

Forum:[Hack Forums](#)

Thread: [bitjws - Capture The Flag game for 1 BTC Prize](#)

deginner - November 10, 2015, 3:52 pm

Introducing [bitjws](#)

Bit - As in Bitcoin, which lends bitjws its message signing algorithm.

JWS - JSON Web Signature - JWS represents content secured with digital signatures or Message Authentication Codes (MACs) using JSON-based data structures. [link to spec](#)

Authenticate users in Bitcoin-native apps. All constructive feedback about bitjws is welcome, and to encourage participation, we are hosting a 1 BTC contest.

Official Contest Page: <https://github.com/deginner/swagxample/wiki/Capture-The-Flag-Game-1>

Copy of details follows. Will try to keep this up to date with the official page.

#####

Now that [bitjws](#) and [flask-bitjws](#) are free of known security issues, they are ready for pen testing. This [swagxample](#) application is perfect, as it demonstrates how to protect a valuable secret (a coin) from theft.

1 Bitcoin Prize

This capture the flag (CTF) game will feature a pot containing 1 [Bitcoin](#).* The server will sign and send replies using the private key that holds the pot, the respective Bitcoin address has been published below, and all the messages exchanged between client and server will follow the bitjws implementation.

Rules

Participants will have open access to all [documentation](#) and [source code](#) for the server, as well as an [example Python client](#).

There is one voluntary rule we ask competition participants to follow:

The winner must publish the details of their attack online, preferably as an issue on the relevant github repository.

Week 1

Nov 10 2015 00:00:00 UTC - Nov 17 2015 00:00:00 UTC

Use any means of attack except against the app hosting. The app is hosted cheaply at [swagxample.deginner.com](#) and it is the code that is the focus of the game, not deployment.

Week 2 Sudden Death

Nov 17 2015 00:00:00 UTC - Nov 24 2015 00:00:00 UTC

If, after week 1, no one has managed to capture the flag from the [hosted](#) server a sudden death rule will be triggered, simulating partial server access:

Contestants are allowed to run the swagxample app on their own up to date Ubuntu 14.04 server under a new system user. The first documented attacks against bitjws itself via memory leaks or other side channel attack that another system user could perpetrate against the swagxample app user will win the pot. Examples of such attacks are proposed [here](#) and [here](#).

Resources

Pot Bitcoin Address: <http://btc.blockr.io/address/info/1AVV83Xa8E4yQGKrE4bZgi9rB2fDAEmySE>

Host server: <http://swagxample.deginner.com/>

Client examples: <https://github.com/deginner/swagxample/blob/master/example/ctf1.py>

Developer live chat: <https://gitter.im/deginner/bitjws>

GOOD LUCK!

* While additional issue reports are appreciated, the organizers have a limited budget and cannot promise any monetary rewards beyond the bitcoins attached to the "flag" coin.