

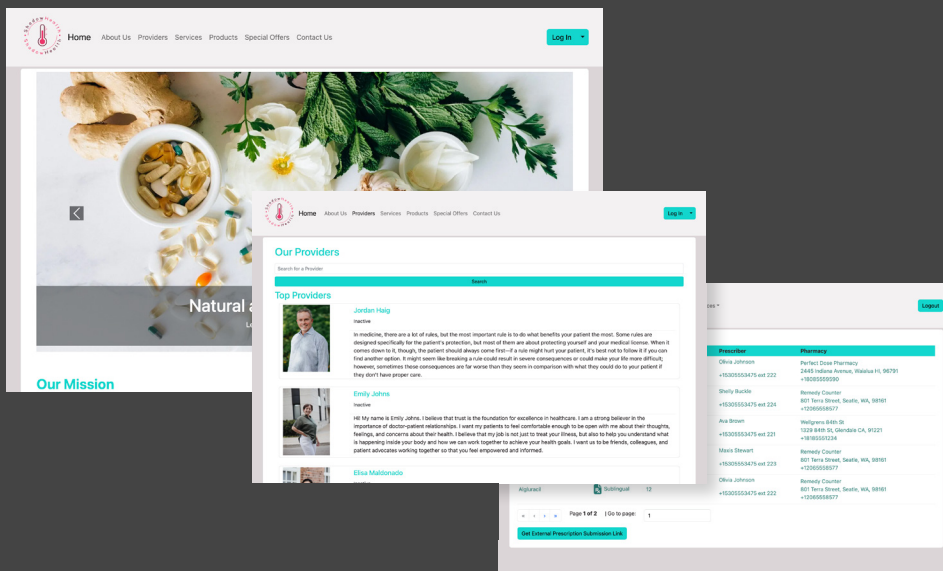
BASIC	INTERMEDIATE	ADVANCED
LEVEL	INTERMEDIATE DIFFICULTY	

TYPE	Health Management Portal
TIMELINE	Full day or longer



SHADOW HEALTH

Shadow Health is a real, fully-functional health management portal — but with a gamified twist. It is designed specifically to modernize your software development teams' application security skills.

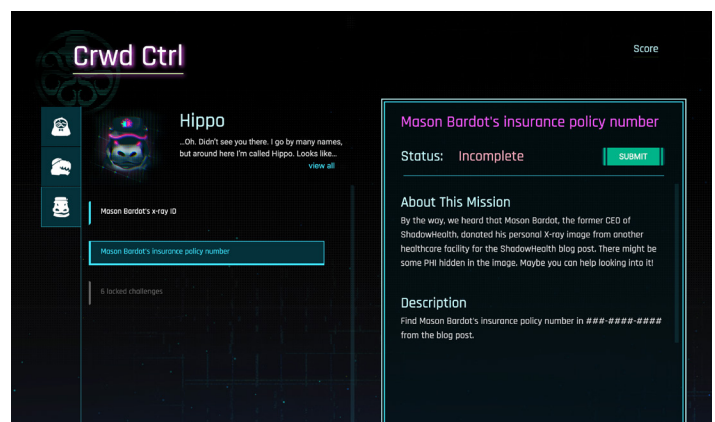


INCLUDES

- A mission-based storyline
- Multiple attack surfaces
- Over a dozen vulnerability types
- Over 45 total challenges
- Challenges appropriate for all roles and experience levels

BACKSTORY

The elite hacking group **CRWD-CTRL** has discovered ties between **Shadow Health** — a seemingly innocuous healthcare provider — and an evil supergroup dubbed **The Illumistrami**. Participants will be given top secret missions called "Bug Bounties" from the CRWD-CTRL Hacker Generals that will help lead them to infiltrate and sabotage Shadow Health from within.





Shadow Health at-a-glance

STORYLINE	It is up to the crowd-sourced ethical hackers at CRWD CTRL to find out what is really going on at Shadow Health... and put a stop to it.
EXPERIENCE LEVEL	Intermediate
APPLICATION TYPE	Health Management portal
TIME CONSTRAINT	Full day or longer, Proctor required
ENVIRONMENT	Traditional web; multiple, single-page applications
NUMBER AND DIFFICULTY OF CHALLENGES	<ul style="list-style-type: none">• 44 challenges• Approximately 50% Easy / 25% Intermediate / 25% difficult
TARGET ROLES	<ul style="list-style-type: none">• Developers• Application security testers• Security Champions• Wide range of SDLC roles
KNOWLEDGE/ TOOLS REQUIRED	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• How vulnerabilities work in a realistic environment• Real-world implications of insecure applications• Restricting access to sensitive data
HIGHLIGHTED CHALLENGE TYPES	<ul style="list-style-type: none">• Broken access control• Parameter tampering• Insecure design• Integer overflow• API parameter tampering• Injection• Password Cracking• Cross-site scripting (XSS)• And more.. Including SSRF and Log4Shell

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 cmdntrlsecurity.com to learn how we can help you launch a best-in-class training program.