OWASP OWTF

Anant Shrivastava

OWTF

O.W.T.F.

Offensive Web Testing Framework

Who am i

Anant Shrivastava

Information Security Consultant

OWASP + G4H + null

http://anantshri.info

@anantshri

Agenda

- What is OWTF
- OWTF Demo
- Things not covered
- How to Contribute

Offensive Web Testing Framework

Need of W.T.F.

- Automated Pentest operations
- Organize finding as per standard
- standard could be OWASP, NIST or others
- custom notes and rankings
- identify type of execution Passive, active

History

- We started out as a way to run OWASP test's without accessing the website directly i.e. via indirect / passive ways.
- Written in Python by Abraham (@7a_)
- One of the most active OWASP projects alongside (ZAP and TestingGuide)

U. S. P.

- Automated task execution
- Single Dashboard
- result aggregation (in future co-relation)
- Raw tools output available
- Single point dashboard for all data.
- Control Task's : Pause and resume.

HOW


Run Tools
• theHarvester
• Nikto
• Arachni
• w3af etc..
Run Tests directly
• Crafted requests
• Header searches
• html body searches etc..
Knowledge Repo
• POC Links
• Resource Links
• Test guide mappings
Help User Analysis
• Automated ranking
• User notes
• User rankings

But its primarily a

DEMO

So lets Launch the demo parts first.

Project hosted at http://github.com/owtf/owtf

Officially supports

KALI LINUX & **Samurai WTF**

Demo Setup

1. Kali Machine with OWTF configured on it
2. scan : http://demo.testfire.net
3. scan : http://testasp.vulnweb.com

Basic setup

- git clone http://github.com/owtf/owtf.git
- cd owtf
- python2 install/install.py

DEMO

Development

In a Nutshell, OWASP OWTF...

... has had 2,998 commits made by 22 contributors
representing 981,065 lines of code

... is mostly written in JavaScript
with an average number of source code comments

... has a young, but established codebase
maintained by a large development team
with increasing Y-O-Y commits

... took an estimated 271 years of effort (COCOMO model)
starting with its first commit in January, 2012
ending with its most recent commit about 1 month ago

Not covered

- OWTF botnetmode
- OWTF inbuilt proxy
- OWTF PlugnHack support
- OWTF Waf Bypasser and other plugins

contribute?

- GSoC
- Winter of Code
- Just Code
- Issue tracker comments on Github page.

Useful links

1. http://owtf.org
2. http://github.com/owtf/owtf
3. Video Demos @ youtube (owtfproject)
4. http://bit.ly/owtf-demo-lionheart

Social Connect

Twitter: @owtfp

Freenode IRC : #owtf

Any Questions?

slide credits

Not all slides were mine.

credits to

@tunnelshade_ and @7a_

for some slides.

Thank You