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

السلام عليكم ورحمه الله و بركاته ::
ازيكم شباب ايه اخباركم كلكم ؟ اتمنى تكونوا بخيرو.
اعذرونى على غيبتى و انقطاعى عنكم و لكن و الله ظروف رهيبه :)
و الان خلونا نرغى فى شويه كلام فاضى على رأى بروكن ;)
كنت اتصفح الانترنت و ادعبث شوى :) و بعدين جمعت بعض من
المعلومات من ملفات مختلفه و هى تتحدث عن اليونى كود (طبعا الان
معظمكم سيستعجل و يقول ياه ه ه ه يونى كود قديمه ....الخ :)
) و لكن انا اقوله اصبر :) لقد ذكرت اليونى كود فى المنتديات
ثلاث مرات مره عن الصديق بلاك هنتر و مره من الاخ هكس و مره عن
الصديق ديمون او ابو خلود :) لكن هذه المره صدقونى ستكون مختلفه
تمام الاختلاف عن المرات السابقه :) (Trust Me)
و الان دعونا من ها الخرابيط و خلونا نقول الدرس يمكن يعجبكم::

==========

اولا:
====

متى وجدت اليونى كود؟
Found On 15 May 2001 BY NSFOCUS

السيستيمز التى تتأثر بالثغره هى ::
All running IIS 4 / IIS 5 web server
Windows 2k
Windows 2k SP1 + SP2

==========

ثغره اليونى كود ::هى عباره عن ثغره تسمح للهاكر بأن يشغل
اوامر بالقوه بصلاحيه مسموح بها (اى يكون له امتياز
IUSR_machinename account)

و تحدث هذه الثغره اصلا نتيجه ان روتين ال cgi الموجود على
الويب سرفر نفسه يفك شفره عنوان الموقع مرتين و هذا ما نسميه
بال DeCode (لا تقلق ستفهم بعد ذلك :))

تعالى معى خلينى اوضحلك ايه الخرابيط الى انا كاتبها فوق دى :)

و ليكن مثلا ::
http://IISserver/scripts/..%255c..%255cwinnt/system32/cmd
.exe?/c+dir+c ===> ثغره يونى كود

http://IISserver ====> سيكون هذا هو هدفنا اى الموقع المصاب
بالثغره المذكروه

* /scripts/ - و هذا الفولدر لديه امتيازات تنفيذيه على السرفر (اى يمكن لليوزر تنفيذ اى امر على الوب سرفر من خلاله) وهذا الفولدر ايضا هو المستخدم فى تنفيذ سكربتس ال cgi الموجوده على الوب سرفر و بالتحديد هذا الفولدر يسمى الفولدر التنفيذى اى executable directory)

و طبعا هذا الفولدر ليس له اسم ثابت هذا فقط مثال و لكن يمكن ان يكون له اسماء كثيره على الملقم iis و ملحوظه هامه:: لا يوجد على كل ملقم iis هذا الفولدرالتنفيذى اى executable directory

و اعتقد ان الصديق بلاك هنتر و الاخ هكس قد ذكرو معظم اسامى هذه الديريكتورز فى شرحهم (فأنا اريد ان اربط الدروس مع بعض حتى تكون سلسله متكامله)

* winnt/system32/cmd.exe ===> و طبعا هذا هو ال cmd الذى يسمح لنا بأدراج سطور الاوامر التى نريد تنفيذها (و على فكره ممكن تستعمل هذا ال cmd فى استخدام اوامر مثل ping و netstat و traceroute ....الخ ;) اعتقد انها فكره لم يلاحظها بعضنا :))

* ?- علامه الاستفهام :) تخيلو حتى علامه الاستفهام فى هذه الثغره لها دور فهذه العلامه تعنى الحاله التى ينفذ بها الامر (طبعا مش فاهم يعنى ايه :)) و لا يهمك تعالى معى افهمك يعنى ايه علامه الاستفهام تعنى كلمه argument و هذه الكلمه هى التى تعنى الحاله التى سينفذ بها الامر اى انه امر مثلا ينفذ فى لحظه ثم ينتهى مثل copy مثلا ام انه امر مثلا ينفذ و لكن يستمر مفعوله و حقيقه ان طبعا معظم الاوامر التى نستخدمها هى الاوامر العاديه و هى من نوع argument /c و هذا ال /c يعنى ان الامر ينفذ فى لحظه ثم ينتهى :)
تعالى افهمك اكثر :: لو عندك ويندوز 2000 افتح ال cmd بتاعك و اكتب هذا (cmd /?) و اضغط انتر ,سيظهر لك كلام كثير جدا و لكنى اخترت منه جزء بسيط فقط للتوضيح و انت عليك الباقى :)
شوف ايه الى راح يظهر لك ::

```
==========================================================
                                                ==========
Starts a new instance of the Windows 2000 command
interpreter

CMD [/A | /U] [/Q] [/D] [/E:ON | /E:OFF] [/F:ON | /F:OFF]
                                        [[/V:ON | /V:OFF
                                    [S] [/C | /K] string/]]
```

C Carries out the command specified by string and / then terminates
K Carries out the command specified by string but / remains
S Modifies the treatment of string after /C or /K / ((see below
Q Turns echo off/
D Disable execution of AutoRun commands from / (registry (see below

==========

هذا جزء بسيط جدا مما راح يظهر لك و لكن تعالى نشوف هذا الجزء ايه معناه اولا يقولك ::

Starts a new instance of the Windows 2000 command interpreter و هذه الجمله تعنى بالعربيه بدايه حاله جديده من مترجم ال ويندوز 2000 و هذا طبعا وضح لنا ان كل cmd يمكن ان يتخكم صاحبه فى حالته حسب ما يفتح او يغلق الarguments . و بعدها يظهر لنا arguments كثيره و منها الذى نستعمله دائما فى الثغره و هو /c شوفو كده ما المكتوب امامه ::

Carries out the command specified by string and then terminates و هذا الكلام معناه انه ينفذ الامر الموجود فى سطر الاوامر ثم ينتهى و طبعا هذا للاوامر العاديه التى نعرفها تعالو نشوف السطر الى تحتيه ::سوف نجد انه يتكلم عن argument لا نراه فى ثغره اليونى كود و هو ال /k شوفو ايه مكتوب امامه::

Carries out the command specified by string but remains و طبعا معناه انه ينفذ الاوامر الموجوده فى السطر و لكن يستمر مفعولها (ما زلت ابحث عن اوامر مثل هذه و لكن هذا ما هو مكتوب امامى :) و لكن تقدر تقول انها الاوامر التى تأخذ فتره طويله حبتين مثل ping مثلا)

و مثلا هناك argument أخر مثل /Q و هذا نستخدمه فى اغلاق تفعيل امر echo كما هو واضح فى المثال فوق

و هناك الكثير من هذه ال arguments و طبعا منها ما هو اساسى لا يمكنك التحكم فيه (يعنى فتحه او غلقه مثل ال /c و ال /k) و هناك اخرين يمكنك ان تجعلهم on او off و بهذا تكون انت تتحكم بحاله ال cmd خاصتك (ياريت تنفذ الامر و تقرأ المكتوب لانك راح تلاقى تفاصيل الفتح و الغلق بالتفصيل) و اصبروا على قليلا حتى انتهى من الامتحان الاول فى MCSE فى خلال اسبوعين ان شاء الله تعالى و بعد ذلك نعود اكثر قوه و نشرح لكم هذه النقطه بالتفصيل ان شاء الله :) بس اصبرو شوى :)

اعتقد انك الان فهمت ما هى ال arguments و ما فائده /c التى تكتبها فى الثغره و انا متأكد انك لا تعرف معناها :)

تعالو نروح لنقطه سهله و بسيطه جداا ا فى الثغره ,انت تشغل ال cmd.exe لانك تريد ان تتحكم بالموقع و تغير الاندكس و الخ و و لكن تعالى مثلا نشغل اى ملف تانى ياترى كيف نشغله :)؟
انا راح اقلك كيف ::كل ما عليك فعله هو ان تقوم بوضع اسم الفايل الذى تريد تشغيله بهذا الشكل Ping.exe+PRINT بلا من cmd.exe?/c و بهذا تكون قد شغلت الفايل الذى تريده :)
(enjoy this) .حيث تصبح الثغره بهذا الشكل ::
http://issserver/scripts/..%255c..%255cwinnt/system32/ping.exe+PRINT

* /c+ - و بالتالى كما عرفنا فوق انا /c هى ال argument للcmd.exe او الحاله التى سينفذ عليها ال cmd الامر اما علامه ال + التى بجانب ال /c فهى بمقام المسافه بين الكلمتين فى الثغره و لكن لا يمكننا اسبدالها بمسافه عاديه و بعدها يكون الامر الذى يحمله سطر الاوامر لينفده ثم علامه + ثانيه و بعدها اسم الدرايف الذى تعرض محتوياته على الشاشه حاليا .

**و نأتى الان لاهم نقطه فى الثغره و هى اساسا سبب الثغره كما ذكرنا فى اول الكلام (هو ان سبب الثغره يكون حل شفره العنوان اكثر من مره)و هذا ما نطلق عليه الdecode و انا شخصيا افصل الديكودز على انه تحليل حتى نصل لابسط الحل كما فى الرياضيات يعنى simplyfiey اى تبسيط و فك المعادله تعالو خلينا نفهمكم هذا على الثغره نفسها ::

/..%255c255%..c هذا هو الديكود اى التحليل للاصل /..\..\
ولكن ما الذى نحاول ان نفعله بهذه التحليلات الغريبه ؟
فنحن بذلك نحاول ان نحسن و نلعب فى مسارات الديريكتورز و لكن للاسف لا يمكنك تغيير او اللعب فى الديريكتورز لان ال iis مزود بخاصيه عمل check على مثل هذه الديكودز و منعها من التنفيذ و هنا يقع اصل ثغره اليونى كود و هو التحليل لمرتين او لاكثر من مره فهمتم قصدى الان :) اى ان الiis مزود فعلا بخاصيه ال check على هذه الديكودز و لكن انت تضع الثغره و بها اكثر من تحليل واحد لنفس اسم الموقع و لذلك يقوم ال iis بوظيفته المعتاده و هى ال check و المنع على الديكود الاول و يظهر له ان كل شئ بخير و انه يسيطر على الموقف خخخخخخخ و لكن الحقسقه انه يعمل الcheck مره واحده فتكون النتيجه ان الديكود الثانى ينجح تماما فى محاوله اللعب فى الديريكتورز و بالتالى يكون نتيجه الديكود الثانى هو ان يرجع الى اصله اى / (slash)

و تعالو ندخل و نتعمق اكثر فى تفاصيل الديكود للثغره بعد ان عرفنا فكرتها ::
شوفو فيه ماده اسمها computer logic و الماده دى راح درس فيها شئ يسمى HexaDecimal Values و هذه ال values هى اساس الديكود الذى نفعله فى الثغره اى ان كل حرف صحيح او حركه مثل

/ فى الكمبيوتر لها ما يسمى بال hex value تعالى اوضحلك اكثر ::
مثلا: %20 تعنى مسافه (space)
هذا مثال بسيط و اعتقد انك فهمت الان كلامى و طبعا يوجد جدول لهذه ال hex values المساويه للحروف و الحركات العاديه فى الكمبيوتر , اذن اعتقد انك ادركت تماما الان انك ترسل hex values عوضا عن الحروف و الحركات العاديه الى السرفر و هذا بالضبط ما نسميه التحليل او فك الشفره او الdecode :)

تعالى نخش فى تفاصيل الثغره اكثر و سنأخذ الحركه التى نشرح عليها هى ال / (slash) حيث انها من اساسيات الديكود فى هذه الثغره ::
شوف فى جدول ال hex value راح نجد ان ال / = %c5 , طبعا هذا هو الديكود الاول الذى ستفكر الان فى انك تحذف ال / و تضع بدلا منها هذا الvalue فتنجح الثغره و لكن انا اقول لك هذا خطأ لان هذا هو الديقود الاول و انا ذكرت ان الديكود يحدث مرتين او ممكن اكثر يعنى لو وضعت هذا الديكود الاول فستجد ان ال iis لديه القدره على ان يمسك هذا الديكود و يمكنعه من التنفيذ و لذلك علينا ان نحلل هذا ال value حتى يتم الديكود التانى فتنجح الثغره :)

و بالنظر الى جدول ال hexadecimal values شوف نجد هذا ::
% = %25
5 = %35
c = %63

و بالتالى نجد انفسنا قد خدعنا ال iis checker بأننا حللنا ال شفره مرتين و بالتالى فسنحصل فى المقابل على الاصل و هو / و بالتالى تكون قد نجحت الثغره .

فهمتم الان شباب معنى ديكود العنوان مرتين و فهمتم اساس الثغره و الديكود مرتين ليس معناه تكرار التحليل الاول مرتين و لكن معناه تحليل و فك التحليل الاول اى simplify الى ابسط و اطول صوره ممكنه فى نفس الوقت :)

و عشان توضح اكثر معك راح احطلك كيف التركيبه الصح للتحليل ::

%255c	%25 = %	%35 = 5 c	= c = %5c
%%35c	% = %	%35 = 5 c	= c = %5c
%%35%63	% = %	%35 = 5 %63	= c = %5c
%25%35%63	%25 = %	%35 = 5 %63	= c = %5c

ثم : %c5 =/

ارائيتم التحليل طبعا فى الاخر يجب ان يساوى الديكود الاصل و هو كما واضح فى مثالنا كل التحليلات تساوى c5% و كما ذكرنا c5% = / و لكننا حللنا هذا الرمز الى اطول و ابسط تحليل حتى نخدع ال iis checker .

و فى النهايه بعد فهمنا للثغره و اساسها هيا تعالو نطبقها مع بعض :) :)

سوف نضع الثغره فى هذا الشكل ::
http://IISserver/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\+/s

و ستدخلون على الموقع بنجاح و لكن اكيد تلاحظون شئ جديد قد زاد على الثغره و هذا الشى هو +/s
هذا الرمز :)
و عندما تدمج هذا الرمز مع الثغره كما فى المثال السابق سوف تأتيك لسته بكل فايل كبير و صغير فى كمبيوتر الويب سرفر

و الان ادعكم تطبقون دروس الاخ هكس و بلاك و ابو خلود

و الله تعبت فى هذا الدرس و تعبت فى قرائه المعلومات و تجميعها عن اليونى كود حتى اصل لهذا الشكل و ياريت الاخوه يوضحو طريقه مفصله و كامله لعمل كراش للسفر حتى نكون نحن العرب غطينا هذه الثغره من الاف الى الياء لانى و الله ما فاضى اكتب عن الطريقه شباب معلش و ان شاء الله انتظرو موضوعى القادم بعدما اكون انهيت امتحانى الاول فى MCSE (ادعولى بالنجاح) و سيكون عباره عن تلخيص للتعامل مع شبكات ويندوز 2000 و كيفيه اختراقها و فائده ال WIN2000 RESOURCE KIT

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

==========

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