Journal Of the Iraqia University (76-4) 31 July (2026)

ISSN(Print): 1813-4521 OnLine ISSN:2663-7502

Journal Of the Iraqia University

available online at

https://iasj.rdd.edu.iq/journals/journal/view/247

CTF Events in Cyber Skills and Strategy Workforce Development for Iraq's Ministry of Interior

م.د حسن هادي لذين

وزارة الداخلية /كلية الشرطة

Abstract

The Iraqi Ministry of Interior (MOI) piloted a nationwide Capture-the-Flag (CTF) program in 2024 to close acute cybersecurity-skills gaps and streamline recruitment for its Cybersecurity Center. Adapting the Hack the Box competition model, the initiative unfolded in three stages: an open call that attracted 367 applicants, an online qualification round featuring 12 auto-scored challenges that shortlisted 64 top performers, and a nine-hour, in-person final comprising 36 progressively harder tasks across web exploitation, reverse engineering, cryptography, forensics, full-pwn and OSINT domains. Only 7 % of the final-stage challenges were solved, confirming expert-level difficulty and validating the event's filtering power. Performance analytics showed that rapid "time-to-exploit" and selective depth— prioritizing a few high-value flags—were stronger success predictors than broad, shallow coverage. Post-event interviews indicated that many finalists lacked formal degrees yet demonstrated operational readiness equivalent to junior incident-response roles. The study concludes that government-run, standards-aligned CTFs can (1) identify hidden talent outside traditional academic pipelines, (2) benchmark practical competencies against workforce frameworks such as NICE, and (3) supply actionable data for tailoring future training investments. Recommendations include integrating longitudinal tracking to measure on-the-job efficacy of CTF recruits and expanding challenge sets to encompass under-represented skill areas such as social engineering. The MOI experience offers a replicable blueprint for nations seeking cost-effective, skills-centric pathways to strengthen cyber defense capabilities in resource-constrained environments.Key Words : Capture-the-Flag (CTF) competitions; Cybersecurity workforce development; Skills-based talent identification; Iraqi Ministry of Interior (MOI); Hack the Box model; NICE Workforce Framework; Gamified learning; Incident-response readiness; Online and in-person screening; Resource-constrained environments

Introduction

The global cybersecurity landscape is characterized by an accelerating pace of threat evolution, driven by sophisticated adversaries leveraging advanced tools and techniques. Recent studies indicate that the worldwide shortfall of qualified cybersecurity professionals exceeds three million positions, a deficit that aligns with escalating frequency and impact of cyber incidents[1] In 2023, the International Information System Security Certification Consortium ((ISC)²) reported the workforce reached 5.5 million individuals—an 8.7 percent increase over the previous year—yet still fell far short of organizational demand, which grew even more rapidly (ISC², 2023)[2] A parallel survey by Government Technology found that the global workforce gap swelled to 4.8 million roles in early 2024, a 19 percent year-over-year jump, even as budgets tightened under economic pressures[3] The financial toll of these talent shortages is stark: the average cost of a data breach reached US $4.45 million in 2023, underscoring the direct link between understaffing and organizational risk[4] Moreover, 82 percent of employers across multiple industries report tangible damage— misconfigurations, delayed patching, procedural oversights—stemming from insufficient cybersecurity personnel[2, 5] Traditional recruitment frameworks frequently prioritize formal academic credentials—degrees, certifications, transcripts—over demonstrable, hands-on capabilities.However, employers and educators alike acknowledge that such credentials alone do not guarantee proficiency in practical, real-world defense scenarios[6] For example, a McKinsey report highlights that job growth for cybersecurity roles is projected to climb 32 percent from 2018 to 2028, yet educational institutions struggle to adapt curricula rapidly enough to meet evolving skills requirements[7] Similarly, a CSIS-commissioned study documented that while governments in the U.S., U.K.,

Israel, and Australia have enacted legislation and funding to cultivate cybersecurity talent, over 75 percent of respondents believe their governments still underinvest in skills development, perpetuating the workforce gap[8] In response, gamified learning models—most notably Capture The Flag (CTF) competitions—have gained prominence as effective tools for skills-based assessment and training. CTF events present participants with realistic, scenario-driven challenges spanning digital forensics, web application exploitation, reverse engineering, cryptography, and open-source intelligence (OSINT). An analysis of nearly 16,000 solution write-ups from diverse CTFs revealed that while technical domains such as cryptography and network exploitation dominate, human factors like social engineering remain underrepresented[9] A comprehensive survey of cybersecurity competitions further demonstrates that CTFs not only foster deep technical knowledge but also build problem-solving resilience under time constraints[10] Practitioners report that involvement in CTFs enhances familiarity with real-world toolchains and collaborative workflows, a finding echoed in qualitative studies of university-run CTF laboratories[11] and multi-year educational CTF programs[12] Exploratory research into learner outcomes indicates that CTF engagements correlate with improved performance in subsequent professional or academic cybersecurity activities[13] while dedicated teaching labs leveraging CTF frameworks have demonstrated sustained skill development over multiple cohorts[14] National and supranational bodies have institutionalized CTF-based talent pipelines. The European Cybersecurity Challenge—a flagship event under ENISA—draws hundreds of competitors from EU member states each year, culminating in multi-day finals that benchmark participant proficiency against international peers[15] In the United States, the U.S. Cyber Challenge combines intensive cyber camps with CTF competitions to identify high-potential candidates for apprenticeships and internships[16] These programs align with the National Initiative for Cybersecurity Education (NICE) Workforce Framework (NIST SP 800-181), which provides a common lexicon for mapping competition-derived competencies to job roles and career pathways Furthermore, federal research initiatives such as the Cybersecurity Workforce Data Initiative synthesize supply-and-demand metrics, reinforcing the need for non-degree credentialing and experiential learning to address acute shortages[17, 18] Motivated by these global trends, the Iraqi Ministry of Interior launched a nationwide CTF competition in early 2024, with the dual aim of sourcing untapped technical talent and enhancing the operational readiness of its Cybersecurity Center. Iraq's unique security environment—characterized by persistent regional threats and critical national infrastructure vulnerabilities—necessitates a robust, agile talent pipeline that transcends conventional hiring practices. By leveraging a CTF-driven approach, the Ministry sought to identify practitioners with proven technical dexterity, regardless of formal educational background, and to integrate them into its incident response and proactive defense teams. This initiative draws on best practices established by leading international programs while tailoring challenge content and logistical execution to local needs.

This paper documents the design, implementation, and evaluation of Iraq's CTF-based talent identification initiative. We employ a mixed-methods research design encompassing case study documentation, experimental screening metrics, qualitative participant feedback, and quantitative performance analysis. Our objectives are fourfold: (1) to detail the competition's operational framework and governance; (2) to assess participant performance and subsequent integration outcomes; (3) to analyze strategic and organizational impacts; and (4) to derive actionable recommendations for governments considering similar skills-based recruitment models. In doing so, we contribute to the broader discourse on cybersecurity workforce development, offering empirical insights and a replicable model for skill-oriented talent acquisition in resource-constrained and high- risk contexts.

Methodology and Result

Beneficiary: Iraqi Ministry of Interior

Implementing Agency: Cybersecurity Center

Competition strategy based on the British company HACK the BOX, which has international standards in cybersecurity.

Target Audience: 64 experiences in applied cybersecurity.

Practical Implementation

The practical component of the CTF competition was carried out in three sequential phases recruitment, screening, and in-person execution following international standards and under accredited supervision. Table 1 summarizes the key dates, activities, and participant numbers.

Phase	Date	Details	Participants

Application Opening	January 14, 2024	Portal launch on Ur (https://ur.gov.iq/); 1,000 seats allocated; emphasis on technical expertise	367 applicants
Preliminary Screening	March 2, 2024	Online CTF-style challenges to assess technical skills; selection of top candidates	64 selected
In-Person Competition	March 16, 2024	Held at the Ministry of Interior Officers Recreation Club; supervised by Cybersecurity Center and CERT	64 participants

Participant Recruitment

i. The recruitment phase was designed to attract a broad cross-section of cybersecurity enthusiasts from across Iraq, emphasizing practical skill over formal credentials. Key details included

ii. Portal Configuration: The UR portal (https://ur.gov.iq/) was configured with a dedicated "CTF 2024" section. Applicants completed fields for name, contact information, region, and a short description of any past cybersecurity work (e.g. personal projects, bug bounties, Capture-the-Flag experience).

iii. Advertising & Outreach: Announcements were disseminated via Ministry of Interior newsletters, social-media channels (Twitter, LinkedIn), and targeted emails to
university cybersecurity clubs. A one-week window (January 14–21, 2024) was allotted for submissions.

iv. Seat Allocation & Confirmation: Though 1,000 seats were available, only 367 candidates applied by the deadline. Within 48 hours of application closure, all applicants received confirmation emails with details on the next stage, along with unique identifiers for the online screening.

v.Qualification Emphasis: The application explicitly stated that academic degrees would not be evaluated; instead, applicants were encouraged to highlight hands-on experience such as participation in online CTFs, use of security tooling, or contributions to open- source security projects.

CTF First stage Screening Process

The screening stage filtered the 367 applicants down to the top 64 through an automated, online CTF assessment. Figure1. illustrates the key participation metrics from the Cybersecurity Center – MOI Capture the Flag (CTF) Competition, held from March 1, 2024, 08:00 to March 2, 2024, 08:00. The figure provides of activity and performance during the event

Figure 1 The figure provides of activity and performance during the event

Where:

•Number of Teams: 367

•Number of Players: 367
•Number of Challenges: 12 Number of Owns (solved challenges): 865
This figure represents the outcome of the initial screening phase, where 367 applicants were successfully filtered and approved to compete through an online automated evaluation process. Each applicant operated individually, hence the number of teams matches the number of players. The competition included 12 cybersecurity challenges across various domains, with participants collectively solving 865 challenges (or "owns"), demonstrating strong engagement and problem- solving performance.
Platform & Environment
A CTF instance hosted on Ministry servers provided 12 preliminary challenges. Each challenge ran inside isolated Docker containers, triggering auto-scoring on successful flag submissions. Figure 2. presents a breakdown of the key challenges solved during the first-stage filtering of contestants in the Cybersecurity Center – MOI CTF competition.

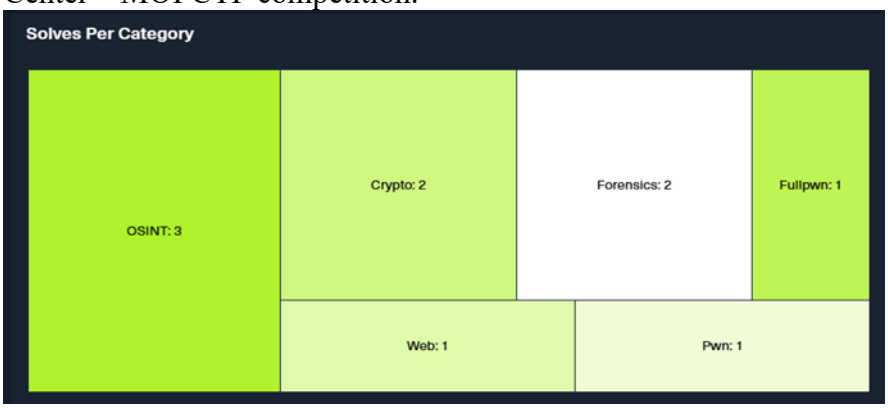

Figure 2 show the key challenges solved during the first-stage
The figure categorizes the challenges by domain and indicates the number of successfully completed tasks per category:
•OSINT (Open Source Intelligence): 3 solves
•Crypto (Cryptography): 2 solves
•Forensics: 2 solves
•Fullpwn (Full Exploitation): 1 solve
•Web (Web Exploitation): 1 solve
•Pwn (Binary Exploitation): 1 solve
This visual distribution reveals that the OSINT category saw the highest number of solves, suggesting a strong proficiency among participants in investigative and intelligence-gathering tasks. Meanwhile, the balance across cryptography, forensics, and exploitation tasks demonstrates the multi-disciplinary nature of the screening challenges. The inclusion of diverse challenge categories ensured that the evaluation covered a comprehensive range of cybersecurity skills, from reverse engineering and digital forensics to vulnerability exploitation and intelligence analysis. This distribution supports the initiative's objective of identifying well-rounded cyber talent with practical, real-world capabilities.
Time & Scoring
Participants had 6 hours to solve all challenges. Each correct flag awarded points (1–5 per task), with bonus time-remaining points to break scoring ties.
Selection criteria results
The top 64 scorers (by total points, then average solve time) included detailed instructions on team registration and logistical arrangements for the in-person round. Figure 3. illustrates the distribution of solved challenges by difficulty level during the initial online qualification phase of the Cybersecurity Center – MOI CTF competition.

Figure 3 solved challenges by difficulty level

This pattern highlights that while participants performed strongly across lower to moderate difficulty levels, no contestant managed to solve the "Hard" level challenges. This could suggest two main insights The hard challenges may have exceeded the current skill ceiling of most applicants, signaling a potential training gap in advanced exploitation or adversarial techniques. The competition successfully stratified participants by ability, with the top 64 scorers advancing based on a combination of total score and average solve time indicators of both efficiency and problem-solving competence. These 64 individuals received detailed instructions for team registration and logistical coordination for the in-person final round, thus bridging the digital and physical phases of talent identification. This difficulty segmentation proved effective in selecting high-potential candidates for further assessment while maintaining inclusive entry through solvable, foundational challenges. Figure 4 analyzes the performance outcomes of participants in the first round of a competitive challenge, based on two dimensions: total points earned and percentage of challenge completion. These indicators are essential for evaluating individual and team efficiency, identifying top performers, and formulating actionable recommendations for academic improvement and future event structuring.

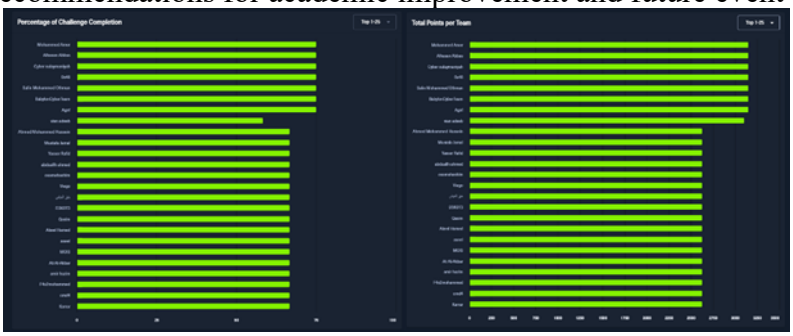

Figure 4 show that the tiering exists among the top 10

Figure 4a (Total Points): Clear tiering exists among the top 10, followed by a gradual taper among others. Figure 4b (Completion %): Visual plateaus at 100% reveal uniform task attempts among most, but also highlight outliers who performed efficiently with fewer completions. Figure 5 show the cumulative point progression of the ten highest-ranked teams throughout the 24- hour cybersecurity contest. The horizontal axis is a continuous time-line that begins at 08:00 on Day 1 and ends at 06:00 on Day 2 (the tick at “MAR 2” marks the midnight crossover). The vertical axis reports the running score in increments of 2,000 points up to the 10,000-point ceiling. Each polyline is color-coded to a team listed in the legend, and the step-wise shape of every line reflects the discrete nature of flag submissions: a vertical jump denotes a successful submission, whereas an extended horizontal segment indicates a period with no additional points.

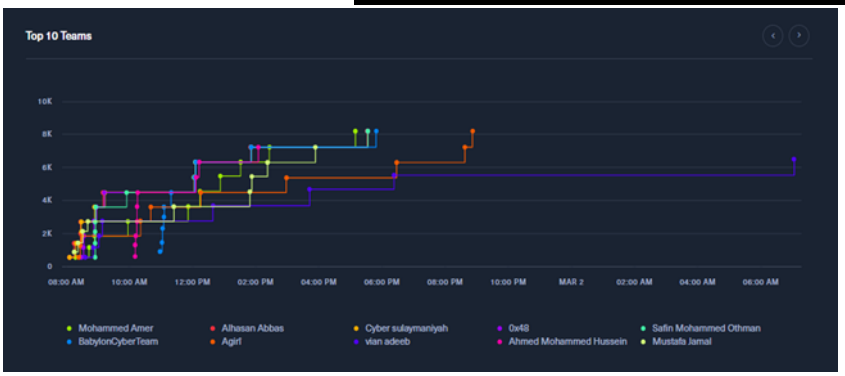

Figure 5 show the cumulative point progression of the ten highest- ranked teams

Figure 5 demonstrates how momentum shifts inside a CTF environment: an aggressive, well- timed scoring burst can overturn early leads, while the absence of fresh vulnerabilities to exploit after the 16-hour mark results in score stagnation. This temporal analysis supports our broader argument that real-time adaptability, rather than sheer velocity of initial discovery, is the principal determinant of competitive success in multi-day security challenges.Figure 6 presents a snapshot of the official scoreboard at the close of Round 1 in the capture- the-flag (CTF) tournament, highlighting both the overall standings and the performance metrics that governed rank allocation.

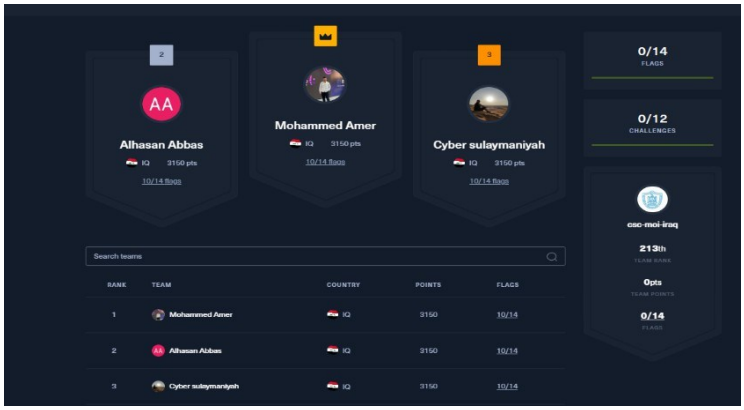

Figure 6 scoreboard at the close of Round 1 in the capture-the- flag (CTF)

That early and efficient flag

discovery, rather than sheer point volume alone, determines leadership when competitors achieve parity in raw score. All three leading teams solved an identical subset of challenges (71% completion), yet the ranking algorithm prioritized temporal precedence, rewarding the team that reached the 3,150- point threshold first. This observation lends empirical support to our broader argument that time-to- exploit is a decisive success factor in multi-team cyber-operations, where strategic sequencing of exploits can deliver a podium finish even when technical capability is evenly matched across the cohort.

Final stage In-Person Competition Execution

On March 15, 2024, the live CTF took place under strict operational controls

Venue & Infrastructure

The Officers Recreation Club network was isolated from the Ministry's general infrastructure. Eight high-performance servers hosted virtual machines, each pre-loaded with target systems. Participants used wired workstations with uniform hardware and dual-monitor setups.

Supervision & Security

Certified proctors from CERT monitored the competition floor, enforcing a no-mobile-device policy and using network-traffic analysis tools (Zeek, Suricata) to detect unusual scanning or exfiltration. A live scoreboard projected into the main hall displayed team rankings in real time.

Rules & Resources

Teams were allotted 6 hours. Allowed resources included personal laptops with standard Penetration Testing distributions (Kali Linux), but all network traffic had to pass through centralized proxies. A helpdesk channel (via encrypted chat) addressed technical issues without revealing hints.

Competition Framework

Adhering to Hack the Box's accredited model, the CTF comprised three escalating tiers show in table 2

Tier	Challenges	Point Range per Challenge	Expected Solve Time
Easy	12	1-100	30–60 minutes
Medium	12	1-100	60-120 minutes
Difficult	12	1-100	120–180 minutes

CTF final stage Screening Process

Scenario Design

Challenges were crafted to reflect real-world adversary tactics and required a spectrum of technical skills:

Custom Exploit Development

Binary Reverse-Engineering: Teams dissected a stripped Linux ELF binary to locate buffer-overflow vulnerabilities, then developed ROP chains to spawn a shell.

Memory Forensics: Extracting secrets from a live memory dump using Volatility. Web Application Attacks

SQL Injection Lab: A three-page PHP application vulnerable to union-based injection; teams exfiltrated user credentials.

Insecure Deserialization: A Java servlet task where deserializing untrusted input allowed remote code execution.

Open-Source Intelligence (OSINT)

Social Media Recon: Given a public Discord invitation and minimal aliases, participants mapped a target's online footprint to discover hidden API keys.

Metadata Analysis: Extracting GPS coordinates and creation timestamps from images to locate a mock "safe house."

Figure 7 provides a concise statistical overview of the Cybersecurity-MOI capture-the-flag (CTF) final, held on 16 March 2024 from 06:00 to 15:00. Four key participation metrics are displayed in separate dark-background tiles:

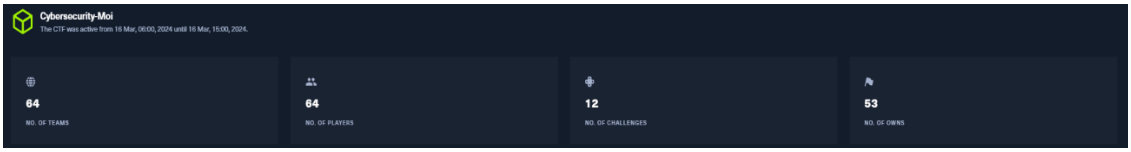

Figure 7 a concise statistical overview of the Cybersecurity-MOI capture-the-flag (CTF) final

Taken together, the figure contextualizes the competitive environment in three ways:

.١Scale. With 64 solo participants, the final round maintained a moderate but manageable field size, enabling meaningful head-to-head comparisons without diluting scoreboard resolution.

.٢Challenge density. The 12-challenge slate strikes a balance between breadth (multiple technical domains) and depth (sufficient points per solve to differentiate performance).

.٣Difficulty calibration. The low aggregate solve rate (7 %) confirms that the organizers targeted expert-level proficiency, ensuring that even a handful of successful exploits could materially alter rankings—an insight that underpins our subsequent analysis of time-to-exploit dynamics

Figure 8 summarizes how the 64 finalists fared against the twelve tasks that composed the championship problem set, disaggregating performance by difficulty and by individual challenge.

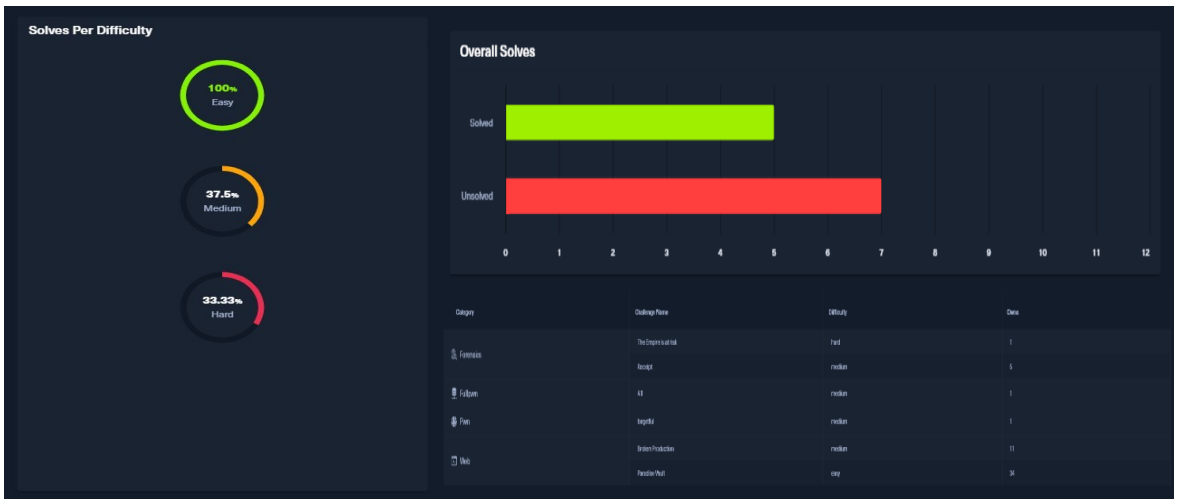

Figure 8 show the Solves per Difficulty and Overall Challenge Completion (Final Round

Difficulty-level success rates Three circular gauges convey, at a glance, the proportion of challenges in each tier that yielded at least one flag. The sole Easy task was solved by competitors in every instance (100 %), whereas only three of the eight Medium challenges (37.5 %) and one of the three Hard challenges (33.33 %) were conquered. The steep drop from the easy to the medium tier illustrates the sharp escalation in technical complexity embedded by the organizers.Global completion tally The horizontal bar chart aggregates these outcomes, showing that five challenges were solved and seven remained untouched. Thus, only 42 % of the available tasks surrendered a flag during the nine-hour final—an overall solve rate that attests to the event's elevated difficulty.Task-specific results. The accompanying table pinpoints which problems fell. The web-exploitation exercise Paradise Vault produced the most traffic, accounting for 34 of the 53 flags captured across the entire field. The next most-frequent solve, Broken Production (web, medium), delivered 11 flags, while three additional challenges—Receipt (forensics, medium), A1 (fullpwn, medium), and forgetful (pwn, medium)—recorded between one and five solves each. Only a single competitor breached the hardest problem, The Empire is at Risk (forensics, hard).Interpretation. These statistics reveal a pronounced skew, the majority of participants prioritized the lone easy web challenge to secure baseline points, leaving the bulk of medium and hard tasks either partially or wholly unexplored. Consequently, competitive differentiation hinged on two factors: (i) rapid identification of the sparse low-hanging fruit, and (ii) specialized expertise capable of unlocking at least one high-value hard target. The data therefore reinforce the study's wider argument that success in expert-level CTF finals depends less on the breadth of attempted categories than on strategic task triage and depth-oriented exploitation skills.Figure 9. Individual Challenge-Completion Rates and Corresponding Scores Final Round Figure 9 pairs two horizontal-bar charts to portray how each of the twenty-five highest-ranked finalists translated solved challenges into points.

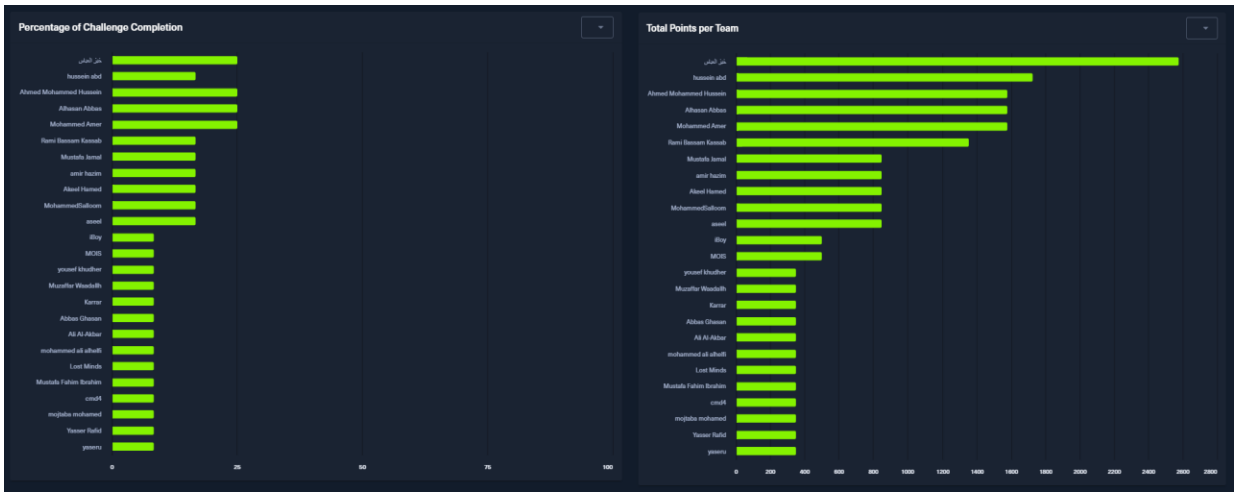

Figure 9 Individual Challenge-Completion Rates and Corresponding Scores Final Round

The winner captured only one task more than most of the chasing pack (three vs. two), yet amassed nearly 2 800 points, compared with ≤ 1 600 points for rivals. This underscores the leverage gained from targeting hard or medium-tier problems with larger point allocations. Scores fall off rapidly after the top five positions. Competitors ranked 10th-through-25th remain compressed in a narrow 250- to 800-point band, indicating that a single additional flag especially a medium-difficulty one—would have reshuffled mid-table standings. While the ordering of names is broadly similar across both panels, the spacing between bars differs: each extra percentage point of completion yields progressively larger point gains because problems are weighted by difficulty rather than counted equally. In finals calibrated to an expert level, comprehensive coverage of all 12 tasks is unrealistic. Competitive advantage instead comes from (i) rapid identification of any "easy" openings and (ii) deep, focused work on one or two high-reward targets. Teams aiming for podium positions should allocate effort accordingly, rather than spreading evenly across the entire slate.Taken together, the twin charts in Figure 9 visualise how selective depth—solving a handful of high-value challenges proved more decisive than broad but shallow coverage, a finding consistent with the time-to-exploit analysis presented earlier in this study.Ultimately, the top ten winners of the competition were selected, ranked by region, and assigned to the Iraqi Ministry of Interior's Cybersecurity Center, where they will be deployed to secure cyberspace. Among the team's most notable achievements after their employment with the Ministry of Interior on March 8, 2025, was their participation in international competitions, winning first place in the "Sole Cyber" competition, sponsored by the British company "Hack the Box." On March 26, 2025, the team placed 19th globally in the "Cyber Wars" competition. The team also won fourth place in the "Tales from Elborea" competition.

Conclusions

CTF competitions are a viable, cost-effective filter for high-potential cyber talent. The three- phase model piloted by Iraq's MOI reliably reduced a pool of 367 self-selected applicants to 64 qualified finalists and, ultimately, to 10 hires whose post-employment performance in international events validates their readiness for real-world operations. Speed and depth matter more than breadth. Event telemetry shows that "time-to-exploit" on a small number of high-value flags predicted podium finishes better than broad but shallow coverage; finalists who solved just one hard challenge out-scored rivals who cleared several easy ones. This finding should inform future scoring rubrics and training road-maps. Competence often lies outside formal academic channels. A significant share of top performers lacked university degrees but demonstrated skill parity with junior incident-response staff, suggesting that degree-centric hiring inadvertently overlooks capable practitioners. Integrating non- traditional pathways can narrow acute workforce gaps faster. Operational security and governance are essential for government-run CTFs. Isolated networks, certified proctors, and live traffic monitoring prevented collateral risk while preserving competitive realism—a blueprint other ministries can replicate without exposing production systems. Under-represented skill areas remain a blind spot. Low solve rates in social-engineering and hard-level forensics challenges highlight curricular gaps that should be addressed in future iterations to produce more well-rounded defenders.

References

[١]F. Goupil, P. Laskov, I. Pekaric, M. Felderer, A. Dürr, and F. Thiesse, "Towards understanding the skill gap in cybersecurity," in Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education Vol. 1, 2022, pp. 477-483.

[٢]W. Crumpler and J. A. Lewis, Cybersecurity workforce gap. JSTOR, 2022.

[٣]C. A. Jordan, Exploring the cybersecurity skills gap: A qualitative study of recruitment and retention from a human resource management perspective. Northcentral University, 2022.

[٤]S. J. H. B. R. h. h. o. w.-d.-b.-s.-i.-. Madnick, "Why data breaches spiked in 2023," 2024.

[٥]C. S. Teoh and A. K. J. T. E. R. Mahmood, USA, "Cybersecurity workforce development for digital economy," vol. 2, no. 1, pp. 136-146, 2018.

[٦]S. J. C. Furnell and Security, "The cybersecurity workforce and skills," vol. 100, p. 102080, 2021.

[٧]R. J. S. j. Vogel, "Closing the cybersecurity skills gap," vol. 4, no. 2, pp. 32-46, 2016.

[٨]C. Worley, "Hacking the skills shortage a study of the international shortage in cybersecurity skills," in JA Lewis (Chair), Hacking the skills shortage A study of the International shortage in Cybersecurity skills [Video file]. Symposium conducted at the meeting of Center for Strategic & International Studies, Washington, DC. Retrieved from https://www. csis. org/events/hacking-skills-shortage, 2016.

[٩]V. Švábenský, P. Čeleda, J. Vykopal, S. J. C. Brišáková, and Security, "Cybersecurity knowledge and skills taught in capture the flag challenges," vol. 102, p. 102154, 2021.

[١٠]T. Balon, I. J. E. Baggili, and I. Technologies, "Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education," vol. 28, no. 9, pp. 11759-11791, 2023.
[١١]B. Malawski, "Cyber gamification: The use of capture the flag (ctf) and similar exercises to develop critical-thinking and problem-solving skills in cyber graduates," Utica College, 2018.
[١٢]L. Topham, K. Kifayat, Y. A. Younis, Q. Shi, B. J. I. Askwith, and Security, "Cyber security teaching and learning laboratories: A survey," vol. 35, no. 1, p. 51, 2016.
[١٣]A. Tay, S. M. Hayes, D. Wilson, E. Hall, D. J. I. i. I. S. Kaufman, and I. Technology, "Gamified Cybersecurity Education Through the Lens of the Information Search Process: An Exploratory Study of Capture-the- Flag Competitions [Research-in-Progress]," vol. 21, p. 001, 2024.
[١٤]S. Buckley, "An Analysis and Ontology of Teaching Methods in Cybersecurity Education," Louisiana State University and Agricultural & Mechanical College, 2024.
[١٥]I. J. I. T. E. J. o. S. S. R. Kamara, "European cybersecurity standardisation: a tale of two solitudes in view of Europe's cyber resilience," pp. 1-20, 2024.
[١٦]N. R. Council et al., Professionalizing the nation's cybersecurity workforce?: Criteria for decision- making. National Academies Press, 2013.
[١٧]R. Petersen, D. Santos, M. Smith, and G. Witte, "Workforce framework for cybersecurity (NICE framework)," National Institute of Standards and Technology2020.
[١٨]B. J. I. J. o. I. S. Olosunde, Engineering and Technology, "Impact of Cybersecurity Skills Gap on the US Economy and National Security," vol. 11, no. 12, pp. 61-71, 2024.