**Ερώτημα 7**

Σε αυτό το ερώτημα καλούμαστε να κάνουμε αποτίμηση κινδύνων(risk assessment) για το υπό μελέτη ΠΣ. Ουσιαστικά από τις απειλές που έχουμε εντοπίσει από τα προηγούμενα ερωτήματα, θα πρέπει να αποφασίσουμε ποιος θα έχει τις σημαντικότερες επιπτώσεις στην εφαρμογή μας, σε περίπτωση που πραγματοποιηθεί. Οι απειλές που έχουν εντοπιστεί και βαθμολογηθεί σε προηγούμενο ερώτημα είναι οι παρακάτω:

* Μη εξουσιοδοτημένη πρόσβαση στο σύστημα (Unauthorized Access).
* Επίθεση από κακόβουλο πρόγραμμα που κρυπτογραφεί τα δεδομένα και επιτρέπει ζητά την καταβολή χρηματικού ποσού για να επαναφέρει τα δεδομένα (Ransomware).
* Παραποίηση ιστοσελίδας (Web Defacement).
* Μη εξουσιοδοτημένη εκτέλεση κώδικα (Code Injection).
* Άρνηση υπηρεσίες (Denial of Service).

Οι παραπάνω απειλές έχουν λάβει ξεχωριστή βαθμολογία για κάθε ένα από τα 3 υπολογιστικά συστήματα που διαθέτει η εφαρμογή. Στην παρούσα φάση θα τα προσεγγίσουμε σε ένα γενικότερο επίπεδο, για όλο το ΠΣ, και θα καταλήξουμε στο ποια είναι τελικά η πιο ζημιογόνα. Οι σειρά με την οποία τους κατατάσσουμε είναι η εξής:

1. **Άρνηση υπηρεσίες (Denial of Service).**

Για εμάς ο σημαντικότερος κίνδυνος αποτελεί η άρνηση υπηρεσίας από την εφαρμογή μας. Το να καταφέρει κάποιος κακόβουλός να θέσει την εφαρμογή εκτός υπηρεσίας, θα ήταν κάτι το καταστροφικό. Η εφαρμογή μας έχει σκοπό την εξυπηρέτηση το σύνολο των ασθενών και των γιατρών, για την πραγματοποίηση ραντεβού κ.λπ., συνεπώς μία τέτοια ενέργεια ακυρώνει τον ίδιο το σκοπό ύπαρξης της εφαρμογής. Η άρνηση υπηρεσίας σημαίνει, πως κανείς από τους χρήστες δεν θα μπορεί να εκτελέσει την οποιαδήποτε ενέργεια, καθιστώντας την εφαρμογή άχρηστη. Εν’ κατακλείδι, σε εφαρμογές αυτού του τύπου το σημαντικότερο είναι να εκτελούνται οι λειτουργίες που προσφέρνουν, κάνοντας αυτόν τον κίνδυνο να είναι και ο σημαντικότερος.

1. **Μη εξουσιοδοτημένη εκτέλεση κώδικα (Code Injection)**

Ο δεύτερος σημαντικότερος κίνδυνος είναι η μη εξουσιοδοτημένη εκτέλεση κώδικα(Code Injection). Η πραγματοποίηση αυτής της επίθεσης είναι ιδιαίτερα επικίνδυνη για την εφαρμογή, καθώς θα μπορούσε κάποιος να παραποιήσει δεδομένα ή να κάνει ανεπιθύμητες ενέργειες στο ΠΣ. Για παράδειγμα στο επίπεδο του Data Base Server θα μπορούσε κάποιος να αλλάξει όλα τα δεδομένα των χρηστών με αποτέλεσμα να μην μπορεί κανείς να εισέλθει στην εφαρμογή. Το αποτέλεσμα μιας τέτοιας πράξης, αν και προσωρινό, θα καθιστούσε την εφαρμογή άχρηστη για όλους τους χρήστες ακυρώνοντας και πάλι τον ίδιο το σκοπό της. Ως αποτέλεσμα η απειλή αυτή παίρνει την δεύτερη θέση επικινδυνότητας, αφού όπως έχουμε προαναφέρει το σημαντικότερο είναι η λειτουργικότητα της εφαρμογής.

1. **Παραποίηση ιστοσελίδας (Web Defacement)**

Ο τρίτος σημαντικότερος κίνδυνος είναι η παραποίηση της ιστοσελίδας της εφαρμογής. Η πραγματοποίηση αυτής της επίθεσης θα μπορούσε να αλλάξει το Interface που είναι διαθέσιμο στο χρήση. Μία τέτοια ενέργεια, αν και δεν θα παρεμπόδιζε την λειτουργίας της εφαρμογής, θα έβλαπτε όχι μόνο την φήμη του οργανισμού που χρησιμοποιεί την εφαρμογή, αλλά και την εμπειρία που θα είχε ο χρήστης της εφαρμογής, καθώς πολλά στοιχεία της θα είχαν παραποιηθεί. Τελικά, θεωρούμε πως η 3η θέση είναι η σωστή για το συγκεκριμένο κίνδυνο καθώς δεν βλάπτει την πραγματική λειτουργία της εφαρμογής.

1. **Μη εξουσιοδοτημένη πρόσβαση στο σύστημα (Unauthorized Access)**

O τέταρτος σημαντικότερος κίνδυνος είναι η μη εξουσιοδοτημένη πρόσβαση στο σύστημα μας (Unauthorized Access). Η πραγματοποίηση αυτής της επίθεσης θα έδινε πρόσβαση στην εφαρμογή μας σε κάποιον κακόβουλο. Μία τέτοια ενέργεια, αν και θα μπορούσε να οδηγήσει σε κάποια σύγχυση, για παράδειγμα να κλείσει κάποιος ραντεβού με όλους τους γιατρούς και να μην παρευρεθεί σε κανένα, δεν αποτελεί άμεσος κίνδυνος λόγο της πολύ μικρής πιθανότητας να μπει κάποιος στον κόπο να την εκτελέσει. Θα ήταν ιδιαίτερα παράλογο να προσπαθήσει κάποιος να αποκτήσει πρόσβαση, αφού το μόνο που θα μπορούσε να καταφέρει θα ήταν η καταχώρηση κάποιον άκυρων-ραντεβού μέσω της εφαρμογής. Με βάση τα παραπάνω η συγκεκριμένη απειλή κατατάσσεται στην 4η θέση.

1. **Επίθεση από κακόβουλο πρόγραμμα που κρυπτογραφεί τα δεδομένα και επιτρέπει/ ζητά την καταβολή χρηματικού ποσού για να επαναφέρει τα δεδομένα (Ransomware)**

Ο πέμπτος σημαντικότερος κίνδυνος είναι η υποκλοπή/κρυπτογράφηση των δεδομένων με, από κακόβουλος, με σκοπό χρηματικές απολαβές. Ένας τέτοιος κίνδυνος θεωρείται απίθανο να πραγματοποιηθεί στην εφαρμογή μας, λόγο της φύσης των δεδομένων. Η εφαρμογή δεν διαθέτει <<ευαίσθητα δεδομένα >>, μόνο αυτά που χρειάζονται οι χρήστες για να συνδεθούν και να καταχωρήσουν τα ραντεβού τους. Συνεπώς δεν υπάρχει κίνητρο και ουσία να πραγματοποιήσει κάποιος μία τέτοια επίθεση. Με βάση τα παραπάνω αυτός ο κίνδυνος είναι μικρότερης σημασίας από όλους.

Τα παραπάνω μπορούν να εκφραστούν και από το παρακάτω πίνακα αποτίμησης κινδύνων ασφαλείας:

|  |  |  |  |
| --- | --- | --- | --- |
| Επικινδυνότητα  /Πιθανότητα Πραγματοποίησης | Κρίσιμη  (Critical) | Μεσαία(Median) | Αμελητέα(negligible) |
| Πολύ Πιθανό | Άρνηση υπηρεσίες (Denial of Service) | Μη εξουσιοδοτημένη εκτέλεση κώδικα (Code Injection) |  |
| Πιθανό |  | Παραποίηση ιστοσελίδας (Web Defacement) | Μη εξουσιοδοτημένη πρόσβαση στο σύστημα (Unauthorized Access) |
| Απίθανο |  |  | υποκλοπή/κρυπτογράφηση των δεδομένων |

High

Serious

Medium

Low

Σχόλια:

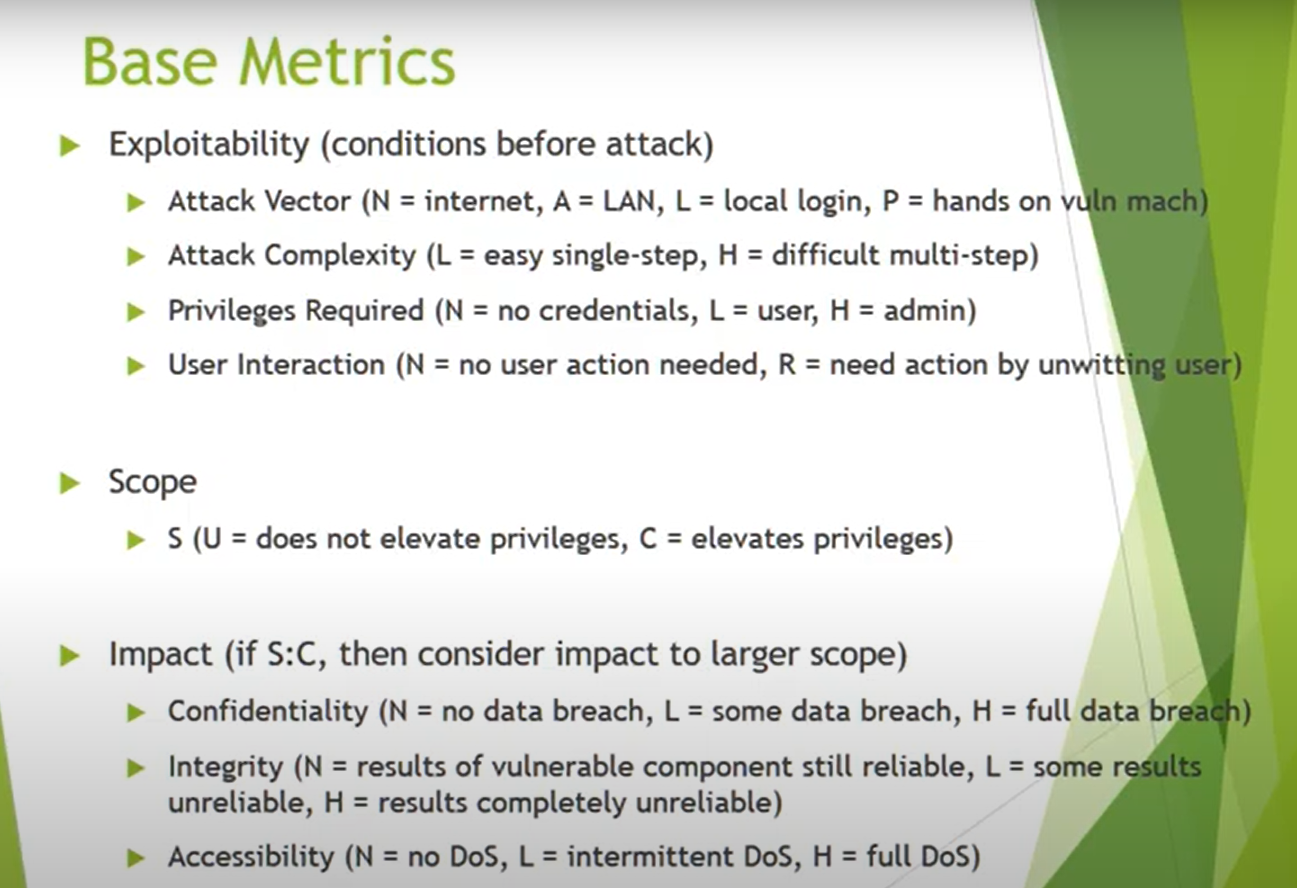
* Για την παραγωγή τον παραπάνω λάβαμε υπόψη μας τα ερωτήματα 4,5,6 της εργασίας.
* Δόθηκε σειρά επικινδυνότητας στις απειλές που έχουμε μελετήσει με βάση την πιθανή ζημιά που μπορούν να κάνουν και το πόσο πιθανό είναι να γίνουν.

**Ερώτημα 8**

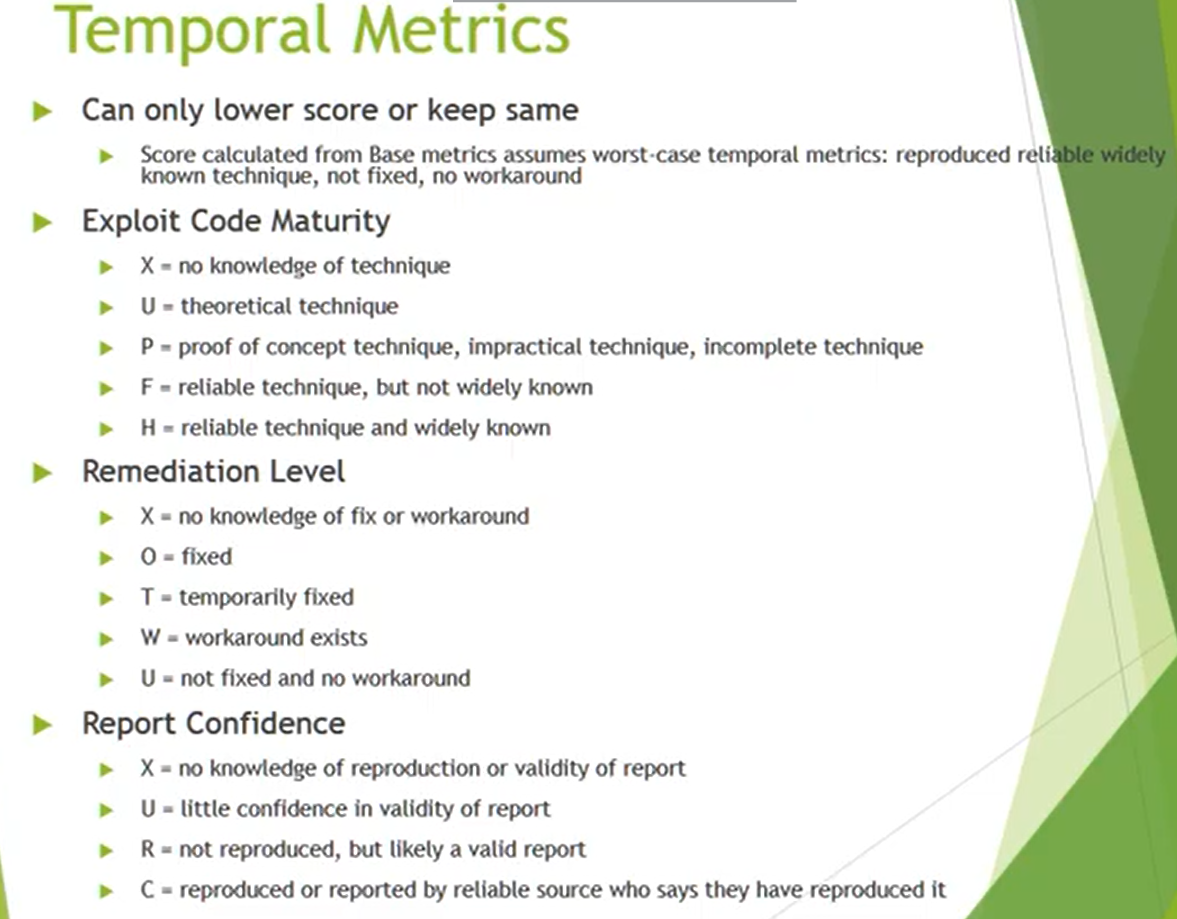
Σε αυτό το ερώτημα πρέπει να πραγματοποιήσουμε επανεκτίμηση των αδυναμιών ασφάλειας που είχαμε αποτιμήσει στο βήμα (6), κάνοντας χρήση του εργαλείου CVSS V3. Για κάθε μία από τις απειλές του προηγούμενου ερωτήματος, θα τροποποιήσουμε κατάλληλα το temporal score και το environmental score του calculator, αλλά και θα τεκμηριώσουμε, ποια επιπρόσθετα μέτρα ασφάλειας, που υλοποιήσαμε, επηρέασαν την απόφαση μας, όσο αναφορά τις τροποποιήσεις μας.

Αρχικά θα εξηγήσουμε, τι σημαίνει η κάθε παράμετρος στα scores του calculators ώστε να μην χρειάζεται να αναφέρουμε κάθε φορά τι αλλαγή κάνουμε, παρά μόνο να παραθέτουμε ένα σχετικό screenshot. Αναλυτικά έχουμε:

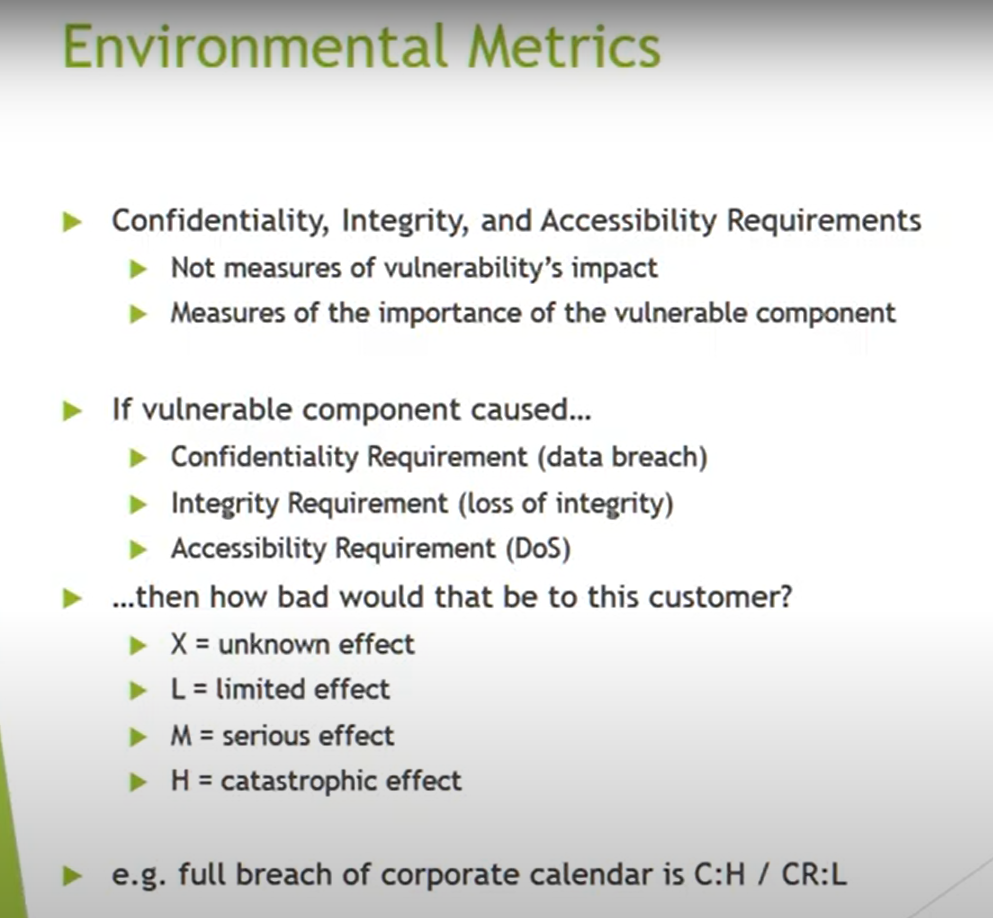
* **Base Metrics**

****

* **Temporal Metrics**

****

* **Environmental Metrics**

****

**Σχόλια:**

* Έκδοση CVSS Version 3.1
* Τα παραπάνω είναι επεξηγήσεις των παραμέτρων που θα δώσουμε για να πάρουμε την τελική βαθμολογία (Score).
* Το Base-Metrics δεν θα το αλλάξουμε σε κανένα κίνδυνο, καθώς έχει ήδη οριστεί από το NIST στην αρχική αξιολόγηση των κινδύνων και δεν επηρεάζεται από την φύση της εφαρμογής μας ή τα μέτρα ασφαλείας που έχουμε λάβει.
* Πηγή: https://www.youtube.com/watch?v=ui4l0lBBSlw

Οι κίνδυνοι που θα διερευνήσουμε, για κάθε ένα αγαθό ξεχωριστά, είναι αυτοί του ερωτήματος 6. Αναλυτικότερα:

1. **Λειτουργικό Σύστημα: Windows 10 x64**

* Windows TCP/IP Remote Code Execution Vulnerability
* Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability
* Server Service Remote Protocol Elevation of Privilege Vulnerability.

1. **Εξυπηρετητής Ιστού και εφαρμογής: Αpache Tomcat v. 8.5.6**

* Application Continues Using Socket After It Has Been Closed.
* An Incorrect Default Permissions Vulnerability In The Packaging Of Tomcat
* Βug\_63362 Introduced Α Memory Leak **(για την συγκεκριμένη δεν θα αναφερθούμε καθώς αποτελεί περισσότερο Bug/Error παρά κακόβουλη επίθεση)**

1. **Εξυπηρετητής βάσης δεδομένων: MySQL v 8.0.31**

* Vulnerability in the MySQL Server product of Oracle MySQL.
* Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer).

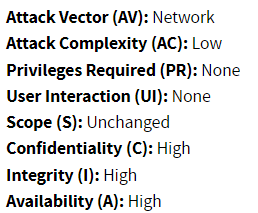
Τα μέτρα ασφαλείας που έχουμε υλοποιήσει και θα λάβουμε υπόψη μας για την διαμόρφωση των παραμέτρων, συνεπώς και των τελικών βαθμολογιών, είναι:

* Η Εισαγωγή στην εφαρμογή απαιτεί την εκχώρηση ονόματος και κωδικού από τον χρήστη.
* Εξουσιοδότηση με λειτουργία ‘’Radio Buttons’’. O χρήστης επιλέγει το ρόλο του και υπάρχει κατάλληλη αυθεντικοποίηση του ρόλου που έχει επιλεγεί (Server Side)
* Input Validation με χρήση ‘’Regular Expressions’’ (Client Side και Server Side).
* Χρήση πρωτόκολλου https για την λειτουργία της εφαρμογής.

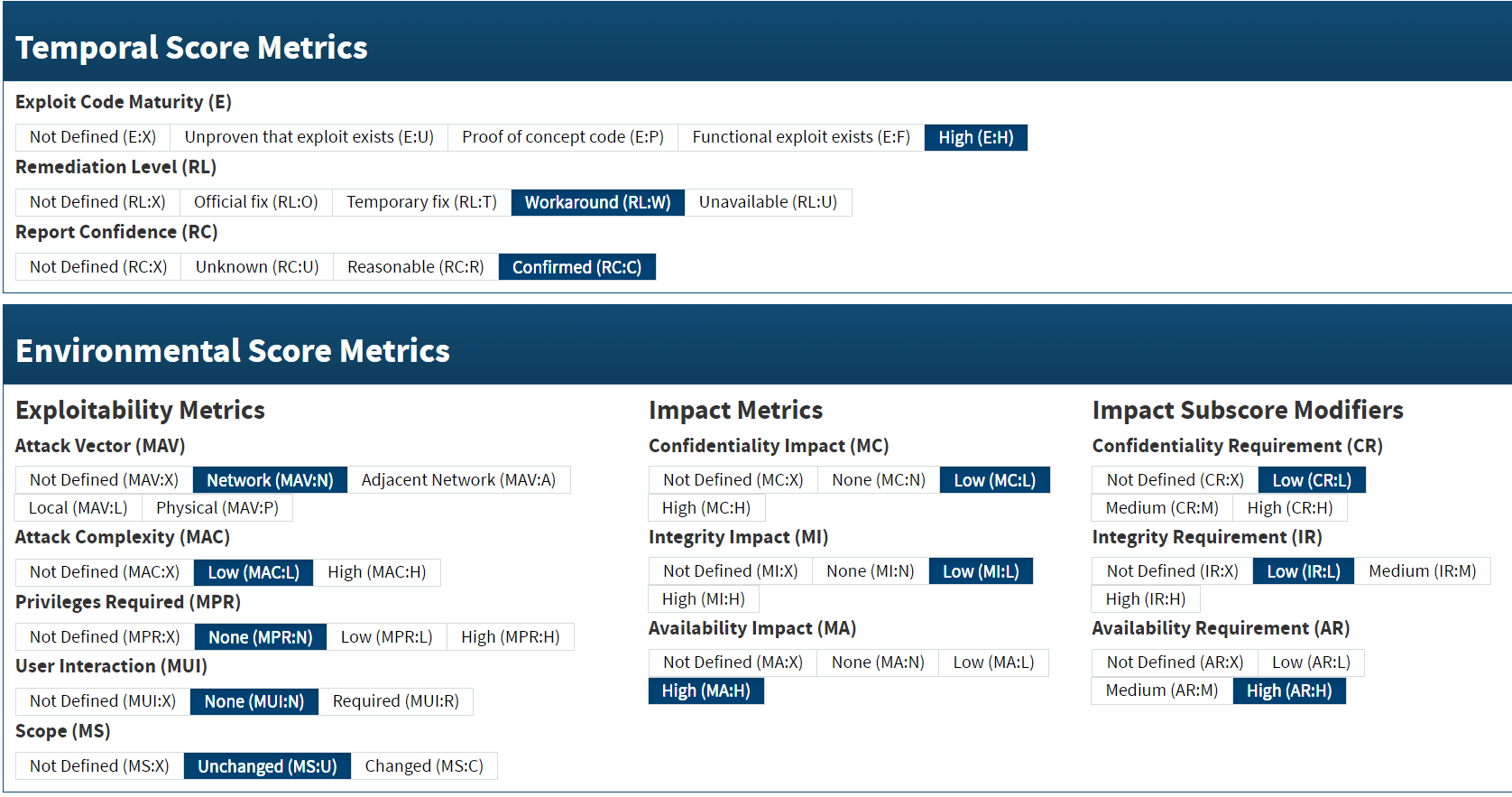
Το Base Metrics παραμένει αυτούσιο καθώς τα μέτρα ασφαλείας που λαμβάνουμε επηρεάζουν μονάχα τις Environmental και Temporal Metrics (Θα παραθέτουμε screenshot με τις τιμές που έχει λάβει στο Base Metrics από τον NIST)**.** Αναλυτικότερα έχουμε:

1. **Windows TCP/IP Remote Code Execution Vulnerability**

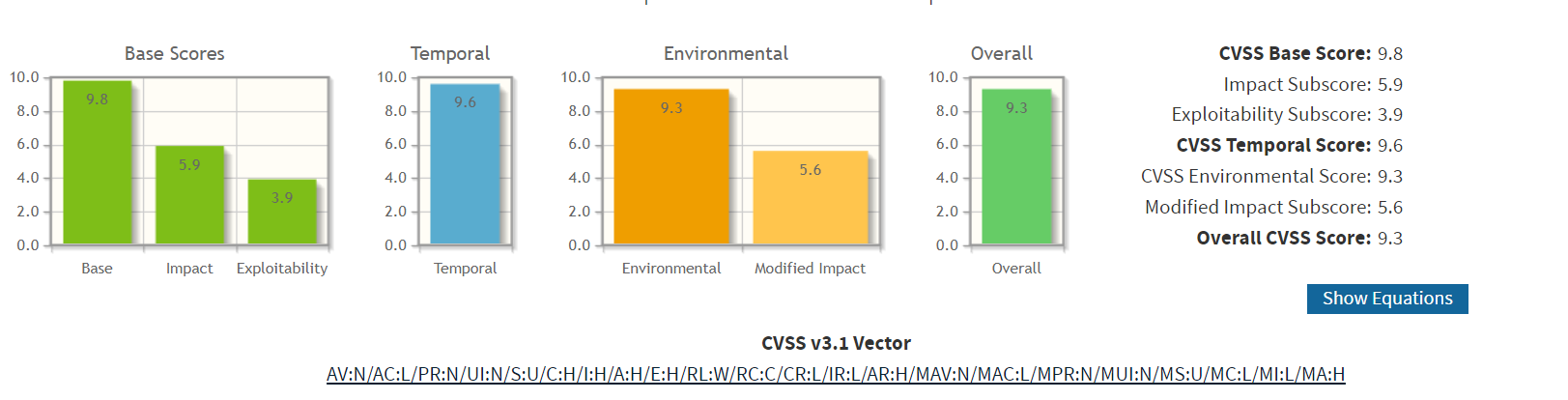
Base Metrics:



Temporal and Environmental Metrics:



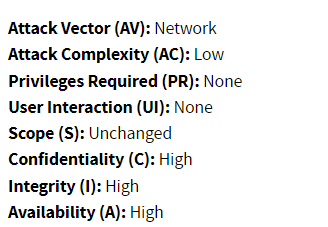
Scores:



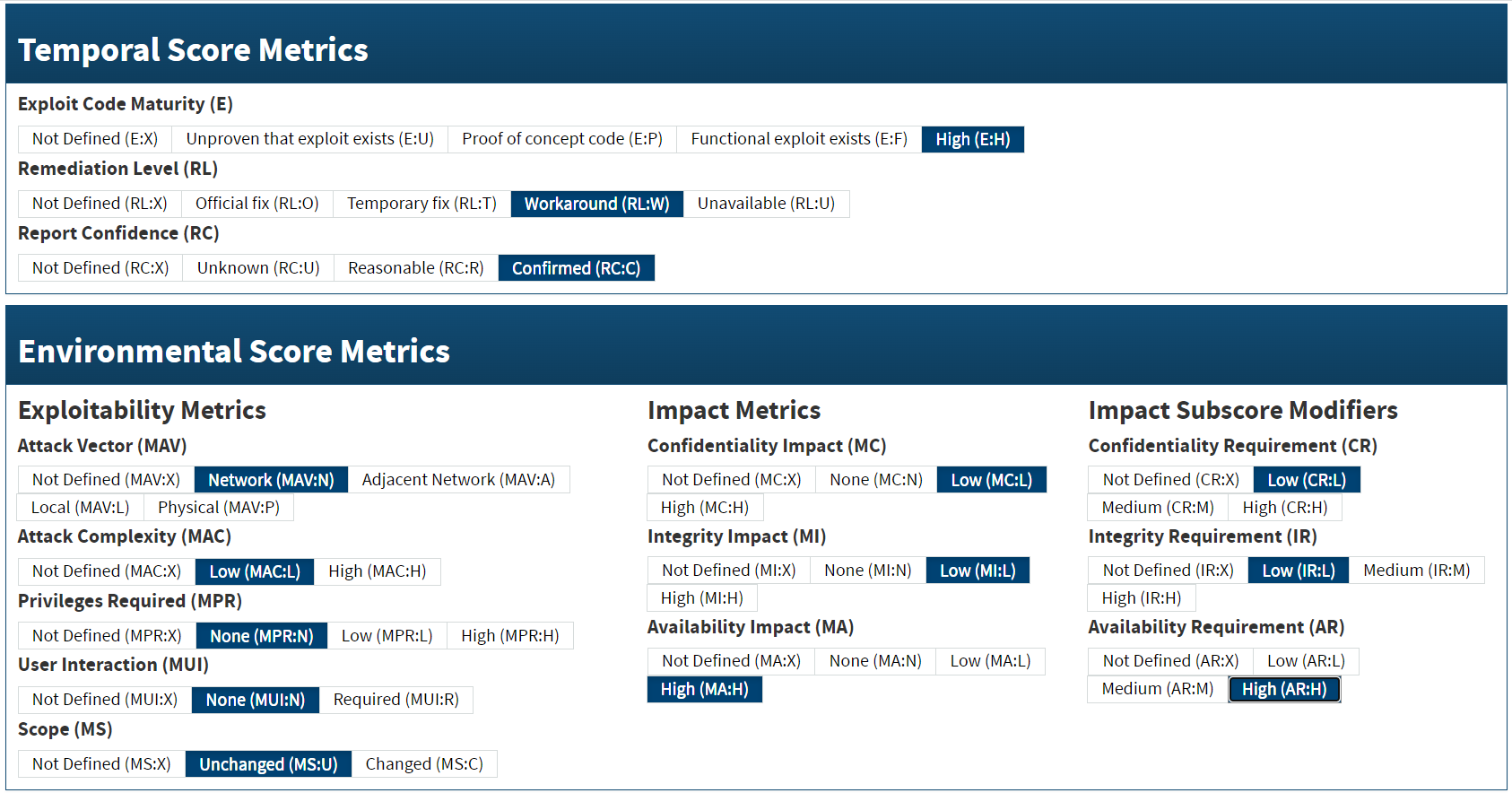
**Σχόλια**: Έχουμε καταφέρει να μειώσουμε το Overall-Score από 9.8 σε 9.3. Αυτό συμβαίνει, καθώς η ίδια η φύση της εφαρμογής μας κάνει να ενδιαφερόμαστε κυρίως για το αντίκτυπο στην διαθεσιμότητά της. Ως αποτέλεσμα τα Impact Metrics της εμπιστευτικότητας και της εμπιστευτικότητας θεωρούνται ως χαμηλής σημασίας (Low). Παρ’ όλα αυτά, δεν παύει να είναι μία σημαντική παραβίαση του ίδιου του λειτουργικού συστήματος εκτελώντας κακόβουλο κώδικα και γι’ αυτό το Overall-Score παραμένει υψηλό.

1. **Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability**

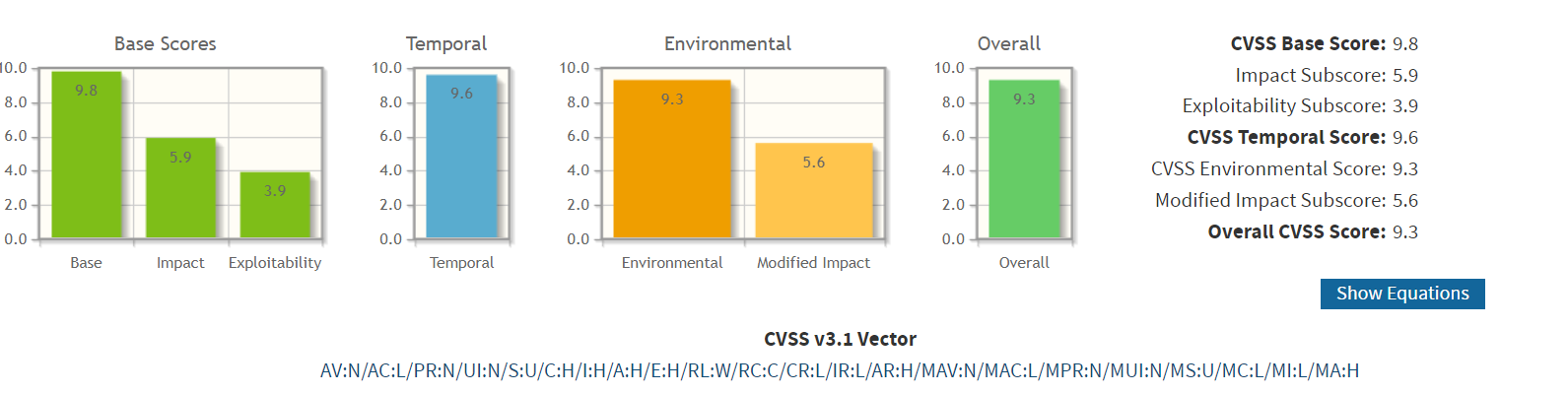
Base Metrics:



Temporal and Environmental Metrics:



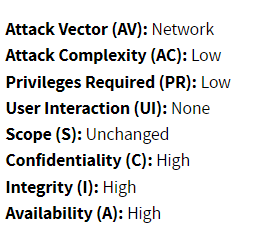
Scores:



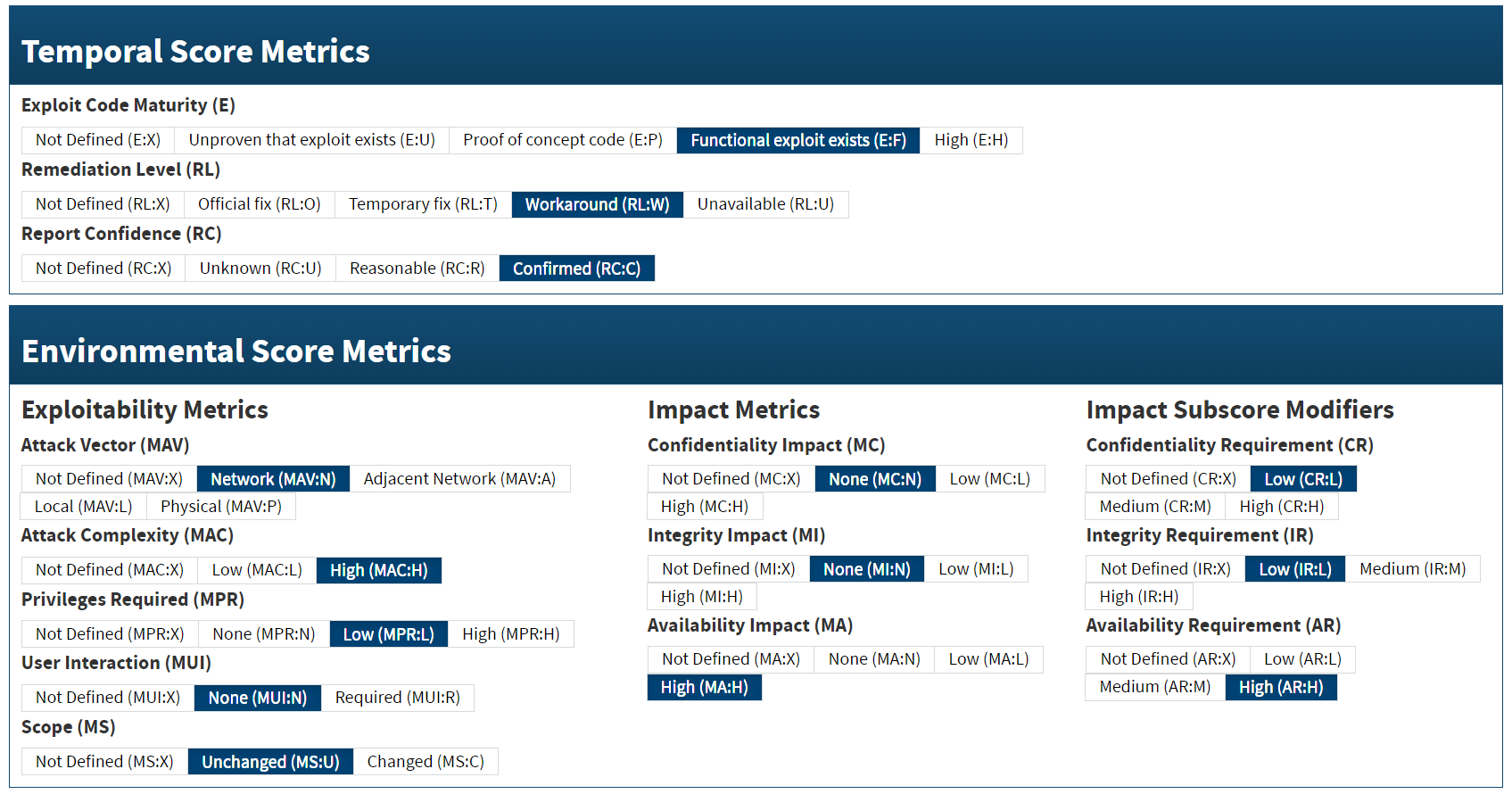
**Σχόλια**: Η συγκεκριμένη επίθεση είναι παρόμοια με την προηγούμενη. Έχουμε καταφέρει να μειώσουμε το Overall-Score από 9.8 σε 9.3. Αυτό συμβαίνει, καθώς η ίδια η φύση της εφαρμογής μας κάνει να ενδιαφερόμαστε κυρίως για το αντίκτυπο στην διαθεσιμότητά της. Ως αποτέλεσμα τα Impact Metrics της εμπιστευτικότητας και της εμπιστευτικότητας θεωρούνται ως χαμηλής σημασίας (Low). Παρ’ όλα αυτά, δεν παύει να είναι μία σημαντική παραβίαση του ίδιου του λειτουργικού συστήματος εκτελώντας κακόβουλο κώδικα και γι’ αυτό το Overall-Score παραμένει υψηλό.

1. **Server Service Remote Protocol Elevation of Privilege Vulnerability**

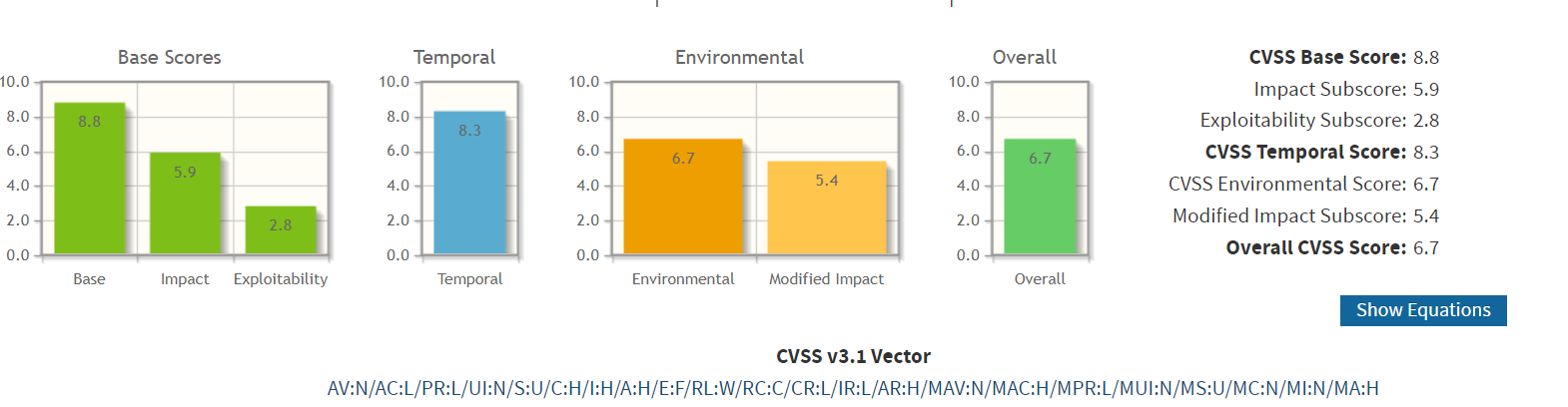
Base Metrics:



Temporal and Environmental Metrics:



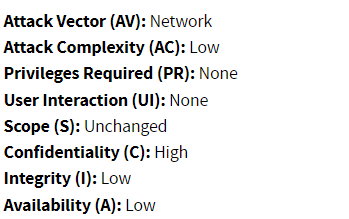
Scores:



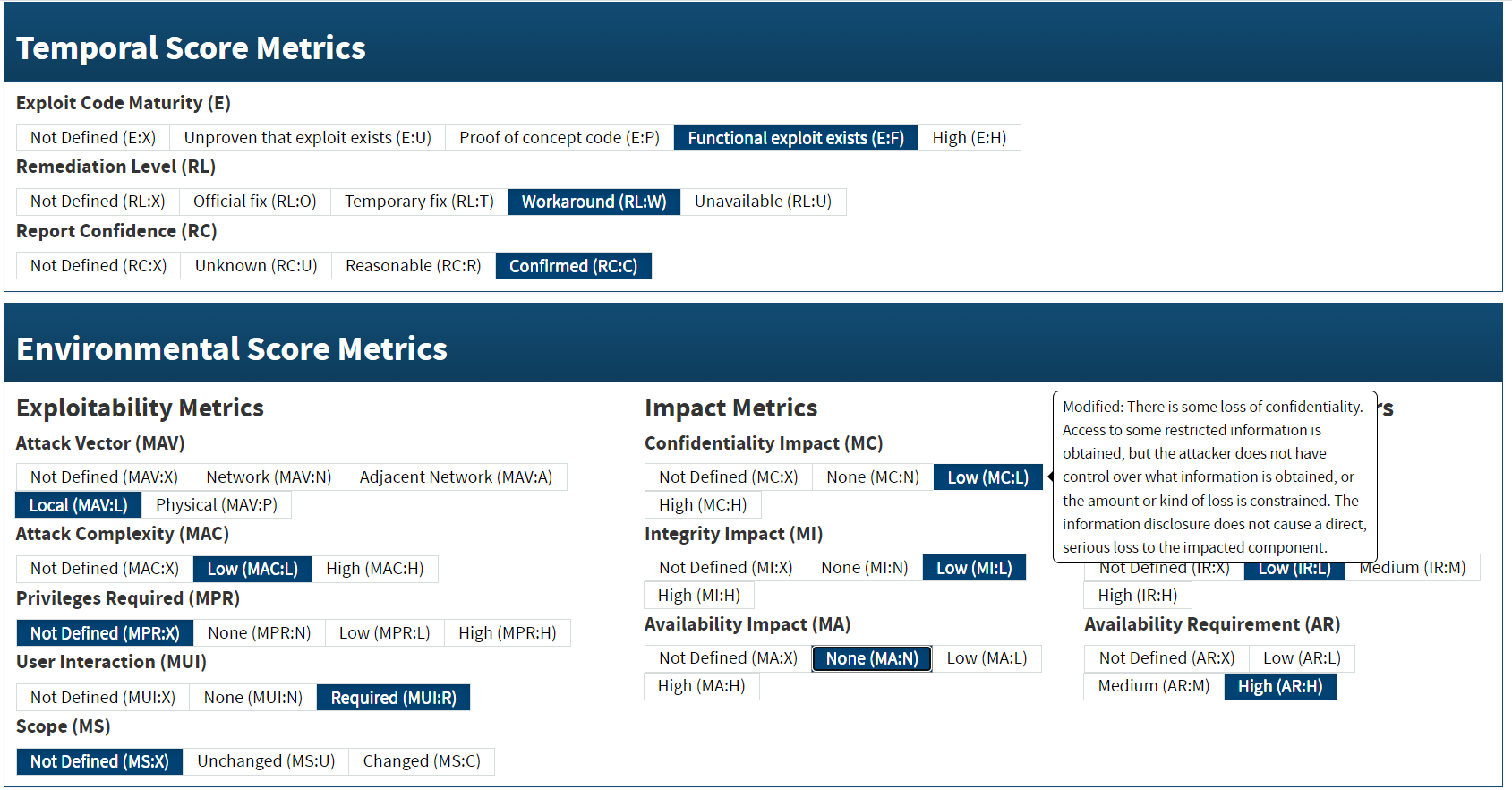
**Σχόλια**: Έχουμε καταφέρει να ρίξουμε το Overall-Score από 9.8 σε 6.7. Αυτό συμβαίνει, καθώς μία τέτοια επίθεση απαιτεί αρκετές γνώσης από τον ίδιο τον επιτιθέμενο, μειώνοντας πολύ τις πιθανότητες κάποιος τόσο ικανός να στοχεύσει μία απλή εφαρμογή σαν την δική μας. Ένας άλλος παράγοντας είναι, ότι η συγκεκριμένη επίθεση δεν μπορεί να αλλάξει ή να τροποποιήσει τα αρχεία μας παρά μόνο να διαγράψει κάποια από αυτά. Συνεπώς δεν έχουμε κάποια επίπτωση στην εμπιστευτικότητα ή την ακεραιότητα των δεδομένων μας, παρά μόνο στην διαθεσιμότητα.

1. **Application Continues Using Socket After It Has Been Closed**

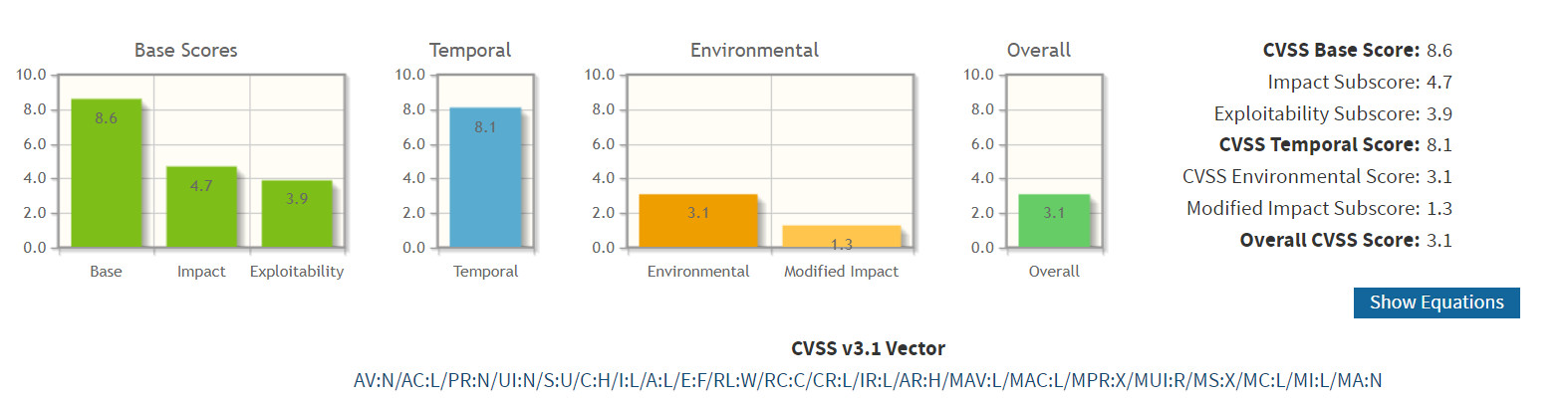
Base Metrics:



Temporal and Environmental Metrics:



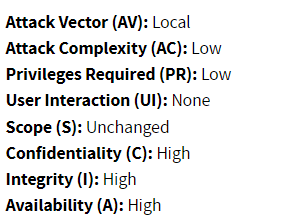
Scores:



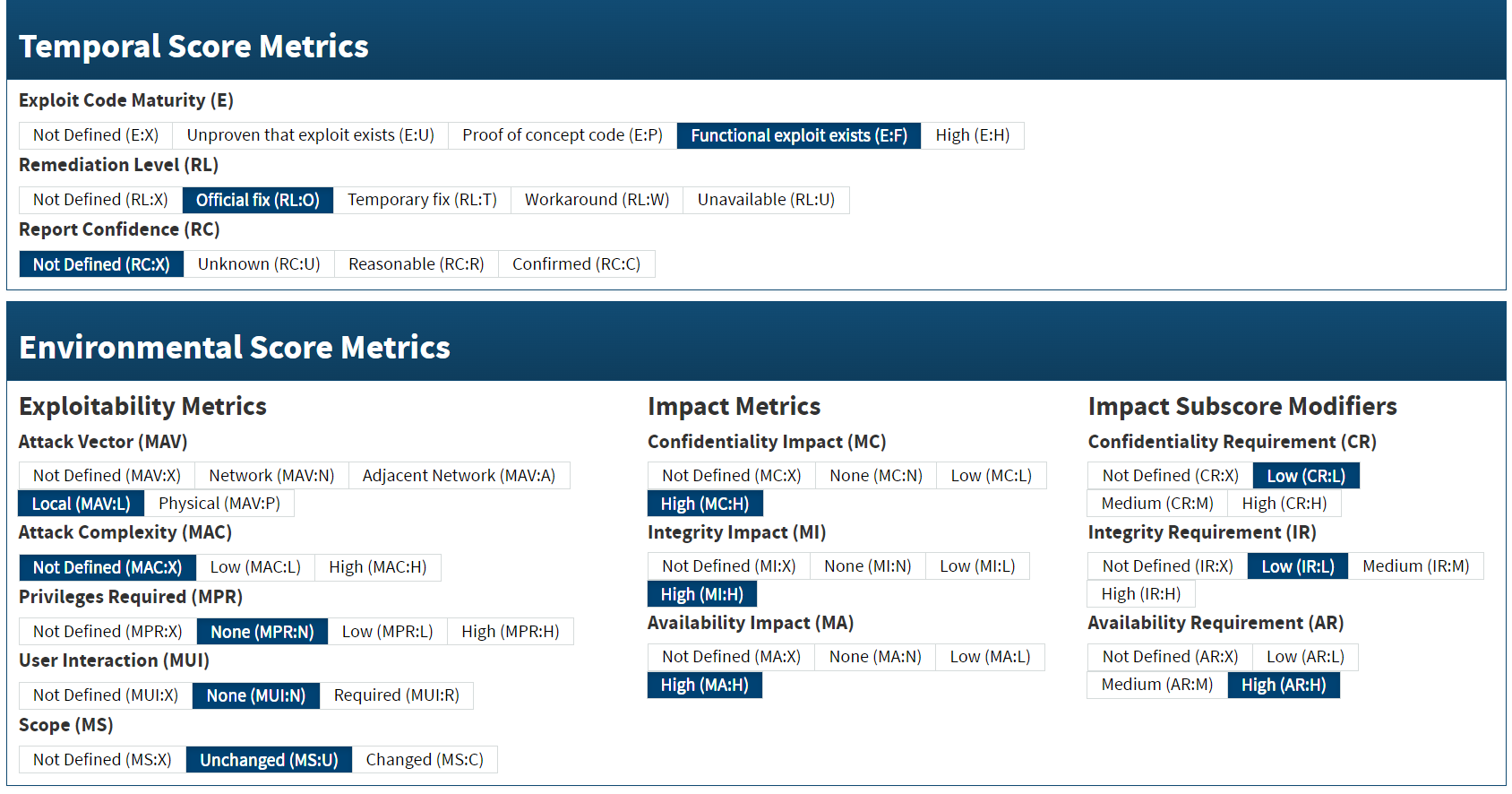
**Σχόλια**: Καταφέραμε να ρίξουμε το Overall-Score από 8.6 σε 3.1. Αυτό συμβαίνει καθώς κάποιο τέτοιο σφάλμα θα απαιτούσε την ενέργεια του ίδιου του χρήστη, όμως οι χρήστες στη δική μας περίπτωση είναι αυθεντικοποιημένοι και συμμορφωμένοι στην χρήση της εφαρμογής από την πολιτική ασφαλείας. Επιπροσθέτως, μία τέτοια επίθεση θα μπορούσε απλά να παραποιήσει λίγο τα δεδομένα (π.χ. να αλλάξει την ημερομηνία κάποιου ραντεβού), χωρίς να υπάρχει κάποια ουσιαστική ζημιά στην εφαρμογή.

1. **An Incorrect Default Permissions Vulnerability In The Packaging Of Tomcat.**

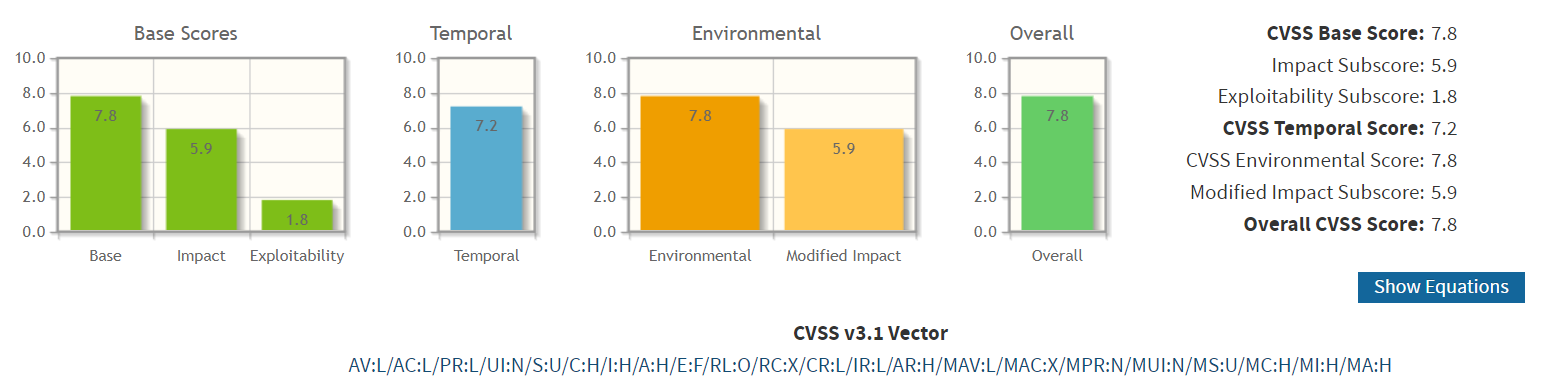
Base Metrics:



Temporal and Environmental Metrics:



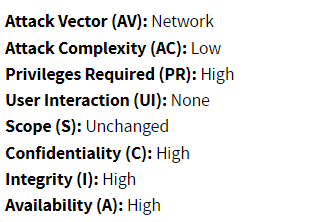
Score:



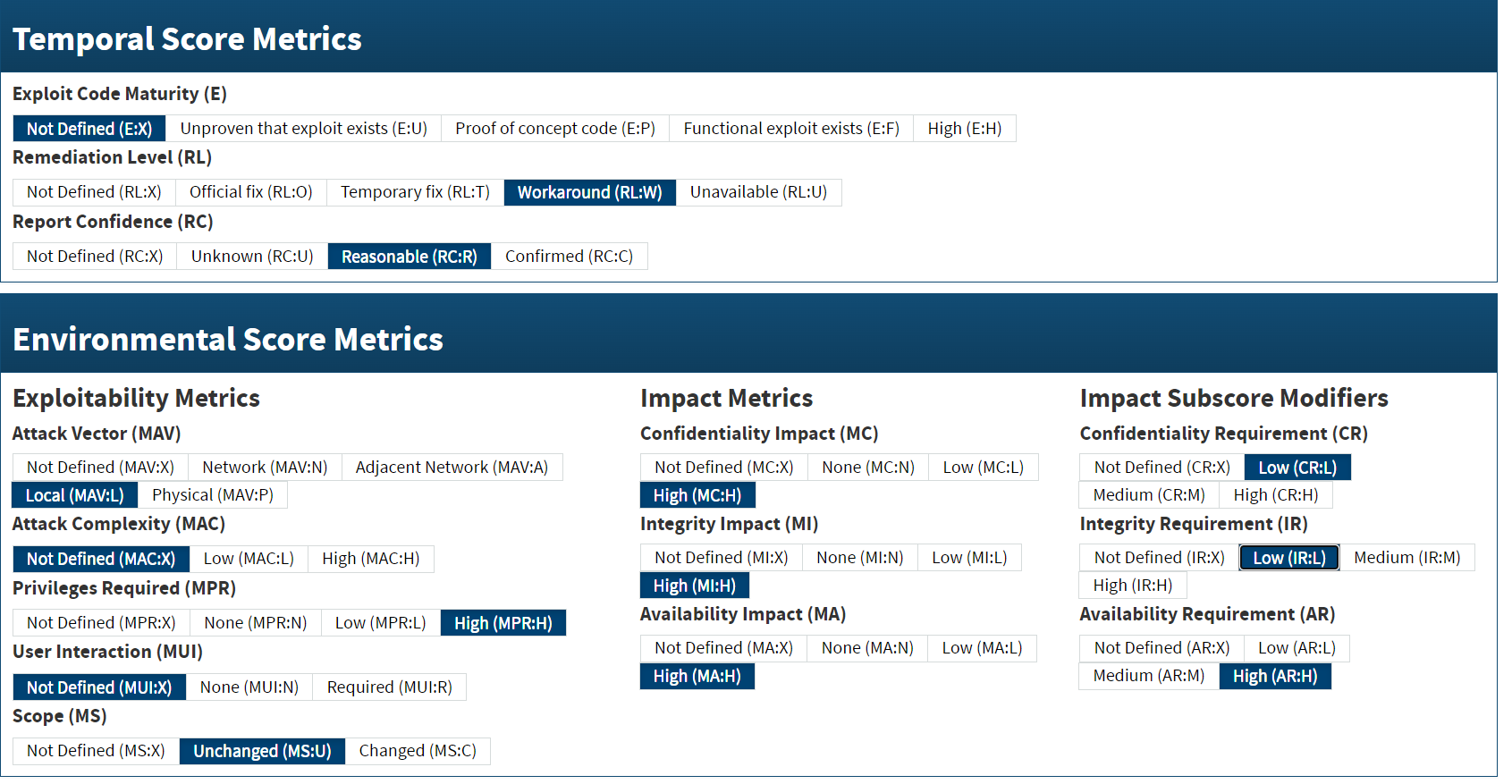
**Σχόλια**: Δεν καταφέραμε να ρίξουμε την σοβαρότητα αυτής της επίθεσης και παραμένει το Overall-Score στο 7.8. Ο λόγος είναι ότι μία τέτοια επίθεση μπορεί να δώσει δικαιώματα διαχειριστή σε κάποιο κακόβουλο. Κάτι τέτοιο θα μπορούσε να έχει καταστροφικές επιπτώσεις για την εφαρμογή, καθώς βλάπτει την εμπιστευτικότητα, ακεραιότητα αλλά και την διαθεσιμότητά της. Ο λόγος που δεν ξεπερνάει την υπάρχουσα βαθμολογία είναι ότι από την πλευρά μας έχουμε λάβει τα αντίστοιχα μέτρα έχοντας υλοποιήσει αυθεντικοποίηση ρόλων στην εφαρμογή, διασφαλίζοντας την ορθή κατανομή των δικαιωμάτων στους χρήστες της.

1. **Vulnerability in the MySQL Server product of Oracle MySQL**

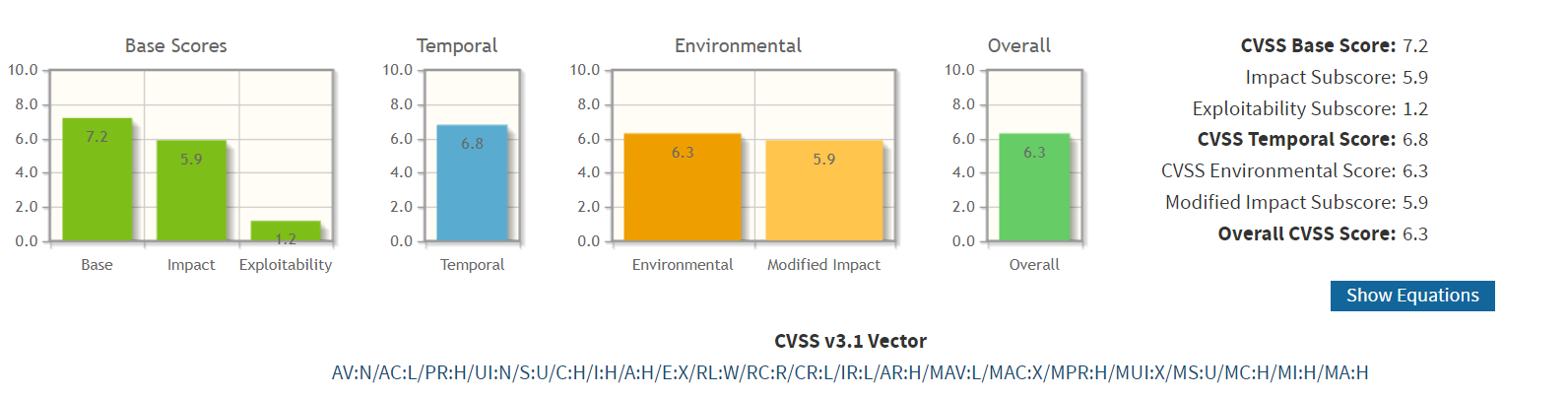
Base Metrics:



Temporal and Environmental Metrics:



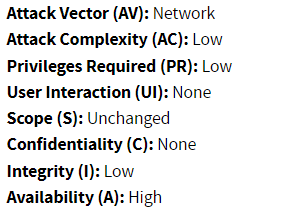
Scores:



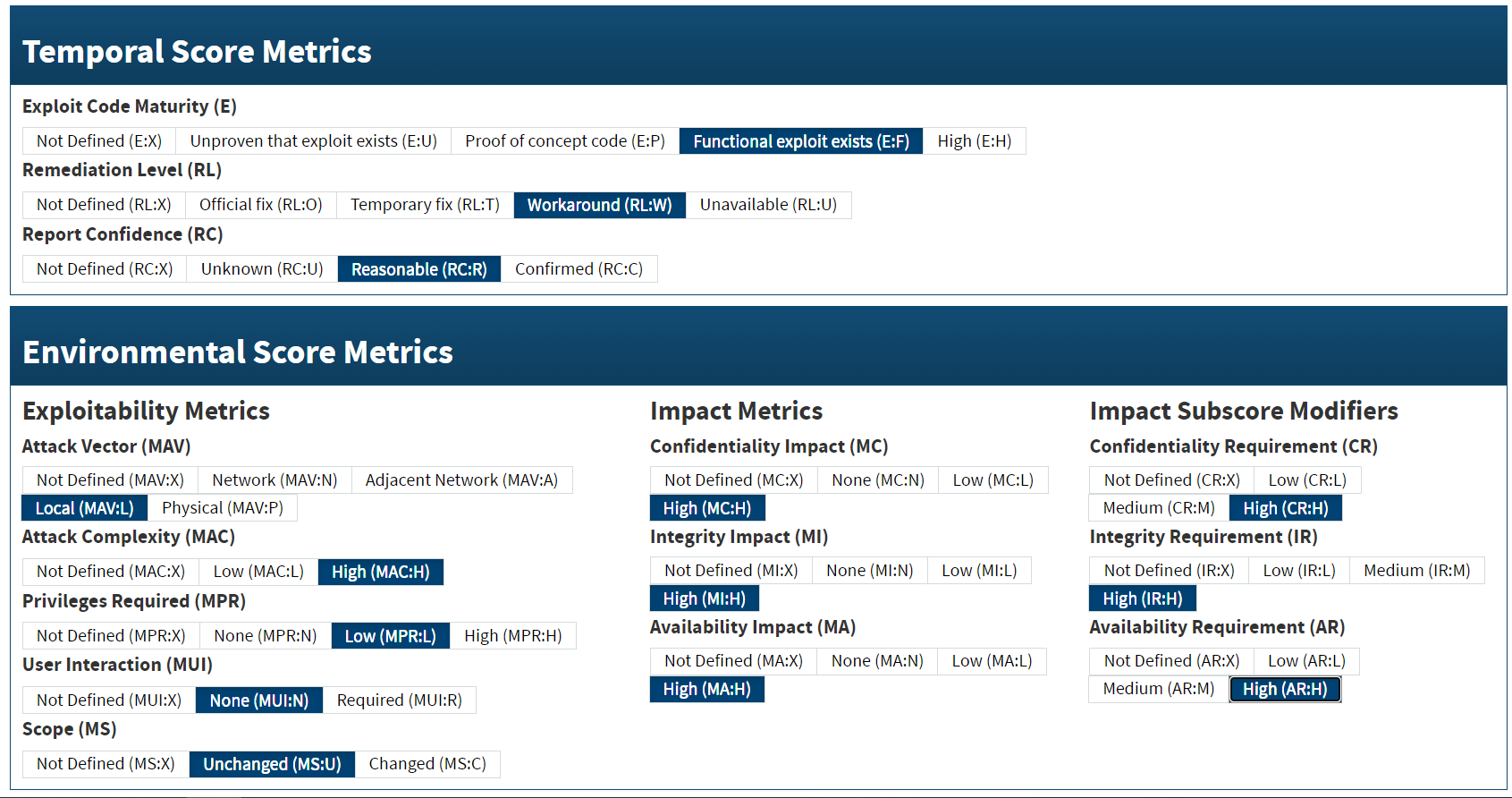
**Σχόλια**: Καταφέραμε να ρίξουμε το Overall-Score από 7.2 σε 6.3. Με τη συγκεκριμένη επίθεση μπορεί κάποιος κακόβουλος να υπονομεύσει όλο τον MySQL Server. Αν και η επίθεση έχει σφοδρά αποτελέσματα στην εφαρμογή μας έχουμε λάβει τα κατάλληλα μέτρα ασφαλείας κρυπτογράφησης των δεδομένων μας. Ως αποτέλεσμα κάποιος κακόβουλος δεν θα μπορέσει να τα εκμεταλλευτεί παρά μόνο να καταστήσει τον Server μας μη διαθέσιμο.

1. **Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer)**

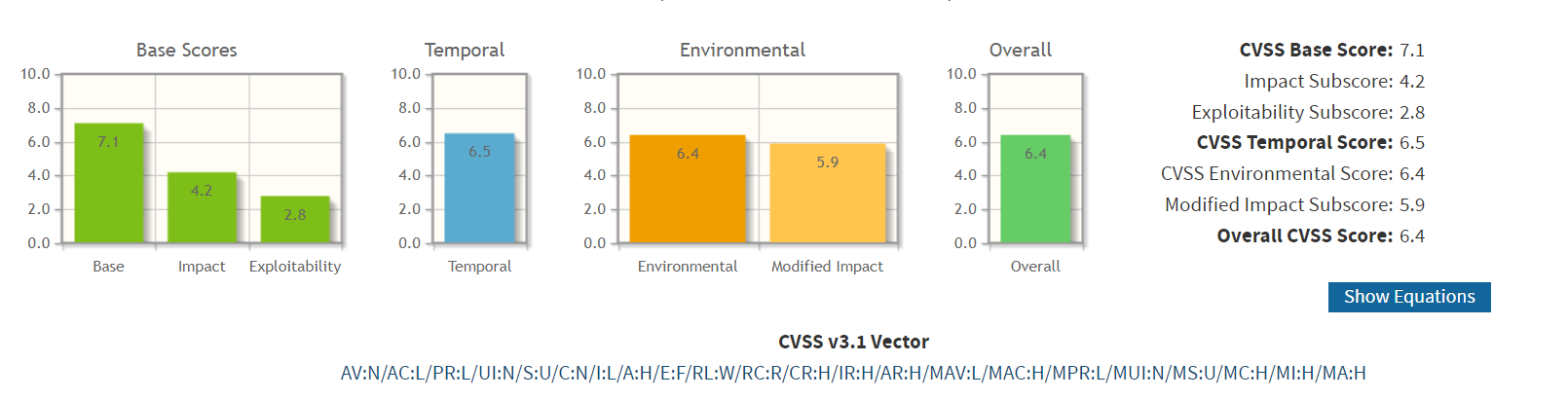
Base Metrics:



Temporal and Environmental Metrics:



Scores:



**Σχόλια**: Καταφέραμε να ρίξουμε το Overall-Score από 7.2 σε 6.4. Η συγκεκριμένη επίθεση όπως και η προηγούμενη έχει μεγάλες επιπτώσεις στην λειτουργία της εφαρμογής. Η διαφορά είναι ότι αυτή μπορεί να εκτελεστεί και από κάποιον που δεν έχει απαραίτητα τόσο ανεβασμένα δικαιώματα και ότι μπορεί να επηρεάσει και δεδομένα. Σε κάθε περίπτωση ακόμα και τα αφύλακτα δεδομένα που υπάρχουν την δεδομένη χρονική στιγμή στον MySQL Server δεν είναι ιδιαίτερης αξίας και θα μπορέσουν να αναπαραχθούν ξανά από τους χρήστες και τους υπεύθυνους ασφαλείας.