KEEP TALKING and NOBODY GETS HACKED

BOMB DEFUSAL MANUAL

Bombs

Bomb Identification

Just as all applications are different as are all bombs however, they tend to fall into broad categories based on common characteristics. Your bomb will have model information which will help to defuse it.

Archetypes

Model Numbers starting BB are Desktop Applications.
Model Numbers starting C3 are Mobile Applications.
Model Numbers starting FN are Web Applications.
Model Numbers starting R2 are Services Applications.

Methodologies

Model Numbers ending 8R are using Agile methodology.
Model Numbers ending D2 are using Waterfall methodology.

Modules

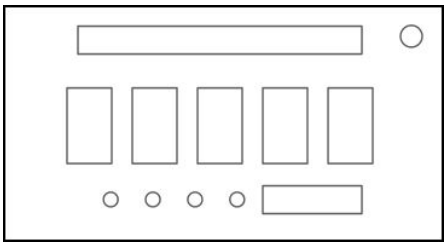
Bombs are made up of multiple modules, each module is discrete and all modules must be disarmed to defuse the bomb.

When modules are armed the LED in the top right corner will be on (see diagram), the LED will turn off when the module has been disarmed.

Modules can be disarmed in any order.

On the Subject of OWASP

OWASP is the Open Web Application Security Project, they publish a list of the ten Most Critical Web Application Security Risks, commonly known as the OWASP Top 10.



Your task is to turn the switches on which map to recognized mitigations for the current risk. When the correct switches are set, hit the submit button. The module will disarm when all four status lights along the bottom of the module are on.

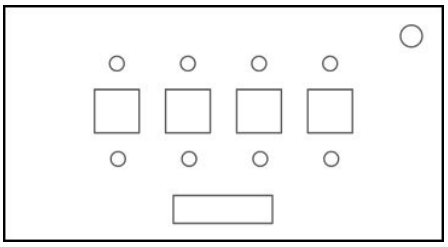
The Switches

Switch one is HTML output encoding.
Switch two is encrypt data at rest.
Switch three is access control lists.
Switch four is positive input validation.
Switch five is using synchronizer tokens.

The switches read left to right.

On the Subject of Assurance

Many different types of tests are run to assure a piece of software is secure however, needs can vary. Your task is to put the tests in the right order for your model of bomb.



Decoding the Symbols

 Threat Modelling/Design Review

 Static Application Security Testing (SAST)

 Dynamic Application Security Testing (DAST)

 Penetration Testing

 Manual Code Review

 Fuzzing

Filled Symbols are fully automated tests, hollow symbols are tests which are manually triggered or executed.

The Rules

All release types should perform Threat Modelling first.
Agile releases should run SAST as early as possible.
DAST runs before Pen Testing but not as early as SAST.
We currently don't so any Fuzzing.
If there is a choice, Agile always fully automate testing.
Manual Code Reviews are never run for Agile releases.
Pen Testing is the last tests that are run.