Qualys Security Advisory QSA-2017-02-22

February 22, 2017

Insecure CrossDomain.XML in D-Link DCS Series Cameras

SYNOPSIS:

D-Link DCS series network cameras have a weak/insecure CrossDomain.XML file which allows sites hosting malicious flash object to access and/or change device's settings.

Reference: http://us.dlink.com/product-category/home-solutions/view/network-cameras/

CVE: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-7852

Vendor Response: In 2016 we phased in CSRF mitigation on all CGI on the cameras so an injection like this would not be allowed authenticated or unauthenticated.

Please refer to the tracking table at the bottom of this report which includes the H/W Revision and firmware when this CSRF mitigation was enabled.

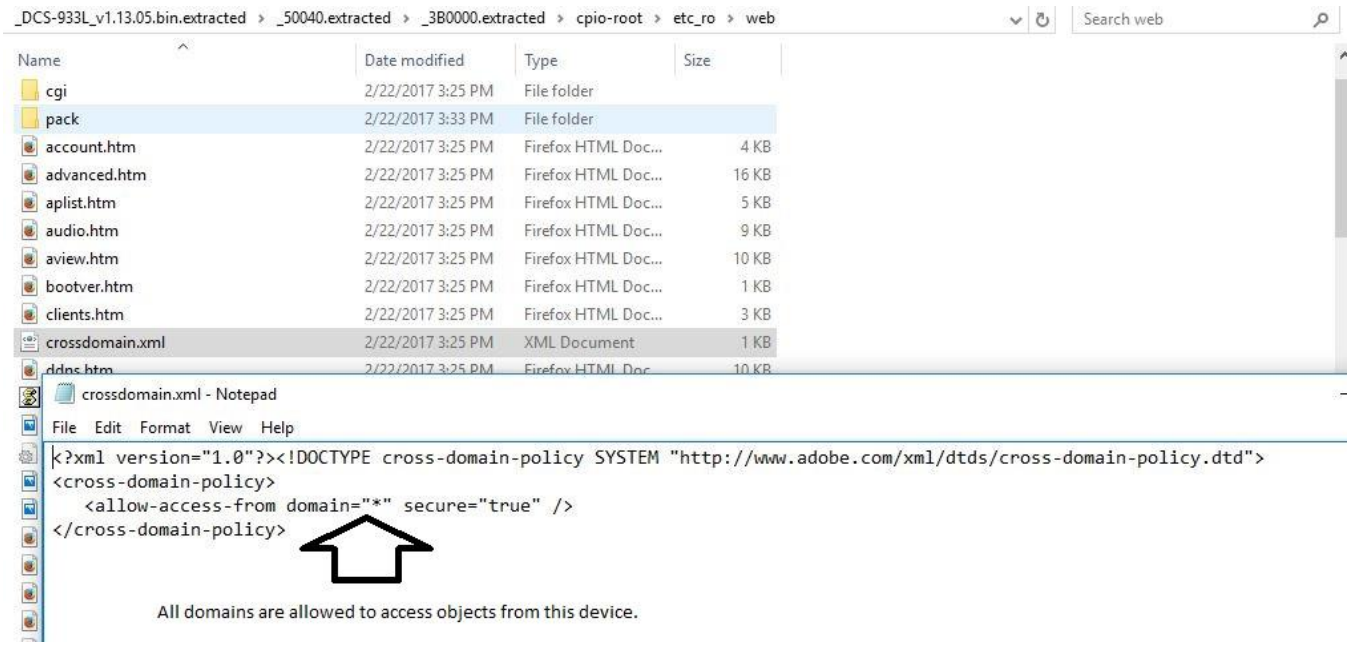
VULNERABILITY DETAILS:

Lab Setup:

1. Target Camera: DCS-933L with firmware version 1.03
2. Target IP Address: 10X.X.X.X
3. Site Hosting Malicious Flash Object: http://Maliciousxxxx.com
4. Camera settings sent to: http://MyMaliciousSite.com

Vulnerable/Tested Version:

DCS-933L running firmware version 1.03 is affected. However, the latest firmware for this device and as well as other devices like **DCS-5030L, DCS-5020L, DCS-2530L, DCS-2630L, DCS-930L, DCS-932L, DCS-932LB1** etc. have same file containing weak or improper configurations



Note: It seems that all DCS series network cameras have same file containing weak or improper configurations but I haven't checked it on all models.

Vulnerability: Insecure CrossDomain.XML file vulnerability

An unauthenticated, remote attacker could host a malicious Flash file on his website that makes requests to the victim's device without having credentials.

Risk Factor: High

Impact:

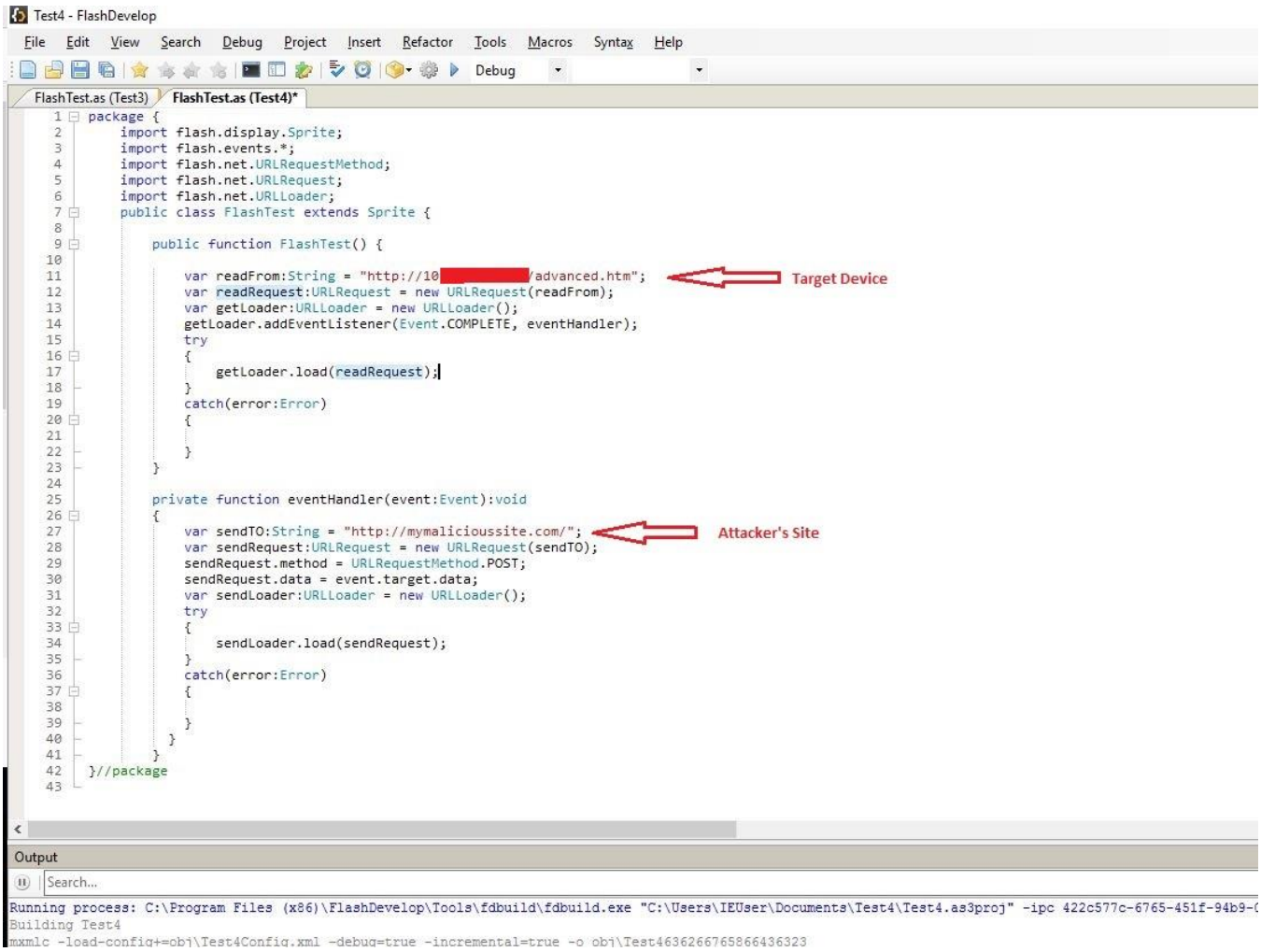
If a victim is logged in to the camera's web console and visits a malicious site hosting a malicious Flash file from another tab in the same browser, the malicious flash file then can send requests to the victims DCS series Camera without knowing the credentials.

An attacker can host a malicious Flash file which can retrieve Live Feeds or information from victims DCS series Camera, add new admin users or make other changes to the device.

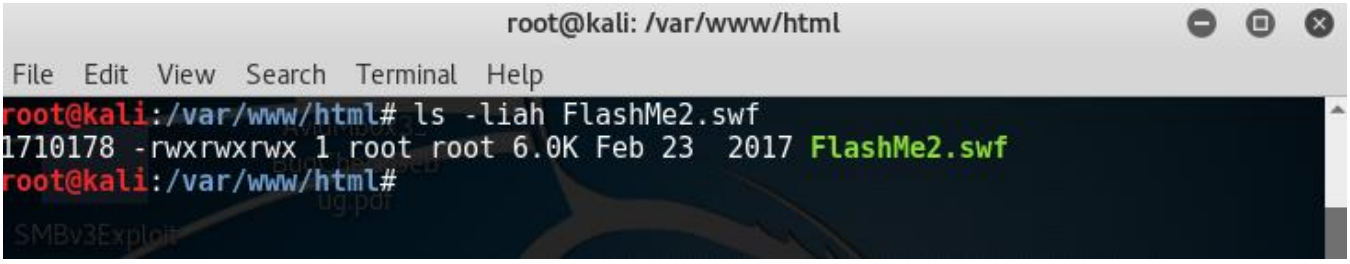
CVSS Score: AV: N/AC: L/AU: N/C:C/I: N/A:C

Proof-Of-Concept:

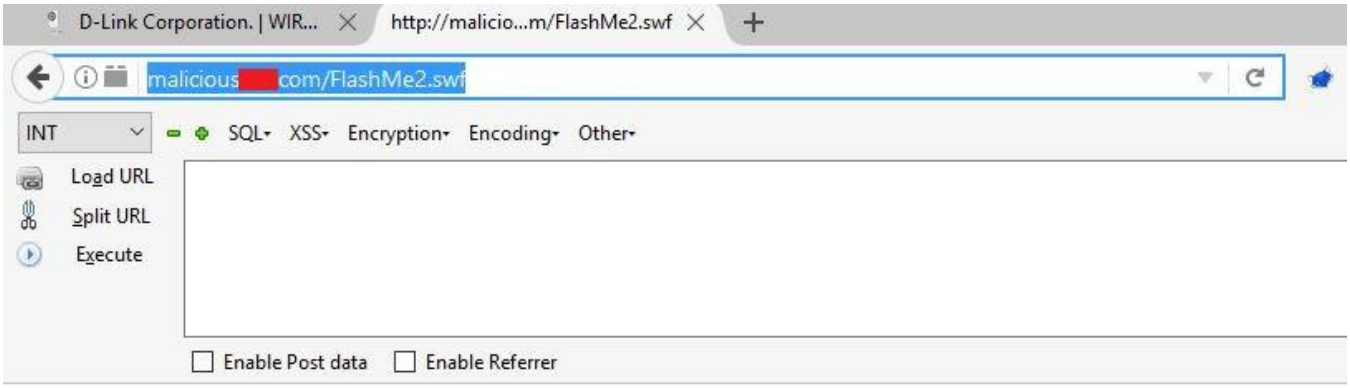
1. Build a Flash file using Flex SDK which would access Advance.htm from target device and send the response to attacker's site.



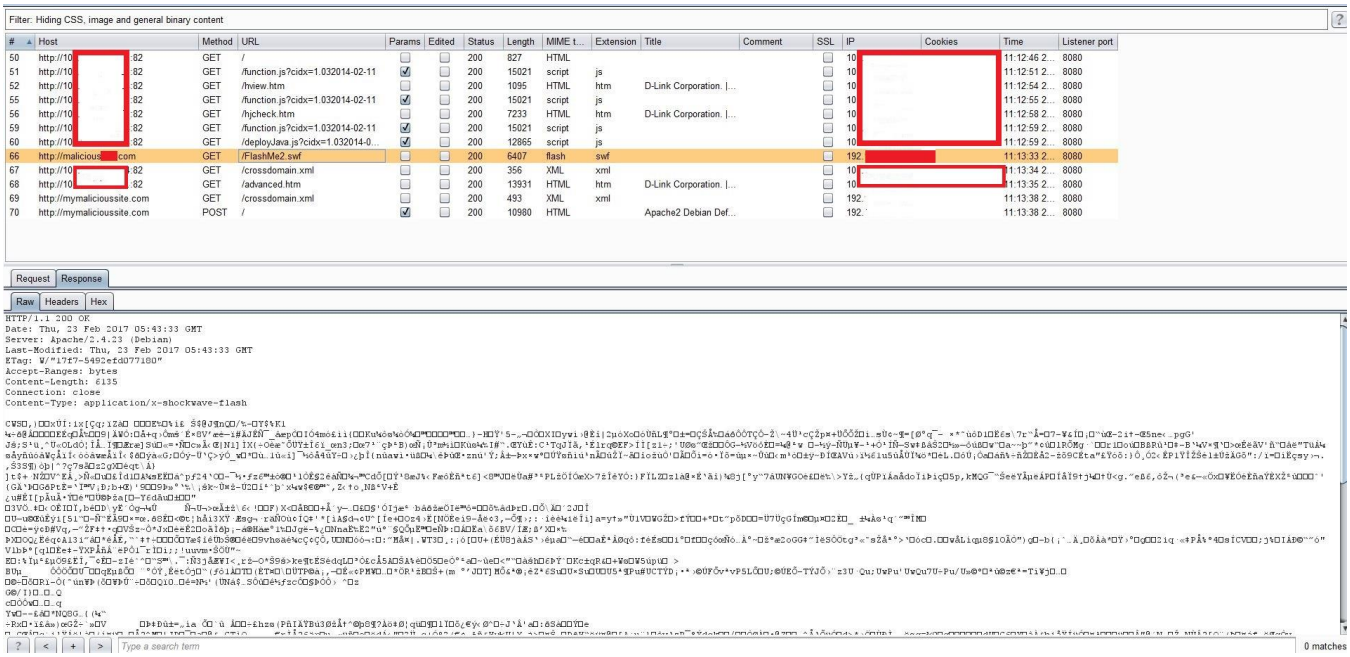
2. Download this file and copy it to the WebRoot of http://Maliciousxxxx.com



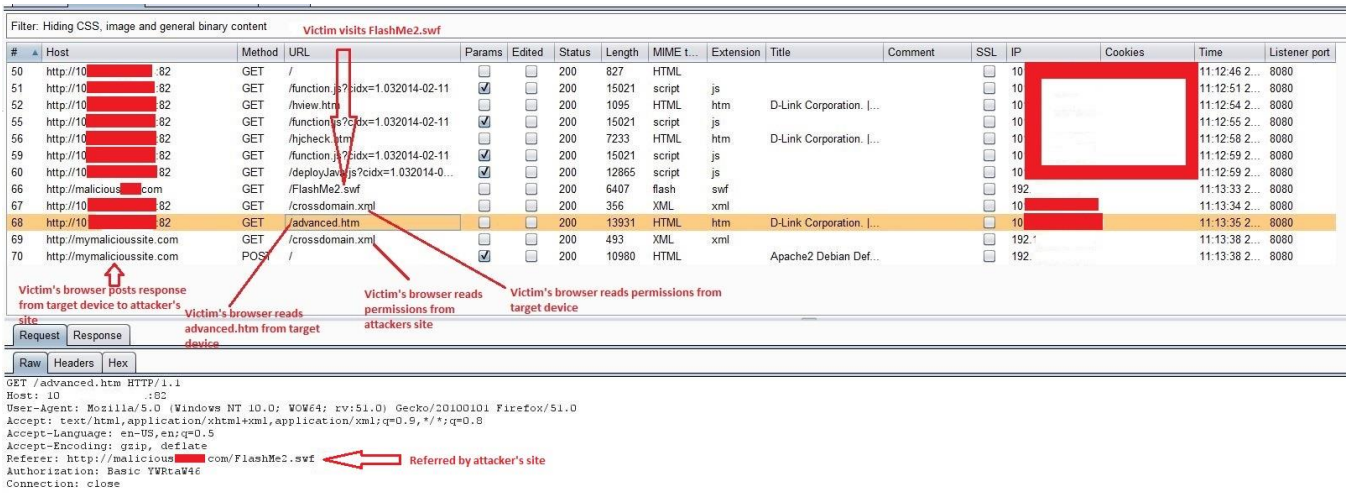
3. Log into the Camera's web admin console and then visit http://Maliciousxxxx.com/FlashMe2.swf



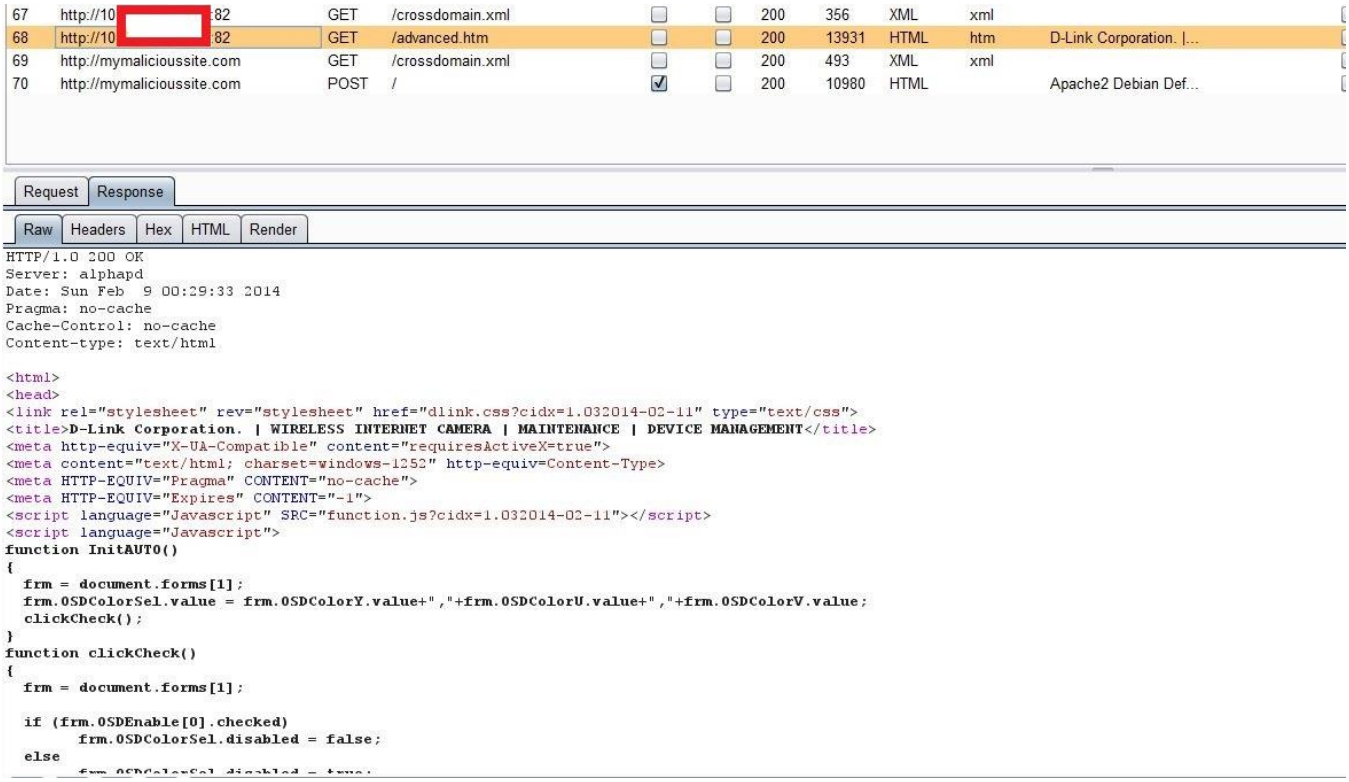
4. Response to above request



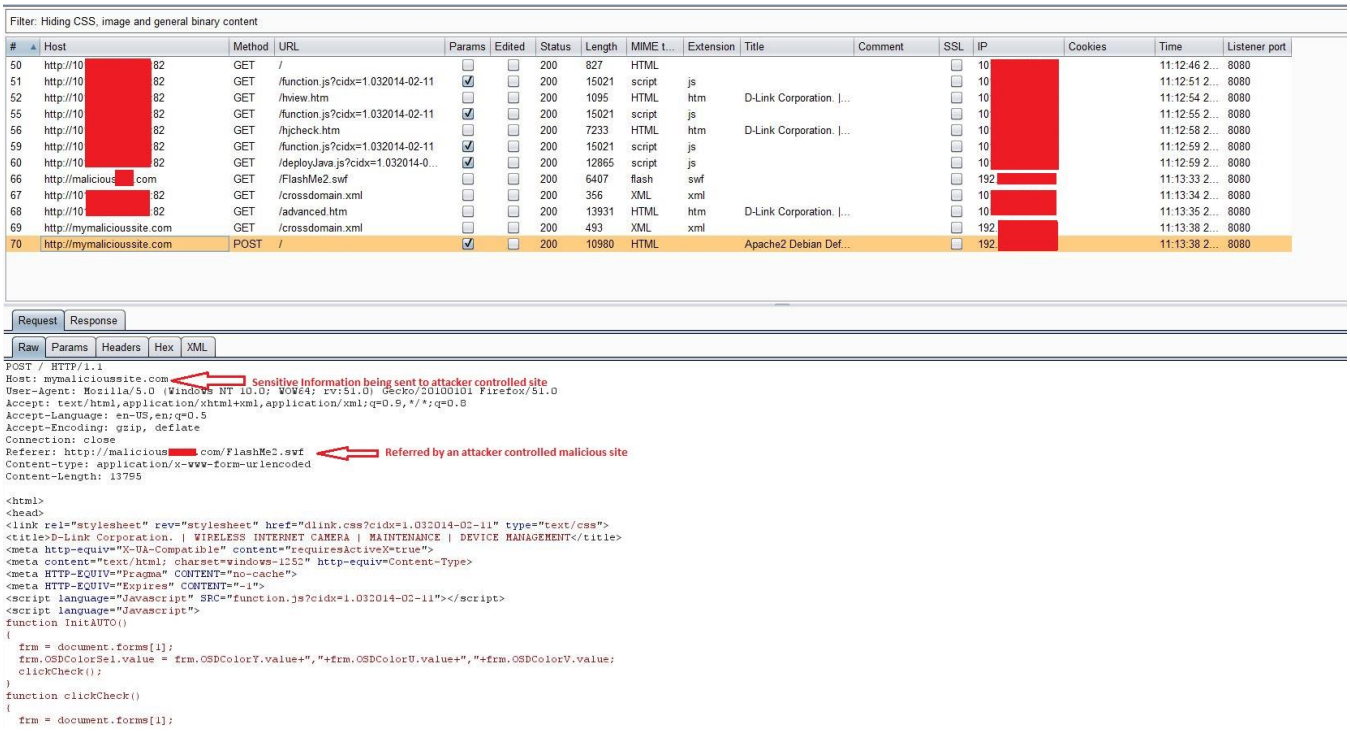
5. Flash object from Request#4 sends a GET request to http://CameraIP/advanced.htm



Response to this request:

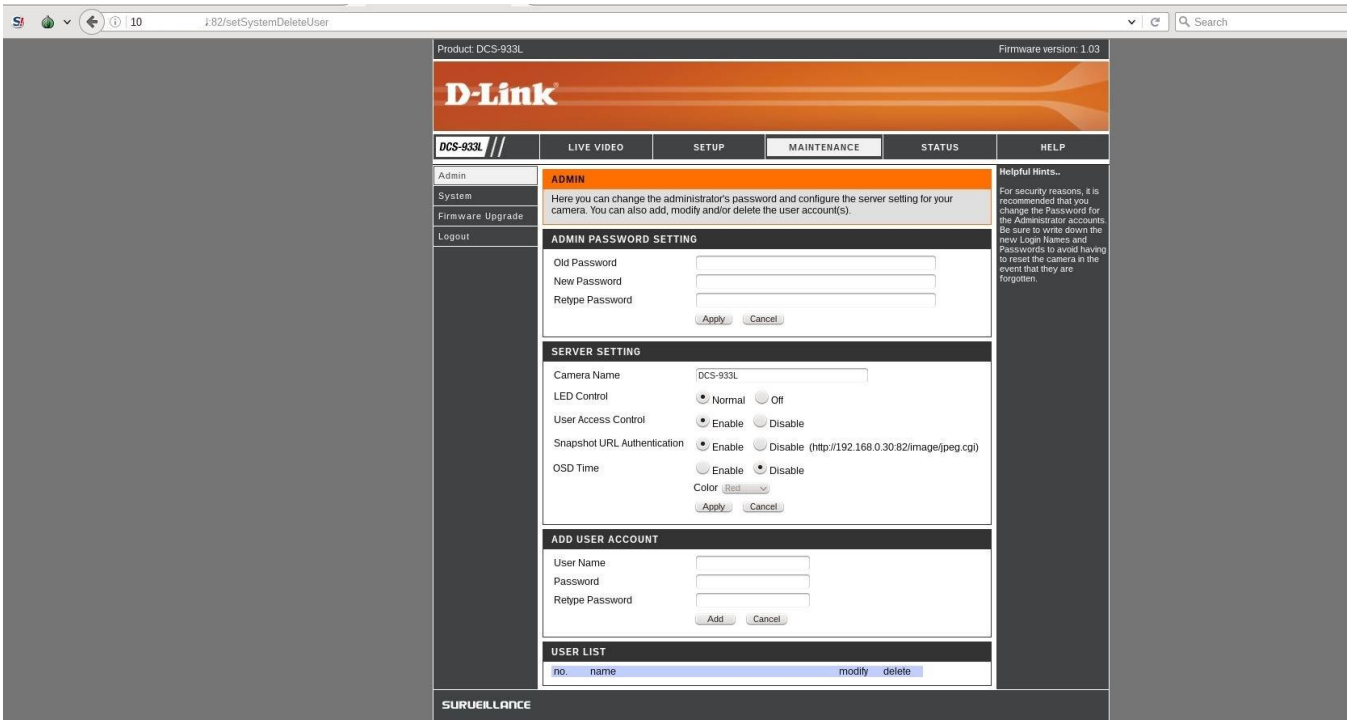


6. Flash object then sends above response that it received from the Camera to attacker's site

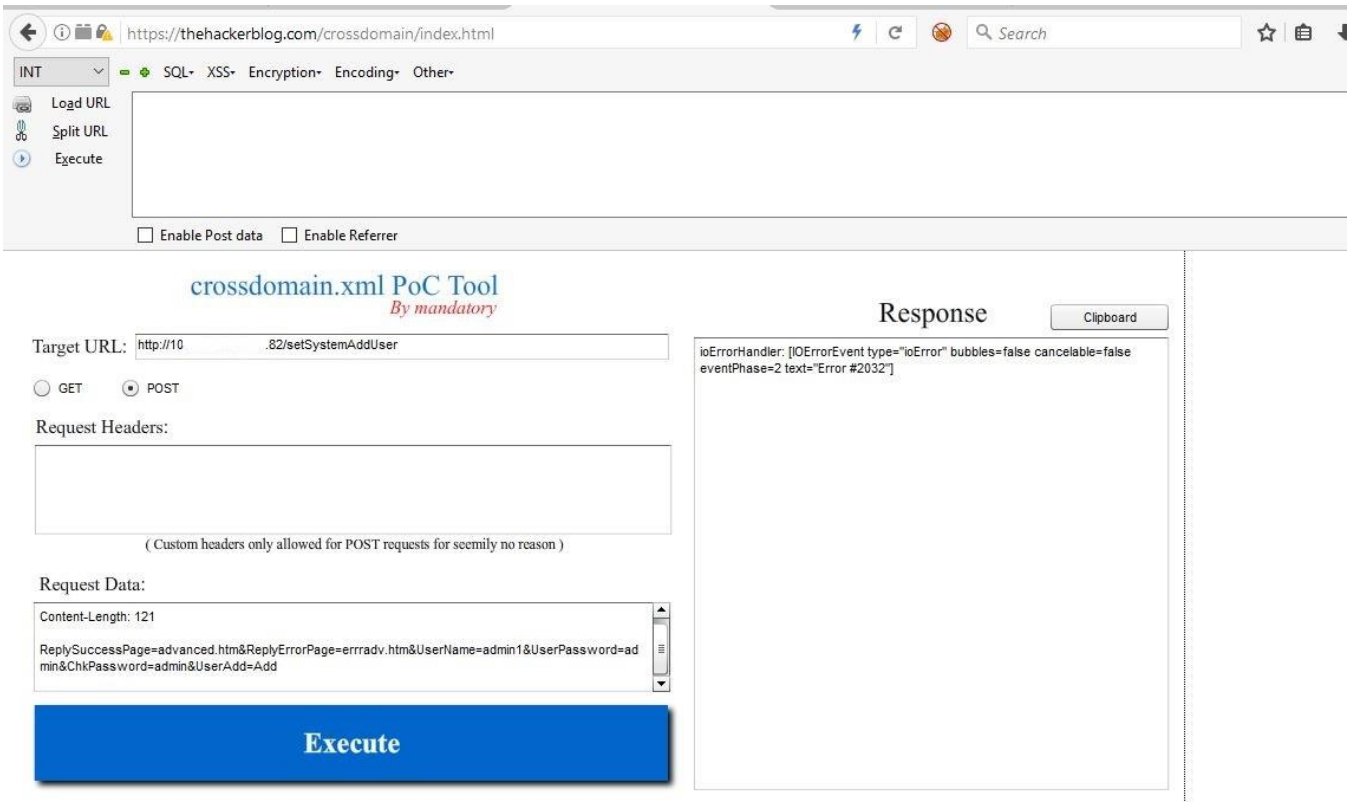


This way I could request other pages and retrieve sensitive information from the device like Live Video feed etc**. I could even add an admin user to the device and following are the screenshots for the same**. I used a publically available CrossDomain.XML Hacking Proof-of-Concept tool to do so.

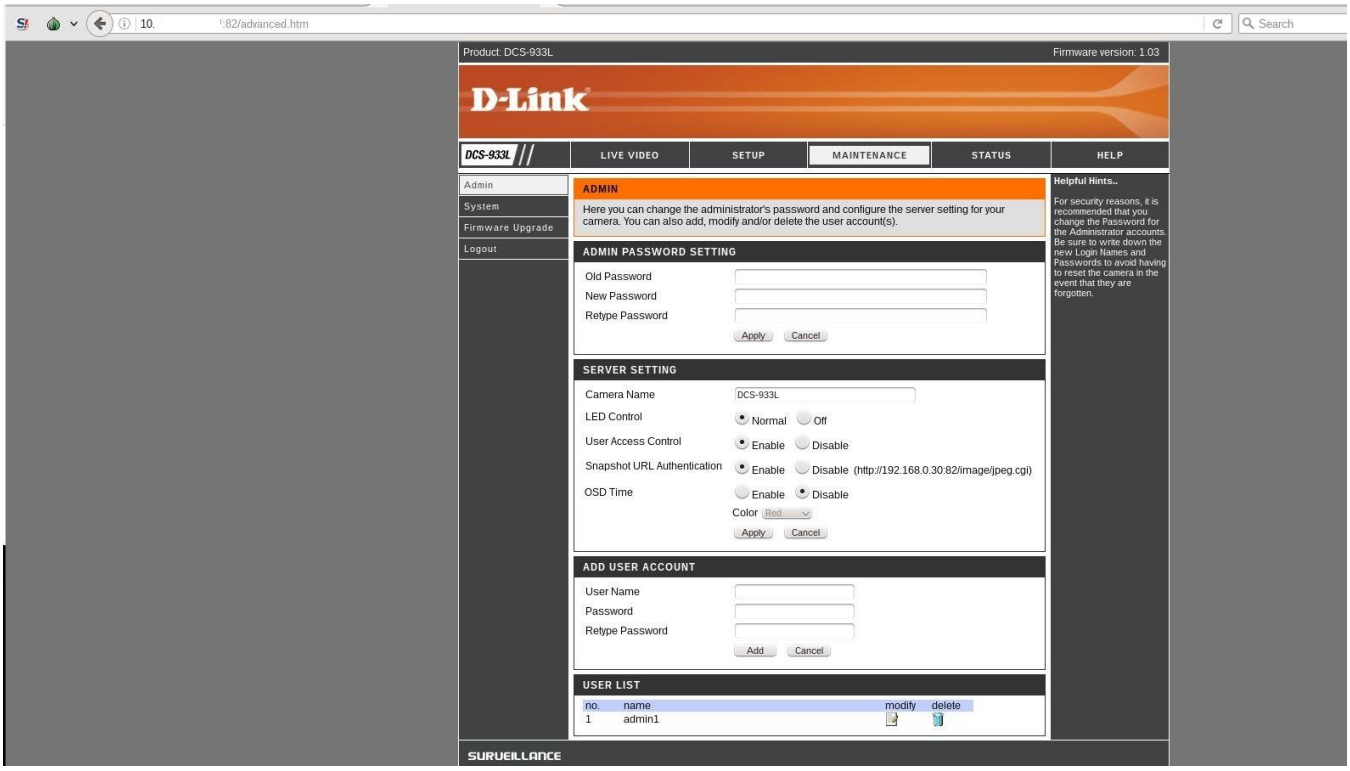
1. Following screenshots show there are no other users on the device at the moment:



2. Request to add user **admin1**:



3. User **admin1** added successfully:



Tracking Table:

D-Link Model	H/W version	FW version
DCS-2132L	B	v2.12.00
DCS-2330L	A	v1.13.00
DCS-2310L	B	v2.03.00
DCS-5029L	A	v1.12.00
DCS-5222L	B	v2.12.00
DCS-6212L	A	v1.00.12
DCS-7000L	A	v1.04.00
DCS-2132L	A	v1.08.01
DCS-2136L	A	v1.04.01
DCS-2210L	A	v1.03.01
DCS-2230L	A	v1.03.01
DCS-2310L	A	v1.08.01
DCS-2332L	A	v1.08.01
DCS-6010L	A	v1.15.01
DCS-7010L	A	v1.08.01
DCS-2530L	A	v1.00.21
DCS-930L	A	v1.15.04
DCS-930L	B	v2.13.15
DCS-932L	A	v1.13.04
DCS-932L	B	v2.13.15
DCS-934L	A	v1.04.15
DCS-942L	A	v1.27
DCS-942L	B	v2.11.03
DCS-931L	A	v1.13.05
DCS-933L	A	v1.13.05
DCS-5009L	A	v1.07.05
DCS-5010L	A	v1.13.05
DCS-5020L	A	v1.13.05
DCS-5000L	A	v1.02.02
DCS-5025L	A	v1.02.10
DCS-5030L	A	v1.01.06

Potential Mitigation per CWE:

Avoid using wildcards in the cross-domain policy file. Any domain matching the wildcard expression will be implicitly trusted, and can perform two-way interaction with the target server.

For Flash, modify crossdomain.xml to use meta-policy options such as 'master-only' or 'none' to reduce the possibility of an attacker planting extraneous cross-domain policy files on a server.

Adobe Recommendation: http://www.adobe.com/devnet/flashplayer/articles/cross_domain_policy.html

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**

LEGAL NOTICE: