Focus Outset and Judging: 70% on Security

As this is a Security hackathon, participants must have worked to implement security on their applications. The following is an outline of how teams will be judged:

a) Vulnerability Assessments Reports/Evaluation [Vulnerability Score]

- Option 1: Vulnerability scan reports using tools like OWASP ZAP will be collected in time intervals throughout the Hackathon
- Option 2: Participants go through how they resolved the vulnerabilities they said to have mitigated; Show processes, configurations, etc.

* These will be submitted to the judges to assist in the judging process. Judges must give/rate a vulnerability score for a team, based on effort of Risk Mitigation. Mentors assessments will also be considered for this aspect.

b) Show&Tell [Security Score]

- Inject into own application with scripts on forms and others.
- Show backend (database, instances) configurations and usage of special mechanisms
- OWASP Top 10 Vulnerabilities prevalent
- List all tools used and for what… are these modern or best practices?
- Policy and Regulation: Are they talking NCPF, PoPI, GDPR, etc.

c) Best Practices [SDLC Score]

- Explain the Document Secure SDLC process outline to get an idea of the process flow
- Mentors will assess and submit their teams' work and practice by 16:00 on the 28th of May, based on a set rubric criteria. ***This will be a Google Form.***

NOTE: Bonus points must be given for: Outstanding work, having hacked onto other teams, teamwork and coordination, presentation skills and/or Security Innovation.

#SS19Hack | 28 - 29 May 2019, Sandton Convention Centre

Judging Rubric: 29 May 2019

Team Name	Innovation 0 - 15	SDLC 0 - 10	Vuln Score 0 - 5	Security 0 - 15	Bonus 0 - 5	TOTAL	Comment
CTF Blue Team	N/A						
CTF Red Team	N/A						
Reafithla							
Datawranglers							
CodeWizzards							
4th Hackers							
DeepHacks							
HAK4AF							

Guardians						
Rebels						
Khululeka						
True Author						
Makakole and the Others						
Dark Phoenix						
BonMido						