Threats

- Tampering of the voting application by introducing malicious code
- Obtaining the encryption keys that are hardcoded
- Casting of multiple votes by the same user
- Casting of vote by an attacker using a legitimate voter's account
- Modifying the candidates' information participating in the election
- Modifying the results of the election
- Voting application unable to process the votes due to unavailability
- Leakage of voters' personally identifiable information
- Premature termination of the online voting process
- Exposure of election information to unauthorized parties

Vulnerabilities

CWE ID	Weakness	Description
20	Improper Input Validation	The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly.
22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	The software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory.
23	Relative Path Traversal	The software uses external input to construct a pathname that should be within a restricted directory, but it does not properly neutralize sequences such as ".." that can resolve to a location that is outside of that directory.
79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.
89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	The software constructs all or part of an SQL command using externally influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.
119	Improper Restriction of Operations within the Bounds of a Memory Buffer	The software performs operations on a memory buffer, but it can read from or write to a memory location that is outside of the intended boundary of the buffer.
200	Exposure of Sensitive Information to an Unauthorized Actor	The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.
209	Generation of Error Message Containing Sensitive Information	The software generates an error message that includes sensitive information about its environment, users, or associated data.
269	Improper Privilege Management	The software does not properly assign, modify, track, or check privileges for an actor, creating an unintended sphere of control for that actor.
276	Incorrect Default Permissions	During installation, installed file permissions are set to allow anyone to modify those files.
287	Improper Authentication	When an actor claims to have a given identity, the software does not prove or insufficiently proves that the claim is correct.

306	Missing Authentication for Critical Function	The software does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources.
319	Cleartext Transmission of Sensitive Information	The software transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.
400	Uncontrolled Resource Consumption	The software does not properly control the allocation and maintenance of a limited resource, thereby enabling an actor to influence the amount of resources consumed, eventually leading to the exhaustion of available resources.
401	Missing Release of Memory after Effective Lifetime	The software does not sufficiently track and release allocated memory after it has been used, which slowly consumes remaining memory.
434	Unrestricted Upload of File with Dangerous Type	The software allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment.
522	Insufficiently Protected Credentials	The product transmits or stores authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval.
532	Insertion of Sensitive Information into Log File	Information written to log files can be of a sensitive nature and give valuable guidance to an attacker or expose sensitive user information.
613	Insufficient Session Expiration	"Insufficient Session Expiration is when a web site permits an attacker to reuse old session credentials or session IDs for authorization."
614	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute	The Secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over an HTTP session.
732	Incorrect Permission Assignment for Critical Resource	The product specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.
770	Allocation of Resources Without Limits or Throttling	The software allocates a reusable resource or group of resources on behalf of an actor without imposing any restrictions on the size or number of resources that can be allocated, in violation of the intended security policy for that actor.
787	Out-of-bounds Write	The software writes data past the end, or before the beginning, of the intended buffer.
862	Missing Authorization	The software does not perform an authorization check when an actor attempts to access a resource or perform an action.
863	Incorrect Authorization	The software performs an authorization check when an actor attempts to access a resource or perform an action, but it does not correctly perform the check. This allows attackers to bypass intended access restrictions.