

Cloud Architecture and Security

Practical Synopsis

Group:

Soham Prasad Dhoke (21030121182)

Jay Rohit Suratwala (21030121234)

Siddhartha Saha (21030121244)

Topic:

Common Vulnerabilities and Exposure

In our current project, we aim to point out and attempt to resolve some known vulnerabilities from sources such as OWASP (Open Web Application Security Portal) and CVE (Common Vulnerabilities and Exposures) as dedicated by National Vulnerability Database in an open-source project.

This project will be carried out with the help of tools such as GitHub Fork, Testfire, NMap, and Burp Suite and most importantly, Docker and hosted on Microsoft Azure.

We aim to implement CVE by using the public repository WackoPicko (<https://github.com/adamdoupe/WackoPicko>) which is a part of the OWASP Broken Web Applications Project and has the main objective of being used to test application vulnerability scanners.

Some of the vulnerabilities that could be looked into from this repository include:

- Stored SQL Injection
- SessionID Vulnerability
- Command Line Injection
- File Exclusion
- XSS
- Forceful Browsing

Our attempt will be to address at least four of the aforementioned vulnerabilities that are identified in the project or the scope may go beyond the same and we may end up with yet-undiscovered vulnerabilities all the same.
