DIGVIJAY BHOSALE CompTIA Network+ Certified
digvijayb1729@gmail.com | +91 8999672644 | IIT Varanasi | Pune
Github | Linkedin

Improving SecureTea firewall, IDS, adding multiple new features like a persistent AntiVirus, remote motnitoring and improving GUI.

Synopsis

OWSAP SecureTea requires a few updates to its features. These are -

1. Improvements in IDS and FireWall
2. Complete Web GUI and Remote Monitoring
3. Shift Backend REST API from Flask to Django
4. Fixes bugs in Angular Frontend
5. Improve Web App FireWall GUI
6. Fix all issues and ensure Zero Bugs

For Improvements pertaining to GUI

1. The Angular Frontend contains several bugs -

- GUI looks very different in different Browsers
- Scrolling changes font and textboxes for the duration of the scroll
  Changes to the Angular GUI will fix these bugs and will improve User Experience

2. Implement “Hover for Details’ for critical symbols

Benefits to Community

OWASP SecureTea is a endpoint Security tool that can be used by BlueTeam professionals to secure devices from internet attacks. A better GUI and more Secure Backend will serve a vital role in improving System Security and User Experince.

Deliverables

Week 1 to Week 2 – Required

1. Shift backend REST API from Flask to Django
2. Ensure all standard safety procedures are followed in setting up Django REST API

Week 3 to Week 6 – Required

1. Research on Different types of Web App FireWalls and IDS
2. Start improving Features – Web Application FireWall and IDS
3. Add new features like a continuously working antivirius
4. Implement Remote Monitoring Feature

Week 7 to Week 8 – Required

1. Identify all GUI related bugs and research possible improvements
2. Start fixing all bugs and implement all GUI improvements
3. If required change the template to a more stable one

Week 8 – Optional

This will be a testing and release phase where we will offer SecureTea to various members of the OpenSource Community and get a final review.

Week 9 to Week 10 – Optional
This period is a buffer time period and the purpose is

1. To smooth out all rough ends of the application
2. To Solve problems brought forward during the testing phase of Week 8
3. To fix all remaining bugs that might have crept in during the development phase.

Biographical Information

Current Education – Indian Institute of Technology (BHU) Varanasi

Open Source Experience

1. 442 total Open Source commits on GitHub and 356 commits in the past year.
2. 3797 additions and 1339 deletions made to SecureTea via 131 commits.
3. Have been contributing to SecureTea since October 4 2021.

Skills

1. Python – Django and Flask – have been using both frameworks to develop web applications and REST APIs since September 2021
2. Angular – Proficient in Angular and Node and have written and updated routable applications using Angular Including SecureTea.
3. OWASP Top 10 – Studied OWASP top 10 and have used this to solve challenges in multiple CTFs.
4. Web Exploitation – Have completed the entire Natas challenge series of OverTheWire – for Web Exploitation
5. Security Frameworks – Proficiency with popular security frameworks – Metasploit Framework (CLI and GUI-Armitage), Burpsuite, Wireshark, Nmap, Ettercap, ARP Poisoning, Nessus, SQLMap

Certifications

1. CompTIA Network+ - Security and Architecture – March 2021 – Certificate
2. Website Hacking / Penetration Testing & Bug Bounty Hunting - Certificate

3. Programming for Everybody (Python) - Certificate
4. Introduction to Artificial Intelligence (AI) - Certificate

CTFs

1. picoCTF 2021 (March 16 – March 31, 2021) – Challenge Based CTF – Solo International rank – 999
2. Played Multiple CTFs – Hack.lu, Syskron, SShell, Hacker101
3. OWASP Chandigarh Seminar Attendee – Interacted with Sanjeev Multani, Sankarraj Subramanian and Chloe Messdaghi

Open Source Projects

1. RevShell - A combination of server side and client-side python scripts that give complete control over to the server using a reverse shell.
2. LineBrowser – A command line tool that utilizes an installed browser and Selenium WebDriver to automate the process of searching and clicking in an easy and user friendly way.
3. ftp_brute – A CLI python script that bruteforces an FTP server using a Dictionary.
4. Local_DOS_Flood – A command line python script that can DOS an IP or hostname. Network traffic of 2-8 Mbps can be achieved, drastically reducing network access.