$# AciD-WarZ #$
^^^^^^^^^^^^^^^^^^^
Found At :: ACIDBURN_EG@Hotmail.Com
^^^

:SSL (Secure Sockets Layer)
==========

:INTRODUCTION TO SSL
==========

طبعا اكيد فى يوم و انت تتصفح الانترنت و اتصلت بأى موقع عن طريق الصدفه فأنك تلاحظ ما يسمى بال PADLOCK ICON و هى عباره عن ايقونه موجوده فى الشريط فى اسفل متصفحك و هى تكون عباره عن علامه تعجب ! صفراء او علامه X حمراء و لها اشكال اخرى كثيره تختلف حسب متصفحك
و الان سؤالنا هو ماذا تعنى هذه العلامه؟
و الاجابه ان هذه العلامه تعنى ان هذا الويب محمى ب ssl اى طبقه امنيه و كما هو ظاهر فى العنوان ان ال ssl هى ال (Secure Sockets Layer) و هى تشير الى بروتوكول او تيكنيك معين يؤكد الاتصال الامن بالويب سيت و تفعل هذا بطريقتين . الاولى:هى ان ال SSL توفر طرق عديده للتعرف على هويه المتصل بالويب سيت و طبعا لانه من الدورى معرفه هويه المتصل بالويب سيت قبل بدايه تبادل المعلومات بينهم :) و تكون ال SSL مطلوبه جدا ا ب ال digital certificates و سنعرف ما هى . و الطريقه الثانيه هى :انها تحول المعلومات الى UNREADABLE FORMAT اى الى صيغه لا تستطيع قرائتها اى تشفرها عند انتقالها خلال شبكه غير امنه مثل الانترنت .
اذن نرجع نقول تعريف بسيط عن ال SSL لتسهيل الفهم :
هى نظام أمني يسمح للتطبيقات بتشفير البيانات التي تنتقل من المتصفح الى وحدة الخدمة المقابلة
و سوف نتكلم عن اشياء كثيره فى هذا الدرس عن ال SSL فسوف نتكلم عن قوه حمايه هذا البروتوكول و سوف نتحدث ايضا عن عن كيفيه عملها و لماذا تكون صلاح للدفاع ضد الهاكرز و كيف تساعد الهاكرز فى بعض الاحيان ايضا
و الان قد ذكرت كلمه اعتقد ان البعض لم يفهمها جيدا و هى كلمه Digital Certificates و سنقوم الان بالتفسير لمعناها.

: Digital Certificates
==========

لكى تفهم ال SSL جيدا يجب اولا ان تفهم ال Digital Certificates و هو عباره عن ميكانزم او بروتوكول يستطيع تحديد اى شئ او التعرف عليه بوضوح تام مثل شخص او ويب سرفر فى نظام متكامل و واسع مثل الانترنت . و نحن نسمى الانترنت نظام مفتوح و واسع لاننا لا نملك السيطره و المعرفه بالاشخاص الذين يستخدمون هذا النظام. ال Digital Certificates هذا يحتوى على المعلومات الذى تحدد هويه المستخدم للنظام و يؤمن الاتصال بين

المستخدم و النظام ايضا كما قلنا بالتعرف الكامل على هويته.
و يمتلك هذا ال Digital Certificates ثلاث جهات عاليه و هم الحكومات و البنوك و و الشركات الكبرى .و يحتوى ال Digital Certificates على ما يسمى ب ال public encryption key لحامل هذا ال Digital Certificates سواء كان بنك او شركه ...الخ.

و لنعطى مثل للتوضيح:
و لنفرض ان بنك من البنوك يريد نقل معلومات بنكيه مهمه بأستخدام ال encryption و طبعا الان عرفنا معنى هذه الكلمه و معناها تشفير :) و طبعا هذه التشفير يجب ان يكون له مفاتيح و هذه المفاتيح هى ما يسمى ب الpublic encryption key .اعتقد الان فهمنا ما هى مفاتيح التشفير الذى يتضمنها ال Digital Certificates . و طبعا يجب وجود هذه المفاتيح حيث ان الانتقال عبر الانترنت غير امن و لذلك توجد هذه المفاتيح لكى تؤمن وصول المعلومات دون تسرب و دون معرفه الجهه الاخرى التى تصل اليها المعلومات.
و بالتالى فتجتاز ال SSL هذا المانع اى تسرب المعلومات عن طريق استخدام ال Digital Certificates و على فكره الترجمه الحرفيه لهذه الكلمه هى "شهادات رقميه" و لكن من الافضل ان تتعامل معها على انها نظام عالمى للتعرف على الهويات و التشفير و يستخدم عن طريق ال SSL.
و طبعا فقد فهمنا الان ان ال Digital Certificates يحتوى ايضا على مفاتيح التشفير التى تستخدم عند الحاجه لفك التشفير عن المعلومات.
عندما نستخدم ال SSL لتشفير اصال ب ويب سرفر معين فيكفى ان يكون السرفر وحده لديه ال certificate.و يمكن للمستخدمين تعريف انفسهم للويب عن طريق اليوزر نيمز و ال PIN CODES او الباسوردس و كما نرى ان ال SSL V3 الان تستطيع اعطاء الصلاحيه للمستخدم بتعريف نفسه بأستخدام ال Digital Certificates اى نظام التشفير :).و هذا التعريف يسمى ب ' client side authentication' اى توثيق جانب المستخدم و هذا طبعا يزيد من امن الموقع .

:The Value of Server Certificates of Authentication
==========

استخدام ال DIGITAL CERTIFICATES يسمح لل SSL بتقديم ال authentication للمستخدم اى بتقديم التوثيق او الثقه بمعنى انها تعطى الوعد بأن السرفر الذى يتصل به اليوزر هو فعلا السرفر الذى يريده اليوزر. و هذه طبعا تعتبر نقطه هامه جدا بالنسبه لليوزر خاصه اذا كان سيقوم بأستعمال معلومات شخصيه مهمه مثل الكريدت كارد نمبر الخاص به او ال PIN CODE لشئ ما مهم بالنسبه له.
و لكن كيف حدث ان السرفر الذى يتصل به اليوزر هو ليس السرفر الذى يطلبه ؟

العمليه تعتبر سهله فى الانترنت. ففى الانترنت نعرف ان الويب سرفرس تكون معروفه ب الIP نمبر الخاص بكل سرفر و بالنسبه للIP فتعريفه هو انه رقم فريد من نوعه يسمى UNIQUE 32-BIT NUMBER و صعب جدا ا على الانسان تذكره او حفظ كميه كبيره منه. ال DNS اى ال Domain Name System و ميكانزمات اخرى كثيره تتحكم فى تنظيم و تحويل الIP الى اسماء سهله يستطيع الانسان تذكرها مثل 'www.internetbanking.com' . ارجو من الاخوه مراجعه موضوعى الاول عن ال DNS لمعرفه القصه بالتفصيل.
و الان عندما يكتب يوزر عنوان مثل هذا 'www.internetbanking.com' فى متصفحه و يضغط انتر تحصل عمليه معقده لايجاد هذا السرفر او الموقع المطلوب "راجعو الموضوع الاول لمعرفه العمليه" و لكن يوجد جزء كبير من هذه العمليه يكون دائما ما بعد تحكم اليوزر و الويب ادمنستراتور و تكون العمليه لها قابليه للهجوم عليها من عده نقاط.بمعنى ادق انه عندما يطلب اليوزر موقع مثل هذا 'www.internetbanking.com' اى موقع بنك اذن فهو معرض لان يكون متصل بسرفر يتحكم فيه مهاجم او هاكر و ليس البنك نفسه.
بمعنى اكثر توضيحا:
تخيل معى لو ان هاكر صمم ويب مماثل تماما دون ادنى اختلاف اى تعتبر نسخه مطابقه الى موقع هذا البنك فسوف يستعملون اليوزرس طبعا ارقام الكردت كارد و ال PIN CODES الخاصه بهم فى الموقع و بعد الكتابه و الضغط على زر انتر لتنفيذ اى عمليه مثل تحويل مبلغ معين مثلا كل ما يظهر على الشاشه هو there was a technical problem with the site and "please try again later". اى ان هناك مشكله فى السرفر و حاول مره اخرى . و فى نفس هذه اللحظه يكون الهاكر قد بدء بأستخدام الرقم المكتسب الجديد لسرقه بعض الاموال من الموقع الحقيقى فى راحه تامه دون اى ازعاج من البوليس :) هل رأيتم كيف تكون الانترنت خبيثه و ذكيه :). و هناك الكثير مما يمكن التحدث عنه و عن انواع مثل هذه الاختراقات و لكننا سنتركه الان و لنركز فى الموضوع الاصلى :).
و دور ال SSL هنا هى انها تحاول تخطى هذه المشكله او تحاول الوصول الى السرفر الحقيقى المطلوب عن طريق تخزين ال DNS داخل ال digital certificate و بذلك فيقوم بالتعرف عليه بوضوح تام و بشكل صحيح.فعندما يتصل يوزر بموقع يستخدم ال SSL فيقدم السرفر الشهاده بأن هذا العنوان موجود فى ال DNS الفلانى فيقارن المتصفح العنوان للموقع الذى تريده بما تحتويه الشهاده او ال certificate. و لذلك فسيكون اليوزر متأكدمن صحه الموقع و السرفر المتصل بهم و اذا بالموقع فيه اى عطل فسيخبر اليوزر عن طريق ال POP-UP WINDOW و سيكون اليوزر متأكد من ان هذا السرفر فعلا لديه شهاده صحيحه.
و الان تخيل معنا ثانيا لو انه حصل نوع من المهاجمه مثل الذى دكرناه فى الاعلى و هو ان يكوم هاكر بتصميم نسخه طبق الاصل من موقع البنك. للمعرفه طبعا ان الهاكر لا يعرف اى طريقه لسهله ليخدع بها ال SSL authentication mechanism اى ميكانزم توثيق

او ثقه ال SSL و لذلك يترك الهاكر ال SSL جانبا دون ان يضعها فى التصميم لموقعه المطابق للبنك و و لذلك فأن موقع الهاكر لا يكون لديه شهاده من ال digital certificate ليكون هو الموقع الذى يطلبه اليوزر لان موقع البنك الاصلى طبعا يستخدم ال SSL و لديه شهاده ثقه على انه هو فعلا موقع البنك .و يمكن الفارق الوحيد الذى ستراه بين الموقعين هى الايقونه الصغيره التى تكلمنا عنها فى الجزء الاول من الموضوع و هى التى توضح ان هذا الموقع محمى بواسطه ال SSL و لذلك فيكون التفريق بين موقع الهاكر و الموقع الاصلى سهل جدا!. و بذلك فعلى اليوزر ان يمتنع عن استعمال معلوماته الشخصيه فى الموقع المزيف.
للتوضيح اكثر , ان ال SSL technology تقدم توثيق او ثقه مؤثره جدا! و لكن بعد كل هذا فنجد انه هناك عدد غير كاف من اليوزرس هم فقط المقتنعين اقتناع تام بأهميه وجود ال SSL فى المواقع و لذلك يجب علينا التطوير فى انفسنا و يجب علينا الانتباه لمثل هذه الاشياء الصغيره حتى نكون فى أمان تام.

اتمنى ان يكون الجزء الثانى من الموضوع نال اعجابكم هذا الجزء الذى وضحنا فيه قيمه ال SSL و قيمه التوثيق التى تعطيه للسرفر لكى يتأكد اليوزر انه فى أمان تام من امثل الهاكرز ;)

: SSL and Stored Data
==========
عند وضع مستخدم داتا خاصه به فى ويب سيت محمى ب SSL , ماذا تكون حاله هذه الداتا؟ بالطبع نعتبرها فى امان.
عند مثلا وضع يوزر للرقم الكريدت كارد الخاص به فى موقع ما محمى ب SSL هذه الداتا التى وضعها تتشفر و تنتقل فى أمان فى الانترنت الى الويب سرفر حيث يجب ان تعمل هذه الداتا. و ماذا يحدث بعد ذلك لهذه الداتا؟ تنتقل هذه الداتا اى الكريدت كارد نمبر الخاص باليوزر مع بعض الداتا الاخرى مثل مثل اليوزر نيم و معلومات اليوزر الشخصيه و تخزن فى داتا بيز او ترسل الى بعض المفاتيح الماليه للمعالجه الاخرى اى عمليه الشراء. و بعدها نعود و نسأل انفسنا هل هذه الداتا فى مكان امين؟ و من الذى يمكنه الاطلاع عليها فى المكان المخزنه فيه؟.
و بالرغم من ان السيت محمى ب SSL فهذا لا يعنى بالدروره ان الداتا التى وضعها اليوزر و التى تخزنت فى الموقع و الويب سرفر فى امان كامل . و لذلك فنحن نريد التوضيح بأن الSSL تحل جزء بسيط فقط مما يسمى e-commerce security problem اى مشكله امن الحركه التجاريه على الانترنت و تحلها عن طريق اعطاء المستخدم شهاده صحيحه بأن هذا هو الموقع الصحيح المطلوب لوضع الداتا الخاصه به فى امان.و لكن لا تحل مشكله مستوى الامن لمعلومات اليوزر نفسه المخزنه على السيت .
ارجو مراجعه الجزء الاول و الثانى للفهم :)

: The Value of SSLv3 and Client-Side Certificates

==========
مع تقديم ال فيرجان الثالث من ال SSL اى SSL V3 فى عام 96 فأنها تقدم دعم ل 'client-side certificates'. و هذه يعنى ان السرفر نفسه يمكن له ان يطلب يوزرز او يطلب الاجهزه التى تريد فعلا الاتصال بالسرفر لكى يعطيهم هم نفسهم شهاده الثقه الخاصه بهم اى their own digital certificates قبل ان تأخذ ال SSL مجراها فى العمل. و يسجل اليوزر بيم او الايميل الخاص باليوزر فى هذه الشهاده و يستخدمه السرفر فى مطابقته على معلومات اليوزر فى كل مره يدخل فيها الى الموقع حتى يتأكد من انه اليوزر الصحيح . و تذكر ان شهاده الزبون اى اليوزر موقعه ب Certificate Authority اى هيئه الشهادات لمقارنه معلومات اليوزر الحاليه بالمعلومات المسجله و التأكد من صحتها. و تطبيق توثيق الزبون بشكل صحيح يقدم للهاكر عقبه هائله امامه. و لكن هل يا ترى سيستسلم الهاكر لهذا؟ بالطبع لا لان المعروف عن الهاكرز هو عدم التراجع عن التحدى :)

: SSL and Vulnerability to Attacks
==========
استخدام الSSL على ويب سرفر ممكن يوحى للادمنستراتور الاحساس الخاطئ بالامان. بمعنى ان ويب سرفر يستخدم الSSL ممكن ان يهاجم من اى هاكر كأى سرفر أخر و يمكن ايضا يهاجم بنفس الطريقه التى تهاجم بها السرفرات التى لا تستعمل الSSL. و للاختصار :) التشفير و شهاده التوثيق اى الdigital certificate الذان هما المكونان الرئيسيان للSSL لا يمكن ان يحمو السرفر من الاختراق و لكن فقط يمكنهم حمايه المعلومات عند الانتقال من و الى السرفر نفسه. و سنعرف كيف :)

: Certification Weaknesses
==========
كما نلا حظ ان ال CAS العامه مثل الفيرجان غير معصومه.و من الاخطاء الشائعه بين الادمنستراتورز غالبا هى اعطاء الثقه الزياده ل CAS عام مثل فيرجان معين من برنامج معين.
فلو اعطى مثلا هذا الفيرجان شهاده تقول انى JOHN مثلا فسيقبل الادمينستراتور فورا انى JOHN. لسوء الحظ عندما تأتى لتوثيق يوزر تجد ان الهيئات التى تعتمد الشهادات العامه لا تهتم بمن يكون اليوزر مثل اهتمام الادمينستراتور.
مثلا:
فريق من الهاكرز و انا عضو فيه تحت اسم الادمنستراتور اذن الفرست نيم ادمنستراتور و الاسم الاخير تركته فارغ :) . الشى الاول الذى نفعله عندما يطلب منا سيت التوثيق هو تقديم شهاده الادمنستراتور و سيكون من الاحسن استخدام ال IIS اى (Internet Information Server, Microsoft's Web server that runs on Windows NT platforms) التى تحتوى على ميزه ' Client

'Certificate Mapping' التى تنظم و تؤكد الاسماء الموجوده فى الشهاده تحت نظام ال NT .

A Member Of :: D-StoRM-TeaM & $A-TeaM

==========

ممنوع منعا باتا نقل مواضيعى فى اى موقع الا بعد استشارتى

ACIDBURN_EG@HOTMAIL.COM

الماسنجر الجديد ::

Crying_FreeMan2@Hotmail.com

GreetZ::

$A-TeaM :: (AciD-WarZ , TweeTY , Jakal)

SADJackale , B-Hunter , BrokenArroW , KinG-Abdo , DJ-King ,

Egyption Fighter ,

USG-TeaM , ALL OF HACK 4 ARAB MEMBERS