

HACKDONALD'S WRITEUP

For this CTF Challenge, I pentested the <https://hackdonalds.intigriti.io/> website.

At first I got presented with a simple website that had a simple menu and an admin login page.




I ran dirbuster to try and discover new directories, and got the following endpoints:




- /menu
- /admin
- /login

Initially, I tried bruteforcing the login of the application with ffuf and the rockyou.txt wordlist, but I got no results from that.

I also ran SQLmap against the application's login, but that had no effect either.


I analysed the applications tech stack with Wappalyzer, and saw the application using Nextjs with version 13.2.0.

 **Wappalyzer**





TECHNOLOGIES

MORE INFO


 **Export**

JavaScript frameworks


 [React](#)

 [Next.js](#) 13.2.0


Security

 [HSTS](#)


Font scripts


 [Google Font API](#)

Web frameworks


 [Next.js](#) 13.2.0

Miscellaneous


 [Webpack](#)

 [Open Graph](#)


Web servers

 [Next.js](#) 13.2.0

Static site generators

 [Next.js](#) 13.2.0

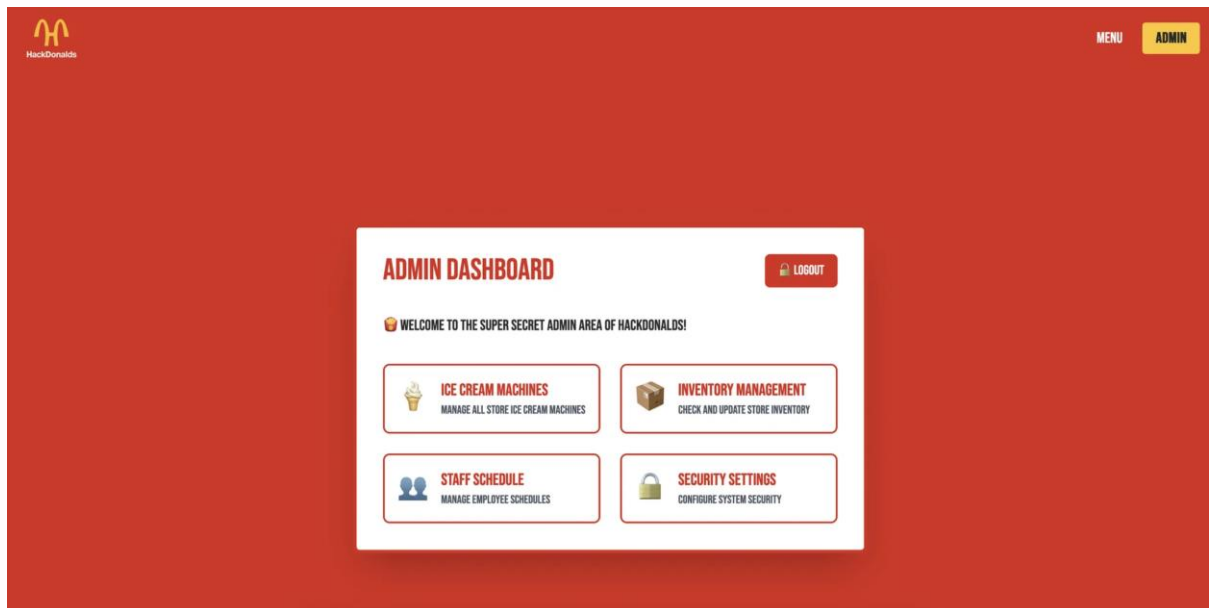
UI frameworks

 [Tailwind CSS](#)

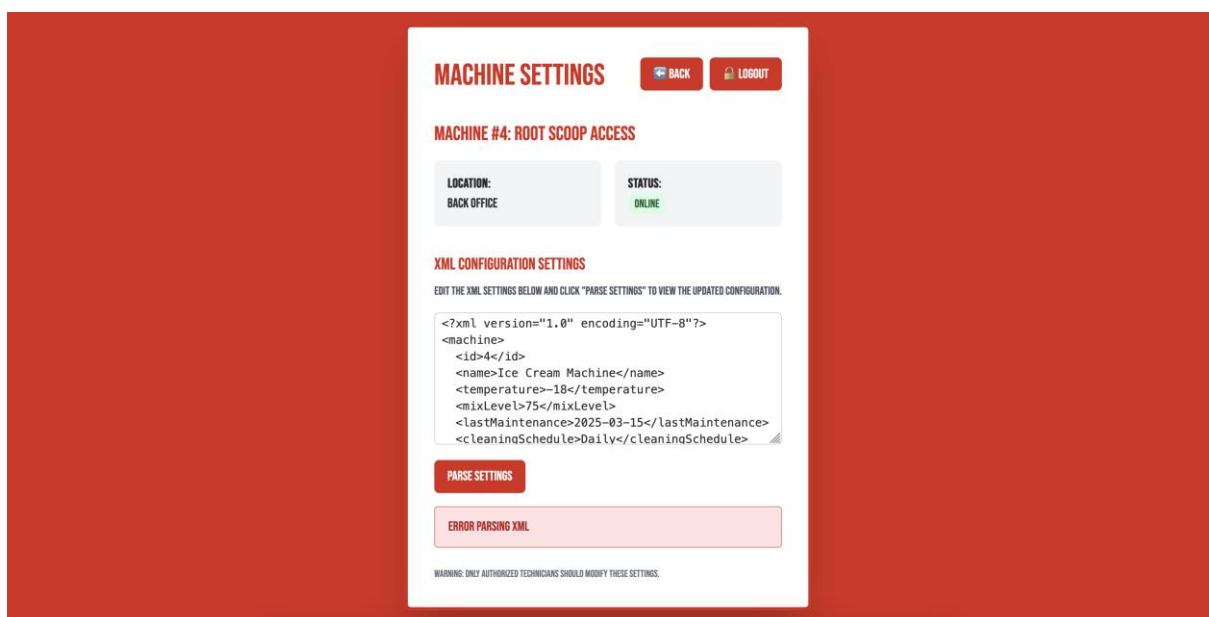
Doing some reseach on it, I saw that authentication bypass for applications using that version of the framework could be possible, and in this case it was, by adding the following header:

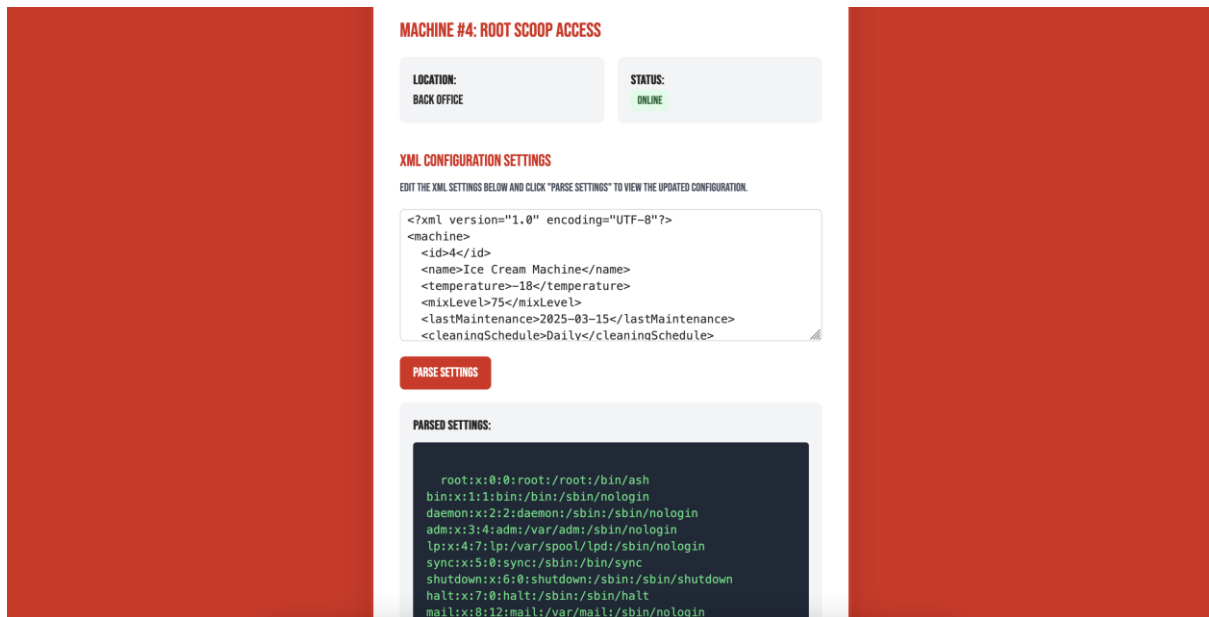
```
x-middleware-subrequest:  
middleware:middleware:middleware:middleware:middleware
```

To the requests done by the application. I added the header to the requests with Burp Suite and bypassed authentication.



After bypassing the authentication, as an admin, there was XML in the ice cream machine's information tab that could be altered. Immediately I checked if the application was vulnerable to XXE, and it was.





After knowing that, I realised I was in a kubernetes environment, when I dumped the contents of /etc/hosts, which had:

```
\n # Kubernetes-managed hosts file.\n127.0.0.1\tlocalhost\n::1\tlocalhost ip6-localhost ip6-loopback\nfe00::0\tip6-localnet\nfe00::0\tip6-mcastprefix\nfe00::1\tip6-allnodes\nfe00::2\tip6-allrouters\n10.14.6.202\thackdonalds-66c868f9c4-5htkx\n\n
```

After realising this, I dumped the contents of /app/package.json and got the flag!
 INTIGRITI{XXE_1n_lC3Cr34m_M4ch1n3s}

