Πανεπιστήμιο Πειραιώς - Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορικής»

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ

ΕΛΕΓΧΟΣ ΑΣΦΑΛΕΙΑΣ ΕΦΑΡΜΟΓΩΝ ΔΙΑΔΙΚΤΥΟΥ

ΣΥΜΦΩΝΑ ΜΕ ΤΟ OWASP

ΠΑΡΑΡΤΗΜΑ Α’

ΕΛΕΓΧΟΣ ΑΣΦΑΛΕΙΑΣ ECLASS ΤΜΗΜ. ΠΛΗΡΟΦΟΡΙΚΗΣ

Μιρτζάνης Εμμανουήλ του Κυριάκου

ΜΠΠΛ / 06049

Επιβλέπων: Επίκουρος Καθηγήτρια Ν. Πολέμη

Πειραιάς, Απρίλιος 2012

Πίνακας περιεχομένων

ΠΑΡΑΡΤΗΜΑ Α'

ΕΛΕΓΧΟΣ ΑΣΦΑΛΕΙΑΣ ΕΦΑΡΜΟΓΗΣ eClass ΤΜΗΜΑΤΟΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

1 ΕΙΣΑΓΩΓΗ

Το τέταρτο μέρος της εργασίας περιλαμβάνει τον έλεγχο ασφάλειας της εφαρμογής eClass του τμήματος Πληροφορικής , του Πανεπιστημίου Πειραιώς στον ιστότοπο : **http://gunet2.cs.unipi.gr/eclass.**

Για την υλοποίηση των ελέγχων ακολουθήθηκε η μεθοδολογία του OWASP , όπως αυτή περιγράφεται στο OWASP testing guide 2008. Τα βασικά της βήματα περιλαμβάνονται στον παρακάτω πίνακα και οι κατηγορίες ελέγχων που περιλαμβάνει είναι:

Information Gthering (OWASP-IG-XXX)
Configuration Management Testing (OWASP-CM-XXX)
Authentication Testing (OWASP-AT-XXX)
Session Management (OWASP-SM-XXX)
Authorization Testing (OWASP-AZ-XXX)
Business logic testing (OWASP-BL-XXX)
Data Validation Testing (OWASP-DV-XXX)
Denial of Service Testing (OWASP-DS-XXX)
Web Services Testing (OWASP-WS-XXX)
AJAX Testing (OWASP-AJ-XXX) , όπου XXX ο αύξων αριθμός του test

Category	Ref. Number	Test Name	Vulnerability
Information Gathering	OWASP-**IG**-00l	Spiders, Robots and Crawlers -	N.A.
	OWASP-**IG**-002	Search Engine Discovery/Reconnaissance	N.A.
	OWASP-**IG**-003	Identify application entry points	N.A.
	OWASP-**IG**-004	Testing for Web Application Fingerprint	N.A.
	OWASP-**IG**-005	Application Discovery	N.A.
	OWAS P-**IG**-006	Analysis of Error Codes	Information Disclosure

Configuration Management Testing **Configuration Management Testing**	OWASP-**CM**-00l	SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity)	SSL Weakness
	OWASP-**CM**-002	DB Listener Testing	DB Listener weak
	OWASP-**CM**-003	Infrastructure Configuration Management Testing	Infrastructure Configuration management weakness
	OWASP-**CM**-004	Application Configuration Management Testing	Application Configuration management weakness
	OWASP-**CM**-005	Testing for File Extensions Handling	File extensions handling
	OWASP-**CM**-006	Old, backup and unreferenced files	Old, backup and unreferenced files
	OWASP-**CM**-007	Infrastructure and Application Admin Interfaces	Access to Admin interfaces
	OWASP-**CM**-008	Testing for HTTP Meth ods and XST	HTTP Methods enabled, XST permitted, HTTP Verb
Authentication Testing	OWASP-**AT**-00l	Credentials transport over an encrypted channel	Credentials transport over an encrypted channel
	OWASP-**AT**-002	Testing for user enumeration	User enumeration
	OWASP-**AT**-003	Testing for Guessable (Dictionary) User Account	Guessable user account
	OWASP-**AT**-004	Brute Force Testing	Credentials Brute forcing
	OWASP-**AT**-005	Testing for bypassing authentication schema	Bypassing authentication schema
	OWASP-**AT**-006	Testing for vulnerable remember password and pwd reset	Vulnerable remember password, weak pwd reset
	OWASP-**AT**-007	Testing for Logout and Browser Cache Management	Logout function not properly implemented, browser cache weakness

	OWASP-**AT**-008	Testing for CAPTCHA	Weak Captcha implementation
	OWASP-**AT**-009	Testing Multiple Factors Authentication	Weak Multiple Factors Authentication
	OWASP-**AT**-0l0	Testing for Race Conditions	Race Conditions vulnerability
Session Management	OWASP-**SM**-00l	Testing for Session Management Schema	Bypassing Session Management Schema, Weak Session Token
	OWASP-**SM**-002	Testing for Cookies attributes	Cookies are set not 'HTTP Only', 'Secure', and no time validity
	OWASP-**SM**-003	Testing for Session Fixation	Session Fixation
	OWASP-**SM**-004	Testing for Exposed Session Variables	Exposed sensitive session variables
	OWASP-**SM**-005	Testing for CSRF	CSRF
Authorization Testing	OWASP-**AZ**-00l	Testing for Path Traversal	Path Traversal
	OWASP-**AZ**-002	Testing for bypassing authorization schema	Bypassing authorization schema
	OWASP-**AZ**-003	Testing for Privilege Escalation	Privilege Escalation
Business logic testing	OWASP-**BL**-00l	Testing for business logic	Bypassable business logic
Data Validation Testing	OWASP-**DV**-00l	Testing for Reflected Cross Site Scripting	Reflected XSS
	OWASP-**DV**-002	Testing for Stored Cross Site Scripting	Stored XSS
	OWASP-**DV**-003	Testing for DOM based Cross Site Scripting	DOM XSS
	OWASP-**DV**-004	Testing for Cross Site Flashing	Cross Site Flashing
	OWASP-**DV**-005	SQL Injection	SQL Injection

Data Validation Testing	OWASP-**DV**-006	LDAP Injection	LDAP Injection
	OWASP-**DV**-007	ORM Injection	ORM Injection
	OWASP-**DV**-008	XML Injection	XML Injection
	OWASP-**DV**-009	SSI Injection	SSI Injection
	OWASP-**DV**-0l0	XPath Injection	XPath Injection
	OWASP-**DV**-0ll	IMAP/SMTP Injection	IMAP/SMTP Injection
	OWASP-**DV**-0l2	Code Injection	Code Injection
	OWASP-**DV**-0l3	OS Commanding	OS Commanding
	OWASP-**DV**-0l4	Buffer overflow	Buffer overflow
	OWASP-**DV**-0l5	Incubated vulnerability Testing	Incubated vulnerability
	OWASP-**DV**-0l6	Testing for HTTP Splitting/Smuggling	HTTP Splitting, Smuggling
Denial of Service Testing	OWASP-**DS**-00l	Testing for SQL Wildcard Attacks	SQL Wildcard vulnerability
	OWASP-**DS**-002	Locking Customer Accounts	Locking Customer Accounts
	OWASP-**DS**-003	Testing for DoS Buffer Overflows	Buffer Overflows
	OWASP-**DS**-004	User Specified Object Allocation	User Specified Object Allocation
	OWASP-**DS**-005	User Input as a Loop Counter	User Input as a Loop Counter
	OWASP-**DS**-006	Writing User Provided Data to Disk	Writing User Provided Data to Disk
	OWASP-**DS**-007	Failure to Release Resources	Failure to Release Resources
	OWASP-**DS**-008	Storing too Much Data in Session	Storing too Much Data in Session
Web Services Testing	OWASP-**WS**-00l	WS Information Gathering	N.A.

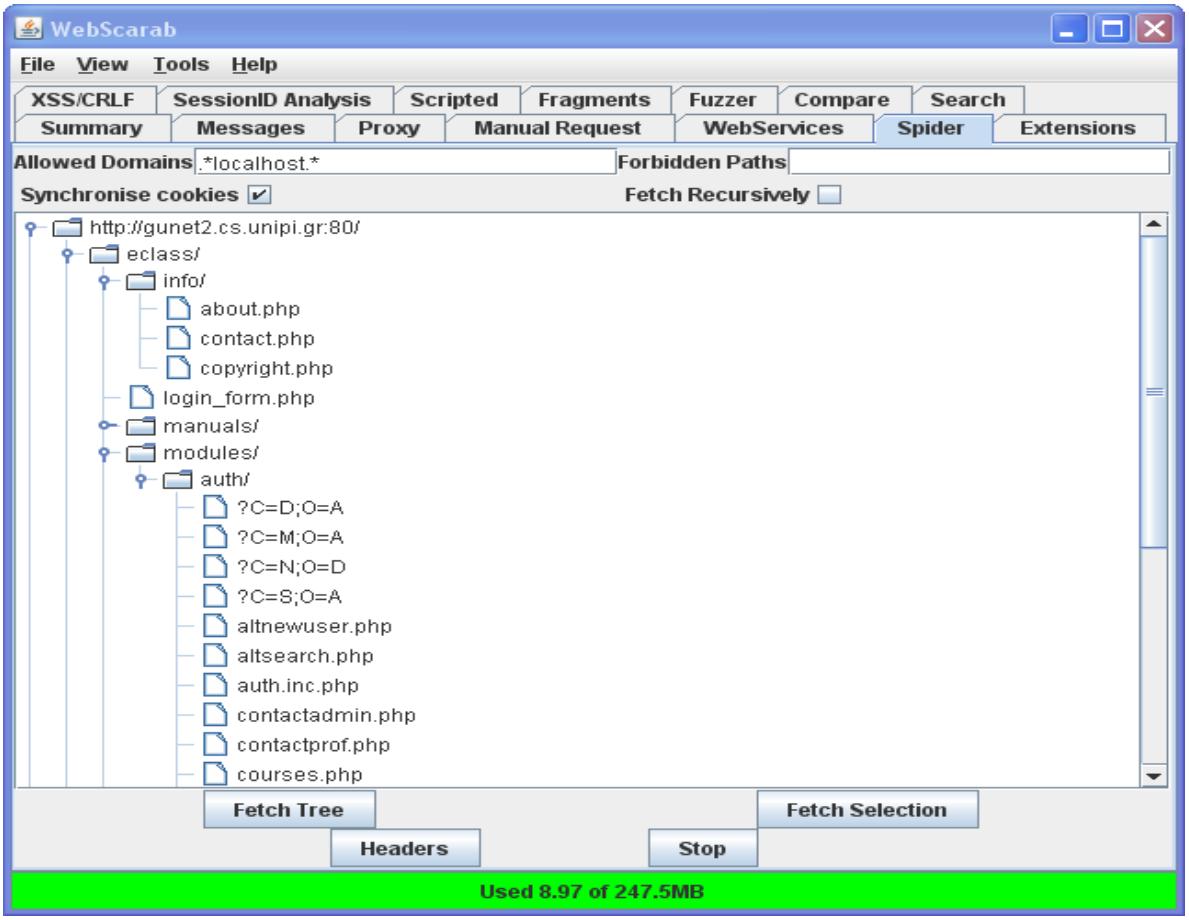
Web Services Testing	OWASP-**WS**-002	Testing WSDL	WSDL Weakness
	OWASP-**WS**-003	XML Structural Testing	Weak XML Structure
	OWASP-**WS**-004	XML content-level Testing	XML content-level
	OWASP-**WS**-005	HTTP GET parameters/REST Testing	WS HTTP GET parameters/REST
	OWASP-**WS**-006	Naughty SOAP attachments	WS Naughty SOAP attachments
	OWASP-**WS**-007	Replay Testing	WS Replay Testing
AJAX Testing	OWASP-**AJ**-00l	AJAX Vulnerabilities	N.A
	OWASP-**AJ**-002	AJAX Testing	AJAX weakness

Πίνακας: Έλεγχοι ανά κατηγορία , αριθμό αναφοράς , περιγραφή και ευπάθεια

2 INFORMATION GATHERING

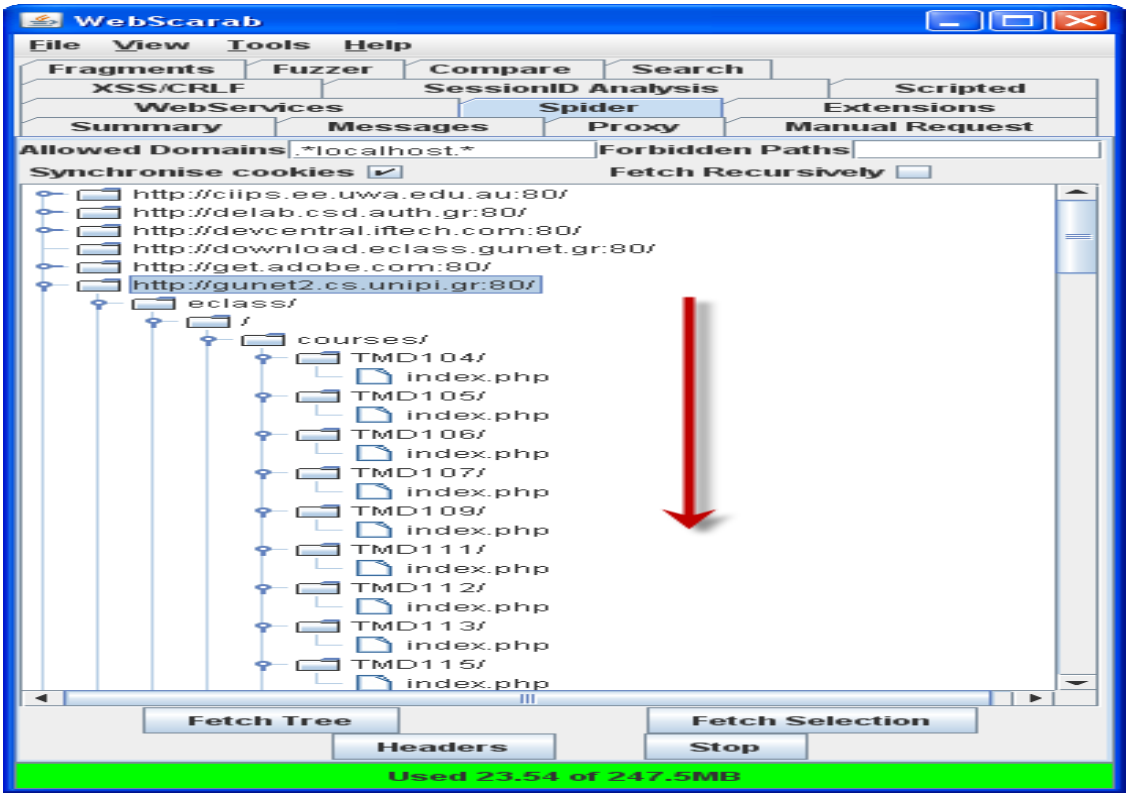
2.1 SPIDERS , ROBOTS , CRAWLERS

Με την πρώτη επίσκεψή μας στο eClass το Spider ενημερώνεται , όπως επίσης σε κάθε περαιτέρω αίτημά μας προς τον server , αφήνοντας μας ν' αποφασίσουμε εμείς σε ποιούς κόμβους επιθυμούμε την περαιτέρω ανίχνευση πόρων (φύλλων του δένδρου) επιλέγοντας έναν κόμβο και με το Fetch Tree ανιχνεύει από τον επιλεγμένο κόμβο και κάτω ή αν θέλουμε ανίχνευση μόνο για ένα συγκεκριμένο κόμβο επιλέγουμε το Fetch Selection.

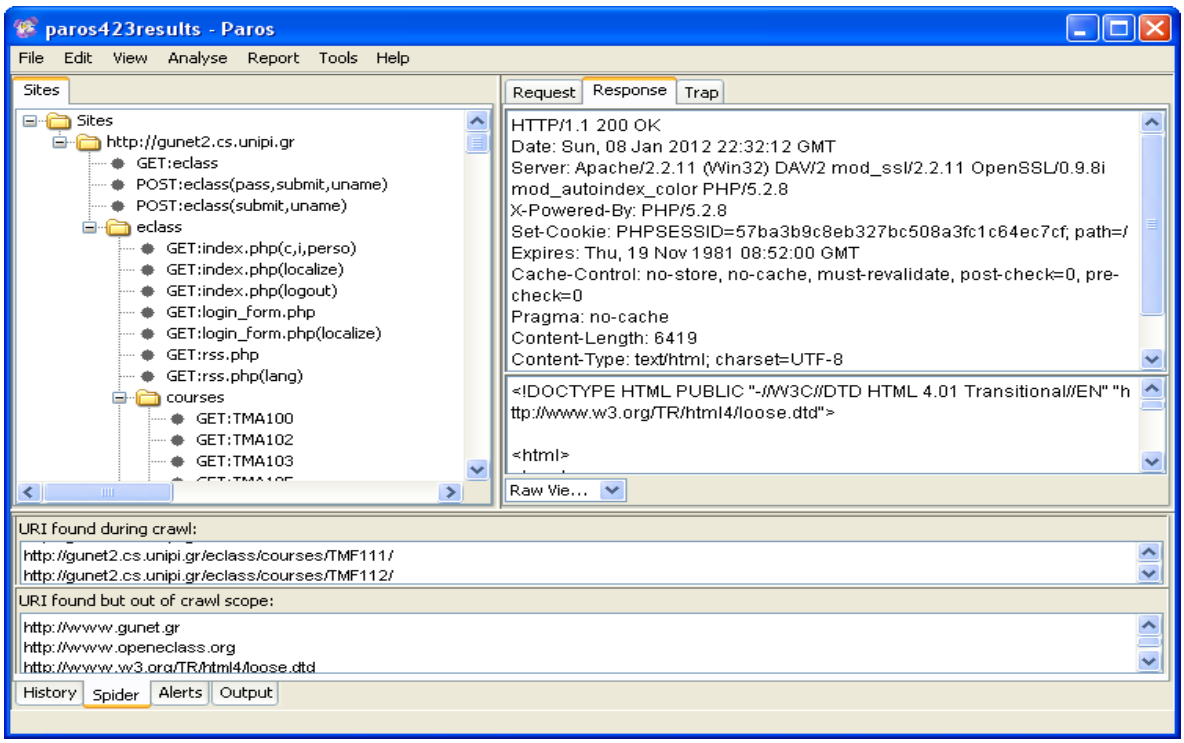


Εικόνα 2.1α. Αξιοποίηση του Spider plugin για τον προσδιορισμό links, πόρων, παραμέτρων.

Παρατηρούμε ότι μπορούμε να έχουμε πλήρη εικόνα των πόρων στο directory: /eclass/modules/auth/ , όπως επίσης και στο /eclass/modules/search (πάλι με το spider plugin). Παρακάτω (2.5 Applications Discovery) έχει εντοπιστεί μέσω Google η δυνατότητα εμφάνισης περιεχομένων διαφόρων directories, όπως και η δυνατότητα μετάβασης και εμφάνισης του parent directory.

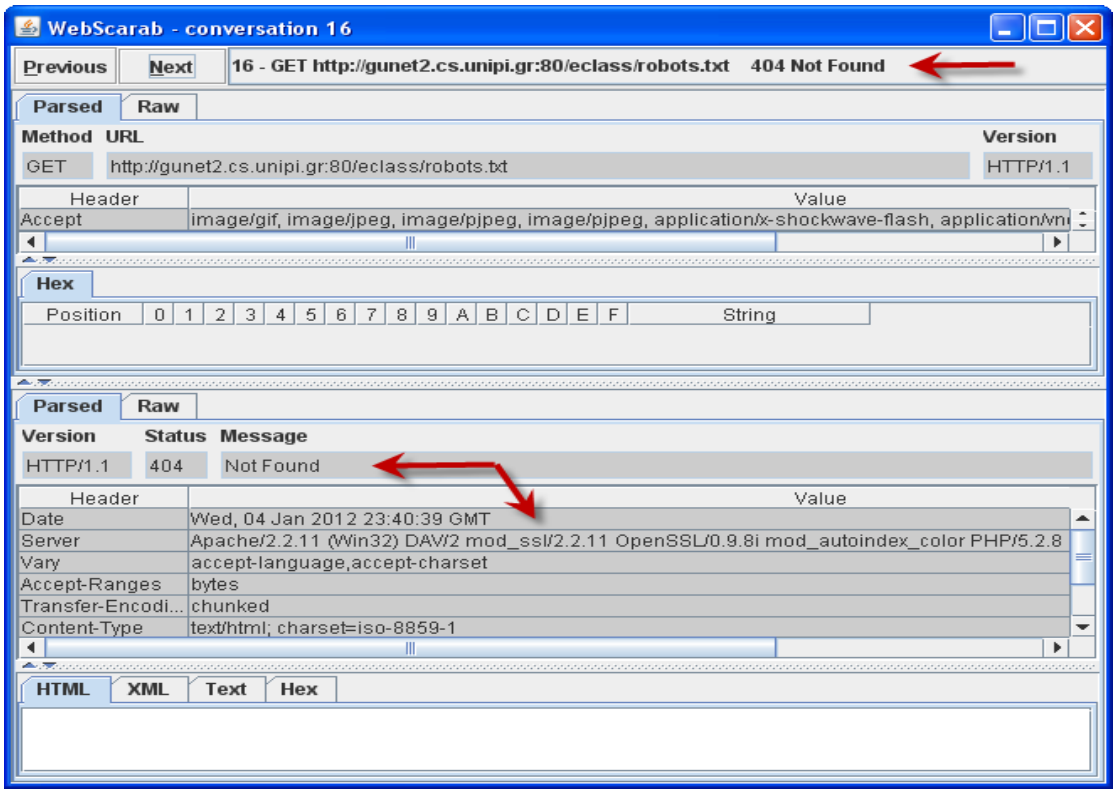


Εικόνα 2.1β . Καταγραφή των links με το **spider** επίσης του WebScarab.



Εικόνα 2.1γ. Καταγραφή των links με το spider του Paros interception proxy.Δεξιά βρίσκονται οι επικεφαλίδες αιτήματος και απόκρισης της επιλογής μας αριστερά.

Ελέγχουμε για την ύπαρξη του αρχείου robots.txt (Robots Exclusion Protocol), που επηρεάζει την καταγραφή του περιεχομένου του ιστότοπου από μηχανές αναζήτησης, διότι σε αυτό καθορίζονται οι περιοχές (directories), που δεν θα πρέπει να καταγραφούν τα περιεχόμενά τους. Αυτό το αρχείο ταυτόγχρονα είναι και πηγή πληροφοριών για έναν επιτιθέμενο, οδηγώντας τον στις περιοχές που πιθανώς περιέχουν σημαντικές πληροφορίες στην προσπάθειά τους για διείσδυση. Όπως φαίνεται στις εικόνες 2.1δ και 2.1ε δεν υπάρχει στον ιστότοπο αρχείο robots.txt. Αυτό σημαίνει. ότι όλες οι μηχανές αναζήτησης μπορούν να αποθηκεύουν ότι βρίσκουν στον ιστότοπο και να το επιλέγουν με τα δικά τους κριτήρια. Ένας hacker μπορεί να ψάξει στα αποθηκευμένα αντικείμενα στις μηχανές αναζήτησης για να εντοπίσει αυτά που ενδεχομένως βρίσκονται εμπιστευτικές πληροφορίες για την εφαρμογή.

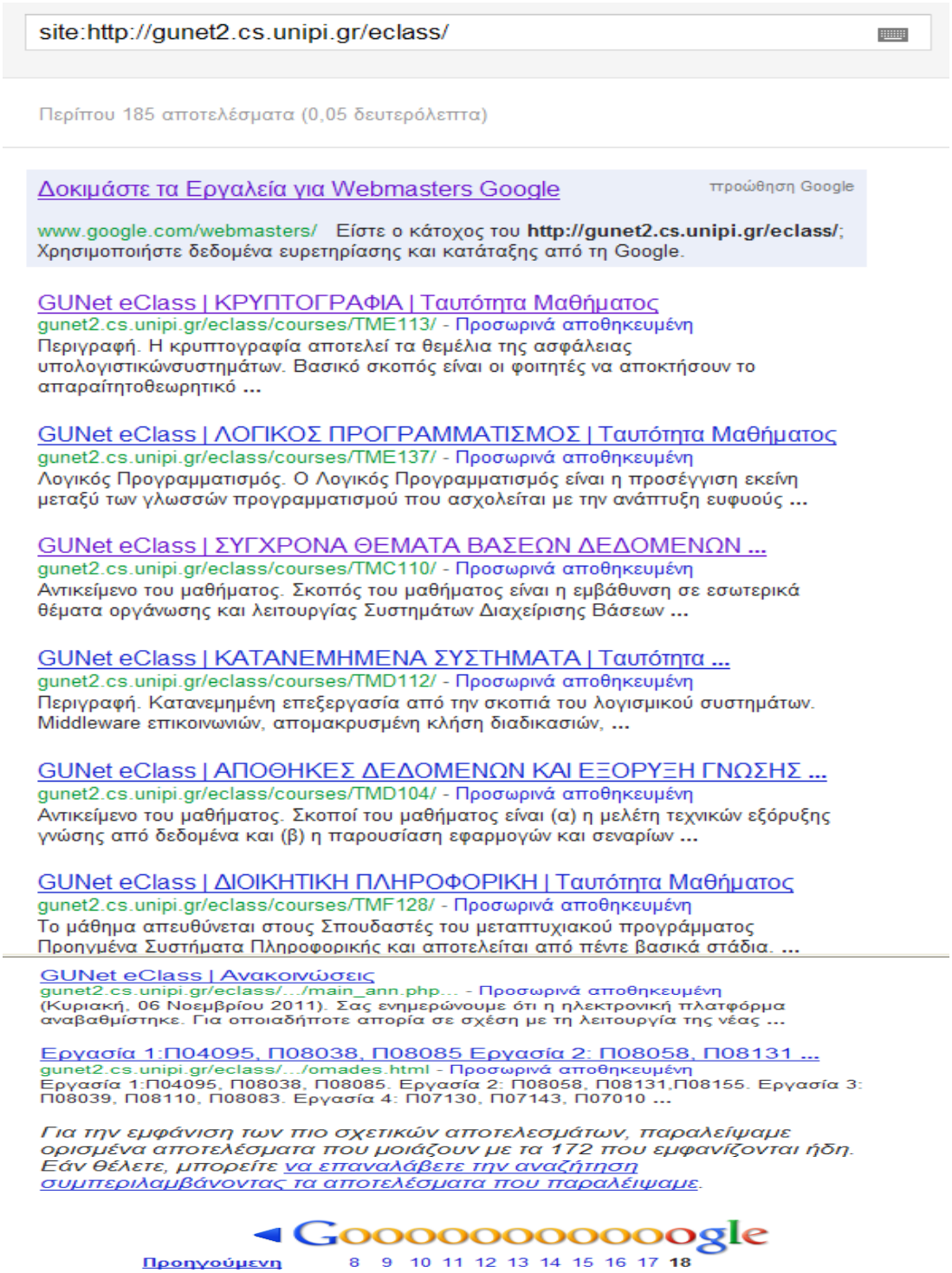


Εικόνα 2.1δ Καταγραφή απόκρισης μέσω του WebScarab στο αίτημα για το robots.txt

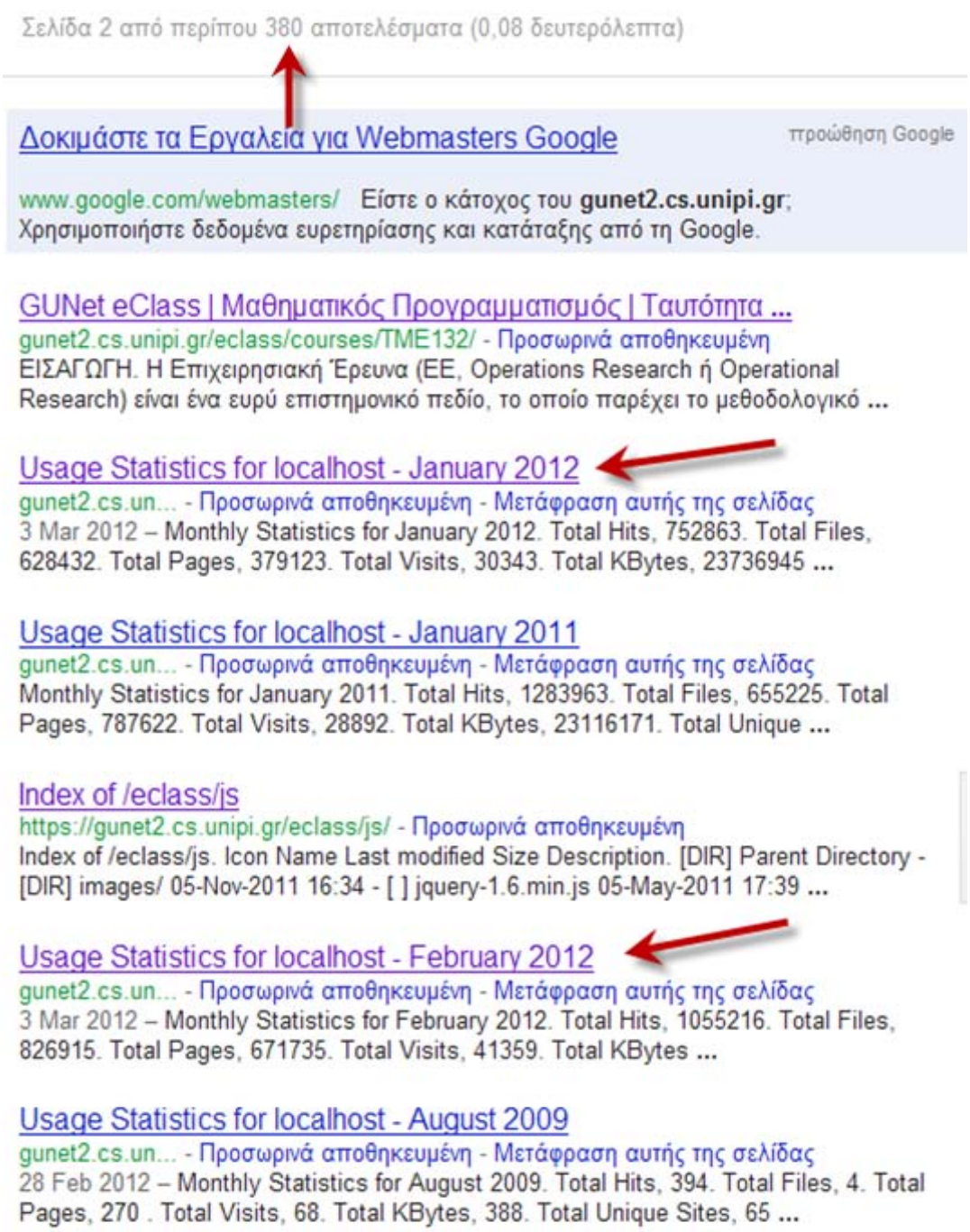
Εικόνα 2.1ε Απόκριση του Internet Explorer στο αίτημα για το robots.txt

2.2 SEARCH ENGINE DISCOVERY / RECONNAISSANCE

Το Google έχει καταγράψει 380 αντικείμενα (δεν περιλαμβάνει αυτά που προσδιορίζει σαν παρόμοια) για την εφαρμογή, τα οποία εμφάνισε με το **site:http://gunet2.cs.unipi.gr/eclass/.**

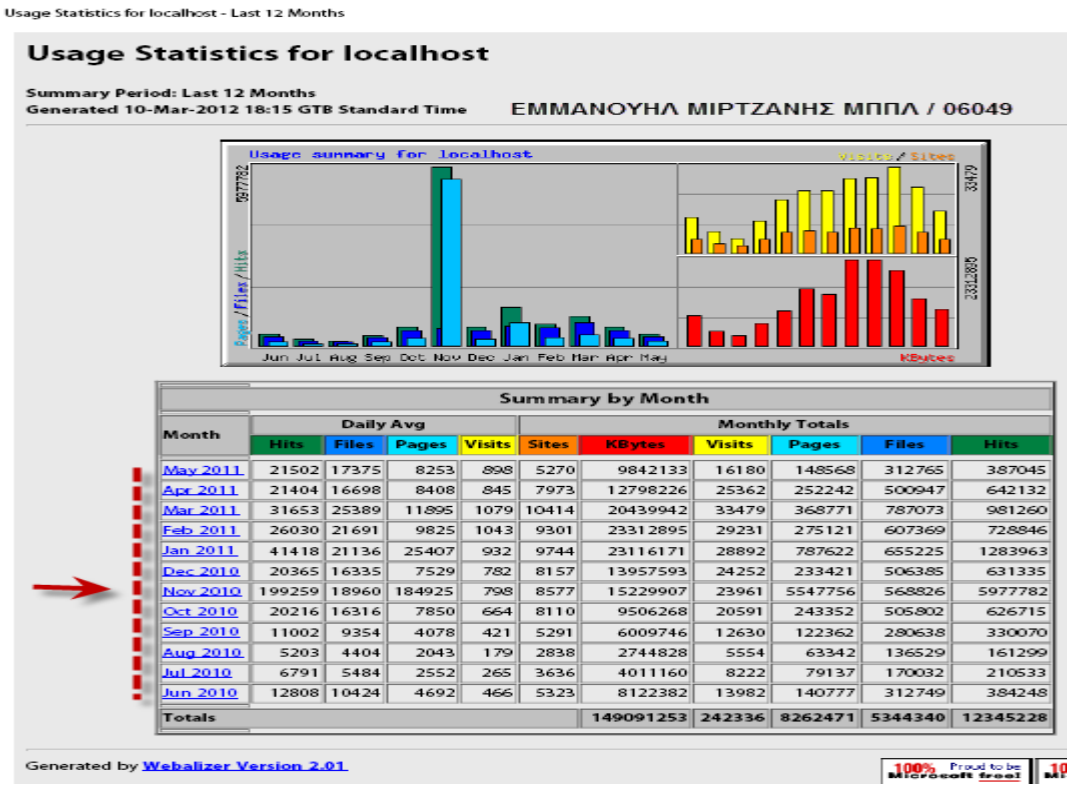


Εικόνα 2.2α Τα αντικείμενα που έχει καταγράψει το Google για την εφαρμογή



Εικόνα 2.2β Εντοπισμός καταγραφής από την Google Reports μηνιαίων στατιστικών

Παρατηρούμε στα βέλη ότι είναι διαθέσιμα τα **reports Usage Statistics January και February 2012**, το οποίο σημαίνει ότι έχουμε στη διαθεσή μας για περαιτέρω αξιοποίηση πληροφορίες π.χ. για τους πόρους που ζητήθηκαν περισσότερο (Urls) , τον πίνακα Referrers , για προσδιορισμό folders και αρχείων εφαρμογών όπως και **υπάρχοντα usernames διαχειριστών!**, όπως φαίνονται στις παρακάτω εικόνες.



Usage Statistics for localhost - Last 12 Months

Usage Statistics for localhost

Summary Period: Last 12 Months
Generated 10-Mar-2012 18:15 GTB Standard Time

ΕΜΜΑΝΟΥΗΛ ΜΙΡΤΖΑΝΗΣ ΜΠΠΛ / 06049

Usage summary for localhost

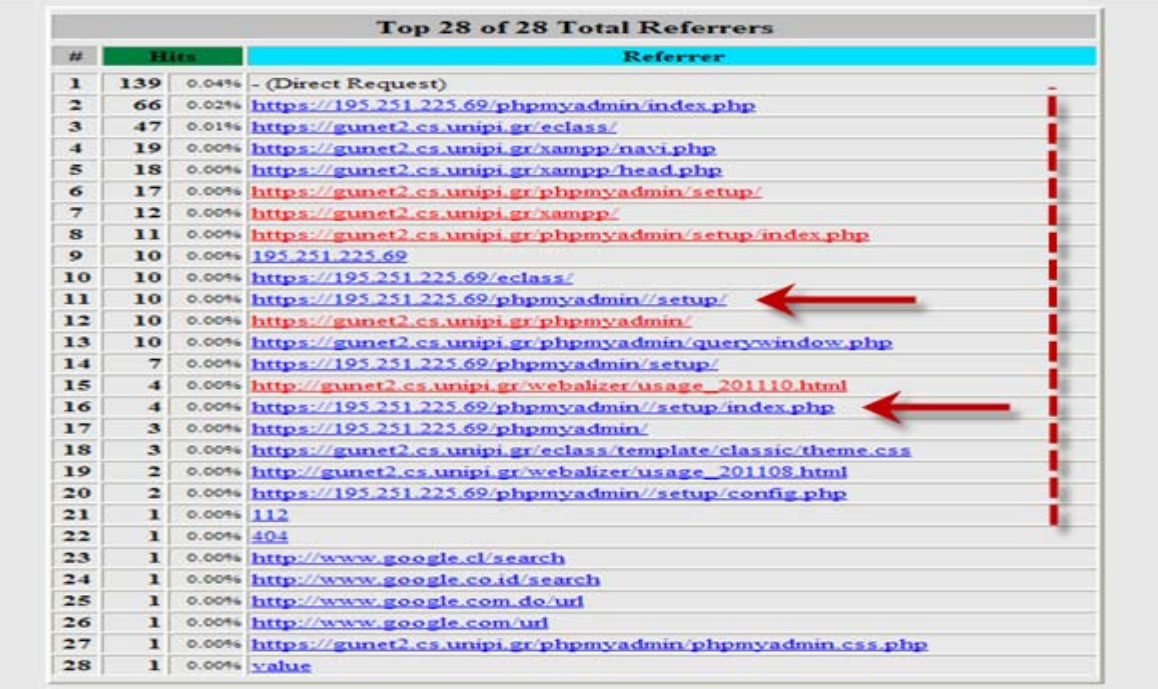
Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May

Summary by Month

Month	Daily Avg				Monthly Totals					
	Hits	Files	Pages	Visits	Sites	KBytes	Visits	Pages	Files	Hits
May 2011	21502	17375	8253	898	5270	9842133	16180	148568	312765	387045
Apr 2011	21404	16698	8408	845	7973	12798226	25362	252242	500947	642132
Mar 2011	31653	25389	11895	1079	10414	20439942	33479	368771	787073	981260
Feb 2011	26030	21691	9825	1043	9301	23312895	29231	275121	607369	728846
Jan 2011	41418	21136	25407	932	9744	23116171	28892	787622	655225	1283963
Dec 2010	20365	16335	7529	782	8157	13957593	24252	233421	506385	631335
Nov 2010	199259	18960	184925	798	8577	15229907	23961	5547756	568826	5977782
Oct 2010	20216	16316	7850	664	8110	9506268	20591	243352	505802	626715
Sep 2010	11002	9354	4078	421	5291	6009746	12630	122362	280638	330070
Aug 2010	5203	4404	2043	179	2838	2744828	5554	63342	136529	161299
Jul 2010	6791	5484	2552	265	3636	4011160	8222	79137	170032	210533
Jun 2010	12808	10424	4692	466	5323	8122382	13982	140777	312749	384248
Totals						149091253	242336	8262471	5344340	12345228

Generated by Webalizer Version 2.01

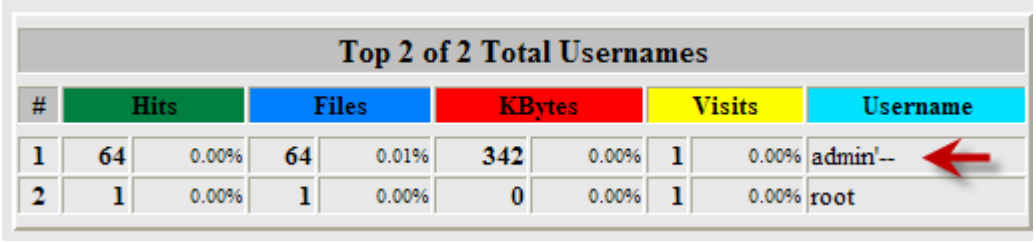
Εικόνα 2.2γ Εντοπισμός Report στατιστικών για **δωδεκάμηνο !!!** (βέλος)



Top 28 of 28 Total Referrers

#	Hits		Referrer
1	139	0.04%	- (Direct Request)
2	66	0.02%	https://195.251.225.69/phpmyadmin/index.php
3	47	0.01%	https://gunet2.cs.unipi.gr/eclass/
4	19	0.00%	https://gunet2.cs.unipi.gr/xampp/navi.php
5	18	0.00%	https://gunet2.cs.unipi.gr/xampp/head.php
6	17	0.00%	https://gunet2.cs.unipi.gr/phpmyadmin/setup/
7	12	0.00%	https://gunet2.cs.unipi.gr/xampp/
8	11	0.00%	https://gunet2.cs.unipi.gr/phpmyadmin/setup/index.php
9	10	0.00%	195.251.225.69
10	10	0.00%	https://195.251.225.69/eclass/
11	10	0.00%	https://195.251.225.69/phpmyadmin//setup/
12	10	0.00%	https://gunet2.cs.unipi.gr/phpmyadmin/
13	10	0.00%	https://gunet2.cs.unipi.gr/phpmyadmin/querywindow.php
14	7	0.00%	https://195.251.225.69/phpmyadmin/setup/
15	4	0.00%	http://gunet2.cs.unipi.gr/webalizer/usage_201110.html
16	4	0.00%	https://195.251.225.69/phpmyadmin//setup/index.php
17	3	0.00%	https://195.251.225.69/phpmyadmin/
18	3	0.00%	https://gunet2.cs.unipi.gr/eclass/template/classic/theme.css
19	2	0.00%	http://gunet2.cs.unipi.gr/webalizer/usage_201108.html
20	2	0.00%	https://195.251.225.69/phpmyadmin//setup/config.php
21	1	0.00%	112
22	1	0.00%	404
23	1	0.00%	http://www.google.cl/search
24	1	0.00%	http://www.google.co.id/search
25	1	0.00%	http://www.google.com.do/url
26	1	0.00%	http://www.google.com/url
27	1	0.00%	https://gunet2.cs.unipi.gr/phpmyadmin/phpmyadmin.css.php
28	1	0.00%	value

Εικόνα 2.2.δ Σε κάθε μήνα καταγράφονται τα 30 Top URL's όπως και τα top 28 Referrers για προσδιορισμό directories, αρχείων εφαρμογών.

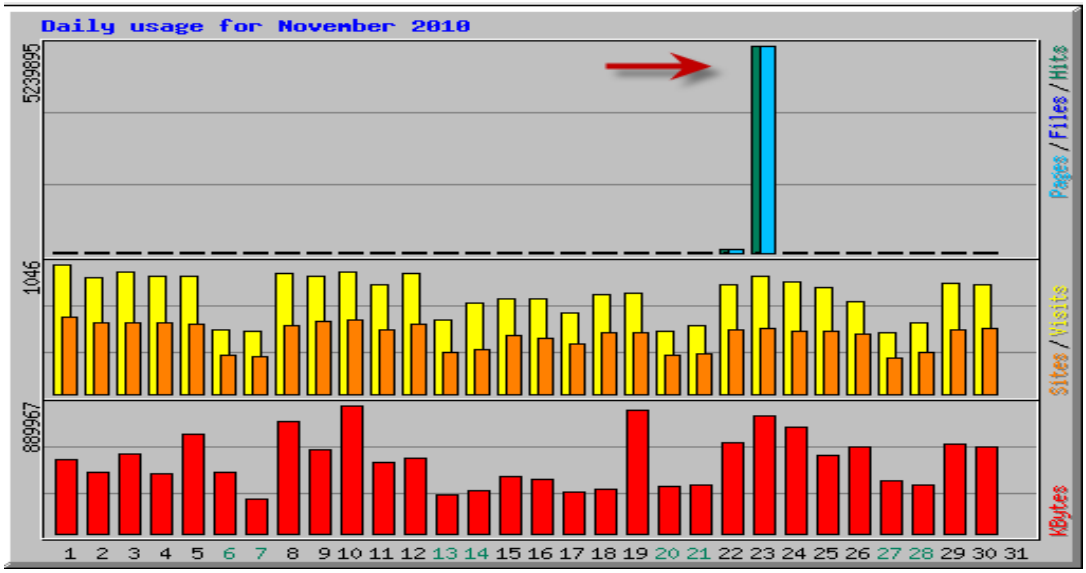


Top 2 of 2 Total Usernames

#	Hits		Files		KBytes		Visits		Username
1	64	0.00%	64	0.01%	342	0.00%	1	0.00%	admin'--
2	1	0.00%	1	0.00%	0	0.00%	1	0.00%	root

Εικόνα 2.2ε . Τμήμα από το Usage Statistics **usernames** !!! (βέλος, Νοέμβριος 2010)

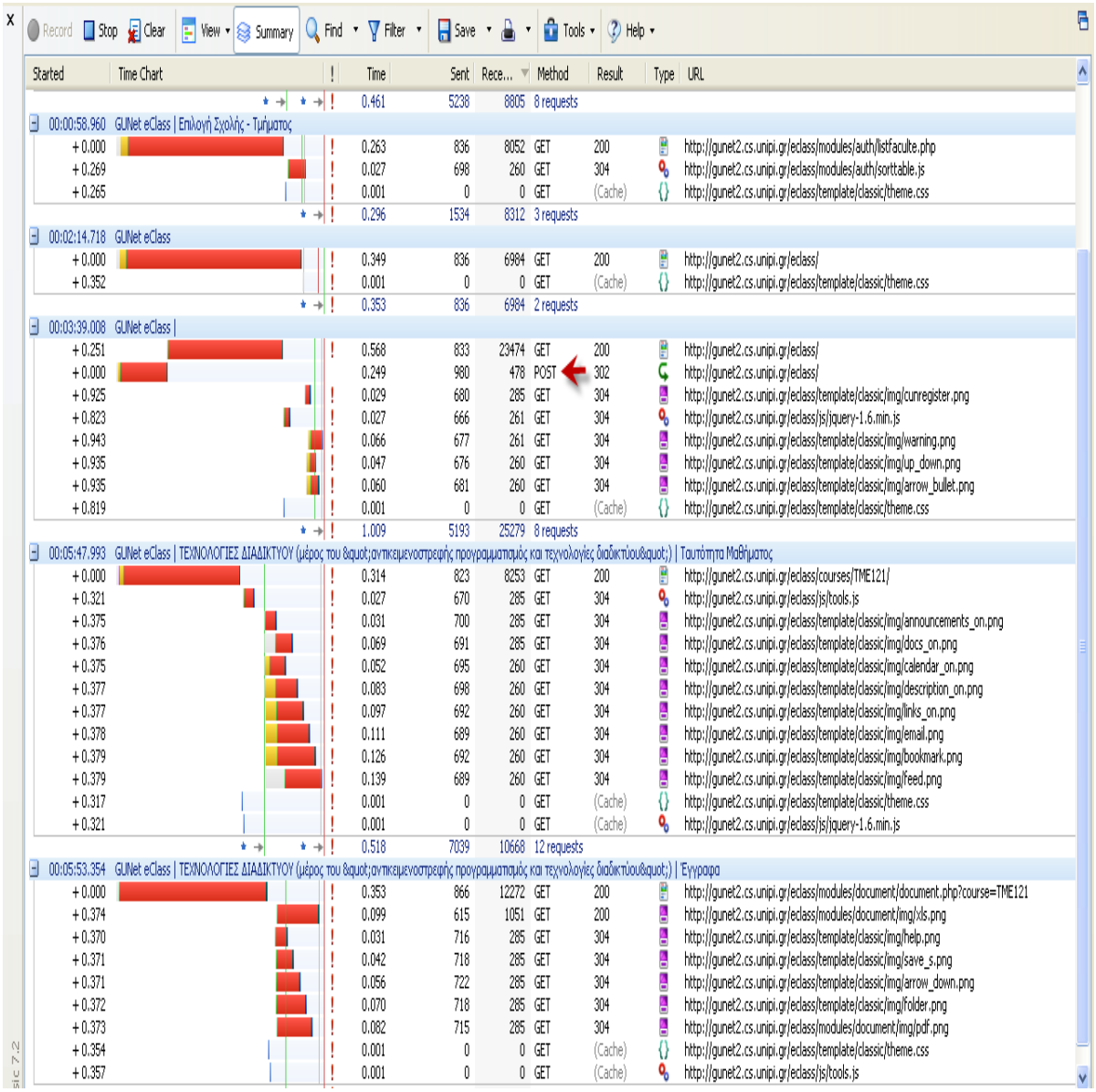
Στα usernames το βέλος δείχνει το admin'-- , που είναι χαρακτηριστικό SQL injection επίθεσης, δεδομένου ότι το admin , έχει παρατηρηθεί σε άλλα usage statistics σαν username.



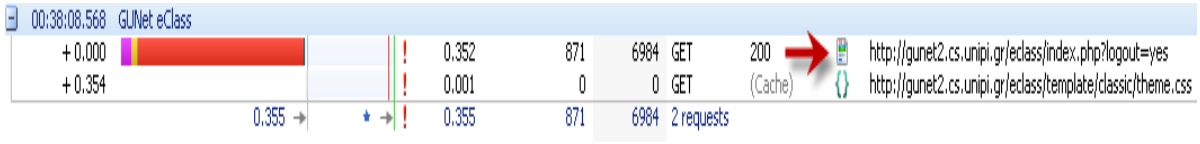
Εικόνα 2.2στ . Τμήμα από το Usage Statistics 23 Nov 2010, που δείχνει ασυνήθιστη ζήτηση σε σελίδες και hits , είτε από ενδεχόμενη δραστηριότητα του διαχειριστή,είτε από επίθεση ή ανίχνευση ιστότοπου με κάποιο εργαλείο .

2.3 IDENTIFY APPLICATION ENTRY POINTS

Όπως φαίνεται παρακάτω στην εικόνα 2.3α ,που πήραμε χρησιμοποιώντας το **httpwatch extension** του IE, το eClass χρησιμοποιεί για όλα τα requests την μέθοδο GET εκτός στην περίπτωση του login (3ο αίτημα , όπως δείχνει το βέλος) με μέθοδο POST με απάντηση που έχει status code 302 , γιατί κάνει redirection . Οι αποκρίσεις έχουν status code 200 ή 304 (not modified) , επειδή ο browser έχει αποθηκεύσει πιο πριν τα αντικείμενα των αντίστοιχων σελίδων. Στα URL's φαίνονται επίσης οι παράμετροι, όπου χρειάζονται, που χρησιμοποιεί το eClass σε κάθε GET αίτημα και αποτελούν σημεία εισόδου για την εφαρμογή και σημεία ελέγχου για έναν ελεγκτή , προκειμένου να προσδιορισθούν ενδεχόμενες ευπάθειες.

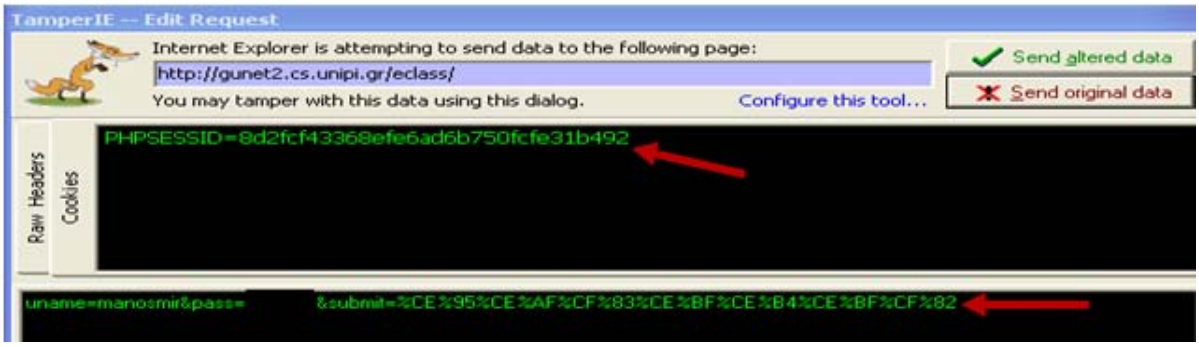


Εικόνα 2.3α . Καταγραφή αιτημάτων και αποκρίσεων με το **httpwatch extension** του IE.

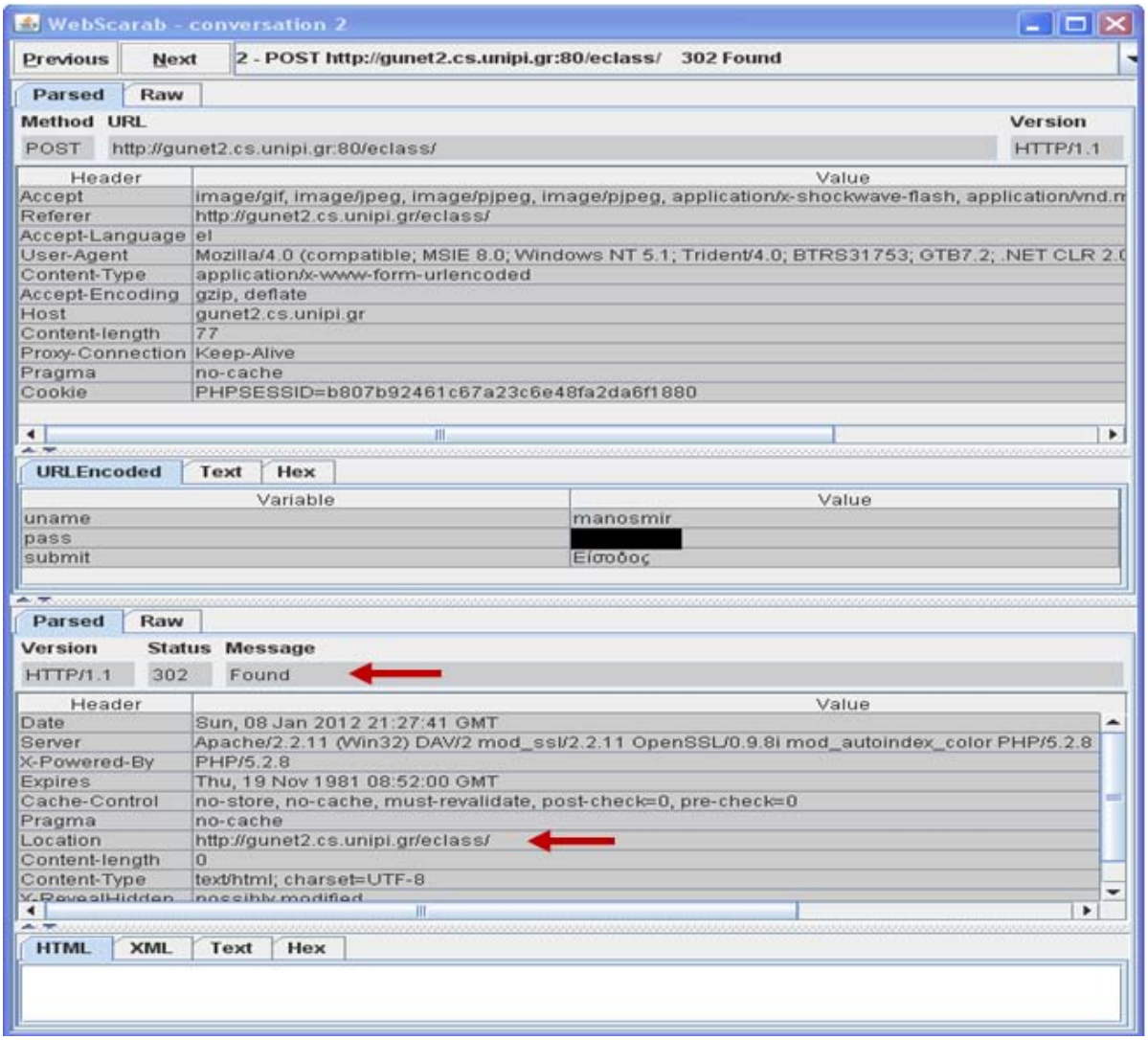


Εικόνα 2.3β . Καταγραφή αιτήματος logout και απόκρισης με το httpwatch extension του IE.

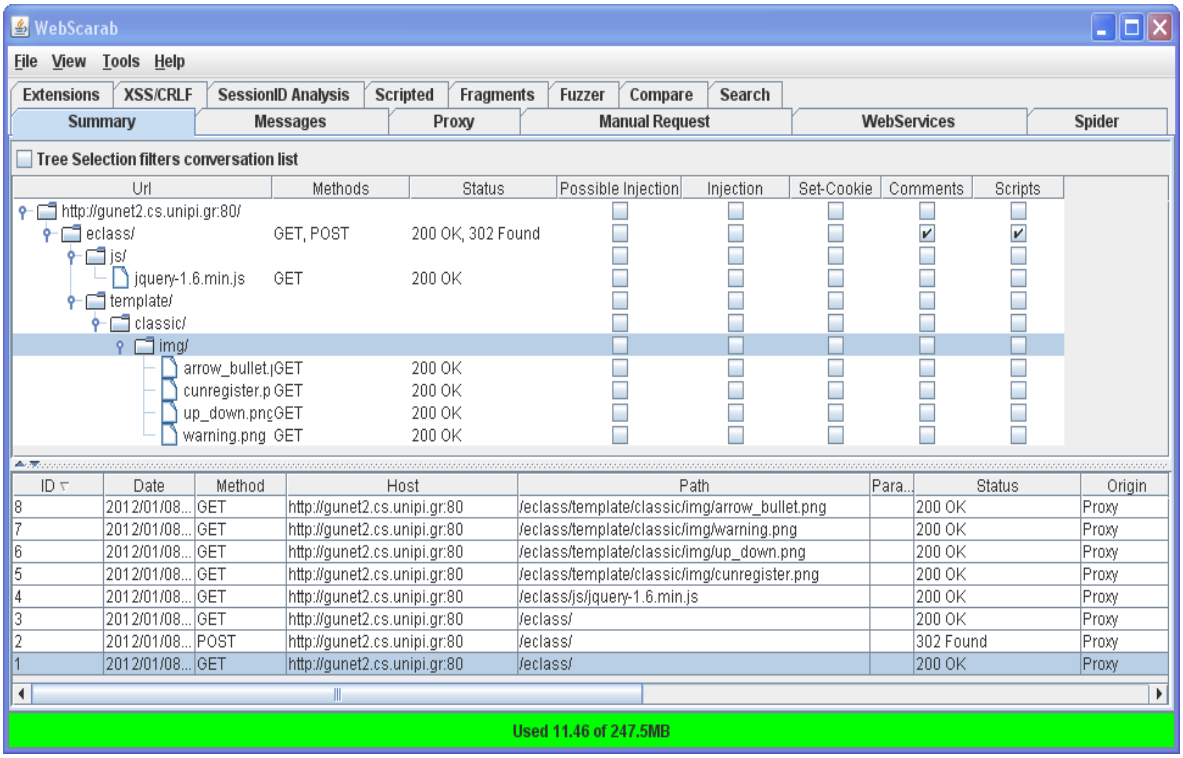
Ανεξάρτητα από το εργαλείο που θα χρησιμοποιηθεί, είναι μια καλή ιδέα να καταγραφούν όλα τα σημεία εισόδου με τις αντίστοιχες παραμέτρους σε ένα φύλλο Excel , ώστε να υπάρχει η δυνατότητα εύκολης εποπτείας του συνόλου των εισόδων (entry points ή gates) της εφαρμογής όπως αναφέρεται παρακάτω.



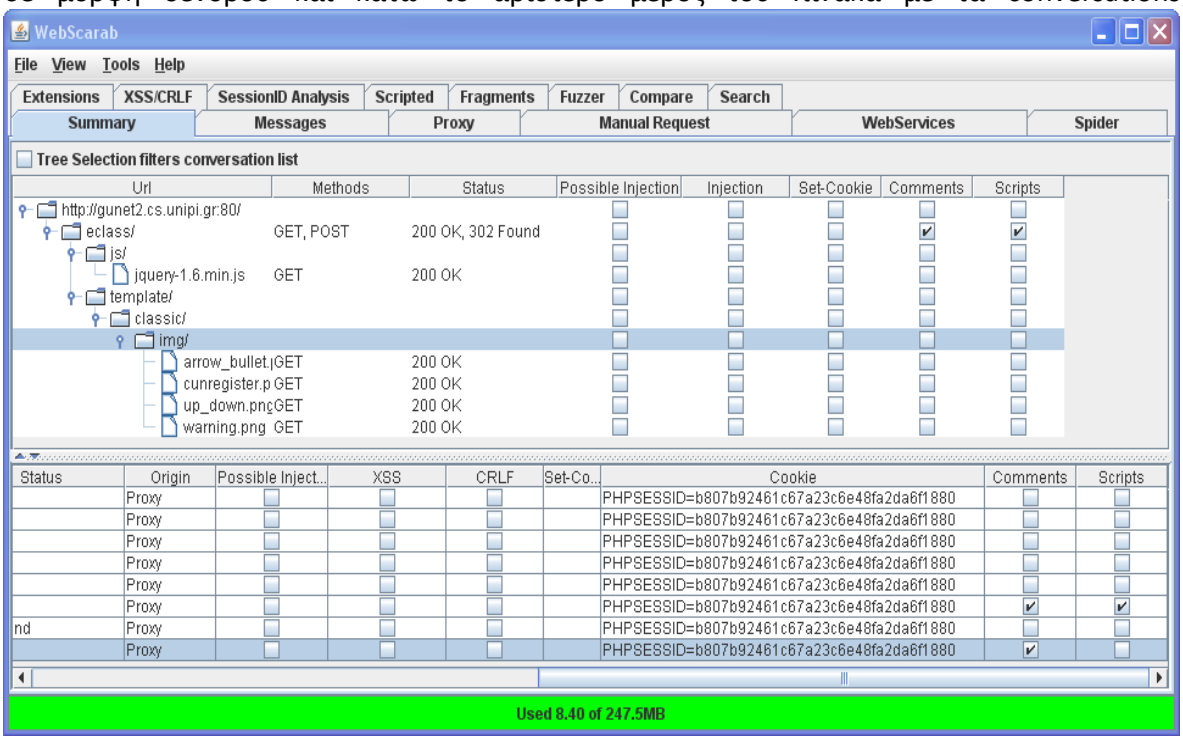
Εικόνα 2.3γ . Καταγραφή αιτήματος login με το TamperIE extension του IE , όπου εμφανίζονται sessionid , uname , pass και το submit με url encoding , στα οποία μπορούμε και να παρέμβουμε.



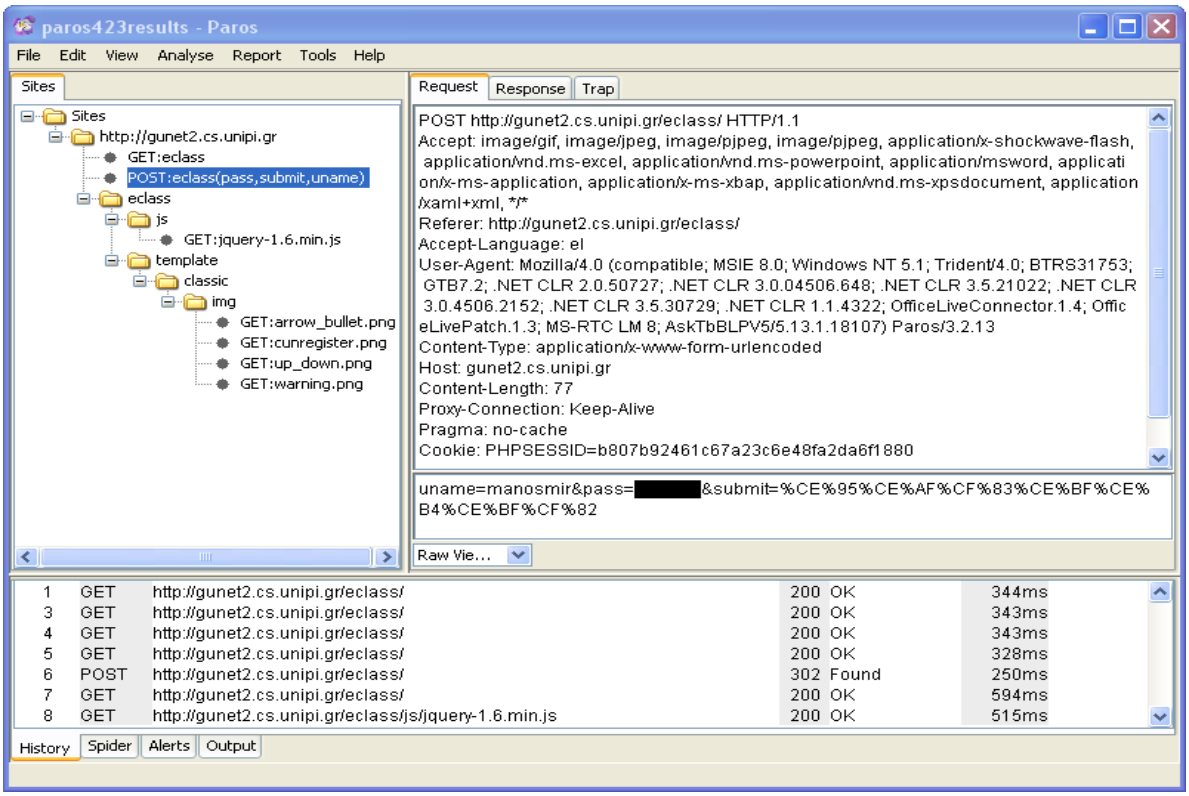
Εικόνα 2.3δ . Καταγραφή αιτήματος login και απόκρισης με το **WebScarab interception proxy**.



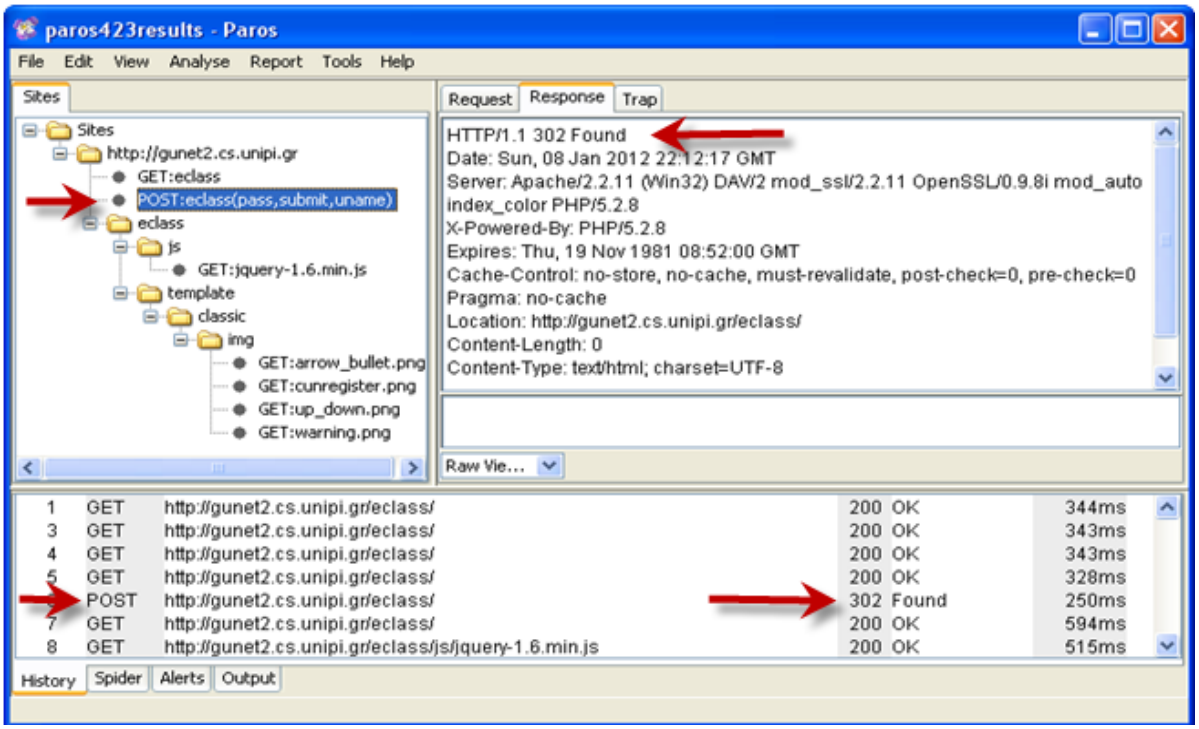
Εικόνα 2.3ε . Συνολική συνοπτική εικόνα αιτημάτων και αποκρίσεων με το WebScarab (πάνω σε μορφή δένδρου και κάτω το αριστερό μέρος του πίνακα με τα conversations).



Εικόνα 2.3στ . Συνολική συνοπτική εικόνα αιτημάτων και αποκρίσεων με το WebScarab (κάτω δεξί μέρος πίνακα με τα conversations) , όπου καταγράφονται οι συνομιλίες που περιλαμβάνουν comments ή Scripts , cookies όπως άλλωστε και στο πάνω μέρος στις στήλες.



Εικόνα 2.3ζ . Καταγραφή επίσκεψης και login (**Request**) με το Paros interception proxy. Δεξιά βρίσκονται οι επικεφαλίδες **του αιτήματος** , στο μέσον οι παράμετροι του αιτήματος πάνω αριστερά οι επισκέψεις σε μορφή δένδρου και κάτω στον πίνακα οι συνομιλίες.



Εικόνα 2.3η . Καταγραφή επίσκεψης και login με το Paros interception proxy. Δεξιά βρίσκονται οι επικεφαλίδες **της απόκρισης (Response)** στο αίτημα για login.

Ο στόχος μας είναι, να δημιουργήσουμε έναν χάρτη της εφαρμογής με όλα τα σημεία πρόσβασης (gates) σε αυτήν, καταγράφοντας όνομα σελίδας, full path, αν η σελίδα περιέχει authentication, αν απαιτείται SSL , μέθοδο αιτημάτων, επικεφαλίδες, παραμέτρους, σχόλια, απάντηση, επικεφαλίδες, cookies, sessionid. Μπαίνοντας στην αρχική σελίδα του ιστότοπου και επιλέγοντας το Spider plugin του WebScarab, βλέπουμε ένα παράθυρο σαν και αυτό της εικόνας 2.1β. Επιλέγοντας την διεύθυνση του ιστότοπου και κάνοντας κλικ στο Fetch Tree το πρόγραμμα εντοπίζει όλα τα links από τον επιλεγμένο κόμβο και κάτω, τα οποία όπως φαίνονται στην εικόνα οδηγούν σε σελίδες php (φύλλα του δένδρου). Κάθε κόμβο που επισκεπτόμαστε μπορούμε επιλέγοντας το Fetch Selection να εντοπίσουμε όλα τα links που περιέχονται σε αυτόν. Έτσι μπορούμε να δημιουργήσουμε τον συνολικό χάρτη της εφαρμογής, τον οποίο μπορούμε να καταγράψουμε σε φύλλο excel για να έχουμε συγκεντρωτική εικόνα όλων των συνομιλιών αλλά και να καταγράψουμε την δομή σχηματισμού του sessionid με σκοπό την ανακάλυψη της λογικής σχηματισμού του, έτσι ώστε να γίνει εφικτή η παραβίαση του μηχανισμού αυθεντικοποίησης σε επόμενο έλεγχο.

2.4 TESTING FOR WEB APPLICATION FINGERPRINT

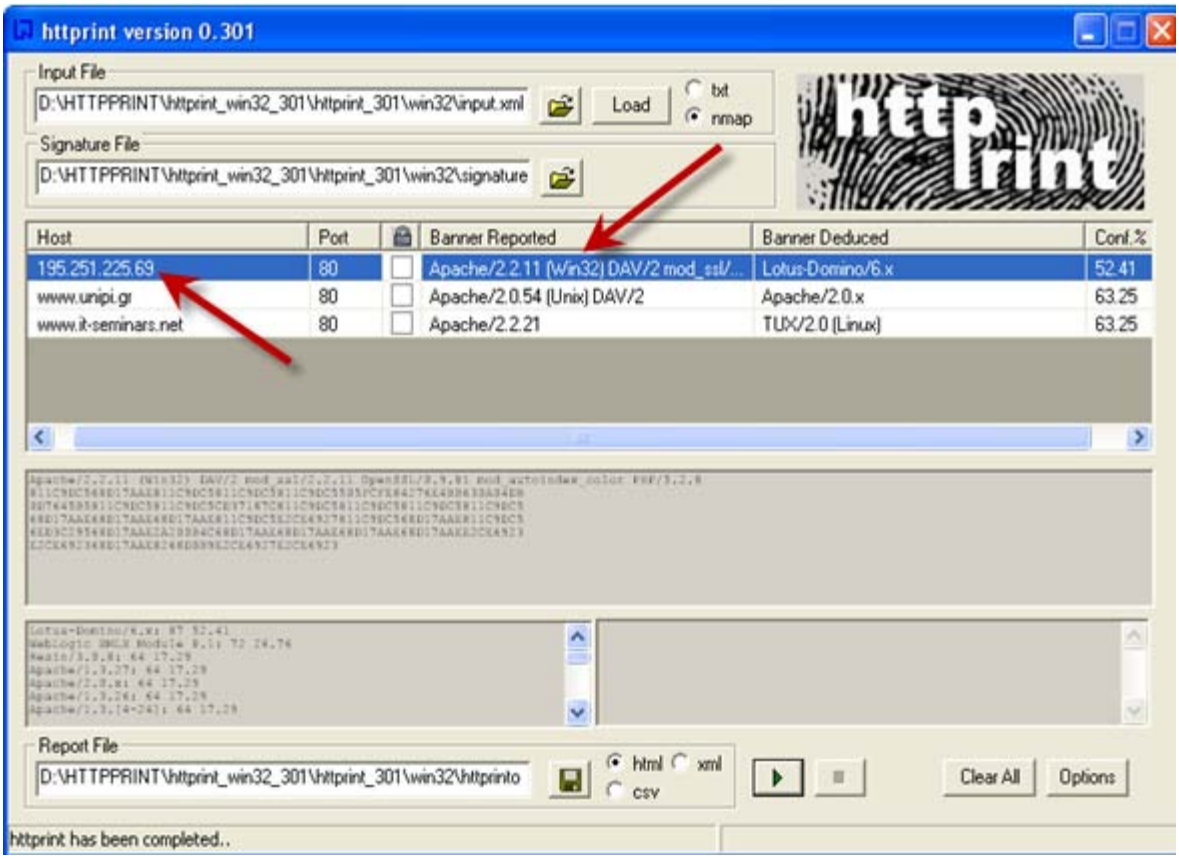
Κάθε απάντηση από τον web server περιέχει την επικεφαλίδα Server, όπου αναφέρεται ο web Server στην Εικόνα 2.3δ με το WebScarab και με το Paros εδώ:

Μπορούμε να πάρουμε αποτύπωμα με το **Netcraft** που προσφέρεται online:

Εικόνα 2.4α . Αποτύπωμα για το gunet.cs.unipi.gr με το online netcraft.

Στην εικόνα 2.4α του netcraft παίρνουμε το αποτύπωμα, που καταγράφεται στο κάτω μέρος στο Hosting History. Διαβάζουμε το OS : windows server 2008 και αμέσως δεξιά τον Web Server.

Το **HttpPrint** μας δίνει την παρακάτω απάντηση για αποτύπωμα :



Εικόνα 2.4β . Αποτύπωμα για το gunet.cs.unipi.gr με το HttpPrint.

Οι πληροφορίες από το αποτύπωμα χρησιμοποιούνται περαιτέρω για αναζήτηση καταγεγραμμένων ευπαθειών του Web Server , της έκδοσης SSL , PHP και του OS .

2.5 APPLICATION DISCOVERY

Μετά από έλεγχο (εικόνα 2.5α επόμενη σελίδα επάνω) στην IP 195.251.225.69 του ιστότοπου αντιστοιχεί **ένα όνομα, το gunet2.cs.unipi.gr**, που με redirection οδηγεί στο /eclass, όπου είναι εγκατεστημένη η πλατφόρμα eClass. Με site:gunet2.cs.unipi.gr είχαμε μέσω Google καταγράψει ότι μόνο η εφαρμογή eClass για χρήστες είναι εγκατεστημένη , όπως έχουμε παρατηρήσει και στην παράγραφο 2.2. Με το Netcraft και στο ερώτημα “what’s that site running” παίρνουμε την αποάντηση εικόνα 2.5β, την οποία άλλωστε είχαμε δεί και στην εικόνα 2.4α. Έλεγχος με το **nmap** μας παρέχει τα αποτελέσματα της εικόνας 2.5γ η οποία μας συμπληρώνει την εικόνα μέσω των ενεργών ports (και τις αντίστοιχες υπηρεσίες) , 80/tcp για τους χρήστες του eClass και το 443/tcp για την διαχείριση του web server από απόσταση , ενώ

όπως θα δούμε το eClass δεν χρησιμοποιεί το 443/tcp (https) ούτε για την αυθεντικοποίηση των χρηστών του eclass (αρνητική επιλογή από άποψη ασφάλειας). Μέσω του Google στην παράγραφο 2.2 έχουμε διαπιστώσει την ύπαρξη μόνο της εφαρμογής eclass στον web server, πληροφορίες του οποίου έχουμε στην παράγραφο 2.4 αλλά και στην εικόνα 2.5β. Πληροφορίες για τα ports και τις αντίστοιχες υπηρεσίες/εφαρμογές παίρνουμε από το Nmap στις εικόνες 2.5γ και 2.5δ. Στην εικόνα 2.5ε έχουμε τις πληροφορίες για τα DNS Records , ενώ η εικόνα 2.5στ, από τα καταγεγραμμένα αντικείμενα του Google, μας δείχνει ότι είναι δυνατή η διερεύνηση των directories για εντοπισμό αντικειμένων της εφαρμογής και του web server.

IP Information - 195.251.225.69

IP address:	195.251.225.69
Reverse DNS:	gunet2.cs.unipi.gr.
Reverse DNS authenticity:	[Verified]
ASN:	12402
ASN Name:	UOPIRAEUS (University of Piraeus)
IP range connectivity:	5
Registrar (per ASN):	RIPE
Country (per IP registrar):	GR [Greece]
Country Currency:	EUR [euros]
Country IP Range:	195.251.0.0 to 195.251.255.255
Country fraud profile:	Normal
City (per outside source):	Unknown
Country (per outside source):	-- []
Private (internal) IP?	No
IP address registrar:	whois.ripe.net
Known Proxy?	No
Link for WHOIS:	195.251.225.69

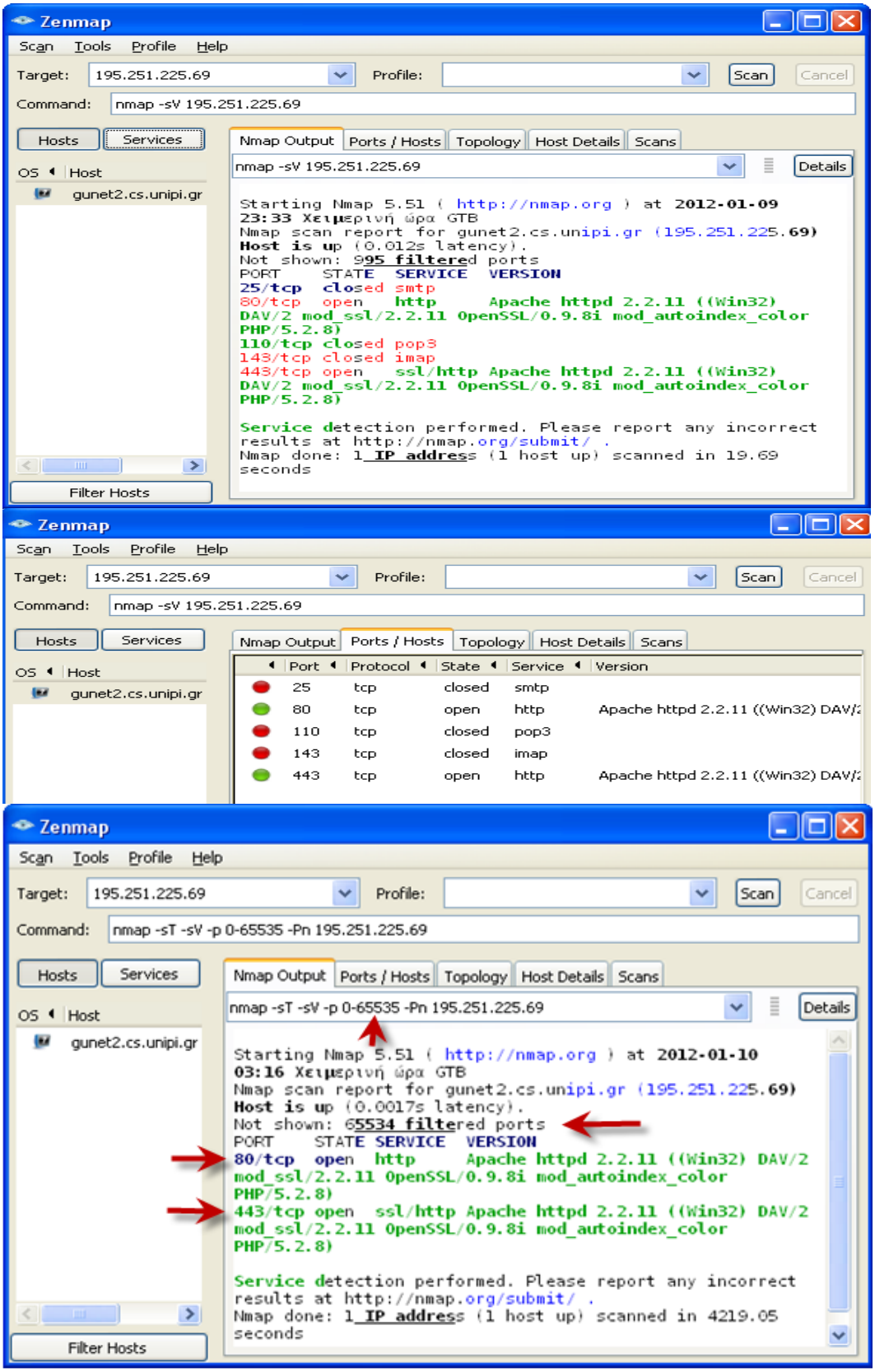
Εικόνα 2.5α Αντιστοίχιση IP και domain name

OS, Web Server and Hosting History for gunet2.cs.unipi.gr

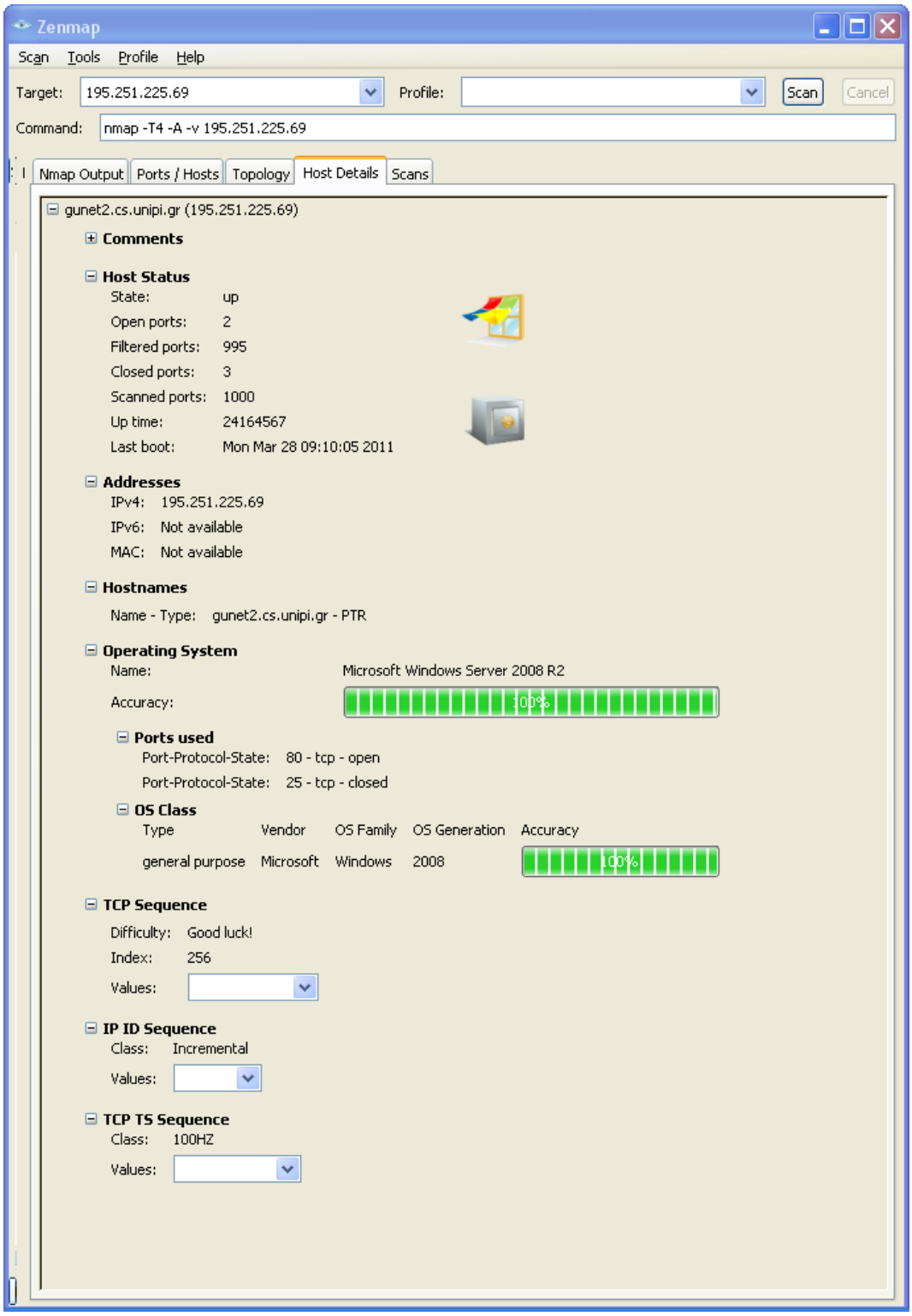
http://gunet2.cs.unipi.gr was running Apache on Windows Server 2008
when last queried at 24-Dec-2011 00:27:05 GMT - refresh now Site Report FAQ
Try out the Netcraft Toolbar!

OS	Server	Last changed	IP address	Netblock Owner
Windows Server 2008	Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i mod_autoindex_color PHP/5.2.8	24-Dec-2011	195.251.225.69	University of Piraeus

Εικόνα 2.5.β Hosting History μέσω του Netcraft για το gunet2.cs.unipi.gr



Εικόνα 2.5γ . Καταγραφή για πόρτες και αντίστοιχες υπηρεσίες (65534 filtered ports).



Εικόνα 2.5δ Σ' αυτό το report μας ενημερώνει ότι οι υπόλοιπες πόρτες φιλτράρονται (εκτός των ανοικτών 80 , 443 και 3 κλειστών).

DNS records

name	class	type	data	time to live
gunet2.cs.unipi.gr	IN	MX	preference: 5 exchange: gunet2.cs.unipi.gr	500s (00:08:20)
gunet2.cs.unipi.gr	IN	A	195.251.225.69	500s (00:08:20)
unipi.gr	IN	SOA	server: ns.unipi.gr email: root.unipi.gr serial: 2011120205 refresh: 1200 retry: 7200 expire: 2419200 minimum ttl: 86400	500s (00:08:20)
unipi.gr	IN	NS	sns0.grnet.gr	500s (00:08:20)
unipi.gr	IN	NS	sns1.grnet.gr	500s (00:08:20)
unipi.gr	IN	NS	ns.unipi.gr	500s (00:08:20)
unipi.gr	IN	MX	preference: 5 exchange: mailhost.unipi.gr	500s (00:08:20)
69.225.251.195.in-addr.arpa	IN	PTR	gunet2.cs.unipi.gr	86400s (1.00:00:00)

Traceroute

Tracing route to **gunet2.cs.unipi.gr [195.251.225.69]**...

IP address: 195.251.225.69
Host name: gunet2.cs.unipi.gr
195.251.225.69 is from Greece(GR) in region Western Europe

TraceRoute to 195.251.225.69 [gunet2.cs.unipi.gr]

Hop	(ms)	(ms)	(ms)	IP Address	Host name
1	0	0	0	206.123.64.46	-
2	0	0	0	8.9.232.73	xe-5-3-0.edge3.dallas1.level3.net
3	2	0	0	4.69.145.254	vlan90.csw4.dallas1.level3.net
4	0	0	0	4.69.151.170	ae-93-93.ebr3.dallas1.level3.net
5	20	20	20	4.69.134.22	ae-7-7.ebr3.atlanta2.level3.net
6	33	33	33	4.69.132.86	ae-2-2.ebr1.washington1.level3.net
7	33	33	34	4.69.134.142	ae-91-91.csw4.washington1.level3.net
8	33	33	33	4.69.134.157	ae-92-92.ebr2.washington1.level3.net
9	114	113	113	4.69.137.49	ae-41-41.ebr2.paris1.level3.net
10	120	120	120	4.69.143.133	ae-45-45.ebr1.frankfurt1.level3.net
11	260	132	136	4.69.135.33	ae-6-6.car1.vienna1.level3.net
12	131	131	131	212.73.203.102	-
13	180	180	180	62.40.112.166	as1.rt1.ath2.gr.geant2.net
14	182	182	182	62.40.124.90	grnet-gw.rt1.ath2.gr.geant.net
15	182	182	182	195.251.24.134	clientrouter.unipi.eie-2.access-link.grnet.gr
16	181	181	182	195.251.225.69	gunet2.cs.unipi.gr

Trace complete

Retrieving DNS records for **gunet2.cs.unipi.gr**...
DNS servers
sns0.grnet.gr
sns1.grnet.gr
ns.unipi.gr [195.251.229.5]

Answer records

gunet2.cs.unipi.gr	A	195.251.225.69		500s
gunet2.cs.unipi.gr	MX	preference:	5	500s
		exchange:	gunet2.cs.unipi.gr	

Authority records

cs.unipi.gr	NS	ns.unipi.gr	500s
cs.unipi.gr	NS	sns0.grnet.gr	500s

Εικόνα 2.5ε DNS records για το gunet2.cs.unipi.gr

Index of /eclass/js/tinymce/jscripts/tiny_mce/plugins

Name	Last modified	Size	Description
Parent Directory		-	
advhr/	05-Nov-2011 16:34	-	
advimage/	05-Nov-2011 16:34	-	
advlink/	05-Nov-2011 16:34	-	
advlist/	05-Nov-2011 16:34	-	
autolink/	05-Nov-2011 16:34	-	
autoresize/	05-Nov-2011 16:34	-	
autosave/	05-Nov-2011 16:34	-	
bbcode/	05-Nov-2011 16:34	-	
contextmenu/	05-Nov-2011 16:34	-	
directionality/	05-Nov-2011 16:34	-	
emotions/	05-Nov-2011 16:34	-	
example/	05-Nov-2011 16:34	-	
fullpage/	05-Nov-2011 16:34	-	
fullscreen/	05-Nov-2011 16:34	-	
iespell/	05-Nov-2011 16:34	-	
inlinepopups/	05-Nov-2011 16:34	-	
insertdatetime/	05-Nov-2011 16:34	-	
layer/	05-Nov-2011 16:34	-	
legacyoutput/	05-Nov-2011 16:34	-	
lists/	05-Nov-2011 16:34	-	
media/	05-Nov-2011 16:34	-	
nonbreaking/	05-Nov-2011 16:34	-	
noneditable/	05-Nov-2011 16:34	-	
pagebreak/	05-Nov-2011 16:34	-	
paste/	05-Nov-2011 16:34	-	

Index of /eclass/js/tinymce

Name	Last modified	Size	Description
Parent Directory		-	
changelog.txt	15-Apr-2011 17:14	122K	
examples/	15-Apr-2011 17:14	-	
jscripts/	05-Nov-2011 16:34	-	

Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i mod_autoindex_color PHP/5.2.8 Server at gunet2.cs.unipi.gr Port 443

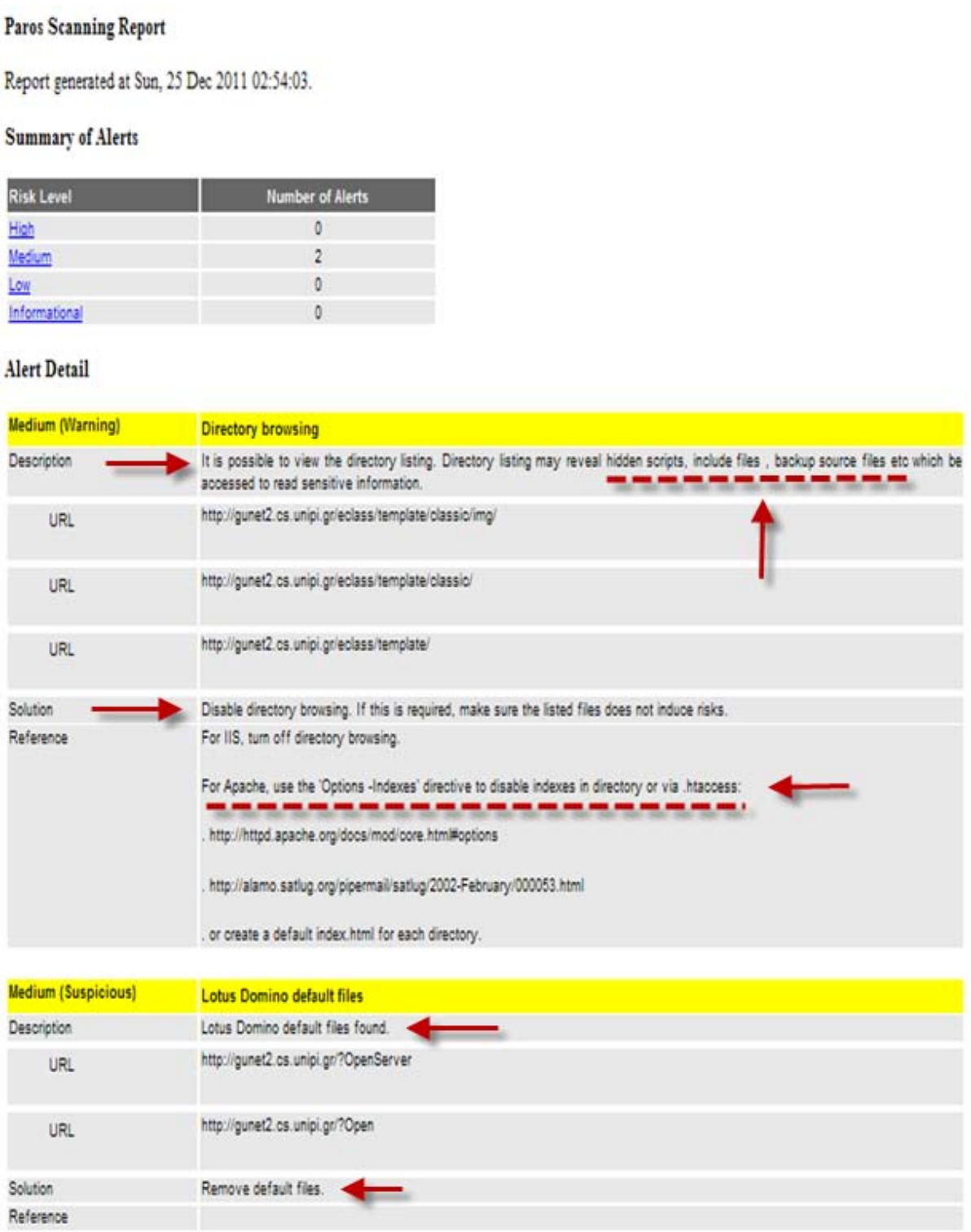
Index of /eclass/js/tinymce/jscripts/tiny_mce

Name	Last modified	Size	Description
Parent Directory		-	
langs/	05-Nov-2011 16:34	-	
license.txt	15-Apr-2011 17:14	26K	
plugins/	05-Nov-2011 16:34	-	
themes/	05-Nov-2011 16:34	-	
tiny_mce.js	15-Apr-2011 17:14	193K	
tiny_mce_popup.js	15-Apr-2011 17:14	5.2K	
tiny_mce_src.js	15-Apr-2011 17:14	409K	
utils/	05-Nov-2011 16:34	-	

Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i mod_autoindex_color PHP/5.2.8 Server at gunet2.cs.unipi.gr Port 443

Εικόνα 2.5στ . Καταγεγραμμένα από το Google directories του eclass !!!.

Δεν έχει απενεργοποιηθεί η δυνατότητα του directory listing, με κίνδυνο εκμετάλλευσης από επιτιθέμενο για κακόβουλο χειρισμό και συμφωνεί με το αποτέλεσμα του Paros παρακάτω.



Paros Scanning Report

Report generated at Sun, 25 Dec 2011 02:54:03.

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	0
Informational	0

Alert Detail

Medium (Warning)	Directory browsing
Description	It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files , backup source files etc which be accessed to read sensitive information.
URL	http://gunet2.cs.unipi.gr/eclass/template/classic/img/
URL	http://gunet2.cs.unipi.gr/eclass/template/classic/
URL	http://gunet2.cs.unipi.gr/eclass/template/
Solution	Disable directory browsing. If this is required, make sure the listed files does not induce risks.
Reference	For IIS, turn off directory browsing. For Apache, use the 'Options -Indexes' directive to disable indexes in directory or via .htaccess: . http://httpd.apache.org/docs/mod/core.html#options . http://alamo.satlug.org/pipermail/satlug/2002-February/000053.html . or create a default index.html for each directory.

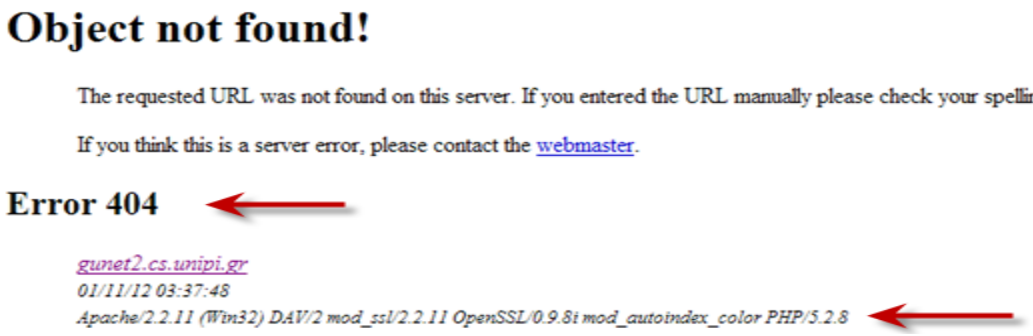
Medium (Suspicious)	Lotus Domino default files
Description	Lotus Domino default files found.
URL	http://gunet2.cs.unipi.gr/?OpenServer
URL	http://gunet2.cs.unipi.gr/?Open
Solution	Remove default files.
Reference	

Εικόνα 2.5ζ : **Summary Report του Scanner του Paros Proxy για το eclass.**

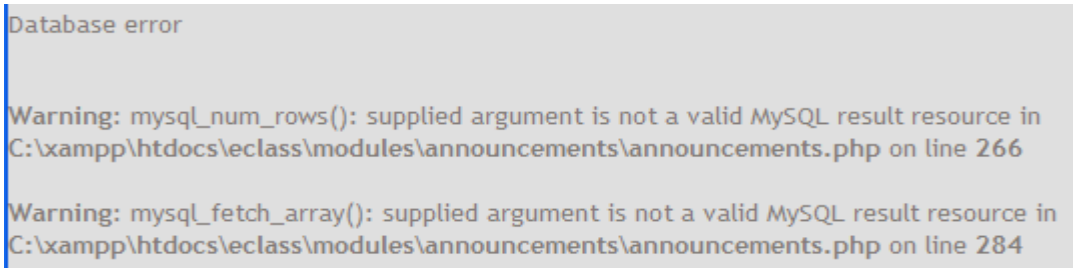
Διαπιστώνει επίσης την δυνατότητα του directory listing και ανακαλύπτει την ύπαρξη default files του Lotus Dominus.

2.6 ANALYSIS OF ERROR CODES

Ένα αίτημα με ανύπαρκτο url μας δίνει το παρακάτω error 404 με τις αντίστοιχες πληροφορίες , οι οποίες μας είναι ήδη γνωστές. Error codes μπορούμε να πάρουμε και από ένα λάθος ερώτημα στη βάση δεδομένων (εδώ MySQL) , οπότε θα μας αποκαλύψει το banner της MySQL.



Εικόνα 2.6α . Η απόκριση του web server σε ανύπαρκτο url του ιστότοπου.



Εικόνα 2.6β . Data base error από την MySQL.

Με τις πληροφορίες που έχουμε συγκεντρώσει για την έκδοση του web server Apache 2.1.11 , PHP 5.2.8 και phpMyAdmin 3.1.1 **συνάγουμε** ότι η βάση δεδομένων που έχει εγκατασταθεί θα πρέπει να είναι η MySQL 5.1.30 , που όλα μαζί περιλαμβάνονται στο XAMPP 1.7.0. Οδηγίες για εγκατάσταση δίνονται στο video : **http://www.youtube.com/watch?v=3Let9JpJ718** (Install Apache 2.2.11, PHP 5.2.8, MySQL 5.1.30, and phpMyAdmin 3.1.1 with XAMPP & Server 2003). Από την εγκατάσταση παίρνουμε επίσης πληροφορίες και για τα **default folders και files** !!!.

3 CONFIGURATION MANAGEMENT TESTING

3.1 SSL/TLS TESTING (SSL Version, Algorithms, Key length, Digital Cert. Validity)

Τα SSL και TLS είναι δύο πρωτόκολλα, τα οποία προσφέρουν ασφαλή κανάλια μεταφοράς δεδομένων, με την υποστήριξη αλγορίθμων κρυπτογραφίας για απόκρυψη της πληροφορίας,

όπως και hash αλγορίθμων για την ακεραιότητά της. Λόγω της κρισιμότητας κάποιων εφαρμογών, είναι αναγκαίο να αξιολογηθεί η διαθεσιμότητα και υλοποίηση ισχυρών αλγορίθμων κρυπτογράφησης, όπως επίσης η σωστή ρύθμιση του web server και του συνοδευόμενου λογισμικού παροχής υπηρεσιών κρυπτογράφησης. Η επιλογή του https για την μεταφορά κρίσιμων δεδομένων από άποψη ασφαλείας, παρέχει την δυνατότητα ταυτοποίησης αποστολέα και παραλήπτη μέσω ψηφιακών πιστοποιητικών και την εγκατάσταση TLS/SSL καναλιών για την κωδικοποίηση και απόκρυψη της διακινούμενης κρίσιμης πληροφορίας. Το πρόγραμμα **nmap (scanner)** (όπως παρατηρήσαμε παραπάνω) μας παρέχει την δυνατότητα αναγώρισης και ταυτοποίησης υπηρεσιών SSL και των αντίστοιχων ports του web server στα οποία διατίθενται. Για τον ιστότοπο **http://gunet2.cs.unipi.gr/eclass** έχουμε ήδη εντοπίσει, εικόνα 2.5γ , την 443 πόρτα και τις αντίστοιχες υπηρεσίες SSL , χωρίς αξιολόγηση των παρεχομένων υπηρεσιών. Το πρόγραμμα **nessus (vulnerability scanner)** και το εξειδικευμένο πρόγραμμα **SSLDigger** (report του οποίου ακολουθεί), μπορούν να ελέγξουν και να αξιολογήσουν τους διαθέσιμους αλγορίθμους αλλά και τις απαραίτητες ρυθμίσεις του web server και του λογισμικού που παρέχει αυτές τις υπηρεσίες.

Report του SSLDigger για τον http://gunet2.cs.unipi.gr/eclass

Foundstone | SSLDigger

SSL Cipher Strength Report

Τετάρτη, 11 Ιανουαρίου 2012 4:50:04 πμ

Summary

Number of Servers Tested	1
Number of Ciphers Used in Testing	26
No Security	2
Weak Security	10
Strong Security	9
Excellent Security	5

Ciphers Supported

Server URL	No Security	Weak Security	Strong Security	Excellent Security	Grade
https://gunet2.cs.unipi.gr/eclass	0	4	5	2	B

Εικόνα 3.1α Συγκεντρωτικά συμπεράσματα του SSLDigger για το gunet2.cs.unipi.gr/eclass

Ακολουθούν τα αναλυτικά συμπεράσματα :

Detailed Results

Server: https://gunet2.cs.unipi.gr/eclass

Grade	B	
	Common Name	gunet2.cs.unipi.gr
	SSL Version	TLS 1.0
	Key Algorithm	RSA_SHA1RSA
	Key Algorithm Parameters	0500
	Key Length	2048
	Certificate Validity	ValidCertificate
	Effective Date	25/10/2011 3:00:00 πμ
	Expiry Date	25/10/2014 2:59:59 πμ
	Certification Authority	TERENA SSL CA
	Format	X509
	Serial No	00FA736E6D2053AA47417D36B929204C5C
	Server Gated Cryptography	Absent
	Certificate Hash	B3DCE264BA895CAF74BDAD102BE15CD0FBF2EB7D
Certificate Details	**Public Key**	3082010A0282010100BBDBE6DDF6FD99942BF1A00B4C7E6569DB3D3C833B 2C4C92C5AF8419E7B93217CC4F151B920812A9A24294277CBF1A8CA0067D 6845C4184EF0CA9A8AE925ACBE577B6A7FDEA446A39D7E8DFEA864E44F7F 4C15894BFB70E7BA96B46D6E685787EF9BF8165E59630719C5BBCF390C933 9C0069F7032D1DD11037A2EC535461407DEAD1C098094FD9302387196BA6 4AB5AD72199C87FAEB178FEE9215D9267CF1C236BCFF39C07B13404F38639 0F93633D451DCBC7F79AEC641FD8E0BC6E7B90C7A9F8EC050C53D5E6FF9B ABC92F6FBE61C04391D78D993EF4374DCA38DF278A800AAEA3E6F27086A0 448DE02A86A4EC131D1197F95204A9C8B8E78664B6887E370203010001
	Raw Certificate Data	308204BB308203A3A003020102021100FA736E6D2053AA47417D36B929204 C5C300D06092A864886F70D01010505003036310B3009060355040613024E 4C310F300D060355040A1306544552454E413116301406035504031 30D544 552454E412053534C204341301E170D3131313032353030303030305A170D 3134313032343233353935395A308192310B30090603550406130247523110 300E060355040813075069726165757331103 00E060355040713075069726 657573311E301C060355040A1315556E697665727369747920 6F6620506972 6165757331223020603550 40B131944657061727 46D656E74206F6620496E 666F726D6174696373311B3019060355040313126775 6E6574322E63732E75 6E6970692E67723082012230 0D06092A864886F70D01010105000382010F0 03082010A0282010100BBDBE6DDF6FD99942BF1A00B4C7E6569DB3D3C833 B2C4C92C5AF8419E7B93217CC4F151B920812A9A24294277CBF1A8CA0067 D6845C4184EF0CA9A8AE925ACBE577B6A7FDEA446A39D7E8DFEA864E44F7 F4C15894BFB70E7BA96B46D6E685787EF9BF8165E59630719C5BBCF390C93 39C0069F7032D1DD11037A2EC535461407DEAD1C098094FD9302387196BA 64AB5AD72199C87FAEB178FEE9215D9267CF1C236BCFF39C07B13404F3863 90F93633D451DCBC7F79AEC641FD8E0BC6E7B90C7A9F8EC050C53D5E6FF9 BABC92F6FBE61C04391D78D993EF4374DCA38DF278A800AAEA3E6F27086A 0448DE02A86A4EC131D1197F95204A9C8B8E78664B6887E370203010001A3 82016530820161301F0603551D230418301680140CBD93680CF3DEABA3496 B2B375747EA90E3B9ED301D0603551D0E041604146535A2C9D8C58AE73EB 76FEF7293CFAC7FDB7AC6300E0603551D0F0101FF0404030205A0300C0603 551D130101FF04023000301D0603551D250416301406082B0601050507030 106082B06010505070302301806035 51D200411300F300D060B2B06010401 B2310102021D303A0603551D1F04333031302FA02DA02B8629687474703A2 F2F63726C2E7463732E746572656E612E6F72672F544552454E4153534C434 12E63726C306D06082B06010505070101046130 5F303506082B0601050507 3002862968747 4703A2F2F6372742E7463732E746572656E612E6F72672F54 4552454E4153534C43412E637274302606082B06010505073001861A68747 4703A2F2F6F6373702E7463732E746572656E612E6F7267301D0603551D110 4163014821267756E6574322E63732E756E6970692E6772300D06092A8648 86F70D01010505000382010100 68C9E5958530656E37B02510D37CF865749 BB1CE0A85525613F18A2BF1A4F406E93B51D1787CCCA846705C4A71B3680 FDCFB3DE19DE3F721DD7149E9D53FB231ED90F8BBD799C73B034D67D8524 AE56F4B4B36A0590B21A45EF8DEFAAABC879C2EF3DE047FC17FFF1CF3D70C 5D5E103B0B63FA115E6B0621B7DD728202584722209A13D5BF8675621C59 34E64FDCF5B1C3BB2493CFB7A83C6AFD44498CE43B8CB013B624E4D07BD2 BF74D63BD8B5B7810741B033640D9BCAE9E4C6149648A1EA22B54D93CAE6 8DBA6C07BFC3899C99C5627794625CDB11957F6E0B07448D53EE93702CD7 E4947ABC0D9649FFEB2F5CD694B0375A11715B39D38C9CF379DC691D

Ciphers

OpenSSL Name	Display Name	Export Grade?	Strength	Supported?
NULL-MD5	Key Exchange: None; Authentication: None; Encryption: None; MAC: MD5	true	No Security	false
NULL-SHA	Key Exchange: None; Authentication: None; Encryption: None); MAC: SHA1	true	No Security	false
EXP-DES-CBC-SHA	Key Exchange: RSA(512); Authentication: RSA; Encryption: DES (40); MAC: SHA1	true	Weak Security	true
EXP-RC2-CBC-MD5	Key Exchange: RSA(512); Authentication: RSA; Encryption: RC2 (40); MAC: MD5	true	Weak Security	true
EXP-RC4-MD5	Key Exchange: RSA(512); Authentication: RSA; Encryption: RC4 (40); MAC: MD5	true	Weak Security	true
EXP1024-DHE-DSS-DES-CBC-SHA	Key Exchange: EDH (EXPORT - 1024); Authentication: DSS; Encryption: DES(56); MAC: SHA1	true	Weak Security	false
EXP1024-DHE-DSS-RC4-SHA	Key Exchange: EDH (EXPORT - 1024); Authentication: DSS; Encryption: RC4(56); MAC: SHA1	true	Weak Security	false
EXP1024-DES-CBC-SHA	Key Exchange: RSA (EXPORT - 1024); Authentication: RSA; Encryption: DES(56); MAC: SHA1	true	Weak Security	false
EXP1024-RC4-SHA	Key Exchange: RSA (EXPORT - 1024); Authentication: RSA; Encryption: RC4(56); MAC: MD5	true	Weak Security	false
DES-CBC-SHA	Key Exchange: RSA; Authentication: RSA; Encryption: DES(56); MAC: SHA1	false	Weak Security	true
ADH-AES128-SHA	Key Exchange: ADH; Authentication: RSA; Encryption: AES(128); MAC: SHA1	false	Weak Security	false
ADH-AES256-SHA	Key Exchange: ADH; Authentication: RSA; Encryption: DES(256); MAC: SHA1	false	Weak Security	false
DH-DSS-AES128-SHA	Key Exchange: DH; Authentication: DSS; Encryption: AES(128); MAC: SHA1	false	Strong Security	false
DH-RSA-AES128-SHA	Key Exchange: DH; Authentication: RSA; Encryption: AES(128); MAC: SHA1	false	Strong Security	false
DHE-DSS-RC4-SHA	Key Exchange: EDH; Authentication: DSS; Encryption: RC4(128); MAC: SHA1	false	Strong Security	false
DHE-DSS-AES128-SHA	Key Exchange: EDH; Authentication: DSS; Encryption: AES(128); MAC: SHA1	false	Strong Security	false
DHE-RSA-AES128-SHA	Key Exchange: EDH; Authentication: RSA; Encryption: AES(128); MAC: SHA1	false	Strong Security	true
RC4-MD5	Key Exchange: RSA; Authentication: RSA; Encryption: RC4(128); MAC: MD5	false	Strong Security	true
RC4-SHA	Key Exchange: RSA; Authentication: RSA; Encryption: RC4(128); MAC: SHA1	false	Strong Security	true
AES128-SHA	Key Exchange: RSA; Authentication: RSA; Encryption: AES(128); MAC: SHA1	false	Strong Security	true
DES-CBC3-SHA	Key Exchange: RSA; Authentication: RSA; Encryption: 3DES(128); MAC: SHA1	false	Strong Security	true
DH-DSS-AES256-SHA	Key Exchange: DH; Authentication: DSS; Encryption: AES(256); MAC: SHA1	false	Excellent Security	false
DH-RSA-AES256-SHA	Key Exchange: DH; Authentication: RSA; Encryption: AES(256); MAC: SHA1	false	Excellent Security	false
DHE-DSS-AES256-SHA	Key Exchange: EDH; Authentication: DSS; Encryption: AES(256); MAC: SHA1	false	Excellent Security	false
DHE-RSA-AES256-SHA	Key Exchange: EDH; Authentication: RSA; Encryption: AES(256); MAC: SHA1	false	Excellent Security	true
AES256-SHA	Key Exchange: RSA; Authentication: RSA; Encryption: AES(256); MAC: SHA1	false	Excellent Security	true

SSL Certificate Details	
Parameter	Value
Server	gunet2.cs.unipi.gr
SSL Version	TLS 1.0
Key Algorithm	RSA_SHA1RSA
Key Algorithm Parameters	0500
Key Length	2048
Validity	ValidCertificate
Effective Date	25/10/2011 3:00:00 πμ
Expiration Date	25/10/2014 2:59:59 πμ
Certification Authority	TERENA SSL CA
Format	X509
Serial No.	00FA736E6D2053AA47417D368
Server Gated Cryptography	Absent
Certificate Hash	B3DCE264BA895CAF74BDAD10
Certificate Public Key	3082010A0282010100BBDBE6D
Certificate Raw Data	308204BB308203A3A003020102

Εικόνα 3.1 . **Αναλυτικό** Report του SSLDigger για τον http://gunet2.cs.unipi.gr/eclass.

3.2 DB Listener Testing

Το DB listener είναι ένα σημείο εισόδου για remote συνδέσεις σε μια Oracle βάση δεδομένων. Το DB listener "ακούει" στην πόρτα, συνήθως, 1521 (2483 για TNS Listener και 2484 για TNS Listener που χρησιμοποιεί SSL). Αν ο administrator δεν έχει ενεργοποιήσει password , τότε ένας επιτιθέμενος μπορεί να το ενεργοποιήσει και να δημιουργήσει DoS στη βάση.

Για τον ιστότοπο **http://gunet2.cs.unipi.gr/eclass** δεν έχει αναγνωρισθεί η ύπαρξή τους και επομένως δεν χρειάζεται κάποιος έλεγχος.

3.3 INFRASTRUCTURE CONFIGURATION MANAGEMENT TESTING

Μία πληρέστερη εικόνα της συνολικής υποδομής , των ρυθμίσεών της και της αξιολόγησής της από άποψης ασφάλειας μας δίνει το report από τον **vulnerability scanner NESSUS**. Ακολουθεί **σύνοψη** των προσδιορισθέντων αδυναμιών και στο **Παράρτημα Β** (συνοδευτικό CD), η αναλυτική παρουσίασή του.

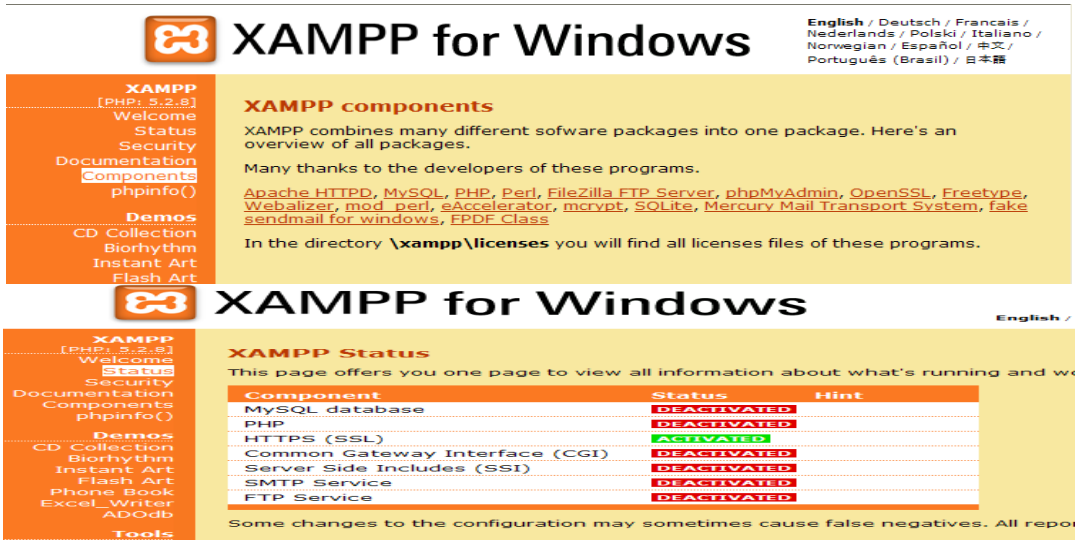
The following plugin IDs have problems associated with them. Select the ID to review more detail.

PLUGIN ID#	# OF ISSUES	PLUGIN NAME	SEVERITY
26928	1	SSL Weak Cipher Suites Supported	Medium Severity problem(s) found
20007	1	SSL Version 2 (v2) Protocol Detection	Medium Severity problem(s) found
42873	1	SSL Medium Strength Cipher Suites Supported	Medium Severity problem(s) found
51192	1	SSL Certificate signed with an unknown Certificate Authority	Medium Severity problem(s) found
51892	1	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue	Medium Severity problem(s) found
51893	1	OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Ciphersuite Disabled Cipher Issue	Medium Severity problem(s) found
22964	3	Service Detection	Low Severity problem(s) found
26194	2	Web Server Uses Plain Text Authentication Forms	Low Severity problem(s) found
11032	2	Web Server Directory Enumeration	Low Severity problem(s) found
42057	2	Web Server Allows Password Auto-Completion	Low Severity problem(s) found
10662	2	Web mirroring	Low Severity problem(s) found
40665	2	Protected Web Page Detection	Low Severity problem(s) found
57323	2	OpenSSL Version Detection	Low Severity problem(s) found
10107	2	HTTP Server Type and Version	Low Severity problem(s) found
39463	2	HTTP Server Cookies Set	Low Severity problem(s) found
49705	2	Gathered e-mail Addresses	Low Severity problem(s) found
49704	2	External URLs	Low Severity problem(s) found
34850	1	Web Server Uses Basic Authentication Without HTTPS	Low Severity problem(s) found
51080	1	Web Server Uses Basic Authentication over HTTPS	Low Severity problem(s) found
10287	1	Traceroute Information	Low Severity problem(s) found
25220	1	TCP/IP Timestamps Supported	Low Severity problem(s) found
51891	1	SSL Session Resume Supported	Low Severity problem(s) found
57041	1	SSL Perfect Forward Secrecy Cipher Suites Supported	Low Severity problem(s) found
21643	1	SSL Cipher Suites Supported	Low Severity problem(s) found
10863	1	SSL Certificate Information	Low Severity problem(s) found
56984	1	SSL / TLS Versions Supported	Low Severity problem(s) found
42880	1	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	Low Severity problem(s) found
53491	1	SSL / TLS Renegotiation DoS	Low Severity problem(s) found
11936	1	OS Identification	Low Severity problem(s) found
19506	1	Nessus Scan Information	Low Severity problem(s) found
43111	1	HTTP Methods Allowed (per directory)	Low Severity problem(s) found
12053	1	Host Fully Qualified Domain Name (FQDN) Resolution	Low Severity problem(s) found
54615	1	Device Type	Low Severity problem(s) found

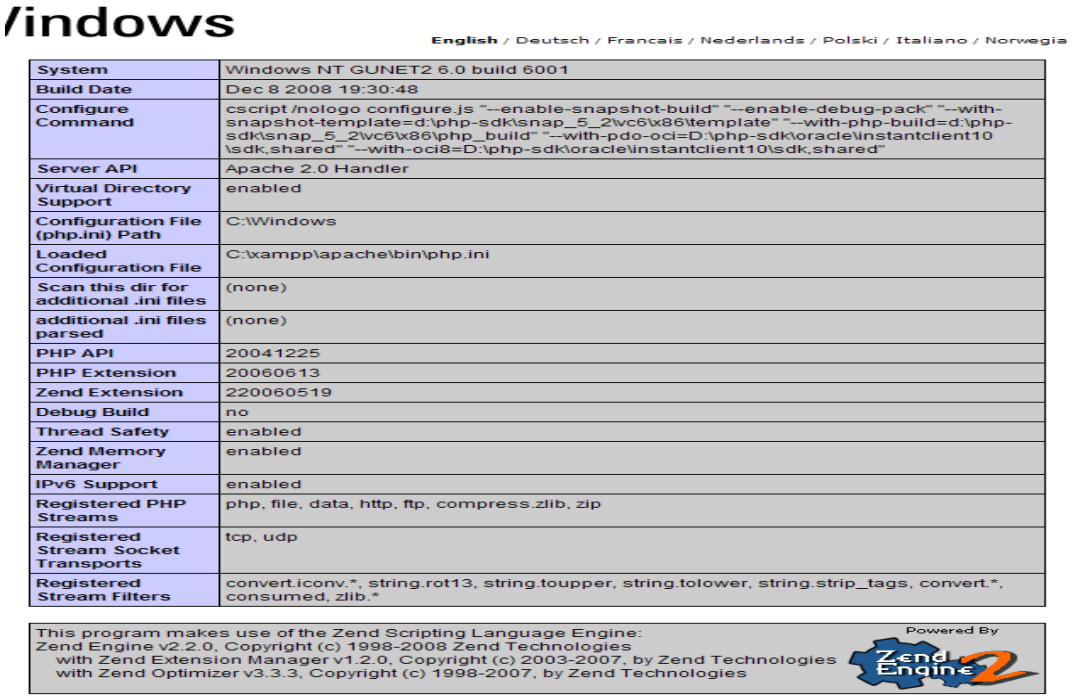
Εικόνα ΠΑ.3.3α . Report (σύνοψη) του Nessus για τον http://gunet2.cs.unipi.gr/eclass.

3.4 INFRASTRUCTURE AND APPLICATION ADMIN INTERFACES

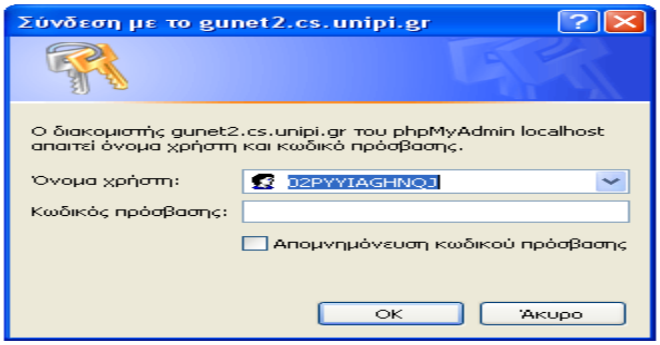
Ο έλεγχος για links του διαχειριστή μέσω του Google έχει εντοπίσει τα παρακάτω (όπως και άλλα) που συνδυαζόμενα θα μπορούσαν να αξιοποιηθούν από κάποιο κακόβουλο χρήστη στην προσπάθειά του να αποκτήσει τον έλεγχο διαχείρισης του ιστότοπου. Αξιοσημείωτο είναι το link της εικόνας 3.4γ για login του διαχειριστή του ιστότοπου , το οποίο θα μπορούσε να αξιοποιήσει ένας επιτιθέμενος σε συνδυασμό με τα usernames που έχουν καταγραφεί στα usage statistics του ιστότοπου , εικόνα 3.4δ , αλλά και σε πολλά άλλα.



Εικόνα 3.4α Links στο XAMPP.



Εικόνα 3.4β. Πληροφορίες για Server,web server, php.



Εικόνα 3.4γ link για **login διαχειριστή** !!!.

Top 11 of 11 Total Referrers

#	Hits		Referrer
1	44	0.01%	- (Direct Request)
2	16	0.00%	https://gunet2.cs.unipi.gr/eclass/
3	13	0.00%	195.251.225.69
4	4	0.00%	https://gunet2.cs.unipi.gr/xampp/head.php
5	3	0.00%	https://gunet2.cs.unipi.gr/eclass/template/classic/theme.css
6	3	0.00%	https://gunet2.cs.unipi.gr/xampp/
7	3	0.00%	https://gunet2.cs.unipi.gr/xampp/navi.php
8	1	0.00%	112
9	1	0.00%	404
10	1	0.00%	https://gunet2.cs.unipi.gr/xampp/start.php
11	1	0.00%	value

Top 2 of 2 Total Usernames

#	Hits		Files		KBytes		Visits		Username
1	16	0.00%	16	0.00%	51	0.00%	3	0.01%	admin
2	1	0.00%	1	0.00%	0	0.00%	1	0.00%	okfoejf

Top 8 of 8 Total Usernames

#	Hits		Files		KBytes		Visits		Username
1	33	0.01%	33	0.01%	136	0.00%	1	0.01%	pma
2	10	0.00%	10	0.00%	32	0.00%	1	0.01%	eclass
3	7	0.00%	7	0.00%	1	0.00%	1	0.01%	root
4	5	0.00%	5	0.00%	35	0.00%	1	0.01%	asdasfas
5	5	0.00%	5	0.00%	35	0.00%	1	0.01%	eclass2
6	3	0.00%	3	0.00%	0	0.00%	1	0.01%	admin
7	1	0.00%	1	0.00%	0	0.00%	1	0.01%	cs
8	1	0.00%	1	0.00%	0	0.00%	1	0.01%	virvou

Εικόνα 3.4δ links σε σελίδες διαχείρισης αλλά και usernames

3.5 TESTING FOR HTTP METHODS AND XST

Μέθοδοι HTTP μπορούν να χρησιμοποιηθούν γα κακόβουλο σκοπό , αν ο Web Server δεν έχει ρυθμισθεί κατάλληλα. Έτσι μπορεί πχ να χρησιμοποιηθεί η μέθοδος TRACE για μία επίθεση Cross Site Tracing (XST), μια μορφή Cross Site Scripting (XSS) . Η μέθοδος TRACE επιστρέφει πίσω στον client ότι έχει προηγουμένως στείλει στον Server και χρησιμοποιείται συνήθως για λόγους διόρθωσης λαθών . Αν δεν έχει αποκλεισθεί από τις διαθέσιμες στον client μεθόδους , μετά την ολοκλήρωση της εφαρμογής , μπορεί να χρησιμοποιηθεί από κακόβουλο χρήστη για να αποκτήσει πρόσβαση στο document.cookie αντικείμενο και να το στείλει στον web server που ελέγχεται από τον επιτιθέμενο, ώστε να υποκλαπεί το session του θύματος.

Άλλοι μέθοδοι που μπορούν να εκμεταλευτούν από κακόβουλους χρήστες είναι :

PUT , μπορεί ν'ανεβάσει στον Web Sever κακόβουλο αρχείο

DELETE , μπορεί να σβήσει στον Web Server αναγκαίο για τη λειτουγία του αρχείο

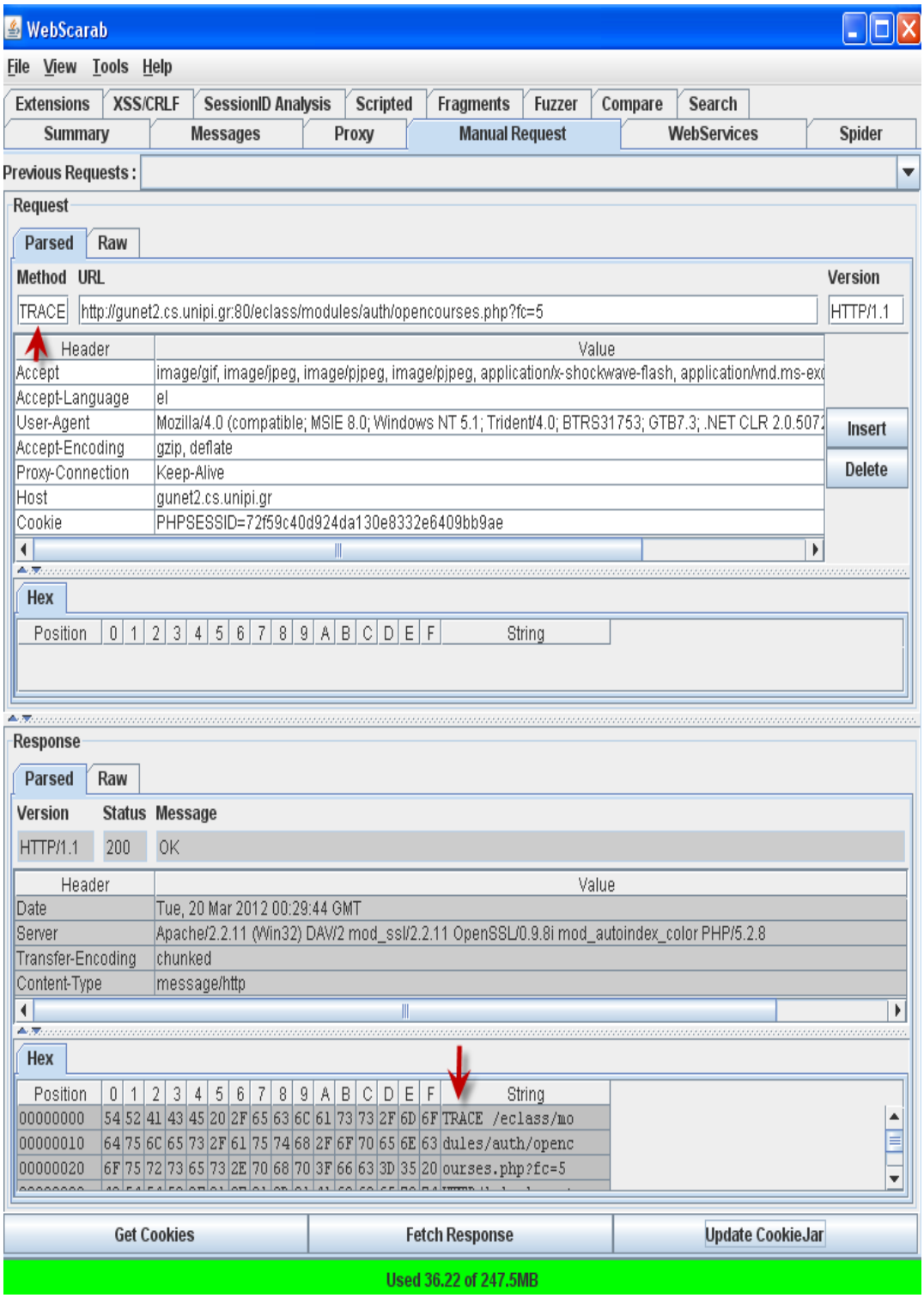
CONNECT , μπορεί να δώσει την δυνατότητα σ' ένα client να χρησιμοποιήσει τον Web Server σαν Proxy

Ο HTTP server πρέπει να ρυθμισθεί έτσι ώστε να παρέχει μόνο τις απαραίτητες για την λειτουργία μεθόδους γα την μείωση του κινδύνου εκμετάλευσης των με κακόβουλο τρόπο.

Η μέθοδος **OPTIONS** σε ένα αίτημα μπορεί να επιστρέψει , άρα και ν' αποκαλύψει τις διαθέσιμες στον client μεθόδους , αποκαλύπτοντας σε κάποιο κακόβουλο χρήστη τις μεθόδους που μπορεί να χρησιμοποιήσει για να εκμεταλευθεί ενδεχόμενες αδυναμίες τους.

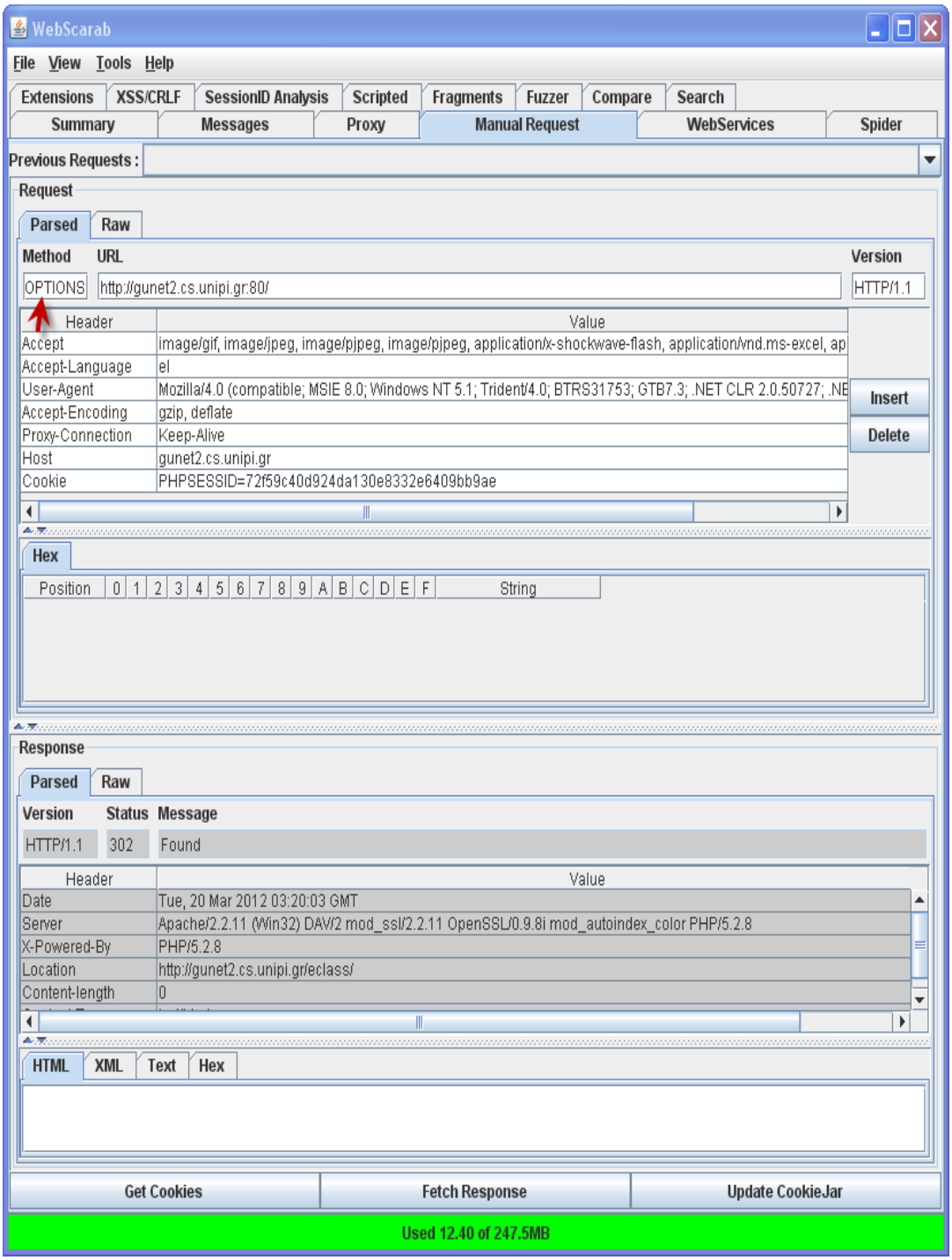
Θα πρέπει να έχουμε υπόψη ότι κάποιες πλατφόρμες ενδέχεται να διεκπεραιώσουν κάποιες μεθόδους σαν άλλες π.χ το **HEAD** σαν **GET.**

Σαν εργαλεία για την διαθεσιμότητα των μεθόδων του HTTP Server μπορούν να χρησιμοποιηθούν το **WebScarab** με το **Manual Request plugin,** και το **NetCat**.



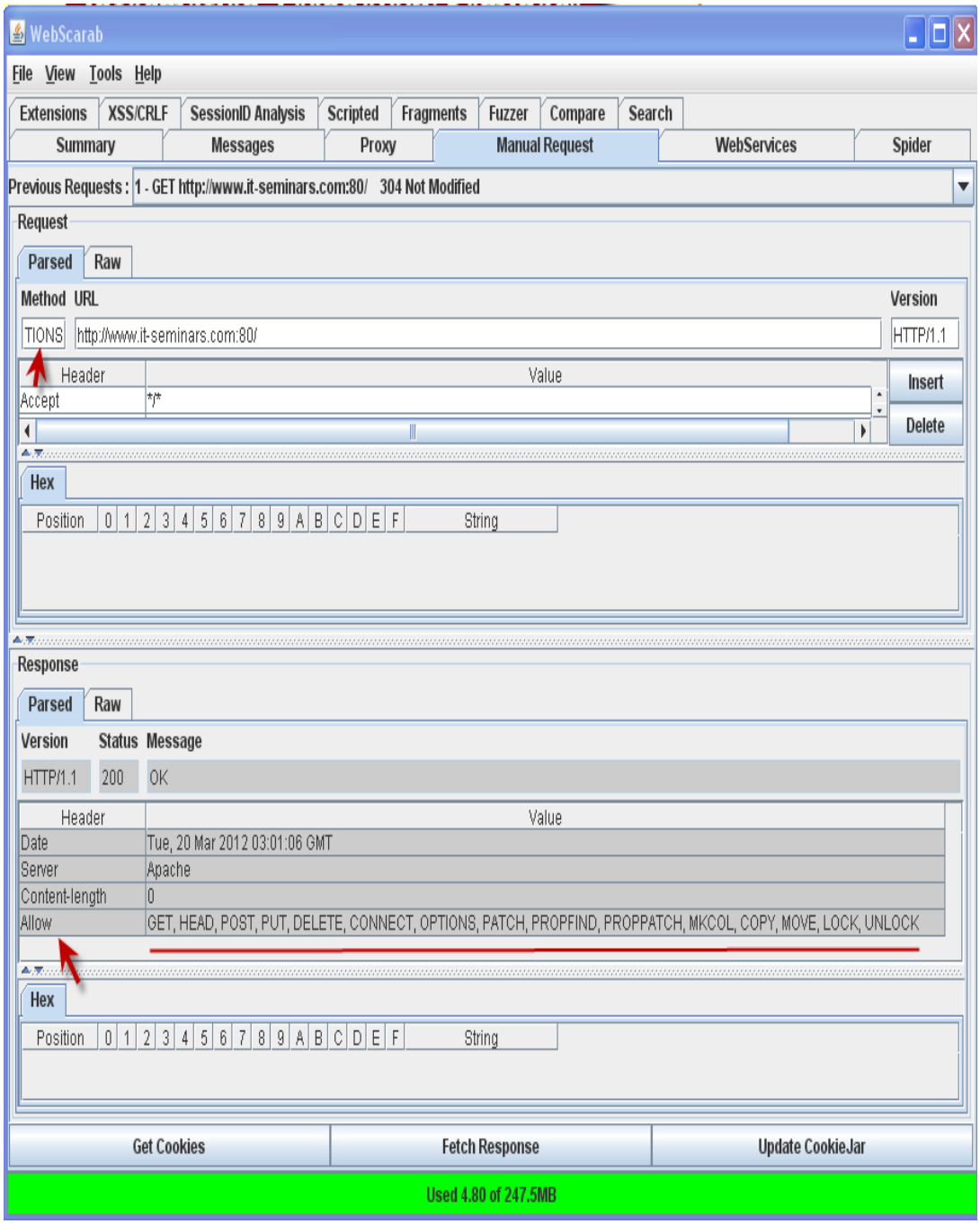
Εικόνα ΠΑ.3.4α . Απάντηση από τον web server του eclass με τη μέθοδο **TRACE**

Άρα το eclass είναι πιθανώς ευπαθές σε επίθεση XST.



Εικόνα ΠΑ.3.4β . Απάντηση από τον web server του eclass με τη μέθοδο **OPTIONS**

Παρατηρούμε ότι δεν επιστρέφει τις διαθέσιμες μεθόδους στον Client που σημαίνει αυξημένη προστασία. Αποκρίθηκε όμως στο αίτημα με την μέθοδο **TRACE ,** που σημαίνει ότι δοκιμάζοντας τις μεθόδους μπορούμε να αποκτήσουμε πληροφορία της διαθεσιμότητάς της.



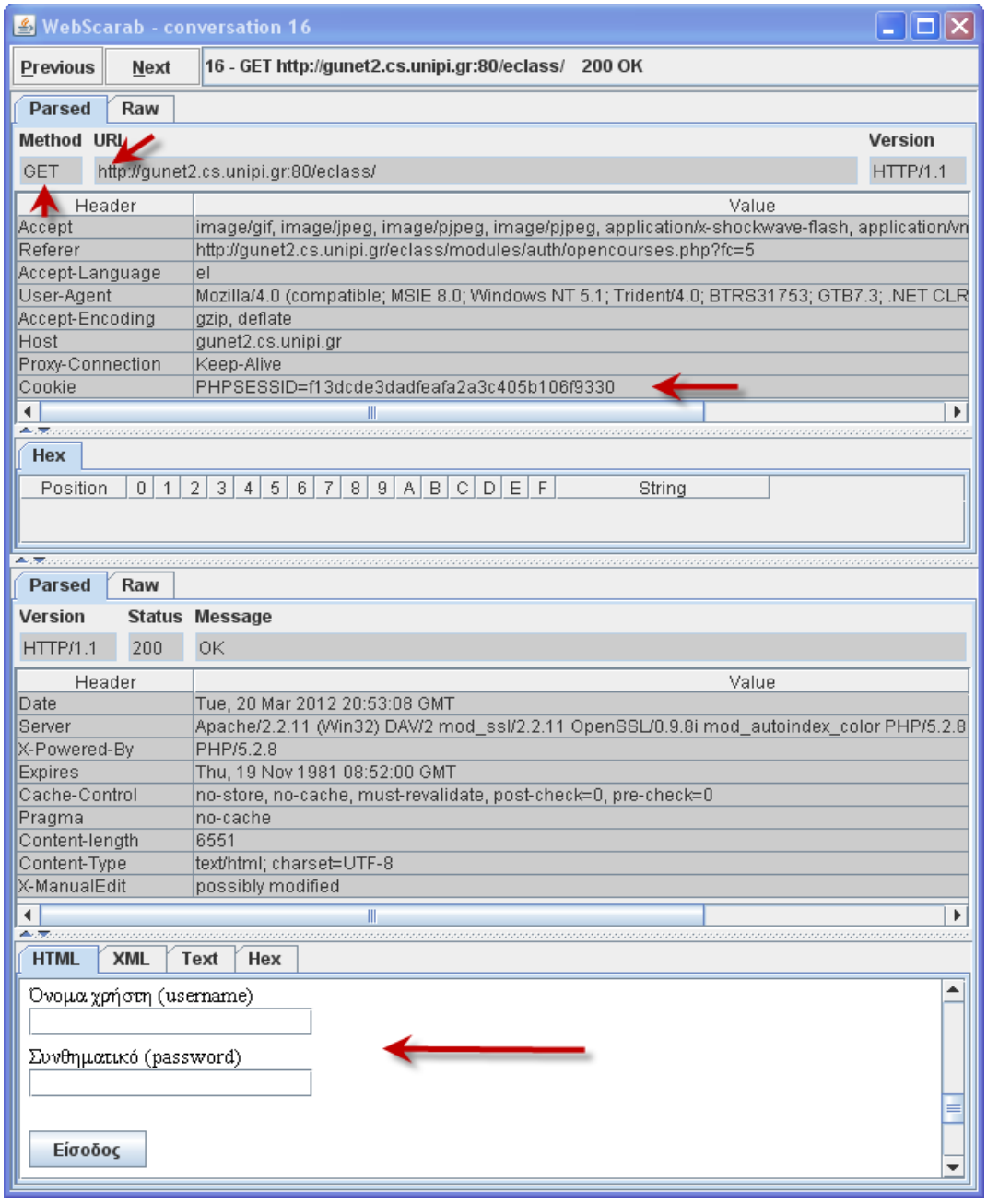
Εικόνα ΠΑ.3.4γ . Απάντηση από τον web server του it-seminars.com στην μέθοδο **OPTIONS** στην ετικέττα **Allow**.

Άρα έχουμε αποκάλυψη των διαθέσιμων μεθόδων στον client και επομένως πιο εύκολη διαπίστωση ύπαρξης ευπάθειας για κακόβουλη εκμετάλλευση της.

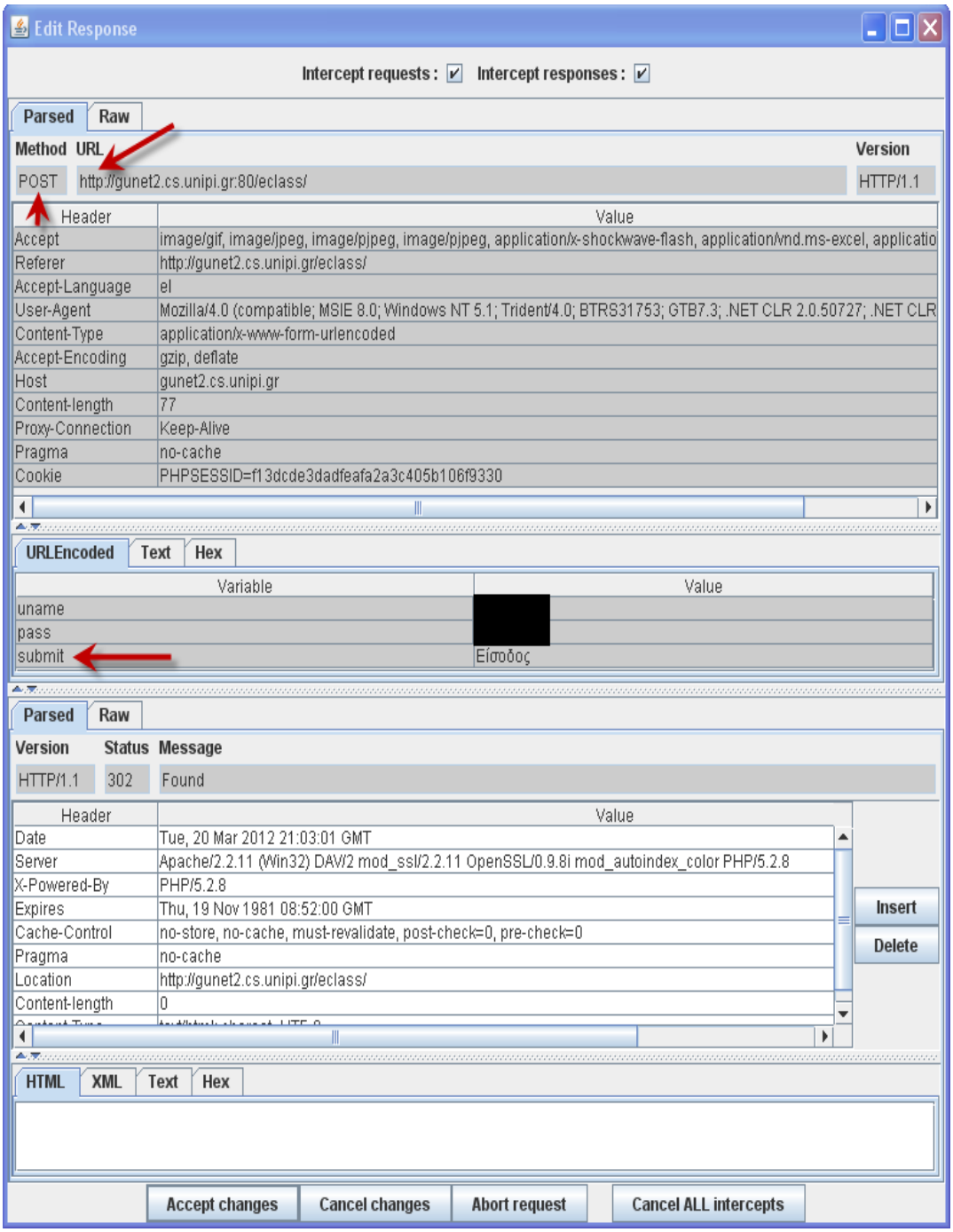
4 AUTHENTICATION TESTING

4.1 CREDENTIALS TRANSPORT OVER AN ENCRYPTED CHANNEL

Εδώ ελέγχουμε αν τα δεδομένα τα οποία εισάγει ο χρήστης στην web φόρμα για την σύνδεσή του στην εφαρμογή στον server, μεταβιβάζονται στον web server με ασφαλή πρωτόκολα για την ασφάλεια τους από κάποιον με MITM επίθεση. Δεν έχει ενεργοποιηθεί το https ! .



Εικόνα 4.1α . Το πρωτόκολλο **παραλαβής σελίδας login** είναι το http και όχι https



Εικόνα 4.1β . Το πρωτόκολλο **αποστολής login αιτήματος** είναι το http και όχι https

Παρατηρούμε λοιπόν ότι και στη παραλαβή της login σελίδας αλλά και στην αποστολή των δεδομένων αυθεντικοποίησης χρησιμοποιείται **το μη ασφαλές http**. Η μέθοδος αποστολής σωστά είναι η **POST**. Το **cookie** έχει δημιουργηθεί στην πρώτη απάντηση και ακολουθεί το ίδιο σε όλες τις συνομιλίες. Η εφαρμογή είναι ευπαθής στην υποκλοπή του sessionid αλλά και των δεδομένων αυθεντικοποίησης κατά την μεταβίβασή τους (MITM επίθεση).

4.2 TESTING FOR BYPASSING AUTHENTICATION SCHEMA

4.2.1 Direct page request (forced browsing)

Επισκεπτόμαστε το μάθημα **ΔΙΚΤΥΑ ΥΨΗΛΩΝ ΤΑΧΥΤΗΤΩΝ (ΠΜΣ),** στο οποίο η πρόσβαση επιτρέπεται μόνο μετά από login και μόνο μετά από εγγραφή στο μάθημα. Επιλέγουμε το έγγραφο : **Δίκτυα Κινητών και Προσωπικών Επικοινωνιών** και αντιγράφουμε την πλήρη διεύθυνση πρόσβασης σε αυτό στο clipboard από τον Browser . Βγαίνουμε από την εφαρμογή με logout , κλείνουμε τον Browser και μετά από λίγη ώρα κάνουμε αίτηση πρόσβασης στο έγγραφο χωρίς login με την παρακάτω διεύθυνσή:

http://gunet2.cs.unipi.gr/eclass/modules/document/file.php/TME129/%CE%A0%CE%B1%CF%81%CE%BF%CF%85%CF%83%CE%B9%CE%AC%CF%83%CE%B5%CE%B9%CF%82/Fundamentals_Elements_of_Mobile_networks.pdf

το έγγραφο αυτό εμφανίζεται χωρίς να έχει προηγηθεί αυθεντικοποίηση.

Το σχήμα αυθεντικοποίησης παραβιάζεται όταν αναφερόμαστε σε συγκεκριμένο πόρο (πχ pdf) Μετά από έλεγχο με το WebScarab παρατηρήσαμε ότι το cookie παραμένει σαν session id στον client και ίσως στον server (δεν καταστράφηκε με το logout) ή δεν ελέγχεται το αίτημα από την εφαρμογή στον server.

Αντίθετα, όταν σε αποθηκευμένο link στο Google που οδηγεί στην κεντρική σελίδα μαθήματος , για το οποίο απαιτείται αυθεντικοποίηση , επιλέξουμε με κλικ στο μενού πχ έγγραφα του μαθήματος, τότε η εφαρμογή απαιτεί αυθεντικοποίηση και εμφανίζει την σελίδα εισόδου όνομα χρήστη και κωδικού. Σε αυτή την περίπτωση η εφαρμογή προστατεύεται από μη εξουσιοδοτημένη πρόσβαση. Παράδειγμα γι αυτή τη περίπτωση το link:

http://webcache.googleusercontent.com/search?q=cache:0s46s3HmtMsJ:gunet2.cs.unipi.gr/eclass/courses/TMA102/+site:gunet2.cs.unipi.gr&cd=66&hl=el&ct=clnk&gl=gr

4.2.2 Parameter Modification

Υπάρχει ένα πρόβλημα, σχετικά με το σχήμα αυθεντικοποίησης όταν η εφαρμογή ελέγχει μια επιτυχή σύνδεση βασιζόμενη στις σταθερές τιμές παραμέτρου. Ένας χρήστης μπορεί να τροποποιήσει αυτές τις παραμέτρους μέσω του Proxy του WebScarab και να αποκτήσει πρόσβαση στις προστατευόμενες σελίδες, χωρίς να απαιτείται ενδεχομένως η παροχή των έγκυρων πιστοποιητικών.

Στο παράδειγμα (link):
http://gunet2.cs.unipi.gr/eclass/modulus/document/document.php?course=TME129

δεν επιστρέφει την αντίστοιχη σελίδα αλλά το παρακάτω error 404.

Object not found!

The requested URL was not found on this server. If you entered the URL manually please check your spelling and try again

If you think this is a server error, please contact the webmaster.

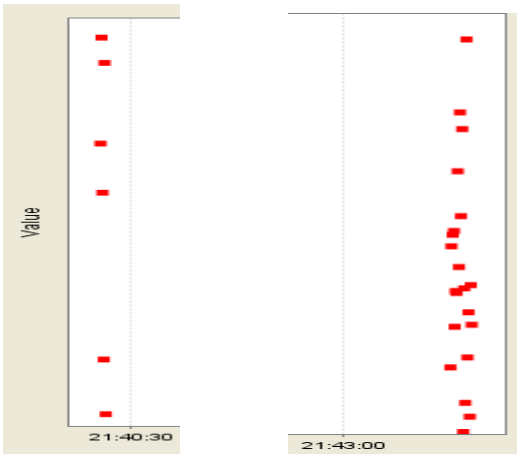
Error 404

gunet2.cs.unipi.gr
04/04/12 19:22:28
Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i mod_autoindex_color PHP/5.2.8

Στις δοκιμές που έγιναν δεν παρατηρήθηκε χρήση παραμέτρων για την επιβεβαίωση αυθεντικότητας πρόσβασης, αλλά η χρήση sessionid .

4.2.3 Session ID Prediction (Πρόβλεψη Ταυτότητας Συνόδου)

Όπως παρατηρήσαμε προηγουμένως στο Summary (στον πίνακα στο κάτω μέρος) δεν καταγράφεται κάποια αλλαγή τιμής στη στήλη SET-COOKIE , το cookie που χρησιμοποιείται για την ταυτοποίηση των συνομιλιών παραμένει το ίδιο σε σχέση προς το χρόνο για το ίδιο login. Αν κάνουμε logout και μετά λίγη ώρα πάλι login το session ID παραμένει το ίδιο. Έτσι έχουμε μια ευπάθεια σχεδιασμού εφαρμογής , διότι γίνεται πιο εύκολο να υποκλαπεί το session ID (π.χ.. με MITM ή με XSS επίθεση) και να χρησιμοποιηθεί για μη εξουσιοδοτημένη πρόσβαση σε προστατευμένους πόρους της εφαρμογής, δίνοντας στον επιτιθέμενο περισσότερο χρόνο για να επιτεθεί χρησιμοποιώντας το κλεμμένο session id. Οι συγκρίσεις των διαφορετικών τιμών session ID 's σε διαφορετικά login's και σε διαφορετικές ώρες δεν αποκάλυψαν το μηχανισμό της δημιουργίας του.Το visualisation μέσω WebScarab είχε την παρακάτω μορφή (εικόνα 4.3.2α) όταν προκλήθηκε η συνεχής παραγωγή νέων cookies , που δείχνει ότι υπάρχει ένα διάστημα ανάμεσα στο οποίο παράγονται οι τιμές.Την πρώτη φορά ζητήθηκαν 6 τιμές , ενώ την δεύτερη 21 τιμές. Η ανάλυση μέσω του WebScarab δεν αποκάλυψε κάποια κανονικότητα στην παραγωγή τους , ούτε χρονική σχέση.



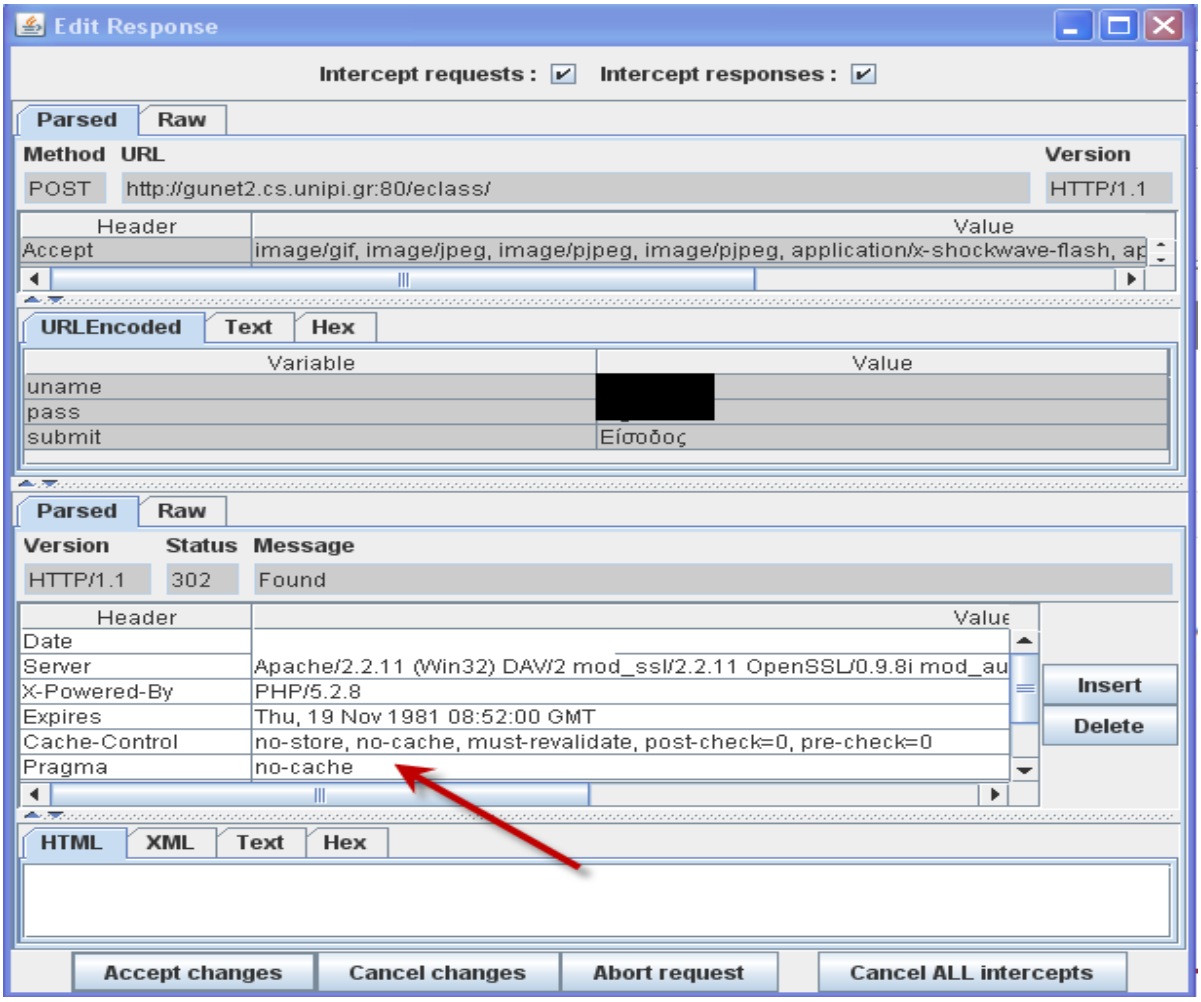
Εικόνα 4.2.3α Visualisation των διαφορετικών τιμών των cookies που καταγράφηκαν δύο φορές σε χρονική απόσταση 3 λεπτών περίπου.

4.2.4 SQL Injection (HTML Form Authentication)

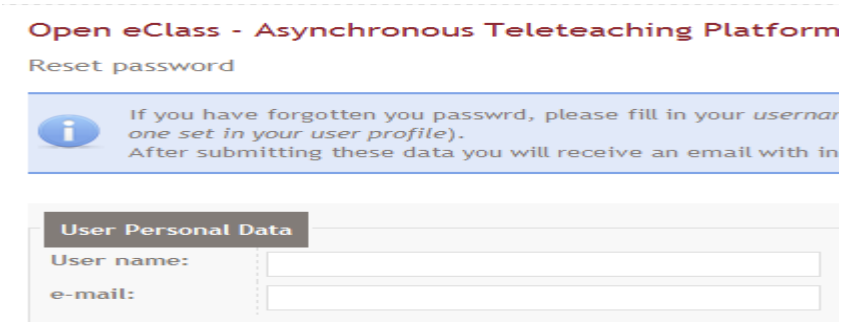
Δοκιμάζοντας 2 εναλλακτικές μορφές SQL Injection , πρώτα με γνωστό το username (username'--) και τυχαίο password και μετά άγνωστα και τα δύο , δεν παρακάμφθηκε ο έλεγχος αυθεντικοποίησης , που σημαίνει ότι ο μηχανισμός αυθεντικοποίησης ελέγχει το είδος των εισαγόμενων δεδομένων για ενδεχόμενο SQL injection. Ο έλεγχος γίνεται στον server , όπως έδειξε ο έλεγχος όταν το SQL injection έγινε και με τροποποίηση στον proxy του WebScarab και χειροκίνητη υποβολή του αιτήματος.

4.3 TESTING FOR VULNERABLE REMEMBER PASSWORD AND PWD RESET

Κατά την αυθεντικοποίηση με login παρατηρούμε στην εικόνα 4.3α , μέσω του WebScarab, ότι απαιτείται η μη αποθήκευση του username και password από τον Browser , που δείχνει την πρόληψη της εφαρμογής για υποκλοπή των διαπιστευτηρίων του νόμιμου χρήστη , σε κοινόχρηστους υπολογιστές.



Εικόνα 4.3α Το βέλος δείχνει τις εντολές που απαιτούν μη αποθήκευση του username και του password.



Εικόνα 4.3β Διεπαφή του eclass για τη λειτουργία password reset.

Η εφαρμογή eClass , εικόνα 4.3β, διαθέτει λειτουργία επαναπροσδιορισμού του password και όπως διαπιστώθηκε ελέγχει και το username και τον λογαριασμό e-mail , πριν αποστείλει το link για νέο κωδικό, σημαντική πρόληψη για μη υποκλοπή. Παραμένει η αδυναμία στην περίπτωση που έχει υποκλαπεί ο λογαριασμός e-mail του χρήστη.

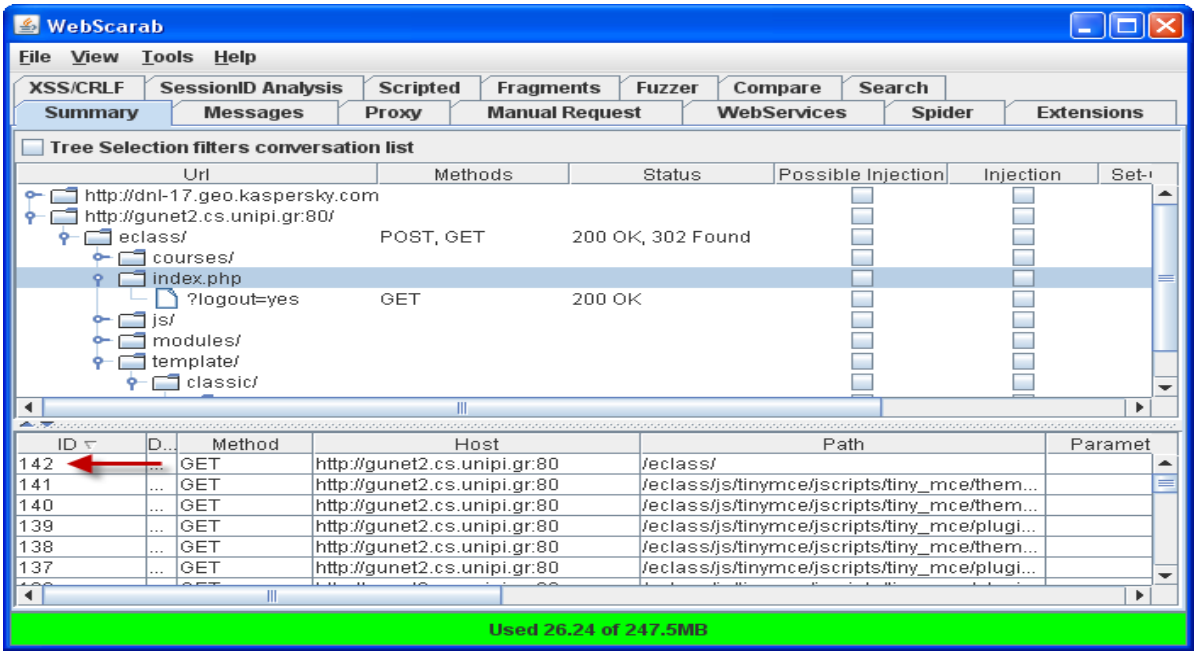
4.4 TESTING FOR LOGOUT AND BROWSER CACHE MANAGEMENT

Κατά τους ελέγχους προέκυψε ότι, μετά το logout από το eClass, ο Browser δεν επιστρέφει σε σελίδες που απαιτούν αυθεντικοποίηση. Η session variable πιθανότατα έχει καταστραφεί στον Web Server. Το sessionID παραμένει το ίδιο και διαθέσιμο στον Browser και επαναχρησιμοποιείται σε περίπτωση νέας επίσκεψης ή ακόμη και σε νέο login. Αυτό δεν σημαίνει κατ' ανάγκη, ότι το sessionID δεν έχει καταστραφεί στον Web Server. Πιθανότατα το επανεργοποιεί , αποδεχόμενος το ίδιο, δημιουργώντας νέο sessionID variable. Η αυθεντικοποίηση μόνο με το sessionID δεν επιτυγχάνει. Σε ένα νέο login, αν τοποθετήσουμε με το SET-COOKIE, στο Response του Web Server, ένα παλαιότερο sessionID ή ακόμη όποιαδήποτε τιμή , τότε την αποδέχεται και το επόμενο αίτημα έχει και τα δύο sessionID's . Χειρίζεται το αρχικό σαν βασικό και το νέο σαν δευτερεύον, που έχει συσχετιστεί με το βασικό. Μετά την αυθεντικοποίηση με αυτό τον τρόπο, αν αφαιρέσουμε το βασικό και μείνει μόνο το δευτερεύον sessionID στα αιτήματα , μπορούμε να επισκεπτόμαστε σελίδες και πόρους που απαιτούν αυθεντικοποίηση κανονικά. Αν αλλάξουμε το δευτερεύον με ένα άλλο τυχαίο και επιλέξουμε σελίδες που απαιτούν αυθεντικοποίηση , τότε κάνει αυτόματα logout και μας οδηγεί στη σελίδα, που κάνει νέο login. Αν κλείσουμε τον Browser θα μας ζητήσει νέο login με νέο SessionID , το παλαιό sessionID καταστρέφεται στον client. Όταν βρισκόμαστε σε σελίδες που απαιτούν αυθεντικοποίηση και παραμείνουμε για κάποιο χρονικό διάστημα χωρίς δραστηριότητα γίνεται logout , δίνει όμως το δικαίωμα επιλογών των σελίδων που ανήκουν στο μάθημα , που βρισκόμασταν.
Οι κίνδυνοι που υπάρχουν είναι η υποκλοπή διαπιστευτηρίων επειδή δεν χρησιμοπιείται το https με επίθεση MITM , όπως επίσης η υποκλοπή sessionID με XSS επίθεση και το ενδεχόμενο να υποδυθεί ο επιτιθέμενος τον νόμιμα ήδη αυθεντικοποιημένο χρήστη.

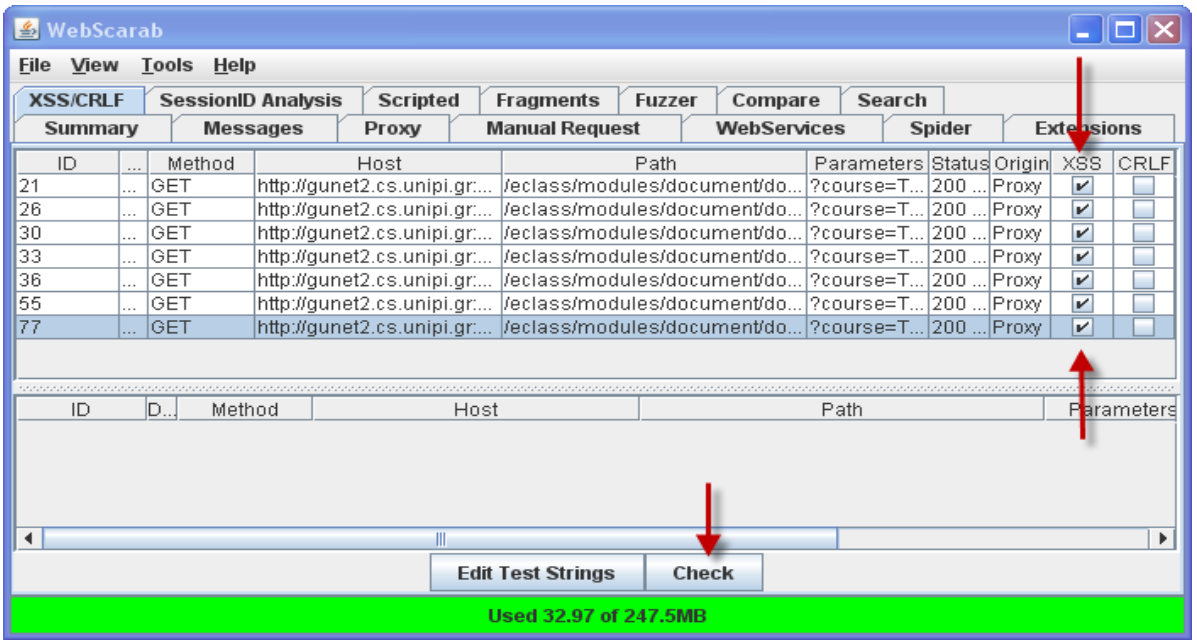
5 DATA VALIDATION TESTING

5.1 CROSS SITE SCRIPTING / CRLF INJECTION

Επειδή το WebScarab καταγράφει τα αιτήματα που είναι ευπαθή σε XSS και CRLF μαζί, επιλέχθηκε ο έλεγχος και των δύο. Κατεγράφησαν παθητικά 142 αιτήματα, (εικόνα 5.1α), από τα οποία τα 7 κατεγράφησαν σαν ύποπτα μόνο για XSS ευπάθεια (εικόνα 5.1β).

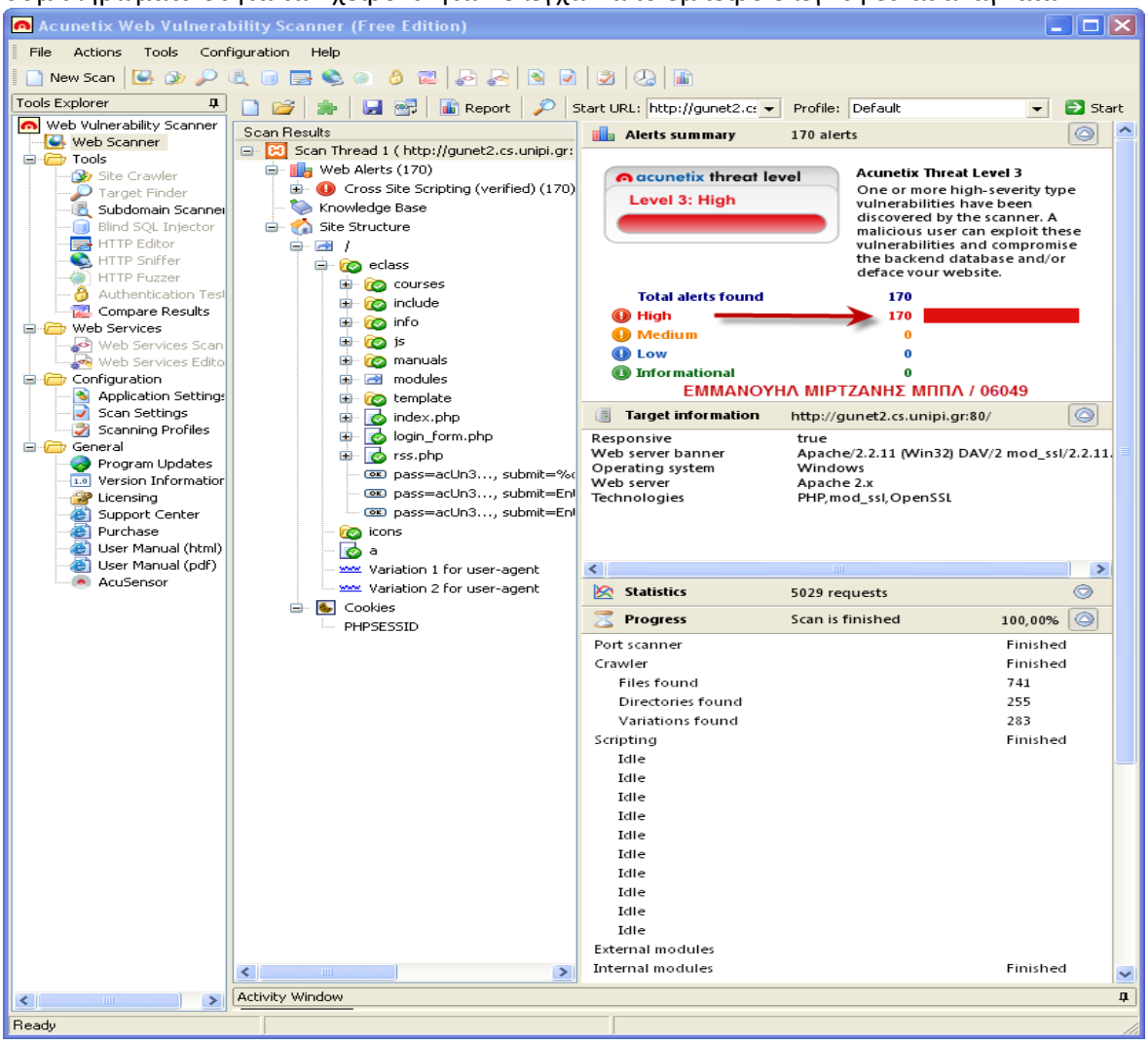


Εικόνα 5.1α Με περιήγηση στο gunet2.cs.unipi.gr/eclass, κατεγράφησαν 142 αιτήματα.

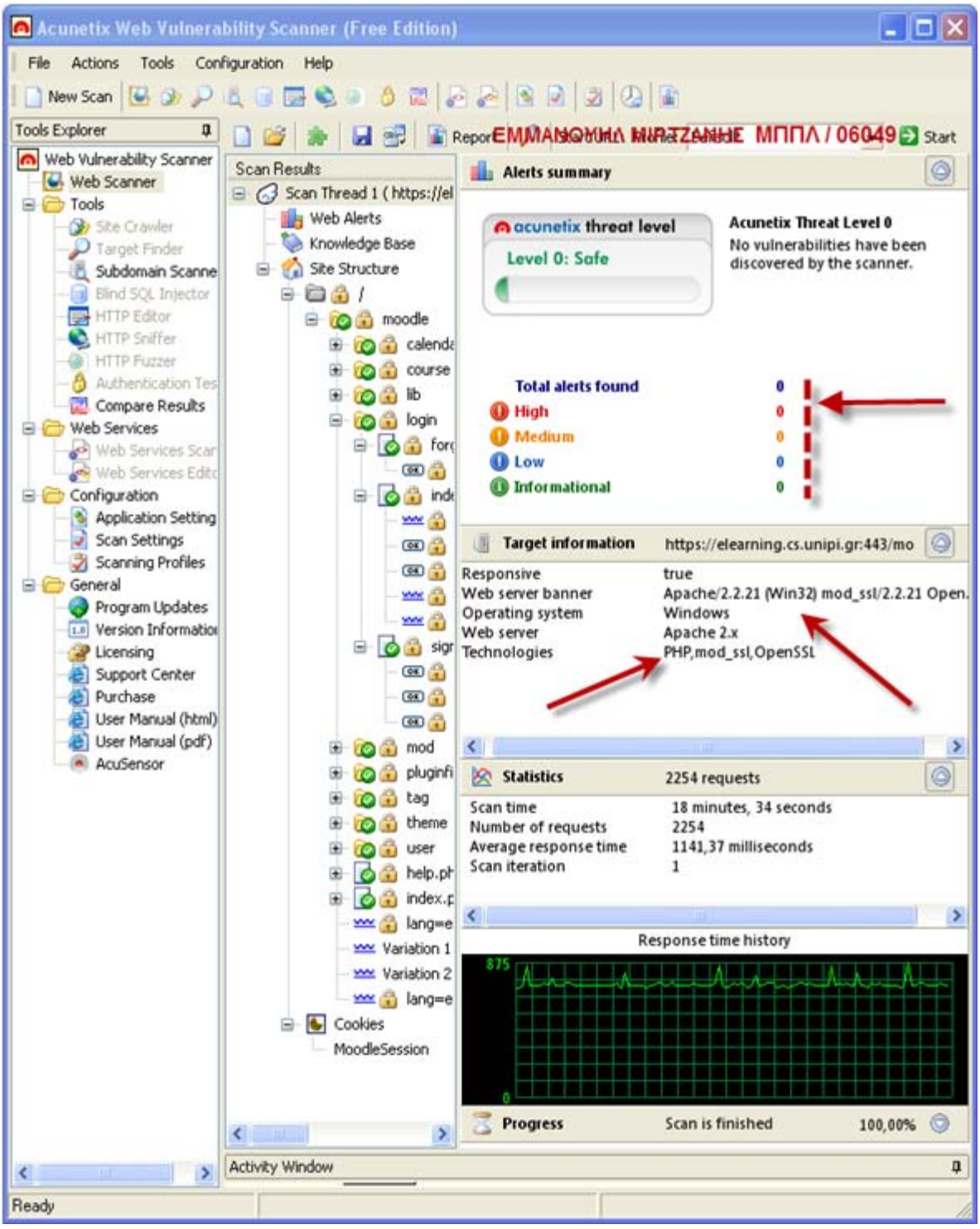


Εικόνα 5.1β Από τα 142 αιτήματα παρατηρούμε ποια επιλέχθηκαν σαν ύποπτα για XSS ευπάθεια.

Μετά την συλλογή των υπόπτων για XSS ευπάθεια αιτημάτων , επιλέγουμε ένα κάθε φορά (μία γραμμή) και μετά επιλέγουμε Check . Αν το αίτημα μεταφέρεται στο κάτω μέρος του παραθύρου τότε έχουμε επιβεβαίωση της υποψίας. Αυτή η ενέργεια επανελήφθη και για τα 7 ύποπτα αιτήματα , χωρίς όμως να μεταφερθεί κανένα αίτημα. Αυτό δεν σημαίνει , ότι δεν υπάρχουν XSS ευπάθειες. Σκόπιμα προκλήθησαν αιτήματα στην εφαρμογή , τέτοια για τα οποία με άλλο εργαλείο , το Acunetix , είχαν εντοπιστεί XSS ευπάθειες . Το Acunetix , εικόνα 5.1γ , είναι ένας scanner ευπαθειών που διατίθεται στο εμπόριο. Ο έλεγχος με το Acunetix διήρκεσε περίπου 25 λεπτά , και υλοποίησε 5029 αιτήματα στην εφαρμογή για την ολοκλήρωσή του. Το αποτέλεσμα ήταν ο εντοπισμός 170 XSS ευπαθειών υψηλού κινδύνου, εντυπωσιακό σε σχέση με το δείγμα ελέγχων του WebScarab και μας δίνει την εντύπωση ότι έχει πολύ καλή αξιοπιστία , τουλάχιστο για την συγκεκριμένη κατηγορία ελέγχων. Γενικά το Acunetix δεν εντοπίζει το σύνολο των ευπαθειών , αλλά και οι άλλοι scanners. Το γεγονός αυτό επιβάλλει και τους χειροκίνητους ελέγχους. Το όφελος βέβαια είναι ο συντομότερος χρόνος εντοπισμού της XSS ευπάθειας , με ακριβή αναφορά του αρχείου και της μεταβλητής στην οποία εντοπίσθηκε η ευπάθεια και κατά συνέπεια η άμεση παρέμβαση διόρθωσης της. Η συμπληρωματικότητα των χειροκίνητων ελέγχων από έμπειρο ελεγκτή είναι αναγκαία.



Εικόνα 5.1γ Τα αποτελέσματα των ελέγχων για XSS με το Acunetix για το eclass.



Εικόνα 5.1δ Τα αποτελέσματα των ελέγχων για XSS με το Acunetix για το elearning.

Ο έλεγχος με το Acunetix στο **https://elearning.cs.unipi.gr** με την πλατφόρμα του Moodle , είχε σαν αποτέλεσμα μηδέν XSS ευπάθειες.

6 DENIAL OF SERVICE TESTING

6.1 LOCKING CUSTOMER ACCOUNTS

Σε αυτό τον έλεγχο πρέπει να εξετάσουμε, αν το eClass, προβλέπει μηχανισμό κλειδώματος ενός λογαριασμού με γνωστό username , σε περίπτωση σχετικά μεγάλου αριθμού προσπαθειών αυθεντικοποίησης με λάθος κωδικό. Αν συμβαίνει κάτι τέτοιο, ένας κακόβουλος χρήστης, θα μπορούσε να προκαλέσει, είτε χειρονακτικά είτε με ένα κατάλληλο λογισμικό , μεγάλο αριθμό login σε γνωστά usernames με σκόπιμα εσφαλμένους κωδικούς , ώστε να κλειδωθούν οι λογαριασμοί και να χρειάζεται παρέμβαση του διαχειριστή της εφαρμογής, για να επαναλειτουργήσει ο λογαριασμός χρήστη. Χρησιμοποιώντας το δικό μου username με λαθεμένους κωδικούς για 25 φορές , έγινε μετά προσπάθεια login την 26^{η} με το σωστό κωδικό. Το eClass με αυθεντικοποίησε κανονικά , που σημαίνει ότι πιθανότατα δεν κλειδώνει τον λογαριασμό. Βέβαια θα μπορούσε κάτι τέτοιο να συμβαίνει σε μεγαλύτερο αριθμό προσπαθειών, μάλλον απίθανο. Ταυτόγχρονα όμως , μία τέτοια πολιτική δίνει τη δυνατότητα για Enumaration επιθέσεις. Η εφαρμογή προβλέπει τη χρήση CAPTCHA, αλλά δεν έχει ενεργοποιηθεί από τον διαχειριστή. Άλλες εφαρμογές δίνουν την δυνατότητα για περιορισμένο αριθμό login και επιτρέπουν την συνέχιση μετά από διακοπή κάποιου χρονικού διαστήματος ή κάποιου άλλου κριτηρίου.