How ESAPI Works

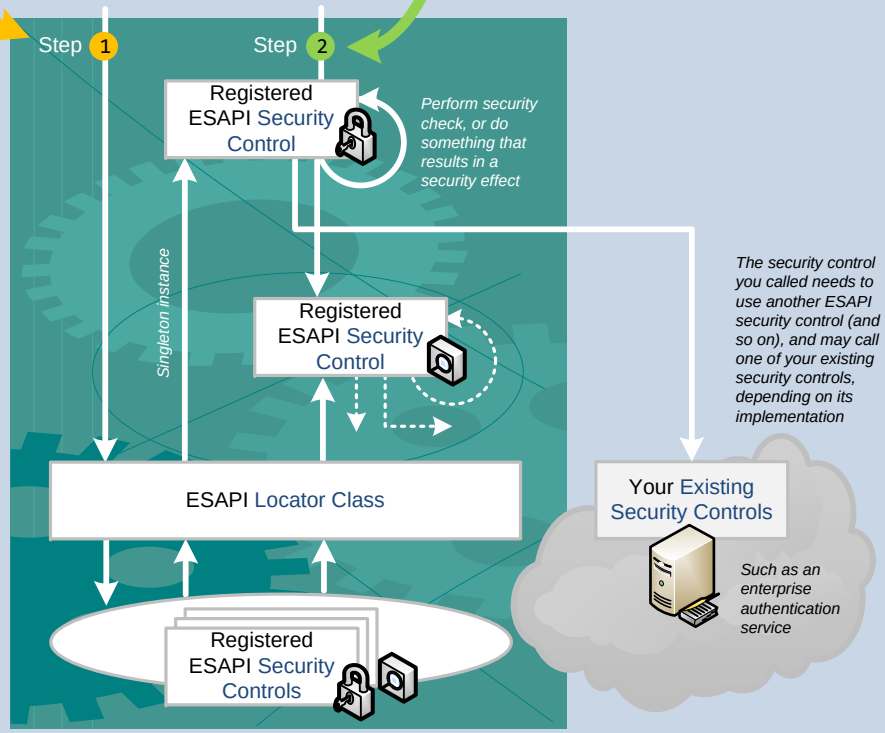
Example

Sample code:

Naming conventions such as this are not part of ESAPI but are good practice

```
$clean = array();
$clean_sql = array();
$clean['id'] = ESAPI::getValidator()->getValidInput( ... );
$clean_sql['id'] = ESAPI::getEncoder()->encodeForSQL( new MySQLCodec(), $clean['id']  );
```

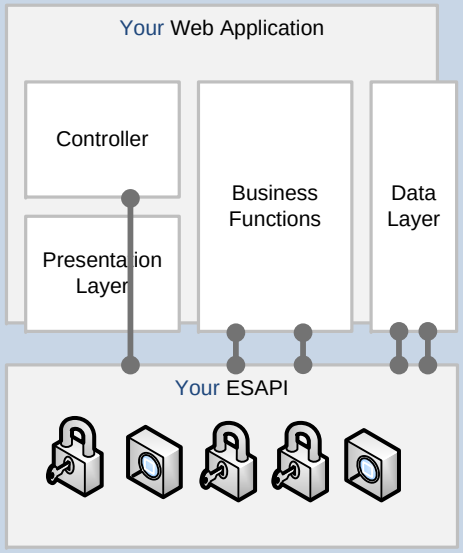
Here is how it works…



OWASP ESAPI includes security control reference implementations. If you don't first register your own implementation, the default will be used when the base class is called to return a security control. ESAPI also has its own configuration mechanism and configuration settings, but these are not depicted for clarity.

One Set of Security Controls

The value of ESAPI is making it easy for the developer to find and use security controls. Using an ESAPI also allows for making security-related fixes (1)quickly, (2)consistently, and (3)correctly across the entire application to target for example an OWASP ASVS level of assurance.



ESAPI is designed to guard against the OWASP Top Ten and to meet OWASP ASVS requirements.