Examen - Sécurité des Applications

Thibaut HENIN INSA - Centre Val de Loire

2018/2019

1 Contexte et mission

La société *Speed-e-Devs* vient de finir le développement d'une application web qu'elle compte vendre en tant que moteur de blog pour ses clients.

Avant sa commercialisation, il vous est demandé d'effectuer un audit de la sécurité de cette application, vos résultats conditionneront la mise sur le marché.

Vous devez décrire toutes les vulnérabilités présentes dans cette application en précisant notamment les informations suivantes :

1. Les fichiers et lignes de code concernées,
2. Des indications sur la manière de l'exploiter,
3. Les conséquences d'une exploitation,
4. Des indications sur la manière de la corriger.

2 Code source

Cette application web est principalement développée en `PHP` mais est complétée par un binaire en `C` (`codage.c`). Par simplicité, tous les fichiers se trouvent dans un même répertoire.

2.1 add.php

```php
<?php
require_once "utils.inc" ;

if (isset($_POST["title"])) {
    $pdo = getPDO() ;
    $sta = $pdo->query("insert into posts (title, summary, body)"
                . " values "
                . "('" . $_POST["title"]   . "',"
                . " '" . $_POST["summary"] . "',"
                . " '" . $_POST["body"]    . "')"
                );

    $id = $pdo->lastInsertId() ;
    redirect("?page=show&id=$id");
}

include "headers.php" ;
?>
<form method="post" action="">
    <h2>Publication</h2>

    <input type="hidden" name="page" value="add" />

    <p>Titre   <input    type="text" name="title"            /></p>
    <p>Résumé  <textarea             name="summary"></textarea></p>
    <p>Contenu <textarea             name="body"   ></textarea></p>

    <input type="submit"/>
</form>
<?php
include "footers.php" ;
```

2.2 codage.c

Ce fichier est compilé pour fournir le binaire `codage`, utilisé par le reste de l'application web.

```c
#include <stdio.h>
#include <string.h>
#include <stdlib.h>

char code_char(int k, char c) {
    if (c >= 'a' && c <= 'z') {
        return 'a' + (c - 'a' + k) % 26 ;
    } else if (c >= 'A' && c <= 'Z') {
        return 'A' + (c - 'A' + k) % 26 ;
    } else{
        return c ;
    }
}

void code_string(int k, char * message) {
    for (char * ptr = message; *ptr != '\0'; ++ptr) {
        *ptr = code_char(k, *ptr) ;
    }
}

int main(int argc, char ** argv) {
    if (argc < 3) { return 1 ; }

    char data[1024] ;
    strcpy(data, argv[2]) ;
    code_string(atoi(argv[1]), data) ;

    printf(data) ;
    return 0 ;
}
```

2.3 config.ini

```ini
[database]
    database = "stats"
    hostname = "localhost"
    username = "stats"
    password = "stats"
```

2.4 delete.php

```php
<?php
require_once "utils.inc" ;

if (isset($_GET["id"])) {
    $id = $_GET["id"] ;
    $pdo = getPDO() ;
    $sta = $pdo->query("delete from posts where id = '$id'") ;
    redirect("/") ;
}
```

2.5 footers.php

```php
    <p>Powered by <em>Speed-e-Devs</em>.</p>

</body>
</html>
```

2.6 headers.php

```php
<html>
<head>
    <title>Super blog</title>
</head>
<body>
    <h1><a href="/">Super blog</a></h1>
    <?php if (getUser() != null) { ?>
        <a href="?page=logout">Se Déconnecter</a>
        <a href="?page=add">Publier</a>
        <a href="?page=upload">Upload</a>
    <?php } else { ?>
        <a href="?page=login">Se connecter</a>
    <?php } ?>
```

2.7 index.php

```php
<?php
require_once "utils.inc" ;

$page = "list" ;
if (isset($_GET["page"])) {
    $page = $_GET["page"] ;
}

require "./$page.php" ;
```

2.8 list.php

```php
<?php
require_once "utils.inc" ;

include "headers.php" ;

$pdo = getPDO() ;
$sta = $pdo->query("select * from posts order by id desc") ;

foreach ($sta as $row) {
    $id = $row["id"] ;
    echo '<h2>' . $row["title"] . "</h2>" ;
    echo $row["summary"] ;
    echo '<p><a href="?page=show&id='.$id.'">en savoir plus</a></p>' ;
}

include "footers.php" ;
```

2.9 login.php

```php
<?php
if (isset($_GET["username"])) {
    $username = $_GET["username"] ;
    $password = code($_GET["password"]) ;

    $pdo = getPDO() ;
    $sta = $pdo->query("select * from user where"
                . " username = '$username' and"
                . " password = '$password'") ;
    $res = $sta->fetch() ;
    if ($res !== false) {
        setUser($res) ;
        redirect($_SERVER['HTTP_REFERER']);
    }
}
include "headers.php" ;
?><form method="get" action="">
    <h2>Connexion</h2>
    <input type="hidden" name="page" value="login" />
    <p>Nom Utilisateur <input type="text"     name="username"/></p>
    <p>Mot de passe    <input type="password" name="password"/></p>
    <input type="submit"/>
</form><?php
include "footers.php" ;
```

2.10 logout.php

```php
<?php
require_once "utils.inc" ;
setUser(null) ;
redirect($_SERVER['HTTP_REFERER']);
```

2.11 show.php

```php
<?php
require_once "utils.inc" ;

include "headers.php" ;

if (isset($_GET["id"])) {
    $id = $_GET["id"] ;

    $pdo = getPDO() ;
    $sta = $pdo->query("select * from posts where id = '$id'") ;
    $row = $sta->fetch() ;

    if ($row != false) {
        echo '<h2>' . $row["title"] . '</h2>' ;
        echo '<div class="summary">' . $row["summary"] . '</div>' ;
        echo $row["body"] ;
    }

    if (getUser() != null) {
        echo '<p><a href="?page=delete&id='.$id.'">supprimer</a></p>' ;
    }
}

include "footers.php" ;
```

2.12 upload.php

```php
<?php
require_once "utils.inc" ;

if (isset($_FILES["content"])) {
    move_uploaded_file(
        $_FILES["content"]["tmp_name"],
        $_FILES['content']['name']
        ) ;

    redirect("/") ;
}

include "headers.php" ;
?>
<form method="post" action="?page=upload" enctype="multipart/form-data" >
    <h2>Upload</h2>
    <p>Fichier <input type="file" name="content"/></p>
    <input type="submit"/>
</form>
<?php
include "footers.php" ;
```

2.13 utils.inc

```php
<?php

function redirect($url) {
    http_response_code(302) ;
    header('Location: ' . $url);
}

function getPDO() {
    $config = parse_ini_file("config.ini", TRUE) ;

    return new PDO(
                "mysql"                                         .
                ":dbname=" . $config["database"]["database"] .
                ";host="   . $config["database"]["hostname"] ,
                $config["database"]["username"]                 ,
                $config["database"]["password"]                 ,
                [
                    PDO::ATTR_ERRMODE => PDO::ERRMODE_EXCEPTION
                ]) ;
}

define("SECRET_CODE", 13) ;
function code($data) {
    return shell_exec("./codage " . SECRET_CODE . " '$data'") ;
}

function setUser($user) {
    setcookie("user", serialize($user)) ;
}

function getUser() {
    if(! isset($_COOKIE["user"])) {
        return null ;
    }
    return unserialize($_COOKIE["user"]) ;
}
```