
w3af - Web application attack and audit framework Documentation

Release 1.7.6






Andres Riancho

January 20, 2016

1	Contents	3
1.1	Installation	3
1.2	Advanced installation	6
1.3	Updating to the latest version	7
1.4	Introduction	8
1.5	Running w3af	10
1.6	Automation using scripts	15
1.7	Authentication	15
1.8	Common use cases	18
1.9	Advanced use cases	18
1.10	w3af inside docker	19
1.11	Exploiting Web application vulnerabilities	20
1.12	Web Application Payloads	21
1.13	Bug reporting	25
1.14	Contribute	28
2	GUI documentation	31
2.1	GUI Introduction	31
3	REST API documentation	47
3.1	REST API Introduction	47
4	Advanced tips and tricks	55
4.1	Advanced tips and tricks	55

This document is the user's guide for the Web Application Attack and Audit Framework (w3af), its goal is to provide a basic overview of what the framework is, how it works and what you can do with it.

w3af is a complete environment for auditing and exploiting Web applications. This environment provides a solid platform for web vulnerability assessments and penetration tests.

Github repository	
w3af homepage	
IRC channel	#irc
Users mailing list	
Developers mailing list	
Twitter feed	

[Click here to download full PDF material](#)