



**ΔΟΜΗ ΑΠΑΣΧΟΛΗΣΗΣ
ΚΑΙ ΣΤΑΔΙΟΔΡΟΜΙΑΣ
ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΜΑΚΕΔΟΝΙΑΣ**

ΠΡΑΞΗ:

«Δομή Απασχόλησης και Σταδιοδρομίας (Δ.Α.ΣΤΑ.) Πανεπιστημίου Μακεδονίας»

Κωδικός MIS 327465

ΥΠΟΕΡΓΟ:

**«Δομή Απασχόλησης και Σταδιοδρομίας (Δ.Α.ΣΤΑ.) Πανεπιστημίου
Μακεδονίας»**

και α/α «01»

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ:

«Εκπαίδευση και Δια Βίου Μάθηση» (Ε.Π.Ε.Δ.Β.Μ.) 2007-2013

Υπουργείο Παιδείας, Δια Βίου Μάθησης και Θρησκευμάτων

ΛΕΩΝΑΣ ΠΡΟΤΕΡΑΙΟΤΗΤΑΣ 5:

**«Αναβάθμιση των συστημάτων αρχικής επαγγελματικής κατάρτισης και
επαγγελματικής εκπαίδευσης και σύνδεση της εκπαίδευσης με την αγορά
εργασίας στις 3 περιφέρειες Σταδιακής Εξόδου»**

ΚΑΤΗΓΟΡΙΑ ΠΡΑΞΗΣ:

«Δομές Απασχόλησης και Σταδιοδρομίας (Δ.Α.ΣΤΑ.)»

Η Πράξη συγχρηματοδοτείται από το Ευρωπαϊκό Κοινωνικό Ταμείο (Ε.Κ.Τ.) και από εθνικούς πόρους, μέσω του Προγράμματος Δημοσίων Επενδύσεων (Π.Δ.Ε.) του Υπουργείου Παιδείας, Δια Βίου Μάθησης και Θρησκευμάτων

Παραδοτέο **Πακέτο Εργασίας Π.Ε.2 «Ανάπτυξη Δικτυακού Τόπου ΔΑΣΤΑ»**

Δράση Δ2.1: **«Ανάπτυξη Δικτυακού Τόπου ΔΑΣΤΑ»**

Παραδοτέο Π2.1.4: **«Ενημέρωση περιεχομένου (updates) ιστοσελίδας ΔΑΣΤΑ (Νέες ενημερώσεις και διορθώσεις σχετικά με την ασφάλεια, διορθώσεις στην υπάρχουσα δομή, γενικότερη διαχείριση τεχνικών αιτημάτων)»**

Για την εκπόνηση του παραδοτέου απασχολήθηκαν τα κάτωθι μέλη της ομάδας έργου
Παναγιώτης Σιδηρόπουλος, Εξωτερικός Συνεργάτης
Τσακνίδου Ασπασία, ΠΕ Πληροφορικής, Προϊσταμένη Κέντρου Υπολογιστών και Δικτύων

Θεσσαλονίκη, 18/12/2012

Π.Ε.2. «Ανάπτυξη Δικτυακού τόπου ΔΑΣΤΑ»

Π.2.1.4. Ενημέρωση περιεχομένου (updates) ιστοσελίδας ΔΑΣΤΑ (Νέες ενημερώσεις και διορθώσεις σχετικά με την ασφάλεια, διορθώσεις στην υπάρχουσα δομή, γενικότερη διαχείριση τεχνικών αιτημάτων)

1 Επιλογή CMS για την κατασκευή του ιστοχώρου

Από τα βασικότερα κριτήρια επιλογής του κατάλληλου content management system αποτελούν πρωτίστως η δυνατότητα υποστήριξης, η επεκτασιμότητα, η ευχρηστία, η ασφάλεια κώδικα καθώς και το αν ανήκει στην κατηγορία λογισμικού ανοιχτού κώδικα. Μεταξύ των δημοφιλέστερων CMS κατατάσσεται και το Drupal, το οποίο αν και δε λογίζεται, συγκριτικά με άλλα, στα πλέον εύχρηστα, υπερτερεί στα περισσότερα από τα παραπάνω κριτήρια, προσφέροντας σημαντικά πλεονεκτήματα στην κατασκευή πολύπλοκων ιστοχώρων, με κυριότερο πλεονέκτημα την επεκτασιμότητα κατ' απαίτηση, καθώς διαθέτει πληθώρα πρόσθετων μονάδων (modules) με εξειδικευμένη για το καθένα λειτουργία.

2 Δοκιμαστικός ιστότοπος (development site)

Κάθε νέα ενημέρωση ή διόρθωση στην υπάρχουσα δομή είναι σκόπιμο να δοκιμάζεται σε test περιβάλλον, πριν εφαρμοστεί στον υπό κανονική λειτουργία δικτυακό τόπο. Γι' αυτό το σκοπό δημιουργήθηκε το δοκιμαστικό περιβάλλον στην διεύθυνση: <http://afroditi.uom.gr/dastadevel/>

3 Αυθεντικοποίηση/εξουσιοδότηση χρηστών

Η αυθεντικοποίηση/εξουσιοδότηση των χρηστών παρέχεται μέσα από έναν κλασικό μηχανισμό εισόδου (login) με την βοήθεια κατάλληλων μονάδων (modules), τα οποία αναλαμβάνουν να πιστοποιήσουν τον κάθε χρήστη επαληθεύοντας τα στοιχεία που αυτός διαθέτει στον διακομιστή LDAP (user credential checking). Αυτό πραγματοποιείται με την βοήθεια των παρακάτω ενεργών μονάδων οι οποίες έχουν και τις ανάλογες προαπαιτήσεις και μεταξύ τους εξαρτήσεις(dependencies):

- LDAP Servers
- LDAP Authentication
- LDAP Authorization
- LDAP Authorization - Drupal Roles
- LDAP Authorization - OG
- LDAP Query
- LDAP Help

Η παραμετροποίηση των παραπάνω μονάδων και η διασύνδεσή τους με τον διακομιστή LDAP έχει οριστεί σύμφωνα με τις υποδείξεις του διαχειριστή του.

4 Ρόλοι χρηστών

Προκειμένου να καταστεί εφικτή η ανάρτηση/δημοσίευση από χρήστες εκτός του διαχειριστή, έχει δημιουργηθεί ρόλος χρήστη με τα ανάλογα δικαιώματα (ΔΑΣΤΑ manager).

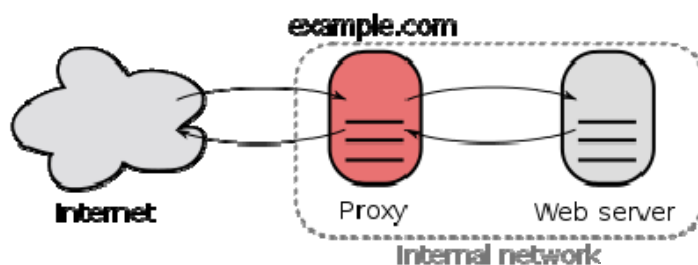
5 Ασφάλεια και ομαλή λειτουργία ιστοχώρου και διακομιστή

Καθοριστικής σημασίας για την ασφάλεια του ιστοχώρου και κατ'επέκταση διακομιστή είναι οι ενημερώσεις ασφαλείας τόσο του πυρήνα του cms όσον και των πρόσθετων modules. Ο έλεγχος των διαθέσιμων ενημερώσεων μπορεί να πραγματοποιηθεί μέσα από το ίδιο το περιβάλλον διαχείρισης και συγκεκριμένα μέσα από την διαδρομή Διαχείριση - Αναφορές - Διαθέσιμες Ενημερώσεις, όπου το drupal εμφανίζει μια αναλυτική λίστα των νεότερων εκδόσεων, με δυνατότητα επιλογής της επιθυμητής ενημέρωσης. Η ρύθμιση ελέγχου/ειδοποιήσεων των ενημερώσεων έχει οριστεί σε ημερήσια συχνότητα.

6 Βελτιστοποίηση λειτουργίας ιστοχώρου

6.1 Επιτάχυνση λειτουργίας με την χρήση web cache

Η web cache γνωστή και ως ανάστροφος διακομιστής μεσολάβησης (reverse proxy) ή web accelerator είναι ένας μηχανισμός προσωρινής αποθήκευσης αρχείων ιστοχώρου, τα οποία βρίσκονται σε έναν ή περισσότερους διακομιστές και προορίζονται για διανομή σε σταθμούς ή εφαρμογές πελάτες (clients). Σε αντίθεση με τους κλασσικούς διακομιστές μεσολάβησης που τυπικά βρίσκονται στην πλευρά του πελάτη, ο ανάστροφος διακομιστής μεσολάβησης βρίσκεται στην ίδια πλευρά με τον διακομιστή web και προτάσσεται αυτού εξυπηρετώντας συχνά μεγάλο αριθμό ομοίων αιτημάτων, ελαττώνοντας σημαντικά το φορτίο στους αρχικούς διακομιστές και ομαλοποιώντας παράλληλα τη χρήση του διαθέσιμου εύρους ζώνης (bandwidth).



«Πηγή εικόνας:Wikipedia»

Πιλοτικά δοκιμάζονται και αξιολογούνται οι ακόλουθες web cache για τον ιστοχώρο του ΔΑΣΤΑ:

- Boost: Παρέχει caching για στατικές σελίδες προσφέροντας σημαντικές αναβαθμίσεις ταχύτητας και επεκτασιμότητα που αφορά κυρίως ανώνυμη διαδικτυακή κίνηση και αιτήματα. Υποστηρίζει πλήρως τον Apache Web server, στον οποίο βασίζεται και η λειτουργία του ΔΑΣΤΑ.
- Varnish: Παρέχει caching για στατικό αλλά και δυναμικό περιεχόμενο. Μέσω της ειδικής γλώσσας παραμετροποίησης που χρησιμοποιεί (VCL) επιτρέπει τη σύνταξη προσαρμοσμένων πολιτικών διαχείρισης αιτημάτων.
- memcache: το οποίο κάνει χρήση της μνήμης RAM για την επιτάχυνση της λειτουργίας.

7 Δοκιμές απόδοσης και ταχύτητας λειτουργίας.

Το apache benchmarking tool ([ab](#)) είναι ένα δημοφιλές εργαλείο για τον έλεγχο της απόδοσης διακομιστών web.

8 Ασφάλεια

8.1 Αντίγραφα ασφαλείας

Επιτακτικής σημασίας για κάθε CMS είναι η λήψη αντιγράφων ασφαλείας που αφορούν την βάση δεδομένων του τρέχοντος συστήματος. Η ενέργεια αυτή είναι δυνατόν να πραγματοποιηθεί είτε χειροκίνητα σε συγκεκριμένη χρονική στιγμή κατ' εντολή του διαχειριστή, είτε αυτόματα από το σύστημα. Για την εκτέλεση μιας τέτοιας ενέργειας, ειδικότερα όσον αφορά την αυτοματοποίησή της, χρησιμοποιείται η πρόσθετη μονάδα Backup and Migrate η οποία είναι διαθέσιμη μέσω της διαδρομής Διαχείριση → Ευρετήριο → Backup and Migrate ή μέσω της διαδρομής Διαχείριση → Παραμετροποίηση → Σύστημα → Backup and Migrate. Οι διαθέσιμες επιλογές-ενέργειες που παρέχονται από την μονάδα απεικονίζονται στο παρακάτω στιγμιότυπο:



Οι καρτέλες Backup και Restore αφορούν την χειροκίνητη δημιουργία αντιγράφων ασφαλείας καθώς και την επαναφορά. Στην καρτέλα Προφίλ χρηστών → Default Setting → επεξεργασία → Advanced Options δίνεται η δυνατότητα αυτόματων ειδοποιήσεων επιτυχούς ή ανεπιτυχούς εκτέλεσης της ενέργειας backup (εδώ επιλέγονται και οι δύο τύποι ειδοποιήσεων). Ως διεύθυνση ηλεκτρονικού ταχυδρομείου δηλώνεται η διεύθυνση του διαχειριστή ΔΑΣΤΑ: dastaweb@uom.gr. Εδώ ορίζεται και η δυνατότητα να τεθεί ο ιστότοπος εκτός λειτουργίας προσωρινά μέχρι την ολοκλήρωση της ενέργειας (ενεργοποιώντας το πεδίο Take site offline), προβάλλοντας παράλληλα ένα σχετικό ενημερωτικό μήνυμα στους επισκέπτες της σελίδας που θα μπορούσε ενδεικτικά να διατυπώνεται ως εξής: «Η σελίδα Δομή Απασχόλησης και Σταδιοδρομίας – ΔΑΣΤΑ : Πανεπιστήμιο Μακεδονίας είναι αυτή τη στιγμή εκτός λειτουργίας λόγω συντήρησης. Θα επανέλθουμε σύντομα. Ευχαριστούμε για την κατανόησή σας».

Προτεινόμενη συχνότητα αυτόματης δημιουργίας αντιγράφων είναι μια φορά την εβδομάδα.

Έμφαση δίνεται στην οδηγία που παρουσιάζεται για την εγκατάσταση της μονάδας και η οποία επισημαίνει ότι τα αντίγραφα ασφαλείας κατά προεπιλογή προστατεύονται από δημόσια πρόσβαση μέσω ενός κανόνα .htaccess που όμως θα δουλέψει μόνο σε κατάλληλα ρυθμισμένο διακομιστή apache. Οι συγκεκριμένες συστάσεις και οδηγίες παρέχονται στην διεύθυνση drupal.org/project/backup_migrate και θα εφαρμοστούν σε συνεργασία με τον διαχειριστή του διακομιστή apache.

Για την αποφυγή πληρότητας του διαθέσιμου χώρου αποθήκευσης αντιγράφων ασφαλείας ο προτεινόμενος μέγιστος αριθμός αντιγράφων (Number of Backup files to keep) είναι πέντε στην καρτέλα schedules.

8.2 Προστασία από διαδικτυακές επιθέσεις.

8.2.1 Flood Control

Υπάρχουν πρόσθετες μονάδες οι οποίες ενισχύουν την ασφάλεια του ιστοτόπου από διαδικτυακές επιθέσεις όπως πχ επιθέσεις τύπου DoS (Denial of Service), flooding κλπ που μπορεί να δημιουργούνται από αυτοματοποιημένους μηχανισμούς (πχ bot). Επιθέσεις με την μέθοδο flooding έχουν ως στόχο την εκμετάλλευση αδυναμιών που παρουσιάζει ο μηχανισμός three way handshake για τη δημιουργία σύνδεσης, δημιουργώντας ημιτελείς συνδέσεις με απώτερο σκοπό την εξάντληση των πόρων του συστήματος και τελικώς την άρνηση περαιτέρω νόμιμων συνδέσεων ή και την παύση της λειτουργίας του. Μια τέτοια πρόσθετη μονάδα είναι η μονάδα Flood Control που διαθέτει παραμέτρους για τον έλεγχο της επιτρεπόμενης συχνότητας αποτυχημένων συνδέσεων είτε με βάση την διεύθυνση IP (Failed login IP limit) ανά συγκεκριμένο χρονικό διάστημα (Failed login IP Window) , είτε με βάση το όνομα χρήστη (Failed login username limit/Failed login username window). Στην ίδια μονάδα υπάρχει επίσης και ο μηχανισμός προστασίας για φόρμες επικοινωνίας που περιορίζει την συχνότητα αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου (τα οποία αποστέλλονται μέσω του μηχανισμού της φόρμας). Ο ορισμός των τιμών των παραπάνω παραμέτρων μπορεί να γίνει αυστηρότερος με την μείωσή τους πράγμα το οποίο όμως θα πρέπει να πραγματοποιηθεί με σύνεση και μετά από κατά περίπτωση εξέταση των ύποπτων καταγραφών στα αρχεία συμβάντων ασφαλείας (logs) του συστήματος, ώστε να μην προκληθούν προβλήματα στις καθ' όλα κανονικές και νόμιμες λειτουργίες του ιστοτόπου. Για παράδειγμα μείωση των επιτρεπόμενων αποτυχημένων προσπαθειών σύνδεσης με βάση την διεύθυνση IP, εγείρει το ερώτημα του πόση θα πρέπει να είναι μια τέτοια μείωση με δεδομένο ότι για παράδειγμα η ίδια διεύθυνση IP θα μπορούσε να "αντιπροσωπεύει" ένα ολόκληρο εργαστήριο υπολογιστών.

8.2.2 Captcha

Τα captcha (**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part) είναι ένας επιπλέον τρόπος προστασίας από ανεπιθύμητους αυτόματους μηχανισμούς οι οποίοι έχουν ως στόχο την απόκτηση πρόσβασης σε ιστοτόπους όπως πχ συγκεκριμένοι τύποι internet bot. Ο τρόπος προστασίας ως γνωστόν βασίζεται στην δημιουργία εικόνων που αναπαριστούν λέξεις ή τυχαία γράμματα με την μορφή εικόνας. Η ανάγνωση της εικόνας είναι απλή υπόθεση για ένα ανθρώπινο ον, αλλά μπορεί είναι ιδιαίτερα σύνθετη ή ακόμη και αδύνατη από έναν αυτοματοποιημένο μηχανισμό. Έτσι

ενσωματώνοντας captcha στον μηχανισμό εισόδου ενισχύεται σημαντικά η προστασία του ιστοτόπου από τέτοιου είδους απόπειρες παραβίασης.

Η ρύθμιση της μονάδας για τα captcha πραγματοποιείται μέσω της διαδρομής Διαχείριση → Παραμετροποίηση → Χρήστες → Captcha.

Υπάρχουν δύο τύποι captcha διαθέσιμοι:

1. Image (from module image_captcha)
2. Math (from module_captcha)

Ο προεπιλεγμένος τύπος είναι ο πρώτος (Image).

Το παρακάτω στιγμιότυπο απεικονίζει ένα τέτοιο captcha.

Λογαριασμός χρήστη

Όνομα χρήστη *

Εισάγετε το όνομα λογαριασμού σας για το ΔΑΣΤΑ DEVELOPMENT version: Πανεπιστήμιο Μακεδονίας.

Συνθηματικό *

Εισάγετε το συνθηματικό εισόδου που συνοδεύει το όνομα λογαριασμού σας.

CAPTCHA

Για αποφυγή προβλημάτων spam, παρακαλούμε, απαντήστε στην παρακάτω απλή ερώτηση.

N H S 5 N B

Ποιός είναι ο κωδικός (συνθηματικό) που φαίνεται στην παραπάνω εικόνα; *

Εισάγετε τους χαρακτήρες που φαίνονται στην εικόνα

Είσοδος