ZENNAKI Sonia - FOUILLEUX Samy - CHAMBREUIL Maxime - UV TechnoWeb -
Année 2001 / 2002

Technologie Web
Sécurité et CGI

But du TP

Le but du TP était de réaliser un petit formulaire de sondage : on choisit une valeur parmi 12 en réponse à une question, et le navigateur nous renvoie les résultats.

Comment-a-t-on utilisé les CGI pour notre formulaire de sondage

Le script CGI est appelé par la page HTML contenant le sondage, au moment ou le surfeur clique sur le bouton "Envoyer".

Tout d' abord, le script CGI va traiter les données : Il récupère le choix du sondé par le navigateur à la date t+1. Il ouvre le fichier de sauvegarde, récupère les données de la date t dans un tableau et referme le fichier.

Ensuite, il incrémente la valeur associée au choix de notre sondé courant. On calcule alors les pourcentages à la date t+1 que l'on renvoie à l'utilisateur sous forme d'une nouvelle page HTML. Cette page contient les différents choix du sondage, le pourcentage de tous les sondés pour chacun de ses choix et une barre dont la longueur est proportionnelle au nombre de voix.

Enfin, on réouvre notre fichier de sauvegarde pour réécrire les résultats de la date t+1. Le fichier est ainsi écraser pour ne conserver que les nouvelles valeurs.

Bugs rencontrés et solutions

Le script CGI se sert de la valeur sélectionnée par le navigateur. N'importe quel utilisateur peut la modifier car celle-ci se trouve dans une page HTML. Ainsi le script CGI contrôle la syntaxe de cette valeur à l'aide d'une expression régulière. Si la valeur a une mauvaise syntaxe, le script n'exécute rien.

Tout script est exécuté par "nobody". De plus, le script sauvegarde des données dans un fichier. Donc ce fichier doit être accessible en écriture par "nobody". Ainsi, "nobody" peut modifier le fichier. C'est pourquoi le script CGI contient les droits SUID : le script s'exécute avec les permissions de l'auteur du script, qui peut écrire dans le fichier. Comme ce fichier n'est accessible en écriture que par son propriétaire, le fichier est protégé de l'extérieur.

A-t-on tout sécurisé et comment ?

Nous avons sécurisé l'exécution du script et l'écriture du fichier de données. Un utilisateur ne peut écrire dans un fichier, exécuter ou faire exécuter certaines commandes dangereuses.

Nous n'avons pas encore sécurisé la multi-exécution par plusieurs utilisateurs faisant leurs choix en même temps. Il faut pour cela changer l'extension du fichier pour éviter la multi-écriture du fichier et fausser les résultats ou même le plantage du script (ouverture d'un fichier déjà ouvert).

Conclusion et avis sur le TP

En conclusion, un script CGI n'est jamais assez sécurisé. Cependant, ils sont utilisés par la plupart des sites web.

Ce TP nous a permis de nous familiariser avec le langage PERL ainsi que la gestion des droits et des permissions. Grâce à celui-ci, on comprend mieux les problèmes de sécurité relatifs à un site web.

Le script peut être testé avec le lien suivant : http://asi.insa-rouen.fr/~sfouille/TP2.html

Voici le script avec en bleu les textes qui vont apparaître sur la page web.

```
#!/usr/bin/perl -T -w
# Script de reception d'un formulaire

use CGI;
use strict;

my($query,$vote,@fichier,$total,$i);

print "Content-Type: text/html\n\n";
print "<html> <head>\n";
print "<title> Hello </title>";
print "</head>\n";
print "<body>";

$query=CGI::new();
$vote=$query->param('vote');
die "le  formulaire contient des caracteres interdits" if($vote !~ /[0-
9]/);
die "la valeur n est pas correcte" if ($vote>12 || $vote<1);

print "Numero choisi : ",$vote,"<P>\n";
--$vote;

open (DONNES,'<','/home/etud/asi01/pub/cgi-bin/sfouille/donnes');
@fichier =<DONNES>;
close(DONNES);
$total=0;
```

```
for ($i = 0; $i < 12; $i++)
      {
      $total=$total+$fichier[$i];
      }

print "total ",$total,"<BR>\n";
++$fichier[$vote];

print "<p>\n";
print "Eau : ",$fichier[0],"<BR>\n";
printf("pourcentage = \%.2f<BR>\n",$fichier[0]*100/$total);
print "<BR><IMG SRC=\"http://asi.insa-rouen.fr/icones/divers/blue.gif\"
WIDTH=$fichier[0] HEIGHT=10><P>\n";

print "Cafe : ",$fichier[1],"<BR>\n";
printf("pourcentage = \%.2f<BR>\n",$fichier[1]*100/$total);
print "<BR><IMG SRC=\"http://asi.insa-rouen.fr/icones/divers/red.gif\"
WIDTH=$fichier[1] HEIGHT=10><P>\n";

print "Chocolat chaud : ",$fichier[2],"<BR>\n";
printf("pourcentage = \%.2f<BR>\n",$fichier[2]*100/$total);
print "<BR><IMG SRC=\"http://asi.insa-rouen.fr/icones/divers/green.gif\"
WIDTH=$fichier[2] HEIGHT=10><P>\n";

print "The : ",$fichier[3],"<BR>\n";
printf("pourcentage = \%.2f<BR>\n",$fichier[3]*100/$total);
print "<BR><IMG SRC=\"http://asi.insa-rouen.fr/icones/divers/blue.gif\"
WIDTH=$fichier[3] HEIGHT=10><P>\n";

print "Jus d'orange : ",$fichier[4],"<BR>\n";
printf("pourcentage = \%.2f<BR>\n",$fichier[4]*100/$total);
print "<BR><IMG SRC=\"http://asi.insa-rouen.fr/icones/divers/red.gif\"
WIDTH=$fichier[4] HEIGHT=10><P>\n";

print "Biere : ",$fichier[5],"<BR>\n";
printf("pourcentage = \%.2f<BR>\n",$fichier[5]*100/$total);
print "<BR><IMG SRC=\"http://asi.insa-rouen.fr/icones/divers/green.gif\"
WIDTH=$fichier[5] HEIGHT=10><P>\n";

print "Tequila : ",$fichier[6],"<BR>\n";
printf("pourcentage = \%.2f<BR>\n",$fichier[6]*100/$total);
print "<BR><IMG SRC=\"http://asi.insa-rouen.fr/icones/divers/blue.gif\"
WIDTH=$fichier[6] HEIGHT=10><P>\n";

print "Vodka : ",$fichier[7],"<BR>\n";
printf("pourcentage = \%.2f<BR>\n",$fichier[7]*100/$total);
print "<BR><IMG SRC=\"http://asi.insa-rouen.fr/icones/divers/red.gif\"
WIDTH=$fichier[7] HEIGHT=10><P>\n";

print "Gin : ",$fichier[8],"<BR>\n";
printf("pourcentage = \%.2f<BR>\n",$fichier[8]*100/$total);
print "<BR><IMG SRC=\"http://asi.insa-rouen.fr/icones/divers/green.gif\"
WIDTH=$fichier[8] HEIGHT=10><P>\n";

print "Guronsan : ",$fichier[9],"<BR>\n";
printf("pourcentage = \%.2f<BR>\n",$fichier[9]*100/$total);
print "<BR><IMG SRC=\"http://asi.insa-rouen.fr/icones/divers/blue.gif\"
WIDTH=$fichier[9] HEIGHT=10><P>\n";
```

```
print "Rien, je dors : ",$fichier[10],"<BR>\n";
printf("pourcentage = \%.2f<BR>\n",$fichier[10]*100/$total);
print "<BR><IMG SRC=\"http://asi.insa-rouen.fr/icones/divers/red.gif\"
WIDTH=$fichier[10] HEIGHT=10><P>\n";

print "Rien, pas le temps : ",$fichier[11],"<BR>\n";
printf("pourcentage = \%.2f<BR>\n",$fichier[11]*100/$total);
print "<BR><IMG SRC=\"http://asi.insa-rouen.fr/icones/divers/green.gif\"
WIDTH=$fichier[11] HEIGHT=10><P>\n";
print "<p>\n";

open (DONNES,'>','/home/etud/asi01/pub/cgi-bin/sfouille/donnes');
for($i=0;$i<12;$i++)
        {
        if ($i eq $vote)
                {
                print DONNES "$fichier[$i]\n";
                }
        else
                {
                print DONNES "$fichier[$i]";
                }
        }
close(DONNES);
print "</body></html>\n";
```