Report Submission

CON101- Introduction to Computer Science and Engineering

Indian Institute of Technology Delhi

Name: Deepanshu Entry Number: 2019CS50427 Group: 04

1 Introduction

According to the OWASP Industry survey, top 3 vulnerabilities include Insufficient Logging and Monitoring, Injection Flaws and Sensitive Data Exposure. As discussed by the professor in the lecture, billions of dollars are invested by companies to prevent their data centres, softwares etc. from attacks.

2 Why is the study important

Even till now, many government websites are vulnerable to attacks. Even some IITD websites are vulnerable and we get to see minor attacks occasionally. So, there is a need to protect the data both from administrative point of view and maintain technical authenticity.
Many startups are also emerging in this field. **Cohesity, founded by IIT Delhi alumni Mohit Aron** is one such example which focuses on safety of data and servers.

3 Various software vulnerability issues

3.1 Insufficient logging and Monitoring

Most of the movies show hacker in a way that they break in a server and say with proud "I am in". That usually refer to logging in and monitoring the server. It is the underlying principle of almost every major incident. It is considered the most dangerous attack and all of the admin panel is exposed to the attacker.
How does it affect
It basically gives the attacker all the rights equivalent to the admin rights. In financial things involving bank transactions etc. it becomes even more "lethal". Exam papers may get leaked in the case when it is held online and stored in a server.

3.2 Injection flaws

It mainly works by injecting malicious software in the system (especially to an interpreter). It is relatively less harmful than injection flaws. Though admin panel is not exposed, it sends various calls that may either slow down or entirely break the system.

How does it affect

If servers of big tech companies get down (for example: Amazon), millions and billions worth of transaction will hinder. If servers of some exam is bought down, all the students will suffer.

3.3 Sensitive data exposure

It occurs when company or organisation inadvertently exposes personal data. Sensitive data exposure differs from a data breach, in which an attacker accesses and steals information.

How does it affect

Data is sometime hidden in the page itself (For example: to increase performance). If this data is somehow available to any third party, it may cause serious administrative and legal issues. If websites don't use SSL and don't have HTTPS, there is a risk of data exposure.

4 What can be done at a college level

1. Conducting various events like CTF's that involve attacking and saving of a test server.
2. Taking up courses involving verification of parallel systems, distributed systems etc.
3. Looking up various research papers for projects involving cryptography, verification etc.

5 References

1. https://jyx.jyu.fi/bitstream/handle/123456789/55806/URN:NBN:fi:jyu-201711084167.pdf
2. https://www.lynda.com/JavaScript-tutorials/Insufficient-logging-monitoring/758646/807224-4.html
3. https://www.perforce.com/blog/kw/common-software-vulnerabilities
4. https://owasp.org/www-project-top-ten/