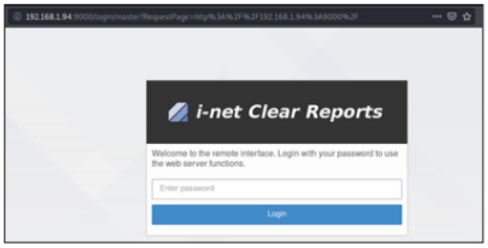
CVE-2020-28150

I-net – Clear Reports – Version 20.10.136 – Open Redirect.

The I-net Clear Reports web application accepts a user-controlled input that specifies a link to an external site, and uses the user supplied data in a redirect. This can aid an attacker when creating phishing attacks.

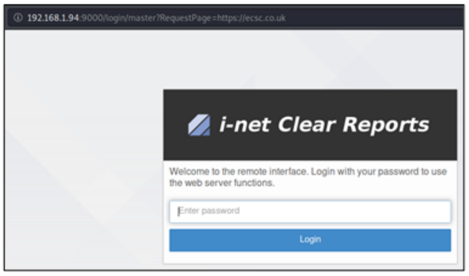
The latest version of Clear Reports with a default configuration was installed on the latest ubuntu release. When attempting to authenticate to the application using the master password the 'RequestPage' URL parameter was detected, this type of parameter Is commonly vulnerable to an open redirect; whereby a malicious attacker can utilise the legitimate application to redirect a user to a phishing page.


192.168.1.94:9000/login/master?RequestPage=http%3A%2F%2F192.168.1.94%3A9000%2F

Welcome to the remote interface. Login with your password to use the web server functions.

Normal use of the application with an unmodified URL.

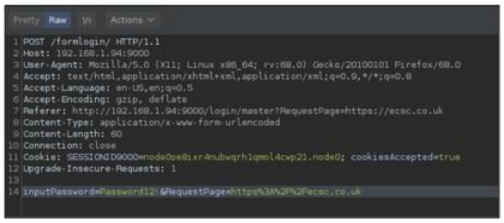
The above displays what would be expected pre-authentication, it is now possible to modify the value of the 'RequestPage' URL parameter to point to our malicious phishing page, in this case the https://ecsc.co.uk website is used for proof of concept.


192.168.1.94:9000/login/master?RequestPage=https://ecsc.co.uk

Welcome to the remote interface. Login with your password to use the web server functions.

The URL parameter has now been modified with the POC destination.

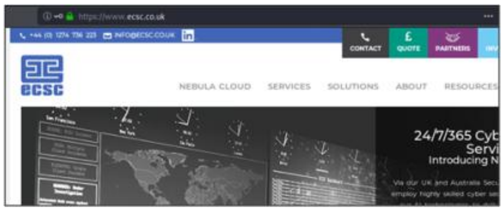
After modification (Figure 2) it is possible to see that no change has been made to the application, valid credentials are now sent to the application, creating the following request:



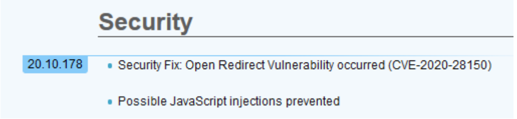
```
POST /formlogin/ HTTP/1.1
Host: 192.168.1.94:9000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.94:9000/login/master?RequestPage=https://ecsc.co.uk
Content-Type: application/x-www-form-urlencoded
Content-Length: 60
Connection: close
Cookie: SESSIONID9000=node0oe8ixr4nubwqrh1qmol4cwp21.node0; cookiesAccepted=true
Upgrade-Insecure-Requests: 1

inputPassword=Password12!&RequestPage=https%3A%2F%2Fecsc.co.uk
```

Burpsuite shows the request sent by the browser when authenticated.

Post authentication the application will now redirect the user to the target site specified within the application URL parameter, utilising the legitimate application URL for our phishing campaign.


https://www.ecsc.co.uk

Result of authenticating to the application with a modified URL parameter.



Security

20.10.178

- Security Fix: Open Redirect Vulnerability occurred (CVE-2020-28150)
- Possible JavaScript injections prevented

A fix has been implemented for this finding; https://www.inetsoftware.de/support/news/i-net-pdfc-new-release-20.10