017 criminals stole from users more than $80 million.

3) Send letters to email addresses that we have agreed in advance withthe person versed in social engineering. Users should believe in the letter and follow the link, as it did not lead to a third-party site, but to the crypto currency exchange.

4) ??

5) We get data for the entry, now withdraw the money.

3. iDOR in adding a comment, we can add a message on behalf of the userwho created the ticket.

Short Request:

POST /v2/support/cs/work-order/reply HTTP/1.1 Host:

http://www.okcoin.com *workId=718&content=test_message*

4. **Html injection** in the HTML file that was attached to the ticket, but on the domain bafangpublic.oss-cn-hangzhou.aliyuncs.com. The domain is no longer available and whois says that it belongs to Hangzhou Alibaba Advertising Co., Ltd.

5. Disclosure information. I noticed that the developers of exchanges wantto hide the user’s phone number as much as possible while criminals hacking the account. On the security page, the phone is displayed as 636818 ****, in cookies it is 6 * 6. But in the response of the api support service /v2/support/cs/work-order/2550/replies it completely displays, so it’s not good.

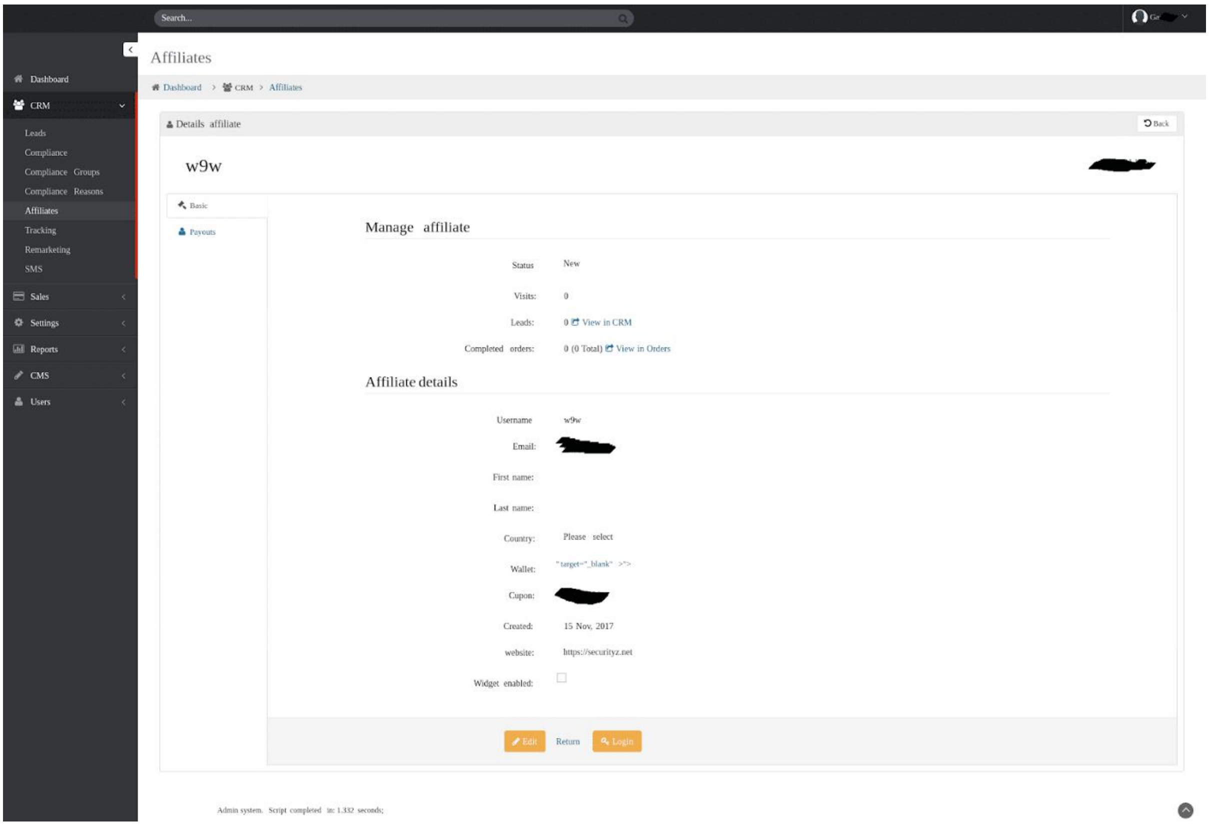
I understand that all exchanges have one owner and there is no point in writing to everyone separately, so I sent a report to the chat and to the email of the okex exchange. Very quickly received a message from official account okex in twitter and vulns have been fixed.

Then I started testing the example3.com exchange. The Exchange did not allow disclosing information about vulnerabilities, I quote:

> *Regarding posting on your blog, we would appreciate if you do not do this at the moment. Our site is not 100% secure yet.*

Discovered **XSS** in the wallet, , namely — in the affiliate program department, it turned out to make it from self XSS to stored XSS using csrf exploit, it was possible to steal cookies since there was no httponly flag. I could attach a video that I had already recorded, but I can’t — the name of the exchange is revealed there.

For this XSS in the support service I was offered $ 100, but almost at the same time on the sniffer came logs from their domain for employees.



Affiliates

Details affiliate

w9w [redacted]

Manage affiliate

Status New

Visits: 0

Leads: 0 View in CRM

Completed orders: 0 (0 Total) View in Orders

Affiliate details

Username w9w

Email: [redacted]

First name:

Last name:

Country: Please select

Wallet: "target="_blank" >">

Cupon: [redacted]

Created: 15 Nov, 2017

website: https://securityz.net

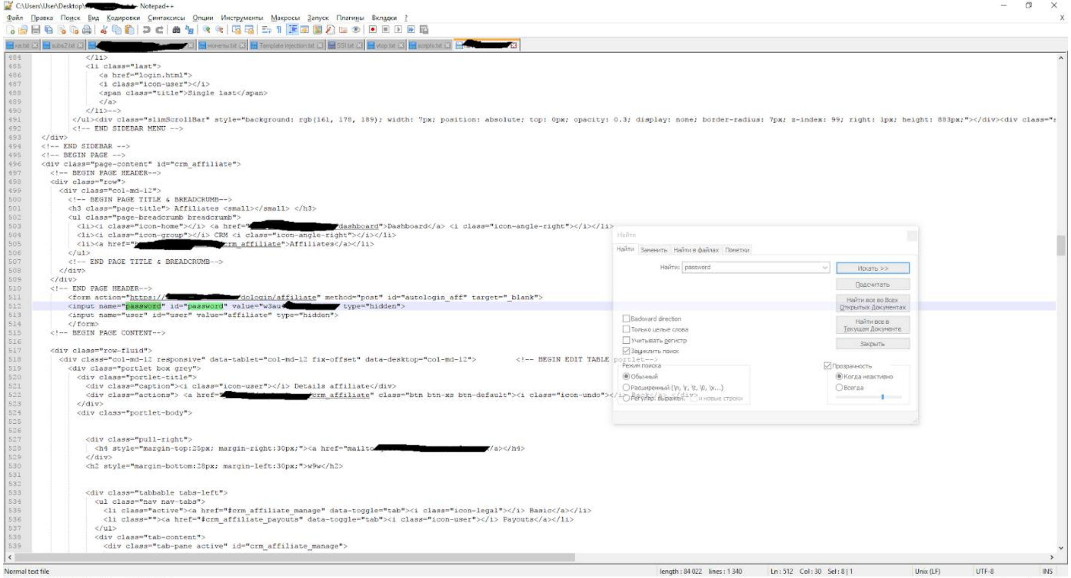
Widget enabled: □

Admin system. Script completed in: 1.332 seconds;

In the logs there was only a cookie

AWSELB=2EB3B1851EC08CCFEEC18E2DB93AE1EF2A69A2A2F9D65DCC84A B785C7C7773319F1F769CCF35CA8F430D5785D5AE4AB2C48C46EE6BE8F3 3Cy293D40F3CCA9F92E38E62AA65

**session cookie** (most important) was missing, we can not get into the admin panel through the substitution of cookies. I carefully checked the report and found the administrator’s login and password in the source code.



C:\Users\User\Desktop\[redacted] - Notepad++
Файл Правка Поиск Вид Кодировки Синтаксисы Опции Инструменты Макросы Запуск Плагины Вкладки ?
xe.txt
subs2.txt
[redacted]
монеты.txt
Template injection.txt
SSI.txt
vtop.txt
scripts.txt
[redacted]
Найти
Найти Заменить Найти в файлах Пометки
Искать >>
Подсчитать
Найти все во всех Открытых Документах
Найти все в Текущем Документе
Закрыть
□ Backward direction
□ Только целые слова
□ Учитывать регистр
☑ Зациклить поиск
Режим поиска
● Обычный
○ Расширенный (\n, \r, \t, \0, \x...)
○ Регуляр. выражен. □ . и новые строки
☑ Прозрачность
● Когда неактивно
○ Всегда
Normal text file
length : 84 022 lines : 1 340
Ln : 512 Col : 30 Sel : 8 | 1
Unix (LF)
UTF-8
INS

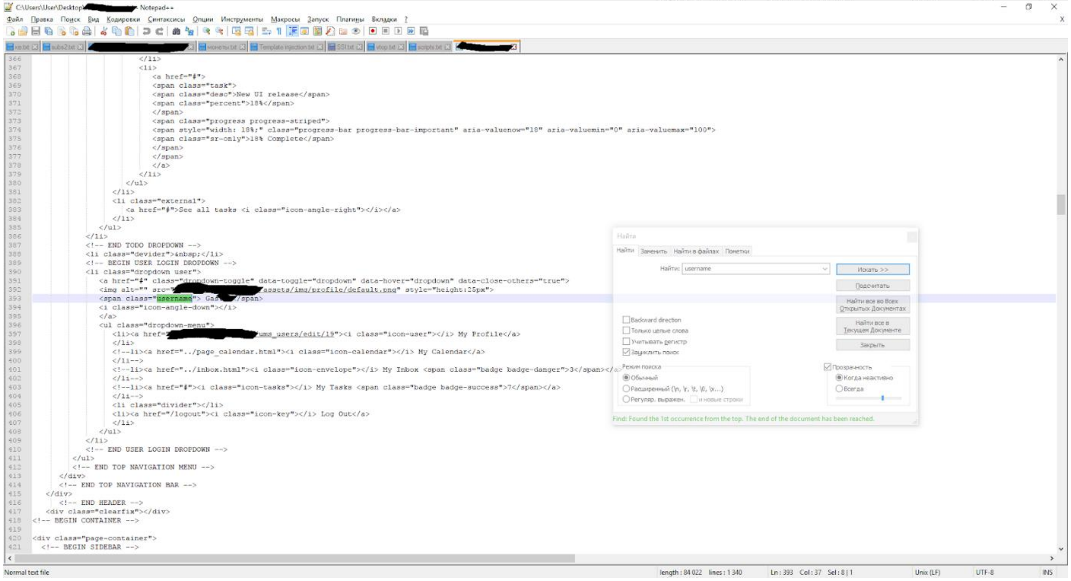
Найти: password

```
          </li>
          <li class="last">
            <a href="login.html">
            <i class="icon-user"></i>
            <span class="title">Single last</span>
            </a>
          </li>-->
        </ul><div class="slimScrollBar" style="background: rgb(161, 178, 189); width: 7px; position: absolute; top: 0px; opacity: 0.3; display: none; border-radius: 7px; z-index: 99; right: 1px; height: 883px;"></div><div class="
        <!-- END SIDEBAR MENU -->
    </div>
    <!-- END SIDEBAR -->
    <!-- BEGIN PAGE -->
    <div class="page-content" id="crm_affiliate">
      <!-- BEGIN PAGE HEADER-->
      <div class="row">
        <div class="col-md-12">
          <!-- BEGIN PAGE TITLE & BREADCRUMB-->
          <h3 class="page-title"> Affiliates <small></small> </h3>
          <ul class="page-breadcrumb breadcrumb">
            <li><i class="icon-home"></i> <a href="[redacted]dashboard">Dashboard</a> <i class="icon-angle-right"></i></li>
            <li><i class="icon-group"></i> CRM <i class="icon-angle-right"></i></li>
            <li><a href="[redacted]crm_affiliate">Affiliates</a></li>
          </ul>
          <!-- END PAGE TITLE & BREADCRUMB-->
        </div>
      </div>
      <!-- END PAGE HEADER-->
          <form action="https://[redacted]dologin/affiliate" method="post" id="autologin_aff" target="_blank">
          <input name="password" id="password" value="w3au[redacted] type="hidden">
          <input name="user" id="user" value="affiliate" type="hidden">
          </form>
      <!-- BEGIN PAGE CONTENT-->

      <div class="row-fluid">
        <div class="col-md-12 responsive" data-tablet="col-md-12 fix-offset" data-desktop="col-md-12">         <!-- BEGIN EDIT TABLE portlet-->
          <div class="portlet box grey">
            <div class="portlet-title">
              <div class="caption"><i class="icon-user"></i> Details affiliate</div>
              <div class="actions"> <a href="[redacted]crm_affiliate" class="btn btn-xs btn-default"><i class="icon-undo"></i> Back</a></div>
            </div>
            <div class="portlet-body">


              <div class="pull-right">
                <h4 style="margin-top:25px; margin-right:30px;"><a href="mailto[redacted]</a></h4>
              </div>
              <h2 style="margin-bottom:28px; margin-left:30px;">w9w</h2>


              <div class="tabbable tabs-left">
                <ul class="nav nav-tabs">
                  <li class="active"><a href="#crm_affiliate_manage" data-toggle="tab"><i class="icon-legal"></i> Basic</a></li>
                  <li class=""><a href="#crm_affiliate_payouts" data-toggle="tab"><i class="icon-user"></i> Payouts</a></li>
                </ul>
                <div class="tab-content">
                  <div class="tab-pane active" id="crm_affiliate_manage">
```



C:\Users\User\Desktop\[redacted] - Notepad++
Файл Правка Поиск Вид Кодировки Синтаксисы Опции Инструменты Макросы Запуск Плагины Вкладки ?
xe.txt
subs2.txt
[redacted]
монеты.txt
Template injection.txt
SSI.txt
vtop.txt
scripts.txt
[redacted]
Найти
Найти Заменить Найти в файлах Пометки
Искать >>
Подсчитать
Найти все во всех Открытых Документах
Найти все в Текущем Документе
Закрыть
□ Backward direction
□ Только целые слова
□ Учитывать регистр
☑ Зациклить поиск
Режим поиска
● Обычный
○ Расширенный (\n, \r, \t, \0, \x...)
○ Регуляр. выражен. □ . и новые строки
☑ Прозрачность
● Когда неактивно
○ Всегда
Normal text file
length : 84 022 lines : 1 340
Ln : 393 Col : 37 Sel : 8 | 1
Unix (LF)
UTF-8
INS

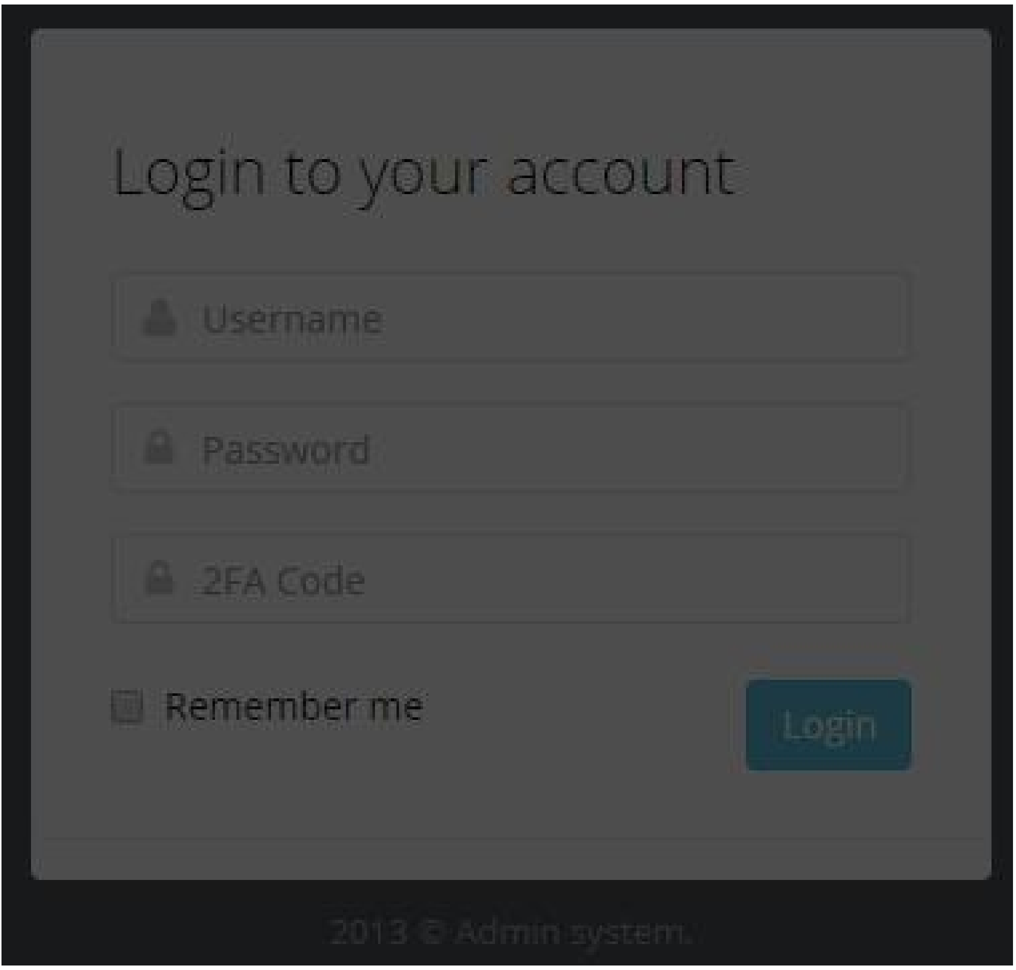
Найти: username

Find: Found the 1st occurrence from the top. The end of the document has been reached.

```
                    </li>
                    <li>
                      <a href="#">
                      <span class="task">
                      <span class="desc">New UI release</span>
                      <span class="percent">18%</span>
                      </span>
                      <span class="progress progress-striped">
                      <span style="width: 18%;" class="progress-bar progress-bar-important" aria-valuenow="18" aria-valuemin="0" aria-valuemax="100">
                      <span class="sr-only">18% Complete</span>
                      </span>
                      </span>
                      </a>
                    </li>
                  </ul>
                </li>
                <li class="external">
                  <a href="#">See all tasks <i class="icon-angle-right"></i></a>
                </li>
              </ul>
            </li>
            <!-- END TODO DROPDOWN -->
            <li class="devider">&nbsp;</li>
            <!-- BEGIN USER LOGIN DROPDOWN -->
            <li class="dropdown user">
              <a href="#" class="dropdown-toggle" data-toggle="dropdown" data-hover="dropdown" data-close-others="true">
              <img alt="" src="[redacted]assets/img/profile/default.png" style="height:25px">
              <span class="username"> Gas[redacted]</span>
              <i class="icon-angle-down"></i>
              </a>
              <ul class="dropdown-menu">
                <li><a href="[redacted]ums_users/edit/19"><i class="icon-user"></i> My Profile</a>
                </li>
                <!--li><a href="../page_calendar.html"><i class="icon-calendar"></i> My Calendar</a>
                </li-->
                <!--li><a href="../inbox.html"><i class="icon-envelope"></i> My Inbox <span class="badge badge-danger">3</span></a>
                </li-->
                <!--li><a href="#"><i class="icon-tasks"></i> My Tasks <span class="badge badge-success">7</span></a>
                </li-->
                <li class="divider"></li>
                <li><a href="/logout"><i class="icon-key"></i> Log Out</a>
                </li>
              </ul>
            </li>
            <!-- END USER LOGIN DROPDOWN -->
          </ul>
          <!-- END TOP NAVIGATION MENU -->
        </div>
        <!-- END TOP NAVIGATION BAR -->
      </div>
        <!-- END HEADER -->
      <div class="clearfix"></div>
    <!-- BEGIN CONTAINER -->

    <div class="page-container">
      <!-- BEGIN SIDEBAR -->
```

But when I went to the login page, I saw



it.

We can not get into the admin panel via username and password, you need to access the google authenticator app, or redirect to the phishing site directly from the admin area, steal its authenticator code and quickly enter it. The second option is quite realizable.

While writing a report about blind xss in the admin panel, I found:

1) CSRF vulnerability in changing details for withdrawal of partner funds,short request:

POST /affiliate_program HTTP/1.1

Host: www.example3.com
wallet=my_wallet&act=wallet a security token is not present, an

exploit was written.

2) iDOR in order removing, vulnerable request https://example3.com/account?act=cancel&order=ID_of_order. The essence of the vulnerability is that if a user has already created order and wants to transfer his bitcoins to the wallet of the exchange — we can cancel this action. At best, his order will simply retire from the system, at worst — he will transfer the bitcoins and lose his money. This vulnerability is mainly useful only for exchanges — competitors, not for hackers.

After I sent a new report in support, I was contacted by the chief security officer to discuss the vulnerabilities. He wanted to call me on Skype or on the phone, but at that moment my knowledge of English was at an average level, so we decided to limit ourselves to chat. For the vulnerability I was offered 0.1 btc ($ 1130):

> After consulting with our finance and regarding our situation, we can pay you 0.1 btc. This is the highest amount we paid for a bug and is much higher than what we usually pay. It’s to show our appreciation to you and the way you handled the situation.

I’m very grateful for the bounty. They are responsible for safety, it was very pleasant to communicate with their CTO.

**In total, with the search for vulnerabilities on these sites dealing with cryptocurrency I got:**

Trust management of example1.com: **1 BTC**.

Trust management example2.com: **0.122 BTC**.

Exchange livecoin.net: **$ 200** by fiat means.

Exchange okex.com: **2 BTC**, I’m very grateful to okex for the bounty, the Exchange’s CTO allowed to publicly disclose the vulnerability.

Exchange example3.com: **0.1 BTC**.

1 + 0.122 + 2 + 0.1 + $200 = **$59 400** from the search for the vulnerabilities on these sites dealing with crypto currency, and with the growth rate bitcoin this amount will grow.

**The conclusion from the article:** Always hire highly qualified programmers for your projects, especially if your budget allows it. In the first two cases, the companies are large enough, they can afford to hire quality specialists, but they save money and because of this, users and reputation may suffer — they leave the admin board completely “naked” and ignore the problems pointed out by the security specialist.

**P.S:** If you need a quality security audit at an affordable price, then contact me.

**P.P.S:** Also I can tell you about vulnerabilities in bug bounty on hackerone, the most interesting and dangerous of them:

1. IDOR on mail.ru, through which you could access 3,000,000 tickets inthe support service, — $1000.

2. Blind XSS on mail.ru (most likely out-of-scope), with the help of it Ihacked the admin panel, in which there were 2,100,000 users, there were not only users of mail.ru, but users from 20 online stores (also a link with OAuth was attached to each user, through which you could log into his account).

3. IDOR on the support site (private bug bounty), with which you couldaccess all tickets on > 1000 sites, — $2500.

* I will tell you about the vulnerabilities on mail.ru only from the permission of the developers, so far I have not received it.