



replit.dev/logs

Attack Logs

Detailed log of all SSH attack attempts

Attack Log Entries

Showing 1 - 6 of 6 entries

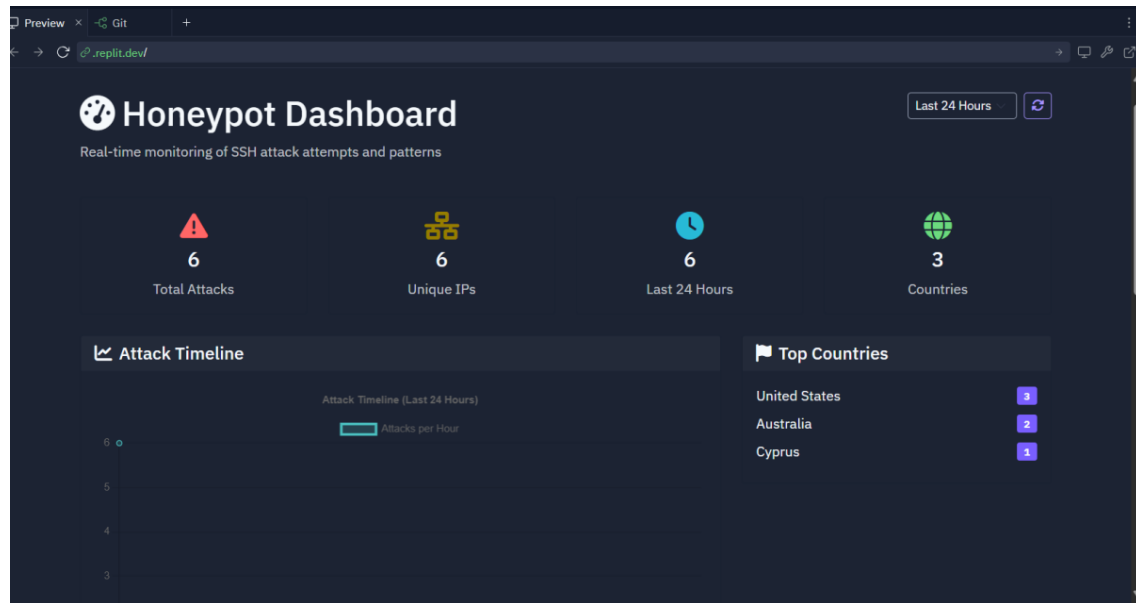
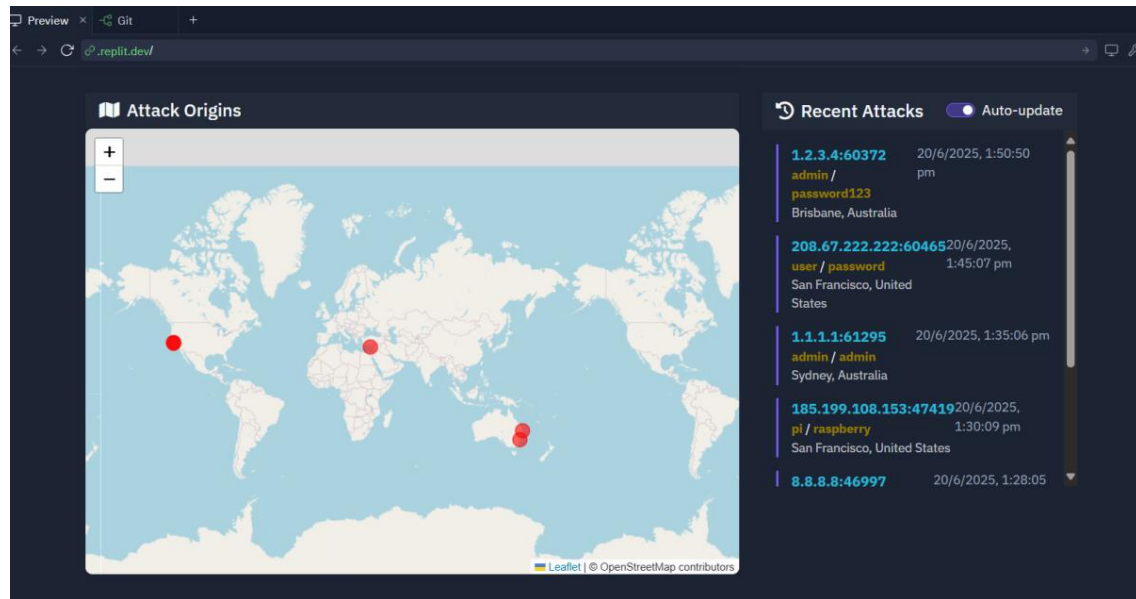
Timestamp	Source IP	Location	Credentials	Session	Type
2025-06-20 13:50:50	1.2.3.4:60372	Brisbane, Australia	admin / password123	demo-ses...	ssh_login
2025-06-20 13:45:07	208.67.222.222:60465	San Francisco, United States	user / password	session-...	ssh_login
2025-06-20 13:35:06	1.1.1.1:61295	Sydney, Australia	admin / admin	session-...	ssh_login
2025-06-20 13:30:09	185.199.108.153:47419	San Francisco, United States	pi / raspberry	session-...	ssh_login
2025-06-20 13:28:05	8.8.8.8:46997	Mountain View, United States	root / 123456	session-...	ssh_login
2025-06-20 13:26:08	176.103.130.130:56715	Limassol, Cyprus	root / toor	session-...	ssh_login

SSH Honeypot System

Monitoring and logging SSH attack attempts for cybersecurity research.

Server running on port 2222

Dashboard on port 5000



Security Insights

**High Attack Volume**
Monitor for unusual spikes in attack attempts

**Credential Patterns**
Common username/password combinations indicate automated attacks

**Geographic Spread**
Attacks from multiple countries suggest botnet activity

Honeypot Status

SSH Honeypot Active

Service Port:2222

Protocol:SSH v2.0

Logging:Enabled

Geolocation:Active

Export Data

Export attack data for further analysis or reporting.

Export as JSON

Export as CSV

Generate Report

SSH Honeypot System

Monitoring and logging SSH attack attempts for cybersecurity research.

Server running on port 2222

Dashboard on port 5000