

main ctf-writeup / 2023-ARA / Web-Exploitation-Dewaweb /



masnurrm feat: dewaweb

1 hour ago

History

..



assets

1 hour ago



readme.md

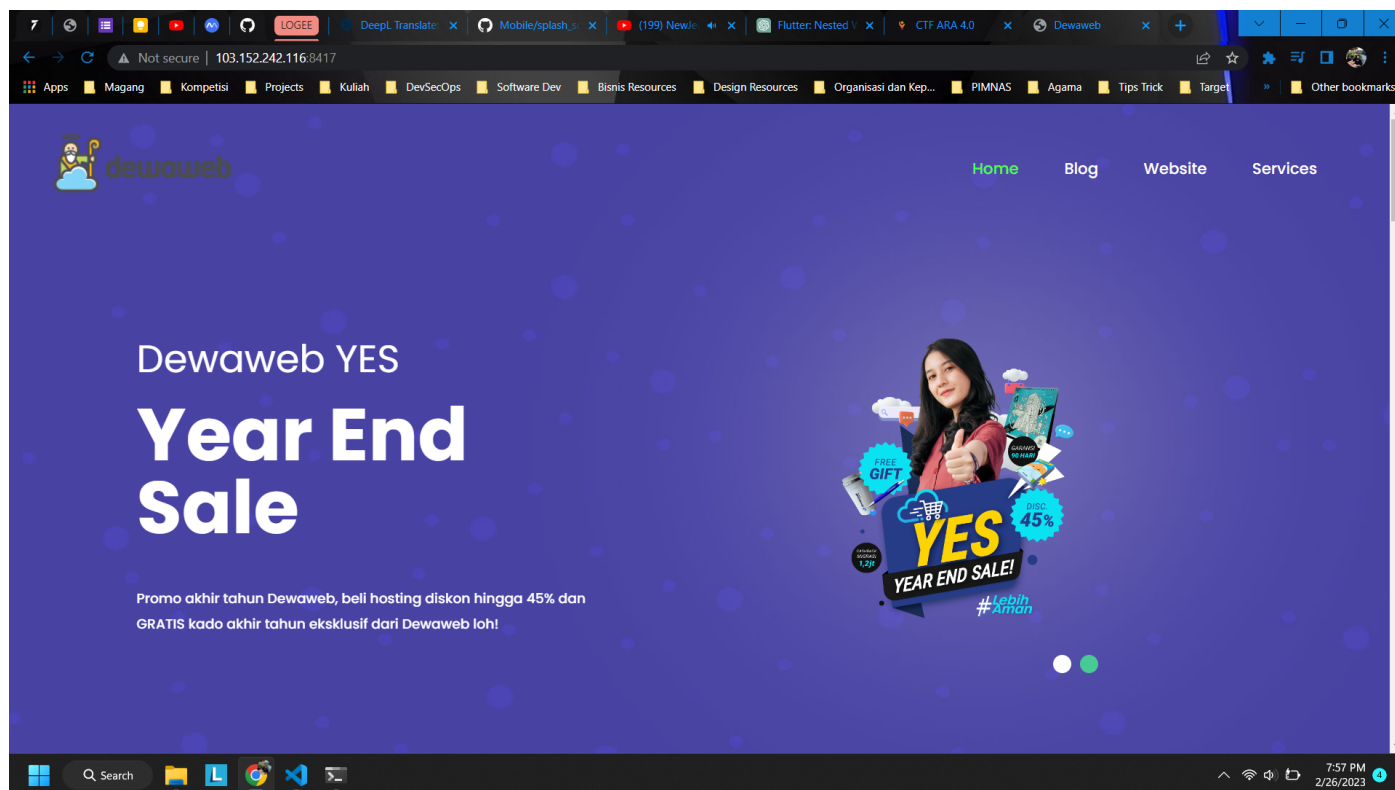
1 hour ago

readme.md



Web Exploitation - Dewaweb

In this challenge, we were given an IP Address of a website.



Our approach was checking the sources of the website. First, we checked the HTML source of the given website. It gives us the first part of the flag here.

```
Elements Console Sources Network Performance insights Memory Performance
<!-- end banner -->
<!-- three_box -->
<div class="three_box">...</div>
<!-- three_box -->
<!-- end products -->
<!-- laptop section -->
... <!-- part-1 : ARA2023{s4nt4I_ --> == $0
<div class="laptop">...</div>
<!-- end laptop section -->
<!-- customer -->
<div class="customer">...</div>
<!-- end customer -->
<!-- contact -->
html body.main-layout.vsc-initialized <!-->
```

part-1 : ARA2023{s4nt4I_

Next, we try to check the CSS sources of the website. It gives us the third part of the flag instead of the second part. It located in `/css/style.css`.

```
Page Filesystem Overrides Content scripts Snippets
jquery.mCustomScrollbar.min.css
meanmenu.css
nice-select.css
normalize.css
owl.carousel.min.css
responsive.css
slick.css
style.css
swiper.min.css
images
js
node_modules/popper.js/dist/esm
506 .text-bg a:hover {
507     background-color: #48ca95;
508     color: #fff;
509     transition: ease-in all 0.5s;
510 }
511
512
513 /** end banner section */
514 /** part-3 : g4k_ */
515
516 .titlepage {
517     text-align: center;
518     padding-bottom: 60px;
519 }
{} 21 characters selected
```

part-3 : g4k_

Then, we check the JS sources of the website. It gives us the second part of the flag here. It located in `/js/custom.js`.

```
Page Filesystem Overrides Content scripts Snippets
images
js
src
bootstrap.bundle.min.js
custom.js
jquery-3.0.0.min.js
jquery.mCustomScrollbar.concat.min.js
jquery.min.js
popper.min.js
node_modules/popper.js/dist/esm
scss
(index)
60
61
62 });
63
64 /** part-2 : dUlu_ */
{} 21 characters selected
```

part-2 : dUlu_

The last part, we got it in response header.

× Headers Preview Response Initiator Timing

Referrer Policy: strict-origin-when-cross-origin

▼ Response HeadersView source

Connection: Keep-Alive

Content-Encoding: gzip

Content-Length: 5555

Content-Type: text/html; charset=UTF-8

Date: Sun, 26 Feb 2023 13:09:19 GMT

Keep-Alive: timeout=5, max=100

Server: Apache/2.4.54 (Debian)

Vary: Accept-Encoding

X-4th-Flag: s1h?XD}

X-Powered-By: PHP/7.4.33

X-4th-Flag: s1h?XD}

So, when all of part were arranged, it will be full flag.

ARA2023{s4nt4I_dUlu_g4k_s1h?XD}

Give feedback