ΚΑΣΣΙΟΠΕΙΑ

Κινητό Σύστημα Επιθεώρησης Ασφαλείας

Πανεπιστήμιο Μακεδονίας
Τμήμα Εφαρμοσμένης Πληροφορικής

Μαυρουδής Βασίλειος
mavroudisv@gmail.com

Μαυρίδης Ιωάννης
mavridis@uom.gr

Περιεχόμενα

- Απαιτήσεις διαχείρισης ασφαλείας
- Καταγραφές δραστηριότητας
- Οπτικοποίηση δεδομένων
- ΚΑΣΣΙΟΠΕΙΑ
- Αρχιτεκτονική συστήματος
  - Επιμέρους συστήματα
  - Ασφαλή κανάλια μετάδοσης δεδομένων
- Παράδειγμα χρήσης
- Λογισμικό ΕΛ/ΛΑΚ
- Συμπεράσματα

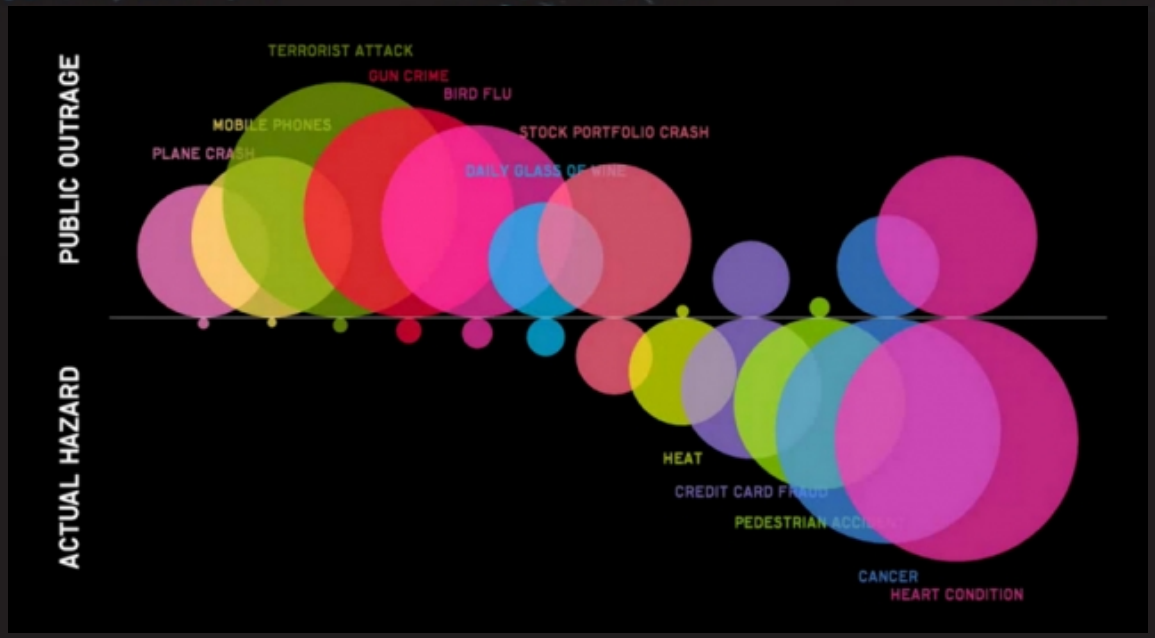
Διαχείριση Ασφάλειας Διακομιστών

- Απρόσκοπτη και αδιάλειπτη επίβλεψη
- Αποτίμηση κατάστασης ασφαλείας
- Εφαρμογή πολιτικών ασφαλείας
- Χρονική και χωρική ανεξαρτησία

Καταγραφές Δραστηριότητας (Log files)

- Λεπτομερής καταγραφή δραστηριότητας διακομιστή
- Χιλιάδες γραμμές πληροφοριών
- Δυσκολία στην παρακολούθηση
- Ανάγκη για διαχείριση και ανάλυσή τους

Οπτικοποίηση δεδομένων



- Επεξεργασία πρωτογενών δεδομένων (raw data)
- Αφαιρετική αναπαράσταση πολύπλοκων δεδομένων με γραφικά, κίνηση κ.α.
- Απαιτεί αρκετούς υπολογιστικούς πόρους

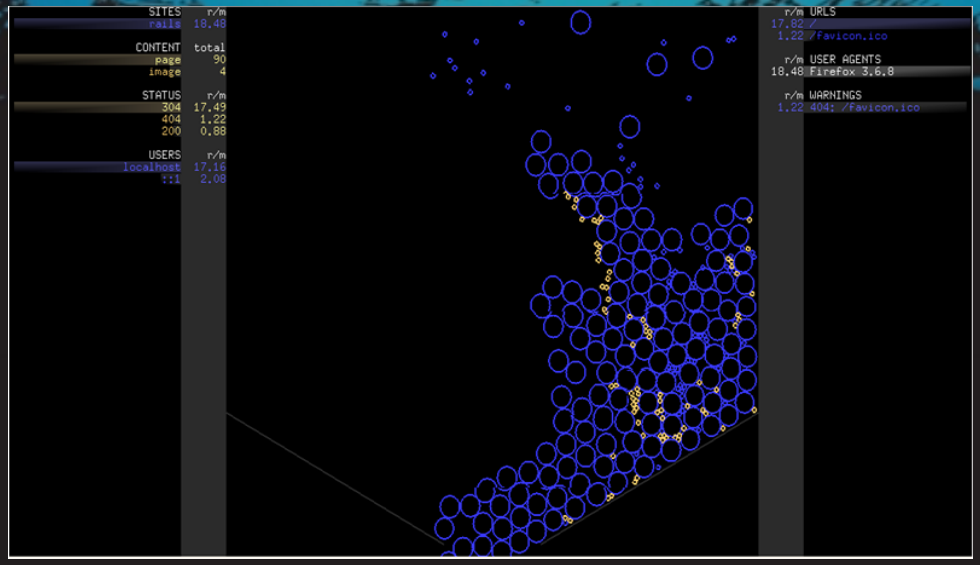
ΚΑΣΣΙΟΠΕΙΑ
Αρχιτεκτονική του συστήματος

Επιτηρούμενος διακομιστής

- Webserver (apache) αλλά και οποιαδήποτε υπηρεσία καταγράφει την δραστηριότητα της
- Αρχεία καταγραφών δραστηριότητας (Log Files)
  - access.log
  - error.log

```
67.195.115.217 - - [29/Oct/2010:20:36:53 +0300] "GET /index.php?option=com_content&view=article&id=51&Itemid=54 HTTP/1.0" 200 2714 "-" "Mozilla/5.0 (compatib
le; Yahoo! Slurp/3.0; http://help.yahoo.com/help/us/ysearch/slurp)"
184.73.89.175 - - [29/Oct/2010:21:25:28 +0300] "HEAD / HTTP/1.1" 200 - "http://www.netcraft.com/survey/" "Mozilla/4.0 (compatible; Netcraft Web Server Survey
)"
67.195.115.217 - - [30/Oct/2010:01:41:51 +0300] "GET /robots.txt HTTP/1.0" 200 145 "-" "Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/
ysearch/slurp)"
67.195.115.217 - - [30/Oct/2010:01:41:51 +0300] "GET /index.php/photosvideos HTTP/1.0" 200 2926 "-" "Mozilla/5.0 (compatible; Yahoo! Slurp/3.0; http://help.y
ahoo.com/help/us/ysearch/slurp)"
194.72.238.61 - - [30/Oct/2010:05:38:21 +0300] "HEAD / HTTP/1.1" 200 - "http://www.netcraft.com/survey/" "Mozilla/4.0 (compatible; Netcraft Web Server Survey
)"
194.153.113.7 - - [30/Oct/2010:11:42:19 +0300] "GET / HTTP/1.1" 200 10070 "-" "oBot"
194.153.113.7 - - [30/Oct/2010:11:42:19 +0300] "HEAD / HTTP/1.1" 200 - "-" "oBot"
194.153.113.7 - - [30/Oct/2010:11:42:19 +0300] "GET / HTTP/1.1" 200 10076 "-" "oBot"
65.52.51.180 - - [30/Oct/2010:17:59:18 +0300] "GET /robots.txt HTTP/1.1" 200 319 "-" "msnbot/2.0b (+http://search.msn.com/msnbot.htm)"
92.243.84.187 - - [30/Oct/2010:19:11:24 +0300] "GET /plugins/editors/tinymce/jscripts/tiny_mce/plugins/tinybrowser/tinybrowser.php?type=file&folder= HTTP/1.0
" 404 275 "http://algor.uom.gr/plugins/editors/tinymce/jscripts/tiny_mce/plugins/tinybrowser/tinybrowser.php?type=file&folder=" "Mozilla/4.0 (compatible; MSI
```

Διακομιστής Οπτικοποίησης



- Είσοδος: Αρχεία καταγραφών δραστηριότητας υπηρεσίας
- Επεξεργασία/Οπτικοποίηση: gl_tail (modified)
- Έξοδος:
  - Αλφαριθμητικά στατιστικά στοιχεία
  - Εικόνα οπτικοποιημένων δεδομένων

Εφαρμογή gl_tail v. 0.18 (modified)

- Υλοποίηση ασφαλούς σύνδεσης ssh
- Συλλογή και ανάλυση αρχείων καταγραφών
- Οπτικοποίηση πρωτογενών δεδομένων και υπολογισμός διαφόρων δεικτών δραστηριότητας
- ruby on rails & opengl
- Διανέμεται ελέυθερα (GPLv2)

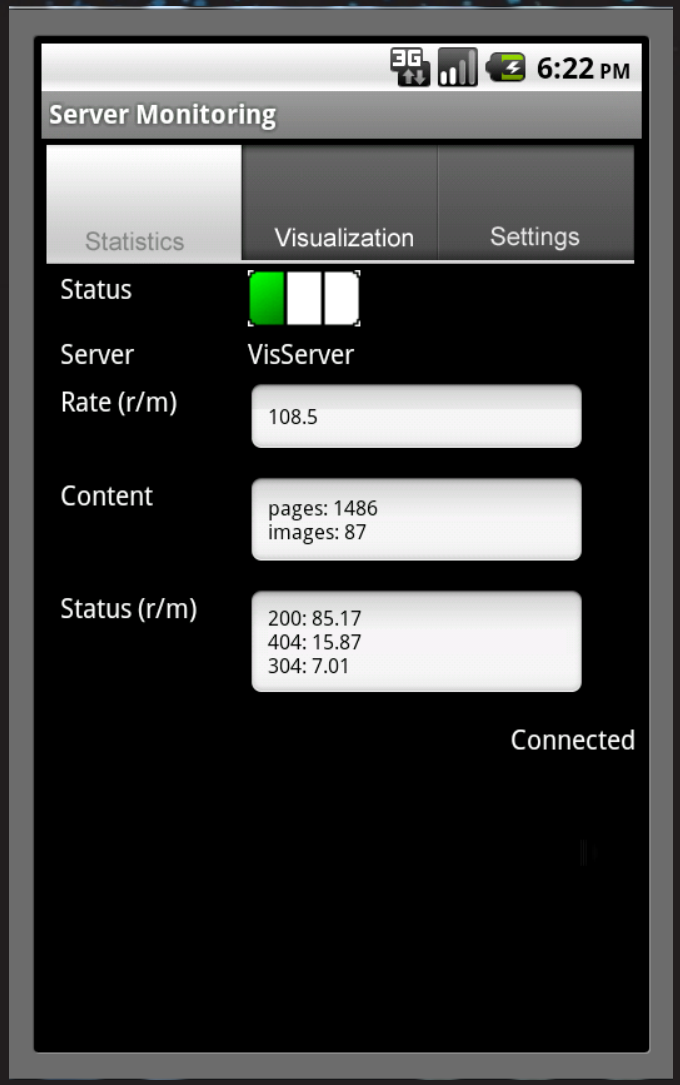
Κινητή συσκευή

- Τελικός αποδέκτης των πληροφοριών
- Smartphone ή PDA με Wifi
- Λειτουργικό σύστημα:
  - Android

Η εφαρμογή ΚΑΣΣΙΟΠΕΙΑ

- Στατιστικά στοιχεία σε πραγματικό χρόνο
- Τρέχουσα εικόνα της οπτικοποίησης
- Ένδειξη αποτίμησης κατάστασης διακομιστή
- Ασφαλής μετάδοση δεδομένων
- Ρυθμίσεις σύνδεσης και ρυθμού λήψης στοιχείων
- Java SDK
- Διανομή του κώδικα με άδεια ΕΛ/ΛΑΚ και εκτενές documentation

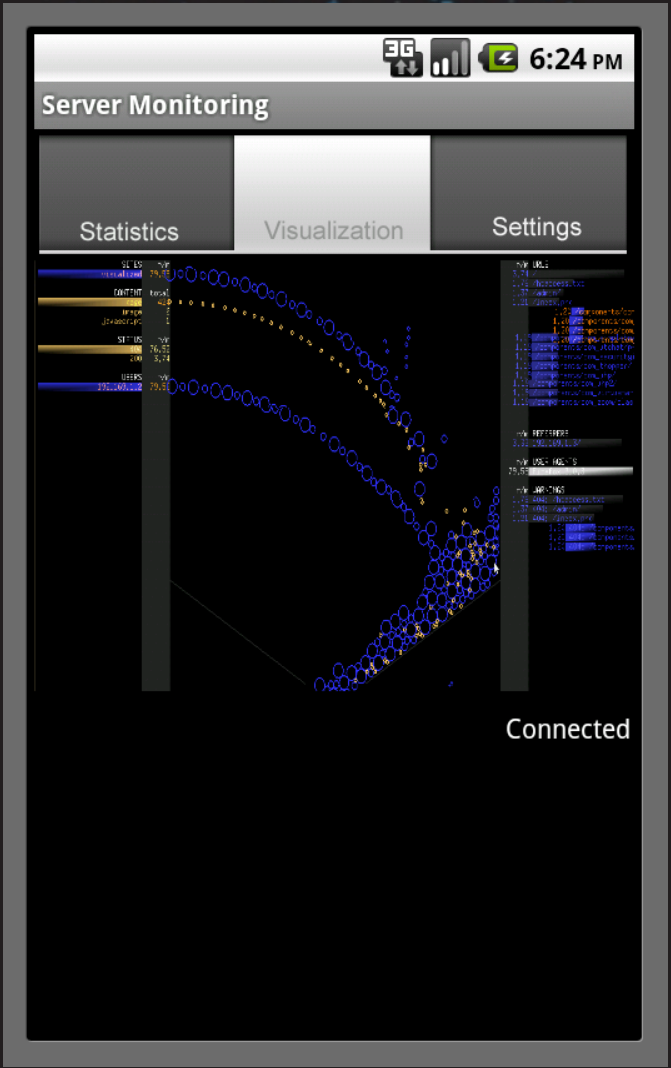
Στατιστικά στοιχεία



- Ένδειξη τρέχουσας κατάστασης

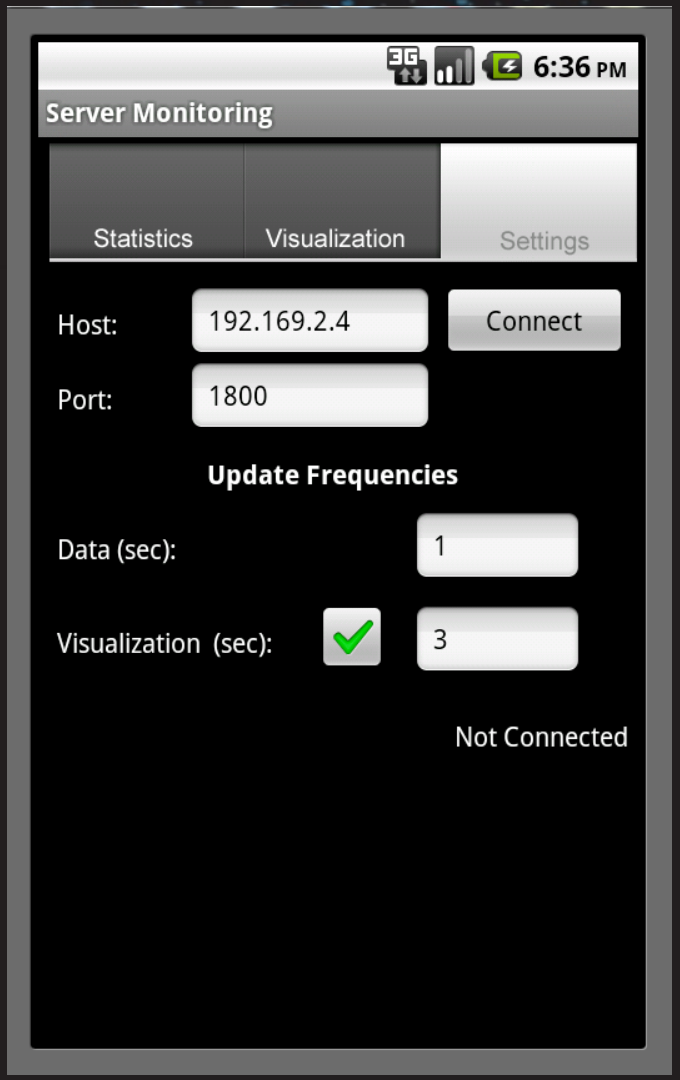
- Στατιστικά στοιχεία
  - Αιτημάτων
  - Περιεχομένου
  - Status

Εικόνα οπτικοποίησης



- Εικόνα οπτικοποίησης
- Στοιχεία δραστηριότητας
  - URLs
  - Warnings
- Δυνατότητα μεγέθυνσης περιοχής

Ρυθμίσεις



- Σύνδεσης
  - IP Διεύθυνση
  - Αριθμός θύρας
- Λήψης στοιχείων
  - Στατιστικών
  - Οπτικοποίησης

Ασφαλή κανάλια μετάδοσης δεδομένων

- Επιτηρούμενος διακ. - διακ. Οπτικοποίησης
  - SSH
  - Ψηφιακή υπογραφή DSA
- Διακομιστής Οπτικοποίησης – Κινητή Συσκευή
  - WiFi – GPRS/3G
  - IEEE 802.11i (WPAv2)

Παράδειγμα χρήσης 1

Προσομοίωση επίθεσης σε CMS (joomla) με το Joomscan (OWASP)

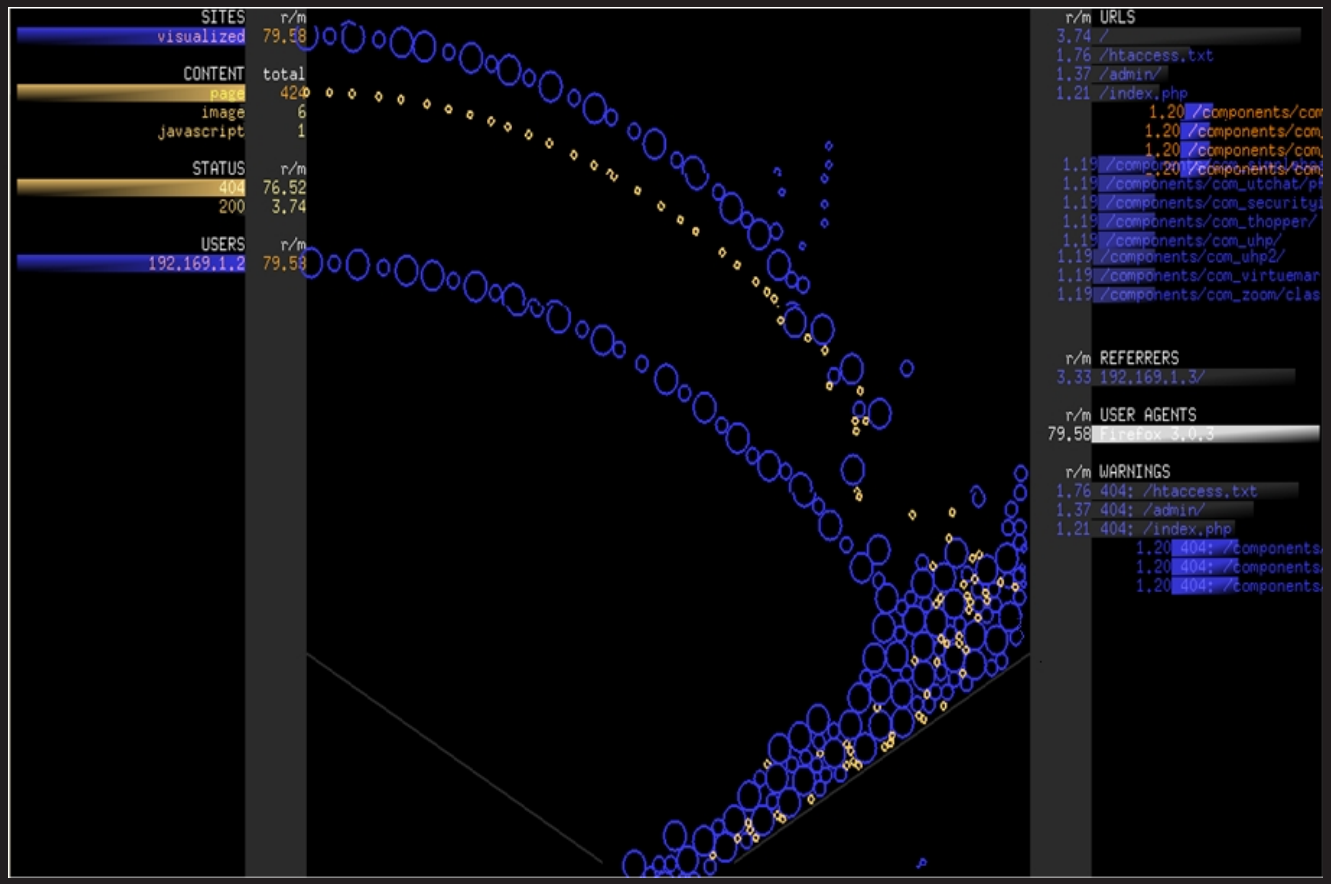
- Αναζητά ευάλωτα components ή modules σε joomla σελίδες
- Δεν έχει ιδιαίτερες απαιτήσεις σε γνώσεις και εξοπλισμό
- Υλοποιείται με απλά αιτήματα (requests)

Παράδειγμα χρήσης 2

```
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "HEAD /components/com_detail/ HTTP/1.1" 404 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "GET /admin_dir_was_renamed/components/ HTTP/1.1" 404 509 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "HEAD /admin_dir_was_renamed/components/ HTTP/1.1" 404 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "GET /components/com_foevpartners/ HTTP/1.1" 404 504 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "HEAD /components/com_foevpartners/ HTTP/1.1" 404 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "GET /components/com_inter/ HTTP/1.1" 404 497 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "HEAD /components/com_inter/ HTTP/1.1" 404 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "GET /components/com_emcomposer/ HTTP/1.1" 404 502 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "HEAD /components/com_emcomposer/ HTTP/1.1" 404 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "GET /components/com_ixxocart/ HTTP/1.1" 404 500 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "HEAD /components/com_ixxocart/ HTTP/1.1" 404 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "GET /components/com_publication/ HTTP/1.1" 404 503 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "HEAD /components/com_publication/ HTTP/1.1" 404 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "GET /components/com_lexikon/ HTTP/1.1" 404 499 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "HEAD /components/com_lexikon/ HTTP/1.1" 404 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "GET /components/com_filebase/ HTTP/1.1" 404 500 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "HEAD /components/com_filebase/ HTTP/1.1" 404 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "GET /components/com_aclassf/ HTTP/1.1" 404 499 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "HEAD /components/com_aclassf/ HTTP/1.1" 404 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "GET /components/com_pms/ HTTP/1.1" 404 495 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "HEAD /components/com_pms/ HTTP/1.1" 404 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "GET /components/com_joomloads/ HTTP/1.1" 404 501 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "HEAD /components/com_joomloads/ HTTP/1.1" 404 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "GET /components/com_kunena/ HTTP/1.1" 404 498 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "HEAD /components/com_kunena/ HTTP/1.1" 404 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "GET /components/com_misterestate/ HTTP/1.1" 404 504 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "HEAD /components/com_misterestate/ HTTP/1.1" 404 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "GET /templates/be2004-2/ HTTP/1.1" 404 495 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "HEAD /templates/be2004-2/ HTTP/1.1" 404 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "GET /modules/mod_as_category.php HTTP/1.1" 404 503 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "HEAD /modules/mod_as_category.php HTTP/1.1" 404 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "GET /modules/mod_quick_question.php HTTP/1.1" 404 506 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "HEAD /modules/mod_quick_question.php HTTP/1.1" 404 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "GET /modules/mod_pxt/ HTTP/1.1" 404 492 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "HEAD /modules/mod_pxt/ HTTP/1.1" 404 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "GET /modules/mod_calendar.php HTTP/1.1" 404 500 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "HEAD /modules/mod_calendar.php HTTP/1.1" 404 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "GET /ajaxim/ HTTP/1.1" 404 483 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
127.0.0.1 - - [13/May/2011:18:58:16 +0300] "HEAD /ajaxim/ HTTP/1.1" 404 182 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3"
```

- Δημιουργήθηκαν 994 γραμμές καταγραφών

Παράδειγμα χρήσης 3

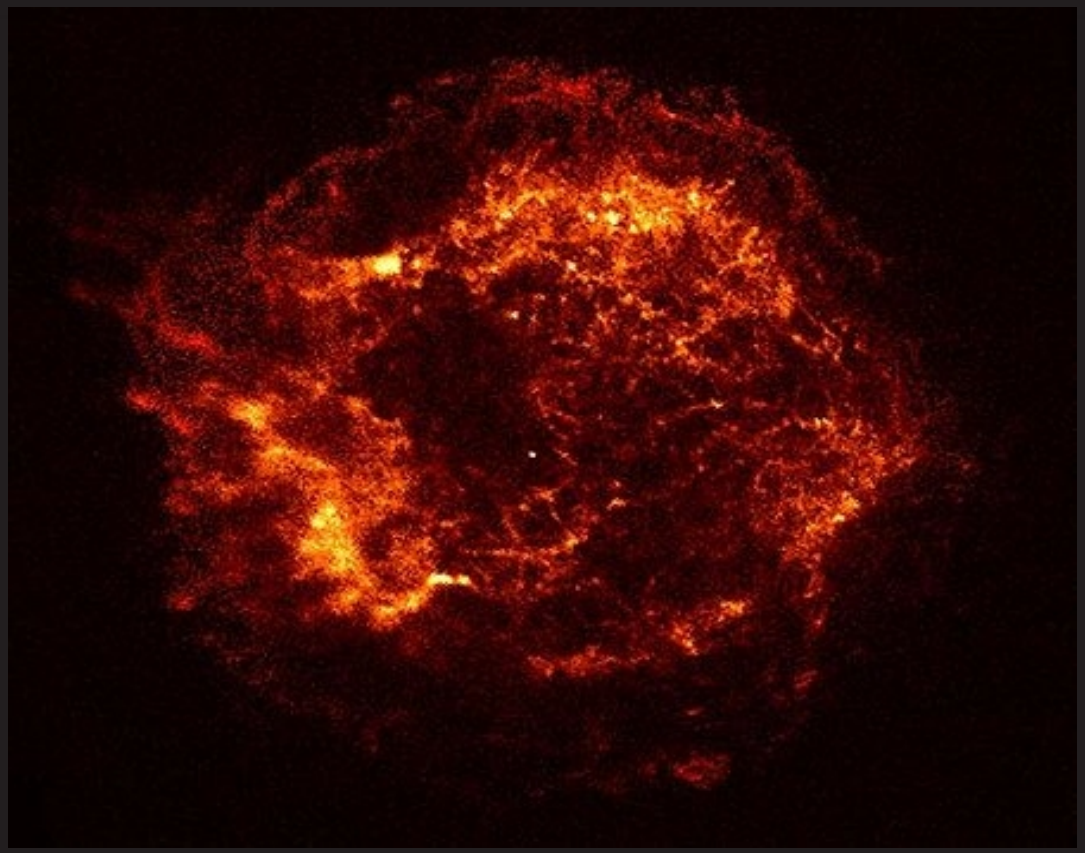


Έργα ΕΛ/ΛΑΚ που χρησιμοποιήθηκαν

- php 5
- Apache webserver
- gl_tail v. 0.18
- Open-ssh
- Android platform

Συμπεράσματα

- Οπτικοποίηση
  - Ισχυρό εργαλείο επιθεώρησης ασφαλείας
  - Εφαρμογή σε σημαντικούς διακομιστές
- Φορητότητα
  - Ευελιξία και αυτονομία
  - Αστάθεια σύνδεσης και μικρή υπολογιστική ισχύς
- ΕΛ/ΛΑΚ
  - Ελευθερία πειραματισμού
  - Δυνατότητα βελτίωσης και επέκτασης λογισμικού

ΚΑΣΣΙΟΠΕΙΑ

Ευχαριστούμε για την προσοχή σας