JEMURAI

CTF Intro

JEMURAI

- **WARNING**: Please do not attempt to hack any computer system without legal permission to do so. Unauthorized computer hacking is illegal and can be punishable by a range of penalties including loss of job, monetary fines and possible imprisonment.

- **ALSO:** The *Free and Open Source Software* presented in these materials are examples of good secure development techniques. You may have unknown legal, licensing or technical issues when making use of *Free and Open Source Software*. You should consult your company's policy on the use of *Free and Open Source Software* before making use of any software referenced in this material.

JEMURAI

https://github.com/jemurai/juice-shop

JEMURAI

Rules

DO

- Work individually or in teams
- Use any tools you wish—but Firefox Developer Tools and Burp should be sufficient for all challenges
- Use the internet as a resource for attack vectors or information—exercise your Google Fu
- Use the hints if you don't know where to start
- Ask fellow competitors or me for help if you get stuck
- **HAVE FUN!**

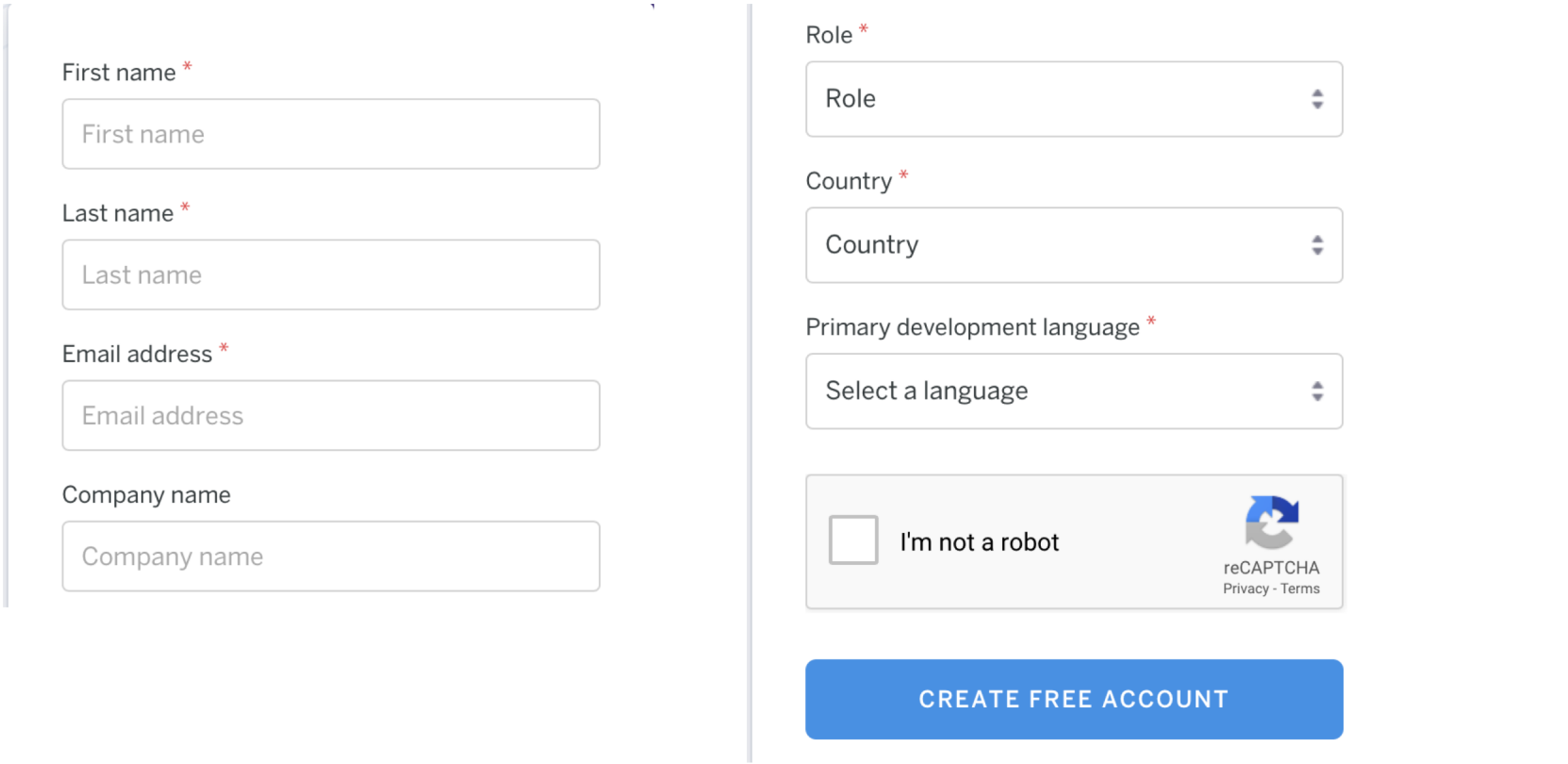
DON'T

- Attack the scoring server (CTFd)
- Directly search for or use solutions or flag values
- Review the source or test suite in the GitHub repo

JEMURAI

Step 1 — Create a Heroku Account

https://signup.heroku.com



JEMURAI

Step 1 — Create a Heroku Account

Almost there ...

Please check your email (joe+w2_heroku@jemurai.com)
to confirm your account.

JEMURAI

Step 2 — Confirm your E-mail Address

Thanks for signing up with Heroku! You must follow this link to activate your account:

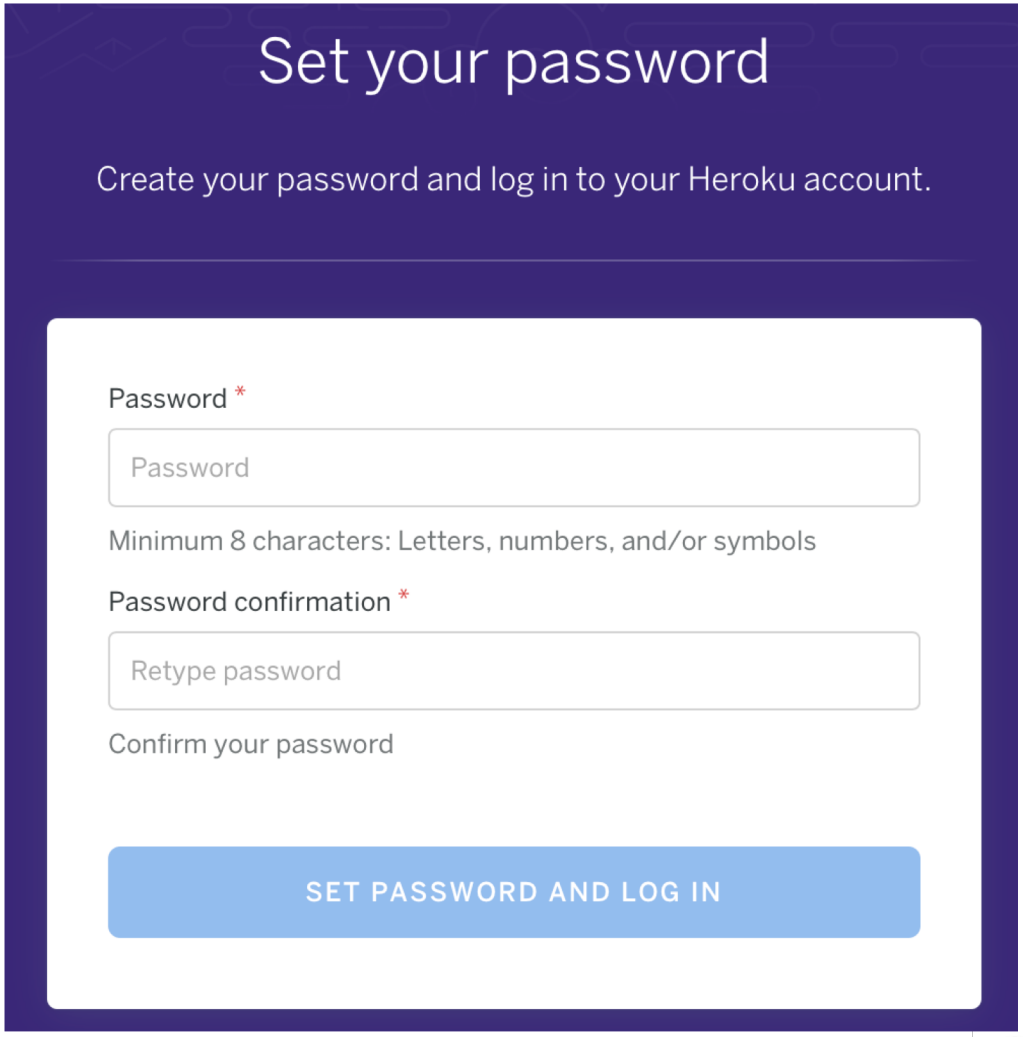
https://id.heroku.com/account/accept/5800984/c326ebdd6f9c18b270a21ea4104e591c

Have fun, and don't hesitate to contact us with your feedback.

The Heroku Team
https://heroku.com

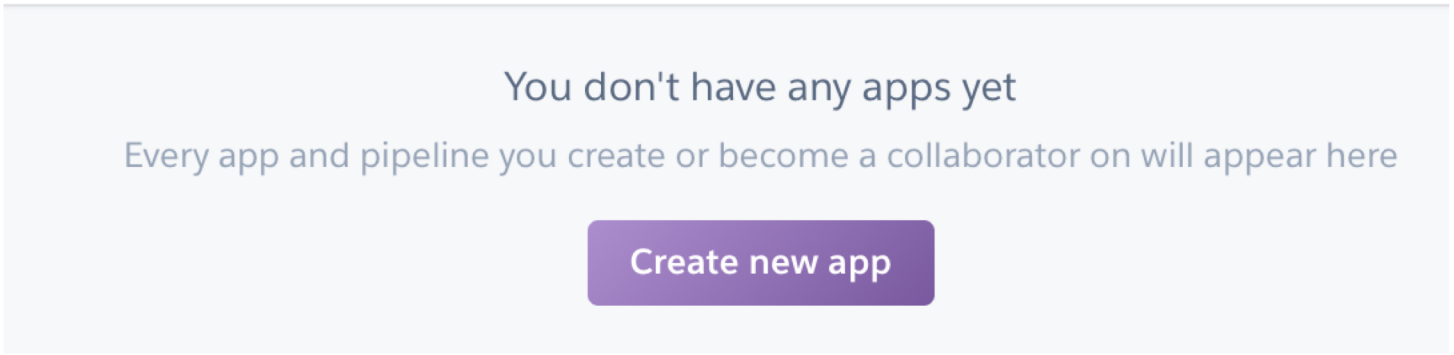
JEMURAI

Step 3 — Set your Heroku password



JEMURAI

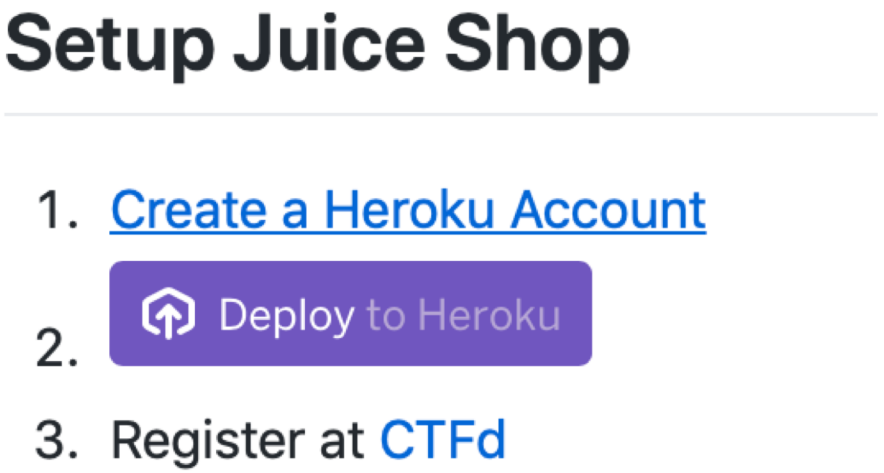
Step 4 — Confirm Account Creation



JEMURAI

Step 5 — Deploy your Juice Shop

https://github.com/jemurai/juice-shop



JEMURAI

Step 5 — Deploy your Juice Shop

Deploy your own

OWASP Juice Shop

An intentionally insecure JavaScript Web Application

jemurai/juice-shop#ctf

App name

joes-juice-shop-ctf

joes-juice-shop-ctf is available

App owner

jasp

Choose a region

United States

Add to pipeline...

Config Vars

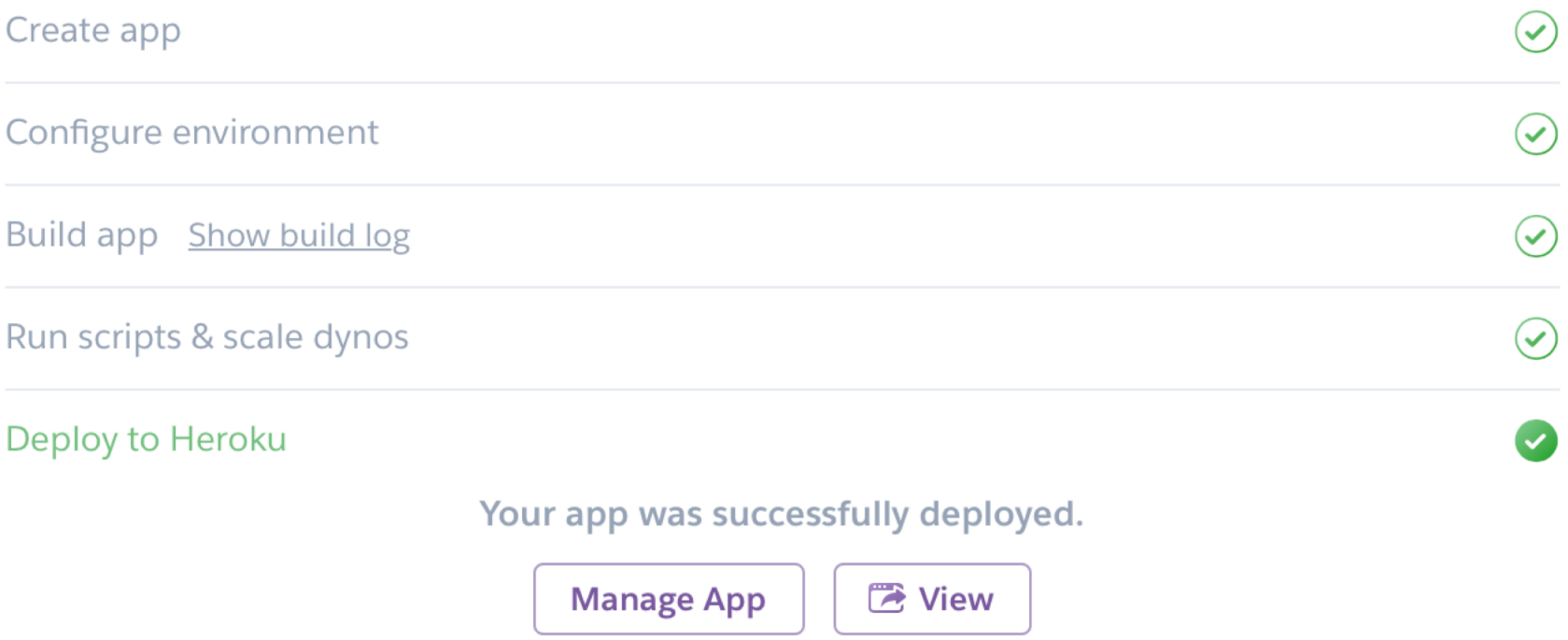
NODE_ENV Required

ctf

Deploy app

JEMURAI

Step 6 — Wait for deploy & view



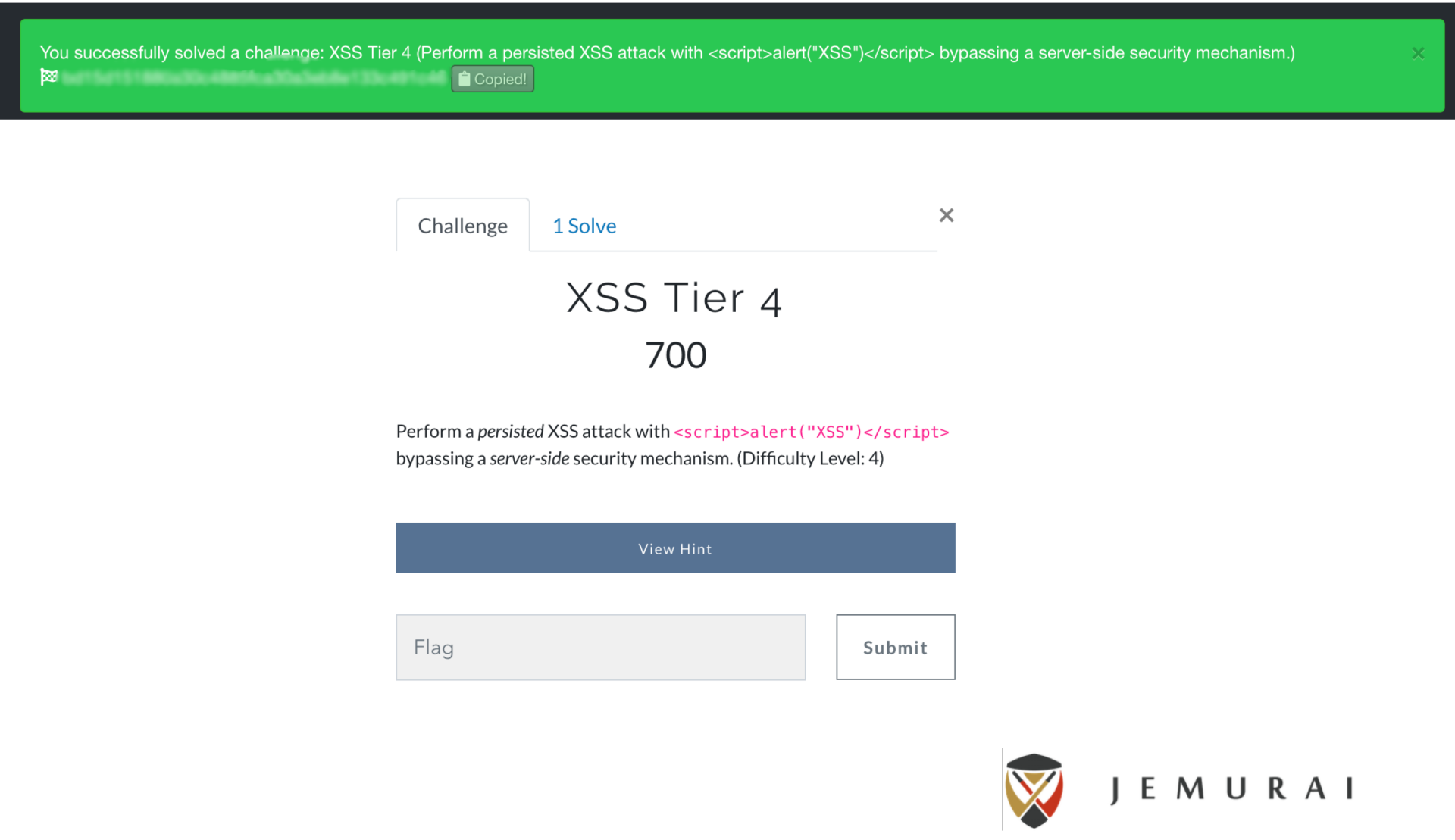
JEMURAI

Step 7 — Register for the CTFd

1. Go to https://ctfd.jemurai.com
2. Click **Register**
3. Select at team name (don't forget to prefix so we can separate sessions)
4. Enter e-mail & password
5. Check your e-mail for a verification link.
6. Click link to verify e-mail address.

JEMURAI

Collecting a Flag



JEMURAI

GitHub, Inc. [US] | https://github.com/jemurai/juice-shop

TROUBLESHOOTING.md	Remove all references to `/bower_components`	9 months ago
app.js	Apply `no-strict` transform from `lebab`	a year ago
app.json	Add env to app.json and CTF heroku deploy button	21 days ago
crowdin.yaml	Reformatted YAML files	6 months ago
ctf.key	Externalize key for flag HMACs	2 years ago
karma.conf.js	Move cookie banner out of the way for Protractor	7 months ago
master-README.md	Make CTF instructions default	7 days ago
package.json	Bump to v7.4.1	2 months ago
protractor.conf.js	Add e2e test for CAPTCHA bypass	6 months ago
server.js	Add robots.txt	2 months ago
stryker.client-conf.js	Use stryker-javascript-mutator	8 months ago
stryker.server-conf.js	Remove unnecessary node_modules/** from sandbox	8 months ago
swagger.yml	Reformatted YAML files	6 months ago

README.md

Capture the Flag

Get tools

1. Firefox Developer Edition
2. Burp Suite Community Edition

Setup Juice Shop

1. Create a Heroku Account
2. Deploy to Heroku
3. Register at CTFd

Full Juice-Shop Readme

JEMURAI

Jemurai CTF

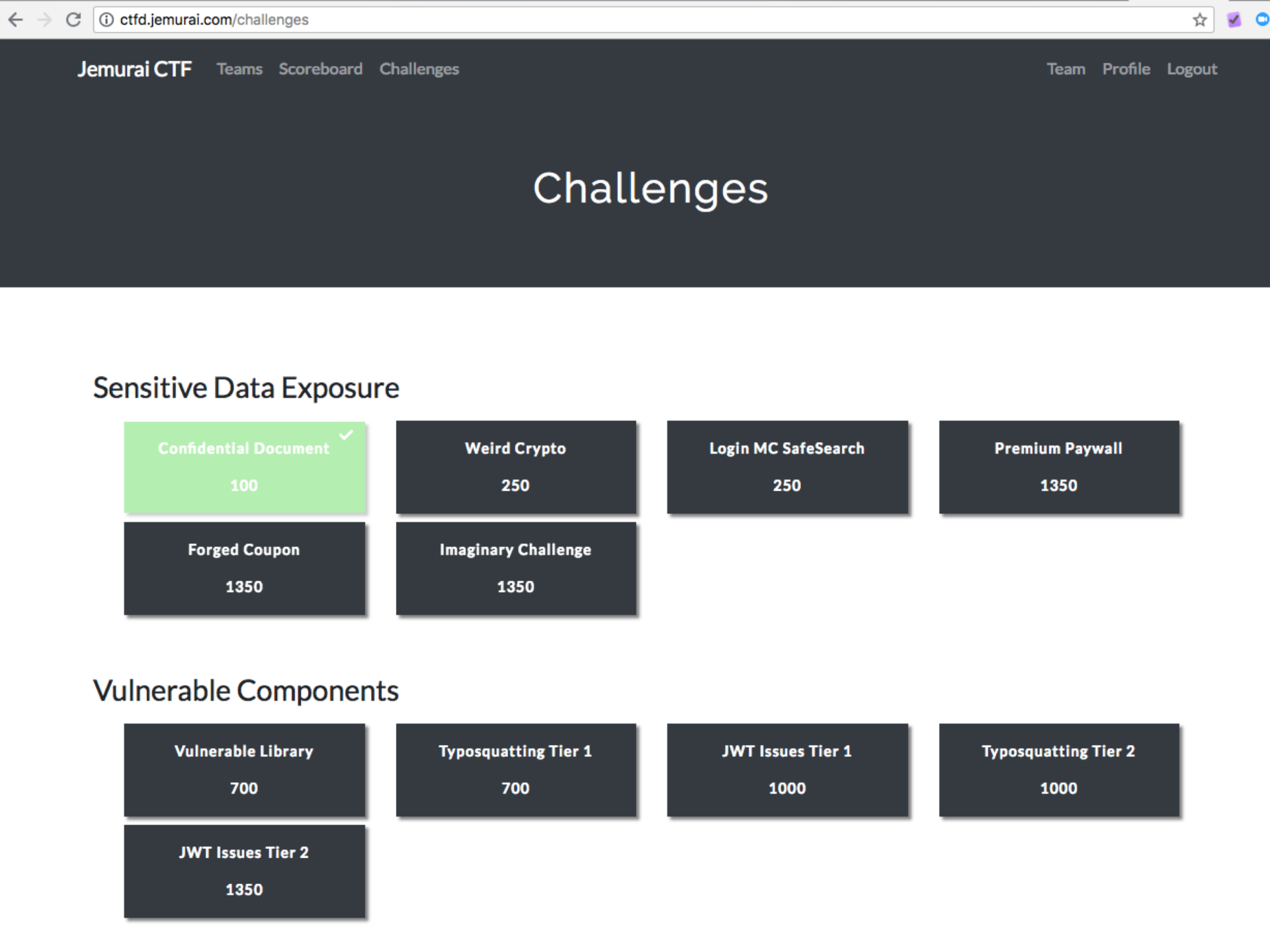
Not Secure | ctfd.jemurai.com

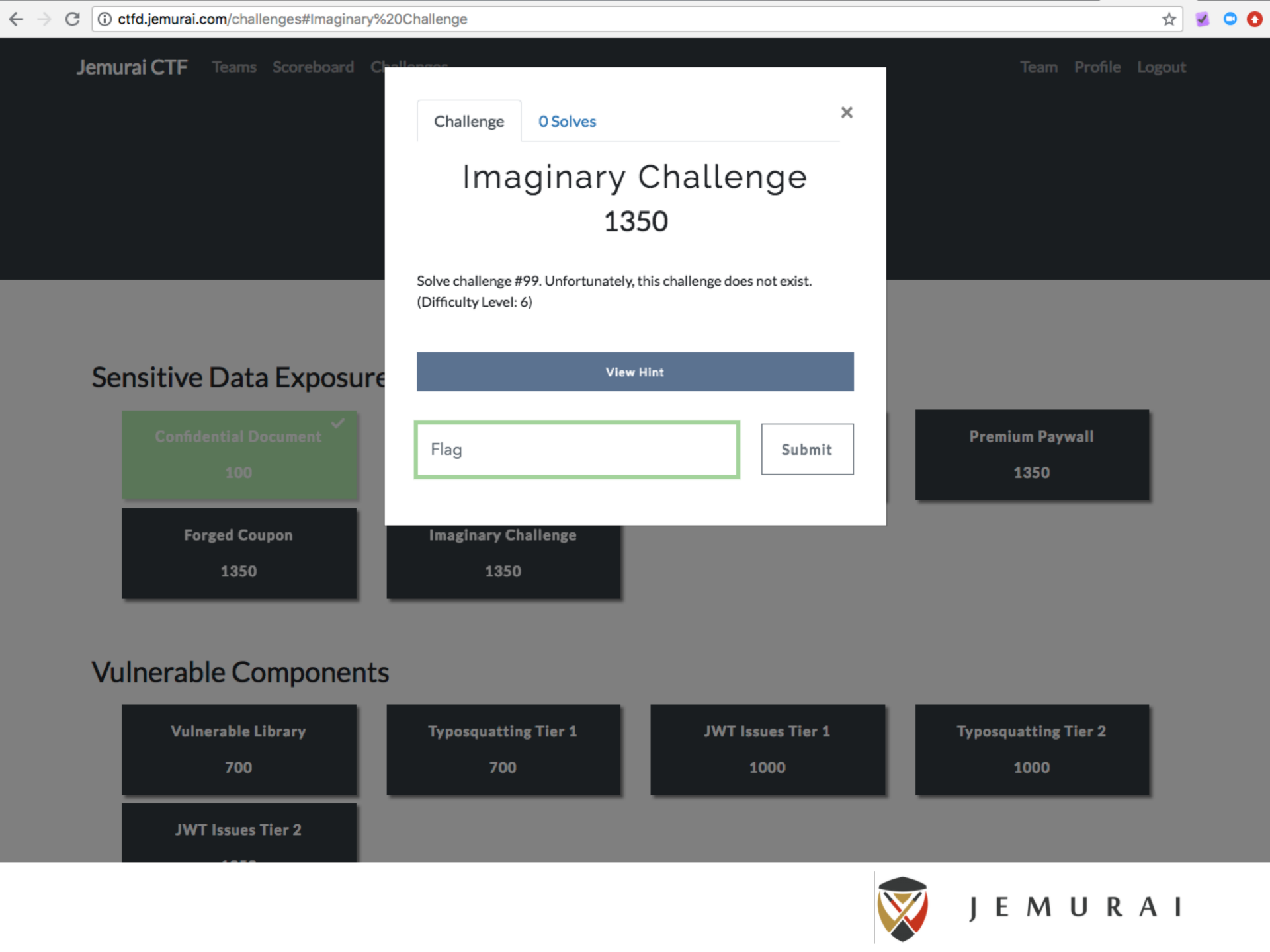
Jemurai CTF Teams Scoreboard Challenges Register | Login

A cool CTF platform from ctfd.io

Follow us on social media:

Click here to login and setup your CTF

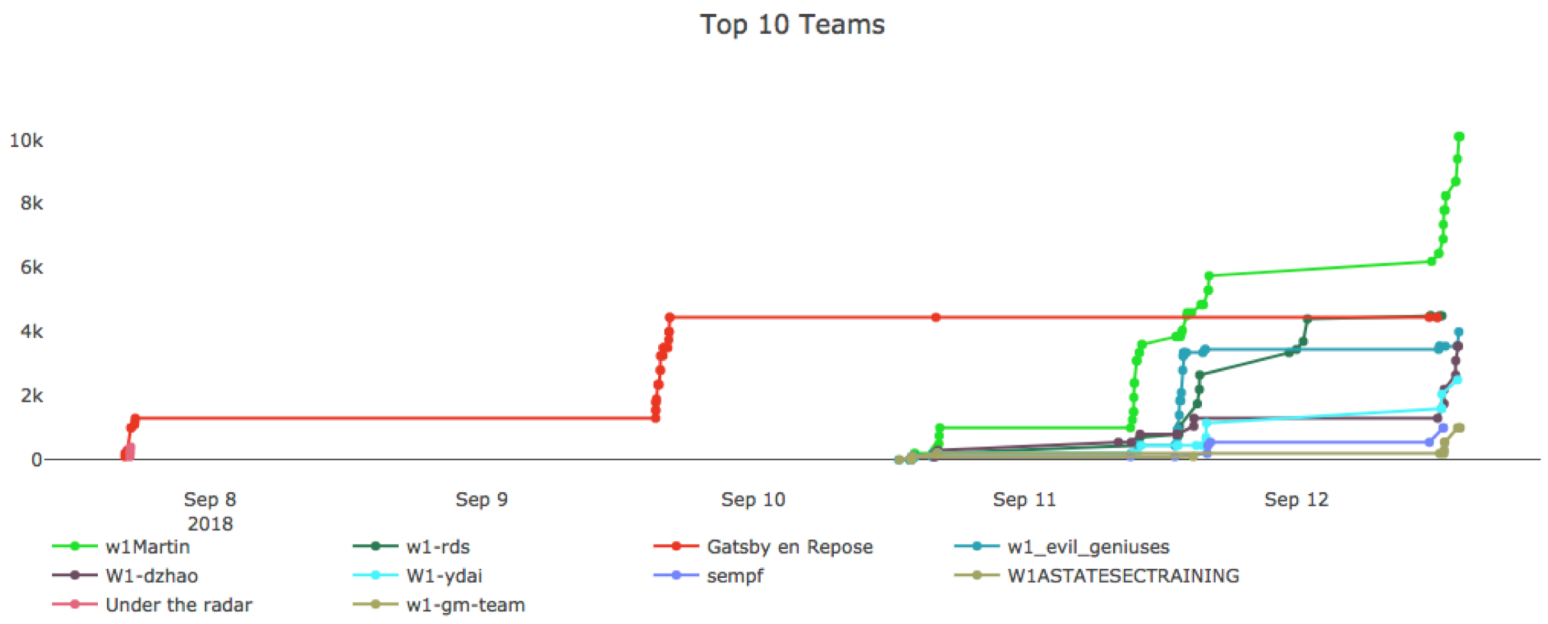

ctfd.jemurai.com/challenges
Jemurai CTF
Teams
Scoreboard
Challenges
Team
Profile
Logout
Challenges
Sensitive Data Exposure
Confidential Document
100
Weird Crypto
250
Login MC SafeSearch
250
Premium Paywall
1350
Forged Coupon
1350
Imaginary Challenge
1350
Vulnerable Components
Vulnerable Library
700
Typosquatting Tier 1
700
JWT Issues Tier 1
1000
Typosquatting Tier 2
1000
JWT Issues Tier 2
1350


ctfd.jemurai.com/challenges#Imaginary%20Challenge
Jemurai CTF
Teams
Scoreboard
Team
Profile
Logout
Challenge
0 Solves
Imaginary Challenge
1350
Solve challenge #99. Unfortunately, this challenge does not exist.
(Difficulty Level: 6)
View Hint
Flag
Submit
Sensitive Data Exposure
Confidential Document
100
Premium Paywall
1350
Forged Coupon
1350
Imaginary Challenge
1350
Vulnerable Components
Vulnerable Library
700
Typosquatting Tier 1
700
JWT Issues Tier 1
1000
Typosquatting Tier 2
1000
JWT Issues Tier 2
JEMURAI

ctfd.jemurai.com/scoreboard

Jemurai CTF Teams Scoreboard Challenges Team Profile Logout

Scoreboard



JEMURAI

JEMURAI

THANK YOU

JEMURAI