Memo Réseaux - Système

La sécurité des formulaires

Github du campus sécurité-web.

Les failles de sécurité classiques dans le web :

- les failles XSS
- les injections SQL

Exemple de faille XSS

Dans le champs message, un script javascript peut être envoyé

```
<script>alert("Je vous est compris !");</script>
```

Solution de protection

Documentation PHP.

Dans le code html de la page, lancer systématiquement la fonction php suivante lorsqu'une info d'affichage arrive de l'extérieur :

```
htmlspecialchars ("code d'affichage du message");
```

- Protection du login
- Protection du message

Cette fonction remplace toutes les balises < > du message par des caractères pour que le navigateur ne puisse plus interpréter les balises javascript comme telles

< sera remplacé par <
> sera remplacé par >

Exemple d'injection SQL

Dans le champs message, la chaîne suivante permet d'écrire un message sous le nom de quelqu'un d'autre

```
test', 'tutu') #
```

test' le message est remplacé par test et l'apostrophe ferme le champs du message ,'tutu' le nom de l'utilisateur est remplacé par 'tutu' et le # met la fin de la requête en commentaire.

```
INSERT INTO message (message, author_login) VALUES ('Vacances', 'J oublie
tout')
```

deviendra

```
INSERT INTO message (message, author_login) VALUES ('test', 'tutu')
#Vacances', 'J oublie tout')
```

Solution de protection

Documentation PHP.

Devant la requête $POST, lancer systématiquement la fonction php suivante :

```
mysql_escape_string ($_POST['message','user']);
```

Cette fonction remplace les ' par \'

Le message qui s'affichera sera le suivant :

```
INSERT INTO message (message, author_login) VALUES ('Vacances\', \'J oublie
tout\')
```

Attention : Dans les deux exemple faire attention aux apostrophes dans le texte.

A noter que ces failles sont difficiles à exploiter car la plupart du temps contournées par les Framework comme LARAVEL