WebSec Framework

Advanced Training-based Web Application Security Platform

Table Of Content

About The Project

Introduction

This project was started because of the fact that students of Information Security field don't have clear understanding of how Web Application Security works.

Background of this project is experience in training and educating other Computer Security Professionals worldwide performed by the author of this project, Dalibor Vlaho.

From the field, we learned that even some great Security Professionals don't have a clear understanding of Information Security because they " follow the book " and don't put effort to gain some knowledge on their own.

With this project, we'll try to create a platform for learning how to understand things around us and teach how to do things on our own. Thinking is something that an Ethical Hacker MUST DO otherwise he will always be one step behind a malicious hacker.

WebSec will learn us how to perform Sql Injection, Cross Site Scripting, Local File Inclusion, Remote file Inclusion, Code Execution and many more attacks on our own websites to test for vulnerabilities.
On every attack method we will provide explanation and teach others how to prevent those attack methods on their own sites to avoid being hacked.

We know that there is some great Web Applications showing and teaching about Web Application Security but we trying to make some differences with this project.

And just to have in mind, OWASP is a perfect place when we talking about Web Application Security so take your time and visit official website – http://www.owasp.org.

What is WebSec Framework?

WebSec Framework is an Advanced Training-based Web Application Security Platform.

It's meant to be used by individual educators and Training Centers in situations where they need to show, perform and explain Web Application attack methods and give an explanation on how to prevent each attack method.

It's written in PHP and MySQL so it's really easy to setup and use.
Basically, it's a Web Application that you host on your web server (local network).

Donations

Because this is an Open Source, users are not forced to donate but if someone likes our project and effort we put in it, it can donate to our team.
Donations are some kind of showing support for this project.

Team

Team behind this project is well known in Information Security field. Starting with **Dalibor Vlaho**, Ethical Hacker from Croatia, author of this project and many others like **Coulibaly Laïcana**, Wise president of COJI Internationals.

There are some great developers working on this who are responsible for creating new modules and attack tests by following OWASP (Open Web Application Security Project) TOP 10.

How to participate

You can participate in this Project by doing one of the following:

- Suggest modifications that are recognized and implemented
- Create new module or improve existing one
- Write a whitepaper about Web Application attack of your choice and explain it from ground-up including how to prevent that attack

OWASP Top Ten

Please help us make sure that every developer in ENTIRE WORLD knows about OWASP TOP TEN.

A1: Injection
A2: Cross-Site Scripting (XSS)
A3: Broken Authentication and Session Management
A4: Insecure Direct Object References
A5: Cross-Site Request Forgery (CSRF)
A6: Security Misconfiguration
A7: Insecure Cryptographic Storage
A8: Failure to Restrict URL Access
A9: Insufficient Transport Layer Protection
A10: Unvalidated Redirects and Forwards

Visit official OWASP website to stay up-to-date with all new threads and attack methods.
There is also some great information, projects and many more interesting things so please click on the link below:

http://www.owasp.org

Development

Contributors

On this project we have contributors from around the world that put their effort creating new and modify an existing features in this Web Application.
Just because this is an Open Source Project, anyone around the world can join us and become contributor and make this project bigger and better.

Technology

Ahh, it's quite simple, this Web Application is written in PHP and relay on MySQL. It's very flexible and easy customizable.
There is some JavaScript Libraries written by our members and contributors but they are not yet implemented in this project.

Also there will be some AJAX-based attacks so students will learn how to use this technology against websites.

Technology section will be updated later on, after we implement new features.

Modules

Well, modules are the core of this project. Modules contain attack tests that student need to pass in order to gain clear knowledge and understanding of Web Application Security.
They also show and explain how each attack method work and how to prevent those attacks.
Modules are grouped as follow:

Basic Skills
Advanced Skills
Realistic Attacks
Real World Hacking

Basic Skills
Basic Skills Group contains tests like Sql Injection, Cross Site Scripting, Password Cracking etc. attacks.
Students will be presented with the basic web application attack methods.

Advanced Skills
Advanced Skills will teach students how to analyze, discover and fix vulnerable code inside web applications. Also there are some more tests for learning.

Realistic Attacks
Realistic Attacks are great way to learn how Web Application Security works in real world. Students will try to break into websites by following test rules.

After the test is over, student will learn how a particular attack method works and learn to prevent that kind of attack.

Real World Hacking
This is for professionals. On a local network, there will be vulnerable machine that student need to exploit and follow the test rules and instructions.

Actually, this is not a Web Application Security but it will be a part of an test about Web Application Security.

Usage

For security reasons, we recommend to host this application on a private server located inside local network. For this you can use:

WAMP – Windows
MAMP – Mac OS X
LAMP – Linux

Above applications are easy to download and install. Setup a server in your local network, install above application and then access it by navigating to:

http://localhost

Be sure to set a port to 80 (Default http protocol port).

After you configure your web server it's time to add WebSec to it.
Download WebSec from the GitHub and put " websec " directory to your web server root folder. It should look like this:

http://localhost/websec/

Navigate to above web location to be sure that everything works properly.

If you got an error or something is missing, then navigate to:

websec/inc/config.php

And

websec/inc/menu.php

And change settings in those two php files.

When you done with the settings, it's time to rock 'en roll.

Now you ready to use WebSec Application with your students and show them some great way on how to learn and understand how Web Application Security works in real life.

Don't panic! WebSec will notify you about new updates. When our development team release new updates, WebSec will show you about that so you can download new version of WebSec.

FAQ

1. What is WebSec Framework?
WebSec Framework is an Advanced Training-based Web Application Security Platform. Basically, it's a Web Application that you host on your web server.

2. Who can use it?
WebSec it's meant to be used by Training Centers and individual educators who provide training services and need to show some practical examples of Web Application attacks.

3. Can I host it on production server?
Of course! But we DO NOT recommend this. Instead, create a server on your local network. Example of this would be: WAMP for Windows, MAMP for Mac OS X and LAMP for Linux.

4. How to participate in this Project?
You can participate in this Project by doing one of the following:

- Suggest modifications that are recognized and implemented
- Create new module or improve existing one
- Write a whitepaper about Web Application attack of your choice and explain it from ground-up including how to prevent that attack

5. Who is Security Consulting?
Security Consulting is an Information Security Organization located in Croatia but consist of Computer Professionals from worldwide.

Author's Note

WebSec Framework is updated on dally basis and this documentation will be updated once on the month. Modules are also changed couple of times in a week.

GitHub is a place where you can download WebSec Framework and use it for free without paying a cent.

This is an Open Source so everyone is invited with their own ideas, suggestions and attack tests (modules).