A green chameleon logo

Description automatically generated

Forced Browsing Attack

​​

Executive summary:

This report covers the forced browsing vulnerability scan performed on the Chameleon website

Introduction:

A forced browsing attack, also known as forceful browsing, is a type of web application attack where an attacker attempts to access unauthorized resources on a website or web application by manually guessing or using automated tools to try different URLs.

This technique can be used to discover sensitive information, such as internal documents, configuration files, or even user credentials. How a forced browsing attack works Attackers typically carry out forced browsing attacks by exploiting vulnerabilities in the web application's design or implementation.

These vulnerabilities may include Predictable URL patterns: If the web application uses predictable URL structures, attackers can easily guess the names of directories or files that are not publicly accessible.

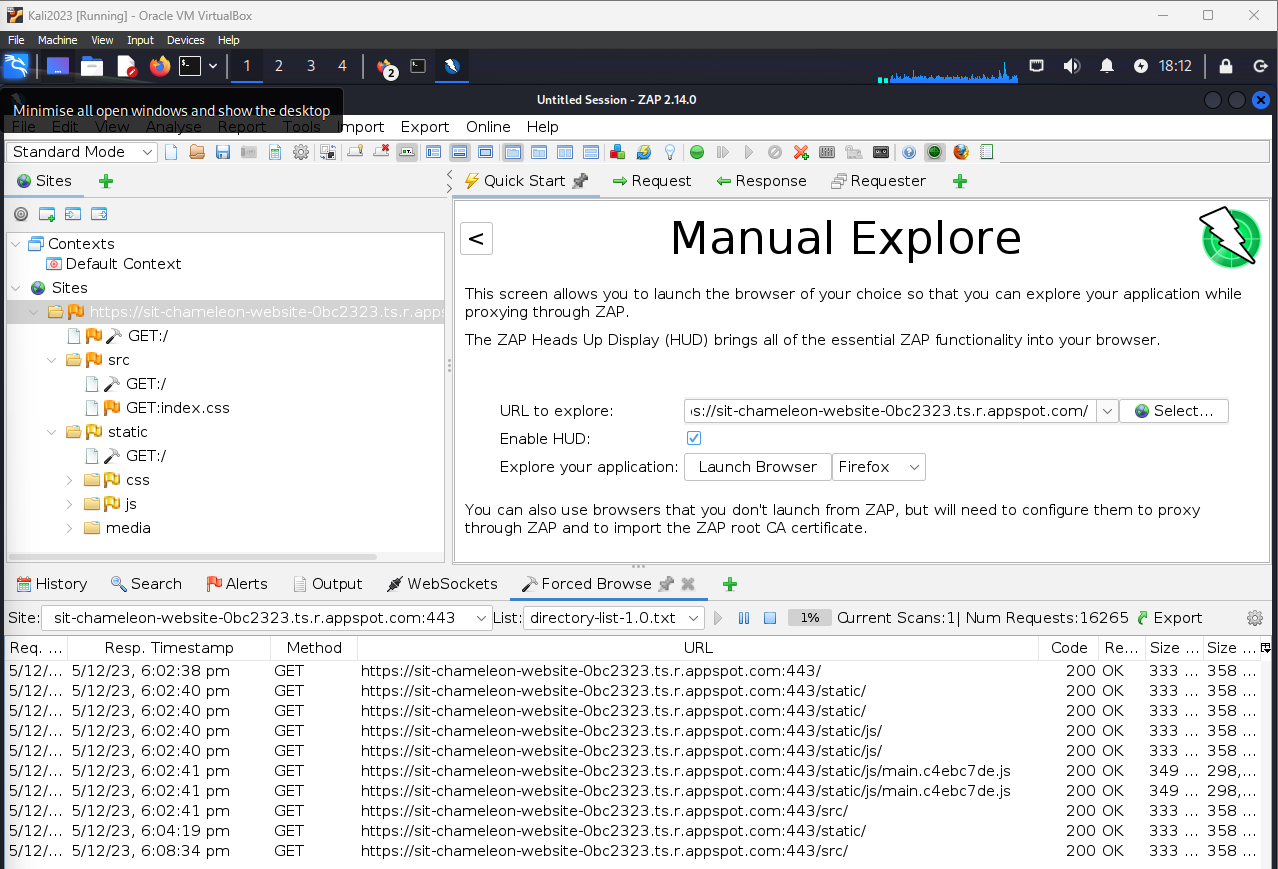
Tools used:

* Kali Linux
* OWASP ZAP

Scope of Testing

Scope of testing covered the Chameleon website found here: http://chameleon-test-v1.s3-website-ap-southeast-2.amazonaws.com/

Results



The results above have shown that once the scan was complete, and after careful review of all the pages scanned, there were no directories that could be used to force your way into the website through those pages.

The pages found showcased the static pages. This refers to information on a webpage that remains the same for every visitor, regardless of their device, location, or browsing history. It's like a printed page in a book - the text and images are fixed and don't change unless someone physically edits them.

Other options of the scan showcased src. The src attribute on a website stands for source, and it's used to specify the location of an external resource that the website needs to display or use.

Other than the above, there javascript found in the lines with .js were found. All pages found determined there was nothing found that could be exploited.

Next steps:

The next steps that can be undertaken is to perform this type of scan regularly to determine and possibly detect any exploitable requests from within the directory.