

# Forum:[Hack Forums](#)

Thread: [Pdf Password](#)

**Spammino** - January 28, 2024, 11:57 pm

Hi guys, i'm kinda new to this so go easy on me ?

Is it possible to access to the content stored in a password protected pdf in any way?

**ubas** - January 29, 2024, 12:57 am

(Jan 29, 2024 12:57 AM)Spammino Wrote: [\[CITE\]](#) Hi guys, i'm kinda new to this so go easy on me ?

Is it possible to access to the content stored in a password protected pdf in any way?

<https://www.kali.org/tools/pdfcrack/>

ez stuff :)

not to hijack the thread, but if anyone has any info on whether or not injects still work on pdfs/word docs i would appreciate that. i know it depends on the reader but typically people just open in chrome or office, but that's the extent of my knowledge

**chormet** - January 29, 2024, 1:25 am

depend which version it encrypted, if you able obtain version, you will be better for crack password. but without crack password no you cant see content

**resetti** - January 29, 2024, 5:59 am

(Jan 29, 2024 01:57 AM)eirian Wrote: [\[CITE\]](#) <https://www.kali.org/tools/pdfcrack/>

ez stuff :)

not to hijack the thread, but if anyone has any info on whether or not injects still work on pdfs/word docs i would appreciate that. i know it depends on the reader but typically people just open in chrome or office, but that's the extent of my knowledge

By "injects", do you mean like shit that is built into Reader (like JS functionality) or Word (like VBA/Macro functionality)??? In the case of Adobe Reader, there is no publicly available exploit which will execute a payload after opening a PDF file currently, the last publicly disclosed one was <https://hacksys.io/blogs/adobe-reader-resetform-cagg-rce-cve-2023-21608>

And the JS shit that u used to be able to do, they got rid of, so theres no type of "pdf macro" you can do.

Either way, it wouldnt be useful since 90% of computers now use Microsoft Edge as a default PDF reader, so now you need a sandbox escape zero day and an browser RCE zero day.

Regarding Macros, they have been disabled by default by Microsoft since 2019, but XLS and XLSM files still accept macros considering their file extensions. Though Word Macros dont work as well anymore since they disabled it.

Overall, your question is kinda vague and im not quite sure what you mean by "Injects", maybe you could elaborate.

Apart from that, i'll say the same thing i say to every kid who asks for a "silent pdf/word exploit", they do not exist without zero day exploits, and a zero day exploit that can silently execute code from a real PDF/Word document, would be worth upwards of \$75,000-\$150,000+, possibly and most likely raising to a higher price depending on the reliability and maturity of the exploit.

Good luck.

**ubas** - January 29, 2024, 12:50 pm

(Jan 29, 2024 06:59 AM)resetti Wrote: [\[CITE\]](#) By "injects", do you mean like shit that is built into Reader (like JS functionality) or Word (like VBA/Macro functionality)??? In the case of Adobe Reader, there is no publicly available exploit which will execute a payload after opening a PDF file currently, the last publicly disclosed one was

<https://hacksys.io/blogs/adobe-reader-resetform-cagg-rce-cve-2023-21608>

And the JS shit that u used to be able to do, they got rid of, so theres no type of "pdf macro" you can do.

Either way, it wouldnt be useful since 90% of computers now use Microsoft Edge as a default PDF reader, so now you need a sandbox escape zero day and an browser RCE zero day.

Regarding Macros, they have been disabled by default by Microsoft since 2019, but XLS and XLSM files still accept macros considering their file extensions. Though Word Macros dont work as well anymore since they disabled it.

Overall, your question is kinda vague and im not quite sure what you mean by "Injects", maybe you could elaborate.

Apart from that, i'll say the same thing i say to every kid who asks for a "silent pdf/word exploit", they do not exist without zero day exploits, and a zero day exploit that can silently execute code from a real PDF/Word document, would be worth upwards of \$75,000-\$150,000+, possibly and most likely raising to a higher price depending on the reliability and maturity of the exploit.

Good luck.

just needed some pointers since im curious about vulnerabilities ive heard about before. that does make sense for something that easy of access to be in that sort of demand. same with the sandbox escapes, although would it be possible to extract browser cache/cookies without one? i had a vague understanding of how they worked, so thank you for the information :)

**DramaKing** - January 29, 2024, 2:04 pm

(Jan 29, 2024 01:50 PM)eirian Wrote: [\[CITE\]](#) just needed some pointers since im curious about vulnerabilities ive heard about before. that does make sense for something that easy of access to be in that sort of demand. same with the sandbox escapes, although would it be possible to extract browser cache/cookies without one? i had a vague understanding of how they worked, so thank you for the information :)

Sure, but you can't do it with a document, namely because they don't actually use cookies, and JS can't do things like grab the entire Cookies file. This is done with XSS.

**whits** - January 29, 2024, 3:35 pm

crack password no you cant see content