Chrissy Morgan
@5w0rdfish

July 2020

Web Panel Testing: Directory Traversal – CVE-2017-7577

OWASP TOP 10: I5 Use of Insecure or Outdated Components

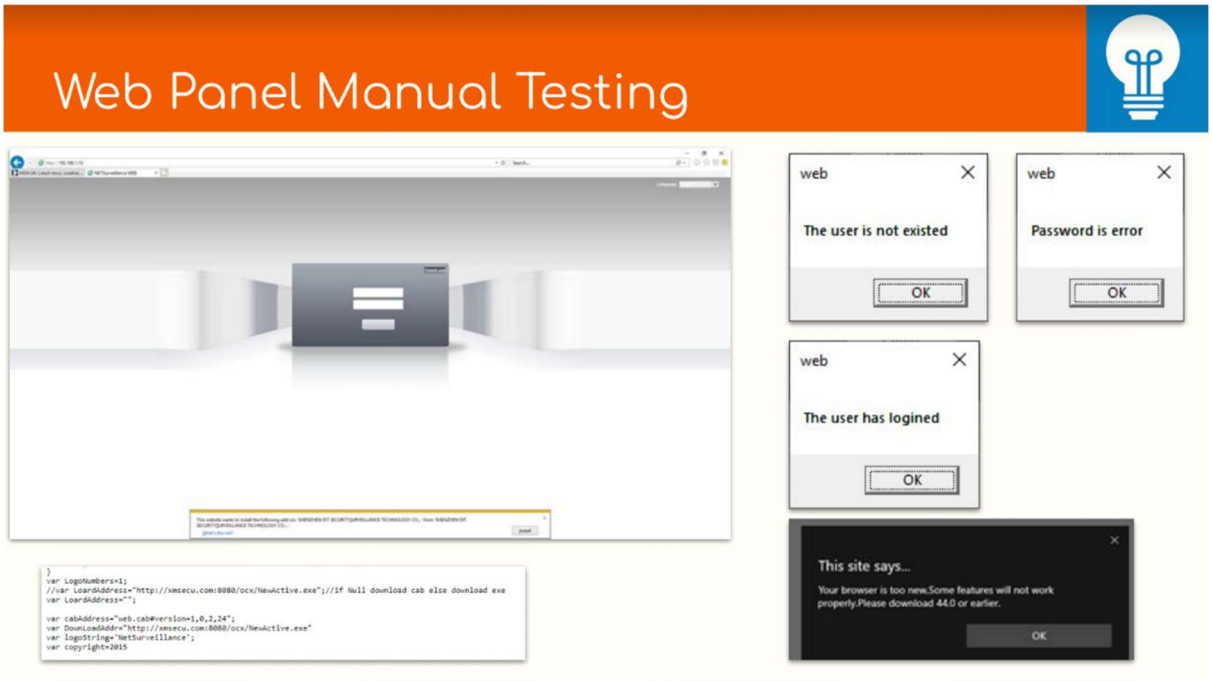
Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain

The DVR system used the UC-HTTPD Server which allows for CVE-2017-7577

Overview:

During web panel testing you may encounter the following pop up boxes when testing the web panel of the DVR system. It kindly tells us where we are going wrong. It asks for an installation of an Active-X plugin. This is not required to carry out testing. The web panel shown is a generic type seen on many DVR systems.

Testing has been undertaken using Firefox, although preference for the system will be internet explorer or outdated browsers.



Chrissy Morgan
@5w0rdfish

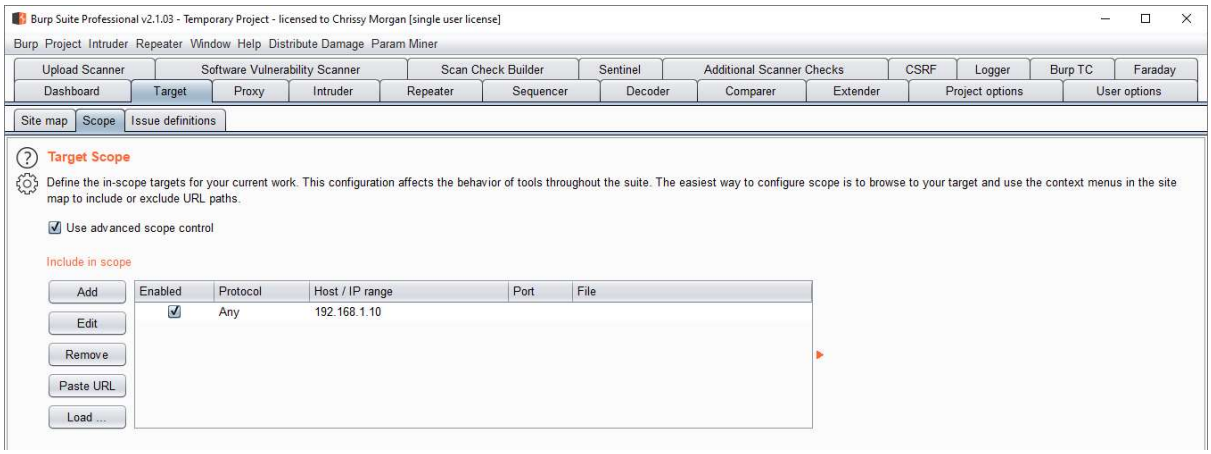
July 2020

Directory Traversal

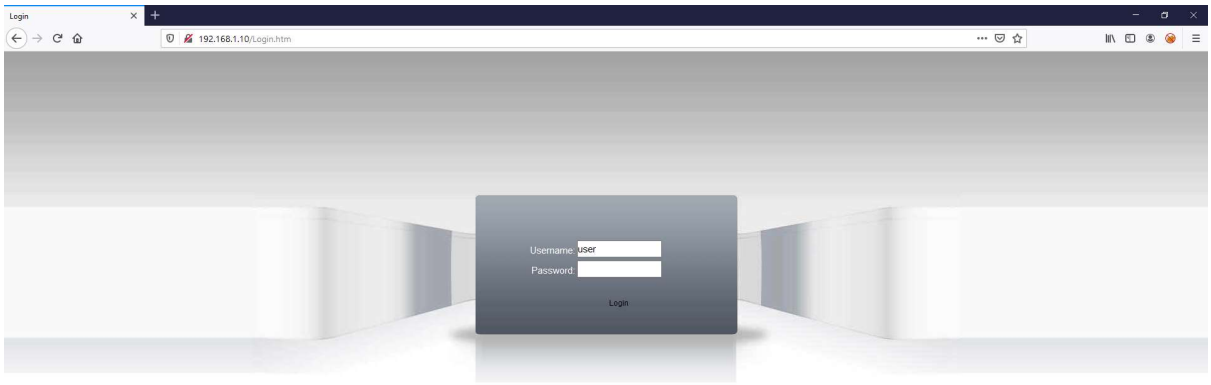
Using a directory traversal bug in the UC-http Server (uc-http1.0.0.0 CVE-2017-7577) I was able to get to the files on the CCTV box.

Process:

Set Burp Target scope

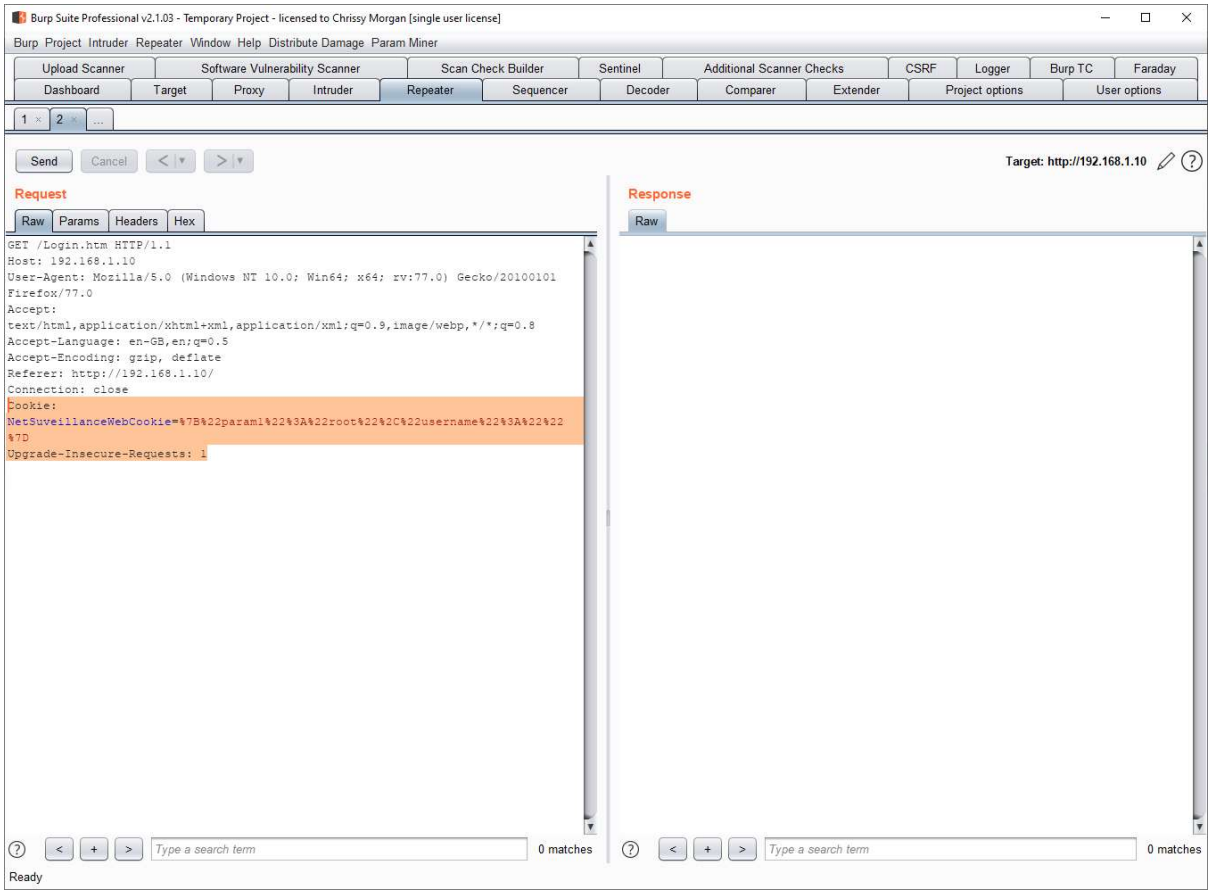


Visit 192.168.1.10 The web page to login it will look something like this

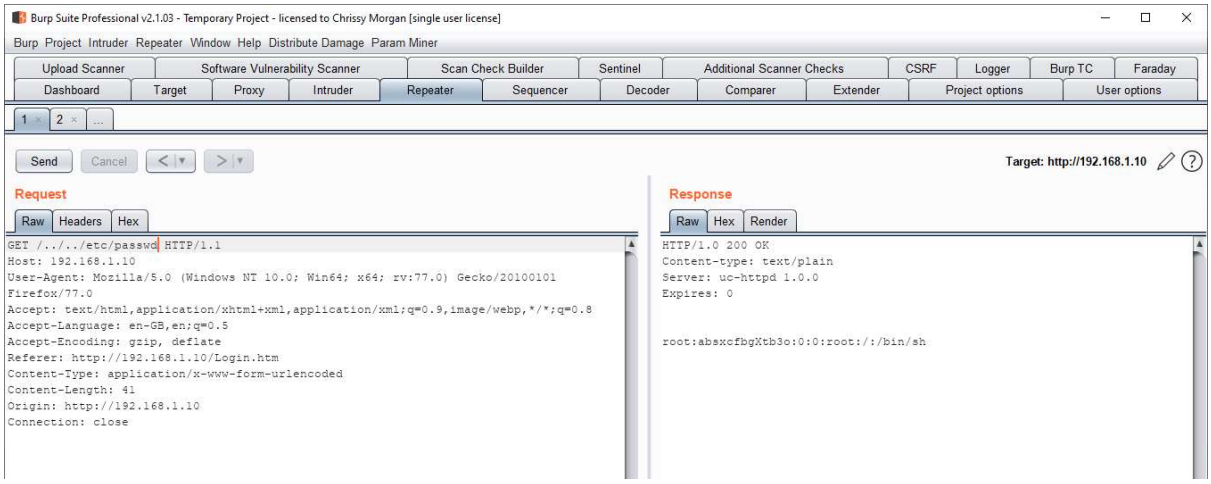


Once you have burp set up and running the web page may change, do not worry about this as the login prompts are not required at this time.

Send any request from the Proxy – HTTP History tab to Repeater. If you have selected the main login.htm page you must remove the cookie information highlighted below.



Change the request to GET /../../etc/passwd



This will give you the hashed root credentials which can now be cracked by using a tool like HashCat.