**Bezpieczeństwo Aplikacji Webowych**

**OWASP Juice Shop**

Raport

Celem zadania jest znalezienie oraz exploitacja jak największej liczby podatności. W aplikacji znajdują się wyzwania, które w projekcie będą kolejno wykonywane od najłatwiejszego do najtrudniejszego poziomu:

* Trivial challenge
* Easy challenge
* Medium challenge
* Hard challenge
* Dreadful challenge
* Diabolic challenges.

Wyzwania podzielone są na różne kategorie, głównie w oparciu o OWASP TOP 10:

* Broken Access Control
* Broken Anti Automation
* Broken Authentication
* Cryptographic Issues
* Improper Input Validation
* Injection
* Insecure Deserialization
* Miscellaneous Challenges
* Security Misconfiguration
* Security through Obscurity
* Sensitive Data Exposure
* Invalidated Redirects
* Vulnerable Components
* XSS
* XXE