

# Forum:[Hack Forums](#)

Thread: [Need a Python "Expert"](#)

**Tinkabell** - June 2, 2016, 1:21 pm

Hello, i have a .doc exploit from a friend coded in Python and i dont understand enithing, please help

Thanks Jonas?

**SIM-1866423** - June 2, 2016, 1:44 pm

Let me guess its CVE2012 RTF or CVE2010.And your vague question actually "how can i refud this script", right?

ps : you dont need any "Python Expert" coz its just create a file.

**ItsUzi** - June 2, 2016, 6:07 pm

Step 1: Spell Python correctly

**Goodies** - June 3, 2016, 1:26 pm

Do you know what python does in this scenario?

I'll give you an example. I recently wrote a crack for cobalt strike. I just had to replace a few functions in a compiled .class file. When I was done, I took the class file, compressed it with bzip, and encoded it with base64 so I can store it in my bash script... this is the result

PHP Code

```
<?php
read -d '\n' PATCHFILE << ENDOFFILE
QlpoOTFBWSZTWfLg51oABP///P///+Rr///9////////0AAQQAw452QAwAAVQBRvTK6drbtnN
3Doolw0JNNE1T2kxEHhR6m1DQeo9T1PUaep6NEep4p6jyjagAAGgAB6jTRmU/
Sj1MgZBJEmIETU2
NSn6FNmJpR4U2keoGTRoaA0AAGgADQANAAAD1ANMkig8IP1MpkZGj0nqNBp6jJpoNGQ0ANAA
Bkwg
xABo0A9TT0jTTE0QYBMRgmTCDcYmBMAQwjAQWjgTCYlwAAE0MJiaYECSSFT9NJinqeNMIP1
T1NPR
qGgD1D1AaBoBkABkDQeoAAAAHpaIqr/IRTCkOBYG+
qu2zrkae1U68drq5FyLI1oOjvIXmRmDOYF
NM9JVifeuGKxdiFOL9mq+ZjBADrb0z99hmAvt/ImcEUihoKKMwCD2G0Ahomi+
leLQoWm4pSgTSME
xSZBKinECyr0BuiBGk0+eN64p2kH45Ycvr698yS9ntMeViKE1zNqZmaZorVYwzM2Hy7HJjnpNkVI
6cTlq0K777bgsC7KsrFWfJlupaOtO1I4yqEUDOMc+atplauZPQliK2SnO+6oBReREziSpGFN7kh8
CPiDTP1MRqHNdZ+f+3FKYWJLCocyq/MvUm8K/
YDz9NTzz3jQ75o9DhYH4TbbWp9mmQLUbZ4EUhuN
aLnDg88n+Nt1rJX7K9T2ToWSmlzBkSZB1bAjpfk5z2BmAFX30n4/ajSe5GhEBEPHO6YlStLsad+D
BMdlaHzS8YiUUsVvWvp02/q4V7VQgujev34IMH3yJoethEUiQGoxwDHwH4nO5NSplZbuX9vvjfi/
dIRJdkruSxGI26DBuWQPFgkbvDTCqCbtwuxMxDkTxjqqqyhzGSJXEeOcywYp4dcsK5LuionQE8Y
mgczBLC4ilhxOMAvFYgGI8lhFykiWxrXBWY9epuK2H0sFDdlXrk6gaNB5Jdu7GbAkgyLZyFMRoEZ
NSHHdyI2c7x1NiYaINtL1/uhnjS4xspkLNvskuj1kBKMmonEqRAECsgkmN5QEJZziNOGjJix/MnB
YXprKQCIQxCWRmQPhrUM5pLB7eYtjMn2hjGQldl8Ld1fbPxDQqrn20IMzECGOyejDDd7nUooV433
0XXWyUTy6B2pl9jwFLmsCkUbOaXpDWGefLtfjfuRHgb/
```

```
Gly4uLQaZHwsK8mOjUDAHGWRBTwsseH0G
/YykiQnhByayS5dzaaEy2hV4wRiAHFK8IKkCtRwlfCSMU3eUbYJ3Crzic63K2dEM4C1LxQ9ZfuFZ
MqPKx3w7cOJTxlzQiqCIIDBzwHI4OaRicX6ULYi1o1z7Ey0R3oBRgUgiEylewHBBEFAWKJDO2m51
99899oX1gKzaJq09TTcJrA5dWlrtox9VSMPI93EVal/
BvWqxqMIWmXnaRq2HZDHHoMmm0JuKJiG
pZwS0U9jmy0LYmYFVcFSxLksQGHWKUczTLhHQba2AYGdsjpGvpLzdfS0yjAZbKjgZI3b25BVmIZ
b
RHNI TDDYIQyNFEYJLRp4zMwGYw50JBZVtIHmQ5lcSTqOy7rrjbwpNViIVN06TMjb6a2BYunJDhv
g2CU4EhkUzYpE8GTpJkh2Lyc0SGg4yYccnqh/Yr6MMIWZqw1DjFA9lpFZgTNR2QKImtTmKlua3nG
SMMGG8Wq1aSUXyral4PyaSwojY554KCdZKI4YHDplvEEVsMaxmCJkkqpblogOMrKHU7KIQtioyX
R
5+CKIMpKMKyZHW2pVjDE7CAoDHlci+VF2GVirRDx93Yo4bg3acd69hfRVfuFlhRkmRJ08hiqblJB
mWdy1zEgM+Wlwps7DfJjAgW4IjV19KShSGYGBkKqFdUyMkkDTZwgvrU8MxzNk5KMKhG+
UJ4kOLDD
0JMNmx4qYmqThUmHv1ixwBdLidZ+z2xm5PNm+WMJNDnPwcSNcG5mVhxluf7zWxaeNr/
8XckU4UJ
Dy4OdaA=
ENDOFFILE
```

Now, it is true that this is actually bash scripting... however, if you decode/decompress that with something like this, you can open it up in a java decompiler and find out that it's actually a class file:

PHP Code

```
<?php
```

```
echo $PATCHFILE | sed 's/\s//g' | base64 --decode | bunzip2 > testfile.class
```

To reiterate, it's a FUCKING JAVA CLASS FILE encoded in base64, stored in a bash script. The only thing bash is doing is delivering the data.

If the crack stopped working, you wouldn't ask for a fucking 'byash' scripting expert.  
You wouldn't ask for a base64 expert.

You would ask a fucking java programmer because that's what the payload is written in...

Python is nothing but the syringe. It's the delivery method. It's NOT the god damn exploit...

Fucking christ. How many more of these threads are there going to be?