HackEd: A Pedagogical Analysis of Online Vulnerability Discovery Exercises

Daniel Votipka, Eric Zhang, and Michelle L. Mazurek

Research Questions

Do hacking exercises follow pedagogical best practices?

What challenges do exercise organizers face when applying these principles?

Exercise Criteria

- **Educational –** Intended to teach, not purely competitive
- **Hands-on –** active practice
- **Online –** publicly accessible
- **Popular –** Tranco/Alexa rank

CSAW 365, RootMe –Hacking platform–, HackEDU, picoCTF, Hack The Box PEN-TESTING LABS, girls go cyberstart, hackerone

Pedagogical Dimensions

Connecting to Prior Knowledge

Personalization: Does the exercise provide challenges tailored to student age or experience?

Utilization: Does the exercise leverage knowledge from prior challenges to solve later ones?

Results
- Difficulty/point indicators were common
- Not always optimal
- Almost all exercises have concept progression

Organizing Declarative Knowledge

Organization: Are challenges grouped by concept to create a hierarchy or highlight a related problem path?

Context: In what context were challenges presented? Are there lectures, projects, an overarching story, or realistic challenges?

Results
- Many exercises lacked clear structure
- Stories commonly used to provide context
- Few exercises included realistic challenges

Practice and Feedback

Actionability: Are there challenges where the student had to exploit insecure code or write secure code?

Feedback: Do exercises provide direct feedback to guide the student? Are there hints or a forum to ask questions?

Results
- Secure development practice was uncommon
- Feedback is rare
- Students can get help from the community

Metacognitive Learning

Transfer Learning: Do challenges teach *how, when,* and *why* a mitigation or exploit technique should be used?

Support: Are there additional materials linked to provide clarity beyond the exercises' scope?

Results
- Very few exercises guided transfer beyond "How"
- Most exercises provided additional materials

Conducive Learning Environment

Peer Learning: Does the exercise provide support for team formation or an online discussion forum?

Inclusive: Do challenges contain extraneous load? Is supportive terminology used to reassure students?

Results
- Community through online forums
- Teams were rarely explicitly supported
- Extraneous load varies
- Most exercises use supportive terminology

Recommendations

1. Support metacognition through prompts to predict and reflect.
2. Use a graphical syllabus to provide structure.
3. Incentivize creating educational elements in community submissions.