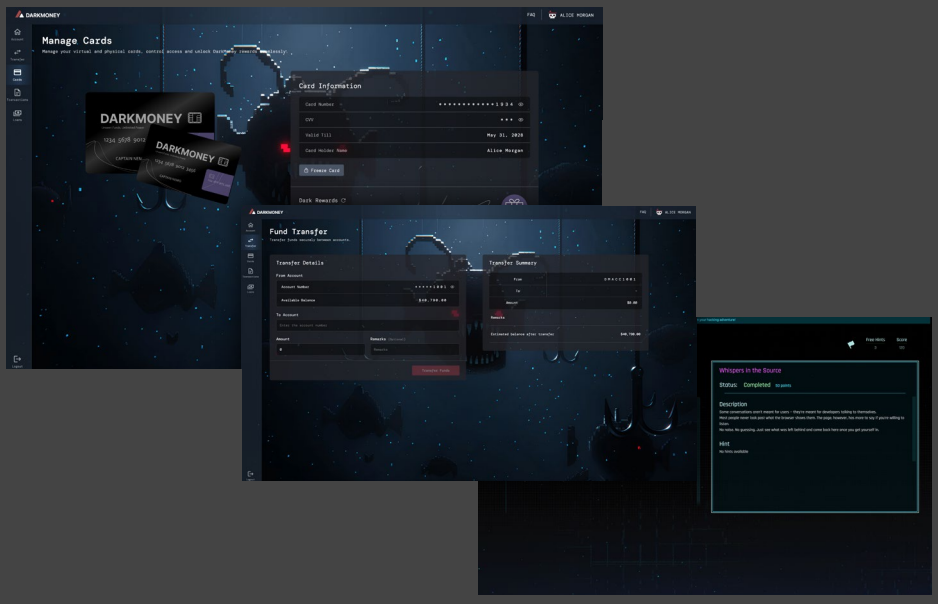
CORE INTERMEDIATE ADVANCED ELITE

LEVEL	INTERMEDIATE DIFFICULTY
TYPE	Digital Banking Platform + Prediction-Market Module
CHALLENGES	33

DARKMONEY

DARK MONEY

Dark Money is a real, fully-functional digital banking platform — but with a gamified twist. It is designed specifically to sharpen ethical hackers' skills against high-stakes financial application attack surfaces: transfers, loans, bill pay, card management, and a live prediction market called the Oracle.

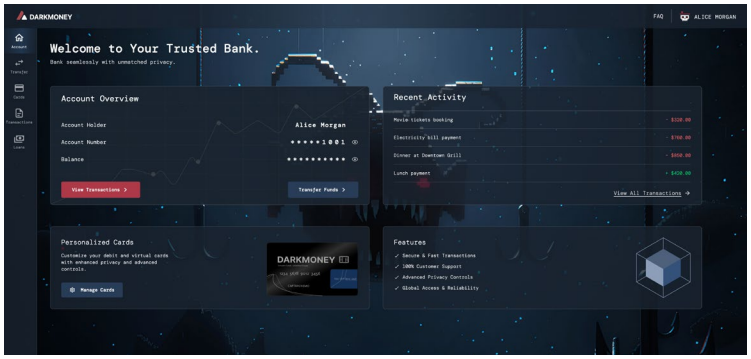


INCLUDES

- A mission-based storyline
- 8 distinct attack surfaces
- Over a dozen vulnerability types
- 33 total challenges
- Challenges appropriate for all roles and experience levels

BACKSTORY

CRWD-CTRL has traced the Illumistrami's laundered funds into **Dark Money**, a bank running its own prediction market known as the Oracle. Participants take on missions that follow the money through the bank's accounts, loans, and bill-pay rails, and through the Oracle's prophecies and tributes — exposing how both the bank and the market are being used to launder funds and manufacture false outcomes.



cmd+ctrl

DARKMONEY

Dark Money at-a-glance

STORYLINE	It's up to the ethical hackers at CRWD-CTRL to follow the Illumistrami's laundered funds through Dark Money's accounts and the Oracle's prediction markets — and shut the operation down.
EXPERIENCE LEVEL	Intermediate
APPLICATION TYPE	Digital banking platform + prediction-market module
TIME CONSTRAINT	Full day or longer, proctor required
ENVIRONMENT	Traditional web; multiple, single-page applications (banking portal + Oracle prediction-market module)
NUMBER AND DIFFICULTY OF CHALLENGES	• 33 challenges • Approximately 24% Easy / 46% Medium / 30% Difficult
TARGET ROLES	• Developers • Application security testers • Security Champions • Wide range of SDLC roles
KNOWLEDGE/ TOOLS REQUIRED	Recommended to have played at least one cyber range prior if not in a technical/ security role; No other special knowledge or tools required
SKILLS GAINED	• How vulnerabilities work in a realistic financial-services environment • Real-world implications of business-logic flaws and access-control gaps in banking and trading systems • Restricting access to accounts, loans, and payment records
HIGHLIGHTED CHALLENGE TYPES	• Business logic flaws • Broken/missing access control • Cross-site scripting (XSS); SQL injection • Account manipulation • Security misconfiguration • XML injection • SSRF • API rate limiting • Credential dumping • And more

ABOUT CMD+CTRL SECURITY

CMD+CTRL Security is a pioneer in software security training. For over two decades, organizations of all sizes, from mid-sized to Global 100 companies, have relied on our training solutions to transform their software security. Our role-based modules, skill labs, and hands-on cyber ranges are designed to build skills that stick. Visit cmdnctrlsecurity.com to learn how we can help you launch a best-in-class training program.

cmd+ctrl