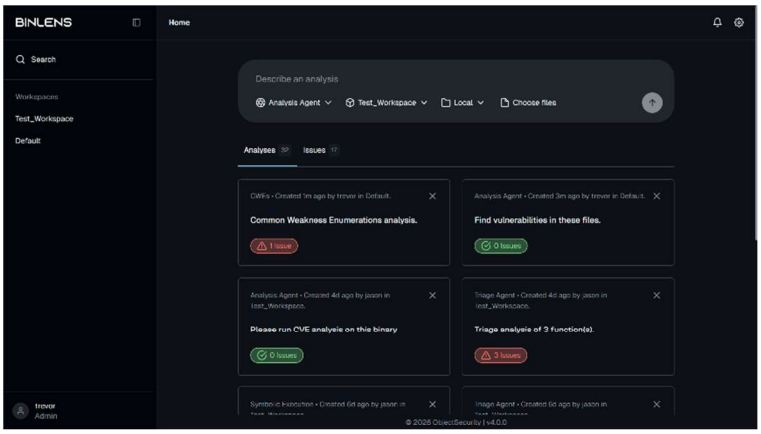
ObjectSecurity BinLens™ Automated Binary Vulnerability Analysis

ObjectSecurity™ BinLens™ 4.0.0

Automated Binary Vulnerability Analysis

Effortlessly uncover zero-day vulnerabilities in binaries and source code with cutting-edge accuracy and minimal false positives.



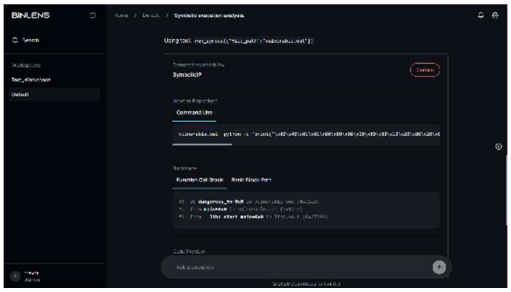
Why:

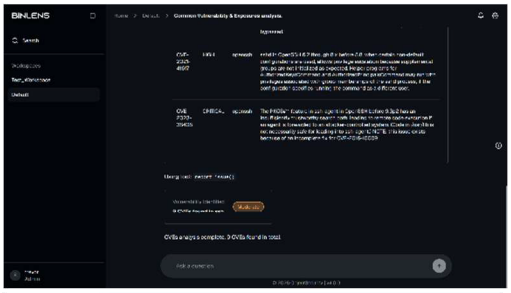
- SBOM generation is limited to detecting only known vulnerabilities in published software.
- Source code analysis and static application security testing (SAST) produce too many false-positives, slowing down remediation.
- Network scanning fails in cases where devices are not connected to the network.
- ~20-70% of OT/ICS assets are end-of-life/legacy devices, lack source, or there are no patches.
- Talented reverse engineers are hard to find and manual reverse engineering is time consuming.

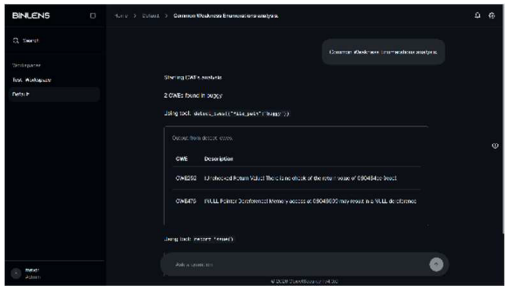
What:

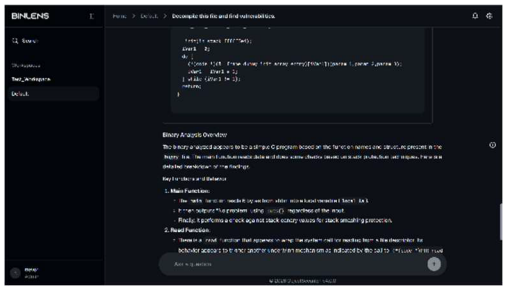
- Unlock deeper security insights with BinLens™ advanced binary analysis.
- Coordinates teams of AI agents to uncover potential zero-days with unmatched precision.
- Powered by automated symbolic execution, it excels at detecting memory-safety violations and other undefined behaviors in binaries, delivering a dramatically lower false-positive rate than competing tools.
- Automates key manual reverse engineering tasks like static analysis, disassembly, and decompilation.
- Primarily does not rely on known vulnerabilities.
- Flexible deployment—on-prem/offline or cloud.
- Supports 30+ CPU architectures, 50+ file formats.

ObjectSecurity™ BinLens™









Features:

- **Agentic AI-Enabled Analysis:** orchestrate AI agent ensembles to detect vulnerabilities
- **Large Project Navigation:** supports projects comprised of 1000s of binaries/source code files
- **Stack Overflows:** detect unsafe writes to the stack frame
- **Heap Overflows:** detect unsafe writes to dynamically allocated memory
- **User Controlled Program Redirection:** detect user-arbitrary code execution
- **Externally Controlled String Violation:** detect unsafe use of the *printf* family, output vital data
- **Out-of-Bound Array Index:** detect out-of-bounds writes/reads
- **Double Free:** detect repeat frees
- **NULL Pointer Dereference**: detect NULL dereferences, unintended memory access
- **Use After Free**: detect the illegal reuse of freed memory
- **Cryptographic Issues:** embedded keys, entropy, encryption schemes
- **18,000 CVEs**: focused on known OT/ICS binary vulnerabilities
- **~25 CWEs:** primarily memory-safety related
- **Malware:** detect known malware signatures
- **Integration**: respond to version control events in GitLab/GitHub; emit automatic notifications

Who:

- **Red Teams, Reverse Engineers, Threat Hunters, and Vulnerability Researchers**
  Speed up your manual reverse engineering workflow. Dive deeper into binary executables using advanced automated analyses that are too unwieldy, expensive, and slow to perform manually.
- **DevSecOps Engineers, Product Security, QA Testers, and Software Developers**
  Detect vulnerabilities that SBOM generators and SAST tools miss. Integrate into your DevSecOps pipeline.
- **Operators, Buyers/Procurement**
  Reduce supply chain risks in your IT/OT/ICS environment. Require analysis in RFPs. Analyze during deployment and patching to ensure no vulnerabilities are introduced. Scan legacy devices to ensure they are safe, even if the manufacturer won't.

Request Quote

On-Prem/Offline Kubernetes Deployment
Or
On-Prem/Offline VM Deployment
Or
Cloud Deployment

Scan to Visit Website

We provide precision vulnerability detection for defense and critical infrastructure.

815 E Street, Box #12070
San Diego, CA 92101
USA

Main US Phone: +1 (650) 515-3391

Email: salesinquiry@objectsecurity.com