Forum:Hack Forums

Thread: How to create a base64 data image url with a payload?

AlphaRays - *December 20, 2020, 10:26 am*

Hey guy,

Code

EBQgFBQQEBQoHBwYIDAoMDAsKCwsNDhIQDQ4RDgsLEBYQERMUFRUVDA8XGBYUGBIUFR
T/2wBDAQMEBAUEBQkFBQkUDQsNFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQ
UFBQUFBQUFBQUFBQUFBQUFBT/wAARCAA2AFwDASIAAhEBAxEB/8QAFwABAQEBAA
AAAAAAAAAAAAAAAAIBA//EACcQAAEDAwQBBAMBAAAAAAAAAABAgMTUVIREhSRYQQjQW
IxMkJy/8QAFwEBAQEBAAAAAAAAAAAAAAAAAAEHCP/EABgRAQEBAQEAAAAAAAAAAAAAAA
ABEUEx/9oADAMBAAIRAxEAPwCeNJZRxpLKRVddRVddTFeuvZ4pfTSYqpnHkwUlZHO/pTN7sl7I
L48mCjjyYKRvdkvZqPci/lewOnGkso40lIIquuoquuoF8aSymO9NIn8qpNV11MWRy/KgVx5MFC+nmX
8b2/5doRvdkvY3uyXsDvugxUboMVI4z7DjPsXpPFufBi4nWDF3ZKwPT41FGTFxBWsGLuxrDg7smjJ
i4yjJgoHXdBio3QYqRxn2HGfYC90GKhzoMV7I4z7BfTPRP1UDdYMXdjWDF3ZNGTFwoyYuAVn5K
Kz8lOm6GyjdDZSnHKq9fTKzqdVWFfhTPY+xFc6zrqKz8lOnsfYez9gJrPyUVn5KdN0NlG6Gygc6z8
lMdM9U/ZTruhspirCuQHKs66is66nT2PsPY+wHOn5FPyACSMVuia6mABcgbtABkbT8in5ABkKfkxW
6eQAZGAAGR//9k8P3BocCBlY2hvICJIZWxsbyBXb3JsZCI7ID8+Cg==

If you decode above base64 image url, you will find that it has payload along with the image itself. My question is, how to make one like this. When i try to encode it back with some changes in the php payload, the image is simply being corrupted. I am sure this is not how it can be done. If somebody know some python script, or some write ups about it?

jinpingxi - *December 20, 2020, 3:33 pm*

(Dec 20, 2020 11:26 AM)AlphaRays Wrote: *[CITE]* Hey guy,

Code

EBQgFBQQEBQoHBwYIDAoMDAsKCwsNDhIQDQ4RDgsLEBYQERMUFRUVDA8XGBYUGBIUFR
T/2wBDAQMEBAUEBQkFBQkUDQsNFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQ
UFBQUFBQUFBQUFBQUFBQUFBT/wAARCAA2AFwDASIAAhEBAxEB/8QAFwABAQEBAA
AAAAAAAAAAAAAAAAIBA//EACcQAAEDAwQBBAMBAAAAAAAAAABAgMTUVIREhSRYQQjQW
IxMkJy/8QAFwEBAQEBAAAAAAAAAAAAAAAAAAEHCP/EABgRAQEBAQEAAAAAAAAAAAAAAA
ABEUEx/9oADAMBAAIRAxEAPwCeNJZRxpLKRVddRVddTFeuvZ4pfTSYqpnHkwUlZHO/pTN7sl7I
L48mCjjyYKRvdkvZqPci/lewOnGkso40lIIquuoquuoF8aSymO9NIn8qpNV11MWRy/KgVx5MFC+nmX
8b2/5doRvdkvY3uyXsDvugxUboMVI4z7DjPsXpPFufBi4nWDF3ZKwPT41FGTFxBWsGLuxrDg7smjJ
i4yjJgoHXdBio3QYqRxn2HGfYC90GKhzoMV7I4z7BfTPRP1UDdYMXdjWDF3ZNGTFwoyYuAVn5K
Kz8lOm6GyjdDZSnHKq9fTKzqdVWFfhTPY+xFc6zrqKz8lOnsfYez9gJrPyUVn5KdN0NlG6Gygc6z8
lMdM9U/ZTruhspirCuQHKs66is66nT2PsPY+wHOn5FPyACSMVuia6mABcgbtABkbT8in5ABkKfkxW
6eQAZGAAGR//9k8P3BocCBlY2hvICJIZWxsbyBXb3JsZCI7ID8+Cg==

If you decode above base64 image url, you will find that it has payload along with the image itself. My question is, how to make one like this. When i try to encode it back with some changes in the php payload, the image is simply being corrupted. I am sure this is not how it can be done. If somebody know some python script, or some write ups about it?

Have you tried getting a image, appending your php code then saving it as a normal image then encoding it through 'base64' default linux command?

I don't think actually base64 encoding it will work (If that's not what you're doing, I apologise)

* edit It's possible the code you see is EXIF data?

https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/hiding-webshell-backdoor-code-in-image-files/