MANDIANT
YOUR CYBERSECURITY ADVANTAGE

Web Challenge #1

A large group of monkeys on the island think they're super 1337 haxors. Can you find a way to get into their monkey authentication site? We know the site is out there somewhere, they recently registered 'hackermonkeys.com'.

Solution

Overview

Contestants will perform DNS reconnaissance to identify a portal website that valid 'hackermonkeys.com' users authenticate to. Once the site is discovered, a small hint is revealed in the HTML source login page about the type of password the developer needs to try to protect against. Contestants will have to perform a typical password spray attack. Password spray attacks are used by several APT's, UNC's, and Red Teamers that give them initial access into company networks.

The contestants DNS reconnaissance will also help them discover another website where users are listed as employees at 'hackermonkeys.com'. From there, contestants will finally be able to spray the portal using an easily guessable password, keeping note of the source HTML hint (*current MonthYEAR! = March2022!*), with the list of users they discovered. The user cupcake@hackermonkeys.com has the easily guessable password and when logged into the portal will display the flag:

monkeyCTF{wz4yjmnuf6f53q2ar4lmdf1ffgfqhwad}

TECHNICAL DETAILS

Browsing to hackermonkeys.com presents a site that is currently "under construction".

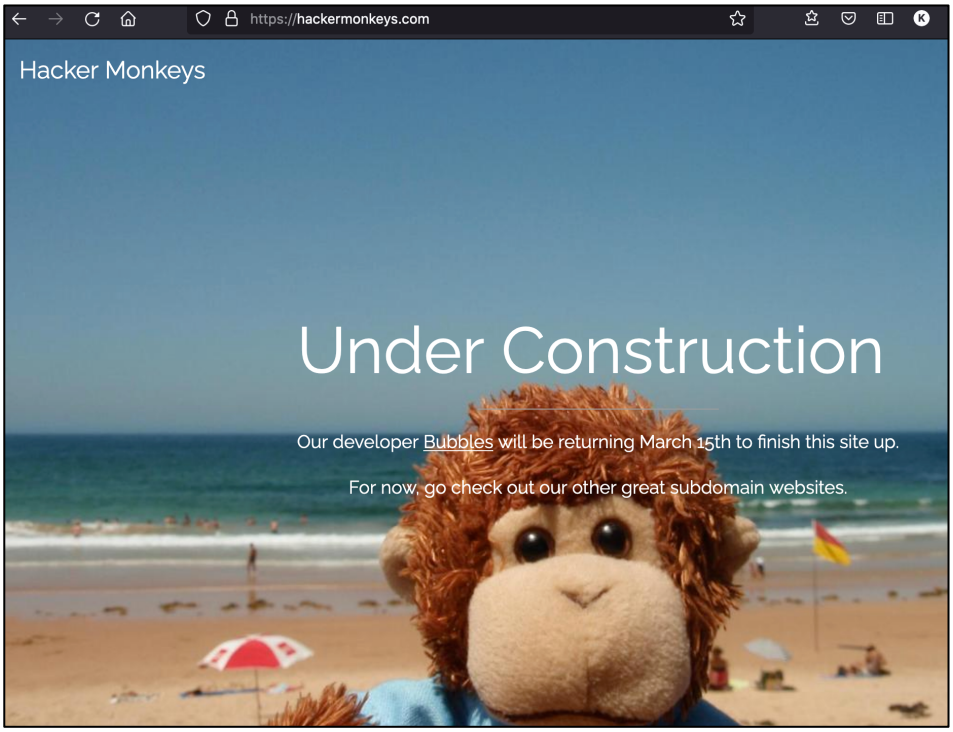


Figure 1: Main hackermonkeys.com domain

After viewing the page referencing for the contestant to go check out the other subdomains, basic DNS reconnaissance should turn up the three (3) main websites:

- hackermonkeys.com

- portal.hackermonkeys.com
- dnd.hackermonkeys.com

```
❯ subfinder -d hackermonkeys.com

        _     __ _          _
____  _| |__ / _(_)_ _  __| |___ _ _
(_-< || | '_ \  _| | ' \/ _  / -_) '_|
/__/\_,_|_.__/_| |_|_||_\__,_\___|_| v2

                projectdiscovery.io

[WRN] Use with caution. You are responsible for your actior
[WRN] Developers assume no liability and are not responsibl
[WRN] By using subfinder, you also agree to the terms of th

[INF] Enumerating subdomains for hackermonkeys.com
www.hackermonkeys.com
portal.hackermonkeys.com
dnd.hackermonkeys.com
```

Figure 2: Subdomain enumeration

Visiting portal.hackermonkeys.com, contestants are presented with a page that redirects them to a login portal.

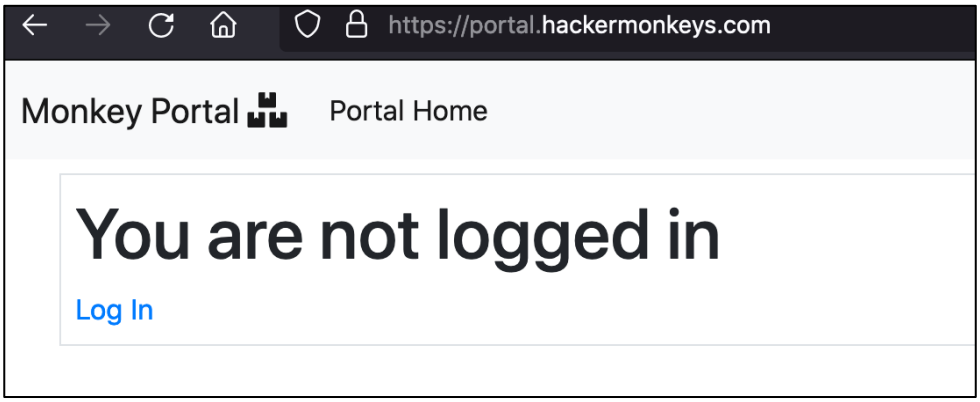


Figure 3: Portal home page

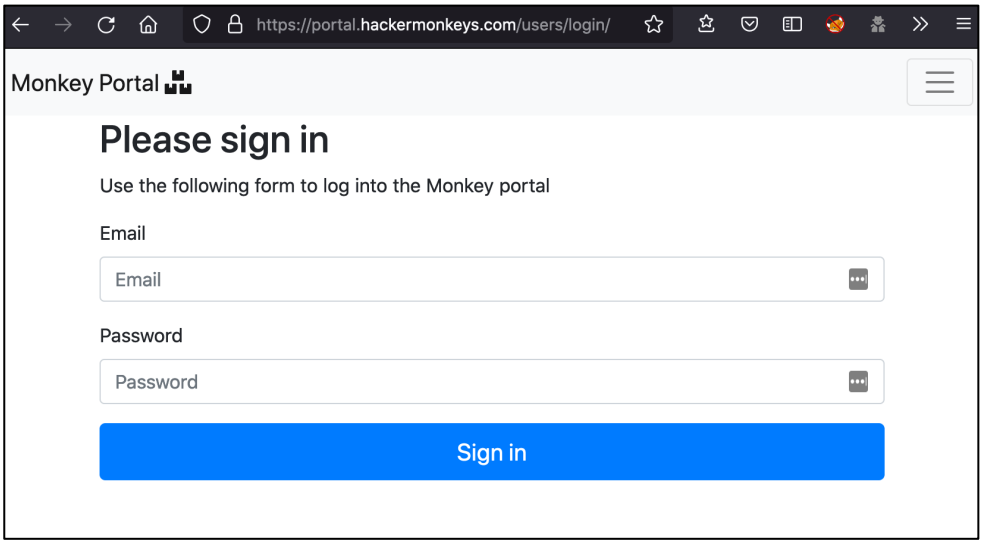


Figure 4: Portal login page

Inspecting and viewing the HTML source of the login form page, contestants will find a small comment from the developer.

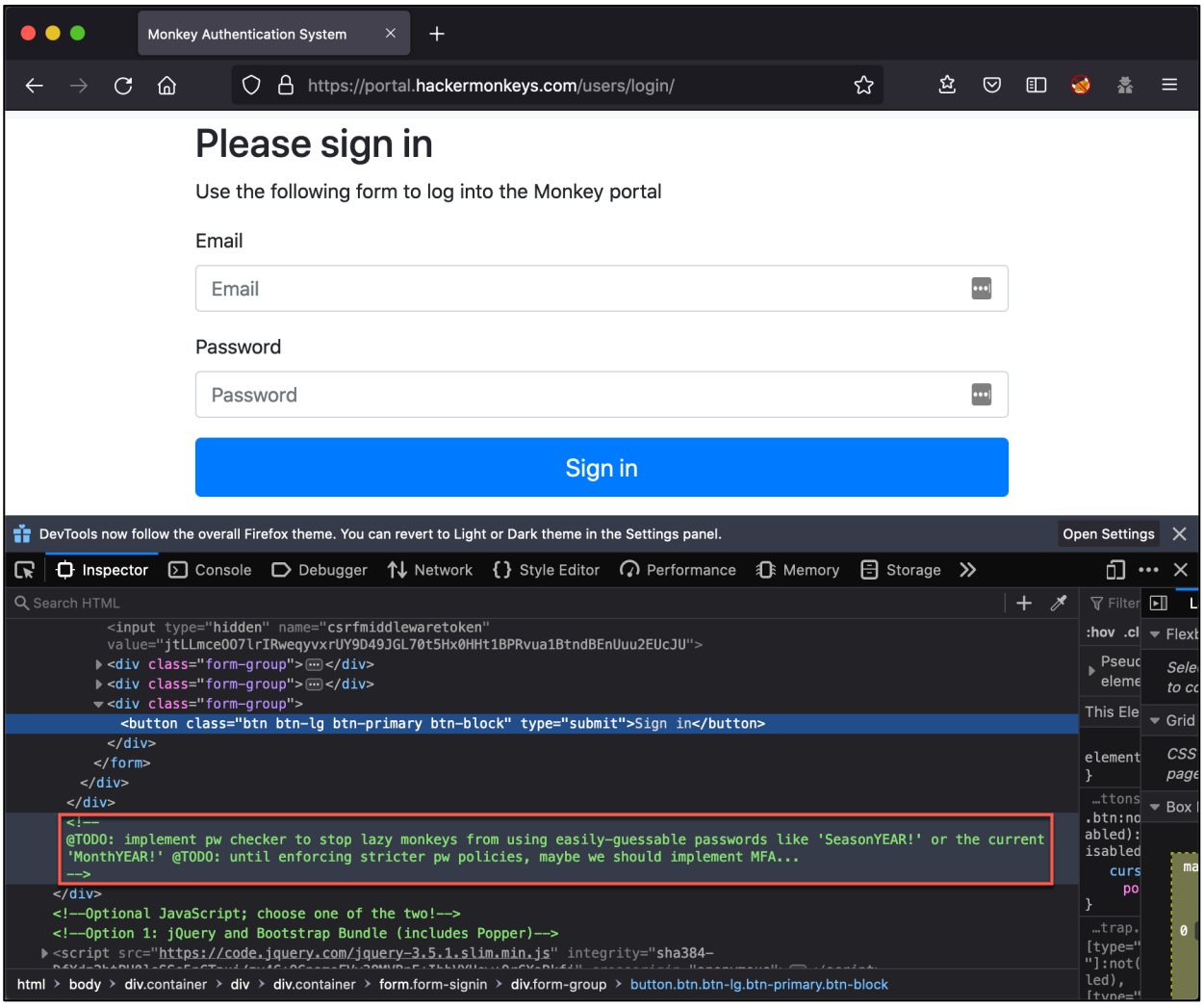


Figure 5: Comment hint of a password spray attack

Indicating a password spray attack, contestants will have to find potential emails to spray against the portal. The third site, discovered during the DNS reconnaissance and located at dnd.hackermonkeys.com, displays a site dedicated to those who work at hackermonkeys.com and are in the Dungeons and Dragons club.

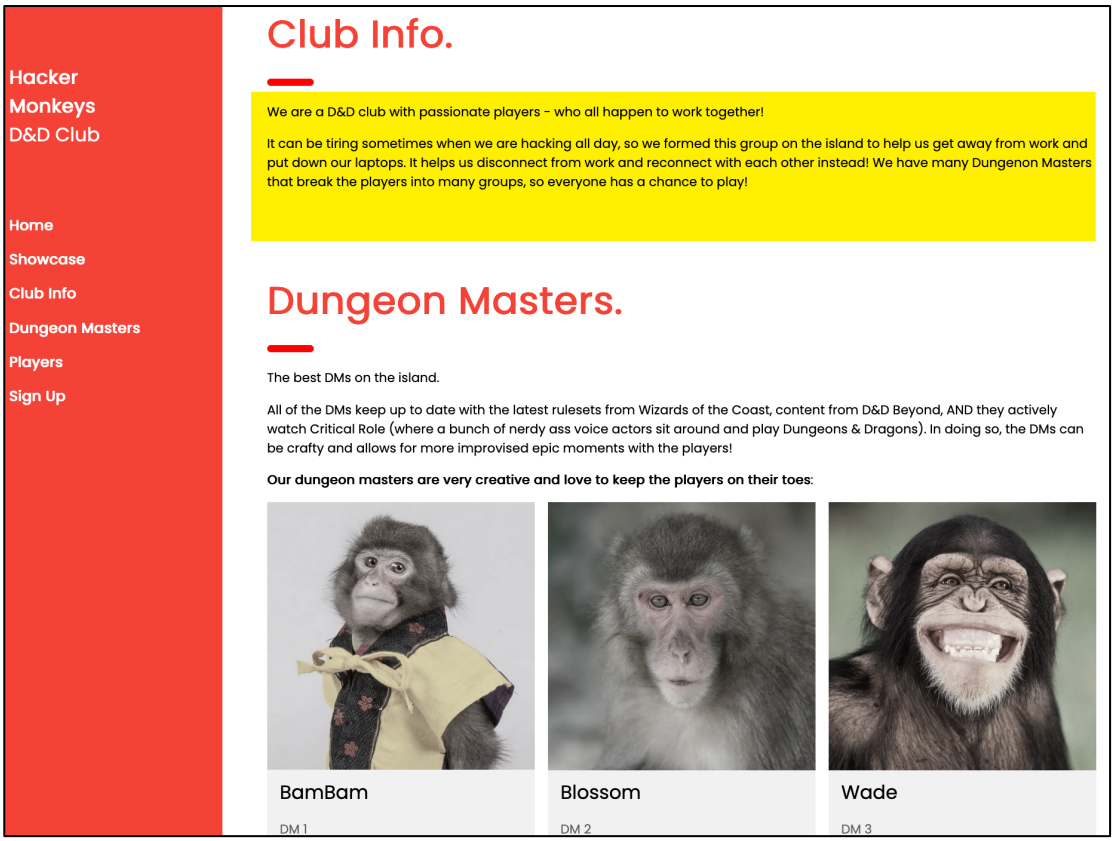


Figure 6: D&D club page of active hackermonkeys.com employees

The site displays Dungeon Masters and several players, giving contestants the ability to create a user list.

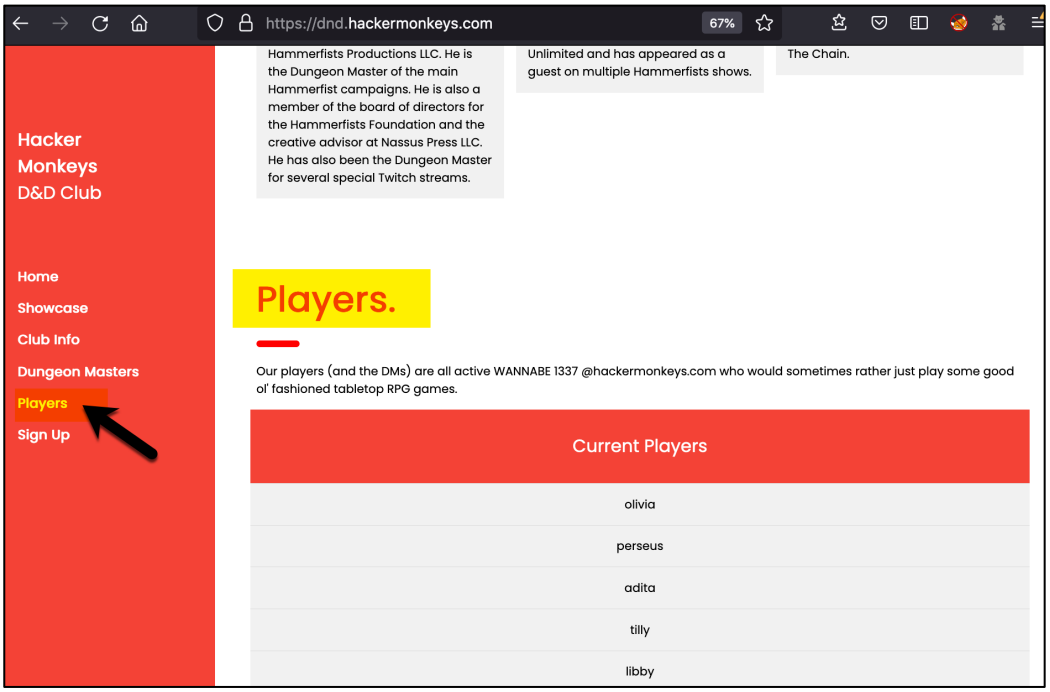


Figure 7: List of "players" who are also employees

Since the portal's login page requires an email, there are several references to the developer throughout two of the sites that displays the email format.

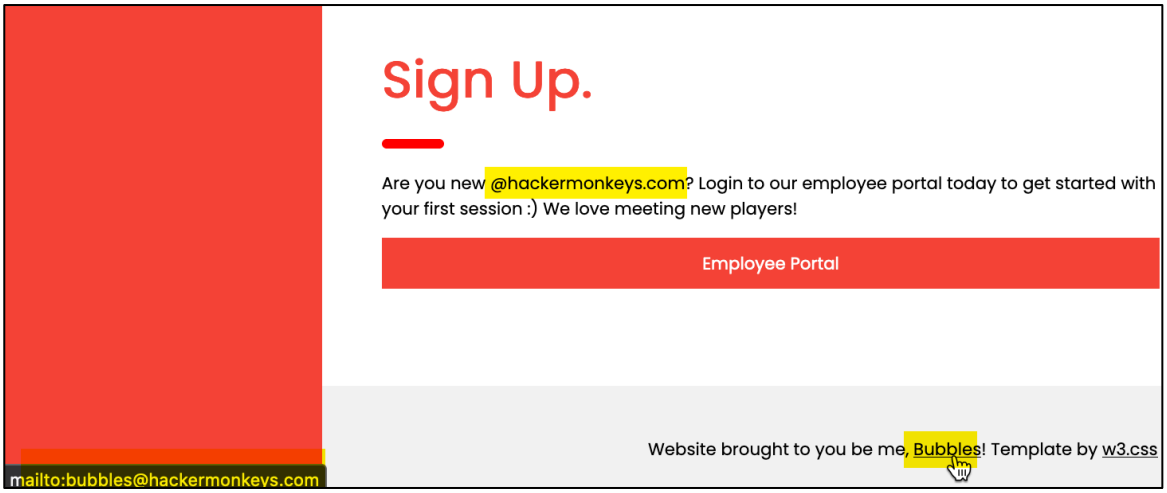


Figure 8: Email format references

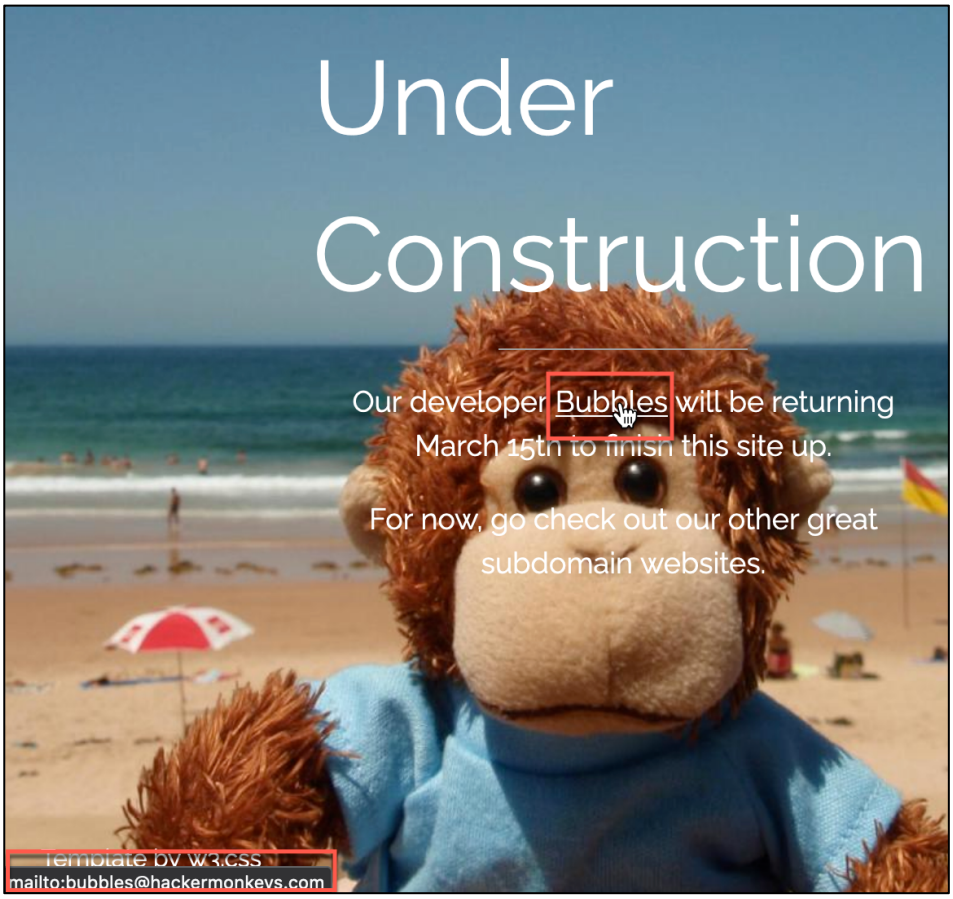


Figure 9: Email format reference

After harvesting all the names from the site, contestants will have to perform a typical password spray attack using a common password. Since the competition is in the month of March, password will be 'March2021!', belonging to cupcake@hackermonkeys.com.

Contestants can use a program such as Burp Suite or create their own password spraying script. If they are using a Burp Community edition it will take longer, so it would be faster for them to do it via a custom script. Either way, the result is the same once they are successful. Successful authentication will present an HTTP 302 Redirect, and the length of the response will be shorter than those that were unsuccessful.

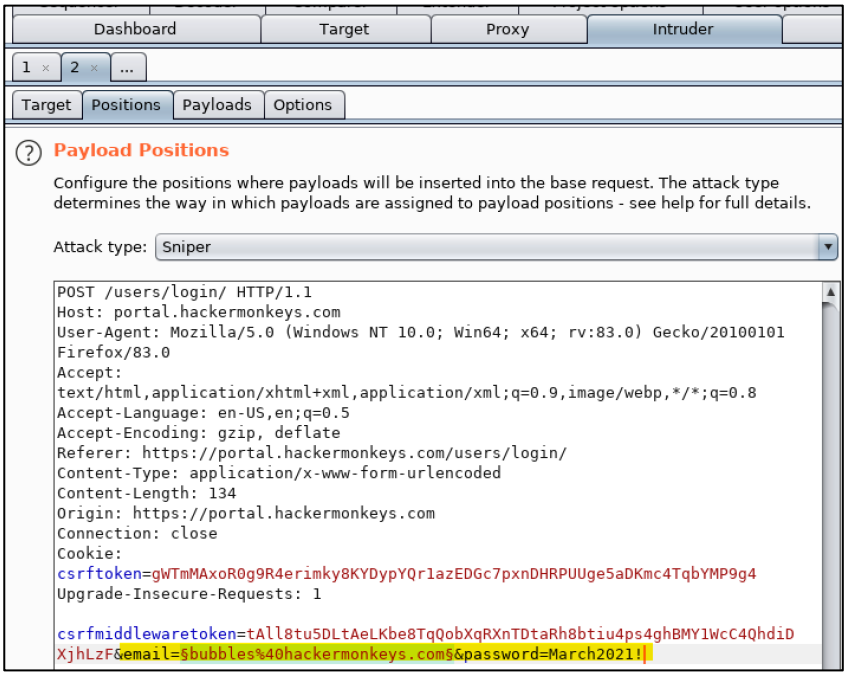


Figure 10: Intruder attack, position set for the email parameter

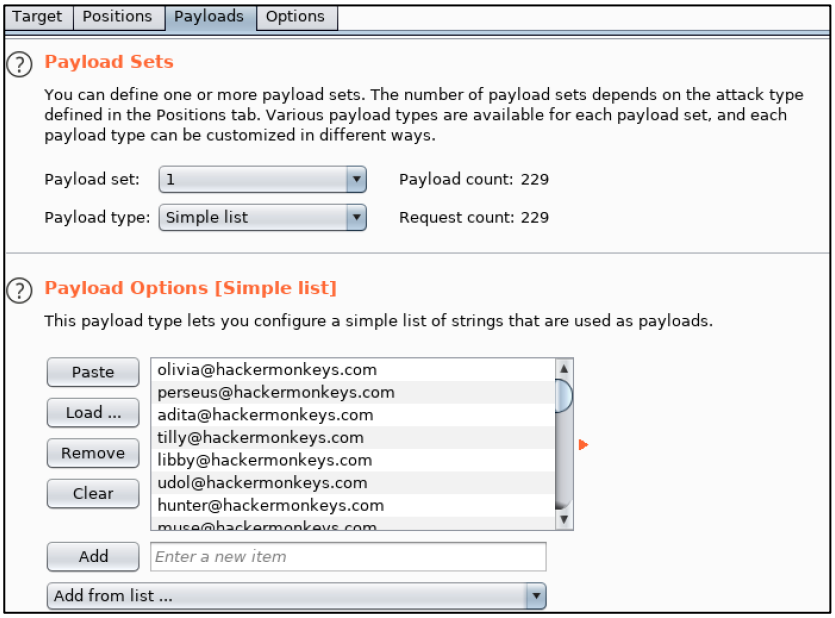
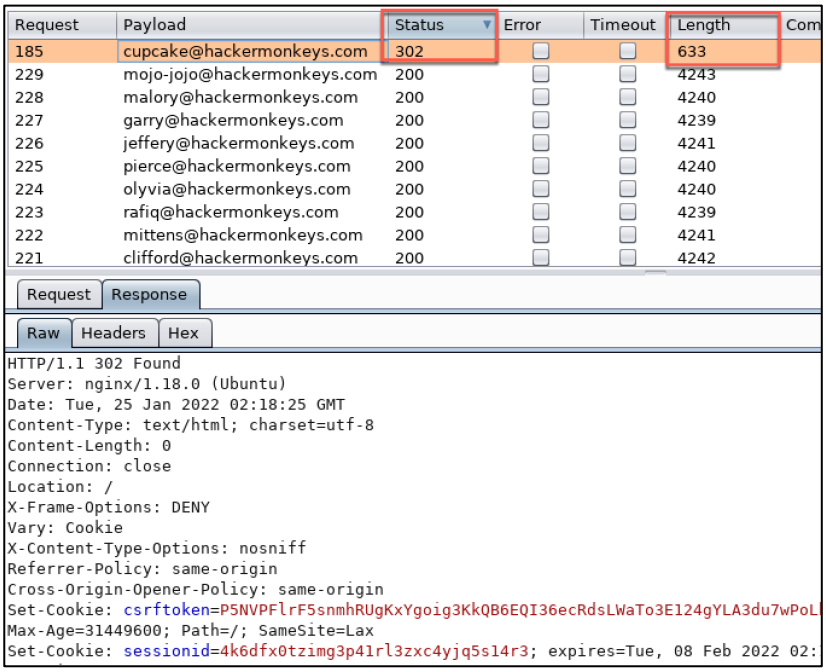


Figure 11: List of curated names as payload



Request	Payload	Status	Error	Timeout	Length	Com
185	cupcake@hackermonkeys.com	302	☐	☐	633	
229	mojo-jojo@hackermonkeys.com	200	☐	☐	4243	
228	malory@hackermonkeys.com	200	☐	☐	4240	
227	garry@hackermonkeys.com	200	☐	☐	4239	
226	jeffery@hackermonkeys.com	200	☐	☐	4241	
225	pierce@hackermonkeys.com	200	☐	☐	4240	
224	olyvia@hackermonkeys.com	200	☐	☐	4240	
223	rafiq@hackermonkeys.com	200	☐	☐	4239	
222	mittens@hackermonkeys.com	200	☐	☐	4241	
221	clifford@hackermonkeys.com	200	☐	☐	4242	

Request | Response

Raw | Headers | Hex

```
HTTP/1.1 302 Found
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 25 Jan 2022 02:18:25 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 0
Connection: close
Location: /
X-Frame-Options: DENY
Vary: Cookie
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Cross-Origin-Opener-Policy: same-origin
Set-Cookie: csrftoken=P5NVPFlrF5snmhRUgKxYgoig3KkQB6EQI36ecRdsLWaTo3E124gYLA3du7wPoL
Max-Age=31449600; Path=/; SameSite=Lax
Set-Cookie: sessionid=4k6dfx0tzimg3p41rl3zxc4yjq5s14r3; expires=Tue, 08 Feb 2022 02:
```

Figure 12: Successfully sprayed the portal and discovered credentials for cupcake@hackermonkeys.com

Logging into the portal platform, contestant is presented with the flag: **monkeyCTF{wz4yjmnuf6f53q2ar4lmdf1ffgfqhwad}**

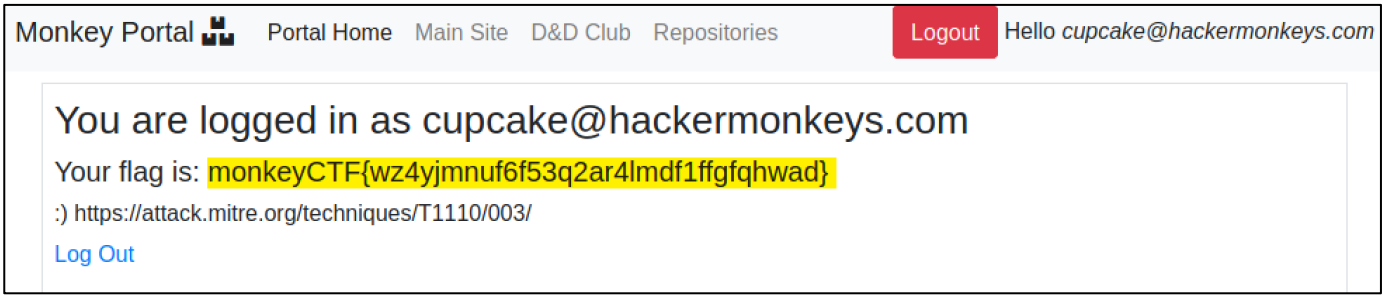


Figure 13: Successfully logged into portal.hackermonkeys.com