Writeup untuk `simplehash`

Berikut sebuah program yang meminta kita memasukkan password:

```
drainvers@halcyon:~/sandbox/beefest$ ./simplehash
Enter password: password
Password must be 10 chars long.
drainvers@halcyon:~/sandbox/beefest$ ./simplehash
Enter password: mypassword
Wrong password.
```

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

int passHash = 72;

int checkPass(char *pass){
	int value = 0, i;
	for(i = 0; pass[i] != 0; i++){
		value += pass[i];
	}
	value /= strlen(pass);
	return value;
}

int main(){
	char buf[16];
	printf("Enter password: ");
	fgets(buf, sizeof(buf), stdin);
	buf[strcspn(buf, "\n")] = 0;
	if(strlen(buf) != 10){
		printf("Password must be 10 chars long.\n");
	} else if(checkPass(buf) == passHash){
		system("/bin/cat flag.txt");
	} else{
		printf("Wrong password.\n");
	}
}
```

Seperti yang dapat kita lihat dari source code, program menghitung hash dari password yang kita masukkan dan mencocokkannya dengan nilai hash yang tersimpan. Function tersebut menjumlahkan nilai ASCII dari semua karakter dalam password dan membaginya dengan panjang password, yakni 10. Maka, dengan info di atas, kita dapat membuat password yang menghasilkan hash yang sama. Kita akan menggunakan yang paling mudah, yaitu HHHHHHHHHH karena ‘H’ bernilai 72.

```
drainvers@halcyon:~/sandbox/beefest$ ./simplehash
Enter password: HHHHHHHHHH
BeeFest{L00k_4_H4sh_C0ll1510n}
```