

Reconnaissance Report on Chameleon website

By

usman tariq

s217034263

s217034263@deakin.edu.au

I did some recon on Chameleon website using "EyeWitness" tool.

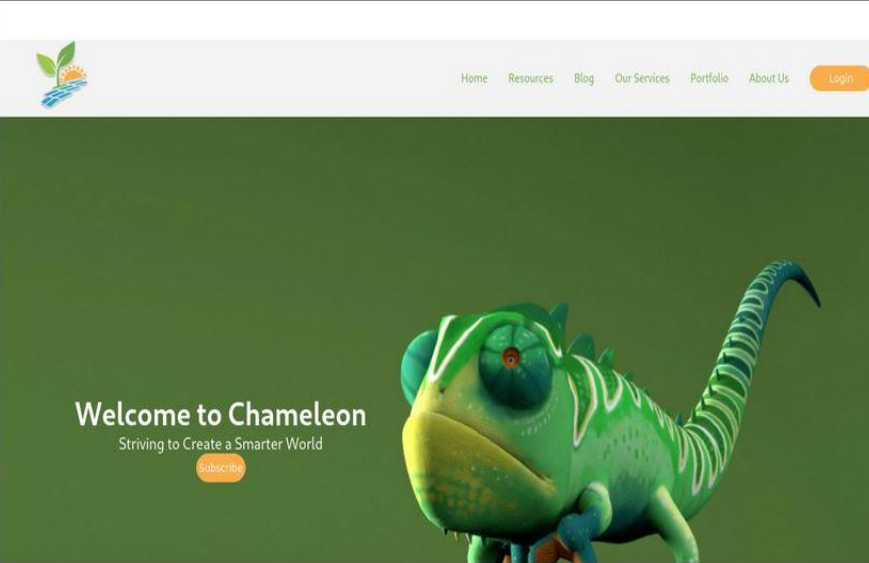
Command I used: **python3 EyeWitness.py --single https://sit-chameleon-website-0bc2323.ts.r.appspot.com/ -d ch-report**

And I found the following

file:///home/kali/EyeWitness/Python/ch-report/report.html

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec dolevf/Damn-Vulnera... nicholasaleks/graphql...

Report Generated on 2024/05/05 at 02:17:50

Web Request Info	Web Screenshot
<div>https://sit-chameleon-website-0bc2323.ts.r.appspot.com/</div> <div>Page Title: Chameleon</div> <div>Date: Sun, 05 May 2024 06:17:57 GMT</div> <div>Expires: Sun, 05 May 2024 06:27:57 GMT</div> <div>Cache-Control: public, max-age=600</div> <div>ETag: "8Ojipw"</div> <div>X-Cloud-Trace-Context: 61c8d57a87c7568ca0b7ff2c38d49331</div> <div>Content-Type: text/html</div> <div>Transfer-Encoding: chunked</div> <div>Server: Google Frontend</div> <div>Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000</div> <div>Connection: close</div> <div>Response Code: 200</div> <div>Source Code</div>	

- **Page Title: Chameleon:**

The page title usually symbolizes the main title of the webpage, which in this case is "Chameleon". This might offer you a general notion of what the webpage is about.

- **Date:**

This shows the date and time the response was created on the server. It is useful in determining the freshness of the response.

- **Expires:**
Indicates the date and time after which the response is considered stale. In this situation, it shows that the response will be valid until Sun, May 5, 2024 06:27:57 GMT.

- **Cache-Control:**

Provides instructions for caching methods in both requests and responses. It specifies that the response can be publicly cached for up to 600 seconds (10 minutes).

- **ETag:**
An entity tag is a unique identifier for a particular version of a resource. It supports caching and conditional requests.

- **X-Cloud-Trace-Context:**
This header is exclusive to Google Cloud Platform and is used to trace requests throughout Google's infrastructure.

- **Content-Type:**
This indicates the resource's media type. The content type "text/html" indicates that the response body contains HTML content.

- **Transfer-Encoding:**
Specifies the type of encoding used to securely convey the item to the user. It indicates that the response body is sent using "chunked" encoding.

- **Server:**
Specifies the name and version of the server software that will handle the request. In this scenario, "Google Frontend" denotes that the website is hosted on Google Cloud Platform.

- **Alt-Svc:**
Alternative services are available that allow the user agent to connect to the origin server. This header specifies HTTP/3 support with alternate service settings.

- **Connection:**

Indicates whether the connection to the server will end after the response is complete. "close" is specified here, indicating that the server will close the connection after sending the response.

- **Response Code: 200:**
The HTTP status code provided by the server indicates that the request was successful and that the server returned the requested resource.

Observations and analysis:

The website's moniker, "Chameleon," implies a potentially dynamic or changeable nature.

1. **Cache Control:** Responses are cached publicly for a maximum of 600 seconds (10 minutes), which improves efficiency for repeat visits.
2. **Content Type:** The response body is HTML, suggesting that the website mostly delivers web pages.
3. **Server:** The website is hosted on Google Frontend, implying that it is using Google Cloud Platform infrastructure.
4. **ETag:** A unique identification for the resource, which is important for caching and conditional requests.
5. **Connection:** After sending the response, the server shuts the connection.
6. **X-Cloud-Trace-Context:** A Google Cloud Platform-specific header used to trace requests across Google's infrastructure.
7. **Alt-Svc:** This indicates that HTTP/3 is supported with alternate service settings.

Recommendations:

1. **Security:** Additional security analysis is necessary to ensure effective protection against potential vulnerabilities.
2. **Performance:** Evaluate your caching approach to improve performance and reduce server load.
3. **Monitoring:** Use monitoring tools to track website performance and availability.
4. **Scalability:** Determine the scalability requirements to support anticipated increases in traffic.

Conclusion:

The reconnaissance analysis of sit-chameleon-website-0bc2323.ts.r.appspot.com reveals useful information about its configuration, caching behavior, and server environment. Additional assessment and action are recommended to improve security, performance, and scalability.