Password Manager Vulnerabilities

By Phoebe Abbruzzese
LMG Security
Institute for Computing Research

Time for a quick poll!

Raise your hand if you have ever reused a password on multiple websites

Raise your hand if you store passwords on a word document or notes app

Why is this an issue?

- If one account is compromised, then all of your account are compromised

- Your accounts contain personal and financial information that should be secure!

- Hackers are able to make money off of your compromised accounts!

- If malware is ever installed onto your computer, then hackers could gain access to your files

What is a password manager?

- Stores all of your passwords and any sensitive information on an encrypted database

- Only need to remember one master password to gain access to all of your passwords

- Some offer more specific features like a password generator, dark web scanner, password sharing, etc.

Are password managers worth it?

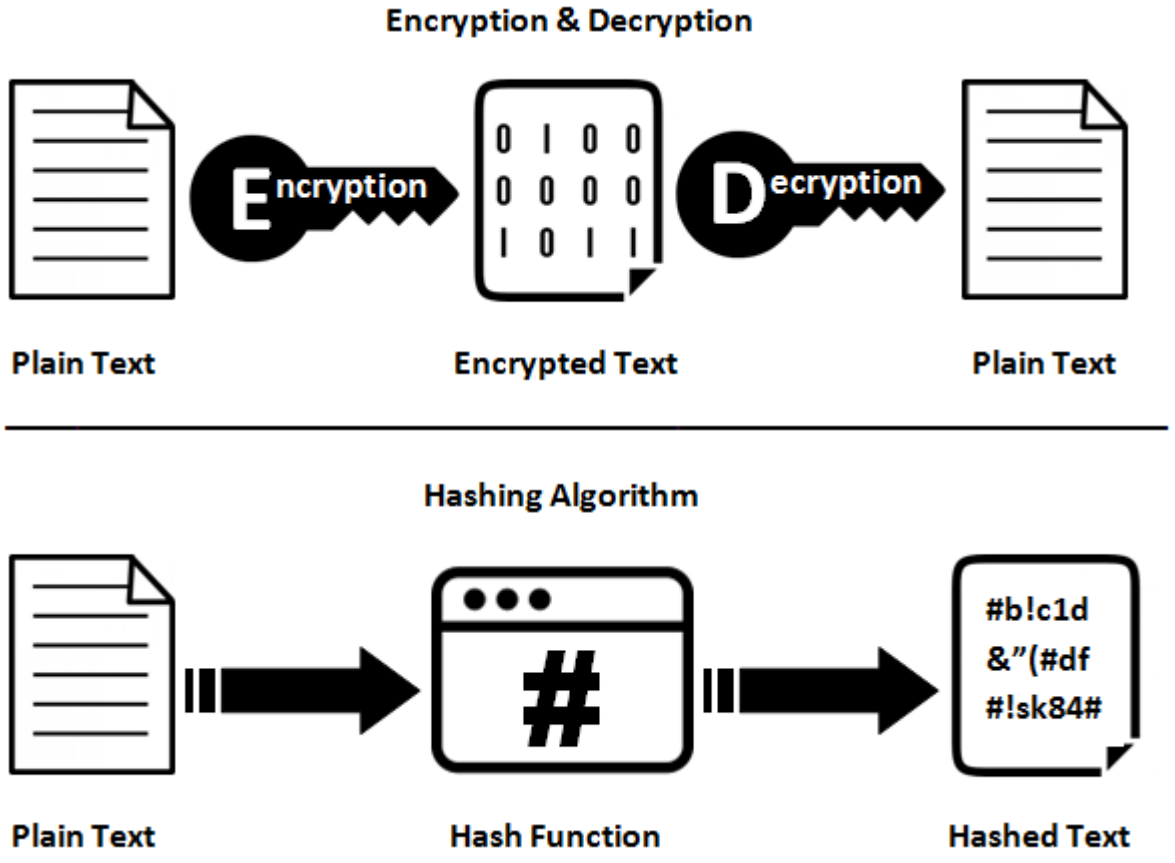
- YES

- If your passwords are strong enough you should not be able to remember all of your passwords by memory

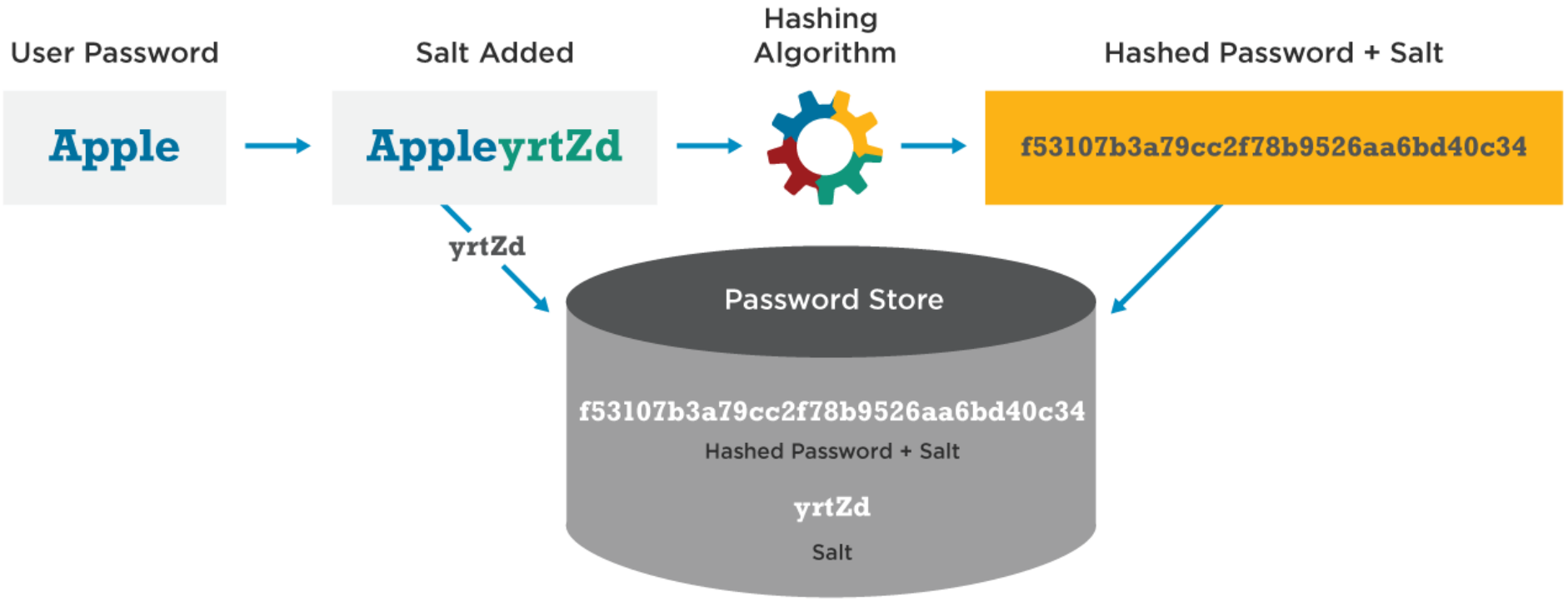
- They are much safer than reusing passwords or storing passwords on plain text documents

- There is a lot of security behind password managers that make them safe to use

How do password managers work?

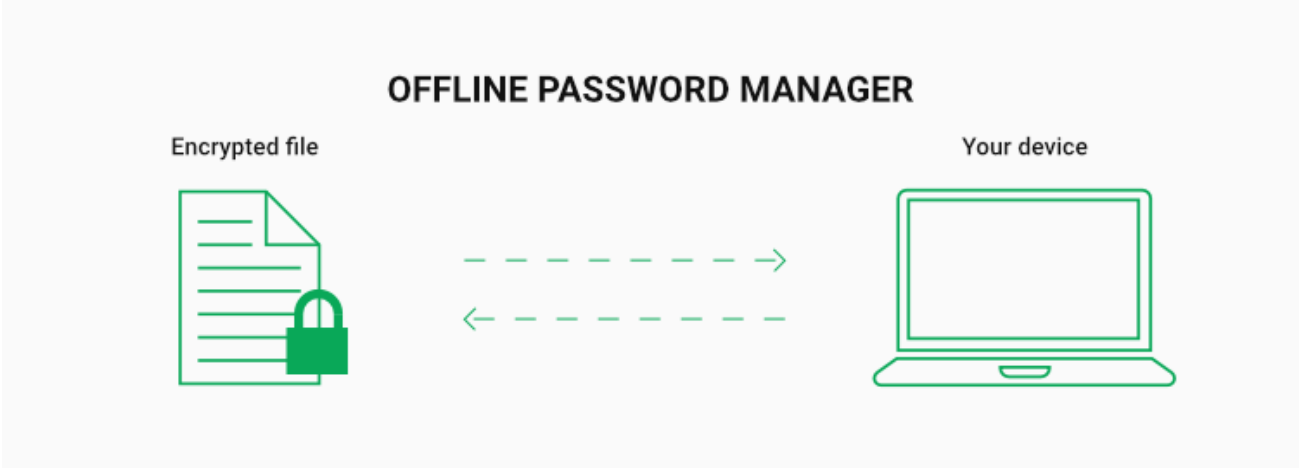

Encryption & Decryption
Encryption
Decryption
Plain Text
Encrypted Text
Plain Text
Hashing Algorithm
#
#b!c1d
&”(#df
#!sk84#
Plain Text
Hash Function
Hashed Text

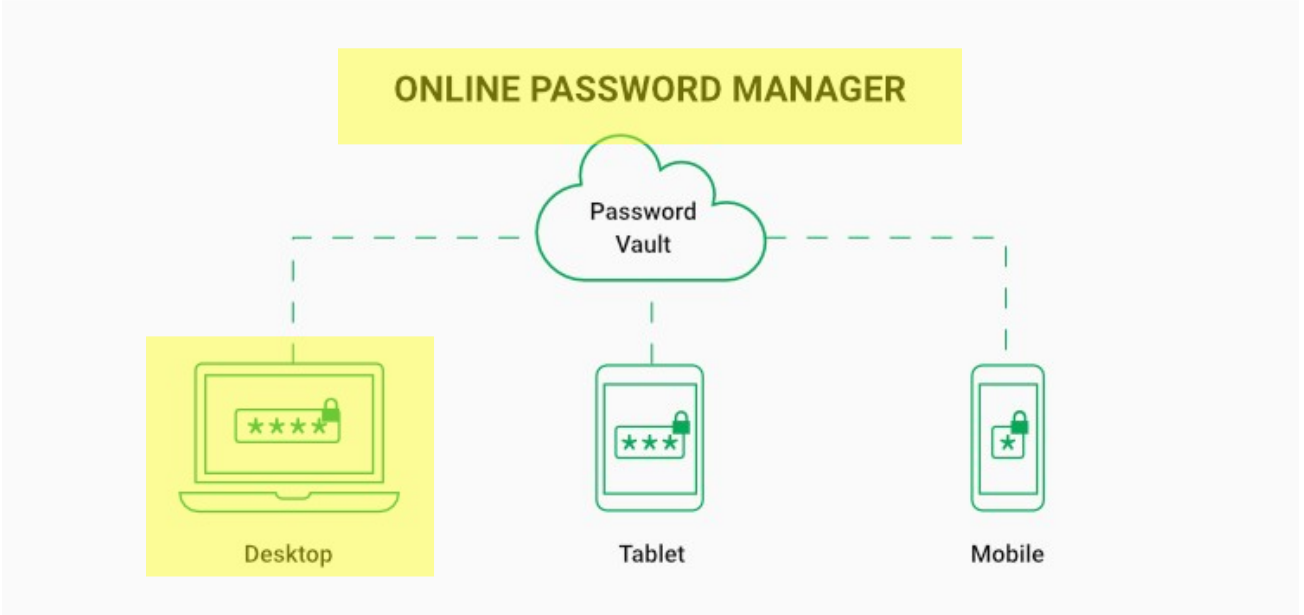
Password Hash Salting



Wordfence™

wordfence.com/learn


OFFLINE PASSWORD MANAGER
Encrypted file
Your device


ONLINE PASSWORD MANAGER
Password
Vault
Desktop
Tablet
Mobile

Project Goal:

Find vulnerabilities on 5 different web-based password managers: Bitwarden, Azure, Roboform, Lastpass, and Dashlane

BeEF Attack

- BeEF is a module in Kali Linux that has several different attack features on browsers

- Essentially it is able to “hook” a browser if someone just clicks on a malicious link

- Wanted to test out the iframe injection and lastpass detection features

- Browsers have updated to stop most of BeEF’s features from working so ultimately this attack was not useful

Pyperclip Attack

- Most password managers have a clipboard feature that allows users to copy and paste their passwords

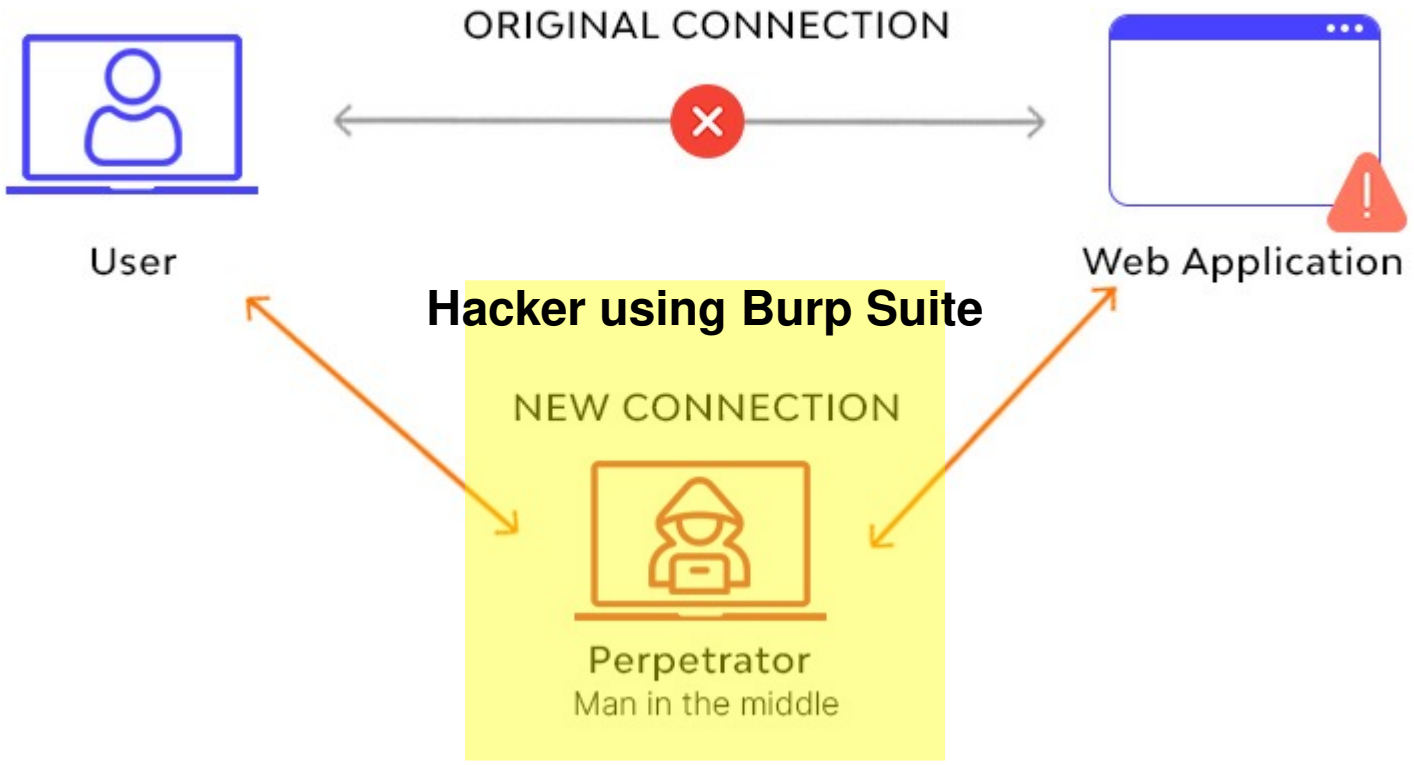
- This code stores everything the victim copies and pastes on a CSV file, and emails the hacker everything on the file

- This is all done automatically without the victim knowing

- This was successful on any password manager that had a copy/paste feature

- The attacker would need the victim to download the python code onto their computer

Man-in-the-middle Attack



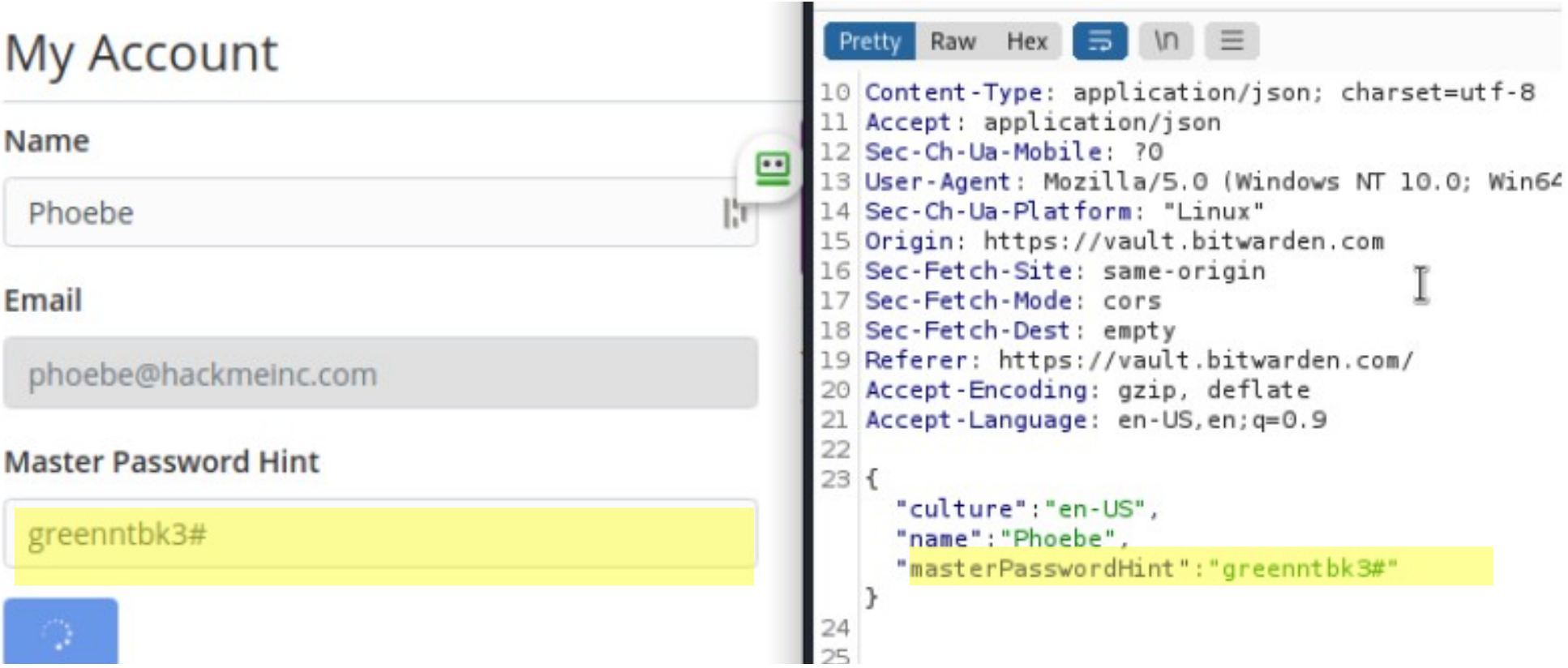
Man-in-the-middle Attack

Main Findings Using MITM Attack

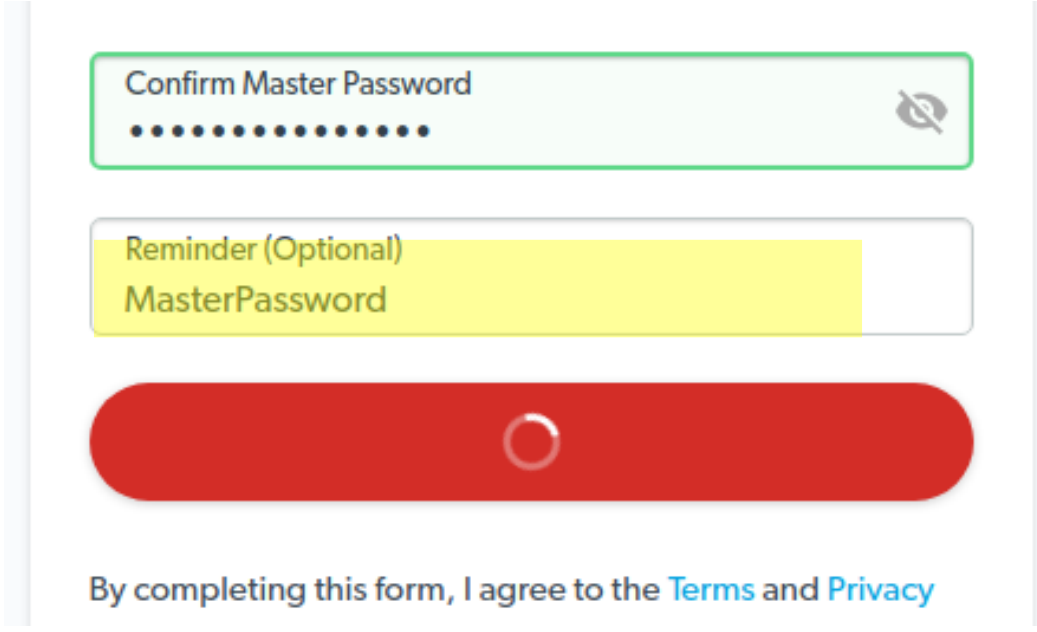
Bitwarden

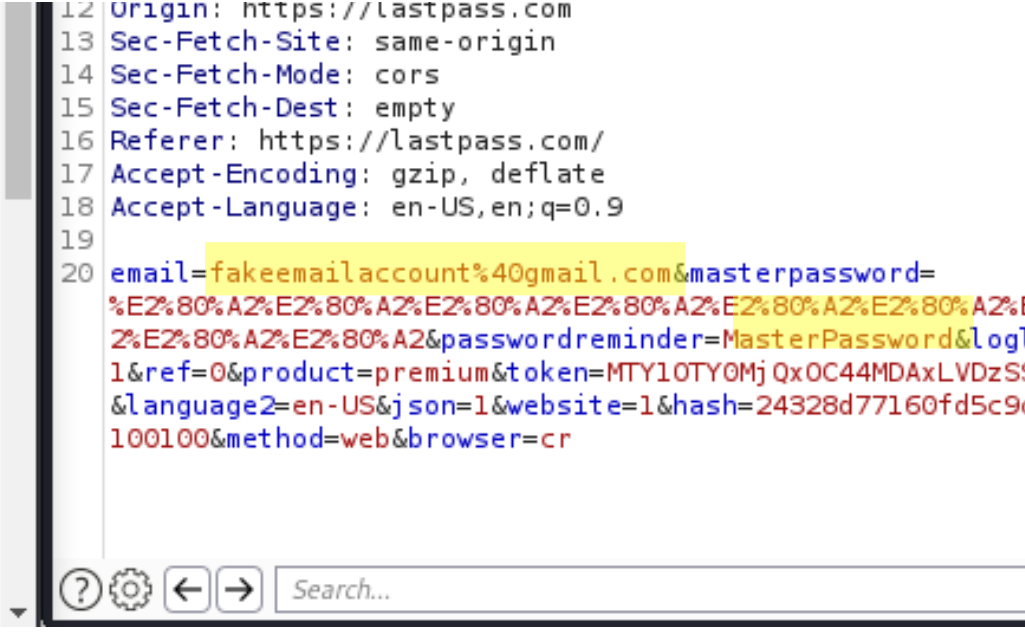

```
{
  "email":"phoebe@hackmeinc.com",
  "name":"Phoebe",
  "masterPasswordHash":"m1SIfD6LD1ugsJ2Xg1HgPH1kdRbw8y5ceL0qDhvn2Xg=",
  "key":"2.HaSfnk+uiIcBE21PjyyiRA==|losvHrH1SKA0E9yKxPu+0yjMnFw0IOo3P+8
  "kdf":0,
  "kdfIterations":100000,
  "referenceData":{
    "id":"1453248666.1659041651"
  },
  "captchaResponse":null,
  "masterPasswordHint":"gnbk3#",
  "keys":{
    "publicKey":
    "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyR6HTXixDU2GSaVzj8A02L
    OxzqQA9PBrj5a4M+e0YBCSuojs0S6pttaua0Ij6n8XMfvL8dKZ5b8eCgM1zL+758L1
    "encryptedPrivateKey":
    "2.0OX2Xje5VkqNA7/OqDKBqQ==|H1/2Zou9vacMx/uBjC1NQ6wpYUybppfO/yO/9pa
    X7KD/VLTX8iOeMsZrErDORKnAPI9CqlL0ZIKEvM5u2VwdVzlCL6mvvOaYmqLwtUxIKE
```

Bitwarden

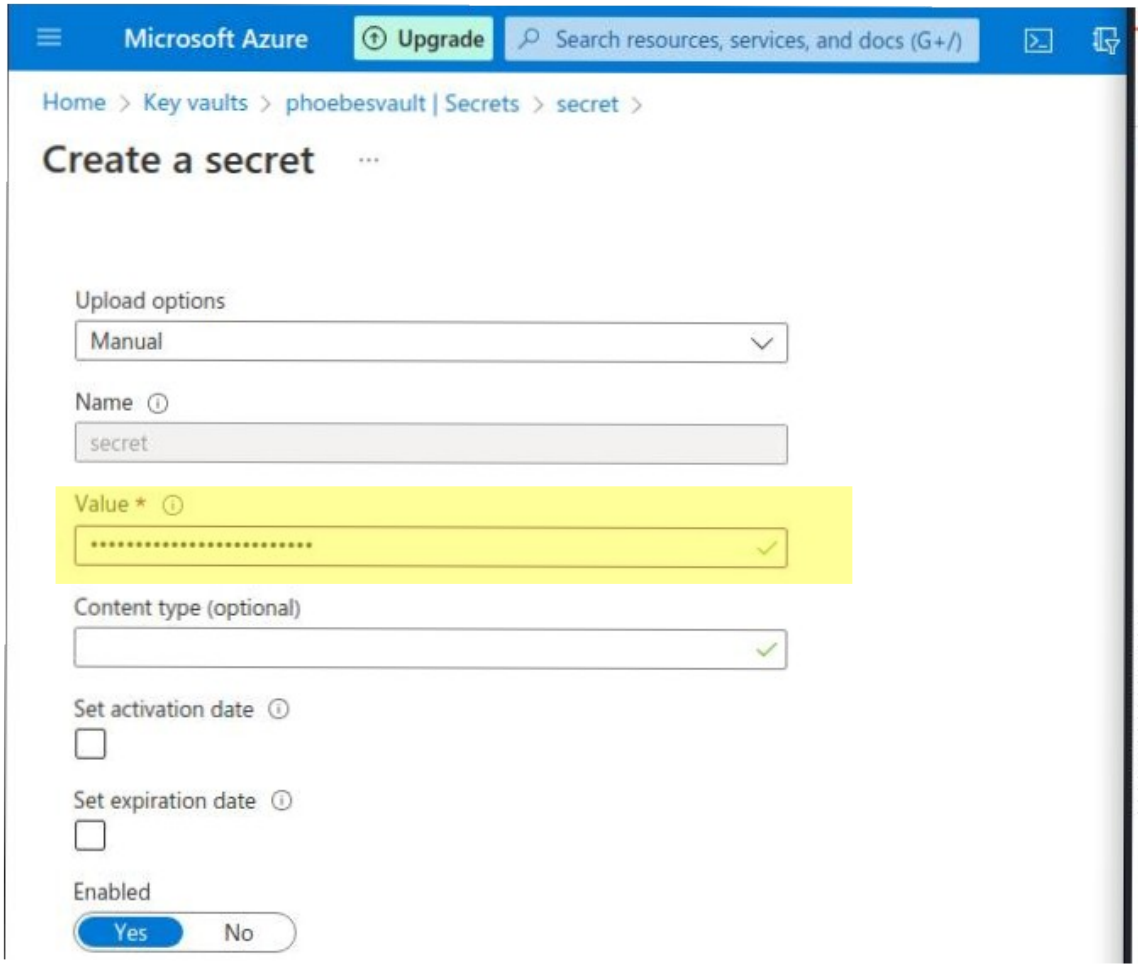

My Account
Name
Phoebe
Email
phoebe@hackmeinc.com
Master Password Hint
greennntbk3#
Pretty
Raw
Hex
\n
10 Content-Type: application/json; charset=utf-8
11 Accept: application/json
12 Sec-Ch-Ua-Mobile: ?0
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64
14 Sec-Ch-Ua-Platform: "Linux"
15 Origin: https://vault.bitwarden.com
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: cors
18 Sec-Fetch-Dest: empty
19 Referer: https://vault.bitwarden.com/
20 Accept-Encoding: gzip, deflate
21 Accept-Language: en-US,en;q=0.9
22
23 {
"culture":"en-US",
"name":"Phoebe",
"masterPasswordHint":"greennntbk3#"
}
24
25

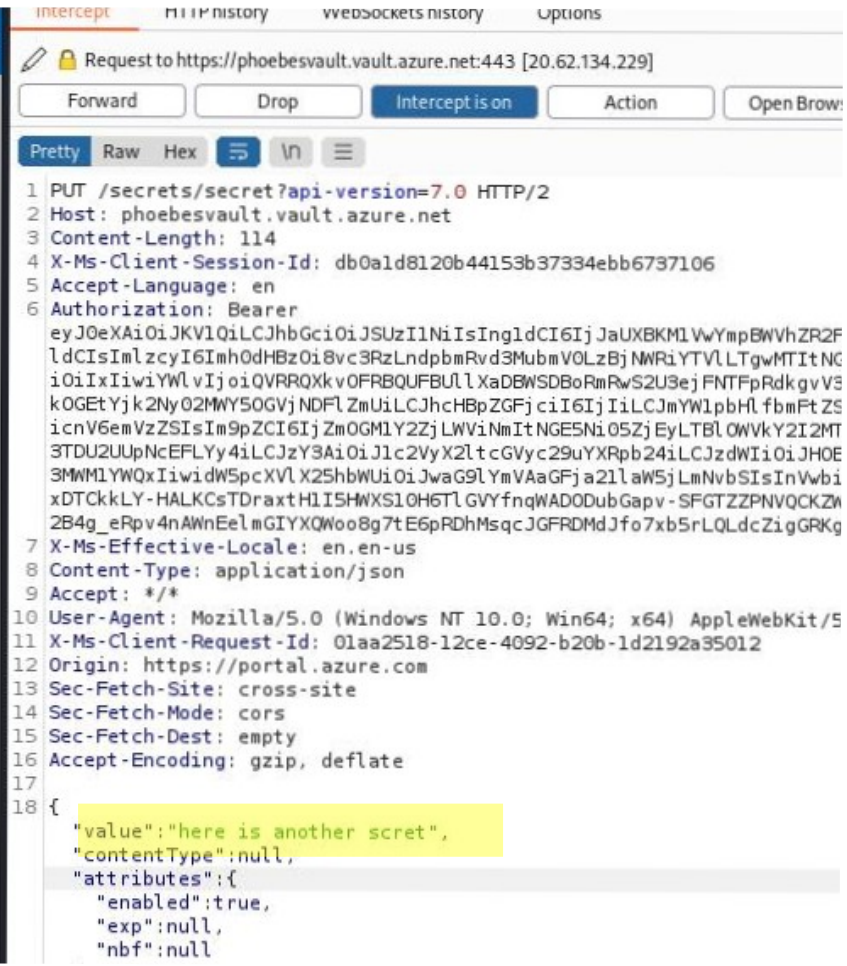
LastPass


Confirm Master Password
Reminder (Optional)
MasterPassword
By completing this form, I agree to the Terms and Privacy


12 Origin: https://lastpass.com
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://lastpass.com/
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.9
19
20 email=fakeemailaccount%40gmail.com&masterpassword=
%E2%80%A2%E2%80%A2%E2%80%A2%E2%80%A2%E2%80%A2%E2%80%A2%E2%80%A2%E2%80%A2%E2%80%A2&passwordreminder=MasterPassword&log
1&ref=0&product=premium&token=MTY1OTY0MjQxOC44MDAxLVDz
&language2=en-US&json=1&website=1&hash=24328d77160fd5c9
100100&method=web&browser=cr
Search...

Azure


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Home > Key vaults > phoebesvault | Secrets > secret >
Create a secret
Upload options
Manual
Name
secret
Value *
Content type (optional)
Set activation date
Set expiration date
Enabled
Yes
No


Intercept
HTTP history
WebSockets history
Options
Request to https://phoebesvault.vault.azure.net:443 [20.62.134.229]
Forward
Drop
Intercept is on
Action
Pretty
Raw
Hex
PUT /secrets/secret?api-version=7.0 HTTP/2
Host: phoebesvault.vault.azure.net
Content-Length: 114
X-Ms-Client-Session-Id: db0a1d8120b44153b37334ebb6737106
Accept-Language: en
Authorization: Bearer
X-Ms-Effective-Locale: en.en-us
Content-Type: application/json
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/5
X-Ms-Client-Request-Id: 01aa2518-12ce-4092-b20b-1d2192a35012
Origin: https://portal.azure.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Accept-Encoding: gzip, deflate
{
"value":"here is another scret",
"contentType":null,
"attributes":{
"enabled":true,
"exp":null,
"nbf":null

Conclusion

- Browser and app updates are important!

- Be cautious with the clipboard feature

- More personal information should be encrypted on password managers

- Password managers, despite a few exceptions, are pretty safe and should be more widely used

Questions?