

A decorative border at the top of the slide featuring a honeycomb pattern. Most cells are yellow, but a few are a darker orange color.

# NEPSEd

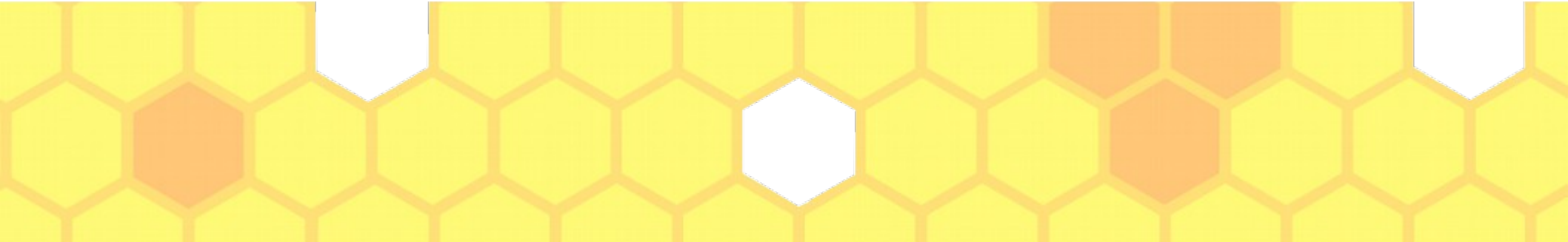
SYDNEY

Risk Assessment

A decorative border at the bottom of the slide featuring a honeycomb pattern. Most cells are yellow, but a few are a darker orange color.



# Learning Outcome

- Vulnerability/Bug Difference
  - Risk
  - Severity
  - Calculation of Severity
  - How to assess Risk?
  - BugBounty
  - What to report in Bugbounty
- 

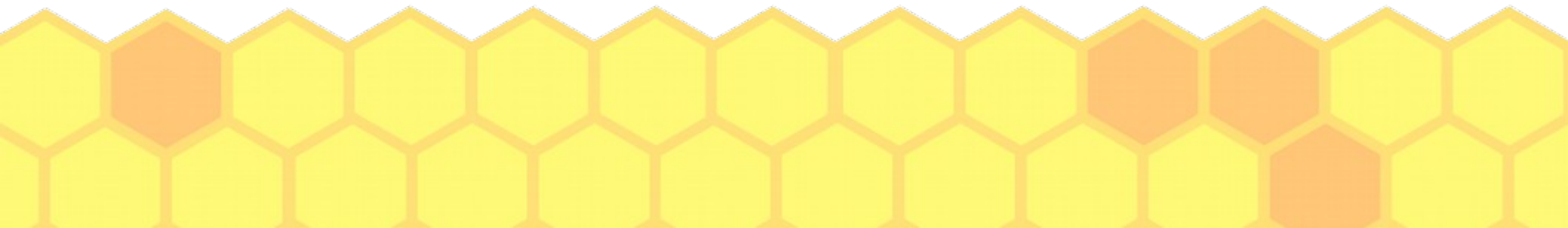
# Vulnerability Vs BUG?

## Bug :

- Anything that is broken!
- Broken Pages/Links
- Broken WebViews in different devices
- Features that does not work

## Vulnerability:

- Anything that compromises any asset of organization.
- Default passwords
- Broken links referring to claimable instances
- Any info that you would not want to be known by others but is leaked



Example time :D



# Threat

- That has tendency to harm the organization
- Internal and External Threats
- Natural calamities → External threat

## Consequences

Result of harm done by the exploits/threats.



# Risk & Severity

Formula : Threat \* Vulnerability \* Consequences

The amount of probable harm due to the amount of asset the organization has that has possibility of being exploited is Risk in simpler terms.

Severity on the other hand means how severe or what is the rating of the specific vulnerability on that scenario where it is being exploited.



# Risk/Severity Calculation for a vulnerability

Likelihood	Near Certainty	5	10	15	20	25
	Highly Likely	4	8	12	16	20
	Likely	3	6	9	12	15
	Low Likelihood	2	4	5	8	10
	Extremely Improbable	1	2	3	4	6
		Minimal	Minor	Major	Serious	Catas- trophic
		Severity / Impact				

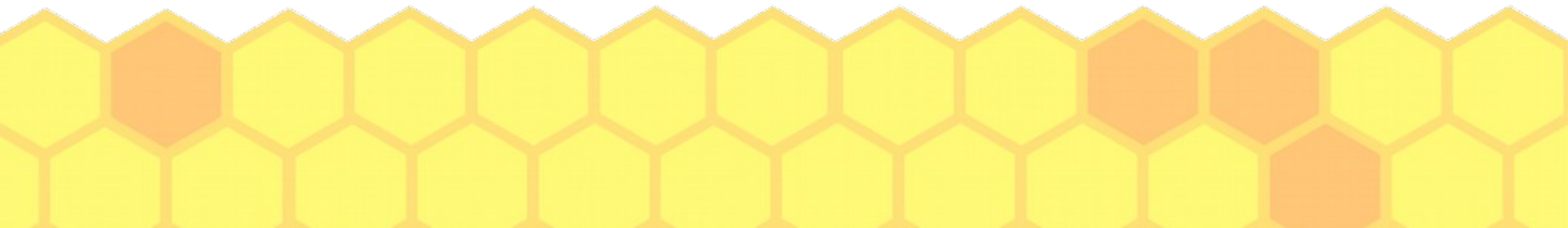
## Risk Value Legend

Low:  $\leq 5$  – Green

Med:  $>5, \leq 12$  – Yellow

High:  $> 12$  – Red

IMPACT	High	Medium	High	High
	Medium	Low	Medium	High
	Low	Low	Low	Medium
		Low	Medium	High
		LIKELIHOOD		



# Risk matrix approach

		Impact			
		None	Small	Moderate	High
Frequency	Very High		High	Very High	Very High
	High		Moderate	High	Very High
	Moderate		Low	Moderate	High
	Low		Low	Low	Moderate
	None	No Risk			





# CVSS Scores

- A metric kind of standard scores that helps you analyse the potential risk rating.



# Demo



# Bugbounty

- Hack → Report → Get Reward
- You get bounty for the Valid Security Bugs(Vulnerability) you report if you're the first reporter
- Good place to practice infosec
- Few percent in the world earns like hell while others like us, will get that in future.
- Dont let \$\$\$\$ change your motive of learning!



# What to report in Bugbounties?

- Anything that has impact atleast one user apart from yourself!!!
- Vulnerabilities/misconfigurations that we will learn in coming meets!!!



# Bugcrowd and How Bugbounties work in it?

