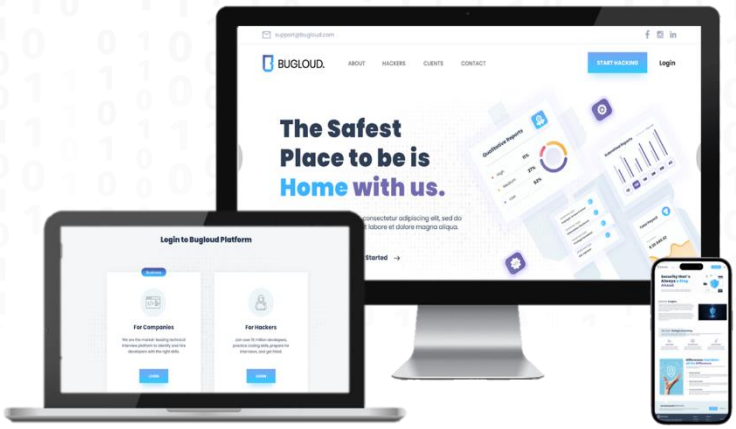
BUGLOUD.



Bug Bounty Challenge

19th IEEE UAE STUDENT DAY, 2025

Ethical Hacking & Cybersecurity Student Competition
Live Platform | Real Targets | Real Impact

Main Category: Web Security

Themes:

1. **Web Application Vulnerabilities**
   (e.g., XSS, SQLi, CSRF, Authentication flaws)
2. **API & Backend Security**
   (e.g., Broken object-level authorization, Insecure endpoints)
3. **Client-Side Security**
   (e.g., DOM-based XSS, Clickjacking, Local storage issues)

GENERAL INFORMATION

This competition offers undergraduate students an opportunity to demonstrate their **cybersecurity skills** in a **real-world bug bounty environment**. Participants will ethically hack a live web application provided by Bugloud.com, identify and report valid vulnerabilities, and submit their findings through the Bugloud platform. The aim is to promote ethical hacking, responsible disclosure, and web security awareness among future engineers.

COMPETITION GUIDELINES

1. Students will have to register here
2. The event will be held in University of Dubai campus.
3. Bugloud will provide each participant/team with:
   - Access to a dedicated live web target
   - A private workspace on the Bugloud platform to report bugs
4. The bug bounty event will be accessible only from onsite at the university campus.
   - A secure event **password** will be entered **by Bugloud staff** to access the platform.
5. All vulnerabilities must be reported exclusively through the Bugloud platform for validation.

6. **Only web-based vulnerabilities are allowed** (XSS, SQLi, CSRF, etc.) — network or infrastructure attacks are strictly prohibited.

Prohibited Activities

- No DDoS or stress testing of any kind
- No Remote Code Execution (RCE)
- No fuzzing, brute-force attacks, or automated scanners
- No social engineering, phishing, or targeting other users or staff
- No accessing or modifying user data
- No public disclosure of any findings during or after the competition
- Only pre-approved targets are in-scope; all other systems are out-of-scope

Evaluation Criteria

Submissions will be judged based on the following:

CVSS v3.1 Score

CVSS Base Metrics — to be filled in the **Platform** per vulnerability:

Metric	Options
Attack Vector (AV)	Network (N), Adjacent (A), Local (L), Physical (P)
Attack Complexity (AC)	Low (L), High (H)
Privileges Required (PR)	None (N), Low (L), High (H)
User Interaction (UI)	None (N), Required (R)
Scope (S)	Unchanged (U), Changed (C)
Confidentiality Impact (C)	High (H), Low (L), None (N)
Integrity Impact (I)	High (H), Low (L), None (N)
Availability Impact (A)	High (H), Low (L), None (N)

Automated Scoring

After choosing the **CVSS base metrics**, the score will be automatically calculated and mapped to a range like this

CVSS Score	Severity Level	Judging Points (/20)
0.0	None	0
0.1–3.9	Low	5
4.0–5.9	Medium	10
6.0–7.9	High	15
8.0–10.0	Critical	20

TERMS & CONDITIONS

All participants are expected to follow the rules strictly. Any violations may lead to immediate disqualification. Bugloud and C-SAR reserve the right to make final decisions in any disputes or rule interpretations.

For further inquiries, please do not hesitate to contact yswalweel@ud.ac.ae