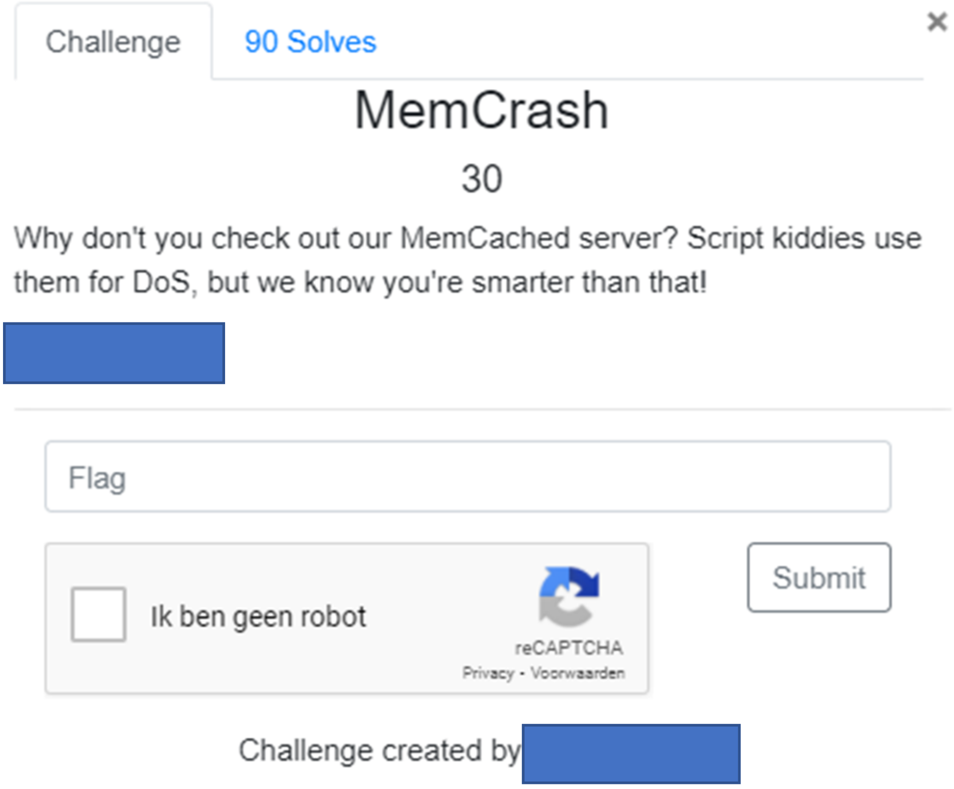
Write-Up Challenge



MemCrash

30

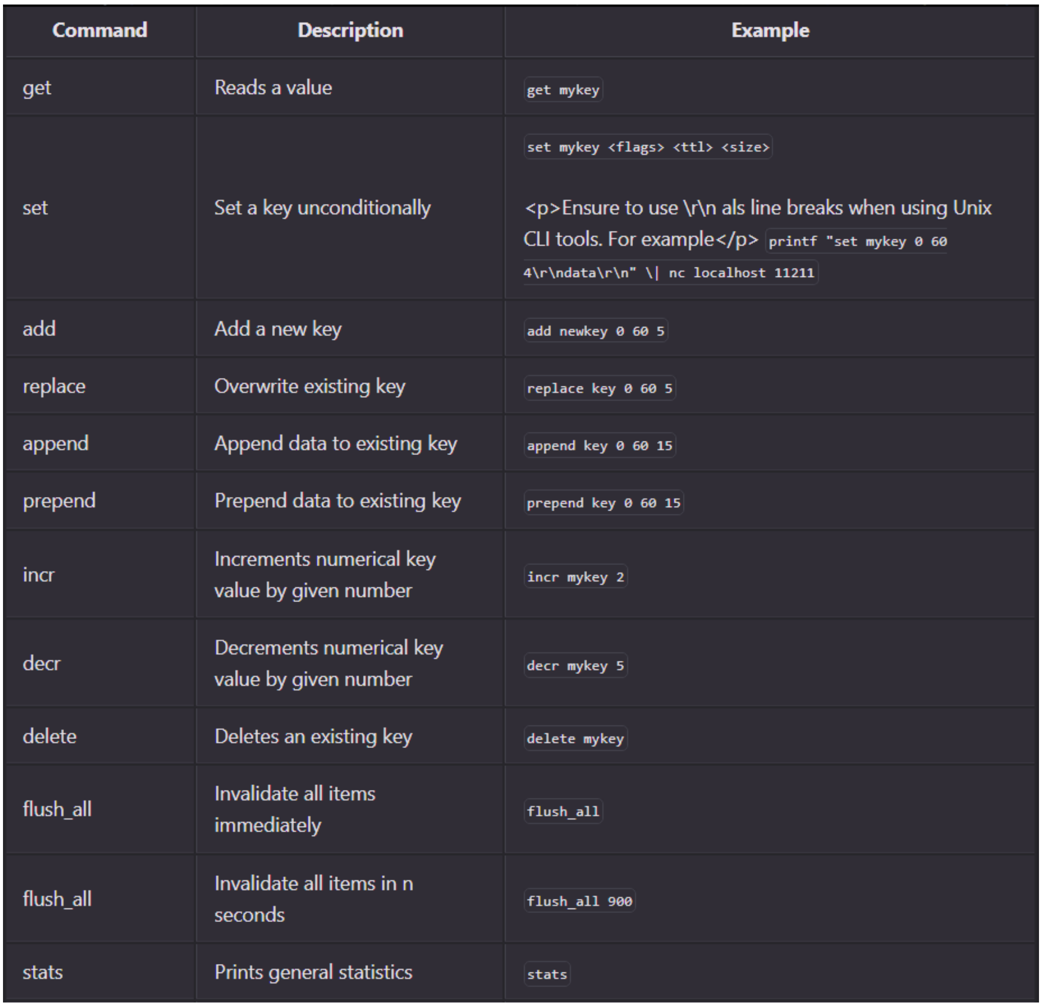
Why don't you check out our MemCached server? Script kiddies use them for DoS, but we know you're smarter than that!

[redacted]

Challenge created by [redacted]

This was a challenge where we only got an IP address and a weird name I've never heard of: MemCached. So of course, I was curious, so I did a telnet session to the IP address. There wasn't much to be found there. So I started looking for things about a memcache server for intel gathering.

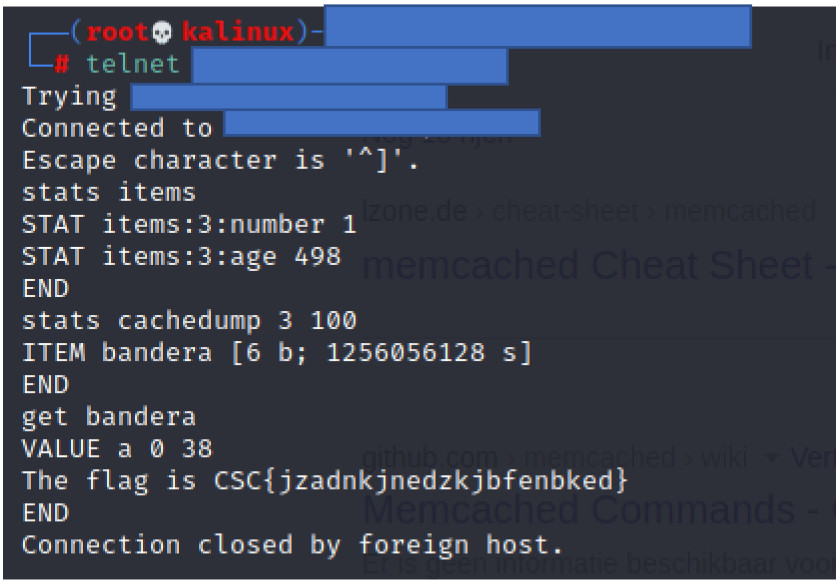
I quickly found out that this server has a specific set of commands you could use.



Command	Description	Example
get	Reads a value	`get mykey`
set	Set a key unconditionally	`set mykey <flags> <ttl> <size>` <p>Ensure to use \r\n als line breaks when using Unix CLI tools. For example</p> `printf "set mykey 0 60 4\r\ndata\r\n" | nc localhost 11211`
add	Add a new key	`add newkey 0 60 5`
replace	Overwrite existing key	`replace key 0 60 5`
append	Append data to existing key	`append key 0 60 15`
prepend	Prepend data to existing key	`prepend key 0 60 15`
incr	Increments numerical key value by given number	`incr mykey 2`
decr	Decrements numerical key value by given number	`decr mykey 5`
delete	Deletes an existing key	`delete mykey`
flush_all	Invalidate all items immediately	`flush_all`
flush_all	Invalidate all items in n seconds	`flush_all 900`
stats	Prints general statistics	`stats`

Link: https://lzone.de/cheat-sheet/memcached

So with this new information, I went back to the telnet session and I used the following commands. And thanks to these commands, I quickly found the answer!



```
┌──(root💀kalinux)-[redacted]
└─# telnet [redacted]
Trying [redacted]
Connected to [redacted]
Escape character is '^]'.
stats items
STAT items:3:number 1
STAT items:3:age 498
END
stats cachedump 3 100
ITEM bandera [6 b; 1256056128 s]
END
get bandera
VALUE a 0 38
The flag is CSC{jzadnkjnedzkjbfenbked}
END
Connection closed by foreign host.
```

Answer: CSC{jzadnkjnedzkjbfenbked}