# Amazon Cookie Stealer

---

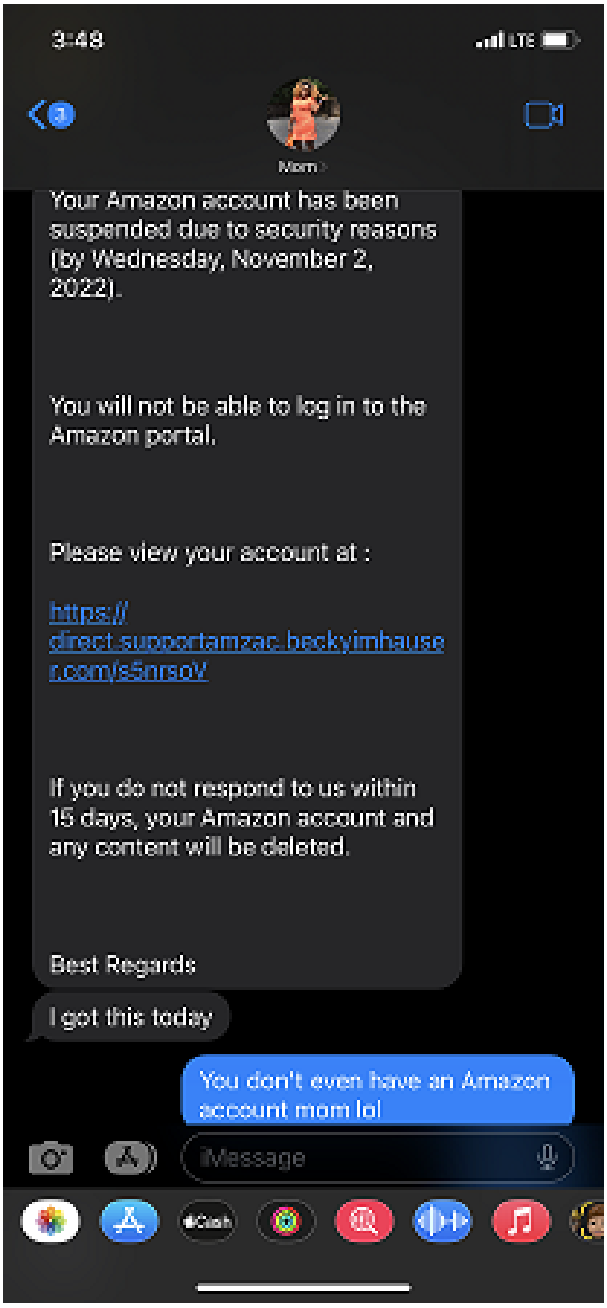
: 11/06/2022
https://rhomaniertaylor.com
https://twitter.com/lotus_infosec
https://www.linkedin.com/in/rhomanietaylorcyber/
https://github.com/lotus-infosec

---

# Background

`https://direct.supportamzac.beckyimhauser[.]com/s5nrsoV`

The link being investigated ^



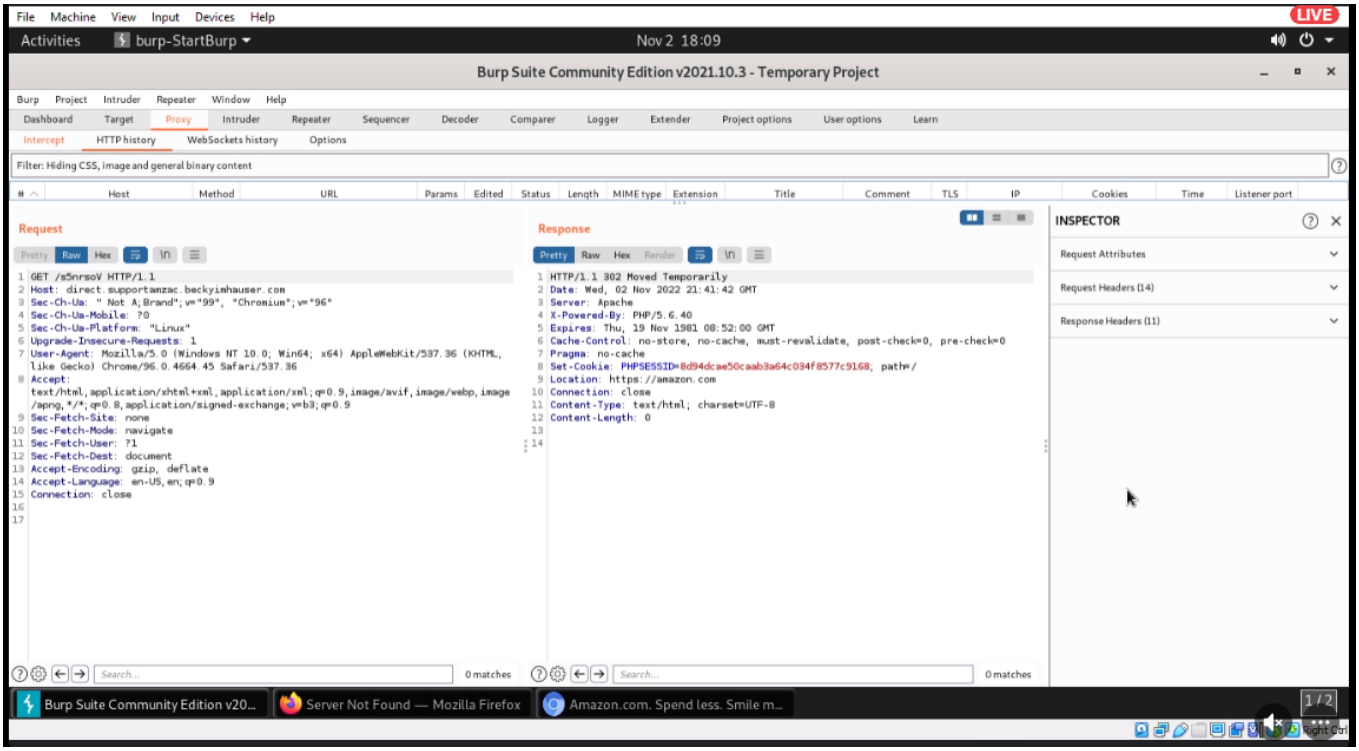

I'll start this off by explaining the interesting relationship me and my mom have with the spam messages she receives. My mother frequently sends/shows me suspicious emails or messages she receives to make sure they're safe. This Amazon link intrigued me and I wanted to take a deeper dive, so I rallied the troops (*Darryl Terrell*). We started our investigation by spinning up our virtual machines, *Remnux* and *Kali Linux*, then got to work discovering the secrets that lay behind the link.

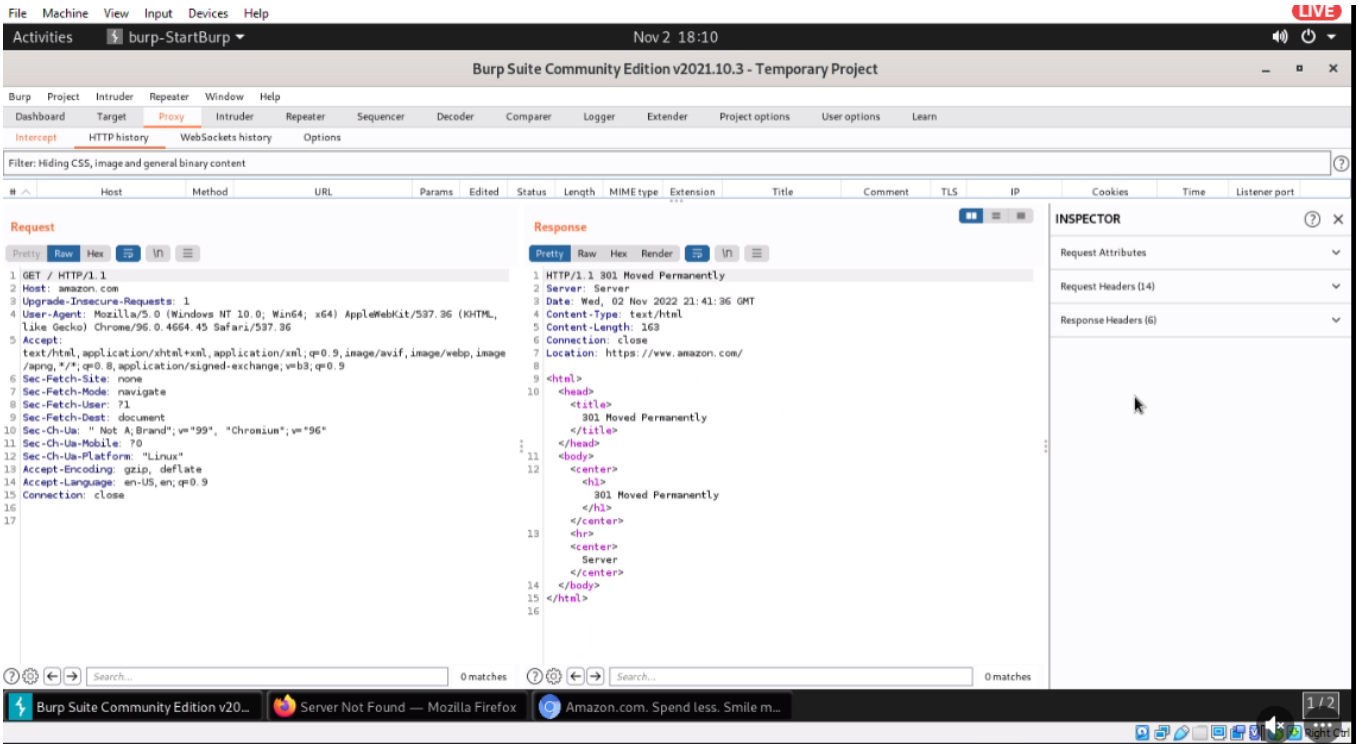
# Analysis

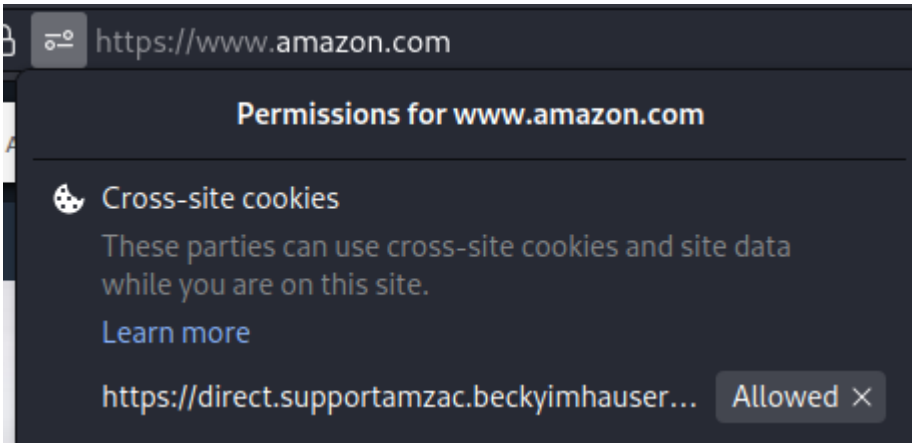
*As soon as you click the link it redirects the victim to Amazon's official website. The attack begins by allowing cookies to be shared with the attacker giving them access to any user data input into the site. Once you put the information in it exfiltrates it back to the attacker. - Darryl*

The attacker uses an XSS (Cross Site Scripting Vulnerability) to send cookies back to themselves. The link itself redirects you to Amazon.com where it embeds a PHP session ID and allows Amazon to generate and send cookies back to the attacking website.

Using Burpsuite we can see exactly what the packets are doing in transit and the responses.

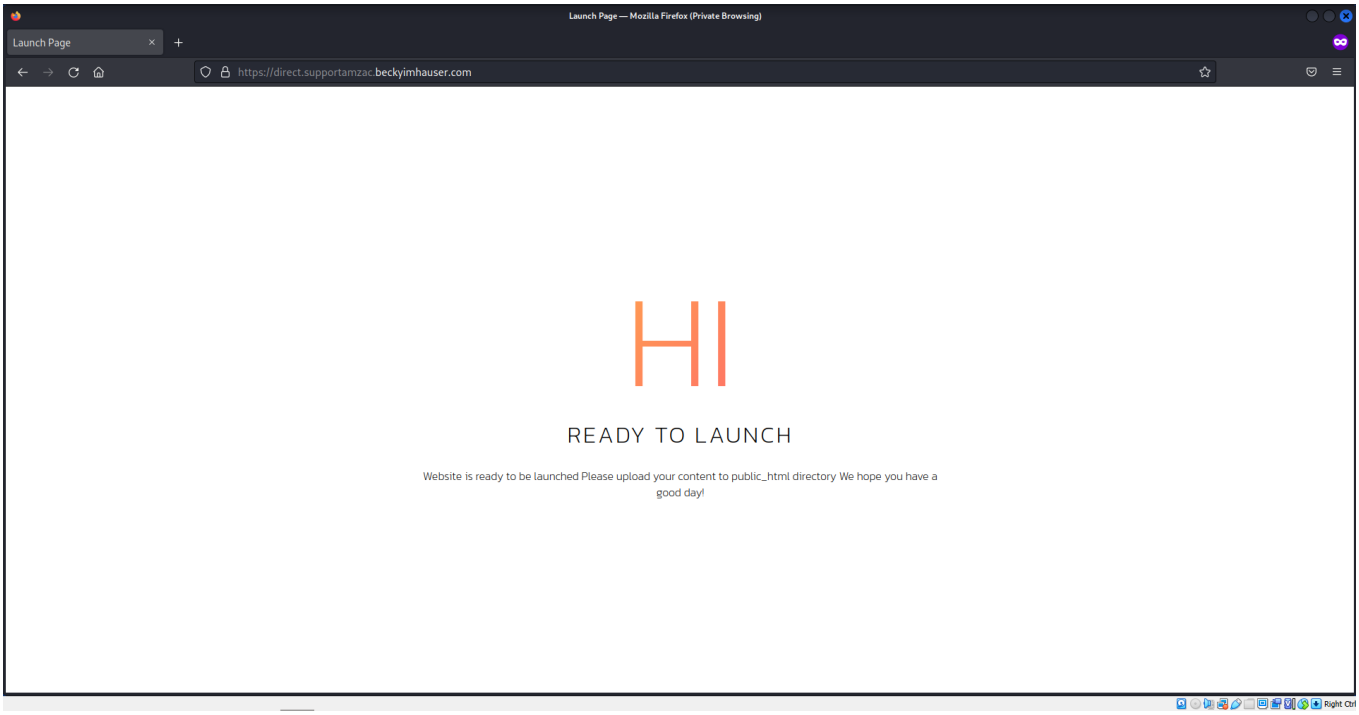




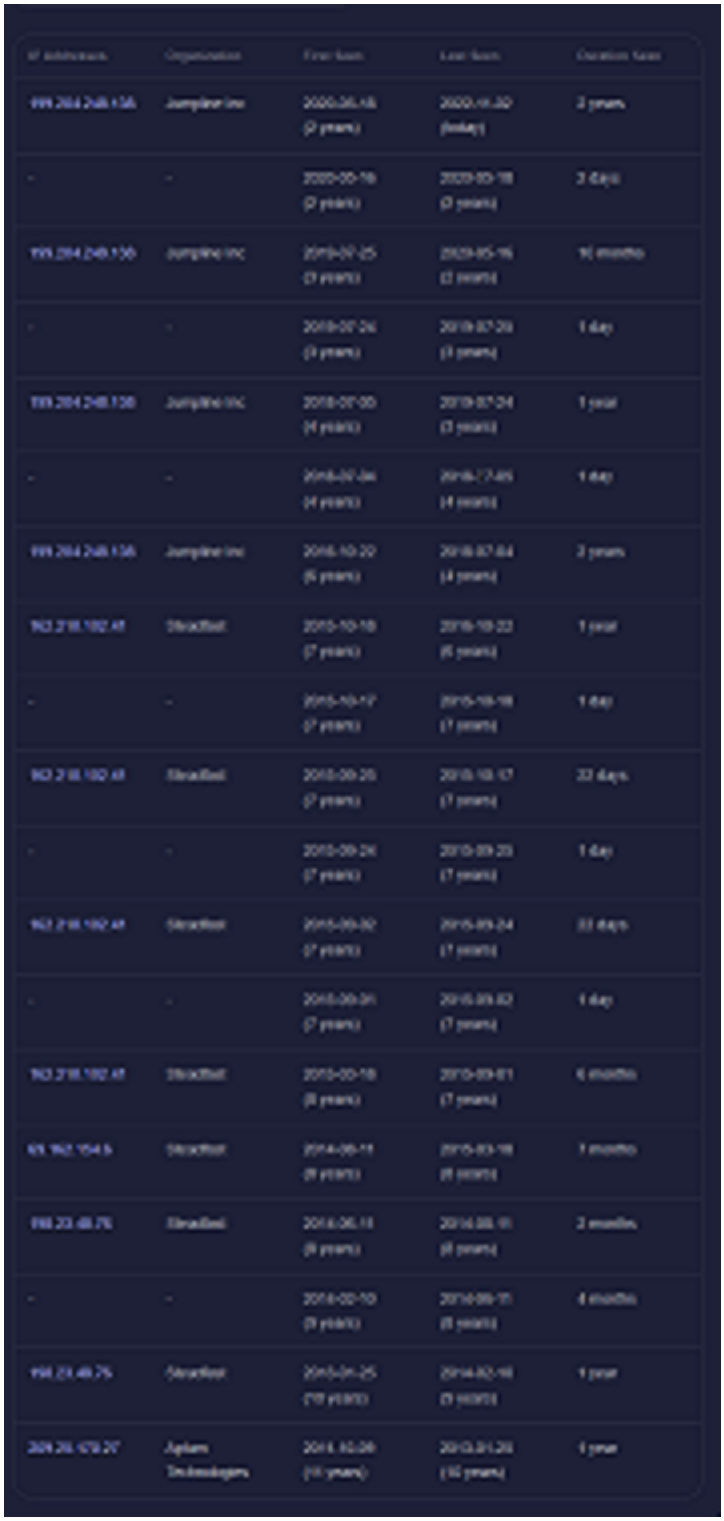

***Side Note: Cookies can be decoded to learn about the data they store.***

Going to the link itself, without the attachment at the end proves less than useful...

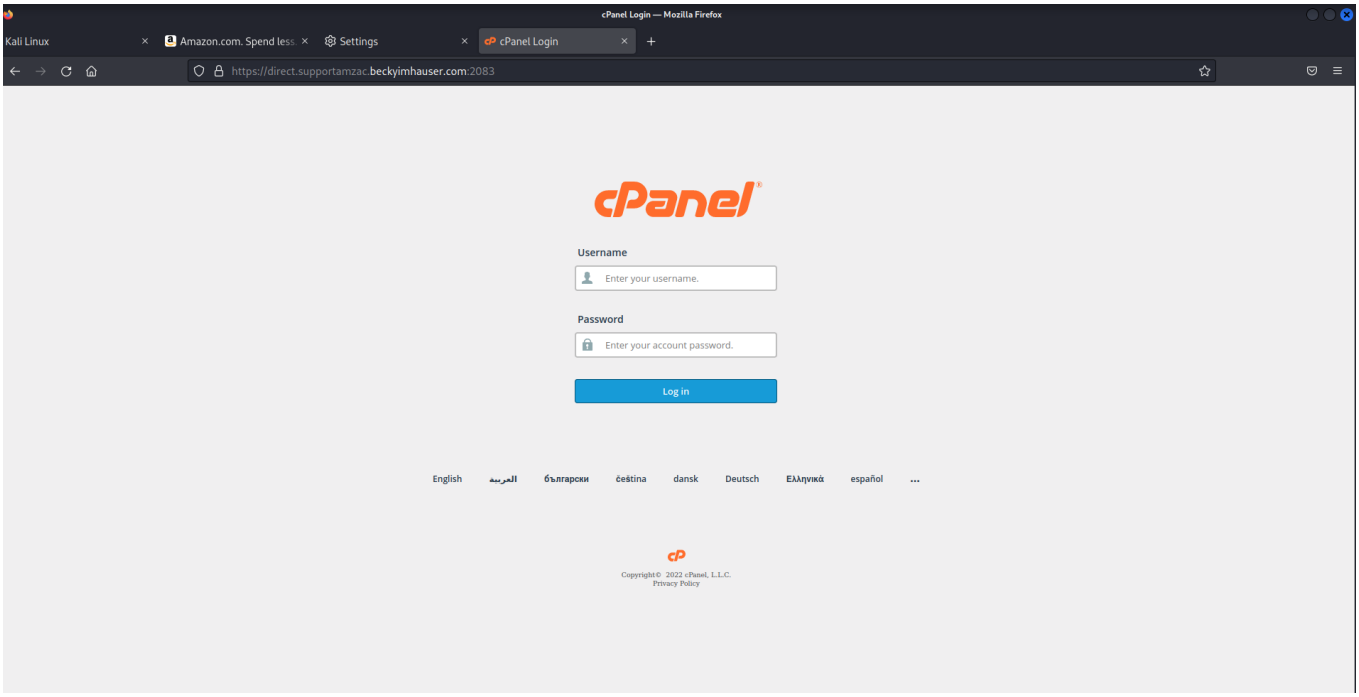



We figured out a decent bit of information about the website itself. I used Securitytrails to look at historical DNS data.

(This screenshot got severely messed up, so as a summary the DNS records changed roughly 3 years ago so I don't believe that is the reason for the attack. )



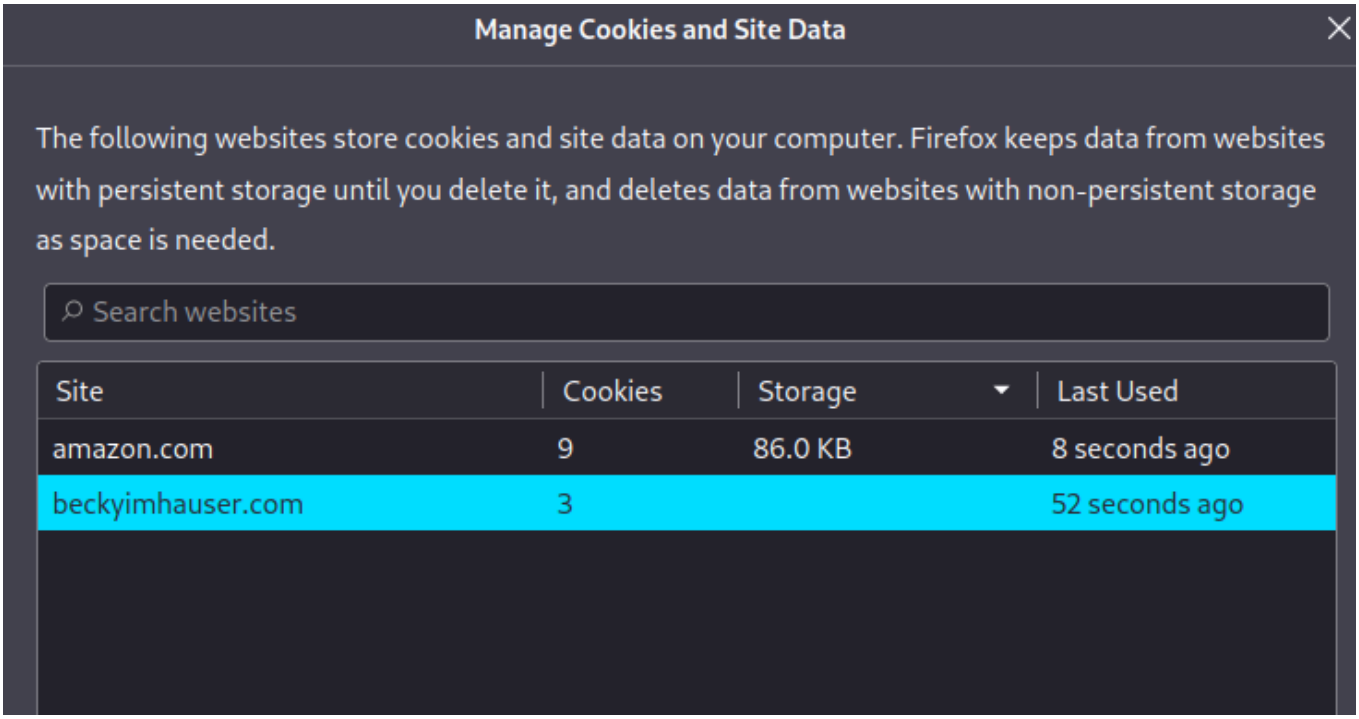
We figured out the website was built on cPanel.



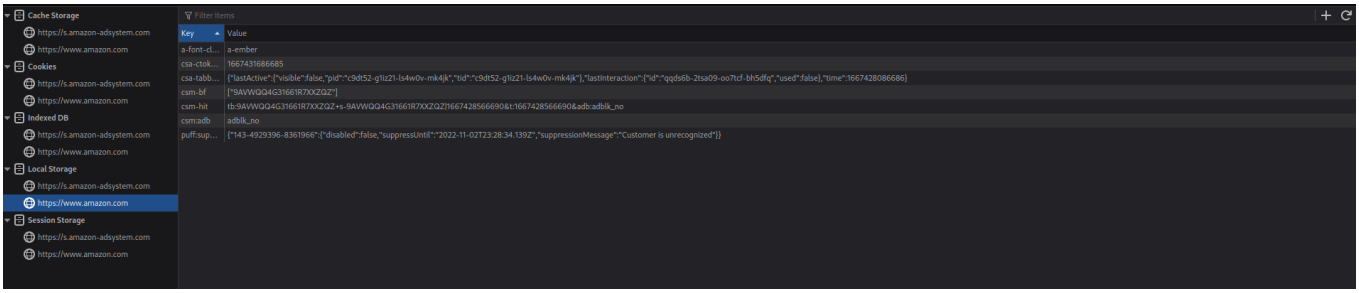

We also noted that it stored the cookies in our Firefox browser. But when trying to view the database in. `~/.mozilla/firefox/<user>/cookies.sqllite` we quickly learned that it doesn't actually store cookies in the database, it's held in a volatile Firefox cache.

Table: moz_cookies

| | id | originAttributes | name | value | host | path | expiry | lastAccessed | creationTime | isSe |
|---|---|---|---|---|---|---|---|---|---|---|
| | ... | Filter | Filter | Filter | Filter | Fi... | Filter | Filter | Filter | Filt |
| 1 | 3 | | i18n-prefs | USD | .amazon.com | / | 1698964078 | 1667428079895851 | 1667428079895851 | |
| 2 | 4 | | sp-cdn | "L5Z9:NL" | .amazon.com | / | 1698964079 | 1667428079895873 | 1667428079895873 | |
| 3 | 6 | ^partitionKey=%28https%2Camazon.com... | abid | e8c21d3a-b771-420d-a036-f4f59c87c6f3 | .associates-amazon.com | / | 1669847288 | 1667428088605745 | 1667428088605745 | |
| 4 | 9 | | session-token | "dVVswxID3qMUhmEUz9UACUWQaIrWmm... | .amazon.com | / | 1698964096 | 1667428096065548 | 1667428096065548 | |
| 5 | 19 | | csm-hit | tb:... | www.amazon.com | / | 1697668106 | 1667428106285907 | 1667428086601742 | |
| 6 | 20 | | ubid-main | 131-4157812-1094806 | .amazon.com | / | 1698964105 | 1667428107326760 | 1667428091513951 | |
| 7 | 21 | | session-id-time | 2082787201l | .amazon.com | / | 1698964105 | 1667428107326847 | 1667428079895829 | |
| 8 | 22 | | session-id | 143-4929396-8361966 | .amazon.com | / | 1698964105 | 1667428107326899 | 1667428079895763 | |
| 9 | 23 | ^partitionKey=%28https%2Camazon.com... | ad-id | A5zAwhycIUzQpVj5MTVPw00 | .amazon-adsystem.com | / | 1688250514 | 1667428116298279 | 1667428115549037 | |
| 10 | 24 | ^partitionKey=%28https%2Camazon.com... | ad-privacy | 0 | .amazon-adsystem.com | / | 1830378514 | 1667428116298374 | 1667428116298374 | |
| 11 | 25 | ^partitionKey=%28https%2Camazon.com... | pt | v2:ceba03f2e2a80ef448f1aff353026c3659... | .ispot.tv | / | 1730500117 | 1667428119373951 | 1667428119373951 | |
| 12 | 26 | ^partitionKey=%28https%2Camazon.com... | sambapxid | 103bd71b2ccbb9cbf | ads.samba.tv | / | 1701556118 | 1667428120266430 | 1667428120266430 | |
| 13 | 28 | ^partitionKey=%28https%2Camazon.com... | c | 1667428119 | .myvisualiq.net | / | 1730500119 | 1667428121051266 | 1667428121051266 | |
| 14 | 29 | ^partitionKey=%28https%2Camazon.com... | tuuid_lu | 1667428119 | .myvisualiq.net | / | 1730500119 | 1667428121051341 | 1667428121051341 | |
| 15 | 30 | ^partitionKey=%28https%2Camazon.com... | ndat | aO2WYGNi7xe+NBrROSZ9Ag== | .ninthdecimal.com | / | 1682980119 | 1667428121399774 | 1667428121399774 | |

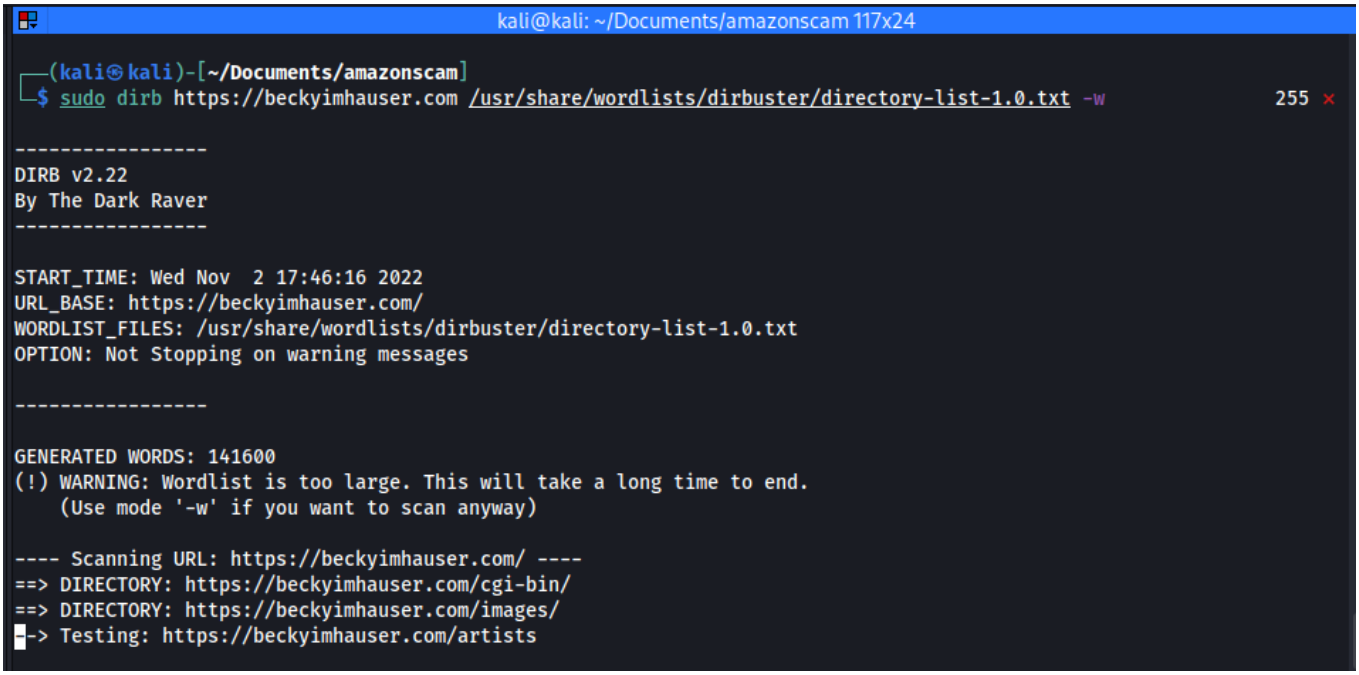



We did try to view cached and session cookie storage but low and behold, that didn't work either.




Another side note:

We also tried using dirbuster to see if we can enumerate more files on the system. But to be honest, that failed horribly... Maybe next time.




# Summary

This is pretty much where the story stops. We tried a few passwords on the CPanel login but ultimately deciding that it'll probably be super illegal if we actually gained access. (Also the passwords didn't really work). We weren't exactly sure what to do after this. We identified how the attack was being done and where the site was being hosted. We weren't exactly sure of how the website itself is being used because the author is definitely a real person who may have just lost control over her domain name servers.

Also, Darryl reached out to the owner via email to inform them that their site might be being utilized for malicious purposes. We have yet to receive response at the time of this writing.

Overall this little excursion was fun. It was one of the first websites Darryl and I did that wasn't protected by Cloudflare and we managed to learn a lot from it. Hopefully on the next one we can figure out how to take the scammer down!!

-- Darryl's LinkedIn (https://www.linkedin.com/in/darrylty/)

---

As usual... **THE LINKS**

https://mxtoolbox.com/DNSLookup.aspx
https://whatismyipaddress.com/ip/199.204.248.138
https://www.inmotionhosting.com/support/edu/cpanel/how-to-log-into-cpanel/
https://unix.stackexchange.com/questions/82597/where-does-firefox-store-its-cookies-on-linux#:~:text=Firefox%20stores%20cookies%20in%20sqlite,%2Fcookies.
https://stackoverflow.com/questions/151026/how-do-i-unlock-a-sqlite-database

https://support.mozilla.org/en-US/questions/1219653
https://firefox-source-docs.mozilla.org/devtools-user/storage_inspector/index.html
https://securitytrails.com/domain/beckyimhauser.com/history/a
https://www.google.com/search?q=xss+using+cookies&oq=xss+using+cookies&aqs=chrome..69i57j0i22i30l5j0i390l3.2080j0j7&sourceid=chrome&ie=UTF-8