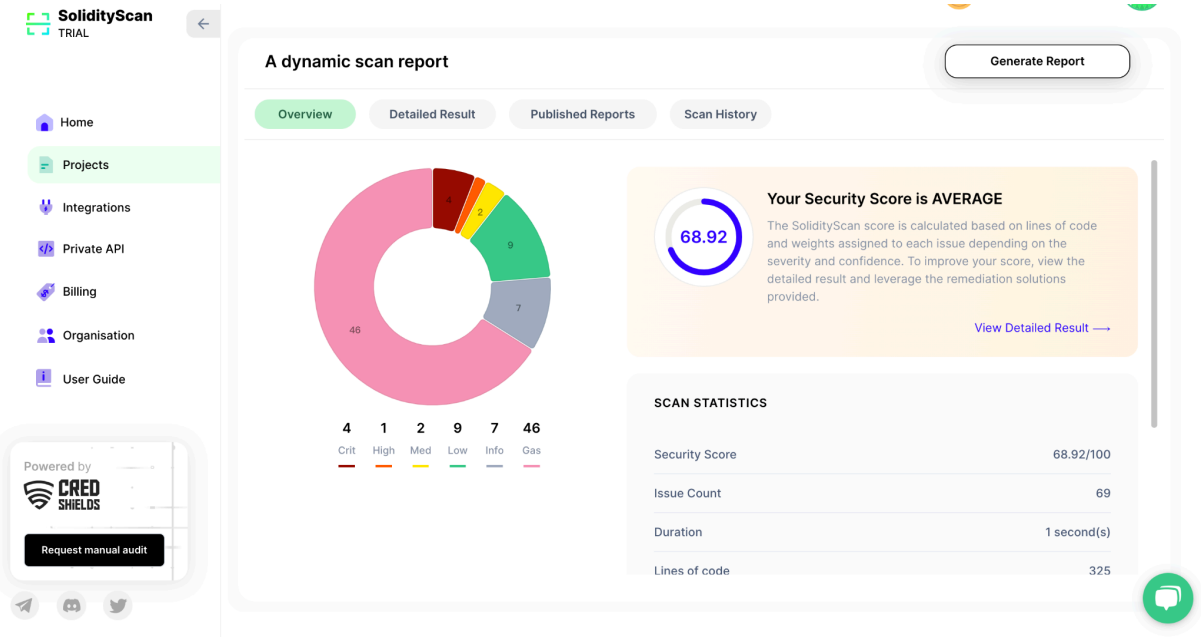
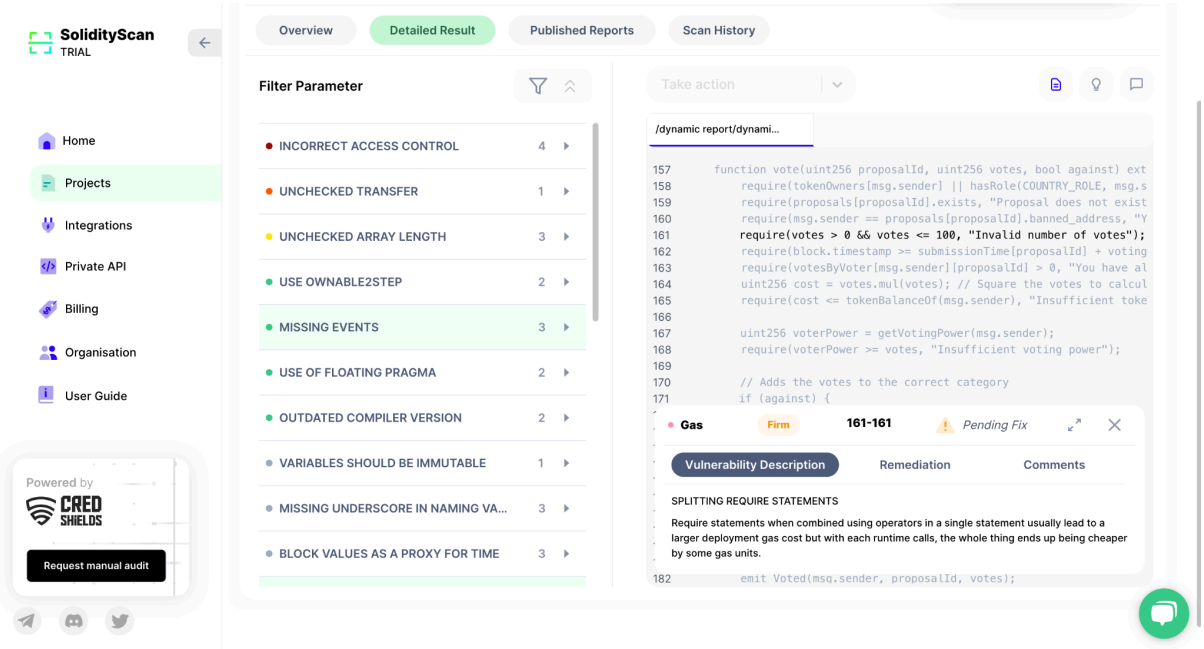
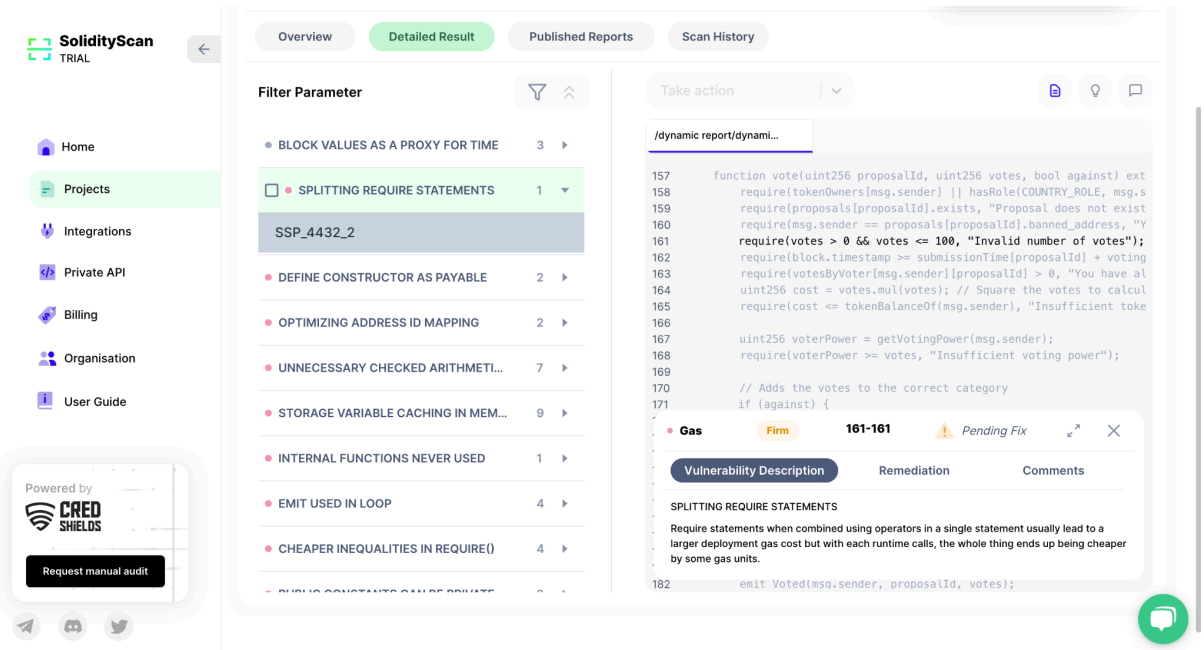
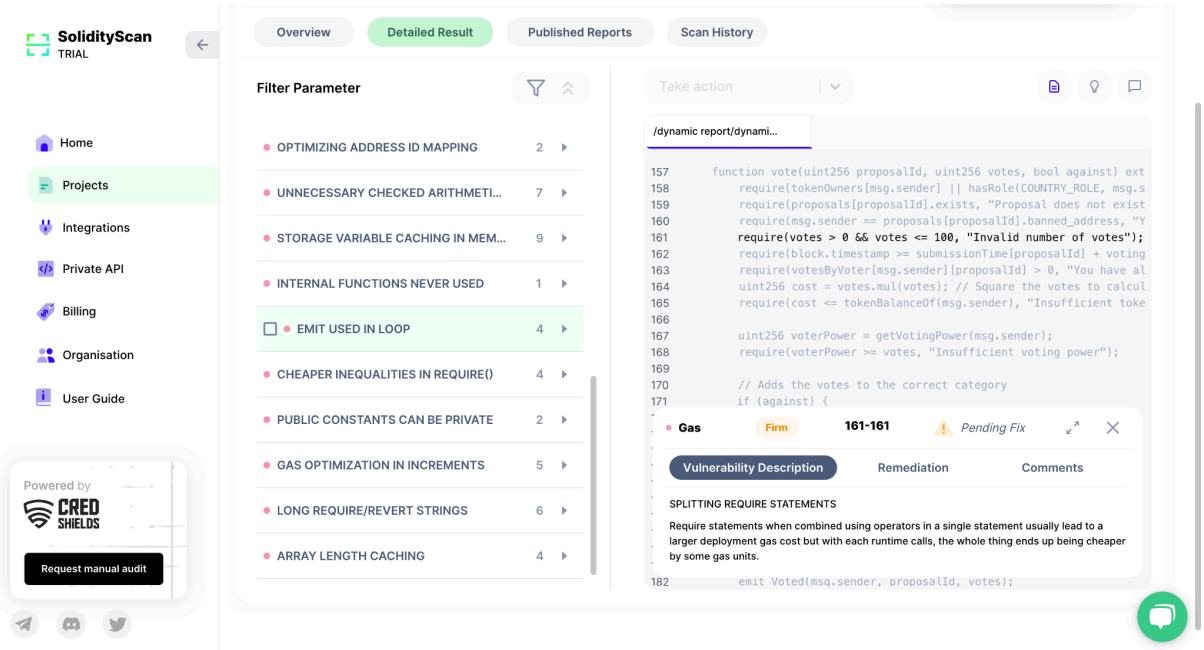
A dynamic scan report






SolidityScan
TRIAL
Home
Projects
Integrations
Private API
Billing
Organisation
User Guide
Powered by
CRED SHIELDS
Request manual audit
Overview
Detailed Result
Published Reports
Scan History
Filter Parameter
BLOCK VALUES AS A PROXY FOR TIME 3
SPLITTING REQUIRE STATEMENTS 1
SSP_4432_2
DEFINE CONSTRUCTOR AS PAYABLE 2
OPTIMIZING ADDRESS ID MAPPING 2
UNNECESSARY CHECKED ARITHMETI... 7
STORAGE VARIABLE CACHING IN MEM... 9
INTERNAL FUNCTIONS NEVER USED 1
EMIT USED IN LOOP 4
CHEAPER INEQUALITIES IN REQUIRE() 4
Take action
/dynamic report/dynami...
157 function vote(uint256 proposalId, uint256 votes, bool against) ext
158 require(tokenOwners[msg.sender] || hasRole(COUNTRY_ROLE, msg.s
159 require(proposals[proposalId].exists, "Proposal does not exist
160 require(msg.sender == proposals[proposalId].banned_address, "Y
161 require(votes > 0 && votes <= 100, "Invalid number of votes");
162 require(block.timestamp >= submissionTime[proposalId] + voting
163 require(votesByVoter[msg.sender][proposalId] > 0, "You have al
164 uint256 cost = votes.mul(votes); // Square the votes to calcul
165 require(cost <= tokenBalanceOf(msg.sender), "Insufficient toke
166
167 uint256 voterPower = getVotingPower(msg.sender);
168 require(voterPower >= votes, "Insufficient voting power");
169
170 // Adds the votes to the correct category
171 if (against) {
Gas
Firm
161-161
Pending Fix
Vulnerability Description
Remediation
Comments
SPLITTING REQUIRE STATEMENTS
Require statements when combined using operators in a single statement usually lead to a larger deployment gas cost but with each runtime calls, the whole thing ends up being cheaper by some gas units.
182 emit Voted(msg.sender, proposalId, votes);


SolidityScan
TRIAL
Home
Projects
Integrations
Private API
Billing
Organisation
User Guide
Powered by
CRED SHIELDS
Request manual audit
Overview
Detailed Result
Published Reports
Scan History
Filter Parameter
OPTIMIZING ADDRESS ID MAPPING 2
UNNECESSARY CHECKED ARITHMETI... 7
STORAGE VARIABLE CACHING IN MEM... 9
INTERNAL FUNCTIONS NEVER USED 1
EMIT USED IN LOOP 4
CHEAPER INEQUALITIES IN REQUIRE() 4
PUBLIC CONSTANTS CAN BE PRIVATE 2
GAS OPTIMIZATION IN INCREMENTS 5
LONG REQUIRE/REVERT STRINGS 6
ARRAY LENGTH CACHING 4
Take action
/dynamic report/dynami...
157 function vote(uint256 proposalId, uint256 votes, bool against) ext
158 require(tokenOwners[msg.sender] || hasRole(COUNTRY_ROLE, msg.s
159 require(proposals[proposalId].exists, "Proposal does not exist
160 require(msg.sender == proposals[proposalId].banned_address, "Y
161 require(votes > 0 && votes <= 100, "Invalid number of votes");
162 require(block.timestamp >= submissionTime[proposalId] + voting
163 require(votesByVoter[msg.sender][proposalId] > 0, "You have al
164 uint256 cost = votes.mul(votes); // Square the votes to calcul
165 require(cost <= tokenBalanceOf(msg.sender), "Insufficient toke
166
167 uint256 voterPower = getVotingPower(msg.sender);
168 require(voterPower >= votes, "Insufficient voting power");
169
170 // Adds the votes to the correct category
171 if (against) {
Gas
Firm
161-161
Pending Fix
Vulnerability Description
Remediation
Comments
SPLITTING REQUIRE STATEMENTS
Require statements when combined using operators in a single statement usually lead to a larger deployment gas cost but with each runtime calls, the whole thing ends up being cheaper by some gas units.
182 emit Voted(msg.sender, proposalId, votes);