# Threat Modeling Report

Created on 3/2/2025 11:46:12 AM

**Threat Model Name:** Open Eclass 1.1

**Owner:** -

**Reviewer:** -

**Contributors:** -

**Description:** Παροχή διαδικτυακών εκπαιδευτικών υπηρεσιών σε φοιτητές και εκπαιδευτικούς. Οι φοιτητές μπορούν να εγγραφούν σε μαθήματα, να κατεβάζουν εκπαιδευτικό υλικό και να ανεβάζουν εργασίες. Οι εκπαιδευτικοί μπορούν να δημιουργούν/επεξεργάζονται μαθήματα, να ανεβάζουν σημειώσεις/διαφάνειες, να διαχειρίζονται βαθμολογίες και να βλέπουν αναφορές προόδου φοιτητών.

**Assumptions:** Διαχείριση Μαθημάτων: Ο εκπαιδευτικός δημιουργεί/διαχειρίζεται το μάθημα, ανεβάζει εκπαιδευτικό υλικό. Υποβολή Εργασιών: Ο φοιτητής ανεβάζει την εργασία του, και ο εκπαιδευτικός τη βαθμολογεί. Ενημέρωση & Συνεργασία: Ανακοινώσεις, δημοσίευση βαθμών.

**External Dependencies:** HTTPS / TLS: Απαιτείται κρυπτογραφημένη επικοινωνία μεταξύ browser και server. Web Server: Apache Firewall: Προστατεύει το εσωτερικό δίκτυο, φιλτράρει απροσδόκητα αιτήματα. Database (MySQL): Αποθήκευση δεδομένων χρηστών, μαθημάτων, βαθμολογιών. File Storage: Χώρος αποθήκευσης των αρχείων (σημειώσεις, διαφάνειες, εργασίες).

### Threat Model Summary:

|  |  |
| --- | --- |
| Not Started | 0 |
| Not Applicable | 6 |
| Needs Investigation | 22 |
| Mitigation Implemented | 15 |
| Total | 43 |
| Total Migrated | 0 |

## Diagram: High-Level-diagram

High-Level-diagram diagram screenshot
            

### High-Level-diagram Diagram Summary:

|  |  |
| --- | --- |
| Not Started | 0 |
| Not Applicable | 6 |
| Needs Investigation | 22 |
| Mitigation Implemented | 15 |
| Total | 43 |
| Total Migrated | 0 |

### Interaction: data

data interaction screenshot
      

#### 1. Web Server Process Memory Tampered  [State: Not Applicable]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Tampering |
| **Description:** | If Web Server is given access to memory, such as shared memory or pointers, or is given the ability to control what Browser Client executes (for example, passing back a function pointer.), then Web Server can tamper with Browser Client. Consider if the function could work with less access to memory, such as passing data rather than pointers. Copy in data provided, and then validate it. |
| **Justification:** | Σενάριο shared memory/pointers σπάνιο σε τυπική web app. Δεν περιγράφεται τέτοια επικοινωνία. |

#### 2. Elevation Using Impersonation  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | Browser Client may be able to impersonate the context of Web Server in order to gain additional privilege. |
| **Justification:** | απαιτείται έρευνα γύρω από τους τύπους αρχείων που θα επιτρέπουμε και τα περιβάλλοντα εκτέλεσης τους |

### Interaction: file request

file request interaction screenshot
      

#### 3. Spoofing the Web Server Process  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Spoofing |
| **Description:** | Web Server may be spoofed by an attacker and this may lead to unauthorized access to File System. Consider using a standard authentication mechanism to identify the source process. |
| **Justification:** | δύσκολο λόγω της δομής, αλλά απαιτείται έρευνα |

#### 4. Spoofing of Destination Data Store File System  [State: Not Applicable]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Spoofing |
| **Description:** | File System may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of File System. Consider using a standard authentication mechanism to identify the destination data store. |
| **Justification:** | Το File System θεωρείται τοπικό. Άρα δεν υφίσταται “spoofing FS” στο ίδιο VM. |

#### 5. The File System Data Store Could Be Corrupted  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Tampering |
| **Description:** | Data flowing across file request may be tampered with by an attacker. This may lead to corruption of File System. Ensure the integrity of the data flow to the data store. |
| **Justification:** | Καλύπτεται από Least Privilege permissions, και τους upload ελέχγους |

#### 6. Data Store Denies File System Potentially Writing Data  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Repudiation |
| **Description:** | File System claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data. |
| **Justification:** | Εφαρμόζεται Logging/Auditing. Αν υπάρχει σωστό log, μπορούμε να αποδείξουμε τι γράφτηκε. |

#### 7. Potential Excessive Resource Consumption for Web Server or File System  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Denial Of Service |
| **Description:** | Does Web Server or File System take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout. |
| **Justification:** | rate limits, size limits, monitoring |

#### 8. Data Flow HTTPS request Is Potentially Interrupted  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Denial Of Service |
| **Description:** | An external agent interrupts data flowing across a trust boundary in either direction. |
| **Justification:** | network and infrastructure, θέλει διερεύνηση, ίσως κάποια εφαρμογή WAF ή άλλης λύσης μελλοντικά |

#### 9. Data Store Inaccessible  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Denial Of Service |
| **Description:** | An external agent prevents access to a data store on the other side of the trust boundary. |
| **Justification:** | network and infrastructure, θέλει διερεύνηση, ίσως κάποια εφαρμογή WAF ή άλλης λύσης μελλοντικά |

### Interaction: file response

file response interaction screenshot
      

#### 10. Spoofing of Source Data Store File System  [State: Not Applicable]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Spoofing |
| **Description:** | File System may be spoofed by an attacker and this may lead to incorrect data delivered to Web Server. Consider using a standard authentication mechanism to identify the source data store. |
| **Justification:** | Το File System θεωρείται τοπικό. Άρα δεν υφίσταται “spoofing FS” στο ίδιο VM. |

#### 11. Cross Site Scripting  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Tampering |
| **Description:** | The web server 'Web Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input. |
| **Justification:** | δεν υλοποιείται ακόμα encoding ή filtering, βέβαια δεν υπάρχουν και υποδοχές εισαγωγής ελεύθερου κειμένου. Χρειάζεται περαιτέρω έλεγχος σε επόμενη φάση |

#### 12. Persistent Cross Site Scripting  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Tampering |
| **Description:** | The web server 'Web Server' could be a subject to a persistent cross-site scripting attack because it does not sanitize data store 'File System' inputs and output. |
| **Justification:** | δεν υλοποιείται ακόμα encoding ή filtering, βέβαια δεν υπάρχουν και υποδοχές εισαγωγής ελεύθερου κειμένου. Χρειάζεται περαιτέρω έλεγχος σε επόμενη φάση |

#### 13. Potential Data Repudiation by Web Server  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Repudiation |
| **Description:** | Web Server claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data. |
| **Justification:** | Εφαρμόζεται Logging/Auditing. Αν υπάρχει σωστό log, μπορούμε να αποδείξουμε τι γράφτηκε. |

#### 14. Weak Access Control for a Resource  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Information Disclosure |
| **Description:** | Improper data protection of File System can allow an attacker to read information not intended for disclosure. Review authorization settings. |
| **Justification:** | Server-Side Auth Checks, least-privilege, RBAC. |

#### 15. Potential Process Crash or Stop for Web Server  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Denial Of Service |
| **Description:** | Web Server crashes, halts, stops or runs slowly; in all cases violating an availability metric. |
| **Justification:** | network and infrastructure, θέλει διερεύνηση, ίσως κάποια εφαρμογή WAF ή άλλης λύσης μελλοντικά |

#### 16. Data Flow HTTPS request Is Potentially Interrupted  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Denial Of Service |
| **Description:** | An external agent interrupts data flowing across a trust boundary in either direction. |
| **Justification:** | network and infrastructure, θέλει διερεύνηση, ίσως κάποια εφαρμογή WAF ή άλλης λύσης μελλοντικά |

#### 17. Data Store Inaccessible  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Denial Of Service |
| **Description:** | An external agent prevents access to a data store on the other side of the trust boundary. |
| **Justification:** | network and infrastructure, θέλει διερεύνηση, ίσως κάποια εφαρμογή WAF ή άλλης λύσης μελλοντικά |

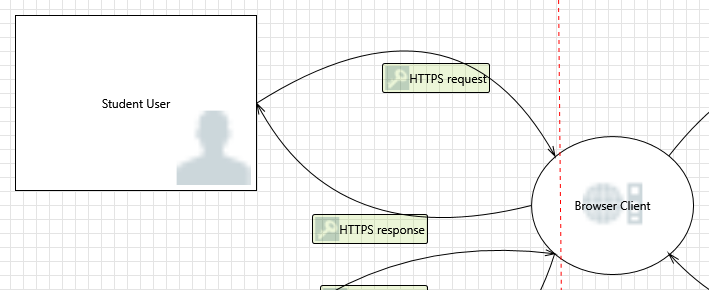
#### 18. Web Server May be Subject to Elevation of Privilege Using Remote Code Execution  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | File System may be able to remotely execute code for Web Server. |
| **Justification:** | απαιτείται έρευνα γύρω από τους τύπους αρχείων που θα επιτρέπουμε και τα περιβάλλοντα εκτέλεσης τους |

#### 19. Elevation by Changing the Execution Flow in Web Server  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | An attacker may pass data into Web Server in order to change the flow of program execution within Web Server to the attacker's choosing. |
| **Justification:** | απαιτείται έρευνα γύρω από τους τύπους αρχείων που θα επιτρέπουμε και τα περιβάλλοντα εκτέλεσης τους |

### Interaction: HTTPS request



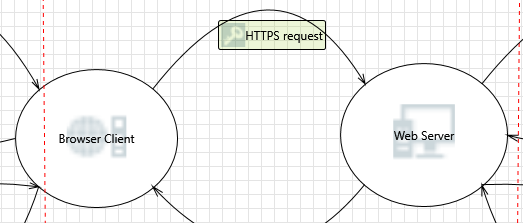
#### 20. Spoofing the Student/Teacher User External Entity  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Spoofing |
| **Description:** | Student User may be spoofed by an attacker and this may lead to unauthorized access to Browser Client. Consider using a standard authentication mechanism to identify the external entity. |
| **Justification:** | Strong Passwords, Brute Force Protection, Session tokens, server-side role ckecks |

#### 21. Elevation Using Impersonation  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | Browser Client may be able to impersonate the context of Student User in order to gain additional privilege. |
| **Justification:** | Strong Passwords, Brute Force Protection, Session tokens, server-side role ckecks |

### Interaction: HTTPS request



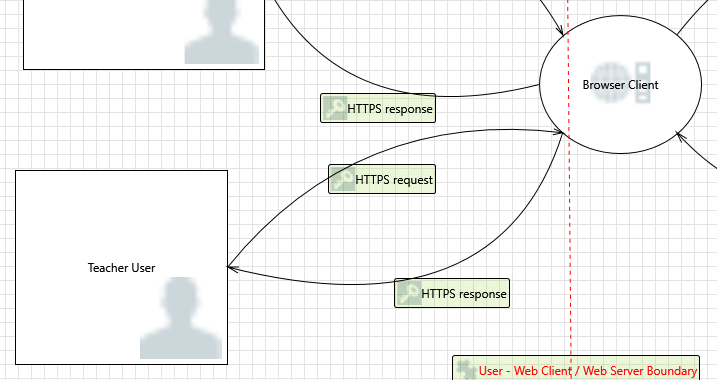
#### 22. Cross Site Scripting  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Tampering |
| **Description:** | The web server 'Web Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input. |
| **Justification:** | δεν υλοποιείται ακόμα encoding ή filtering, βέβαια δεν υπάρχουν και υποδοχές εισαγωγής ελεύθερου κειμένου. Χρειάζεται περαιτέρω έλεγχος σε επόμενη φάση |

#### 23. Elevation Using Impersonation  [State: Not Applicable]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | Web Server may be able to impersonate the context of Browser Client in order to gain additional privilege. |
| **Justification:** | Σενάριο αντίστροφο, συνήθως δεν έχει νόημα. Ο server δεν χρειάζεται να “προσποιηθεί” τον browser. |

### Interaction: HTTPS request



#### 24. Spoofing the Human User External Entity  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Spoofing |
| **Description:** | Teacher User may be spoofed by an attacker and this may lead to unauthorized access to Browser Client. Consider using a standard authentication mechanism to identify the external entity. |
| **Justification:** | Strong Passwords, Brute Force Protection, Session tokens, server-side role ckecks |

#### 25. Elevation Using Impersonation  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | Browser Client may be able to impersonate the context of Teacher User in order to gain additional privilege. |
| **Justification:** | Strong Passwords, Brute Force Protection, Session tokens, server-side role ckecks |

### Interaction: sql query

sql query interaction screenshot
      

#### 26. Spoofing the Web Server Process  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Spoofing |
| **Description:** | Web Server may be spoofed by an attacker and this may lead to unauthorized access to SQL Database. Consider using a standard authentication mechanism to identify the source process. |
| **Justification:** | δύσκολο λόγω της δομής, αλλά απαιτείται έρευνα |

#### 27. Spoofing of Destination Data Store SQL Database  [State: Not Applicable]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Spoofing |
| **Description:** | SQL Database may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of SQL Database. Consider using a standard authentication mechanism to identify the destination data store. |
| **Justification:** | Το Database θεωρείται τοπικό. Άρα δεν υφίσταται “spoofing database” στο ίδιο VM. |

#### 28. Potential SQL Injection Vulnerability for SQL Database  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Tampering |
| **Description:** | SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker. |
| **Justification:** | Parametrized queries, input validation, DB integrity checks. |

#### 29. The SQL Database Data Store Could Be Corrupted  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Tampering |
| **Description:** | Data flowing across sql query may be tampered with by an attacker. This may lead to corruption of SQL Database. Ensure the integrity of the data flow to the data store. |
| **Justification:** | Parametrized queries, input validation, DB integrity checks. |

#### 30. Data Store Denies SQL Database Potentially Writing Data  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Repudiation |
| **Description:** | SQL Database claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data. |
| **Justification:** | Εφαρμόζεται Logging/Auditing. Αν υπάρχει σωστό log, μπορούμε να αποδείξουμε τι γράφτηκε. |

#### 31. Potential Excessive Resource Consumption for Web Server or SQL Database  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Denial Of Service |
| **Description:** | Does Web Server or SQL Database take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout. |
| **Justification:** | rate limits, size limits, monitoring |

#### 32. Data Flow HTTPS request Is Potentially Interrupted  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Denial Of Service |
| **Description:** | An external agent interrupts data flowing across a trust boundary in either direction. |
| **Justification:** | network and infrastructure, θέλει διερεύνηση, ίσως κάποια εφαρμογή WAF ή άλλης λύσης μελλοντικά |

#### 33. Data Store Inaccessible  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Denial Of Service |
| **Description:** | An external agent prevents access to a data store on the other side of the trust boundary. |
| **Justification:** | network and infrastructure, θέλει διερεύνηση, ίσως κάποια εφαρμογή WAF ή άλλης λύσης μελλοντικά |

### Interaction: sql result

sql result interaction screenshot
      

#### 34. Spoofing of Source Data Store SQL Database  [State: Not Applicable]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Spoofing |
| **Description:** | SQL Database may be spoofed by an attacker and this may lead to incorrect data delivered to Web Server. Consider using a standard authentication mechanism to identify the source data store. |
| **Justification:** | Το Database θεωρείται τοπικό. Άρα δεν υφίσταται “spoofing database” στο ίδιο VM. |

#### 35. Cross Site Scripting  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Tampering |
| **Description:** | The web server 'Web Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input. |
| **Justification:** | δεν υλοποιείται ακόμα encoding ή filtering, βέβαια δεν υπάρχουν και υποδοχές εισαγωγής ελεύθερου κειμένου. Χρειάζεται περαιτέρω έλεγχος σε επόμενη φάση |

#### 36. Persistent Cross Site Scripting  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Tampering |
| **Description:** | The web server 'Web Server' could be a subject to a persistent cross-site scripting attack because it does not sanitize data store 'SQL Database' inputs and output. |
| **Justification:** | δεν υλοποιείται ακόμα encoding ή filtering, βέβαια δεν υπάρχουν και υποδοχές εισαγωγής ελεύθερου κειμένου. Χρειάζεται περαιτέρω έλεγχος σε επόμενη φάση |

#### 37. Elevation by Changing the Execution Flow in Web Server  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | An attacker may pass data into Web Server in order to change the flow of program execution within Web Server to the attacker's choosing. |
| **Justification:** | απαιτείται έρευνα γύρω από τους τύπους αρχείων που θα επιτρέπουμε και τα περιβάλλοντα εκτέλεσης τους |

#### 38. Weak Access Control for a Resource  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Information Disclosure |
| **Description:** | Improper data protection of SQL Database can allow an attacker to read information not intended for disclosure. Review authorization settings. |
| **Justification:** | Server-Side Auth Checks, least-privilege, RBAC. |

#### 39. Web Server May be Subject to Elevation of Privilege Using Remote Code Execution  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Elevation Of Privilege |
| **Description:** | SQL Database may be able to remotely execute code for Web Server. |
| **Justification:** | απαιτείται έρευνα γύρω από τους τύπους αρχείων που θα επιτρέπουμε και τα περιβάλλοντα εκτέλεσης τους |

#### 40. Data Store Inaccessible  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Denial Of Service |
| **Description:** | An external agent prevents access to a data store on the other side of the trust boundary. |
| **Justification:** | network and infrastructure, θέλει διερεύνηση, ίσως κάποια εφαρμογή WAF ή άλλης λύσης μελλοντικά |

#### 41. Data Flow HTTPS request Is Potentially Interrupted  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Denial Of Service |
| **Description:** | An external agent interrupts data flowing across a trust boundary in either direction. |
| **Justification:** | network and infrastructure, θέλει διερεύνηση, ίσως κάποια εφαρμογή WAF ή άλλης λύσης μελλοντικά |

#### 42. Potential Process Crash or Stop for Web Server  [State: Needs Investigation]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Denial Of Service |
| **Description:** | Web Server crashes, halts, stops or runs slowly; in all cases violating an availability metric. |
| **Justification:** | network and infrastructure, θέλει διερεύνηση, ίσως κάποια εφαρμογή WAF ή άλλης λύσης μελλοντικά |

#### 43. Potential Data Repudiation by Web Server  [State: Mitigation Implemented]  [Priority: High]

|  |  |
| --- | --- |
| **Category:** | Repudiation |
| **Description:** | Web Server claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data. |
| **Justification:** | Εφαρμόζεται Logging/Auditing. Αν υπάρχει σωστό log, μπορούμε να αποδείξουμε τι γράφτηκε. |