

## 精读 - IoTScope

笔记本: 99 - Paper

创建时间: 2022/5/12 20:39

更新时间: 2022/5/28 10:21

作者: dreamingctf@163.com

PS: 记得每个都要修改 vms 和 urlList

- 1: 文件准备  
python3 init.py D-Link DAP1320
- 2: FirmAE 固件模拟  
sudo ./run.sh -r DAP1320 ./firmwares/DAP1320.bin
- 3: enumerate -> 修改 vms  
python3 enumerating.py
- 4: delivering -> 修改 vms 和 urlList  
python3 delivering.py
- 5: 修改 vms, 生成 uai.txt  
sudo python3 identifyingUnprotected.py
- 6: db  
sudo python3 dbAssistant.py
- 7:  
sudo python3 idH.py

测试结果:

DIR-412 跑不起来

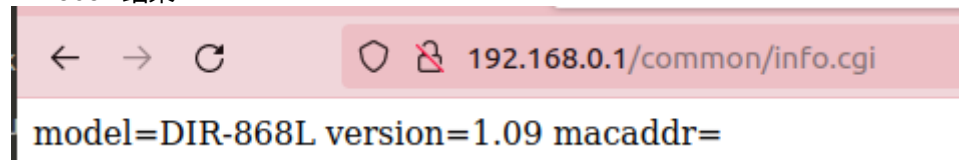
```
ubuntu@ubuntu:~/Desktop/DIR600/FirmAE$ sudo ./run.sh -r dir412 ./firmwares/DIR412.bin
[sudo] password for ubuntu:
[*] ./firmwares/DIR412.bin emulation start!!!
[*] extract done!!!
[*] get architecture done!!!
mke2fs 1.44.1 (24-Mar-2018)
e2fsck 1.44.1 (24-Mar-2018)
[*] infer network start!!!

[IID] 10
[MODE] run
[+] Network reachable on 192.168.0.1!
Creating TAP device tap10_0...
Set 'tap10_0' persistent and owned by uid 0
Bringing up TAP device...
Starting emulation of firmware... None false false -1 -1
```

DIR-816 能用 FirmAE 跑起来

```
sudo ./run.sh -r dir816 ./firmwares/DIR816L.bin
```

DIR868L 结果



model=DIR-868L version=1.09 macaddr=

```
← → ↻ 192.168.0.1/portal/comm/event.php

event.php
~/Downloads

potentialExist.txt × get_LogDnsQuery.asp × event.php ×

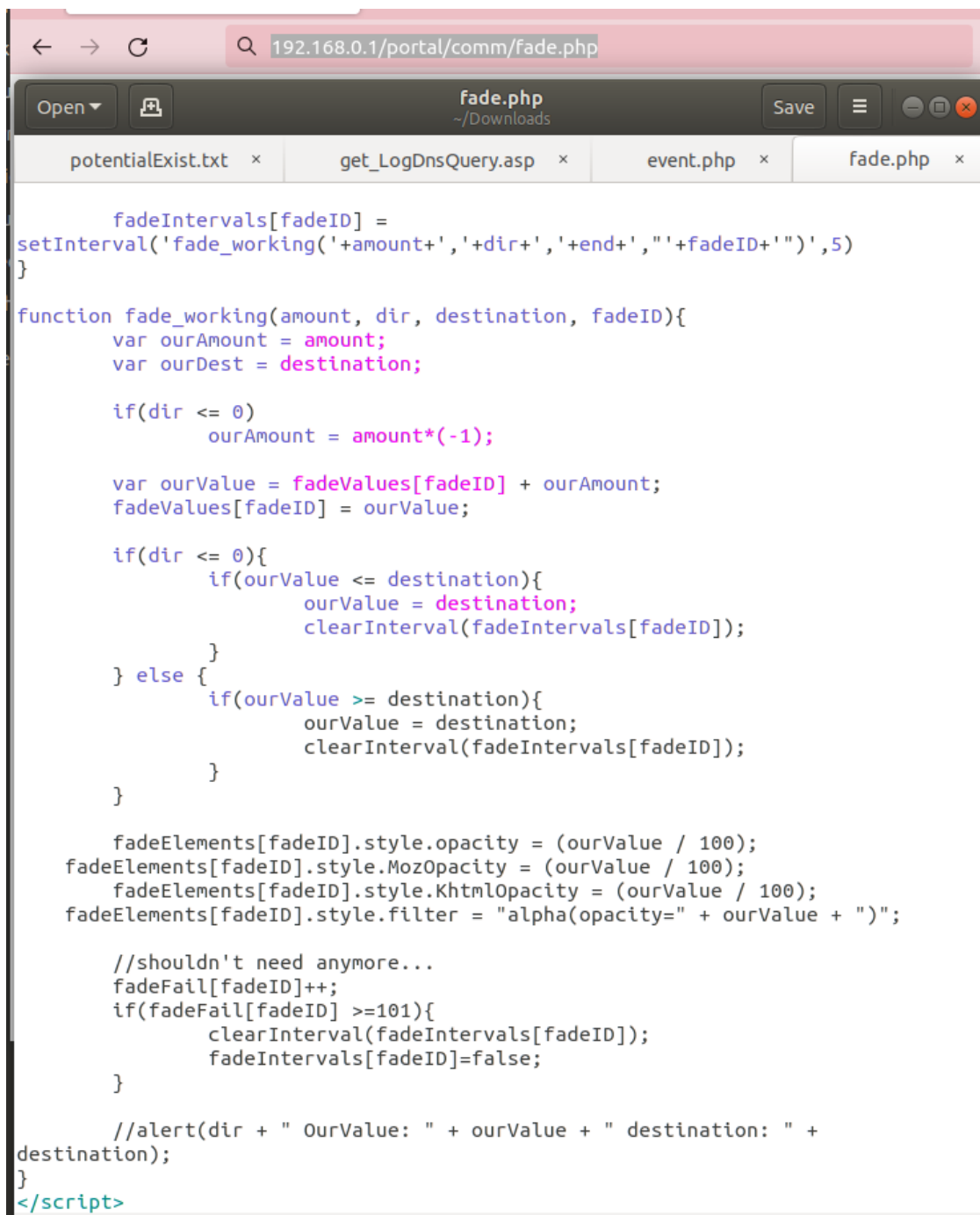
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.

Epiware, Inc., hereby disclaims all copyright
interest in the program 'SSLBridge' written
by Patrick Waddingham.

21 August 2006
James Kern, President of Epiware
*****/
function getEvent(e){
    var eventReturn = (e || window.event);
    //alert(eventReturn.target);
    if(!eventReturn.target)
        eventReturn.target = event.srcElement;
    if(eventReturn.target.nodeType == 3)
        eventReturn.target =
eventReturn.target.parentNode.parentNode.parentNode;
    return eventReturn; //gets the event information
}

function addEvent(event, funct, elem){
    //I assume it is an IE-like browser if this fails - this isn't very
'safe'
    if(elem.addEventListener) //Netscape/FireFox
        elem.addEventListener(event,funct,true);
    else //IE
        elem.attachEvent("on"+event,funct);
}
}
```



```
fadeIntervals[fadeID] =
setInterval('fade_working('+amount+', '+dir+', '+end+', '"+fadeID+"'')', 5)
}

function fade_working(amount, dir, destination, fadeID){
    var ourAmount = amount;
    var ourDest = destination;

    if(dir <= 0)
        ourAmount = amount*(-1);

    var ourValue = fadeValues[fadeID] + ourAmount;
    fadeValues[fadeID] = ourValue;

    if(dir <= 0){
        if(ourValue <= destination){
            ourValue = destination;
            clearInterval(fadeIntervals[fadeID]);
        }
    } else {
        if(ourValue >= destination){
            ourValue = destination;
            clearInterval(fadeIntervals[fadeID]);
        }
    }

    fadeElements[fadeID].style.opacity = (ourValue / 100);
    fadeElements[fadeID].style.MozOpacity = (ourValue / 100);
    fadeElements[fadeID].style.KhtmlOpacity = (ourValue / 100);
    fadeElements[fadeID].style.filter = "alpha(opacity=" + ourValue + ")";

    //shouldn't need anymore...
    fadeFail[fadeID]++;
    if(fadeFail[fadeID] >=101){
        clearInterval(fadeIntervals[fadeID]);
        fadeIntervals[fadeID]=false;
    }

    //alert(dir + " OurValue: " + ourValue + " destination: " +
destination);
}
</script>
```

```
WNDR4000 LOG
[+]Potential UAI: http://192.168.1.1/03/message.cgi
[+]Potential UAI: http://192.168.1.1/wnr2000v2/enu/202-10485-01/genie_detwan.htm
[+]Potential UAI: http://192.168.1.1/site/LAN_lan_h.htm
[-]Error in http://192.168.1.1/wndr3400/enu/202-10581-01/USB_adv_main.htm as
ConnectionError
[-]Error in http://192.168.1.1/31/WPS_h.htm as ConnectionError

[+]Potential UAI: http://192.168.1.1/node/searchform.action
[+]Potential UAI:
http://192.168.1.1/assets/jquery/jScrollPane/genie_detecting.htm
[-]Error in
http://192.168.1.1/assets/jquery/jScrollPane/MNU_access_unauthorized_index.htm as
ConnectionError
[-]Error in http://192.168.1.1/peanuthull/ver_check.cgi as ConnectionError
```

NETGEAR Router WNDR340(X) +

192.168.1.1/ADV\_home2.htm

☆

✓ Router Information

Hardware VersionWNDR4000

Firmware VersionV1.0.2.2\_9.1.84

GUI Language VersionV1.0.2.2\_2.1.17.1

LAN Port

MAC Address00:00:00:00:00:01

IP Address192.168.1.1

DHCPOn

Reboot

⚠ Internet Port

MAC Address00:00:00:00:30:05

IP Address0.0.0.0

ConnectionDHCP

IP Subnet Mask0.0.0.0

Domain Name Server0.0.0.0

Show Statistics

Connection Status

⚠ Wireless Settings (2.4GHz)

Name (SSID)NETGEAR

RegionEurope

ChannelAuto (0)

ModeUp to 145 Mbps

Wireless APOn

Broadcast NameOn

Wireless isolationOff

Wi-Fi Protected SetupNot Configured

⚠ Wireless Settings (5GHz)

Name (SSID)NETGEAR-5G

RegionEurope

Channel0

ModeUp to 450 Mbps

Wireless APOn

Broadcast NameOn

Wireless isolationOff

Wi-Fi Protected SetupNot Configured

192.168.1.1/LAN\_reserv\_add.htm

☆

Address Reservation

+ Add

X Cancel

↺ Refresh

Address Reservation Table

	#	IP Address	Device Name	MAC Address
--	---	------------	-------------	-------------

IP Address

192 . 168 . 1 .

MAC Address

Device Name

192.168.1.1/reserv.cgi?id=506189070

LAN Setup

Apply

Cancel

Device Name

WNDR4000

LAN TCP/IP Setup

IP Address

192

.

168

.

1

.

1

IP Subnet Mask

255

.

255

.

255

.

0

RIP Direction

Both

RIP Version

Disabled

☒ Use Router as DHCP Server

Starting IP Address

192

.

168

.

1

.

2

Ending IP Address

192

.

168

.

1

.

254

Address Reservation

	#	IP Address	Device Name	MAC Address

+ Add

Edit

Delete

Help Center

Show/Hide Help Center