Kevin Umba

Infost 491

Midterm Project Write Up

3/22/2022

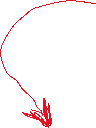
Flag 1:

When I start reconnaissance, I always check the dev tools first. As I navigated the home page, the inspect window reveals an encoded string in the HTML, which I decoded in url with Burp’s decoder.

A screenshot of a computer

Description automatically generatedGraphical user interface, text, application, email

Description automatically generated



Flag 2:

As I proceeded with reconnaissance steps, I looked for a possible path traversal vulnerability which led me to flag 2 in the robots.txt page.

Graphical user interface, text, application, email

Description automatically generated

Flag 6:

The robots.txt file revealed a hidden directory “/theteam”. The page contains a list of employee names and two well-formatted email addresses. I used those 2 emails as a template to write a list of potential emails. Then I sent a login request to Intruder and used the list of emails below as payload to perform a sniper attack. The result showed that [GaGalilei@hipposaregreat.com](mailto:GaGalilei@hipposaregreat.com), [AlEinstein@hipposaregreat.com](mailto:AlEinstein@hipposaregreat.com), [MaCurie@hipposaregreat.com](mailto:MaCurie@hipposaregreat.com), [ChDarwin@hipposaregreat.com](mailto:ChDarwin@hipposaregreat.com) had shorter response lengths. Those different response lengths lead me to believe that the emails above have existing accounts.

Email list on the “hipposaregreat/theteam” page

Graphical user interface, text, application

Description automatically generated

Sniper Attack Result

A picture containing table

Description automatically generated

Flag 3:

Subsquently, I attempted to run a spider attack using OWSAP Zap. Zap returned a sitemap of the hippo site and revealed a hidden directory named “midterm\_pics”. Accessing the midterm\_pics directory gave me access to a list of files within the directory. The flag was stored in hippo.txt.

Graphical user interface, text, application

Description automatically generated

Flag 4:

To discover other hidden directories, I ran a brute force directory attack on the /hipposaregreat.com/ site, which revealed the admin\_area page. The hipposaregreat.com/midterm\_pics/ page was an error page, which I refreshed to get the 4th flag.

Graphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

Description automatically generated

Flag 7:

Going back to the home page, I found a commented tab in the html page. The tab directs to a page called areyouworthy, which stored the flag encoded in hex in the JavaScript alert code. The last step was to remove the all the \x and decode the flag in hex.

Graphical user interface, text, application

Description automatically generated