المقالات العلمية

ملفات تعريف الارتباط الآمنة

الكاتبة: ريمه بنت عبدالله العبداللطيف

تنبيه:

تعتبر هذه المقالة مشاركة من كاتبها في زيادة التوعية والمحتوى الخاص بأمن المعلومات، وقد راجعها مراجع واحد على الأقل، ولا يتحمل مركز التميز لأمن المعلومات أي تبعات لهذه المقالة، ولا أي معلومات تطرح في هذه المقالة ولا يضمن دقة المعلومة وصحتها.

الملخص

سهلت الشبكة العنكبوتية أو ما يعرف بالويب (World Wide Web) التجارة الإلكترونية على الإنترنت عن طريق بروتوكول نقل النصوص التشعيبية (Hypertext Transport Protocol) والذي يقوم بنقل التفاعلات بين خادم الويب (Web Server) و المتصفح (Browser) بمساعدة ملفات تعريف الارتباط (Cookies).

الكلمات المفتاحية

ملفات تعريف الارتباط الآمنة، السرية، السلامة ، التحقق من الهوية

1.المقدمة

اخترعت ملفات تعريف الارتباط للحفاظ عل ى الاستمرارية والحالة على الويب . تتكون هذه الملفات من سلسلة من الحروف والأرقام والرموز والتي تدل على معلومات مشفرة للمستخدم. عندما يزور شخص ما موقع يستخدم هذه الملفات فإنها ترسل للقرص الصلب أو الذاكرة المؤقتة له عن طريق المتصفح وعندما يعود الشخص لخادم الويب الذي حصل منه على هذه الملفات يقوم الخادم باستخدامها . فالهدف من ملفات تعريف الارتباط هي اكتساب معلومات لاتصالات لاحقة بين خادم الويب والمتصفح بدون طلبها كل مرة من المستخدم.

انه ليس بالأمر الصعب تشفير هذه الملفات على أساس معلومات المستخدم ، فعلى سبيل المثال : باستطاعة خادم الويب الذي يهدف إلى التجارة استعمال اسم العميل و رقم البطاقة الإئتمانية كأساس لها . لكن و بالرغم من أن هذه الطريقة تعتبر سهلة للمستخدمين إلا أنها خطرة لأن الملفات تكون مخزنة ومنقولة بنص واضح مما يسهل قرائتها وتزويرها.

إحدى الطرق التي يمكن أن تحل المشكلة السابقة هي أن تجعل ملفات تعريف الارتباط آمنة.

في هذا المقال ستطرح طرق متعددة بكيفية جعل ملفات تعريف الارتباط كفيلة بنقل وتخزين البيانات المهمة.

© CoEIA
الكاتبة: ريمه بنت عبدالله

2.ملفات تعريف الارتباط

ملفات تعريف الارتباط عبارة عن ملفات نص ية صغيرة يخزّنها متصفح الانترنت في جهاز المستخدم . تخدم هذه الملفات أغراض عديدة منها:

- الحفاظ على محتويات سلة التسوق الالكترونية
- الحفاظ على بيانات المستخدم

جميع ملفات تعريف الارتباط متشابهة في الأساس . ملف تعريف الارتباط المثالي ، الصورة 1 ، يتكون من عدة حقول وهي كما يلي:

حقل اسم ملف تعريف الارتباط (Cookie_Name) و حقل قيمة ملف تعريف الارتباط (Cookie_Value) تحتوي على معلومات يحتاجها موقع الويب. حقل التاريخ (Date) يحوي تاريخ انتهاء الملف. حقل المجال (Domain) يحوي اسم المضيف التي تكون فيه ملفات تعريف الارتباط سارية المفعول. حقل المؤشر (Flag) يحدد ما إذا كانت جميع الأجهزة في المجال المحدد تملك الصلاحية للوصول إلى ملف تعريف الارتباط. حقل المسار (Path) يقيد استخدام ملف تعريف الارتباط ضمن موقع الويب بحيث ان استخدامها قاصر على الصفحات التي يتضمنها هذا الحقل.

	Domain	Flag	Path	Cookie_Name	Cookie_Value	Secure	Date
Cookie 1	acme.com	True	/	Name_Cookie	Alice	False	12/31/2000
⋮			⋮		⋮		
Cookie *n*	acme.com	True	/	Role_Cookie	Manager	False	12/31/2000

صورة1: ملف تعريف ارتباط مثالي على الويب

عندما يقوم المتصفح بطلب عنوان موقع ويب (URL) من خادم الويب فإن المتصفح يقوم بإرسال حقلي اسم م لف الارتباط و قيمة ملف الارتباط للخادم . ملفات تعريف الارتباط التي يتلقاها الخادم تستخدم في الاتصالات بين الخادم والمتصفح. في حال أن الخادم لم يتلقى هذه الملفات، فإنه سيعمل بدون استخدمها أو يقوم بصنع ملفات جديدة لتستخدم لاتصالات الخادم والمتصفح اللاحقة . باستطاعة خادم الويب تحديث ملفات تعريف الارتباط حينما يقوم المستخدم بزيارته.

3.مخاوف أمنية

عادة ما يستعمل خادم الويب ملفات تعريف الارتباط لتمييز المستخدمين وحالاتهم. على سبيل المثال، لو وجدت قاعدة بيانات في موقع ويب تجاري للزبائن تحوي معلومات عنهم كأسمائهم، أرقام بطاقاتهم الإئتمانية و مقدار ما دفعوه فإن هذا الموقع يستخدم ملفات تعريف الارتباط ليخزن مؤشرات لسجلات كل زبون. و لكن لأن هذه الملفات يسهل تزويرها فإن المعقول ه و تخزين رقم هوية بسيطة للزبون فيها بدلا من معلوماته.

السرية هي إحدى المخاوف الرئيسية حول ملفات تعريف الارتباط. هذه الملفات تسمح لخوادم الويب تعقب أسلوب تصفح المستخدم.

4.أخطار أمنية

هناك ثلاثة أخطار متعلقة بملفات تعريف الارتباط وجميعها سهلة التطبيق:

1. الشبكة
2. النظام الطرفي
3. حصاد ملفات تعريف الارتباط

أولا: ملفات تعريف الارتباط المرسلة عبر الشبكة بنص واضح معرضة للتطفل والتغيير من أخ طار الشبكة. بالرغم من أنه باستطاعة بروتوكول طبقة المقابس الآمنة (Secure Sockets Layer Protocol) إحباط هذه التهديدات فإنه يستطيع حمايتها ضمن الشبكة فقط.

ثانيا: إذا انتقلت الملفات إلى النظام الطرفي للمتصفح فإنها تستقر على القرص الصلب أو الذاكرة بنص واضح أيضا مما يجعل تعديلها و نسخها من جهاز إلى آخر أمرا سهلا وهو ما يعرف بأخطار النظام الطرفي . القدرة على نسخ وتعديل الملفات تسهل على المهاجمين تزويرها و التنكر بشخصيات المستخدمين.

أخيرا: إذا حاكى المهاجم موقع ويب يقبل ملفات تعريف الارتباط من المستخدمين فإنه سيقوم بجمعها واستخدامها لمواقع ويب أخرى تقبلها. تعرف هذه الحالة بأخطار حصاد ملفات تعرف الارتباط.

5.الكوكيز الآمنة

تحقق ملفات تعريف الارتباط الآمنة ثلاث من الخواص:

1. التحقق: : تتحقق من مالك ملفات تعريف الارتباط
2. السلامة: تحمي معلومات ملفات تعرف الارتباط من التعديل الغير مصرح به عليها.
3. السرية: : تضمن عدم تسرب معلومات ملفات تعريف الارتباط لطرف غير مصرح له بالاطلاع عليها

5.1 التحقق من المستخدم

يمكن التحقق من المستخدمين باستعمال نوع من ملفات تعريف الارتباط التالية (صورة 2):

1. ملفات تعريف ارتباط أساسها العنوان (IP_Cookie)

عندما يزور المستخدم موقع ويب فإن الخادم يأخذ عنوانه ويحفظه في ملف تعريف الارتباط . إذا زار المستخدم الموقع مرة أخرى فإن الخادم يقارن عنوان المستخدم الحالي مع العنوان الموجود في ملف الارتباط فإذا ما تطابقا فإن المستخدم يعتبر المالك الحقيقي لهذه الملفات.

تعد هذه الآلية سهلة لكونها غير ظاهرة للمستخدم لكنها غير مرغوبة دائما. فعلى سبيل المثال: إذا كان المستخدم يحصل على عنوان جديد في كل اتصال بالانترنت فإن ملفات تعريف الارتباط تعد باطلة بالرغم من أنه يستخدم نفس الجهاز.

علاوة على ذلك، في حال أن مجال المستخدم يستعمل خادم بروكسي (Proxy Server) فإن باستطاعة مهاجم ما أن يجمع ملفات تعريف الارتباط للمستخدم تشملها الملفات التي أساسها العنوان عن طريق حصادها ومن ثم التنكر بشخصية المستخدم خلال نفس خادم البروكسي، وذلك لأن خادم البروكسي يعطي نفس العنوان للمستخدمين في نفس المجال . كذلك محاكاة العناوين أمر لا يمكن تفاديه – وهو أن ترسل رسائل لحاسوب بعنوان موثوق به للحصول على وصول غير مصرح به.

2. ملفات تعريف ارتباط أساسها كلمة المرور (Pswd_Cookie)

هذا النوع من الملفات يدعم العناوين المتغيرة و خوادم البروكسي ويتفادى محاكاة العناوين . كلمة المرور التي ستستخدم في هذه الملفات تنقل محمية عبر الشبكة من المتصفح إلى الخادم . إذا حصل الخادم على كلمات المرور من المستخدم فإنه يقوم بتشفيرها و وضعها في ملفات تعريف الارتباط . يتوجب على المستخدم كتابة نفس كلمات المرور متى ما قامت بزيارة الخادم مرة أخرى.

هذه الطريقه معرضة بالأساس للهجمات التي تعتمد على القواميس – و هي أن تجرب جميع المفردات في القواميس ككلمات مرور ومن ثم تشفر و تقارن نتيجة التشفير بالشفرة الموجودة في الملفات – و ظاهرة للمستخدم لأن كلمة المرور تطلب من المستخدم كل مرة يصل فيها للخادم.

© CoEIA
الكاتبة: ريمه بنت عبدالله

3. ملفات تعريف ارتباط أساسها التوقيع الإلكتروني (Sign_Cookie)

لو كانت خوادم الويب تعرف المفاتيح العامة (Public Key) للمستخدمين، فإن تقنيات التوقيع الإلكتروني يمكن أن تستخدم للتحقق من هوية المستخدمين . في هذه الطريقة يحتاج المستخدم إلى برنامج إضافي في المتصفح يولد ملفات تعريف ارتباط تحتوي على طوابع وقت موقعة . فعلى سبيل المثال، إذا أراد المستخدم الوصول إلى خادم ويب يعرف المفتاح العام للمستخدم فإن جهاز المستخدم يولد طابع وقت و يضعها في ملفات تعريف الارتباط التي سترسل للخادم و الذي يتحقق بدوره من هوية المستخدم بمقارنة المفت اح العام بالتوقيع الموجود بطابع الوقت.

	Domain	Flag	Path	Cookie_Name	Cookie_Value	Secure	Date
IP_Cookie	acme.com	True	/	IP_Cookie	129.174.100.88	False	12/31/2000
Pswd_Cookie	acme.com	True	/	Pswd_Cookie	hashed_password	False	12/31/2000
Sign_Cookie	acme.com	True	/	Sign_Cookie	Signature_of_Alice	False	12/31/2000

صورة 2 : ملفات تعريف الارتباط الموثقة

5.2 سلامة البيانات

سلامة بيانات ملفات تعريف الارتباط تعد من المشاكل المتعلقة بها . فعلى سبيل المثال : باستطاعة مهاجم ما نسخ ملفات تعريف الارتباط التي أساسها العنوان لمستخدم و تعديلها بعنوان آخر ومن ثم التنكر بشخصية المستخدم لخادم الويب. أيضا بإمكان المستخدم نفسه أن يقوم بالتعديل عليها.

هناك نوعان من الحلول التي تساعد في المحافظة على سلامة البيانات:

1. حل أساسه المفتاح العام

يستعمل الخادم المصدر لملفات تعريف الارتباط خوارزمية هضم الرسالة مثل MD5 أو SHA ليصدر رسالة مصغرة من ملفات تعريف الارتباط باستخدام المفتاح العام و يوقع عليها باستخدام مفتاحه الخاص و يضع التوقيع في حقل خاص في هذه الملفات . عندما يزور المستخدم خادم ويب يسمح بملفات تعريف الارتباط فإ ن المتصفح يرسل الملفات الآمنة للخادم والذي بدوره يتحقق من التوقيع باستخدام المفتاح العام للخادم الذي أصدر هذه الملفات.

هذا الحل يجعل عملية تحديث الملفات ملقاة على عاتق الخادم المصدر للملفات.

2. حل أساسه مفتاح سري (Secret Key)

يصنع الخادم المصدر لملفات تعريف الارتباط شفرة تصديق خاصة بالرسالة (MAC) لملفات تعريف الارتباط باستخدام خوارزميات مثل HMAC ويضعها في حقل خاص فيها . عندما يتصل المستخدم بخادم الويب فإن الخادم يجمع ملفات تعريف الارتباط من المتصفح . إذا كان الخادم يشترك بمفتاح سري مع الخادم المصدر لملفات تعريف الارتباط فإنه يصدر شفرة تصديق خاصة بالرسالة للملفات ويقارن النتيجة بالقيمة الموجودة في الملفات.

هذا الحل يجعل عملية تحديث الملفات ممكنة لأي خادم دون الحاجة للرجوع للخادم المصدر لها.

5.3 سرية البيانات

لحماية البيانات الحساسة من الاطلاع عليها لطرف غير مخول له بذلك بإمكان خادم الويب تشفيرها . تستخدم ملفات تعريف ارتباط أساسها المفتاح (Key_Cookie) لتخزين مفتاح الجلسة المشفر الذي استخدم لتشفير البيانات في ملفات أخرى. يشفر مفتاح الجلسة باستخدام مفتاح العام أو مفتاح سري للخادم [1].

6. الخلاصة

ملفات تعريف الارتباط الآمنة تحتمل ثلاث من الخواص السرية ، التحقق والسلامة . هذه الخواص قد تتطلبها بعض الخوادم جميعا في حين أن خوادم أخرى تحتاج إلى واحدة أو اثنتان منها. تعتمد الحاجة لهذه الخواص بنوع الخدمات التي تقدمها الخوادم لزائريها.

7. المراجع والمصادر:

[1] جون بارك و رايفي ساندو ،"SecureCookies on the Web"، جامعة جورج ميسن، أوغست 2000