

WINTER - RESUME

[Google Earth adventures]

by `omespino@BSides:~/San Diego$`

whoami

Omar Espino



Twitter (X):

@omespino

Personal Blog:

omespino.com

Security Consultant at Websec (@_websec)



Bug Bounty Hunter



Google



Microsoft



slack

NOKIA



ATLASSIAN

YAHOO!



SONY

agenda

```
omespino@localh0st:~/ $ 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 the conference 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** and **AI AI AI AI AI**
ha!



CALL ME ROMANTIC...

***BUT I STILL BELIEVE IN
HANDCRAFT HACKING***

CASE STUDY

NO. 1

Google Earth `/etc/environment` exfiltration

Google Earth /etc/environment exfiltration

Part 0 - XML everywhere



→ 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 vlw-pushoin</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
1	PATH="/usr/local/sbin:/usr/local/bin:/usr/bin:/bin:/usr/sbin:/sbin"
2	JAVA_HOME="/opt/jre/bin"
3	SUPER_SECRET_VAR="TOP_SECRET"
4	AWS_KEY="OWNED"

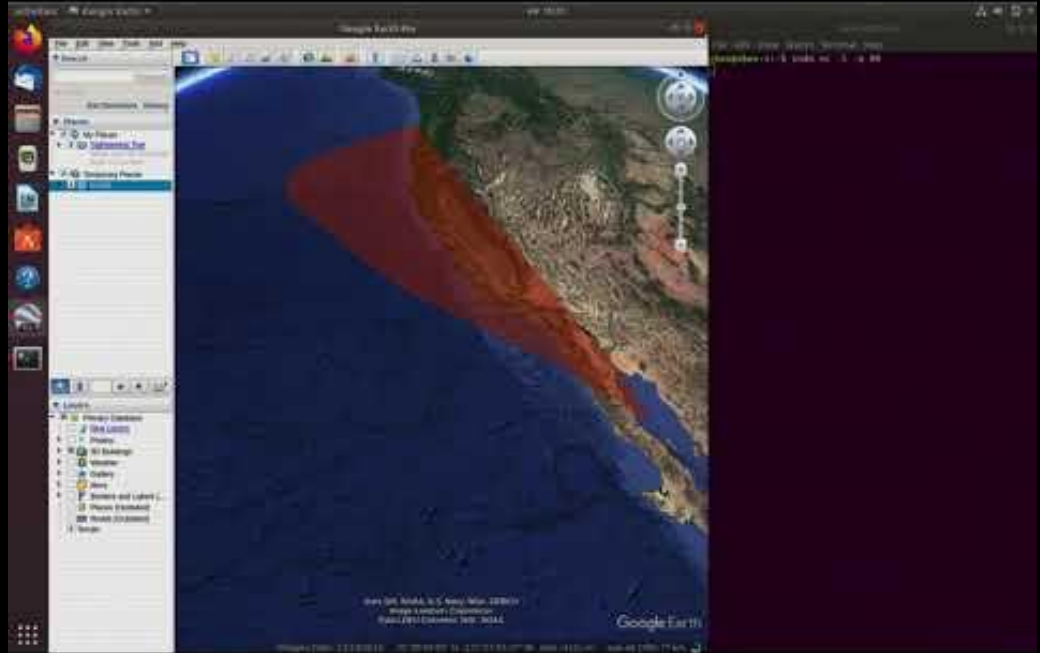
And then the vars are loaded in the DOM and you could send them wherever you want.

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

POC

Google Earth /etc/environment exfiltration

Actual
report



Google Earth /etc/environment exfiltration

iOS/Android
(html5 apis)
Variation



CASE STUDY

NO. 2

Google Earth

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

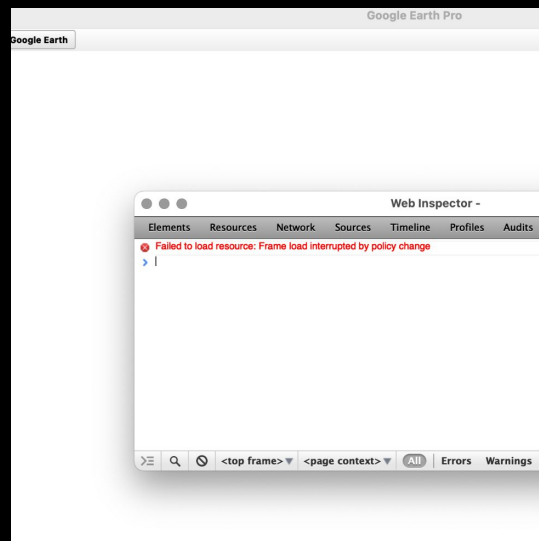
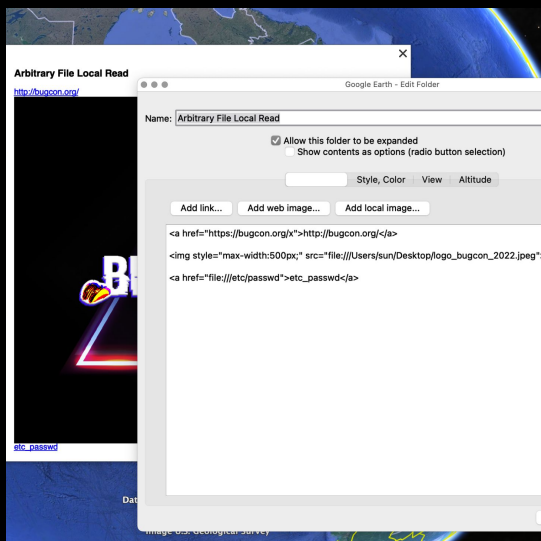


It has a simple Safari webview sandboxed and sanitized

Anti recon by `omespino@localh0st:~/S`

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 not so fast

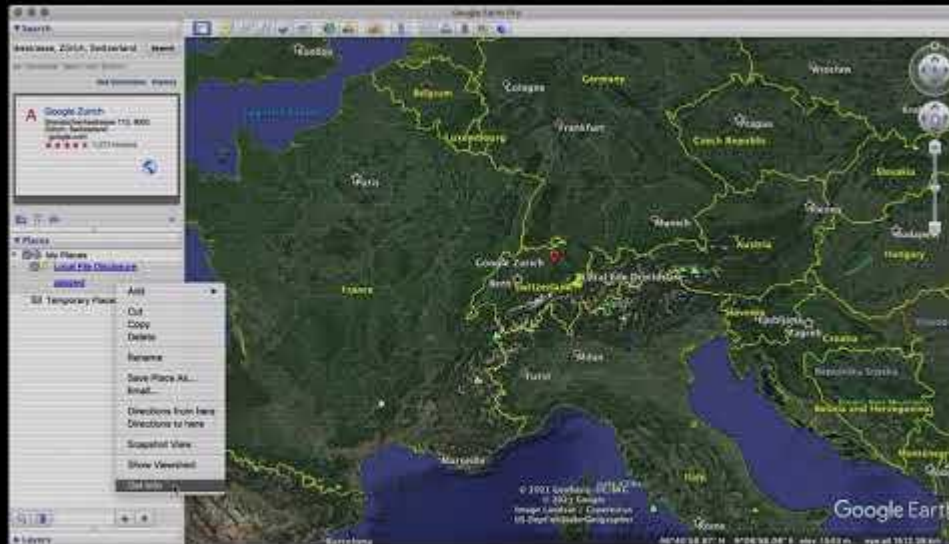


There is a policy that blocks any file to be loaded, after some testing I was able to load successfully images files (jpg, png, gif) and `HTML files`

POC

Google Earth arbitrary local file read

Actual
report



lessons learned

```
omespino@localh0st:~/ $ 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

results

- *A lot of fun*
- */etc/environment loads / acts
a as javascript object
w0000t??*
- *~ X,XXX USD profit*

Q&A



TROPICON

INFORMATION SECURITY CONFERENCE



**JOE
GRAND**

INVITADO ESPECIAL



- ANGEL GANGAS
- CÉSAR ARELLANES
- DAVID BERNAL MICHELENA
- IGNACIO GÓMEZ
- JEAN PAUL GRANADOS
- EDUARDO VELA

- PEDRO JOAQUÍN
- MARCO ALMAGUER
- MARIANO MARINO
- OMAR ESPINO
- JAIME RESTREPO
- IGNACIO GÓMEZ VILLASEÑOR



**BEN
SADEGHIPOUR**

INVITADO ESPECIAL



Locación
Cozumel



Fecha
Abril 17 y 18, 2026

2025 2025 CZM/MX APRIL 17-18



TROPICON
INFORMATION SECURITY CONFERENCE



@_tropicon



wa.me



contact@tropicon.org

www.tropicon.org

ありがとう

ARIGATŌ

GRAZIE

DANKE

DANKON

धन्यवाद

THANK YOU

MERCI

谢谢
XIÈXIÈ

감사합니다

СПАСИБО

GRACIAS