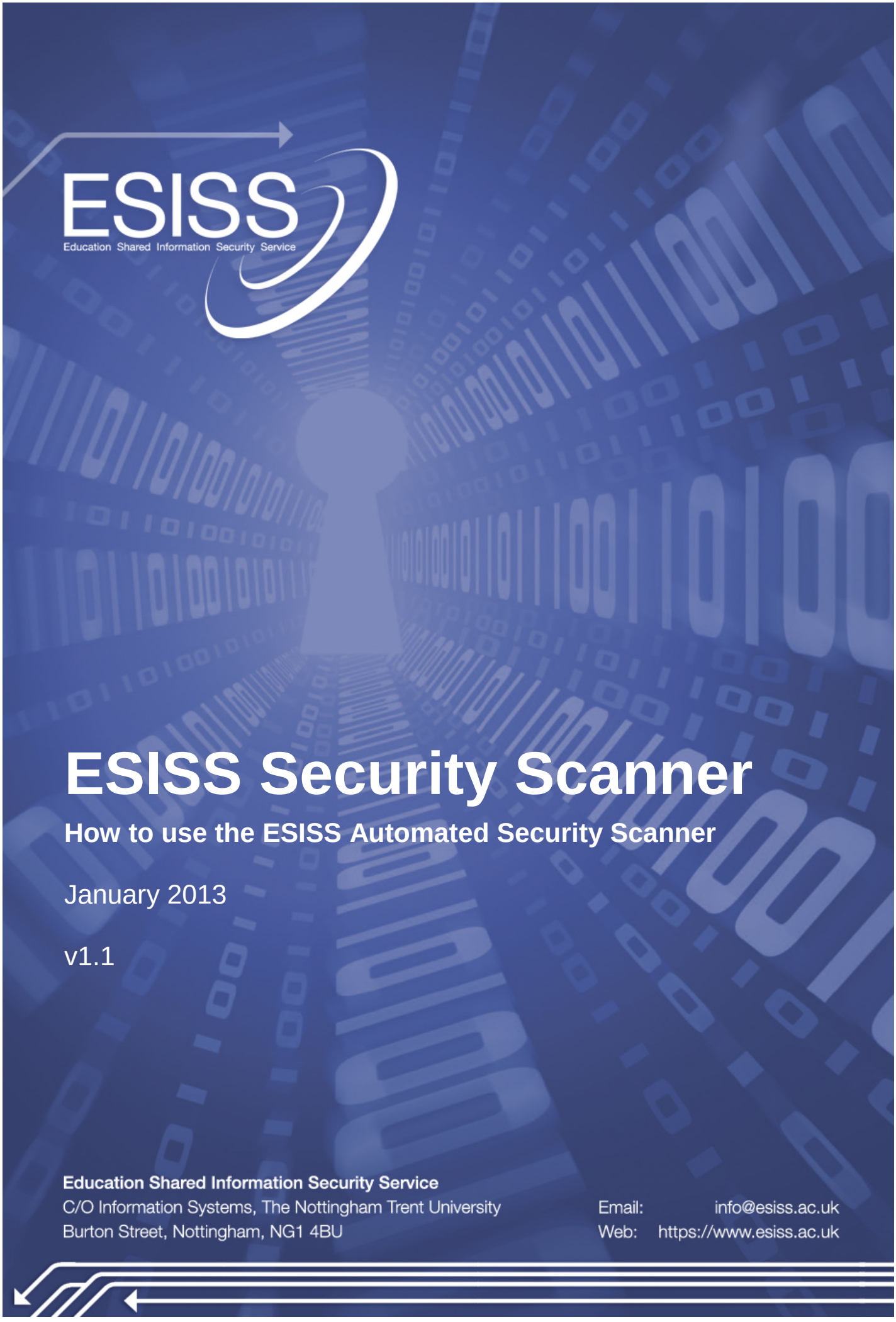


ESISS Security Scanner

How to use the ESISS Automated Security Scanner

January 2013

v1.1

Education Shared Information Security Service
C/O Information Systems, The Nottingham Trent University
Burton Street, Nottingham, NG1 4BU

Email: info@esiss.ac.uk
Web: https://www.esiss.ac.uk

Table of Contents

The ESISS Automated Security Scanner

The ESISS automated security scanner is provided in conjunction with Sec-1[1]. It allows institutions to externally scan servers, web services, IP address ranges or individual IP addresses from their institution for potential security problems.

The scanner features the following:

- **Administration**
  - Single platform to manage application and infrastructure security risks;
  - Flexible scheduling of scans including the ability to pause and resume scans;
  - Provides flexible filtering on either end systems or vulnerability title;
  - Download custom filtered reports in HTML, Docx or CSV format.

- **Infrastructure tests**, which consist of:
  - Port scan against the host to check open ports/service types;
  - AMAP probe of open ports found by the port scan;
  - DNS digging for information about the host/netblock;
  - Vulnerability tests against the open ports discovered. These are aimed at finding common security problems and are “safe” checks so as to not cause undue problems with the hosts being checked.

- **Web Application tests**, which consist of:
  - Each defined website is crawled to map site/application content;
  - A forced browsing scan is performed to test for common issues found in the OWASP top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project), eg email address harvesting, browsable dirs, writeable dirs through to SQL injection, XSS, etc;
  - Checks to identify weak administration interfaces.

These webform submission checks which are part of the web application testing may cause a significant amount of form email to be generated depending on the configuration of the web applications being tested.

Note: All scans will originate from the IP address 62.69.82.10. Janet CSIRT is aware of this IP address being used by ESISS and should not contact you about any potential threat.

[1] http://www.sec-1/com

Using The ESISS Security Scanner

1. Logging On

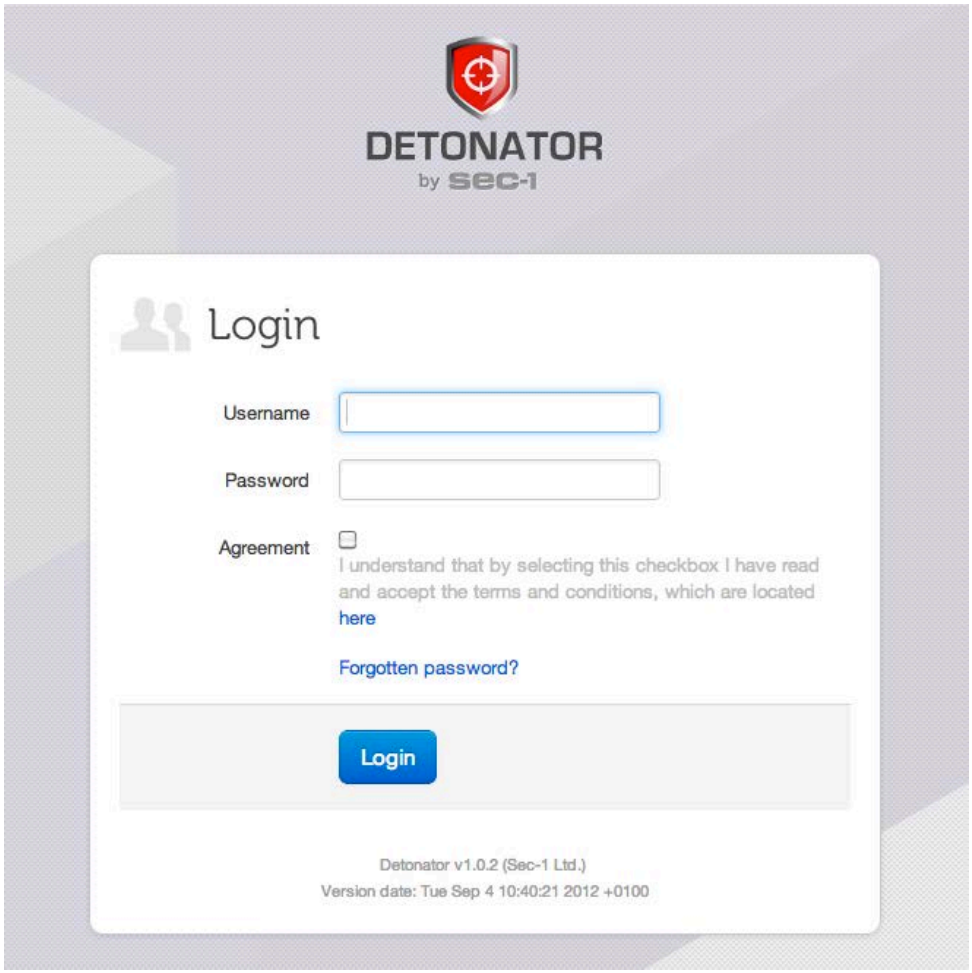
The scanner can be accessed at the following URL:

https://scanner.sec-1.com/

You will need to have had a company definition and user account created by a member of the ESISS team (email info@esiss.ac.uk with any ammendments to your initial connection or if you have any problems with this).

Note: Your logon username is your email address.

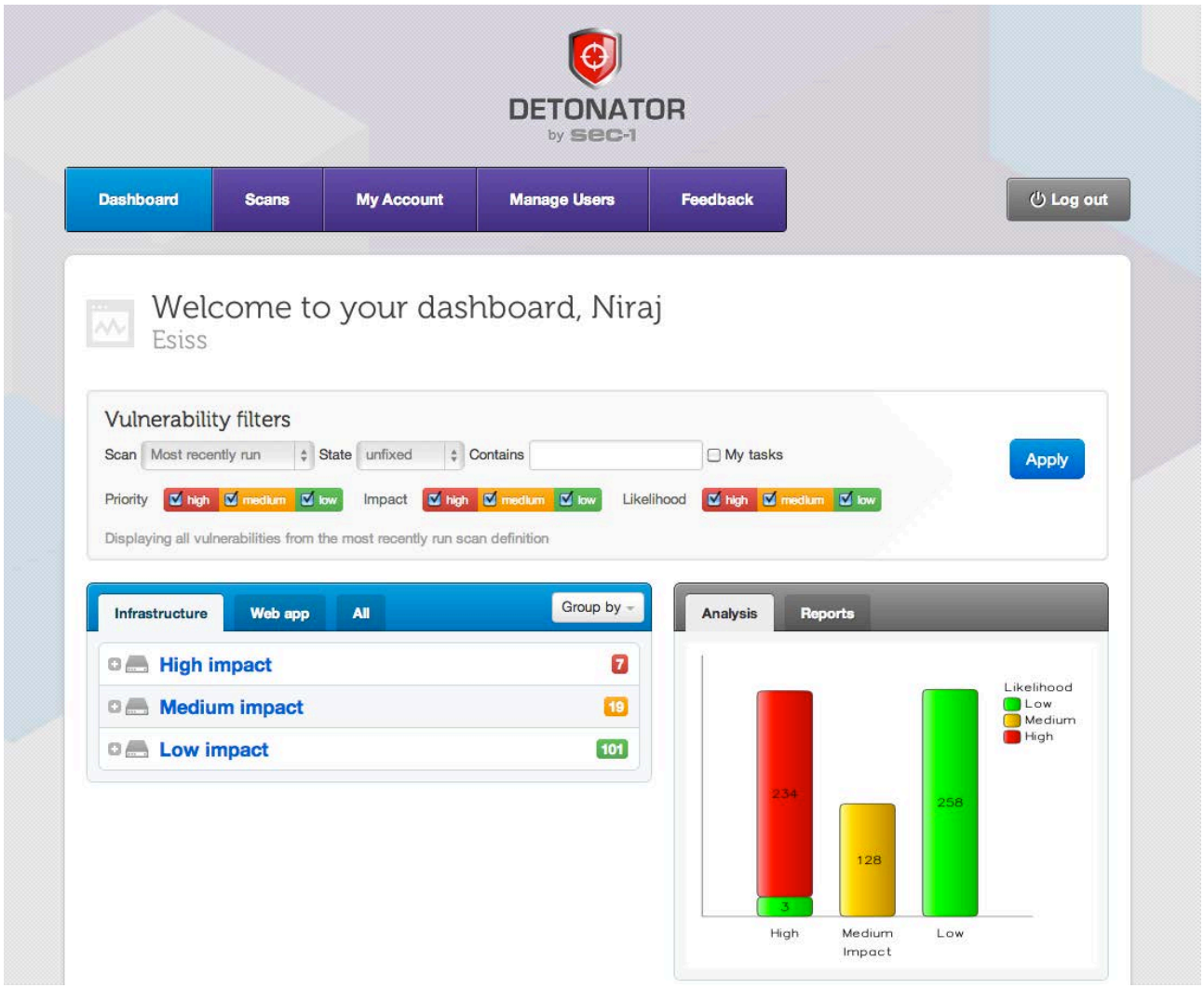
The Logon screen:



2. The Dashboard Screen

After logging on, you will presented with the **dashboard** screen, as shown below. This provides you with a summary of the results for the last completed scan, split by the type of scan (infrastructure or web app). Filters can also be applied based on keywords and/or priority, impact or likelihood of the discovered vulnerabilities. You have the ability to download a report of the completed scan in both Word (docx) or csv format and the ability to review old scans.

Dashboard Screen:

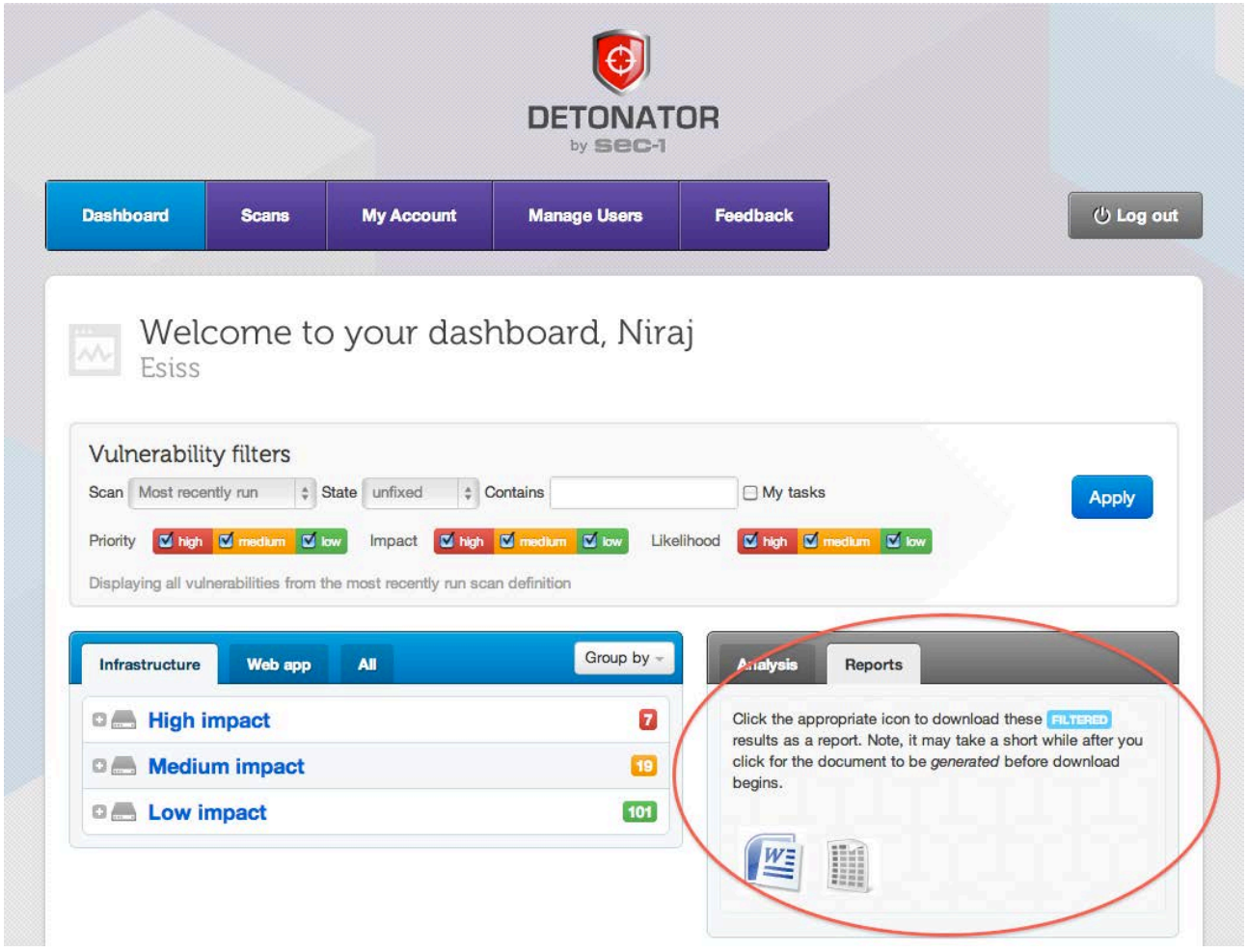


Accessing Reports:

In order to download the report for the last completed scan, you need to click on the **Reports** tab in the right hand frame. This then shows a Word (docx) and a csv of the results.

Note: these are subject to any filters you may have applied to the results.

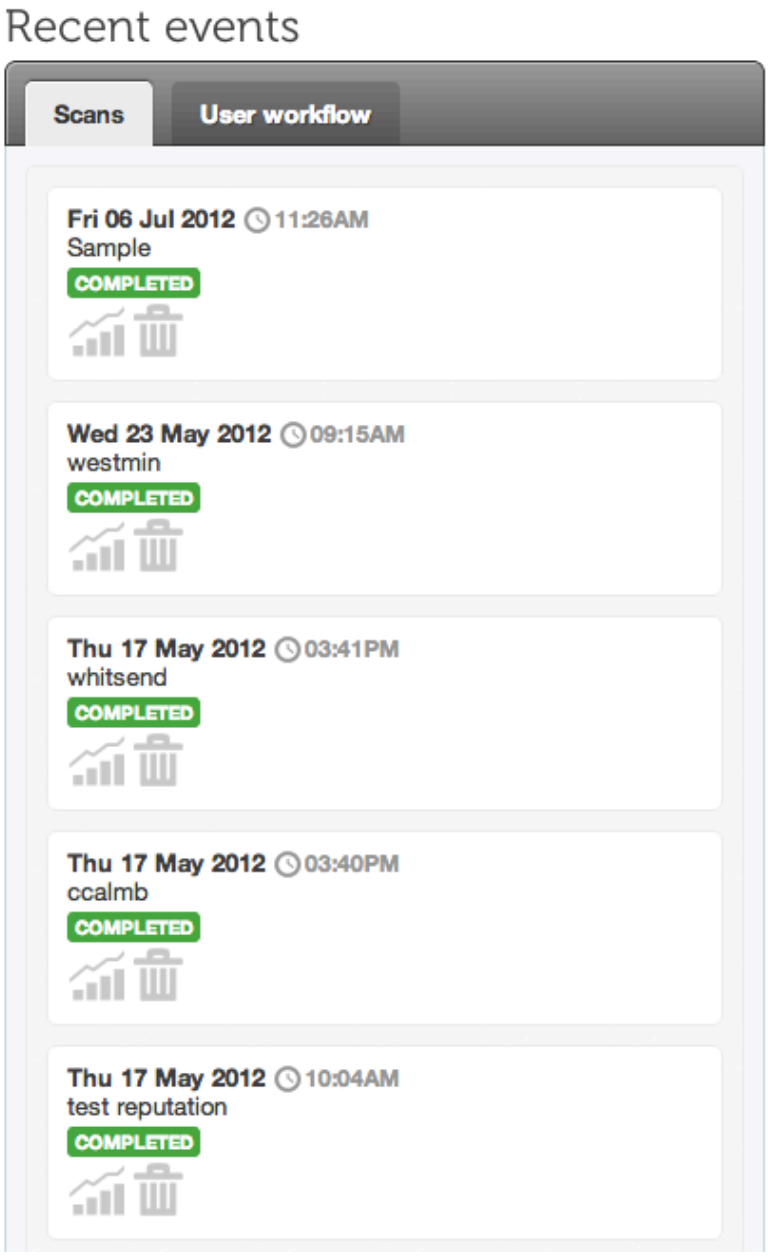
Report Screen:



Recent Events:

The Recent Events box in the bottom right of the dashboard screen shows a list of recent scans carried out. Clicking on the bar graph icon shows the results for that scan in the dashboard and the bin icon will delete the scan results.

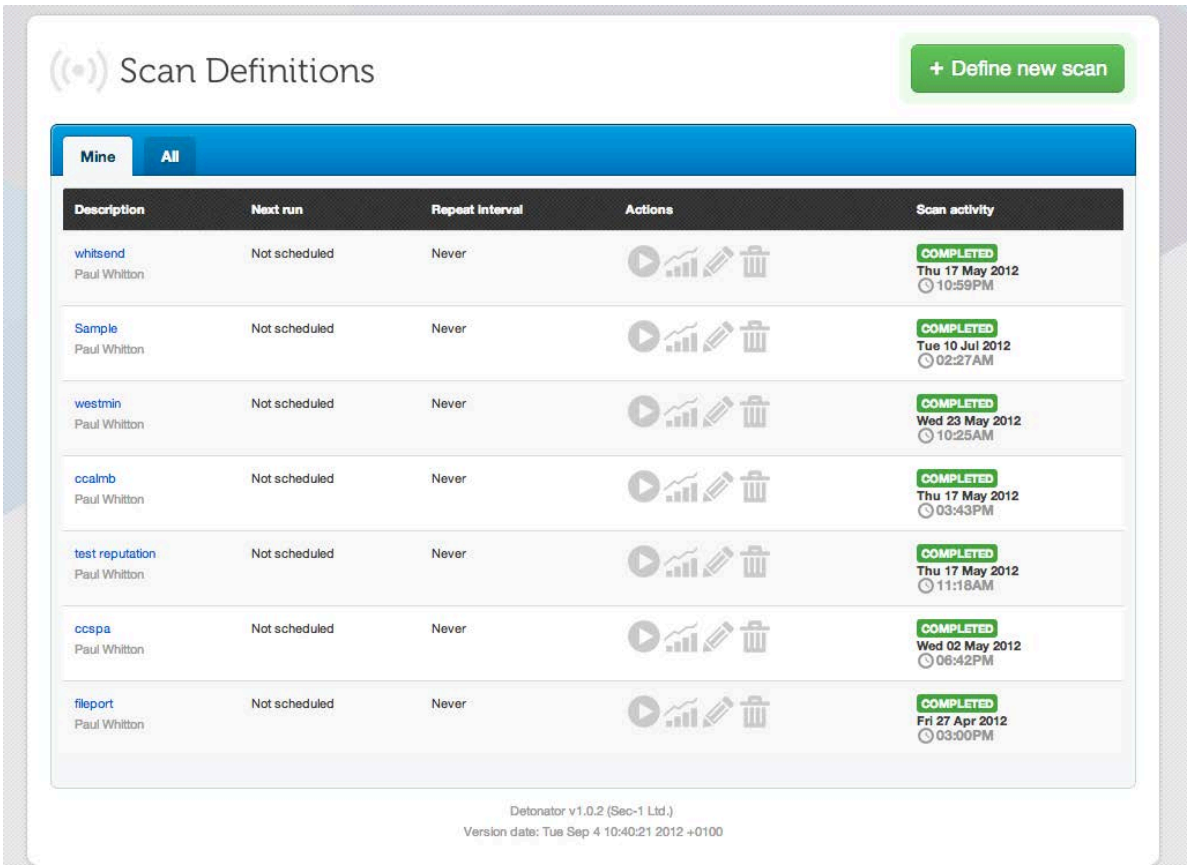
Recent Events:



3. Scans

Clicking the **Scans** tab along the top menu shows all currently defined scans that have been setup, and allows you to create new scans. You are also able to view scans carried out by other members of your organisation by clicking the **All** tab next to the **Mine** tab.

Scans screen:



Scans can be controlled by the following actions:

 This button starts the scan immediately;

 This button shows the latest results for the scan;

 This button edits the scan settings;

 This button deletes the scan.

Defining a new Scan.

Under the scan menu, clicking on "**+ Define new scan**" takes you to the scan definition screen. This allows you to specify the type of test to carry out:

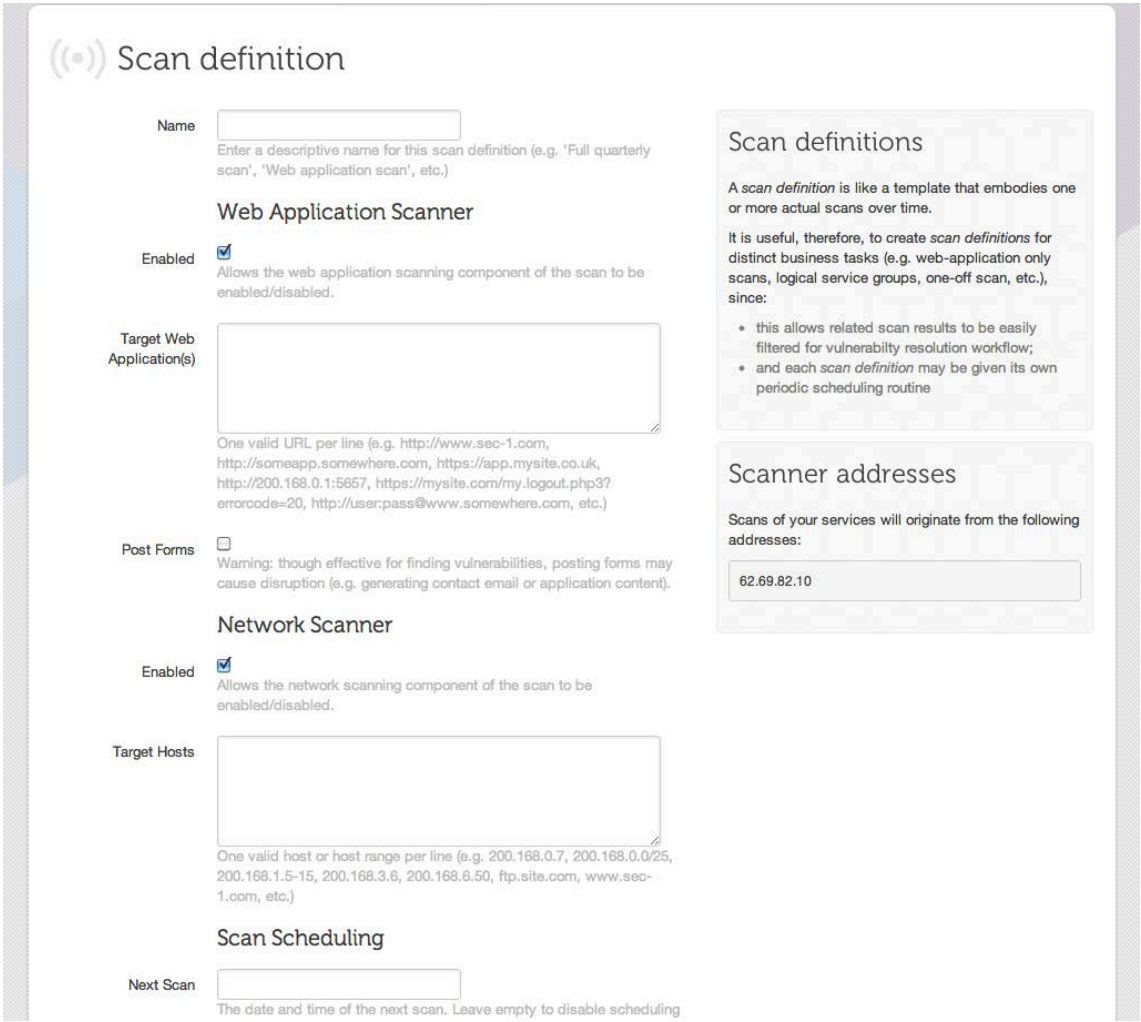
- Web Application Scanner;
- Network Infrastructure Scanner;
- Both.

For Web Application scanning, provide the URLs that you require to be scanned and choose whether to post forms during the web application testing.

For the Network Infrastructure Scanner, select an IP address or a range of IP addresses.

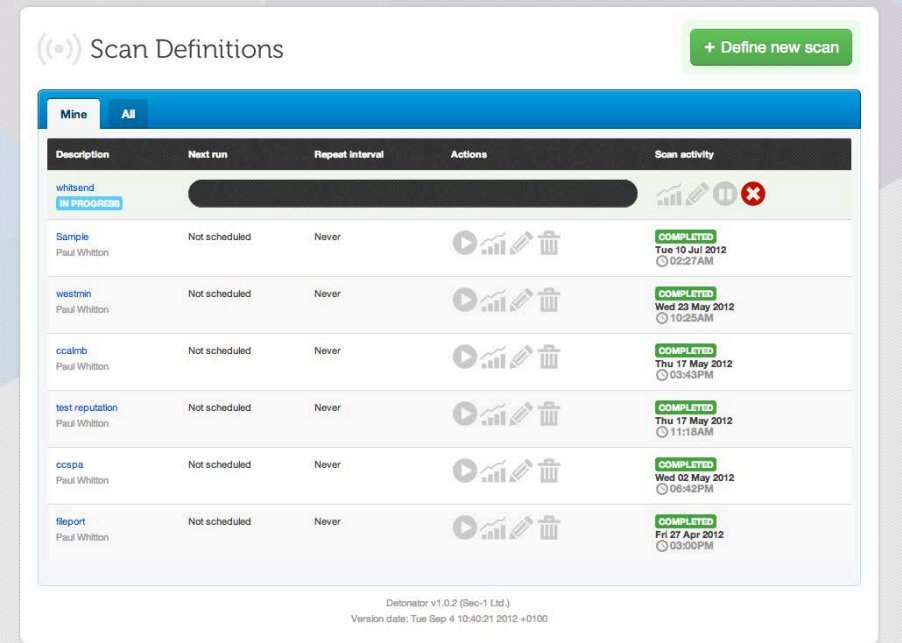
Finally, set the time and date for when you would like the scan to run and whether you wish the scan to repeat and at what intervals.

Scan definition:

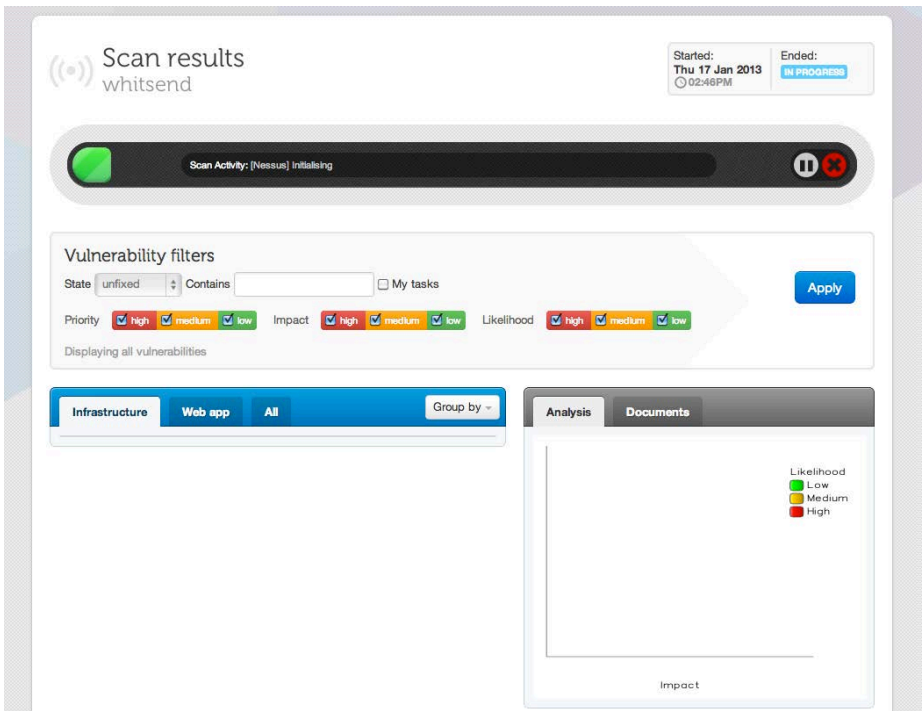


Live scan results:

If a scan is in progress, on the scan screen you will see a black progress bar and icons to cancel and pause the scan as shown below:

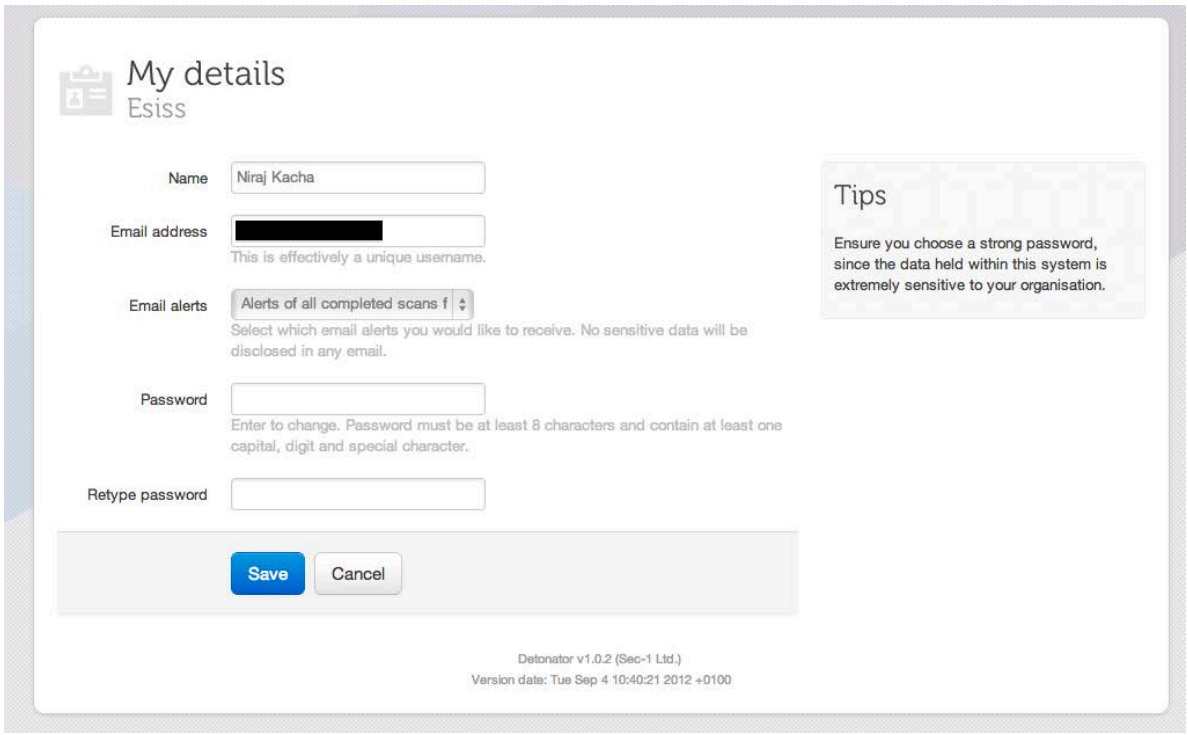


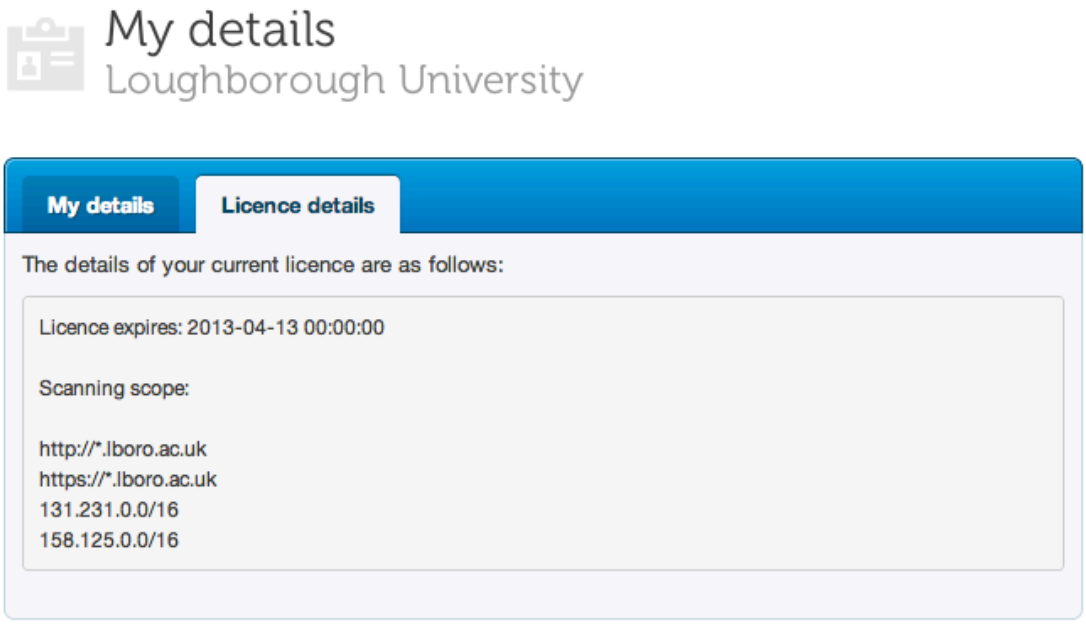
Clicking on the black bar takes you to the scan results screen. This is the same as the dashboard screen, apart from having the live progress of the scan shown by the black bar as can be seen below:



4. My Account

Clicking the **My Account** tab along the top menu allows you to update your details and change the way you get alerted via email about scans. You can also see the licence applied to your account of what you are allowed to scan, as shown below:





5. Manage Users

Clicking the **Manage Users** tab along the top menu shows the current users within your organisation and allows you to add new users if you licence allows. This can be seen below: