



Ασφάλεια διαδικτυακών εφαρμογών: σχεδιαστικές λύσεις και αξιολόγηση της ασφάλειας

Μπεκιάρη Κωνσταντίνα
AM: 59913118

Επιβλέπων καθηγητής: Τριανταφύλλου Ιωάννης

Αντικείμενο πτυχιακής εργασίας

Θέμα:

Ασφάλεια διαδικτυακών εφαρμογών:
σχεδιαστικές λύσεις και αξιολόγηση της ασφάλειας

**Βάσει των παραπάνω,
έχει πραγματοποιηθεί:**

- σχεδίαση και ανάπτυξη μίας διαδικτυακής εφαρμογής και
- αξιολόγηση της ασφάλειας της μέσω hacking

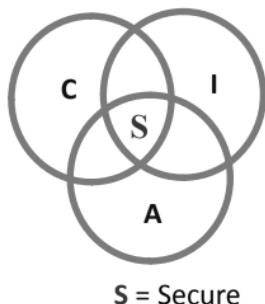
Με στόχο να μελετηθεί το συγκεκριμένο φαινόμενο, έχουν μελετηθεί:

- τα χαρακτηριστικά των διαδικτυακών εφαρμογών
- η ασφάλεια πληροφοριών στο διαδίκτυο
- το hacking (penetration testing) σε σχέση με την αξιολόγηση της ασφάλειας και
- οι προϋποθέσεις σχεδίασης και ανάπτυξης ασφαλών διαδικτυακών εφαρμογών

Θεμελιώδεις αρχές ασφάλειας

1. Εμπιστευτικότητα (Confidentiality)
2. Ακεραιότητα (Integrity)
3. Διαθεσιμότητα (Availability)

Επιπρόσθετα στοιχεία ασφάλειας:



- Αυθεντικοποίηση (Authentication)
- Εξουσιοδότηση (Authorization)
- Μη-αποποίηση (Non-repudiation)
- Λογιστική καταγραφή (Accounting)

Αρχές ασφαλούς προγραμματισμού

Η Αρχή της Ελάχιστης Επιφάνειας Επίθεσης

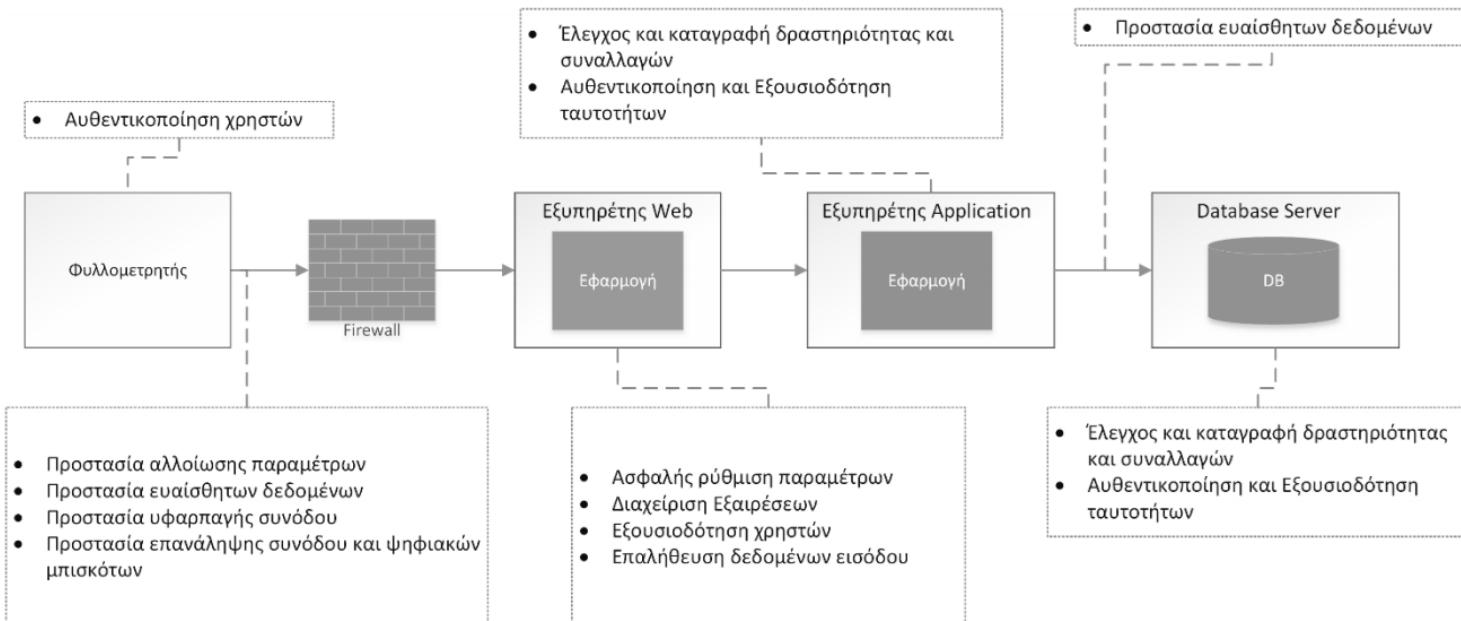
Η Αρχή του Ελάχιστου Προνομίου

Η Αρχή του Διαχωρισμού Καθηκόντων

Η Αρχή της Απλότητας

- + Η χρήση περισσότερων του ενός μηχανισμών ασφάλειας.
- + **Security by obscurity.**

Σημαντικά ζητήματα ασφάλειας



Εικόνα 1. Μία τυπική αρχιτεκτονική μίας διαδικτυακής εφαρμογής συσχετιζόμενη με τα επιμέρους ζητήματα ασφάλειας διαδικτυακής εφαρμογής (πηγή: Μαυρίδης, 2015)



TOP 10
αδυναμίες
από την
OWASP -
2021

Injection

Broken Authentication

Sensitive Data Exposure

XXE (XML External Entities)

Broken Access Control

Security Misconfiguration

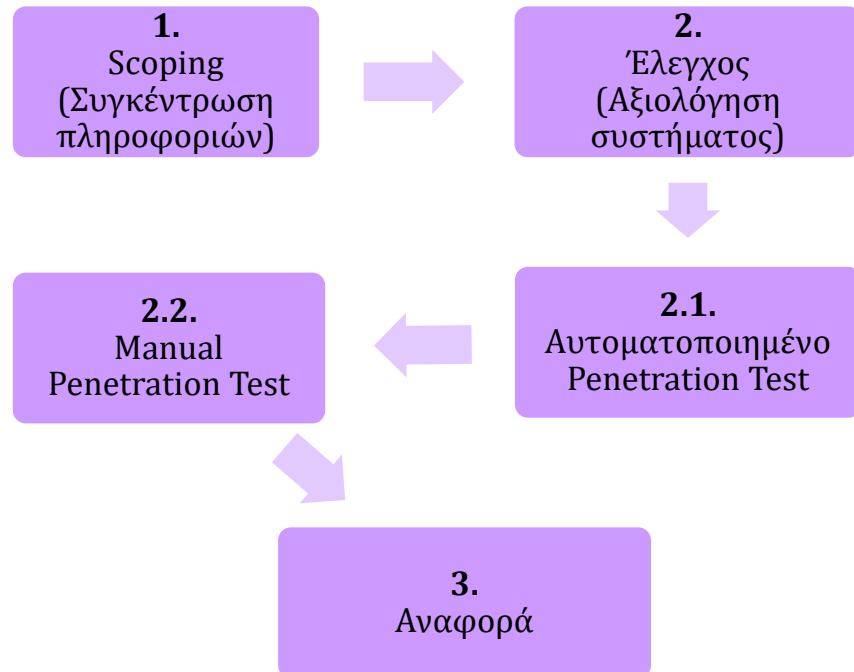
XSS (Cross-Site Scripting)

Insecure Deserialization

Using Components with Known Vulnerabilities

Insufficient Logging and Monitoring

Αξιολόγηση ασφάλειας διαδικτυακών εφαρμογών



Τεχνικές ενίσχυσης ασφάλειας 1/2

Back-end κώδικας

Waf (**Web Application Firewall**)

Two-factor Authentication

Κρυπτογραφία

LDAP (**Lightweight Directory Access Protocol**)

Firewall

IDS/IPS (**Intrusion Detection System/ Intrusion Prevention System**)

Τεχνικές ενίσχυσης ασφάλειας 2/2



Injection

Insecure Deserialization

Sensitive Data Exposure

Broken Authentication

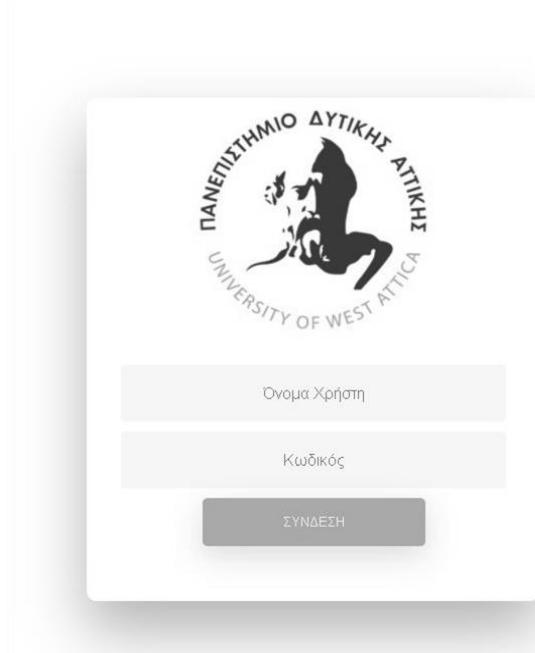
Broken Access Control

Security Misconfiguration

Using Vulnerable Components

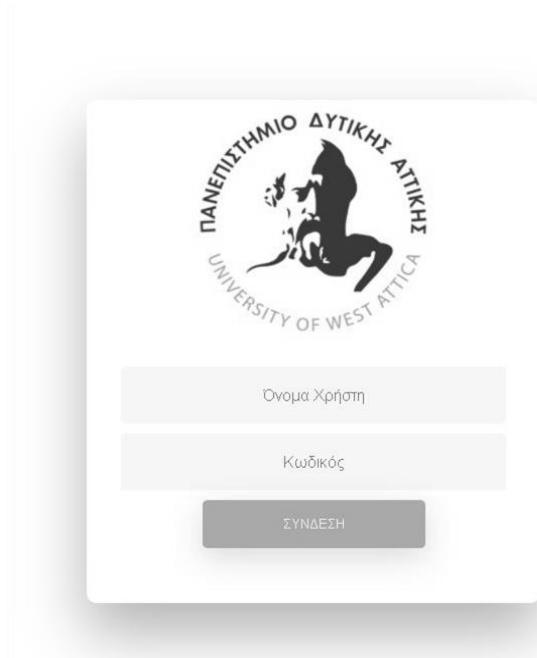
Insufficient Logging and Monitoring

Περιγραφή εφαρμογής “UniStudent”



- Πρόκειται για μία εφαρμογή, τύπου Φοιτητολογίου – E-study, η οποία έχει σχεδιαστεί με βάση την ασφάλεια.
- Απευθύνεται στους φοιτητές που είναι εγγεγραμμένοι σε ένα τμήμα και βρίσκεται online στη διεύθυνση <https://www.unistudent.eu>.

Περιγραφή εφαρμογής “*UniStudent*”



- Αποτελείται από 3 υπηρεσίες (σελίδες):
 - Προφίλ,
 - Δηλώσεις,
 - Βαθμολογίες.

Προφίλ φοιτητή

The screenshot shows a user interface for managing a student profile. The top navigation bar includes the UniStudent logo, a search bar, and a sign-in button. On the left, there's a sidebar with links for 'ΠΡΟΦΙΛ', 'ΒΑΘΜΟΛΟΓΙΕΣ', and 'ΔΗΛΩΣΕΙΣ'. The main content area is titled 'Στοιχεία' (Details) and contains two sections: 'Χρήστης' (User) and 'Διεύθυνση' (Management). The 'Χρήστης' section lists personal information: Όνομα Χρήστη (Name): ηπία, Όνομα (Name): Κωνσταντίνα, Επίθετο (Surname): Μπακιάρη, ΑΕΜ (AEM): lb13118, Τμήμα (Faculty): ΑΡΧΕΙΟΝΟΜΙΑΣ, ΒΙΒΛΙΟΘΗΚΟΝΟΜΙΑΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΗΣΗΣ, Εξάμηνο (Semester): 15, Τηλέφωνο (Phone): 6977262017, and Email: lb13118@uniwa.gr. The 'Διεύθυνση' section lists administrative details: Οδός (Address): Αμυντανδρου 11, Τ.Κ. (Postal Code): 11741, Πόλη (City): Κουκάκι, Αθήνα, and Χώρα (Country): Ελλάδα.

Χρήστης	
Όνομα Χρήστη	ηπία
Όνομα	Κωνσταντίνα
Επίθετο	Μπακιάρη
ΑΕΜ	lb13118
Τμήμα	ΑΡΧΕΙΟΝΟΜΙΑΣ, ΒΙΒΛΙΟΘΗΚΟΝΟΜΙΑΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΗΣΗΣ
Εξάμηνο	15
Τηλέφωνο	6977262017
Email	lb13118@uniwa.gr

Διεύθυνση	
Οδός	Αμυντανδρου 11
Τ.Κ.	11741
Πόλη	Κουκάκι, Αθήνα
Χώρα	Ελλάδα

Δηλώσεις φοιτητή

The screenshot shows the UniStudent application interface. The left sidebar has a dark theme with three main buttons: ΠΡΟΦΙΛ (Profile), ΒΑΘΜΟΛΟΓΙΣΣΕΣ (Grades), and ΔΗΛΩΣΕΙΣ (Applications). The main content area has a light background. At the top, there's a blue header bar with the text "Δηλώσεις". Below it is a purple header "ΠΕΡΙΟΔΟΣ ΔΗΛΩΣΗΣ" with a dropdown menu showing "Όλες οι δηλώσεις", "ΕΑΡ 2016-2017", and "ΧΕΙΜ 2017-2018". The main table lists various applications:

Μάθημα	Εξάμηνο	ECTS	ΔΜ	Τόπος	ΕΑΡ 2016-2017	ΧΕΙΜ 2017-2018
Αρχεία επανειρήσεων	11	4	2	Υποχρεωτικό κατ' επιλογήν	EAP 2016-2017	
Π-8020 Διακείριση πολιτιστικών αγαθών	11	6	3	Υποχρεωτικό	EAP 2016-2017	
Π-6070 Ιστορία γραφής και τεχνολογίας των πληροφοριών	11	4	2	Υποχρεωτικό κατ' επιλογήν	EAP 2017-2018	
Π-7020 Διακείριση ενεργών αρχείων	11	7	2	Υποχρεωτικό		ΧΕΙΜ 2017-2018
Π-7030 Διακείριση έργων	11	5	3	Υποχρεωτικό		ΧΕΙΜ 2017-2018
Π-7010 Εφαρμογές στον παγκόσμιο ιστό	11	6	2	Υποχρεωτικό		ΧΕΙΜ 2017-2018
Π-1040 Κοινωνία και πληροφορία	11	5	3	Υποχρεωτικό		ΧΕΙΜ 2017-2018

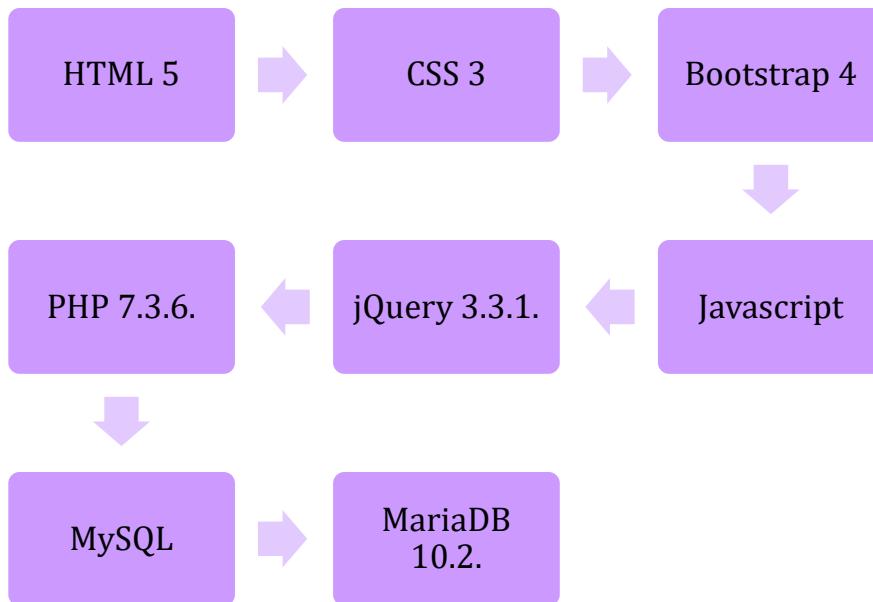
Βαθμολογίες φοιτητή

The screenshot shows the UniStudent mobile application interface. The top navigation bar includes the UniStudent logo, a search bar, and a sign-in button labeled "Εγγραφή". On the left, a vertical sidebar features three tabs: "ΠΡΟΦΙΛ" (Profile), "ΒΑΘΜΟΛΟΓΙΕΣ" (Grades), and "ΔΗΛΩΣΕΙΣ" (Statements). The main content area is titled "Βαθμολογίες" (Grades) and displays a table of academic records. The table has columns for "Κωδικός Μαθήματος" (Course Code), "Μάθημα" (Subject), "Εξάμηνα" (Semester), "ECTS", "ΔΜ" (DM), "Τύπος" (Type), and "Βαθμός" (Grade). The data is as follows:

Κωδικός Μαθήματος	Μάθημα	Εξάμηνα	ECTS	ΔΜ	Τύπος	Βαθμός
Π-7060	Αρχεία επιχειρήσεων	11	4	2	Υποχρεωτικό κατ' επιλογήν	8
Π-7020	Διαχείριση ενεργών αρχείων	11	7	2	Υποχρεωτικό	10
Π-7030	Διαχείριση έργων	11	5	3	Υποχρεωτικό	9
Π-8020	Διαχείριση πολιτιστικών αγαθών	11	6	3	Υποχρεωτικό	10
Π-7010	Εφαρμογές στον παγκόσμιο ιστό	11	6	2	Υποχρεωτικό	10
Π-6070	Ιστορία γραφής και τεχνολογίας των πληροφοριών	11	4	2	Υποχρεωτικό κατ' επιλογήν	8
Π-1040	Κοινωνία και πληροφορία	11	5	3	Υποχρεωτικό	5

Σχεδίαση και ανάπτυξη εφαρμογής 1/2

Για την ανάπτυξη
της εφαρμογής
χρησιμοποιήθηκαν
οι εξής τεχνολογίες:



Σχεδίαση και ανάπτυξη εφαρμογής 2/2

Η εφαρμογή έχει αναπτυχθεί με στόχο να δεχθεί και να αμυνθεί σε επιθέσεις τύπου:

SQL Injection

PHP Injection

Broken Authentication

Sensitive Data Exposure

Security Misconfiguration

Brute Force

XSS

Περιγραφή βάσης



Τεχνικές ασφάλειας εφαρμογής 1/3

- Για την αποφυγή **XSS**, **SQL** και **PHP Injections** φιλτράρεται η εισαγωγή δεδομένων και αποκόπτονται:
 - κενά,
 - ειδικοί χαρακτήρες.
- Οι κωδικοί πρόσβασης είναι αποθηκευμένοι στον πίνακα **uni_users** και κρυπτογραφημένοι με τη χρήση του **Bcrypt**.
- Η εφαρμογή προστατεύεται επίσης από **Επιθέσεις αποκάλυψης πληροφοριών**, αποτρέποντας τον επιτιθέμενο από το να δει τον κατάλογο αρχείων.

Τεχνικές ασφάλειας εφαρμογής 2/3

- Σχετικά με την παραβίαση **Broken authentication**, έχει αποφευχθεί η χρήση **Cookies**. Το session id αποθηκεύεται στον server, οπότε είναι αδύνατο να κλαπούν πληροφορίες της session.
- Για την παρεμπόδιση **Brute Force επιθέσεων**,
 - αν η επίθεση περιέχει αλφαριθμητικούς χαρακτήρες, μετά από 5 αποτυχημένες προσπάθειες εντός 1 ώρας, ο χρήστης ανακατευθύνεται στο αρχείο **blocked.php**. Η IP διεύθυνση και η χρονική στιγμή της πρώτης λανθασμένης εισόδου καταγράφονται στον πίνακα **uni_failed_logins**.
 - αν η επίθεση περιέχει ειδικούς χαρακτήρες, η IP διεύθυνση καταγράφεται στον πίνακα **uni_blacklist**.

Τεχνικές ασφάλειας εφαρμογής 3/3



- Με την ύπαρξη ενός **honeypot** στη σελίδα σύνδεσης, όταν ο επιτιθέμενος (π.χ. bot) συμπληρώσει οτιδήποτε στο πεδίο “Don’t fill if human..” η IP διεύθυνση του μπλοκάρεται από τον server της εφαρμογής και καταγράφεται στην Blacklist.
- Για περισσότερη ασφάλεια έχει **απενεργοποιηθεί** η δυνατότητα μεταφόρτωσης αρχείων (file upload) από τις ρυθμίσεις του server.
- Τέλος, σε ένα κρυφό αρχείο (.htaccess) έχει οριστεί να **αποτρέπεται** η χρήση αιτημάτων **DELETE PUT UPDATE**.

Αξιολόγηση ασφάλειας εφαρμογής 1/6



- To penetration test της εφαρμογής:
 - βασίστηκε στις **OWASP Top 10** αδυναμίες διαδικτυακών εφαρμογών,
 - πραγματοποιήθηκε αρχικά **Black Box** και έπειτα, **White Box**.
- Χρησιμοποιήθηκαν 3 αυτοματοποιημένα εργαλεία:
 - Gobuster
 - Sqlmap
 - Nikto

Αξιολόγηση ασφάλειας εφαρμογής 2/6

Επιθέσεις εφαρμογής "UniStudent"		Αυτοματοποιημένα εργαλεία		
OWASP Top 10 αδυναμίες διαδικτυακών εφαρμογών		Sqlmap	Nikto	Gobuster
Injection		✓	✓	
Broken Authentication		✓		✓
Sensitive Data Exposure		✓		✓
XML External Entities (XXE)	-	-	-	
Broken Access Control		✓		✓
Security Misconfiguration		✓		✓
Cross Site Scripting (XSS)		✓		✓
Insecure Deserialization	-	-	-	
Using Components with Known Vulnerabilities	-	-	-	
Insufficient Logging and Monitoring	-	-	-	
Επιπρόσθετες Αδυναμίες				
Πιθανές άλλες αδυναμίες		✓		✓

Αξιολόγηση ασφάλειας εφαρμογής 3/6

- Το πιο ενδιαφέρον από τα αποτελέσματα του Gobuster είναι το αρχείο `login.php` και γι' αυτό εξετάστηκε πρώτο.
- Όταν υπάρχει σελίδα σύνδεσης, σημαίνει ότι υπάρχει κάποια βάση δεδομένων στο back-end, η οποία εξυπηρετεί την αυθεντικοποίηση.

```
[root@kali kali] $ gobuster dir -u http://192.168.1.20/unistudent/ -w /opt/SecLists/Discovery/Web-Content/directories.txt -t 10 -x php,html,txt --timeout 10 -o ./gobuster -S
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)

[+] Url:          http://192.168.1.20/unistudent/
[+] Threads:      30
[+] Wordlist:     /opt/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Extensions:   txt,html,php
[+] Timeout:       10s

2021/02/09 16:39:22 Starting gobuster

/index.php (Status: 302)
/login.php (Status: 200)
/profile.php (Status: 302)
/img (Status: 301)
/css (Status: 301)
/cgi-bin (Status: 301)
/js (Status: 301)
/logout.php (Status: 200)
/cron.php (Status: 200)
/functions.php (Status: 200)
/statements.php (Status: 302)
/font (Status: 301)
/blocked.php (Status: 200)
/authenticate.php (Status: 200)
/grades.php (Status: 302)
```

Αξιολόγηση ασφάλειας εφαρμογής 4/6

```
$ sqlmap -r sql.r --level 5 --risk 3
Forcer H Drop Intercept is off Action Open Browser Comment this
{1.4.11#stable}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual c
lopers assume no liability and are not responsible for any misuse or damage caused

[*] starting @ 16:35:28 /2021-02-09/

[16:35:28] [INFO] parsing HTTP request from 'sql.r'
[16:35:28] [WARNING] provided value for parameter 'name' is empty. Please, always
[16:35:28] [INFO] testing connection to the target URL
[16:35:28] [WARNING] the web server responded with an HTTP error code (400) which
[16:35:28] [INFO] testing if the target URL content is stable
[16:35:29] [INFO] target URL content is stable
[16:35:29] [INFO] testing if POST parameter 'username' is dynamic
[16:35:29] [WARNING] POST parameter 'username' does not appear to be dynamic
[16:35:29] [WARNING] heuristic (basic) test shows that POST parameter 'username' m
[16:35:29] [INFO] testing for SQL injection on POST parameter 'username'
[16:35:29] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[16:35:30] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[16:35:30] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[16:35:31] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subqu
```

- Το Sqlmap δεν κατάφερε να βρει κάποιο query.
- Παρατηρήθηκε ότι επιστρέφεται διαφορετικό μήνυμα λάθους, ανάλογα με τα δεδομένα εισόδου.
- Αυτό αποτελεί μία ισχυρή ένδειξη ότι η εφαρμογή ενδεχομένως να διαθέτει κάποιον **μηχανισμό ανίχνευσης χαρακτήρων**.
- Στην ίδια σελίδα υλοποιήθηκαν έλεγχοι για **XSS**, αλλά δεν βρέθηκε κάποια αδυναμία.

Αξιολόγηση ασφάλειας εφαρμογής 5/6

- Το μόνο που βρέθηκε στα αποτελέσματα του Nikto είναι το αρχείο **info.php**.

```
(kali㉿kali)-[~] ~ % cd /home/kali/Pictures/Intia
└─$ nikto -host 192.168.1.20
- Nikto v2.1.6
[...]
+ Target IP:          192.168.1.20
+ Target Hostname:    192.168.1.20
+ Target Port:        80
+ Start Time:         2021-02-17 14:30:32 (GMT-5)      sqltest.png
[...]
+ Server: Apache/2.4.46 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 2aa6, size: 5baade549c1c3, mtime: gzip
+ Allowed HTTP Methods: GET, POST, OPTIONS, HEAD
+ /info.php: Output from the phpinfo() function was found.
+ OSVDB-3233: /info.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-5292: /info.php?file=http://cirt.net/rfiinc.txt?: RFI from RSnake's list (http://ha.ckers.org/weird/rfi-locations.dat) or from http://osvdb.org/
+ 7915 requests: 0 error(s) and 8 item(s) reported on remote host
+ End Time:           2021-02-17 14:31:24 (GMT-5) (52 seconds)
```

Αξιολόγηση ασφάλειας εφαρμογής 6/6

Αδυναμίες εφαρμογής "UniStudent"			
OWASP	Top 10	αδυναμίες	Βρέθηκαν
διαδικτυακών εφαρμογών			
Injection		x	Έλεγχος δεδομένων εισόδου
Broken Authentication		x	Αποφυγή χρήσης Cookies
Sensitive Data Exposure		x	Αποφυγή σχολίων, back-up αρχείων και δοκιμαστικών directories
XML External Entities (XXE)		-	Η αδυναμία XML External Entities (XXE) απαιτεί την ύπαρξη xml κώδικα.
Broken Access Control		x	Υπαρξη μόνο 2 απλών χρηστών χωρίς αναβαθμισμένο ρόλο.
Security Misconfiguration		x	Χρήση σωστών ρυθμίσεων και πρακτικών
Cross Site Scripting (XSS)		x	Έλεγχος δεδομένων εισόδου
Insecure Deserialization		-	Η αδυναμία Insecure Deserialization απαιτεί την ύπαρξη αντικειμενοστραφούς προγραμματισμού.
Using Components with Known Vulnerabilities		-	Η αδυναμία Using Components with Known Vulnerabilities απαιτεί την ύπαρξη έτοιμων βιβλιοθηκών και συναρτήσεων.
Insufficient Logging and Monitoring		-	Η αδυναμία Insufficient Logging and Monitoring απαιτεί την ύπαρξη αρχείων logs.
Επιπρόσθετες αδυναμίες			
Information Disclosure		✓	Δεν έχει πραγματοποιηθεί κάποια προσπάθεια αποφυγής της συγκεκριμένης αδυναμίας.

Επίλογος

- Η ασφάλεια διαδικτυακών εφαρμογών κατά τη σχεδίαση και την ανάπτυξη τους θεωρείται πολύ σημαντική.

Εξίσου σημαντική είναι και η αξιολόγηση της ασφάλειας τους μέσω hacking (penetration testing).

- Υπάρχουν διάφορες τεχνικές και μέθοδοι ασφάλειας, τόσο σε επίπεδο εφαρμογής όσο και σε επίπεδο συστήματος και δικτύου.

Οι επαγγελματίες διαφορετικών ειδικοτήτων, οι οποίοι συμμετέχουν στη σχεδίαση και στην ανάπτυξη μίας εφαρμογής, θα πρέπει:

- να έχουν πρακτική και θεωρητική γνώση
- να εξελίσσονται συνεχώς και
- να είναι σε θέση να συνεργαστούν μεταξύ τους, με στόχο να βρεθεί η “χρυσή τομή”.

Βασικός στόχος τους θα πρέπει να είναι η ύψιστη δυνατή ασφάλεια.