

Forum:[Hack Forums](#)

Thread: [BOF Win64 issue](#)

emadaldin1 - January 8, 2019, 1:09 am

Here is the bof program

Code #include <string.h>

```
void do_something(char *Buffer)
{
    char MyVar[8];
    strcpy(MyVar,Buffer);
}
```

```
int main (int argc, char **argv)
{
```

```
    do_something(argv[1]);
```

```
}being learning about bof but got stuck here
```

tried to insert the address in hex but it kept reading it as ascii like EX: AAAAAAABBBB/*55/*99..

Can someone overwrite the EIP address in here making it point to another location of my choice
thanks

Ironic enough after 5 hours I solved it but you could think of it as challenge to overwrite the EIP in
this program

Nomad.Null - January 8, 2019, 11:41 am

(Jan 8, 2019 02:09 AM)emadaldin1 Wrote: [\[CITE\]](#) Here is the bof program

Code #include <string.h>

```
void do_something(char *Buffer)
{
    char MyVar[8];
    strcpy(MyVar,Buffer);
}
```

```
int main (int argc, char **argv)
{
```

```
    do_something(argv[1]);
```

```
}being learning about bof but got stuck here
```

tried to insert the address in hex but it kept reading it as ascii like EX: AAAAAAABBBB/*55/*99..

Can someone overwrite the EIP address in here making it point to another location of my choice
thanks

Ironic enough after 5 hours I solved it but you could think of it as challenge to overwrite the EIP in
this program

I would expect 5 hours minimum for someone new to stack-based buffer overflows. Congratulations
on figuring it out for yourself. If you want to learn more advanced methods on the subject, might I
suggest the [Corelan Blog](#). Shellcoder's Handbook and Hacking: The Art of Exploitation are also
good books to study it more in-depth.