Forum mit variablen SSL Zugang

Autor	Nachricht	
Dungeonwatcher	Betreff des Beitrags: Forum mit variablen SSL Zugang	Sa 01.Dez, 2007 15:14

Hi!

Die Zeiten für "Horch und Kuck" werden in diesem Lande ja leider immer besser... ¦9

Es gibt ja die Möglichkeit das Forum auf SSL Zugang umzuschalten. Dies habe ich Testweise mit meinem Forum und einem selbst erstellten privaten Key getan. Soweit so gut. Nur leider fehlt mir die Möglichkeit diesen Zugang variabel zu gestalten. D.h. der User soll selbst entscheiden ob er sich per SSL oder ohne einloggen will und diese Wahl soll bis zum ausloggen erhalten bleiben.
Aktuell landet er auf dem Portal ohne SSL und nach dem Einloggen hat er eine SSL Verbindung. Das ist insofern unschön, als das ich mich ab und zu von meiner Fa. einlogge und dort der Port 443 gesperrt ist.

Bye

Autor	Nachricht	
oxpus	Betreff des Beitrags:	Sa 01.Dez, 2007 17:25

> Zitat:
> [...] und dort der Port 443 gesperrt ist.

Und wieder einmal Netzwerktechniker am werkeln, die von Sicherheit Null Ahnung haben...

Nun, das phpBB kann man entweder mit Sicherheit (SSL) oder ohne betreiben, da ja auch eben sicherere, bzw. unsichere Cookies verwendet werden.
Da wäre eine Menge anzupassen, wenn man das userabhängig gestalten will.

BTW: Was bringt es dann insgesamt an Mehrwert, wenn User das ablehnen kann?
Sicherer/unsicherer wird das Board mit dieser Möglichkeit auch nicht wirklich...

Autor	Nachricht	
Dungeonwatcher	Betreff des Beitrags:	Sa 01.Dez, 2007 17:41

Hi!

[quote="oxpus";p="79628"]

> Zitat:
>
> [...] und dort der Port 443 gesperrt ist.
>
> Und wieder einmal Netzwerktechniker am werkeln, die von Sicherheit Null Ahnung haben...
> Naja, über die Techniker meiner Behörde sage ich jetzt mal lieber nichts weiter...

> Zitat:
>
> Nun, das phpBB kann man entweder mit Sicherheit (SSL) oder ohne betreiben, da ja auch eben sicherere, bzw. unsichere Cookies verwendet werden.
> Da wäre eine Menge anzupassen, wenn man das userabhängig gestalten will.

Es muss ja nicht direkt Userabhängig sein, reicht es nicht wenn es Sessionabhängig ist? Ich denke da so an einen "Haken" der bei "SSL" auf dem Portal zu entfernen ist und dann geht es weiter ohne SSL.

> Zitat:
>
> BTW: Was bringt es dann insgesamt an Mehrwert, wenn User das ablehnen kann?
> Sicherer/unsicherer wird das Board mit dieser Möglichkeit auch nicht wirklich...

Mir geht es einfach nur darum, das ich das "mitlesen" der Daten im "Klartext" verhindern will.

Autor	Nachricht	
oxpus	Betreff des Beitrags:	Sa 01.Dez, 2007 22:28

Welches "mitlesen"?
Im Internet ist nie etwas sicher.

Autor	Nachricht	
Dungeonwatcher	Betreff des Beitrags:	So 02.Dez, 2007 00:36

Hi big master!

[quote="oxpus";p="79633"]Welches "mitlesen"?
Durch "Horch und Kuck" z.B.

> Zitat:
>
> Im Internet ist nie etwas sicher.

Doch, so ziemlich alles was nicht im "Klartext" durch die Leitung rauscht.

Autor	Nachricht	
oxpus	Betreff des Beitrags:	So 02.Dez, 2007 14:10

Irrtum: SSL wurde bereits schon mehrfach geknackt!

Im Internet ist eben nur eins sicher: Das **nichts** sicher ist

Autor	Nachricht	
Dungeonwatcher	Betreff des Beitrags:	So 02.Dez, 2007 15:24

Hi!

Trotzdem muss doch nicht alles auf dem "Silbertablett" präsentiert werden, oder?

Abgesehen davon, dürfte es doch etwas dauern dies zu "knacken":

SSL-Version: 3
Bevorzugte Verschlüsselung: Triple-DES (168/112 Bit)
Prüfsummenverfahren: SHA-1 (160 Bit)
RSA-Modulus: 2048

und wenn ich dann noch dies dazu sehe:

"**Verbindung hochgradig verschlüsselt (AES-256 256-bit)**"

dann bin ich schon sicher das das mit vertretbarem Aufwand nicht zu knacken ist.

Autor	Nachricht	
oxpus	Betreff des Beitrags:	So 02.Dez, 2007 20:37

> Zitat:
> Trotzdem muss doch nicht alles auf dem "Silbertablett" präsentiert werden, oder?

Sofern die Inhalte Deines Boards sooooo geheim sind, daß die keiner lesen soll

Nochmal:
Ob nun session- oder userbezogen die SSL-Verschlüsselung nicht aktiviert sein soll, bedeutet so oder so eine Menge Arbeit am Forum, genau das zu erreichen.
Denn man muss dem Board ja erst einmal beibringen, überall und in allen Stellen des Boards, wo eben Links zum Forum erstellt werden, zu unterscheiden, ob SSL ja oder nein.
Und ich halte das gerade bei der Aufbereitung von Benachrichtungen zu neuen Beiträgen für eher unmöglich.

Beispiel:
Es wird ein neuer Beitrag erstellt und es sind User zu benachrichtigen.
Nun muss der Server-Link an dieser Stelle (und wie gesagt: Es gibt hier "viele" Stellen im Forum, an denen das gemacht werden muss) eben entschieden werden, für welche Session oder welchen User (je nachdem, wie man das einrichten will) eben SSL gelten soll oder auch nicht.
Aktuell passiert das ja nach den Board-Einstellungen, was einfacher geht, da die Angaben global in der $board_config vorhanden sind.
Mit Umstellzung auf Session/User muss das immer mit abgefragt werden und genau hier gibt es dann Probleme:
Wenn sich ein User mit seiner Session per SSL auf dem Board angemeldet hat, würde er auch z. B. SSL-Links per EMail erhalten. Dann könnte es Schwierigkeiten geben, wenn der User aus dem Link das https:// durch http:// ersetzt, daß Cookie und Session-Code nicht mehr dazu passen.
Auch hier wäre viel Arbeit angesagt, genau das zu berücksichtigen.
Anders herum würde das Forum eine neue Session erstellen, wenn vorher ohne und nun mit SSL das Board besucht wurde, was auch wieder zu einem Cookie-Fehler führen kann.

Ergo:
Abgesehen von der mords Arbeit, hier geziehlt in die vorhandenen Sessions einzugreifen, und das im schlimmsten Fall durch alle Scripte des Boards hindurch(!), müsste man nach meinen Wissen vorhandene Cookies erst löschen, bevor ein Session-Wechsel mit und ohne SSL sauber vollzogen werden kann.
Die Folge wären ggf. Verluste der neuen Beiträge (wenn man keine MODs wie den UPi2DB verwendet) und man müsste auch jedesmal das Login bedienen.

Ich weiß nicht, ob das wirklich soooo viel Sinn macht, wenn eben User dabei sind, die SSL nicht bedienen können, weil z. B. die Ports gesperrt sind.

Und mal unter uns:
Wenn ich den SSL Schlüssel nicht schnell genug knacken kann, melde ich mich einfach am Forum an und spiele zunächst "guter Junge". Bin ich dann nach der Reg. drinnen, habe ich auch alles, was ich will
Eine von vielen Möglichkeiten, ein Forumsystem bezogen auf diese Art der Sicherheit auszuhebeln...

Autor	Nachricht	
Dungeonwatcher	Betreff des Beitrags:	Mo 03.Dez, 2007 14:02

Moin!

[quote="oxpus";p="79648"]

> Zitat:
>
> Trotzdem muss doch nicht alles auf dem "Silbertablett" präsentiert werden, oder?

Sofern die Inhalte Deines Boards sooooo geheim sind, daß die keiner lesen soll

Das nun wieder nicht, aber rein aus Prinzip und Protest gg. die aktuelle Politik ala Schäuble und Co.

> Zitat:
>
> Nochmal:
>
> Ob nun session- oder userbezogen die SSL-Verschlüsselung nicht aktiviert sein soll, bedeutet so oder so eine Menge Arbeit am Forum, genau das zu erreichen.
>
> Denn man muss dem Board ja erst einmal beibringen, überall und in allen Stellen des Boards, wo eben Links zum Forum erstellt werden, zu unterscheiden, ob SSL ja oder nein.
>
> Und ich halte das gerade bei der Aufbereitung von Benachrichtungen zu neuen Beiträgen für eher unmöglich.

Das will ich dir dann mal glauben.

> Zitat:
>
> Ich weiß nicht, ob das wirklich soooo viel Sinn macht, wenn eben User dabei sind, die SSL nicht bedienen können, weil z. B. die Ports gesperrt sind.

Die und auch werden mich dann daran gewöhnen müssen.

> Zitat:
>
> Und mal unter uns:
>
> Wenn ich den SSL Schlüssel nicht schnell genug knacken kann, melde ich mich einfach am Forum an und spiele zunächst "guter Junge". Bin ich dann nach der Reg. drinnen, habe ich auch alles, was ich will

Nicht wirklich. Auch im Forum direkt kann man ja gut mit den jeweiligen Rechten arbeiten und "verstecken". Es geht mir echt nur um das "ausschnüffeln" auf der Leitung und da ist SSL momentan die beste Möglichkeit.

Autor	Nachricht	
oxpus	Betreff des Beitrags:	Mo 03.Dez, 2007 14:13

Zitat:

Das nun wieder nicht, aber rein aus Prinzip und Protest gg. die aktuelle Politik ala Schäuble und Co.

Sehr blauäugig gedacht, denn der Gesetzgeber würde sich sicherlich auch hier etwas einfallen lassen

Zitat:

Nicht wirklich. Auch im Forum direkt kann man ja gut mit den jeweiligen Rechten arbeiten und "verstecken". Es geht mir echt nur um das "ausschnüffeln" auf der Leitung und da ist SSL momentan die beste Möglichkeit.

Zumindest nach dem, was bekannt ist.
Ich möchte nicht wissen, welche Methoden und Hintertüren existieren, um den Strom live mitlesen zu können und das mit dem jeweils gültigen Schlüssel.
Merke: Wenn jemand das ernsthaft will und "ganz oben" sitzt, bekommt er auch, was er will.
Da nützt dann auch SSL überhaupt nichts mehr, sondern nur noch "Stecker ziehen"

Autor	Nachricht	
Dungeonwatcher	Betreff des Beitrags:	Mo 03.Dez, 2007 14:20

[quote="oxpus";p="79664"]

Zitat:

Das nun wieder nicht, aber rein aus Prinzip und Protest gg. die aktuelle Politik ala Schäuble und Co.

Sehr blauäugig gedacht, denn der Gesetzgeber würde sich sicherlich auch hier etwas einfallen lassen
Wenn es denn soweit ist dann fällt auch den Gegnern was neues ein.

[quote="oxpus";p="79664"]

Zitat:

Nicht wirklich. Auch im Forum direkt kann man ja gut mit den jeweiligen Rechten arbeiten und "verstecken". Es geht mir echt nur um das "ausschnüffeln" auf der Leitung und da ist SSL momentan die beste Möglichkeit.

Zumindest nach dem, was bekannt ist.
Ich möchte nicht wissen, welche Methoden und Hintertüren existieren, um den Strom live mitlesen zu können und das mit dem jeweils gültigen Schlüssel.
Das dürfte bei Open Source SW (OpenSSL) ziemlich schnell auffallen, erst recht bei einem solch sensiblem Thema.

Zitat:

Merke: Wenn jemand das ernsthaft will und "ganz oben" sitzt, bekommt er auch, was er will.
Da nützt dann auch SSL überhaupt nichts mehr, sondern nur noch "Stecker ziehen"

Da stimmt zwar, nur muss ich es ihm doch nicht so leicht wie möglich machen.

Bleibt also nur die Frage: Warum gibt es SSL überhaupt, wenn es keinerlei Sinn macht/hat es einzusetzen?

Autor	Nachricht	
oxpus	Betreff des Beitrags:	Mo 03.Dez, 2007 14:29

> Zitat:
> Wenn es denn soweit ist dann fällt auch den Gegnern was neues ein

Davon ist auszugehen.

> Zitat:
> Das dürfte bei Open Source SW (OpenSSL) ziemlich schnell auffallen, erst recht bei einem solch sensiblem Thema.

Sitzen die auch beim Provider, bzw. beim Gesetzgeber?
Eher nicht...

> Zitat:
> Da stimmt zwar, nur muss ich es ihm doch nicht so leicht wie möglich machen.

Noch mal: Wer dem Provider vorschreiben kann, alle Schlüssel und Inhalte zur Verfügung zu stellen, der liest in Echtzeit mit und leider ist der Gesetzgeber jederzeit dazu in der Lage ☹

> Zitat:
> Bleibt also nur die Frage: Warum gibt es SSL überhaupt, wenn es keinerlei Sinn macht/hat es einzusetzen?

Sinn macht das schon, wenn man an alle "anderen" Unbefugten denkt, die keinen Provider anzapfen können, sondern lediglich den Datenstrom ohne zunächst passenden Schlüssel mitschneiden.
Für alle diese "Mitleser" ist SSL gedacht. Für alle, die mehr "Macht" haben, und das ist nun einmal Mr. Schäuble mit seinen Mannen, nutzt SSL nicht wirklich was...

Aber die Diskussion sollte hier besser abgebrochen werden, denn sie führt zu keine Lösung und ist nur philosophisch.
Fakt ist, daß der Umbau am Forum für SSL ja/nein enorm ist und daher dem Sinn nicht gerechtfertigt ist. Zumal dann Verbindungen ohne SSL auch wieder zugängliche Teile des Boards zum Mitlesen "einladen"...