
Seccubus

Scan more, work less...



SCHUBERG PHILIS



I had a wish...

I wish I could scan my
infrastructures for
vulnerabilities every
month/week/day...



Image: Golden Genie, a Creative Commons Attribution Non-Commercial No-Derivative-Works (2.0) image from phototacular's photostream

SCHUBERG PHILIS

I wish...

...I could use all my regular
tools...



SCHUBERG PHILIS

I wish...

...it wouldn't take too much
time...



SCHUBERG PHILIS

I wish...

...I wouldn't have to get up
too early to do it...



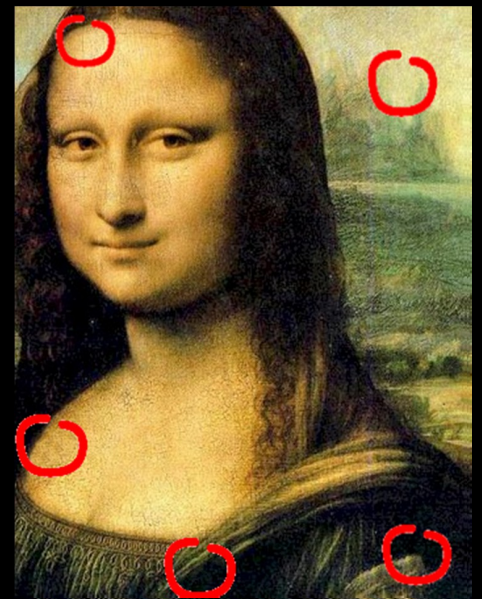
SCHUBERG PHILIS

I wish...



Week 1

It would be worth the effort
Spot the differences...



Week 2

SCHUBERG PHILIS

It calls for some automation...



SCHUBERG PHILIS

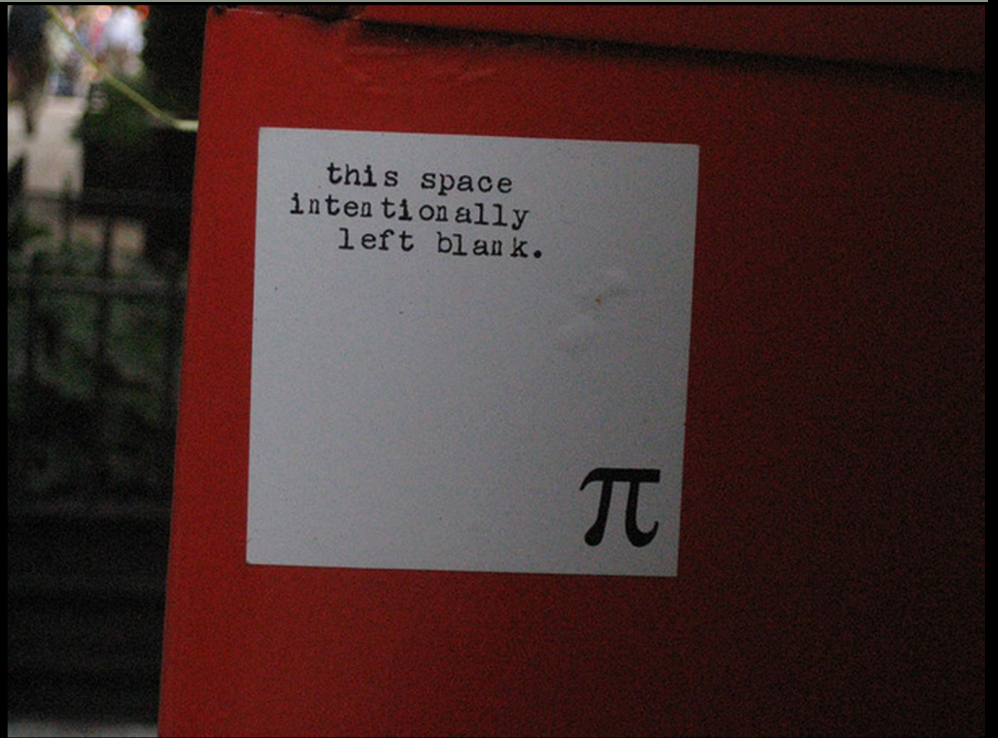
You wish has been granted



SCHUBERG PHILIS

7 maart 2012

Scan



SCHUBERG PHILIS

Compare



SCHUBERG PHILIS

Assign status

Automatically assigned:

- » New
- » Changed
- » Gone

SCHUBERG PHILIS

Assess

The screenshot displays the Seccubus web interface for automated vulnerability scanning. The top navigation bar includes tabs for Status, Runs, Findings, Manage Workspaces, and Manage Scans. The main content area is titled 'Show findings with this status:' and features a filter bar with dropdown menus for Host, Hostname, Port, Plugin, Severity, and Finding, along with a 'Clear' button. Below the filter bar, there is a section for 'Update selected findings:' with buttons for 'Overwrite', 'Update', 'Set to Open', 'Set to No Issue', and 'Set to MASKED'. The central table lists scan findings for the host 'sectionzero.org'. The findings are color-coded: red for high severity (e.g., Apache HTTP Server Byte Range DoS) and yellow for medium severity (e.g., SSL Certificate Cannot Be Trusted). Each finding entry includes columns for IP, Hostname, Port, Plugin, Severity, Finding description, Remark, and Action (Edit, Open, No Issue, Mask).

| IP | Hostname | Port | Plugin | Severity | Finding | Remark | Action |
|-----------------|-----------------|---------|--------|----------|--|--------|----------------------------|
| sectionzero.org | sectionzero.org | 80/tcp | 55976 | 1 | Apache HTTP Server Byte Range DoS The web server running on the remote host is affected by a denial of service vulnerability. Plugin output: Nessus ... | | Edit, Open, No Issue, Mask |
| sectionzero.org | sectionzero.org | 80/tcp | 40984 | 0 | Browsable Web Directories Some directories on the remote web server are browsable. Plugin output: The following directories are browsable : http://... | | Edit, Open, No Issue, Mask |
| sectionzero.org | sectionzero.org | 587/tcp | 56984 | 0 | SSL / TLS Versions Supported The remote service encrypts communications. Plugin output: This port supports SSLv2/SSLv3/TLSv1.0. Description: This ... | | Edit, Open, No Issue, Mask |
| sectionzero.org | sectionzero.org | 587/tcp | 51192 | 2 | SSL Certificate Cannot Be Trusted The SSL certificate for this service cannot be trusted. Plugin output: The following certificates were at the top ... | | Edit, Open, No Issue, Mask |
| sectionzero.org | sectionzero.org | 587/tcp | 31705 | 2 | SSL Anonymous Cipher Suites Supported The remote service supports the use of anonymous SSL ciphers. Plugin output: The remote server supports the fo... | | Edit, Open, No Issue, Mask |

SCHUBERG PHILIS

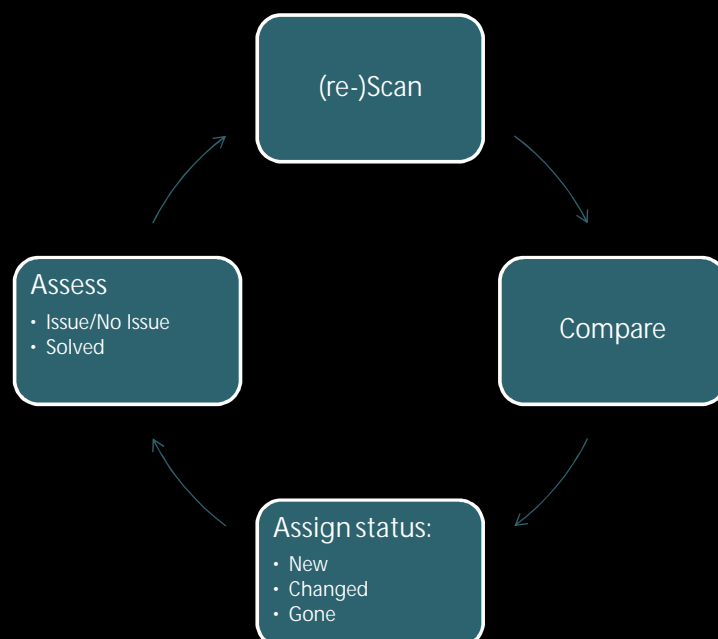
Assess

Manually assigned:

- » Open
- » No Issue
- » Fixed
- » Hard masked

SCHUBERG PHILIS

The scanning cycle...



SCHUBERG PHILIS

Dramatic reduction



SCHUBERG PHILIS

7 maart 2012

Why Seccubus...

- » Scans can be scheduled
- » One place to schedule and assess scans with:
 - Nessus
 - OpenVAS
 - Nikto
 - Nmap
- » Only need to review new/change/gone findings
- » Less boring repetitive work, lower chance of errors
- » Work is proportional to amount of change

SCHUBERG PHILIS

Where do I get it?

Seccubus.com

SCHUBERG PHILIS

Questions?

Image: What now?, a Creative Commons Attribution No-Derivative-Works (2.0) image from laurenclose's photostream



SCHUBERG PHILIS

Frank Breedijk

- » Security Officer at Schuberg Philis
- » Author of Seccubus
- » Blogger for CupFighter.net

Email: fbreedijk@schubergphilis.com
Twitter: [@Seccubus](https://twitter.com/Seccubus)
Blog: <http://cupfighter.net>
Project: <http://www.seccubus.com>
Company: <http://www.schubergphilis.com>



SCHUBERG PHILIS