

# **HACK THE BOX**

Cesena Security Weekly Meeting 24/05/2017

# [ About Hack The Box ]

Hack The Box is an online platform allowing you to test your penetration testing skills and exchange ideas and methodologies with other members of similar interests. It contains several challenges that are constantly updated. Some of them simulating real world scenarios and some of them leaning more towards a CTF style of challenge. As an individual, you can complete a simple challenge to prove your skills and then create an account, allowing you to connect to our private network (HTB Net) where several machines await for you to hack them. By hacking machines you get points that help you advance in the rankings.

# [ How do I join Hack The Box? ]

In order to join you should solve an entry-level challenge that is presented (<https://www.hackthebox.gr/en/invite>). If you are unable to "hack the invite process" you will probably won't be able to do much after joining also.

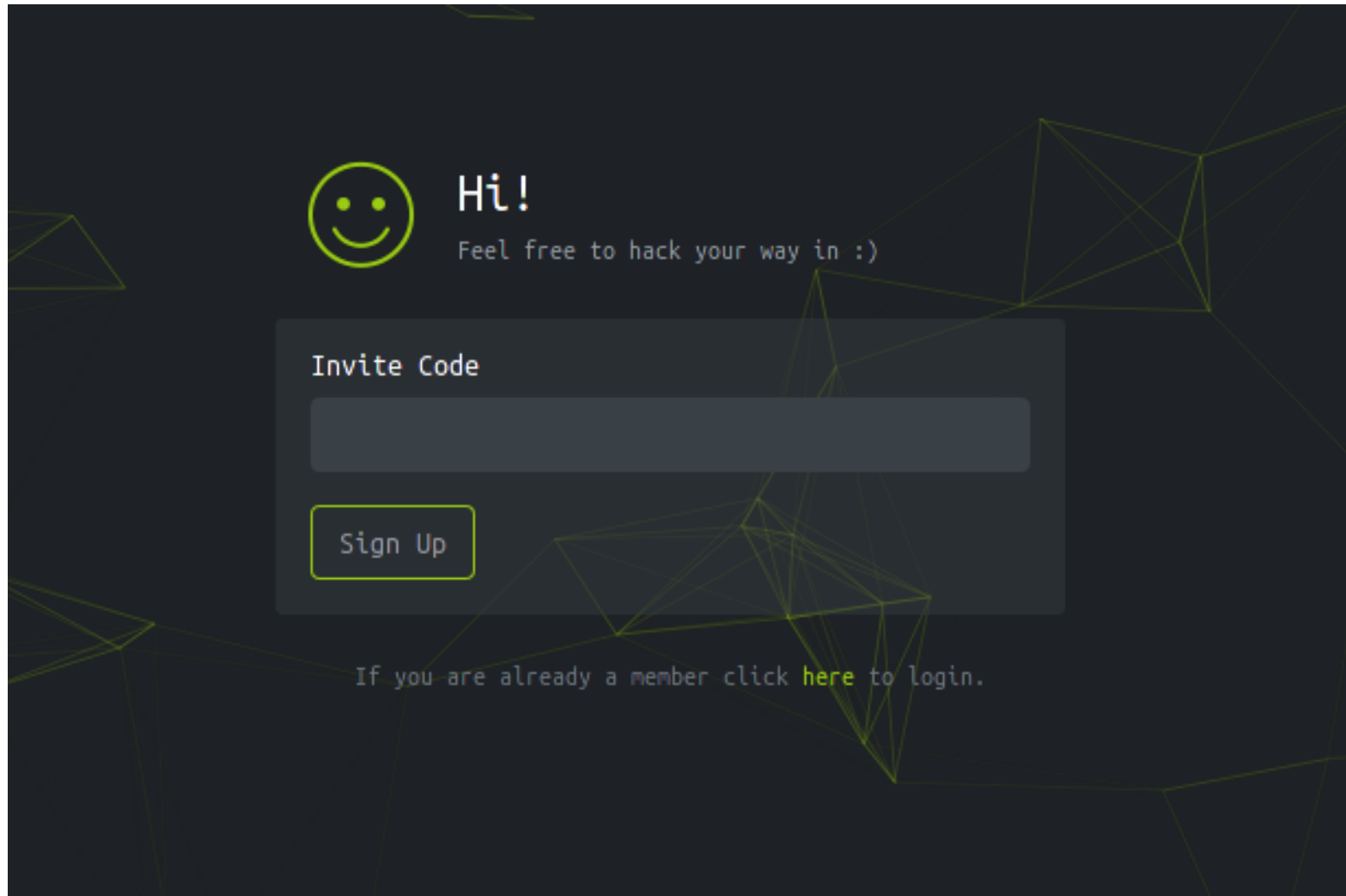
# [ How to get invite code? ]

Let's try together!

**[ 1 Take a look to the source code! ]**

hackthebox

# [ Welcome to HTB login form ]

The image shows the HTB login form. It has a dark background with a green wireframe pattern. At the top left is a green smiley face icon. To its right is the text 'Hi!' and 'Feel free to hack your way in :)'. Below this is a dark grey box containing the text 'Invite Code' above a text input field. Below the input field is a green 'Sign Up' button. At the bottom of the form, it says 'If you are already a member click [here](#) to login.'

Hi!

Feel free to hack your way in :)

Invite Code

Sign Up

If you are already a member click [here](#) to login.

## [ 2 Check the packets exchanged with the server ]

[illegible]

# [ 2 Check the packets exchanged with the server ]

Strumenti di sviluppo - HackTheBox.gr :: Can you hack this box? - <https://www.hackthebox.gr/invite>

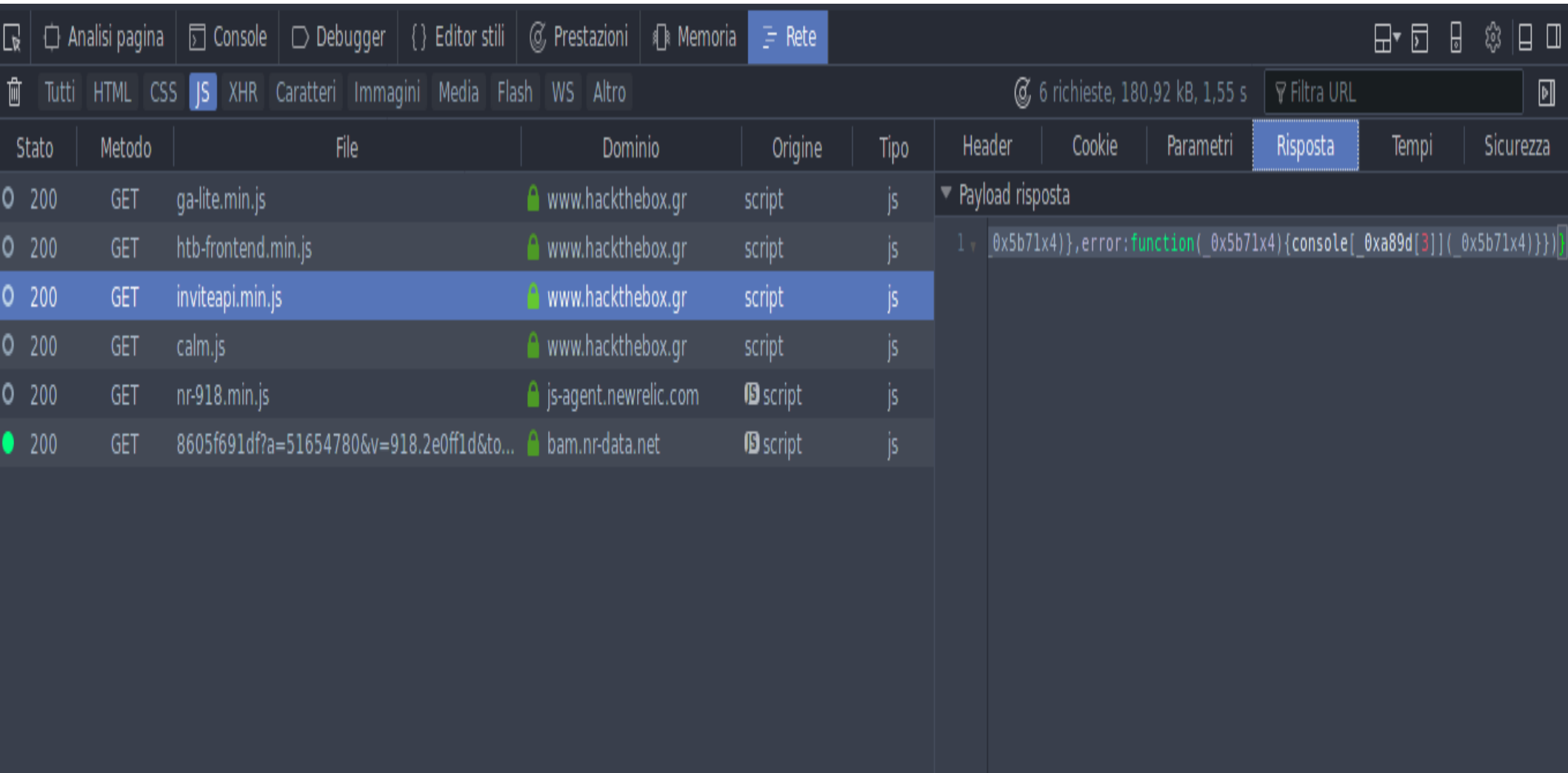
Analisi pagina Console Debugger Editor stili Prestazioni Memoria Rete

Tutti HTML CSS JS XHR Caratteri Immagini Media Flash WS Altro 6 richieste, 180,92 kB, 1,55 s Filtra URL

Stato	Metodo	File	Dominio	Origine	Tipo	Header	Cookie	Parametri	Risposta	Tempi	Sicurezza
200	GET	ga-lite.min.js	www.hackthebox.gr	script	js	Nessun parametro per questa richiesta					
200	GET	htb-frontend.min.js	www.hackthebox.gr	script	js						
200	GET	inviteapi.min.js	www.hackthebox.gr	script	js						
200	GET	calm.js	www.hackthebox.gr	script	js						
200	GET	nr-918.min.js	js-agent.newrelic.com	script	js						
200	GET	8605f691df?a=51654780&v=918.2e0ff1d&to...	bam.nr-data.net	script	js						



# [ 2 Check the packets exchanged with the server ]



The screenshot shows the Chrome DevTools Network tab. The top bar indicates 6 requests, 180,92 kB, and 1,55 s. The 'Rete' (Network) tab is selected. The list of requests is as follows:

Stato	Metodo	File	Dominio	Origine	Tipo
200	GET	ga-lite.min.js	www.hackthebox.gr	script	js
200	GET	htb-frontend.min.js	www.hackthebox.gr	script	js
200	GET	inviteapi.min.js	www.hackthebox.gr	script	js
200	GET	calm.js	www.hackthebox.gr	script	js
200	GET	nr-918.min.js	js-agent.newrelic.com	script	js
200	GET	8605f691df?a=51654780&v=918.2e0ff1d&to...	bam.nr-data.net	script	js

The 'inviteapi.min.js' request is selected. The right pane shows the response payload, which is a JavaScript function call:

```
1 0x5b71x4)},error:function(_0x5b71x4){console[_0xa89d[3]](_0x5b71x4)}}}
```

[ 3 Oh! That's cool ! ]

```

var _0xa89d = ["\x50\x4F\x53\x54", "\x6A\x73\x6F\x6E", "\x2F\x61\x70\x69\x2F\x69\x6E\x76\x69\x74\x65\x2F\x76\x65\x72\x69\x66\x79", "\x6C\x6F\x67", "\x6
function verifyCode(_0x5b71x2) {
    var _0x5b71x3 = {
        "\x63\x6F\x64\x65": _0x5b71x2
    };
    $_0xa89d[4]]({
        type: _0xa89d[0],
        dataType: _0xa89d[1],
        data: _0x5b71x3,
        url: _0xa89d[2],
        success: function(_0x5b71x4) {
            console[_0xa89d[3]](_0x5b71x4)
        },
        error: function(_0x5b71x4) {
            console[_0xa89d[3]](_0x5b71x4)
        }
    })
}

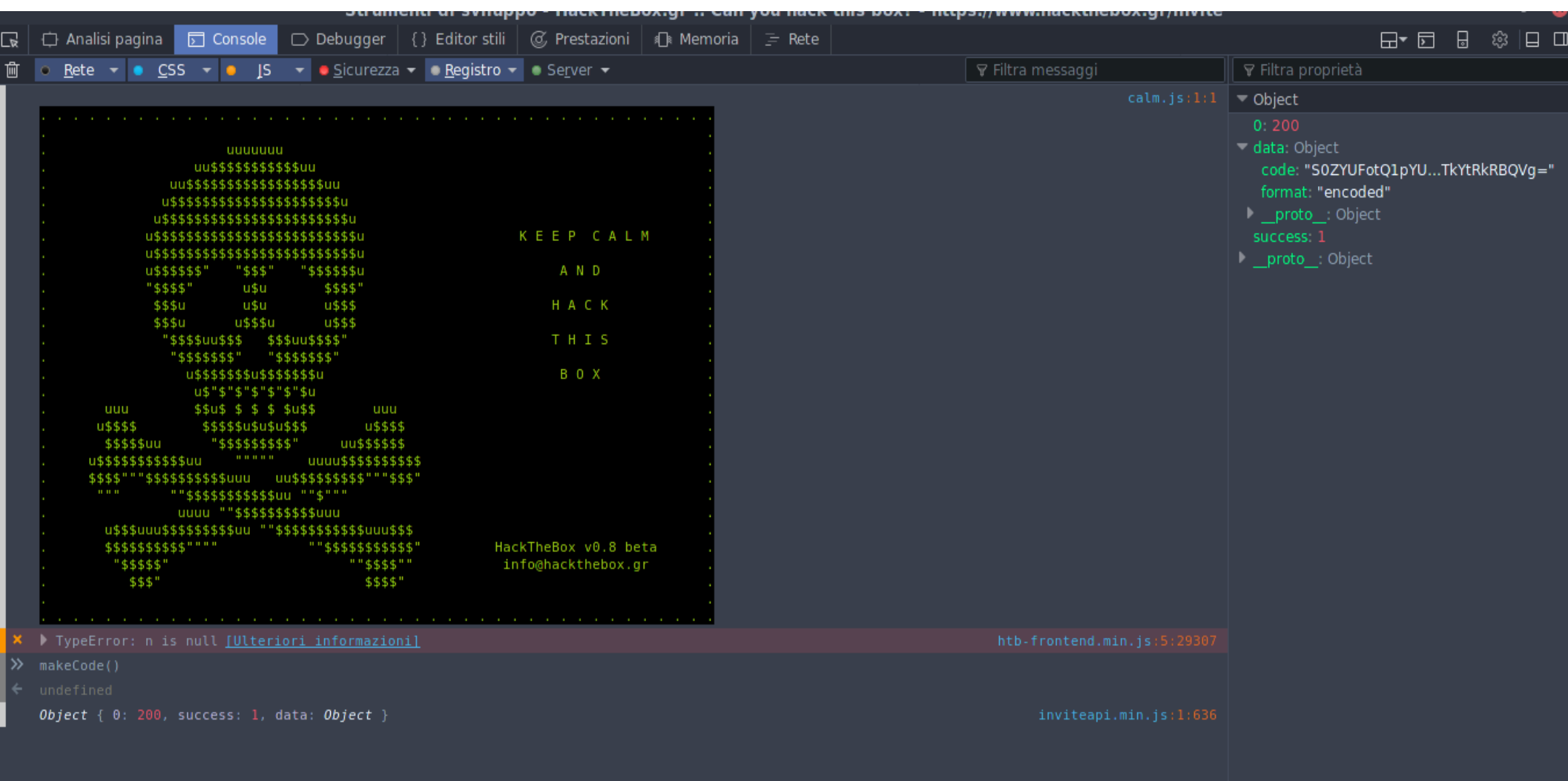
function makeCode() {
    $_0xa89d[4]]({
        type: _0xa89d[0],
        dataType: _0xa89d[1],
        url: _0xa89d[5],
        success: function(_0x5b71x4) {
            console[_0xa89d[3]](_0x5b71x4)
        },
        error: function(_0x5b71x4) {
            console[_0xa89d[3]](_0x5b71x4)
        }
    })
}

```

## [ 4 Try to call the function ]

[illegible]

## [ 4 Try to call the function ]



# [ 5 Right Way , but ... ]

The server response is encrypted, how do we do it?

Any idea?

# [ I've already seen that encoding maybe is base64? ]

Try to decode the base64 encoding and ...

## Decode from Base64 format

Simply use the form below

S0ZYUFotQ1pYU04tS01OWVctQVdHTkYtRkRBQVg=

Seems to have the appearance of an invitation code , what do you say?

< DECODE >

UTF-8



You may also select input charset.

☐ Live mode OFF

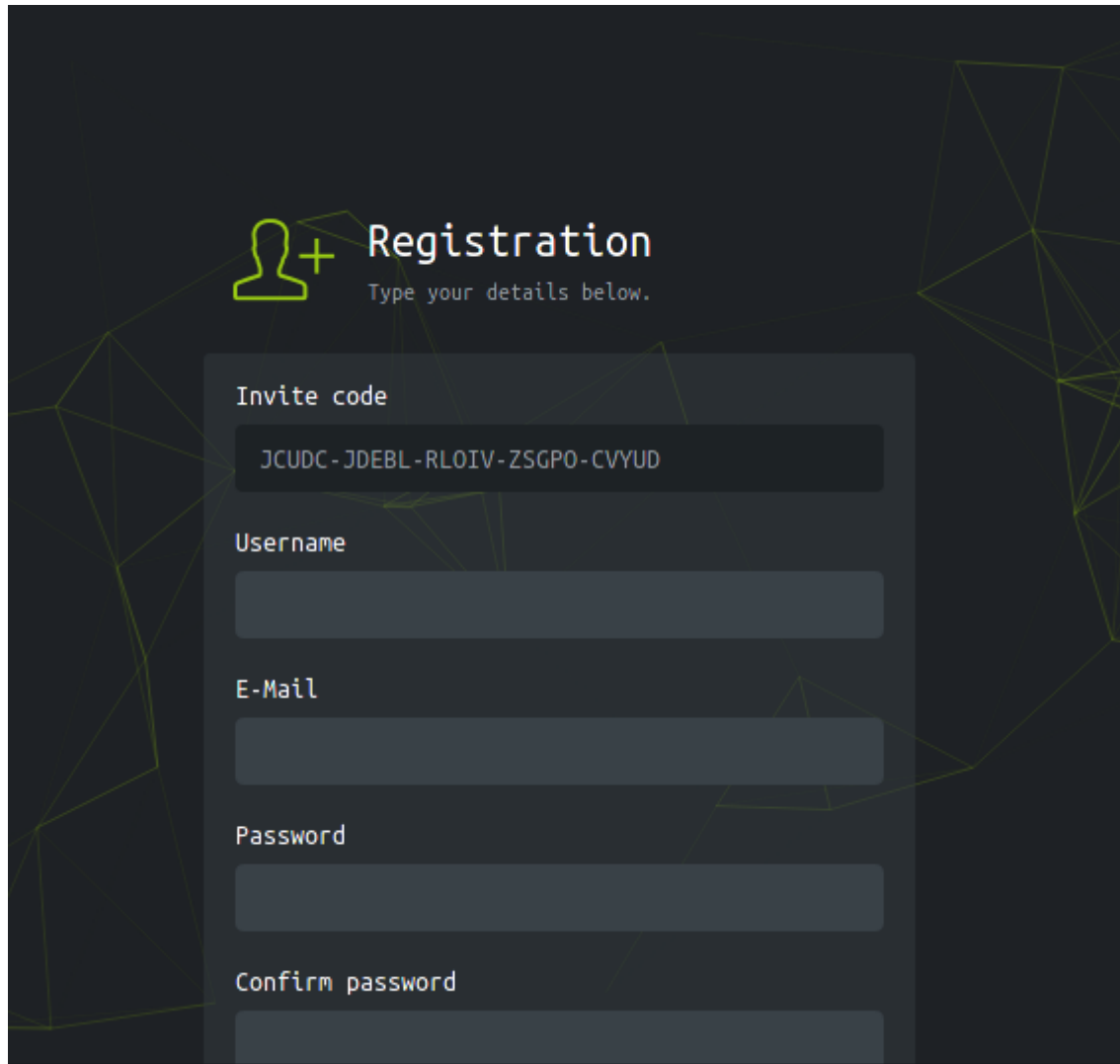
Decodes while you type or paste (in strict mode).


UPLOAD FILE

Decodes an entire file (max. 10MB).

KFXPZ-CZXSXN-KMNYW-AWGNF-FDAAX

# [ Try the code! ]

A screenshot of a registration form on a dark background with a green wireframe pattern. The form is titled 'Registration' with a green person icon and a plus sign. Below the title is the instruction 'Type your details below.' The form contains five input fields: 'Invite code' (pre-filled with 'JCUDC-JDEBL-RLOIV-ZSGPO-CVYUD'), 'Username', 'E-Mail', 'Password', and 'Confirm password'.

 **Registration**  
Type your details below.

Invite code  
JCUDC-JDEBL-RLOIV-ZSGPO-CVYUD

Username

E-Mail

Password

Confirm password

Works!!!!

# **HACK THE BOX**

Cesena Security Weekly Meeting 24/05/2017