Top three vulnerabilities and a DREAD analysis

1. Brute force attacks
2. Denial of Service (DoS) attack
3. Security control attacks.

Vulnerabilities

1. Architecture
2. Brute force
3. DoS attack

Group 3

1. Yin
2. Jonathan
3. Haseeb

	Damage	Reproducibility	Exploitability	Affected users	Discoverability	Risk (Max=3)
Brute force attacks	3	2	3	3	3	2.8
Denial of Service (DoS) attack	2	3	3	3	1	2.4
Security control attacks	3	1	1	3	2	2

Threat	**Damage**	**Reproducibility**	**Exploitability**	**Affected users**	**Discoverability**	**Risk**
Architecture	3	2	3	3	2	2.6
Brute force	3	2	3	3	2	2.6
DoS attack	2	2	3	3	1	2.2

Threat	**Damage**	**Reproducibility**	**Exploitability**	**Affected users**	**Discoverability**	**Risk**
Brute force	3	2	2	3	3	2.6
Denial of Service	2	2	2	3	2	2.2
Security control	2	2	1	3	2	2

Threat	**Damage**	**Reproducibility**	**Exploitability**	**Affected users**	**Discoverability**	**Risk**
Brute force	3	2	3	3	3	2.8 High
Denial of Service	2	2	2	3	2	2.2 Medium
Security control	3	2	1	3	2	2 Medium

Potential mitigations - ranked in order

Which is the risk with the highest rating? What assumptions have you made?

- Both WiFi security protocols WPA and WPS found vulnerabilities, Key Reinstallation Attack (ENISA, 2017) and VU#723755 (CISA, 2013), which should replace by WPA3 (Rob, 2018).
- Implement Content Distribution Network (CDN) and Web Application Firewall (WAF), abnormal traffic or common attack patterns or behaviour could be monitored and blocked.

The use of zero trust architecture, effective security policy including training/education for users, intrusion detection and prevention systems.

The highest rating risk is Brute force attack which is (= 2.8)

•Brute force attacks mitigation by Using (Strong or Hashed Passwords - CAPTCHAs - Two_Factor Authentication).

•Denial of Service (DoS) attack mitigation by Using (Firewalls and Proxies - Limiting Login Attempts - Ingress Filtering).