## Faille de sécurité
Posté par Rémi Lapeyre - 22-11-2010 à 22:52

---

Bonjour. J'utilise Wims en tant qu'élève et souhaite faire part d'une faille de sécurité. Je ne suis pas certain d'être dans le bon forum pour ça mais je n'ai pas trouvé d'endroit plus approprier pour cela donc je me permet de poster quand même.

Cette faille utilise l'identifiant de session pour pouvoir utiliser le compte d'une autre personne conectée simultanément (ou au plus tard une heure après sa dernière action si elle a oublié de se déconnecter). Pour l'éviter, je pense qu'il serait suffisant de noter l'adresse ip de l'utilisateur dans une variable de session lors de sa connexion puis de vérifier que celle-ci reste la même à chaque pages chargées. Si ce n'est pas le cas, on peut alors afficher un formulaire demandant à l'uilistrur de rentrer à nouveau son mot de passe pour vérifier son identité.

Rémi Lapeyre

==========

## Re:Faille de sécurité
Posté par schaersvoorde - 22-11-2010 à 23:25

---

You are right, it's fairly easy to "hack" into a user_session,once you've copied the session_number.
(pen and paper...)

Using the IP adress for extra security won't help , if all users share the same ip-adres from the localnetwork .

On our school we've had a single "serious incident" of a pupil logging into a supervisor/teacher session
All 'exams & sheets' were altered, passwords changed etc etc.

This has proven a very good lesson to all other users/teachers: they now close the session when leaving the computer :)

kind regards,
Joke Evers

==========

## Re:Faille de sécurité
Posté par Rémi Lapeyre - 22-11-2010 à 23:32

---

En effet, la vérification de l'adresse ip n'est valable que si l'utilisateur se connecte depuis un autre lieu et ne dispense pas des règles de sécurité de base. Cela permet cependant d'éviter qu'un élève puisse tomber sur la session de quelqu'un d'autre en faisant des tentatives aléatoires chez lui. Pour éviter la connexion depuis un ordinateur du même réseau  on pourrait marquer dans un cookie un jeton aléatoire que l'on pourrait comparer avec celui comparer dans une variable de session. De cette manière, l'identifiant de session ne servirai a rien seul ; cependant, si j'ai bien compris la politique de Wims au sujet des cookies est de les utiliser au minimum...

==========

## Re:Faille de sécurité
Posté par Rémi Lapeyre - 22-11-2010 à 23:37

---

La seule possibilité d'éviter qu'un élève puisse profiter de l'absence d'un professeur pour se servir de son compte est de demander le mot de passe avant chaques actions "critiques" : suppression d'élèves, modification de notes, de feuilles d'exercices...

==========

## Re:Faille de sécurité
Posté par schaersvoorde - 23-11-2010 à 07:36

---

There is also the possibility to set very "sharp" timings on idle user_sessions.
e.g. kill the idle session after -let's say- 5 minutes. Leaving the "hacker" not much time to intrude and destroy :)

==========

## Re:Faille de sécurité

Posté par bernadette - 23-11-2010 à 09:56

---

Bonjour

Merci de vos remarques. Cette "faille" est connue depuis longtemps et non considérée comme une faille tant qu'il ne s'agit pas d'un examen.

La solution avec les numéros IP est intéressante, c'est ce qui est fait pour les examens ... Il y a une discussion dans le forum au même moment où il est demandé d'enlever cette contrainte car les numéros IP maintenant changent très souvent
au cours d'une même session. Je suis aussi un peu réticente pour le faire. Peut-être faut-il laisser le choix aux enseignants à leurs risques et périls.

Mais la proposition de rajouter un "jeton" est intéressante.

Pour le mot de passe enseignant, il y a la possibilité pour lui d'utiliser un mot de passe jetable (qui ne sert donc qu'une seule fois).
Il y a aussi la possibilité de ne faire les opérations sensibles que d'une adresse IP fixe ou avec envoi d'un courrier. Mais la plupart du temps, les enseignants trouvent cela trop contraignants et désactivent ... Et là, on ne peut
rien faire pour eux !

Peut-être que ton message leur fera faire prendre conscience qu'ils ont tort !

Bernadette

==========

## Re:Faille de sécurité

Posté par Rémi Lapeyre - 23-11-2010 à 19:38

---

Bonjour.

Diminuer la durée d'une session pourrait en effet être une possibilité pour réduire le temps utilisable pour tenter de récupérer l'identifiant de quelqu'un. Je suis surpris que l'utilisation de l'adresse ip soit déprécié à cause de leur durée de vie : je ne savais pas qu'elles étaient changés si souvent.

La solution du jeton aléatoire peut être intéressante mais si j'ai bien compris la politique de Wims à propos des cookies est d'en laisser le moins possible (je n'en ai trouvé qu'un sur mon ordinateur). Cela permettrait quand même (j'ai peur de dire une grosse bêtise, mais bon, soyons fou... ) de rendre la recherche d'accès à un compte à une complexité quadratique (autrement dit, plus la peine d'essayer en une heure... ).

Une possibilité pour rendre la protection la moins contraignante possible serais, je crois :

— À la connexion, on note l'adresse ip de l'utilisateur dans une variable de session, on génère un jeton aléatoire que l'on note dans un cookie et dans une variable de session ;

— À chaque pages chargées, on vérifie si l'adresse ip est bien la même ;

— Si elle a été changée, alors on vérifie le contenu du cookies dans le on a noté le jeton ;

— Si le jeton n'existe pas ou n'est pas le bon : on est alors soit dans le cas où un utilisateur a changé d'adresse ip pendant la session et a désactivé les cookies, soit devant une tentative de piratage ; on affiche alors une fenêtre de connexion pour vérifier à nouveau le mot de passe.

En couplant les deux systèmes, on peut alors rendre la protection moins contraignante pour les utilisateurs et pourtant assez sûre (bien que ça dépende du pourcentage d'internautes ayant une adresse ip dynamique et ayant désactivé les cookies, ce dont je n'ai aucune idée).

Rémi Lapeyre

==========