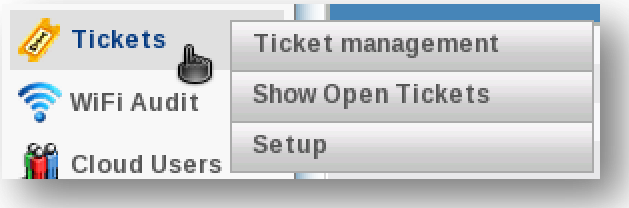
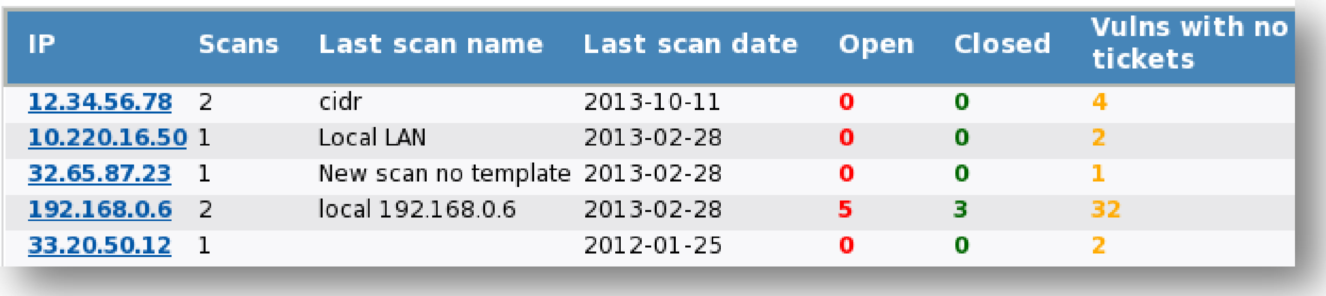
# Vulnerability Scanning Help Desk Ticket System

## - Ticket Management

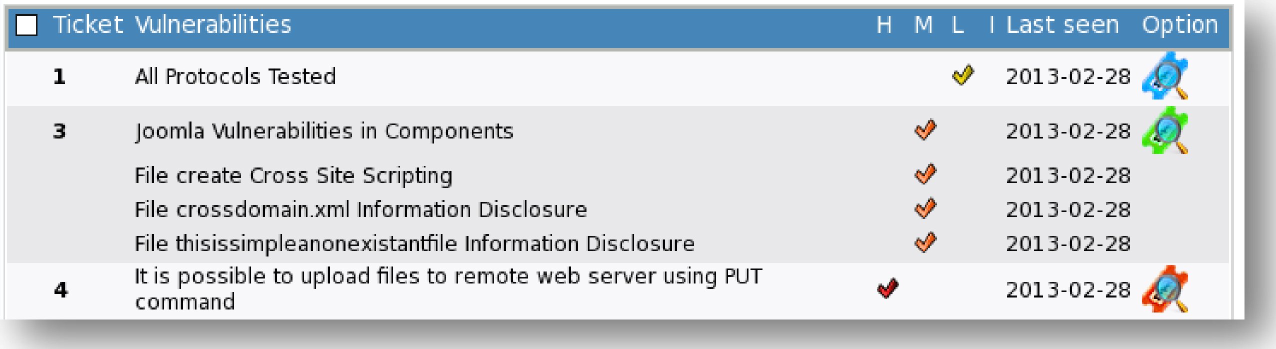


Ticket Management is a new subsystem designed to manage the process of solution of vulnerabilities.
It allows a user to create new tickets based on the vulnerabilities found during a scan, assign them to a person, define a priority, a delivery date etc. The functions are available through the new menu Tickets.



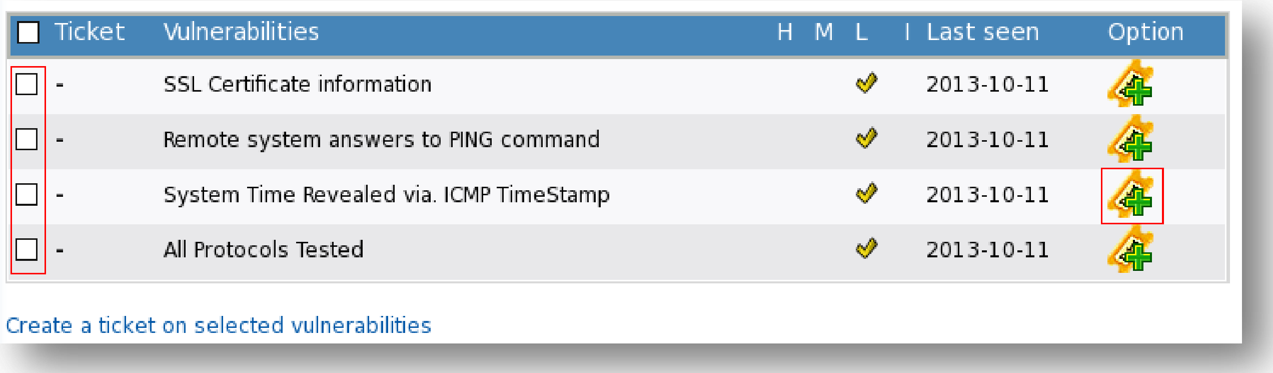
| IP | Scans | Last scan name | Last scan date | Open | Closed | Vulns with no tickets |
|---|---|---|---|---|---|---|
| 12.34.56.78 | 2 | cidr | 2013-10-11 | 0 | 0 | 4 |
| 10.220.16.50 | 1 | Local LAN | 2013-02-28 | 0 | 0 | 2 |
| 32.65.87.23 | 1 | New scan no template | 2013-02-28 | 0 | 0 | 1 |
| 192.168.0.6 | 2 | local 192.168.0.6 | 2013-02-28 | 5 | 3 | 32 |
| 33.20.50.12 | 1 | | 2012-01-25 | 0 | 0 | 2 |

The main list provides a view by IP. It shows a summary of open and closed tickets for each IP and the number of vulnerabilities with no associated tickets. Clicking on the IP, a new list appears, with a detail of the status of tickets for that IP.
The list shows all vulnerabilities associated to a ticket, the risk level of each vulnerability,



| □ Ticket | Vulnerabilities | H | M | L | I | Last seen | Option |
|---|---|---|---|---|---|---|---|
| 1 | All Protocols Tested | | | ✓ | | 2013-02-28 | |
| 3 | Joomla Vulnerabilities in Components | | ✓ | | | 2013-02-28 | |
| | File create Cross Site Scripting | | ✓ | | | 2013-02-28 | |
| | File crossdomain.xml Information Disclosure | | ✓ | | | 2013-02-28 | |
| | File thisissimpleanonexistantfile Information Disclosure | | ✓ | | | 2013-02-28 | |
| 4 | It is possible to upload files to remote web server using PUT command | ✓ | | | | 2013-02-28 | |

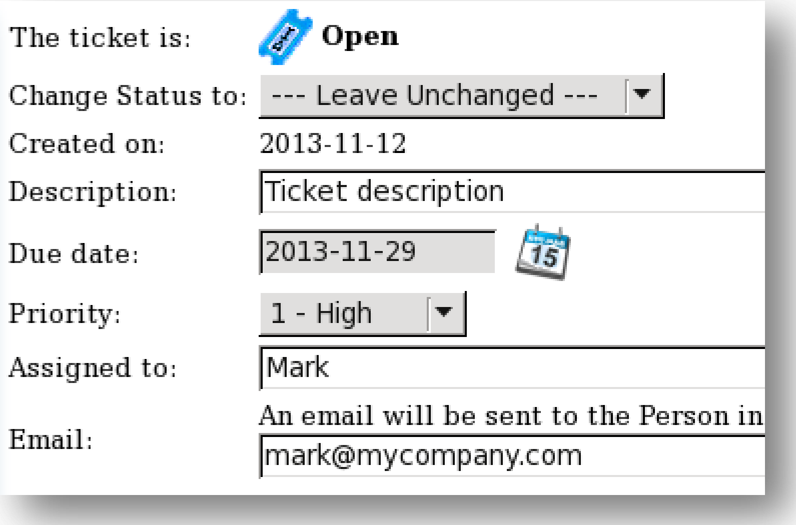
the date when the vulnerability has been seen last time, and the status of the ticket.
If a vulnerability is not associated to any ticket, it will appear as in the following picture and it will be possible to create a new ticket on a single vulnerability (the icon on the right) or on multiple vulnerabilities at once (the check boxes on the left).



| □ | Ticket | Vulnerabilities | H | M | L | I | Last seen | Option |
|---|---|---|---|---|---|---|---|---|
| □ | - | SSL Certificate information | | | ✓ | | 2013-10-11 | ✚ |
| □ | - | Remote system answers to PING command | | | ✓ | | 2013-10-11 | ✚ |
| □ | - | System Time Revealed via. ICMP TimeStamp | | | ✓ | | 2013-10-11 | ✚ |
| □ | - | All Protocols Tested | | | ✓ | | 2013-10-11 | ✚ |

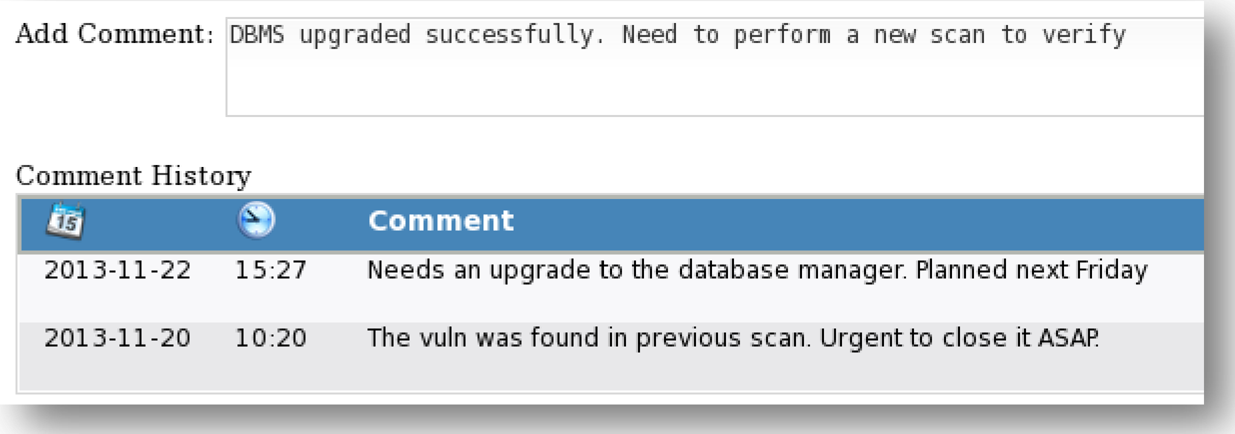
Another list, available through the main menu, shows the full list of open tickets, ordered by due date.

In the Edit page, that appears when a ticket is created or edited, it's possible to enter a due date, a priority and assign it to a person. It's also possible to enter one or more email addresses that will receive automatic notifications when the ticket status changes or is automatically closed by the Penetrator.



| | |
|---|---|
| The ticket is: | Open |
| Change Status to: | --- Leave Unchanged --- |
| Created on: | 2013-11-12 |
| Description: | Ticket description |
| Due date: | 2013-11-29 |
| Priority: | 1 - High |
| Assigned to: | Mark |
| Email: | An email will be sent to the Person in<br>mark@mycompany.com |

In the Edit page it's possible to enter one or more comments, that will be added to the ticket to track its solution history. Comments will be then displayed in a list, as shown in next picture.



Add Comment: DBMS upgraded successfully. Need to perform a new scan to verify

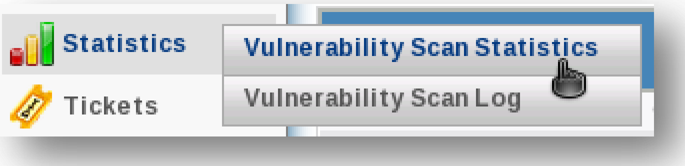
Comment History

| 📅 | 🕒 | Comment |
|---|---|---|
| 2013-11-22 | 15:27 | Needs an upgrade to the database manager. Planned next Friday |
| 2013-11-20 | 10:20 | The vuln was found in previous scan. Urgent to close it ASAP. |

A new Setup function allows to select some parameters useful to automate some processes, such as:

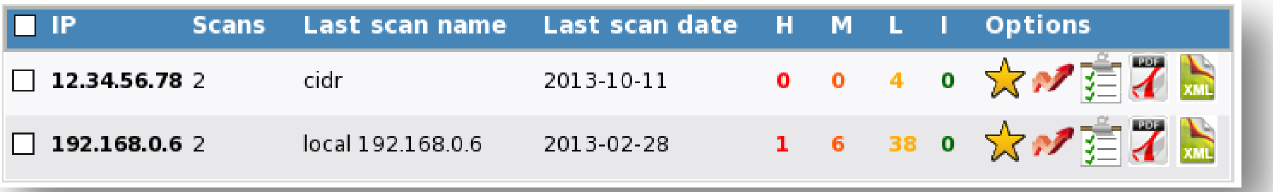
- Automatically closing a ticket when the vulnerability does not appear in a new scan
- Automatically closing a ticket when a vulnerability is marked as False Positive
- Sending an email when a ticket status changes or when the ticket is next to the due date.

## - Statistics



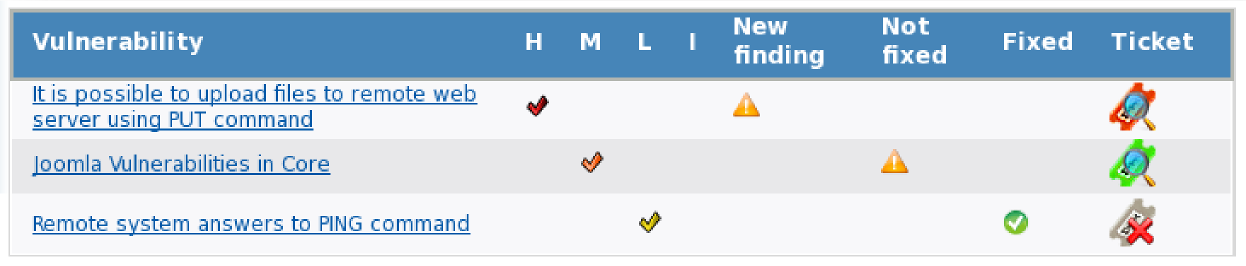
The new Statistics menu includes the old Statistics and History functions. This function has undergone a total redesign and now allows to keep under control the trend of vulnerabilities a scan after another.

The main list shows all IPs audited at least twice, the number of vulnerabilities of each type, and gives the option to make a deeper analysis on the IP. The first option ★ shows the current status of vulnerabilities on the IP. The second one ↗ shows the trend of



| □ IP | Scans | Last scan name | Last scan date | H | M | L | I | Options |
|---|---|---|---|---|---|---|---|---|
| □ **12.34.56.78** | 2 | cidr | 2013-10-11 | 0 | 0 | 4 | 0 | ★ ↗ 📋 PDF XML |
| □ **192.168.0.6** | 2 | local 192.168.0.6 | 2013-02-28 | 1 | 6 | 38 | 0 | ★ ↗ 📋 PDF XML |

vulnerabilities, giving an overview of the number of vulnerabilities found on each scan and the number of new findings, besides fixed and not fixed. Then it gives the same overview with a bar chart at the bottom of the same page.



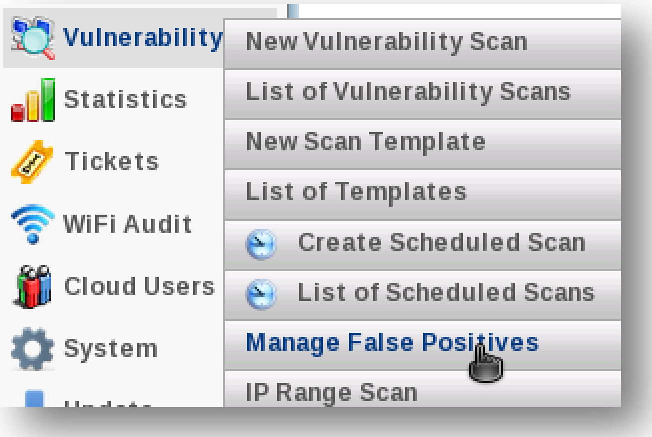
| Vulnerability | H | M | L | I | New finding | Not fixed | Fixed | Ticket |
|---|---|---|---|---|---|---|---|---|
| It is possible to upload files to remote web server using PUT command | ✓ |  |  |  | ⚠ |  |  |  |
| Joomla Vulnerabilities in Core |  | ✓ |  |  |  | ⚠ |  |  |
| Remote system answers to PING command |  |  | ✓ |  |  |  | ✓ |  |

From here, we can click on the scan and see the detail of vulnerabilities for it (see picture above). This list, when shown for the last scan performed, is the same list shown by Current Status ☆. It also gives a direct link to the tickets, if a ticket has ever been open on that vulnerability.

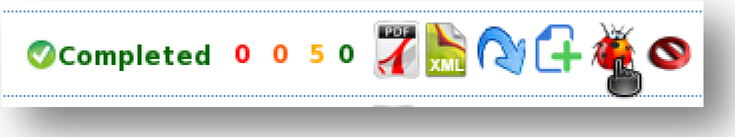
Last option available on the main list shows the complete list of vulnerabilities ever found on an IP and the date of last scan when each vulnerability has been detected. The list is similar to the one above and has a direct link to tickets.

## - Global False Positives

The False Positives function allows to whitelist a vulnerability for an IP. The new Global False Positives function, instead, allows to whitelist a vulnerability independently on the IP where it has been found. A vulnerability added to the Global False Positives will be ignored by the Penetrator on every scan performed by the same user on any IP.

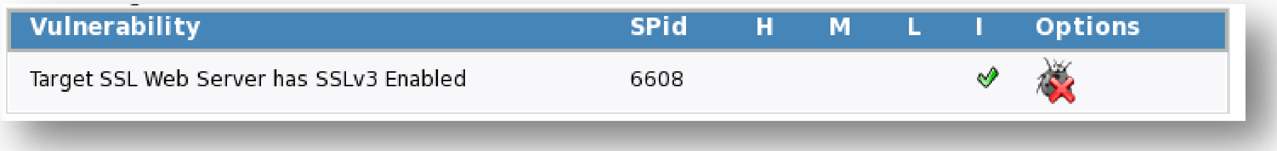


The function is available through the main window to add/delete false positives for a scan or through the menu, to have a complete overview over IP-based and Global False Positives. The page available



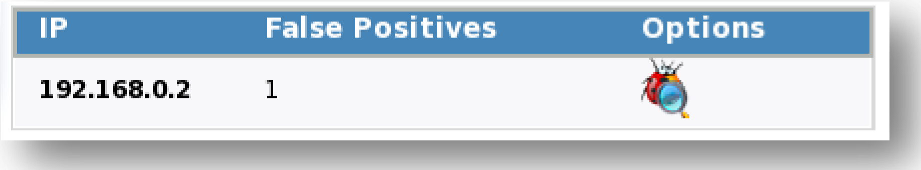
through the menu shows the full list of Global False Positives and a list of IPs for which IP-based False Positives have been added.

The list of Global False Positives appears as in the picture below, and for each vulnerability shows the risk level and allows to delete it from the list. When you delete a vulnerability from the list of Global False positives, IP-based False Positives will not be affected.



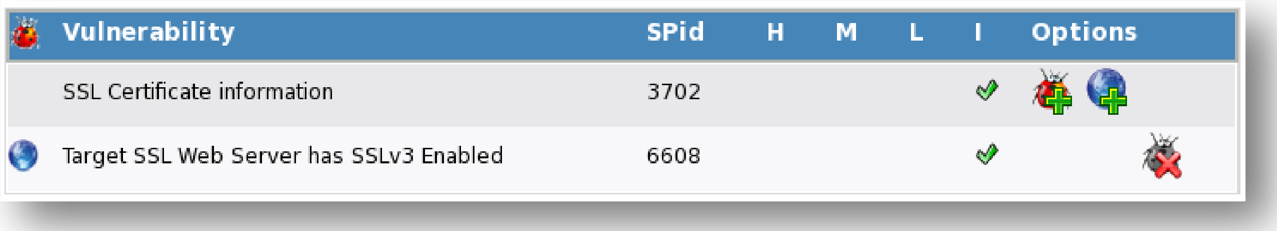
| Vulnerability | SPid | H | M | L | I | Options |
|---|---|---|---|---|---|---|
| Target SSL Web Server has SSLv3 Enabled | 6608 | | | | ✓ | ✗ |

The second list in this page shows the IP-based False Positives and allows to view the list of vulnerabilities that can be added or deleted to False Positives.



| IP | False Positives | Options |
|---|---|---|
| 192.168.0.2 | 1 | |

The link available in the main window shows the following list, where a vulnerability can be added or removed from the IP-based or Global False Positives.



| | Vulnerability | SPid | H | M | L | I | Options |
|---|---|---|---|---|---|---|---|
| | SSL Certificate information | 3702 | | | | ✓ | + + |
| | Target SSL Web Server has SSLv3 Enabled | 6608 | | | | ✓ | ✗ |