CHAMELEON

FOR OUR SMARTER WORLD

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.

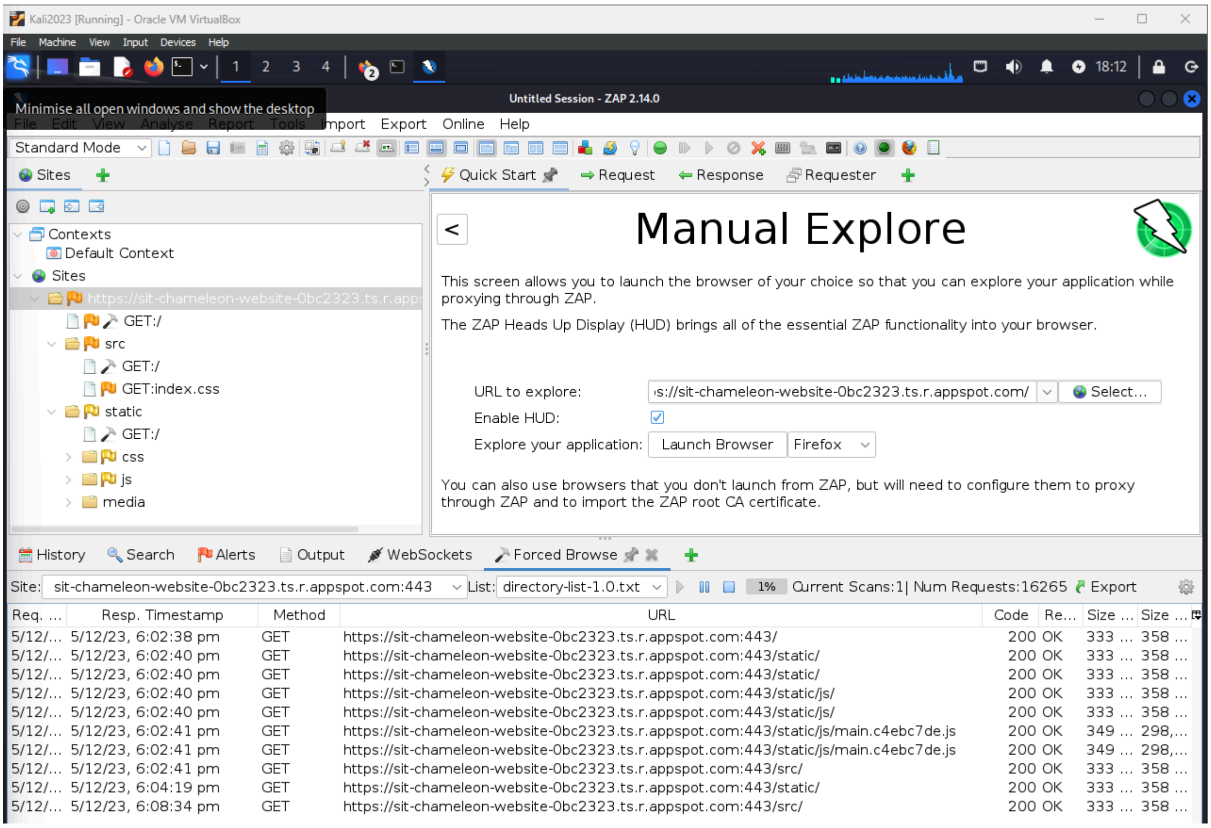
Tools used:

- 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


Kali2023 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
18:12
Minimise all open windows and show the desktop
Untitled Session - ZAP 2.14.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
https://sit-chameleon-website-0bc2323.ts.r.app
GET:/
src
GET:/
GET:index.css
static
GET:/
css
js
media
History
Search
Alerts
Output
WebSockets
Forced Browse
Export

Manual Explore

This screen allows you to launch the browser of your choice so that you can explore your application while proxying through ZAP.

The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser.

URL to explore: ıs://sit-chameleon-website-0bc2323.ts.r.appspot.com/ Select...

Enable HUD: ☑

Explore your application: Launch Browser Firefox

You can also use browsers that you don't launch from ZAP, but will need to configure them to proxy through ZAP and to import the ZAP root CA certificate.

Site: sit-chameleon-website-0bc2323.ts.r.appspot.com:443 List: directory-list-1.0.txt 1% Current Scans:1| Num Requests:16265

Req. ...	Resp. Timestamp	Method	URL	Code	Re...	Size ...	Size ...
5/12/...	5/12/23, 6:02:38 pm	GET	https://sit-chameleon-website-0bc2323.ts.r.appspot.com:443/	200	OK	333 ...	358 ...
5/12/...	5/12/23, 6:02:40 pm	GET	https://sit-chameleon-website-0bc2323.ts.r.appspot.com:443/static/	200	OK	333 ...	358 ...
5/12/...	5/12/23, 6:02:40 pm	GET	https://sit-chameleon-website-0bc2323.ts.r.appspot.com:443/static/	200	OK	333 ...	358 ...
5/12/...	5/12/23, 6:02:40 pm	GET	https://sit-chameleon-website-0bc2323.ts.r.appspot.com:443/static/js/	200	OK	333 ...	358 ...
5/12/...	5/12/23, 6:02:40 pm	GET	https://sit-chameleon-website-0bc2323.ts.r.appspot.com:443/static/js/	200	OK	333 ...	358 ...
5/12/...	5/12/23, 6:02:41 pm	GET	https://sit-chameleon-website-0bc2323.ts.r.appspot.com:443/static/js/main.c4ebc7de.js	200	OK	349 ...	298,...
5/12/...	5/12/23, 6:02:41 pm	GET	https://sit-chameleon-website-0bc2323.ts.r.appspot.com:443/static/js/main.c4ebc7de.js	200	OK	349 ...	298,...
5/12/...	5/12/23, 6:02:41 pm	GET	https://sit-chameleon-website-0bc2323.ts.r.appspot.com:443/src/	200	OK	333 ...	358 ...
5/12/...	5/12/23, 6:04:19 pm	GET	https://sit-chameleon-website-0bc2323.ts.r.appspot.com:443/static/	200	OK	333 ...	358 ...
5/12/...	5/12/23, 6:08:34 pm	GET	https://sit-chameleon-website-0bc2323.ts.r.appspot.com:443/src/	200	OK	333 ...	358 ...

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.