IS SECURITY TERMINOLOGY: A CRASH COURSE.

Mavrofidis Manolis,
B.Sc., M.Sc. Information Systems Security

Administrative Items

- No cellphones/pagers/smartphones.
- No desktops/laptops/netbooks.
- No smoking.
- Breaks.
- Refreshments.
- Emergency exits.
- Fire extinguishers.
- Presentation will be published.

Roadmap

- Σκοπός είναι να υπάρξει μια **κοινή γλώσσα** επικοινωνίας.
- Αναφορά στους σημαντικότερους όρους (crash course).
- Η αγγλική μετάφραση είναι **Security**.
- Showcase of vulnerabilities (No full pwnage this year).

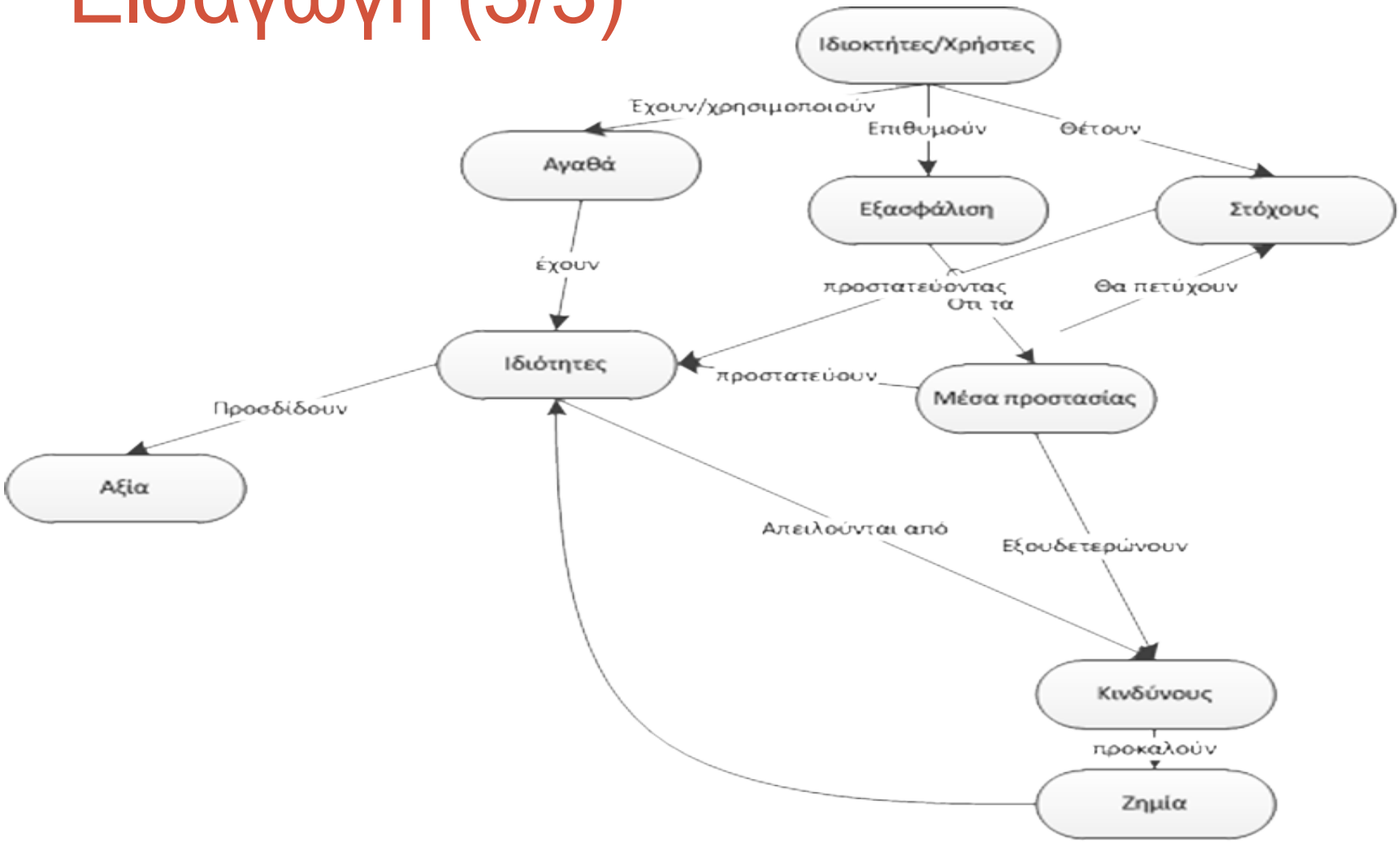
Εισαγωγή (1/3)

- **Αγαθά** (Assets). Πληροφορίες, πόροι κλπ που αξίζει να προστατευθούν γιατί έχουν μια εκτιμώμενη αξία.
- **Αξία** (Value). Η σημαντικότητα ενός αντικειμένου εκφρασμένη με οικονομικό ή άλλο τρόπο.
- **Ιδιότητα** (Attribute). Χαρακτηριστικό το οποίο προσδίδει αξία σε ένα αγαθό και άρα **πρέπει** να προστατευτεί.
- **Ιδιοκτήτης/χρήστης** (Owner/user). Ο κάτοχος ή ο χρήστης ενός (ή μέρους αυτού του) αγαθού.
- **Ζημιά** (harm). Ο περιορισμός της αξίας ενός αγαθού.

Εισαγωγή (2/3)

- **Κίνδυνος** (danger). Η πιθανότητα να προκληθεί ζημιά σε ένα αγαθό.
- **Μέσο προστασίας** (Safeguard). Το σύνολο των ενεργειών στις οποίες μπορεί να προβεί ένας χρήστης για να **μειώσει** τον κίνδυνο.
- **Κόστος** (cost). Οποιαδήποτε επιβάρυνση προκύπτει από την εφαρμογή ενός μέσου προστασίας.
- **Στόχος της ασφάλειας** (Infosec goal). Η επιθυμητή ισορροπία για τον ιδιοκτήτη/χρήστη μεταξύ κόστους και ζημίας σε ένα αγαθό εξαιτίας κάποιου κινδύνου.
- **Εξασφάλιση** (Assurance). Βεβαιότητα ότι οι στόχοι της ασφάλειας επιτεύχθηκαν εξαιτίας των μέσων προστασίας που εφαρμόστηκαν.

Εισαγωγή (3/3)


Ιδιοκτήτες/Χρήστες
Έχουν/χρησιμοποιούν
Επιθυμούν
Θέτουν
Αγαθά
Εξασφάλιση
Στόχους
έχουν
προστατεύοντας
Ότι τα
Θα πετύχουν
Ιδιότητες
προστατεύουν
Μέσα προστασίας
Προσδίδουν
Αξία
Απειλούνται από
Εξουδετερώνουν
Κινδύνους
προκαλούν
Ζημία

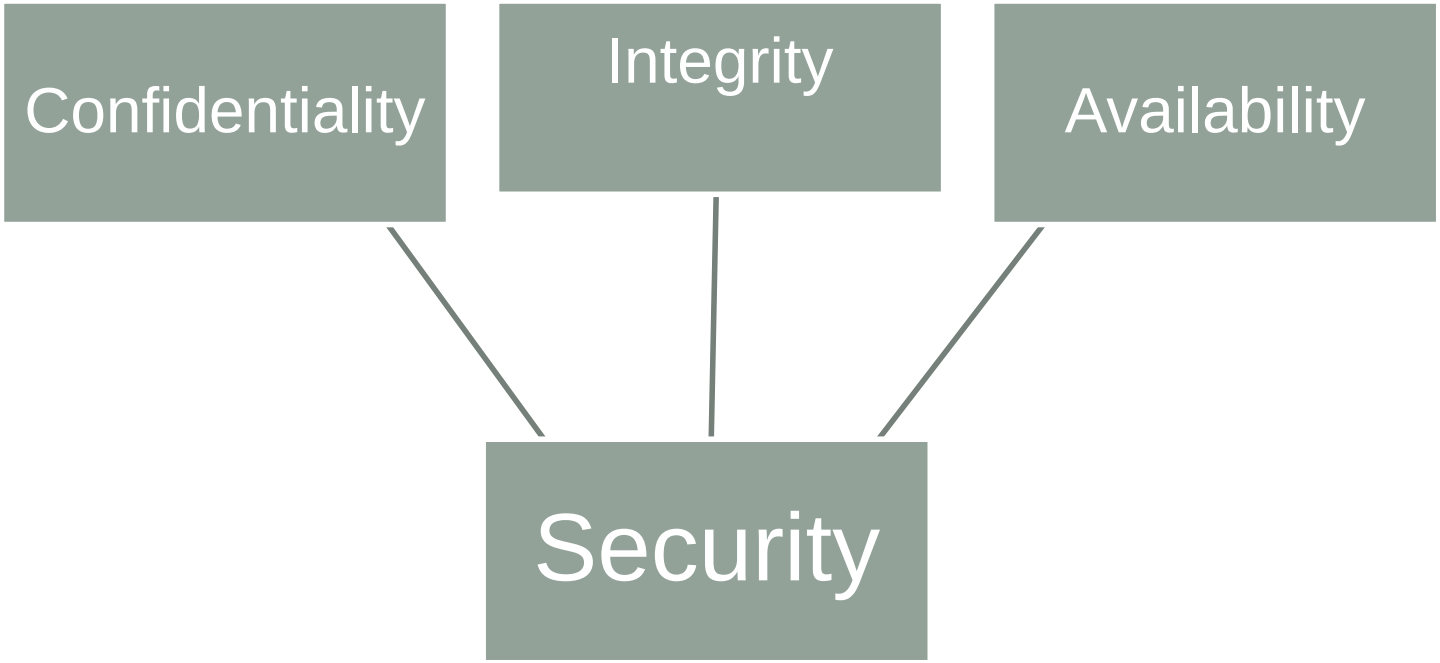
Επιπρόσθετα

- **Δεδομένα** (Data). Καταγεγραμμένα σύμβολα (12).
- **Πληροφορία** (Information). Δεδομένα εντός του πλαισίου στο οποίο ορίζονται. 12 μαθητές του Ιησού.
- **Εξουσιοδότηση** (Authorization). Διαδικασία παροχής δικαιώματος σε κάποιον χρήστη/διαδικασία ενός συστήματος.

Ασφάλεια

- **Εμπιστευτικότητα** (Confidentiality). Οι πόροι/πληροφορίες του συστήματος είναι διαθέσιμοι σε εξουσιοδοτημένους χρήστες/διαδικασίες.
- **Ακεραιότητα** (Integrity). Οι πόροι/πληροφορίες του συστήματος είναι τροποποιήσιμοι μόνο από όσους είναι εξουσιοδοτημένοι ως προς αυτό.
- **Διαθεσιμότητα** (Availability). Οι πόροι/πληροφορίες του συστήματος είναι προσπελάσιμοι σε **εύλογο** χρονικό διάστημα.

Ασφάλεια



Ρήγμα ασφάλειας (Breach of security). Οτιδήποτε παραβιάζει το C.I.A. Επίσης οτιδήποτε αντίκειται στην πολιτική ασφάλειας.

Ασφάλεια

Απειλές

Χρησιμοποιούν

Ευπάθειες

Προκαλούν

Ζημιά στα αγαθά

Ασφάλεια.

- **Πολιτική ασφάλειας** (Security Policy). Σύνολο κανόνων, διαδικασιών, διεργασιών και μέτρων που ορίζονται από έναν ειδικό ασφάλειας ΠΣ για έναν οργανισμό.
  - Η πολιτική ασφάλειας είναι το Σύνταγμα.
  - Τα μέτρα/διεργασίες είναι οι νόμοι.
- Η εκπόνηση πολιτικής ασφάλειας περιλαμβάνει χρήση μεθοδολογιών (**CRAMM, OCTAVE, ORANGE BOOK κλπ**). Επηρεάζεται από την κείμενη νομοθεσία (ν. 2472/97 κλπ) και ευρωπαϊκές οδηγίες.

Ασφάλεια;

- Η ασφάλεια είναι **διαχείριση ρίσκου**.
- Ο αξιωματικός ασφάλειας ενός οργανισμού καλείται να **μειώσει την επικινδυνότητα**.
- Δεν είναι **ούτε εφικτό** αλλά και **ούτε θεμιτό** να μηδενιστεί εντελώς η επικινδυνότητα.
- There’s no such thing as absolute security. Get over it.

Ποιο είναι το πρόβλημα;

- Δεν είναι το λογισμικό.
- Δεν είναι η γνώση γύρω από την ασφάλεια Πληροφοριακών Συστημάτων.
- Είναι οι **διαδικασίες** που ακολουθούνται.
  - Δε θα υπήρχε Heartbleed αν ακολουθούνταν οι σωστές διαδικασίες.

CRYPTOGRAPHY

Core cryptographic concepts

Κρυπτογραφία

- The art of secret writing.

Κρυπτογραφία

- Μαθηματικές συναρτήσεις.
- Δύο προσεγγίσεις.
  - Συμμετρική κρυπτογραφία.
  - Κρυπτογραφία δημοσίου κλειδιού.
- Χρησιμοποιούνται και οι δύο στο web.
- Επιπρόσθετα χρησιμοποιούνται κρυπτογραφικές συναρτήσεις κατακερματισμού (hash functions).
- Ψηφιακές υπογραφές (DigiCerts).

$~:WEB /DISASM

Disassemble the current status of the web and its core technologies.

HTTP

- Hyper Text Transfer Protocol.
- Σχεδιάστηκε από τον Tim Burners Lee το 1989 στο CERN.
- Χρησιμοποιεί requests [GET, POST, PUT, HEAD,…]
- Είναι plain-text πρωτόκολλο.
- Χρησιμοποιεί κωδικούς (1XX, 2XX, 3XX, 4XX, 5XX)
- Κάνει και καφέ.

http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html

GET Request example

- Παρέχει δεδομένα τα οποία ζητήθηκαν μέσω URL (QueryString).

GET /search.php?name=blah&type=1 HTTP/1.1

User-Agent: Mozilla/4.0

Host: www.host.com

<CRLF>

<CRLF>

Data….

Μνήμη στο Web

- Το HTTP δε θυμάται.
- Για να αρχίσει να θυμάται χρειάζεται κάποιο τρόπο.
  - SESSION ID ($_SESSION[] array της PHP).
- Το Session διακινείται μέσω:
  - URL.
  - Κρυφά πεδία φόρμας.
  - Cookies.

Διασύνδεση τεχνολογιών

- Tiers.
- Ο χρήστης κάνει μια αίτηση σε έναν server. Ο Server παίρνει την αίτηση, την προωθεί στην PHP, η PHP αντλεί δεδομένα από τη Βάση Δεδομένων.

Η παραπάνω tier αρχιτεκτονική είναι η πιο απλή.

Τα προβλήματα

- Το Web στηρίζεται στο Internet (OSI Layers).
- Κάθε νέα τεχνολογία που στηρίζεται στο Web εισάγει καινούρια επικινδυνότητα (βλ. HTML 5).
- Η επικινδυνότητα λειτουργεί αθροιστικά.
- Ο Server είναι εκεί συνέχεια, ο αξιωματικός ασφάλειας όχι.

OWASP Top Ten

Injection	Broken Authentication/ Session Management	Cross-Site Scripting (XSS)	Insecure Direct object references
Security misconfigurations	Sensitive Data Exposure	Failure to restrict URL Access	Cross Site Request Forgery (CSRF)
	Components with known vulnerabilities	Unvalidated Redirects and Forwards	

https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013

OWASP Top Ten

Injection	Broken Authentication/ Session Management	Cross-Site Scripting (XSS)	Insecure Direct object references
Security misconfigurations	Sensitive Data Exposure	Failure to restrict URL Access	Cross Site Request Forgery (CSRF)
	Components with known vulnerabilities	Unvalidated Redirects and Forwards	

https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013

Injections. (1/2)

- $query=“SELECT * FROM USERS where u_name=‘”.$_GET[“name”].”’ AND u_pass=‘”.$_GET[‘pass’].”’”

- User inputs “ ’ OR 1=1-- ”
- Query becomes

SELECT * FROM USERS where u_name=‘’ OR 1=1–

- False OR True=True.
- Attacker logs in.

Injections. (2/2)

- Εύκολη η προστασία
- Οι ΒΔ ξέρουν από μόνες τους να το διαχειριστούν.
- Prepared statements (PDO, mysqli etc)
- **Όχι** custom filters, whitelists, blacklists.
- Αν δε προστατευτείτε, τα πράγματα θα γίνουν άσχημα, γρήγορα.
- Είναι Server-side attack τυπικά αλλά στην HTML5 είναι και client-side attack.

OWASP Top Ten

Injection	Broken Authentication/ Session Management	Cross-Site Scripting (XSS)	Insecure Direct object references
Security misconfigurations	Sensitive Data Exposure	Failure to restrict URL Access	Cross Site Request Forgery (CSRF)
	Components with known vulnerabilities	Unvalidated Redirects and Forwards	

https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013

Session management

- Ο επιτιθέμενος γνωρίζει τα sessions και άρα μπορεί να συνδεθεί ως άλλος χρήστης.
- Δε γράφουμε δικό μας κώδικα να κάνει session management αλλά προτιμάμε της γλώσσας.
- Εκτός αν μας λένε Schneier.
- Που δε μας λένε.
- Που ούτε αυτός δε θα το έκανε.

OWASP Top Ten

Injection	Broken Authentication/ Session Management	Cross-Site Scripting (XSS)	Insecure Direct object references
Security misconfigurations	Sensitive Data Exposure	Failure to restrict URL Access	Cross Site Request Forgery (CSRF)
	Components with known vulnerabilities	Unvalidated Redirects and Forwards	

https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013

Cross site scripting

- echo($_GET[“something”]);
- something=“<h1>Hack</h1>”
- Ο επιτιθέμενος μπορεί να εκτελέσει επιθέσεις στο χρήστη.
- Προστασίες.
  - Εύκολη προστασία αλλά μεγάλο σύνολο κανόνων.
  - Γενικά δεν εισάγετε δεδομένα που σας στέλνει ο χρήστης οπουδήποτε αν δε τα φιλτράρετε.
  - Session cookies HttpOnly
  - void session_set_cookie_params (int $lifetime [, string $path [, stri ng $domain [, bool $secure = false [, bool$httponly = false]]]])
  - Filtering rules https://www.owasp.org/index.php/XSS_%28Cross_Site_Scripting%29_Prevention_Cheat_Sheet

OWASP Top Ten

Injection	Broken Authentication/ Session Management	Cross-Site Scripting (XSS)	Insecure Direct object references
Security misconfigurations	Sensitive Data Exposure	Failure to restrict URL Access	Cross Site Request Forgery (CSRF)
	Components with known vulnerabilities	Unvalidated Redirects and Forwards	

https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013

Security misconfigurations

- Μη χρησιμοποιείτε παλαιό software.
- Αποφύγετε legacy συστήματα.
- Συμβουλευτείτε documentation γλώσσας

OWASP Top Ten

Injection	Broken Authentication/ Session Management	Cross-Site Scripting (XSS)	Insecure Direct object references
Security misconfigurations	Sensitive Data Exposure	Failure to restrict URL Access	Cross Site Request Forgery (CSRF)
	Components with known vulnerabilities	Unvalidated Redirects and Forwards	

https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013

Sensitive data exposure (1/2)

- Data is in rest or in transit
- In transit, protection comes with SSL/TLS (HTTPS).
- In rest protection comes with encryption and hashing.
- PHP related.
  - Scrypt (αν έχετε πρόσβαση στο server).
  - Bcrypt (έρχεται by default).
  - hash_algos(). Γυρνάει array με όσα hashing algorithms υποστηρίζει η PHP.
  - Αποφύγετε MD5, SHA-128. Έχουν πρόβλημα.
  - Υποχρεώστε τη σύγκριση να γίνει σε string (===). Με (==) η σύγκριση ίσως γίνει με float, οπότε εισάγετε νέα bugs που δε θέλετε.

Sensitive data exposure (2/2)

- Μην υλοποιήσετε δικούς σας αλγόριθμους hashing ή crypto. Δεν έχετε τις γνώσεις.
- Για το hashing χρησιμοποιήστε salts. Για παράδειγμα, αν θέλετε να δημιουργήσετε το hash ενός χρήστη, hash(algo, u_pass.salt). Πιο ασφαλές και θα σας σώσει από μια γκάμα επιθέσεων, οι οποίες θα γίνουν ανέφικτες.
- Δεν αποθηκεύουμε ευαίσθητα δεδομένα στην πλευρά του χρήστη.

OWASP Top Ten

Injection	Broken Authentication/ Session Management	Cross-Site Scripting (XSS)	Insecure Direct object references
Security misconfigurations	Sensitive Data Exposure	Failure to restrict URL Access	Cross Site Request Forgery (CSRF)
	Components with known vulnerabilities	Unvalidated Redirects and Forwards	

https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013

Failure to restrict access

- Πρέπει να ελέγχετε σε κάθε αρχείο αν αυτός που πάει να το προσπελάσει έχει τα συγκεκριμένα δικαιώματα.
- Παράδειγμα: admin_functions.php. Μπορεί να το προσπελάσει μόνο ο διαχειριστής.
- Παράδειγμα: update_status.php. Μπορεί να το προσπελάσει ένας χρήστης.
- Αν το admin_functions.php δεν ελέγχει αν αυτός που το καλεί είναι διαχειριστής, τα πράγματα θα γίνουν άσχημα, γρήγορα.
- Εύκολος τρόπος ελέγχου είναι το session.
- Access Controls

OWASP Top Ten

Injection	Broken Authentication/ Session Management	Cross-Site Scripting (XSS)	Insecure Direct object references
Security misconfigurations	Sensitive Data Exposure	Failure to restrict URL Access	Cross Site Request Forgery (CSRF)
	Components with known vulnerabilities	Unvalidated Redirects and Forwards	

https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013

CSRF

- Ο εξουσιοδοτημένος χρήστης εκτελεί λειτουργίες εν αγνοία του.
- Αντιμετωπίζεται εύκολα.
- Ο χρήστης ζητάει μια φόρμα
  - *$csrfToken= md5(uniqid(rand(), true));*
  - *$_SESSION[“csrfToken”]=$csrfToken*
  - *<form>*
    <input type=“hidden” name=“csrf” value=“<?php echo($csrfToken);?>”/>
- *Ο χρήστης στέλνει πίσω τη φόρμα*
  - *if($_SESSION[“csrfToken”]==$csrf){*

//do something

}else{

request is forged. Drop it

}

OWASP Top Ten

Injection	Broken Authentication/ Session Management	Cross-Site Scripting (XSS)	Insecure Direct object references
Security misconfigurations	Sensitive Data Exposure	Failure to restrict URL Access	Cross Site Request Forgery (CSRF)
	Components with known vulnerabilities	Unvalidated Redirects and Forwards	

https://www.owasp.org/index.php/Top10#OWASP_Top_10_for_2013

Redirects and Forwards (1/2)

- HTTP 302 Redirect.
- Validate input. Again.
- HTTP/HTTPS regex is not enough.
- $_GET['url']; header("Location: " . $redirect_url);// Λάθος
- <?php header("Location: http://www.mysite.com/"); ?>//OK
- Το ίδιο ισχύει και στα forwards, όμως, εκεί πρέπει να ελεγχθεί αν ο χρήστης ζήτησε αυτή τη σελίδα (CSRF πχ) και αν ο χρήστης δικαιούται να δει αυτή τη σελίδα (Access controls and restrictions).

Redirects and Forwards (2/2)

- Αποφύγετε τα file.php?include=anotherFile.php
- Γενικότερα καλό είναι να μη φορτώνετε αρχεία μέσω παραμέτρων τις οποίες ελέγχει ο χρήστης.
- Αποφεύγετε τα file inclusions με κάθε κόστος.
- Προτιμήστε το require_once().

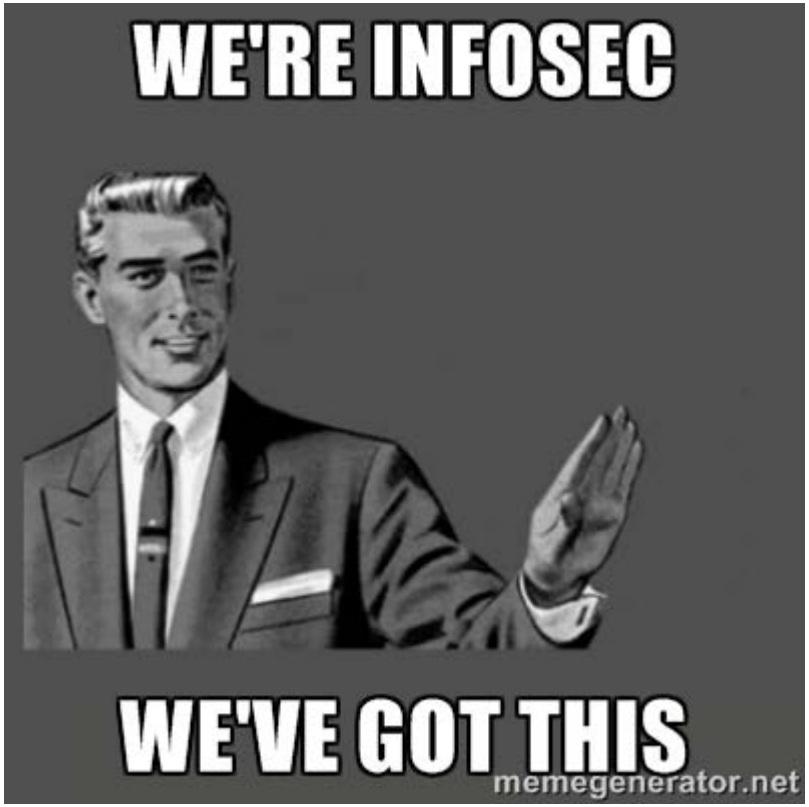
Και άλλα ζητήματα

- Τα stacks δουλεύουν άψογα.Τεχνικά είμαστε ΟΚ επίσης. Να σχολάσω;
  -Όχι.
- Είναι ευθύνη σας και άλλα πράγματα τα οποία εμπίπτουν στην ασφάλεια πληροφοριών.
- Για παράδειγμα, τι πληροφορίες αποθηκεύει η ΒΔ. Απαγορεύεται σύμφωνα με τον 2472/1997 η αποθήκευση ευαίσθητων προσωπικών δεδομένων (θρήσκευμα, κατάσταση υγείας κλπ).
- Γενικότερα, τα νομικά ζητήματα είναι περίεργα και θολά, χρειάζεται προσοχή.

Common misconceptions

- Whoami:$root@yourbox.com
- Μη διακρίνετε GET/POST/οποιοδήποτε request.
- Όλα τα requests είναι το ίδιο εύκολο να τα εκμεταλλευτεί ένας επιτιθέμενος.
- «Δε θα συμβεί αυτό σε μένα». Θα συμβεί.
- Μη χρησιμοποιείτε έτοιμα CMS αν δε τα κάνετε update. Εκτός αν σας αρέσει να μοιράζετε malware. Που δεν αρέσει σε μας.
- Αφιερώστε χρόνο σε documentation/best practices.
- Μην αυτοσχεδιάζετε.
- Προσοχή σε bugs λογικής.

Handling infosec pros



Ερωτήσεις

Ερωτήσεις

Moving forward

- OWASP guidelines
- bWapp
- Damn Vulnerable Web App

AN UNOFFICIAL GUIDE ON SEEKING A JOB.

“Be polite, be professional but have a plan to kill everyone you meet”
General J. Mattis
“Only those who risk going too far, can find out how far a man can go”
T.S. Eliot

whoami

- Τέλειωσα πιο νωρίς τις σπουδές μου από τους φίλους μου και δεν είμαι τύπος «μια δουλίτσα μωρέ να βγάζω κάνα φράγκο».
- Δε πήγα στρατό (ακόμα).
- Ξεκίνησα να ψάχνω για δουλειά.
- Άρα είχα μεγαλύτερη εμπειρία.
- Σε κάποια κουβέντα μου ζήτησαν να τα γράψω για να έχουν κάτι σαν οδηγίες.
- Να έχετε deadlines.
- Work in progress.

0x0-The basics

- Το να ψάχνεις δουλειά είναι full-time δουλειά.
- Δε σημαίνει ότι αφιερώνεις 8ωρο. Σημαίνει ότι το χειρίζεσαι εξίσου σοβαρά.
- Αφορά τη ζωή σου, το χειρίζεσαι τόσο σοβαρά όσο χειρίζεσαι τη ζωή σου.
- Ξέχνα ό,τι έμαθες και ό,τι διάβασες για τα βιογραφικά.
- Το να ψάχνεις για δουλειά είναι δύσκολο και ενίοτε και ψυχοφθόρο.
- Μερικοί θα προσπαθήσουν να υποβιβάσουν την προσπάθειά σας κυρίως γιατί φοβούνται να το προσπαθήσουν.
- **Εικάζω ήδη ότι ξέρετε τι θέλετε να κάνετε.**

0x1- Jobseeking

- Σκεφτείτε εταιρείες που θα θέλατε να δουλέψετε. Σκεφτείτε περίπου 20 τέτοιες εταιρείες.
- Βρείτε για κάθε εταιρεία 1-2 δουλειές τις οποίες πιστεύετε ότι μπορείτε να κάνετε.
- Βρείτε για κάθε εταιρεία πληροφορίες. Μισθοί, οργάνωση εταιρείας, projects με τα οποία ασχολείται, ποιοι εργάζονται σε αυτή την εταιρεία.
- Μιλήστε σε κάποιον εργαζόμενο της εταιρείας.
- Γενικότερα, ενδιαφερθείτε για την εταιρεία.

0x1- Jobseeking

- Μελετήστε κάθε αγγελία ζήτησης εργασίας σε βάθος.
- Πρέπει να ξέρετε ακριβώς τι ζητάει και τι δίνει (Perks, benefits κλπ) συναρτήσει της κουλτούρας κάθε εταιρείας.
- Κρατήστε σημειώσεις, βοηθάνε.

0x2 - CV

- Το CV είναι η ιστορία της ζωής σας.
- Διαχειριστείτε το όπως διαχειρίζεστε τη ζωή σας.
- Το CV γράφεται με βάση το job description, όχι με βάση οτιδήποτε κάνετε.
- 3 σελίδες μέγιστο.
- Θέλετε να πείτε μια ενδιαφέρουσα ιστορία.
- Βάλτε ενδιαφέροντα που έχετε. Όχι άλλη ιππασία και τένις.

0x2 - CV

1. Σκεφτείτε τη ζωή σας.
2. Για κάθε εταιρεία/αγγελία, γράφετε ξεχωριστό CV.
3. Μην υπερβείτε τις 3 σελίδες.
4. Γράψτε το σε Europass. Εκτός αν είστε γραφίστες.
5. Περιγράψτε τι σπουδάσατε.
6. Προσοχή στα χρονικά κενά.

0x3 – Cover Letters

- Είναι μικρό κείμενο.
- Είναι μια πρώτη ευκαιρία να δείξετε ότι δε κάνατε τυχαία αίτηση εκεί αλλά το ψάξατε.
- Είναι βασικό για το αν θα διαβάσει ο άλλος το βιογραφικό σας ή όχι.
- Πάλι, θέλετε να πείτε μια ενδιαφέρουσα ιστορία.

0x3 – Cover Letters

1. Να είστε ευγενικοί.
2. Ναι μεν είναι μικρό το κείμενο αλλά φροντίστε να είναι ενδιαφέρον.
3. Γράψτε τι θα κερδίσετε αλλά και τι θα κερδίσει η εταιρεία από εσάς.
4. Ψάξτε Online για cover letters αλλά προσαρμόστε τα στις ανάγκες σας.
5. Μη στέλνετε γενικά cover letters (point 2).

0x4 - Interviews

1. Ξαναδείτε τις σημειώσεις σας.
2. Οι συνεντεύξεις λειτουργούν αμφίδρομα.
3. Δεν είστε εκεί για να κάνετε νέους φίλους.
4. Το πώς περιγράφεις κάτι, λέει πολλά για σένα. Και για την έρευνα που έκανες.
5. Να είστε ειλικρινείς. Το «δεν το ξέρω» είναι προτιμότερο.
6. Μην είστε αλαζόνες. Ακόμα και αν γνωρίζετε τη σωστή απάντηση, αποφύγετε την αλαζονεία.
7. Ρίξτε μια ματιά σε διάφορα ζητήματα πριν τη συνέντευξη.
8. Μπορεί να σας ρωτήσουν οτιδήποτε.
9. Οι συνεντεύξεις γίνονται με οποιοδήποτε μέσο.
10. Μην είστε νευρικοί.
11. Κρατήστε σημειώσεις.
12. Ζητήστε feedback και κάντε ερωτήσεις.

0xΤυχαίες ερωτήσεις

- Παίζετε videogames? Αν ναι, ποια?
- Γιατί σας άρεσε αυτό το videogame?
- Ο πελάτης δε θέλει firewall. Τι κάνετε?
- Εμείς εδώ χρησιμοποιούμε .NET γιατί είναι πιο ασφαλής από την PHP.
- Από web services τι ξέρετε?
- Περιγράψτε μου το traceroute σε unix και windows.
- Έχω ένα GasGas 300EC αλλά δεν έχω παρέα να πάω για προπόνηση. Τι να κάνω;
- Τι κάνετε για να εξελίξετε την επαγγελματική σας γνώση;

0xIn General

- Αυτός που παίρνει τη συνέντευξη μπορεί να ρωτήσει οτιδήποτε. Μην εκπλαγείτε, ακόμα και αν σας ακουστεί εντελώς ηλίθιο.
- Η συνέπεια δείχνει και κουλτούρα εταιρείας. Αν δε μπορούν, πρέπει να σας ενημερώσουν.
- Μετά το τέλος κάθε συνέντευξης, σκεφτείτε πώς τα πήγατε και τι θα μπορούσατε να κάνετε διαφορετικά.
- Χρησιμοποιήστε τις σημειώσεις σας, ώστε σε μελλοντική συνέντευξη με την ίδια εταιρεία να δείξετε ότι ψάξατε τα ζητήματα που δε γνωρίζατε.

Catching up

mmavrofides@gmail.com

https://www.twitter.com/fr1t3

https://www.github.com/frite

The presentation will be online
http://download.tuxfamily.org/0x109/security/