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. Directory indexing: If the web server is configured to index directories, attackers can simply list the contents of a directory and discover unauthorized files. Lack of access control: If the web application does not properly enforce access control mechanisms, attackers may be able to access resources that are not intended for them. Examples of forced browsing attacks Here are some examples of how forced browsing attacks can be carried out: An attacker might guess the name of a confidential document, such as a customer list or financial report, and try to access it directly by entering the URL into their web browser. An attacker might use an automated tool to scan a website for common directory names, such as "admin" or "uploads," and attempt to access any files or directories that are found. An attacker might exploit a vulnerability in a web application's content management system (CMS) to gain access to unauthorized areas of the website. Preventing forced browsing attacks Organizations can prevent forced browsing attacks by implementing the following security measures: Use strong access control mechanisms: Implement access control mechanisms that ensure that only authorized users can access sensitive resources. Disable directory indexing: Disable directory indexing on the web server to prevent attackers from easily listing the contents of directories. Use unpredictable URL structures: Use unpredictable URL structures to make it more difficult for attackers to guess the names of unauthorized resources. Regularly scan for vulnerabilities: Regularly scan web applications for vulnerabilities that could be exploited for forced browsing attacks. Educate employees: Educate employees about the risks of forced browsing attacks and how to identify and report suspicious activity.

Tools used:

* Kali Linux
* OWASP ZAP

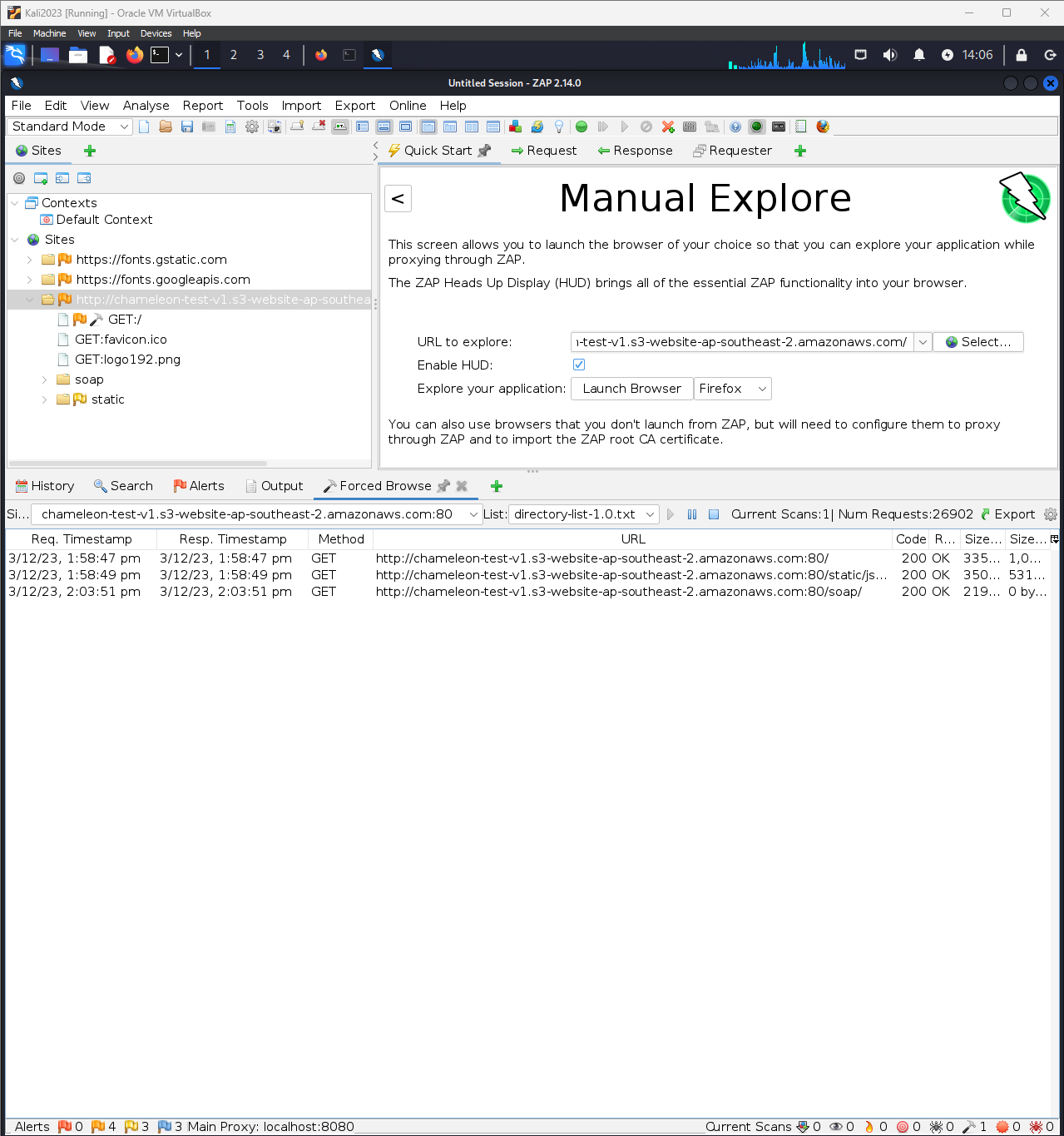
Scope of Testing

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

Methodology

 Mythology used was to scan the website using OWASP ZAP and to see what pages it found

Results



The results above have shown that there was three pages that could get access through a forced browsing vulnerability.