**Internship Summary Report (May 03, 2023- Sep 25, 2023)**

**Gottumukkala Lokesh**

I have joined PrimEra as an TRO intern and for the past 5 months been training in Web Application Security and Penetration testing. I have been mentored by Nagesh sir and Sri Ganesh Malapaka. They have drawn me a detailed course plan for training in Web Security. I have been in constant communication with Ganesh over the 4-month period for discussion and doubt clarification.

Topics Covered as Part of Mentorship by Sri Ganesh Malapaka:

The topics covered are derived from the material of **PortSwigger Web Security Academy** and **Offensive Security Certification Program OSCP WEB-200 material**.Some additional topics were also covered by my own interest.

**Month of May:**

1. OWASP TOP 10 Vulnerabilities
2. Basics of Computer Networking
3. Cross Site Scripting
4. Prevention of XSS- Content Security Policy (CSP)
5. Basics of Proxy and Burp Suite tools
6. SQL Database Discovery and Enumeration-Database specific syntax and tools

**Month of June:**

1. SQL Injection Discovery and Exploitation
2. SQL Injection case study
3. Same Origin Policy and its implications
4. Cross Origin Resource Sharing (CORS) policy and headers
5. Cross Site Request Forgery- Discovery and Exploitation
6. Same Site cookies-LAX, Strict,None
7. DOM based Vulnerabilities and exploitation- Sinks and Sources
8. Improper JavaScript Coding
9. Command Injection- Discovery and Exploitation

**Month of July:**

1. Gaining Reverse Shell Access
2. Reverse Shell Payloads in different programming languages
3. Writing own web shell in python
4. Basics of Socket Programming in python
5. Server-Side Request Forgery (SSRF) attack
6. Broken Access Control- Insecure Direct Object Reference
7. Basics of XML – XPath, XLST and XSD
8. XXE entities
9. XXE Injection
10. Directory Traversal attack

**Month of August to September 1st Week(End of Ganesh Mentorship)**

Advanced Topics in Web Penetration testing

1. HTTP request smuggling
2. Insecure deserialization in java
3. Prototype pollution in JavaScript
4. Server-Side Template Injection (SSTI)
5. OAuth 2.0 and OAuth2.0 workflow
6. Authentication Vulnerabilities
7. Web Cache Poisoning

**September 7th – September 15th**

Additional Topics Covered Regarding Web Application Security

* Basics of API
* Different API architectures –SOAP and REST
* REST API Fundamentals
* API Security- API Gateway
* Microservice Architecture
* Containerization and Docker principles
* Cloud Computing and CDNs
* Basics of Cloud Flare WAF and examples of bypassing WAF
* Serverless computing and FaaS.

**September 15th-Present**

* Recap of all the topics covered
* Basic wireless hacking and Aircrack-ng suite.(PEN-210)

Basics References:

1. Material of OSCP WEB-200 certification course.
2. PortSwigger Web Security Academy
3. Offensive Security Wireless Attacks (PEN-210 course)

Additional References:(O’Reilly)

1. [Hacking APIs [Book]( API](https://www.oreilly.com/library/view/hacking-apis/9781098130244/) Security Reference)
2. [GitHub - swisskyrepo/PayloadsAllTheThings: A list of useful payloads and bypass for Web Application Security and Pentest/CTF](https://github.com/swisskyrepo/PayloadsAllTheThings) (Reverse Shell and other payload reference)
3. [Build Java-Based Microservices with REST, JSON, and XML](https://www.oreilly.com/library/view/pro-restful-apis/9781484292006/) (Web Architecture Reference)
4. [Building Microservices, 2nd Edition [Book] - O'Reilly Media](https://www.bing.com/ck/a?!&&p=f0cecb1ad7b50c9eJmltdHM9MTY5NTYwMDAwMCZpZ3VpZD0xMzMxNWMwZC04OGFmLTZlYzktMTY3NS00Zjg3ODk0MTZmMzgmaW5zaWQ9NTIyMA&ptn=3&hsh=3&fclid=13315c0d-88af-6ec9-1675-4f8789416f38&psq=Building+Microservices%2c+2nd+Edition&u=a1aHR0cHM6Ly93d3cub3JlaWxseS5jb20vbGlicmFyeS92aWV3L2J1aWxkaW5nLW1pY3Jvc2VydmljZXMtMm5kLzk3ODE0OTIwMzQwMTgv&ntb=1)
5. [JavaScript: The Definitive Guide, 7th Edition [Book](For](https://www.oreilly.com/library/view/javascript-the-definitive/9781491952016/) Javascript Reference)
6. Black Hat Python, 2nd Edition [Book] - O'Reilly Media(Writing Offensive python tools)
7. [XML Tutorial](https://www.w3schools.com/xml/) -W3 Schools