

Working towards hosting a SSU Campus CTF

Eduardo Roman, Dallas Womack and Mark Gondree
Computer Science Department, Sonoma State University

Objectives

Capture the Flag (CTF) games have been praised by the security education community widely for their potential:

- For education and as an outreach tool
- To expand security to extracurricular activities
- For training, assessing skills, and job recruitment

That community interest motivates research:

- How can we introduce SSU students to CTFd.
- How can we automate deployment of SSU student oriented challenges.
- How would SSU students interact with an instance of CTFd at Sonoma State.
- Can we stand up an instance that protects the students information.

Project Goal

Stand up an **SSU CTFd supporting SSU CAS**:

Create a student and teacher accessible instance of a CTFd to be hosted at Sonoma State, over HTTPs.

Specifically:

- Integrate SSO into the CTFd instance
 - Does not current support CAS
- Deploy server securely
 - Activate HTTPs and develop "secure" config for all scoreboard services
- Develop student-oriented challenges
- Simple Challenge deployment
 - Easily deploy challenges
 - Able to recycle / tweak / re-deploy games

Project Status

- Stood-up instance of CTFd, hosted at SSU, accessible from the web via HTTPs
- Identified available game / challenge data from 3rd parties
- Reviewed several plugins to customize the CTFd instance
- Wrote a custom Flask application that uses SSU's CAS service to identify users
- Took first steps in extending CTFd to support CAS as an alternate login mechanism

Acknowledgments

This work was partially- funded under the Research, Scholarship, and Creative Activities Program (RSCAP)



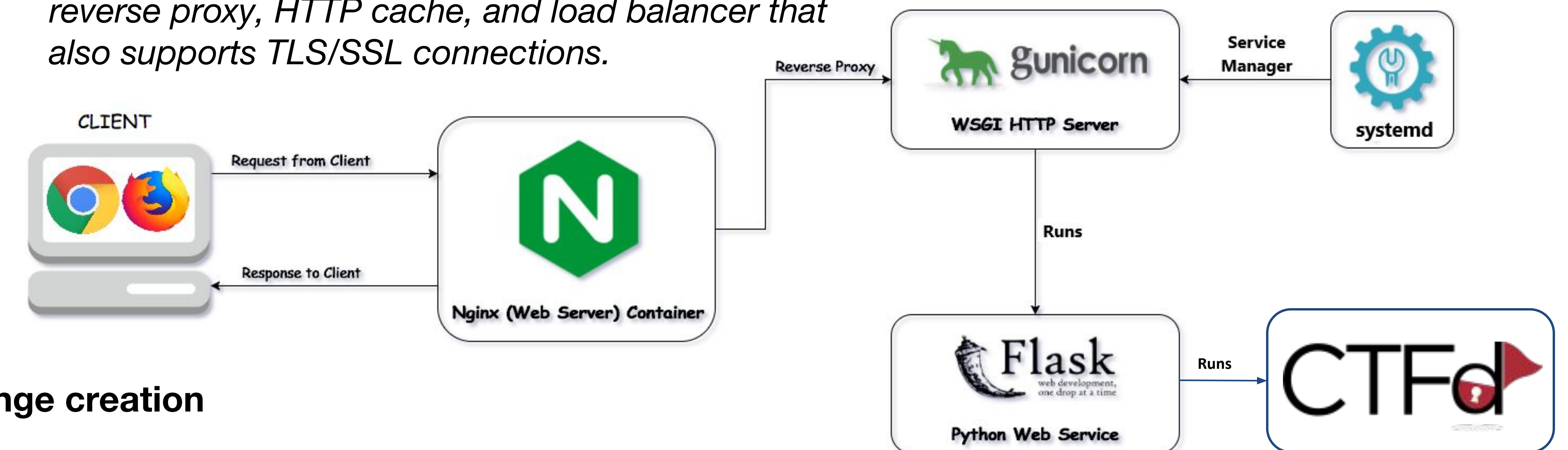
What is CTFd?

A **Capture The Flag (CTF)** contest is a computer security competition where participants practice skills related to cyber attack and cyber defense.

While **CTFd** is an open-source scoreboard / challenge server with a plugin architecture for hosting CTFs.

Summary of CTFd architecture on a production server

Nginx is an open-source web server that is used as a reverse proxy, HTTP cache, and load balancer that also supports TLS/SSL connections.



CTFd administrative web-based interface for challenge creation

CTFd provides both:

- cloud-based solution, and
- locally-hosted solution

Challenges are deployed in a different manner when hosting the CTFd instance locally as opposed to using CTFd hosting service.

Challenge **files** are relatively simply to deploy locally, but challenge **services** are more complex.

Target plugins for customizing SSU's CTFd instance

Learning Theme	<i>Theme that automatically sorts challenges into organized collapsible categories.</i>
Multiple choice challenge plugin	<i>Allows for a different style of CTF challenges to be implemented using multiple choice questions, identical to the plugin used for professional CTF instances.</i>
Hacker Theme	<i>Changes the User Interface to a sleek hacker-esq design that students would enjoy.</i>
Portable-challenges plugin	<i>Input / export challenges to re-deploy or move games more easily.</i>

CTFd login interface for players

Project goal: develop support to use SSU CAS. Eliminates need to store player PII. Follows campus security guidelines.

CTFd challenge interface for players

Concept image: customized challenges for SSU students. It is a notional image of what a SSU CTF game could look like, with challenges accessible to teams comprised of students at different stages in the major

CS215

Hexy writing 100	Color of the hex-bow 100	If you node you node 100
---------------------	-----------------------------	-----------------------------

CS115

Minimize 32	Reverse The String 50	Spagetti string 50
----------------	--------------------------	-----------------------