



Explore

**w3af** (Web Application Attack and Audit Framework) is a comprehensive environment for auditing and exploiting web applications. [It serves as a solid platform for web vulnerability assessments and penetration tests1](http://docs.w3af.org/en/latest/). Here are **five free reference links** where you can learn more about w3af:

1. [**w3af Documentation**](http://docs.w3af.org/en/latest/): The official documentation provides a user guide, installation instructions, and details on using w3af for web application security assessments[1](http://docs.w3af.org/en/latest/).
2. [**Penetration Test Types for (REST) API Security Tests**](https://dzone.com/articles/pen-tests-types-for-rest-api-testing): This article discusses various penetration test types, including those relevant to web APIs, which align with w3af’s capabilities[2](https://dzone.com/articles/pen-tests-types-for-rest-api-testing).
3. [**W3af Walkthrough and Tutorial**](https://resources.infosecinstitute.com/topics/application-security/w3af-tutorial/): A series of articles covering w3af’s features and how to use them for web application penetration testing[3](https://resources.infosecinstitute.com/topics/application-security/w3af-tutorial/).

Feel free to explore these resources to enhance your understanding of web security testing using w3af! 🛡️🔍