

Forum: [Hack Forums](#)

Thread: [PDF/Word Exploit Builder](#)

_Pr0xy - July 31, 2017, 3:23 am

So I'm not sure if this is the correct place to put this thread, but it is related to Python.

Recently I have been researching about PDF exploit builders and how they work, and I understand the basics of it, like how you are meant to inject shellcode into the file, but I would like to understand more than the basics and then attempt to create one, as I have noticed that a few of these builders are written in Python. So how do PDF/Word exploit builders work exactly, and how would someone go about writing one in python?

Benoit balls - *July 31, 2017, 3:24 am*

(Jul 31, 2017 03:23 AM)_Pr0xy Wrote: [\[CITE\]](#) So I'm not sure if this is the correct place to put this thread, but it is related to Python.

Recently I have been researching about PDF exploit builders and how they work, and I understand the basics of it, like how you are meant to inject shellcode into the file, but I would like to understand more than the basics and then attempt to create one, as I have noticed that a few of these builders are written in Python. So how do PDF/Word exploit builders work exactly, and how would someone go about writing one in python?

Do you know assembly?

_Pr0xy - July 31, 2017, 3:29 am

No I don't, only Python and C - but to start with I would use a public CVE, rather than look for 0 days, just to get an understanding of it