

Introduction :

في الدرس السابق تعلمنا كيفية فك ضغط ASPack 2.12 . حسنا درس اليوم لن يختلف كثير فنفس الطريقة تنطبق على PEcompact لكن حيث أن الطريقة هي نفسها التي طبقت في الدرس الماضي دون أي تغيير ، لذا قررت أن أضيف شيئا جديدا كي لا يكون هذا الدرس مجرد تكرار ليس أكثر، فأضفت كيفية ضغط WinUpack و كيفية كتابة script تقوم بإيجاد ال OEP أوتوماتيكيا.

PEcompact 2.X

كالعادة ، أرفقت برنامج PEcompact كي تقوم بضغط ما تشاء من برامج للتدريب على الدرس...لاحظ أن النسخة المرفقة هي trial تعمل لـ 7 أيام...
بداية افتح الملف المسمى asm1 باستخدام PEiD :

PECompact 2.x -> Jeremy Collake

والآن افتحه باستخدام olly العزيز :

00401000	5	B8 505C4000	MOV EAX,asm_1.00405C50	
00401005	.	50	PUSH EAX	
00401006	.	64:FF35 0000	PUSH DWORD PTR FS:[0]	اللكو
0040100D	.	64:8925 0000	MOV DWORD PTR FS:[0],ESP	
00401014	.	33C0	XOR EAX,EAX	
00401016	.	8908	MOV DWORD PTR DS:[EAX],ECX	
00401018	.	50	PUSH EAX	

كما ترى هناك تعليمة PUSH EAX ...هل تذكر الدرس الماضي حينما فككنا ضغط ASPack ؟ حينها كان هناك تعليمة PUSHAD وقلت لك أننا نتوقع وجود تعليمة POPAD في النهاية...
حسنا الفكرة هنا نفس الشيء تقريبا...في أول البرنامج يتم حفظ قيمة EAX إذا في آخره سيقوم ال packer باستعادة هذه القيمة...إذن؟ إذن سوف نضع (HWBP) Hardware Brake Point على قيمة EAX و من ثم نشغل البرنامج وفي النهاية سنصل الى نهاية كود ال packer ونصل الى بداية كود البرنامج أي الى ال OEP...

إذن اضغط F8 مرتين...ها نحن هنا :

00401000	5	B8 505C4000	MOV EAX,asm_1.00405C50	
00401005	.	50	PUSH EAX	
00401006	.	64:FF35 0000	PUSH DWORD PTR FS:[0]	اللكو
0040100D	.	64:8925 0000	MOV DWORD PTR FS:[0],ESP	
00401014	.	33C0	XOR EAX,EAX	
00401016	.	8908	MOV DWORD PTR DS:[EAX],ECX	
00401018	.	50	PUSH EAX	

والآن ألق نظرة على قسم المسجلات :

```

EAX 00405C50
ECX 0012FFB0
EDX 7C90EB94
EBX 7FFDF000
ESP 0012FFC0
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C910738
EIP 00401006

```

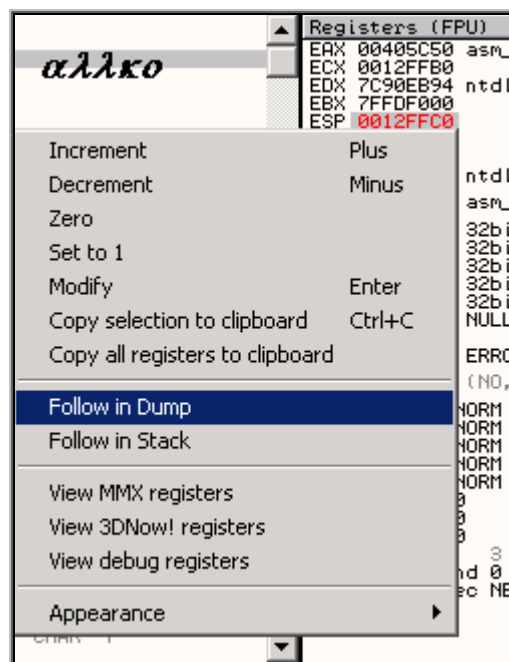
كما ترى فان قيمة EAX هي 00405C50 والآن دعنا نرى هذه القيمة في المكس :

```

0012FFC0 00405C50
0012FFC4 7C816D4F
0012FFC8 7C910738
0012FFCC FFFFFFFF
0012FFD0 7FFDF000
0012FFD4 8054B038
0012FFD8 0012FFC8

```

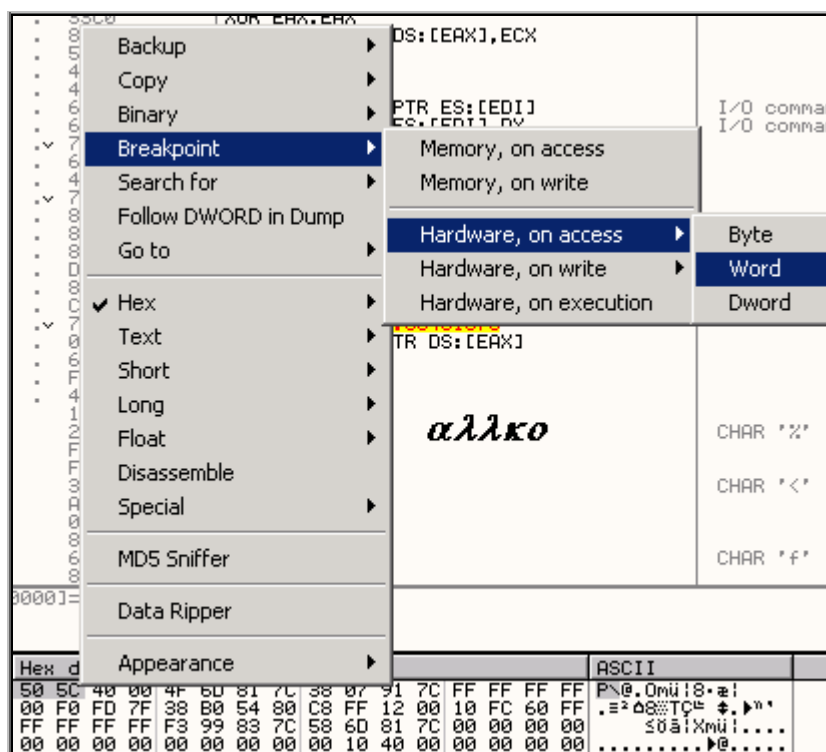
كما ترى فان قيمة EAX تم تخزينها في ال stack عند العنوان 012FFC0 . إذن ما نريده هو الذهاب الى هناك ووضع نقطة التوقف...ببساطة في قسم المسجلات اضغط على قيمة ESP باليسار لتحديدها...والآن اضغط باليمين واختر : follow in dump



ستلاحظ أن قسم ال Dumped Data (أسفل يسار الشاشة) قد أصبح بالشكل التالي :

Address	Hex dump	ASCII
0012FFC0	50 5C 40 00 4F 6D 81 7C 38 07 91 7C FF FF FF FF	P\@.0mü!8.æ!
0012FFD0	00 F0 FD 7F 38 B0 54 80 C8 FF 12 00 10 FC 60 FF	.==Δ@TC±.►™'
0012FFE0	FF FF FF FF F3 99 83 7C 58 6D 81 7C 00 00 00 00	...sôä!Xmü!....
0012FFF0	00 00 00 00 00 00 00 00 00 10 40 00 00 00 00 00	►@.....

كما ترى فقد وضعت مستطيلا أحمر حول قيمة EAX . والآن حدد أول بايتين من القيمة ثم اضغط باليمين و قم بعمل HWBP كما بالصورة :



حسننا الآن اضغط F9 ...ها نحن هنا :

00401000	50 5C 40 00 4F 6D 81 7C 38 07 91 7C FF FF FF FF	MOV EAX,asm_1.00405C50
00401005	FD 7F 38 80 54 80 C8 FF 12 00 10 FC 60 FF	PUSH EAX
00401006	64:FF35 0000	PUSH DWORD PTR FS:[0]
0040100D	64:8925 0000	MOV DWORD PTR FS:[0],ESP
00401014	33C0	XOR EAX,EAX
00401016	8908	MOV DWORD PTR DS:[EAX],ECX
00401018	50	PUSH EAX
00401019	45	INC EBP
0040101A	43	INC EBX

والآن ان حاولت الاستمرار والضغط على F9 فلن تنجح محاولتك ولن يستجيب Olly...لماذا؟ أنظر في الأسفل :

Access violation when writing to [00000000] - use Shift+F7/F8/F9 to pass exception to program

كما ترى هناك exception... ببساطة هي عبارة عن أخطاء تحدث أثناء تشغيل البرنامج...غالبا فإن المبرمج يكون قد توقع وقوع مثل هذه الأخطاء ووضع كود لتصحيحها (تسمى هذه العملية بـ Exceptions Handling) . لن نخوض في التفاصيل البرمجية ، ببساطة اضغط Shift + F7 . سنجد نفسك هنا :

7C90EAF0	8B1C24	MOV EBX,DWORD PTR SS:[ESP]
7C90EAF3	51	PUSH ECX
7C90EAF4	53	PUSH EBX
7C90EAF5	E8 C78C0200	CALL ntdll.7C9377C1
7C90EAF6	0AC0	OR AL,AL
7C90EAF7	74 0C	JE SHORT ntdll.7C90EB0A
7C90EAF8	5B	POP EBX
7C90EAF9	59	POP ECX
7C90EAB0	6A 00	PUSH 0

اضغط F9 :

7C937826	. 3B45 F8	CMP EAX,DWORD PTR SS:[EBP-8]	
7C937829	. 72 09	JB SHORT ntdll.7C937834	
7C93782B	. 3B45 F4	CMP EAX,DWORD PTR SS:[EBP-C]	
7C93782E	. 0F82 F731FFFF	JB ntdll.7C92AA2B	
7C937834	. 50	PUSH EAX	αλλκο
7C937835	. E8 67000000	CALL ntdll.7C9378A1	
7C937838	. 84C0	TEST AL,AL	

F9 مرة أخرى :

7C937849	. 0F85 20720100	JNZ ntdll.7C94EA6F	
7C93784F	. FF73 04	PUSH DWORD PTR DS:[EBX+4]	
7C937852	. 8D45 EC	LEA EAX,DWORD PTR SS:[EBP-14]	
7C937855	. 50	PUSH EAX	
7C937856	. FF75 0C	PUSH DWORD PTR SS:[EBP+C]	αλλκο

أعرف أنك مللت لكن اضغط F9 مرة أخرى (:

00405C83	53	PUSH EBX	
00405C84	51	PUSH ECX	
00405C85	57	PUSH EDI	αλλκο
00405C86	56	PUSH ESI	

الآن F9 للمرة الأخيرة

00405D12	- FFE0	JMP EAX	
00405D14	0010	ADD BYTE PTR DS:[EAX],DL	
00405D16	40	INC EAX	
00405D17	0000	ADD BYTE PTR DS:[EAX],AL	αλλκο

ما رأيك بالضغط على F7 ثم CTRL+A ؟

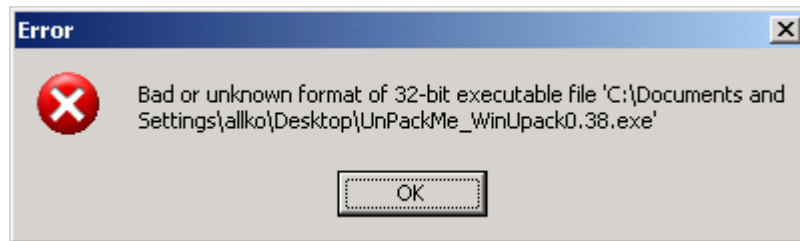
00401000	. 6A 00	PUSH 0	
00401002	. E8 7D010000	CALL asm.1.00401184	[pModule = NULL GetModuleHandleA
00401007	. A3 A0304000	MOV DWORD PTR DS:[4030A0],EAX	
0040100C	. 6A 00	PUSH 0	
0040100E	. 68 29104000	PUSH asm.1.00401029	[lParam = NULL DlgProc = asm.1.004

ها هي ال OEP...والآن أعتقد أنك تعرف بقية الخطوات...أعمل dump ثم افتح ImpREC وأصلح ال IAT كالمعتاد.

MUNing WinUpack

هذا ال packer أصبح من الماضي ، فمبرمجه قد أوقف تطويره...آخر نسخة هي 0.39...مع ذلك لا مانع من معرفة كيفية الضغط لأن الطريقة قد تفيد مع أنواع أخرى...

قمت بإرفاق البرنامج مع الدرس ، لكن لم أستطع ضغط أي ملف باستخدامه ، فكلما ضغطت ملفا وجدت أنه يبقى بنفس الحجم ، إضافة الى أنه عند فحص الملف الناتج بـ PEiD تظهر رسالة خطأ...حاول تغيير الإعدادات فقد أكون أنا المخطئ وليس البرنامج...
حسنا بعد فتح الملف باستخدام Olly ستجد هذه الرسالة:



لا بأس وافق كي تصل الى هنا :

7C901231	03	RETN	
7C901232	8BFF	MOV EDI,EDI	
7C901234	90	NOP	
7C901235	90	NOP	
7C901236	90	NOP	
7C901237	90	NOP	

αλλκο

كما ترى فهذا لا يبدو وكأنه المكان الصحيح للتوقف...يبدوا أن خطأ ما قد حدث...ما العمل؟ نريد أن نصل الى ال entry point لل packer's stub ، حتى نبدأ بفك الضغط من هناك كالمعتاد...أما ونحن هنا فلا يوجد ما نفعله !!
اذن اضغط على زر M الذي تجده بالأعلى...أو من قائمة view اختر memory ليظهر لك التالي :

Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
00010000	00001000				Priv	Rw	Rw	
00020000	00001000				Priv	Rw	Rw	
00012000	00001000				Priv	Rw	Gua: Rw	
00012E00	00002000				Priv	Rw	Gua: Rw	
00013000	00003000				Map	R	R	
00014000	00003000				Priv	Rw	Rw	
00024000	00006000				Priv	Rw	Rw	
00025000	00003000				Map	Rw	Rw	
00026000	00016000				Map	R	R	
00028000	00003000				Map	R	R	
0002C000	000041000				Map	R	R	
00031000	00006000				Map	R	R	
00040000	0000A3000	UnPackMe		PE header	Imag	R	RwE	
7C800000	00001000	kernel32		PE header	Imag	R	RwE	
7C801000	00002000	kernel32	.text	code,import	Imag	R	RwE	
7C803000	00005000	kernel32	.data	data	Imag	R	RwE	
7C808000	00006000	kernel32	.rsrc	resources	Imag	R	RwE	
7C8EE000	00006000	kernel32	.reloc	relocations	Imag	R	RwE	
7C900000	00001000	ntdll		PE header	Imag	R	RwE	
7C901000	00007B000	ntdll	.text	code,export	Imag	R	RwE	
7C907C000	00005000	ntdll	.data	data	Imag	R	RwE	
7C9081000	00002C000	ntdll	.rsrc	resources	Imag	R	RwE	
7C9AD000	00003000	ntdll	.reloc	relocations	Imag	R	RwE	
7F6F0000	00007000				Map	R E	R E	
7FFB0000	00024000				Map	R	R	
7FFD6000	00001000				Priv	Rw	Rw	
7FFDF000	00001000				Priv	Rw	Rw	
7FFE0000	00001000				Priv	R	R	

αλλκο

والآن هل ترى PE header ؟ اضغط باليسار عليها...والآن اضغط باليمين واختر Dump لتظهر لك النافذة التالية:

00400000	4D 5A	ASCII "MZ"	DOS EXE Signature
00400002	4B45	DW 454B	DOS_PartPag = 454B (17739.)
00400004	524E	DW 4E52	DOS_PageCnt = 4E52 (20050.)
00400006	454C	DW 4C45	DOS_ReloCnt = 4C45 (19525.)
00400008	3332	DW 3233	DOS_HdrSize = 3233 (12851.)
0040000A	2E44	DW 442E	DOS_MinMem = 442E (17454.)
0040000C	4C4C	DW 4C4C	DOS_MaxMem = 4C4C (19532.)
0040000E	0000	DW 0000	DOS_ReloSS = 0
00400010	5045	DW 4550	DOS_ExeSP = 4550
00400012	0000	DW 0000	DOS_ChkSum = 0
00400014	4C01	DW 014C	DOS_ExeIP = 14C
00400016	0300	DW 0003	DOS_ReloCS = 3
00400018	BEB0	DW 00BE	DOS_Tabloff = 00BE
0040001A	1140	DW 4011	DOS_Overlay = 4011
0040001C	00AD50FF	DD FF50AD00	PointerToSymbolTable = FF50AD00
00400020	7634EB7C	DD 7CEB3476	NumberOfSymbols = 7CEB3476 (2095789174.)
00400022	4801	DW 0148	SizeOfOptionalHeader = 148 (328.)
00400024	0F01	DW 010F	Characteristics = EXECUTABLE_IMAGE 32BIT
00400026	0B01	DW 010B	MagicNumber = PE32
00400028	4C	DB 4C	MajorLinkerVersion = 4C (76.)
0040002A	6F	DB 6F	MinorLinkerVersion = 6F (111.)
0040002C	61644C69	DD 694C6461	SizeOfCode = 694C6461 (1766614113.)
0040002E	62726172	DD 72617262	SizeOfInitializedData = 72617262 (1918980.)
00400030	79410000	DD 00004179	SizeOfUninitializedData = 4179 (16761.)
00400032	18100000	DD 00001018	AddressOfEntryPoint = 1018
00400034	10000000	DD 00000010	Offset to PE signature

هل ترى ما هو محاط بالدائرة ؟ هذا هو ال RVA ، اذن أغلق النافذتين والآن اضغط على زر :

7C901231	L	C3	RETN
7C901232		8BFF	MOV EDI,EDI
7C901234		90	NOP
7C901235		90	NOP

واكتب ال VA حيث $VA = \text{Image Base} + \text{RVA} = 400000 + 1018 = 401018$ (يمكنك معرفة ال image base باستخدام LordPE)

00401018	BE B0114000	MOV ESI,UnPackMe.004011B0
0040101D	AD	LODS DWORD PTR DS:[ESI]
0040101E	50	PUSH EAX
0040101F	FF76 34	PUSH DWORD PTR DS:[ESI+34]
00401022	EB 7C	JMP SHORT UnPackMe.004010A0

هل ترى PUSH EAX ؟ إذن أعتقد أنك تعرف كيف تكمل !!!

SCRIPTING :

يقصد بال script مجموعة من التعليمات البرمجية لتنفيذ أوامر معينة...طبعا لغة البرمجة المستخدمة هي لغة شبيهة بال assembly في الواقع الأمر يحتاج الى معرفة أساسيات الاسمبلي فقط ولا حاجة لأي خبرات برمجية. وبلا شك ، فيجب أن يكون لديك ال plug in المسماة Olly Script . تجدها بالمرفقات بأية حال... هناك العديد من التعليمات المستخدمة وبالطبع لا مجال للحديث عنها جميعا...لذلك سأشرح التعليمات الأكثر أهمية فقط ، أما بقية التعليمات فتجد شرحا لها في الملف المرفق باسم script

VAR

يقوم بتعريف متغير ما...يجب تعريف المتغير قبل استخدامه

مثال

var x

ADD ,SUB ,INC ,DEC ,MOV ,AND ,OR ,XOR ,SHL ,SHR ,CMP

جميع هذه التعليمات تستخدم كما لو كانت أوامر اسمبلي تماما

STO

تقوم بتنفيذ عملية Step over أي F8

STI

تقوم بتنفيذ عملية Step into أي F7

RUN

تقوم بتشغيل البرنامج أي F9

ESTI

تحاكي الضغط على Shift + F7

DBH

تستخدم لإخفاء الديبجر (DeBugger Hide)

BP

تستخدم لوضع نقطة توقف عند عنوان ما.

مثال:

bp 401000

bp x

bp eip

BC

كالسابقة لكن تقوم بإزالة نقطة التوقف عند العنوان المذكور.

BPHWS

تقوم بوضع نقطة توقف hardware

مثال:

bphws 401000, "x"

هذا يقوم بوضع نقطة توقف hardware من نوع execution عند العنوان المذكور

bphws 401000, "r"

هذا يقوم بوضع نقطة توقف hardware من نوع read(access) عند العنوان المذكور

bphws 401000, "w"

هذا يقوم بوضع نقطة توقف hardware من نوع write عند العنوان المذكور

BPHWC

تقوم بإزالة نقطة التوقف من العنوان المذكور

مثال : bphwc 401000

AN

تقوم بتحليل الكود وتحاكي CTRL+A

MSG

تستخدم لإظهار message box

مثال:

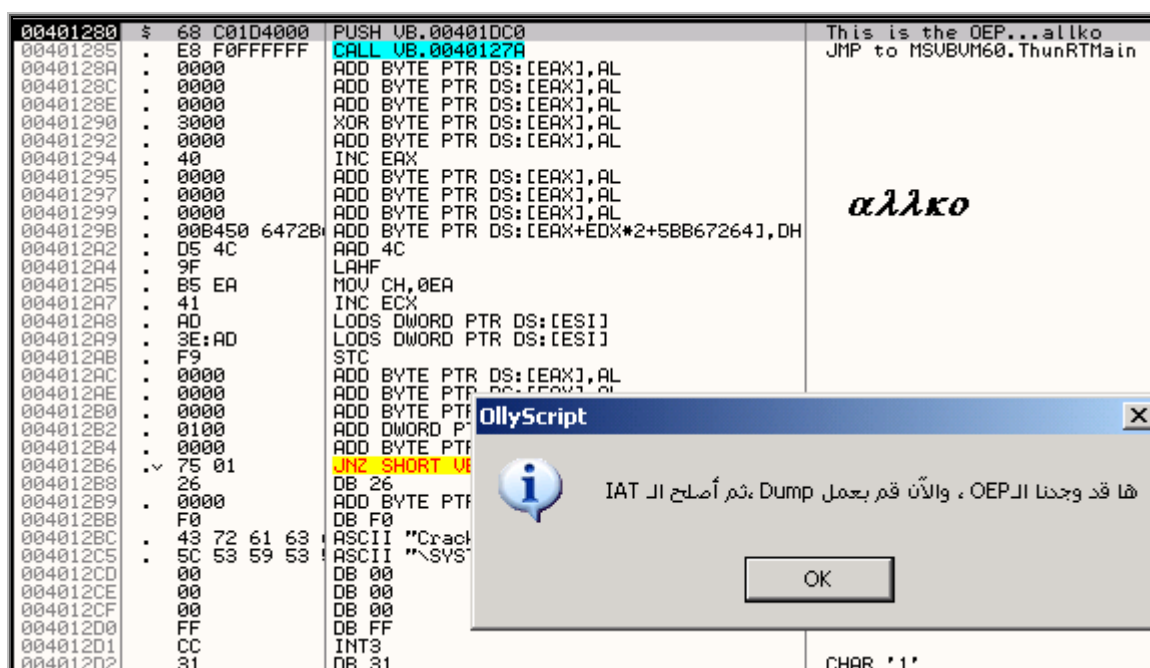
" msg "allko

RET

تستخدم للخروج من السكريبت

طبعاً هذه التعليمات تقوم بكتابتها في النوتباد...ستجد بالمرفقات السكريت التي قمت بكتابتها ، الملف اسمه PEcompact 2.X OEP finder . افتحه وتمعنه جيداً...أعتقد أن كل شيء واضح...ما سيفعله هذا السكريت هو: تنفيذ F7 مرتين ، ثم وضع نقطة توقف هاردوير من نوع on Read عند العنوان الموجود في esp ، ثم F9 ثلاث مرات ، ثم F7 ثم يقوم بتحليل الكود ثم يضع تعليق (comment) عند العنوان الموجود في eip (أي عند ال-OEP)، بعد ذلك يظهر message box وفي النهاية يخرج من السكريت.

سنقوم بتجربة السكريت...افتح أي ملف من المرفقات وليكن vb مثلاً...من قائمة Plug ins اختر Olly Scrip ثم اختر Run Script... اختر السكريت الذي أرفقته ثم موافق...ستلاحظ أن olly ينفذ الخطوات التي كنا ننفذها لكن بسرعة كبيرة...في النهاية ستجد التالي :



رائع أليس كذلك ؟

Do You Know ?

عمر بن عبد العزيز – رضي الله عنه - .

عمر بن عبد العزيز (680م -720م) سابع الخلفاء الأمويين، خامس الخلفاء الراشدين من حيث المنظور السني واسمه بالكامل عمر بن عبد العزيز بن مروان بن الحكم بن أبي العاص بن أمية، ويرجع نسبه من أمه الى عمر بن الخطاب حيث كانت أمه هي ليلي بنت عاصم بن عمر بن الخطاب وبذلك يصبح الخلفية عمر بن الخطاب جد الخلفية عمر بن عبد العزيز. اشتهرت خلافة عمر بن عبد العزيز بأنها الفترة التي عم العدل و الرخاء أرجاء الدولة الأموية حتى إن الرجل كان ليخرج الزكاة من أمواله فيبحث عن الفقراء فلا يجد من في حاجة إليها. كان عمر رحمه الله قد جمع جماعة من الفقهاء والعلماء وقال لهم: " إني قد دعوتكم لأمر هذه المظالم التي في أيدي أهل بيتي، فما ترون فيها؟ فقالوا: يا أمير المؤمنين: إن ذلك أمرًا كان في غير ولايتك، وإن وزر هذه المظالم على من غضبها " ، فلم يرتح عمر إلى قولهم وأخذ بقول جماعة آخرين منهم ابنه عبد الملك الذي قال له: أرى أن تردّها إلى أصحابها ما دمت قد عرفت أمرها، وإنك إن لم تفعل كنت شريكاً للذين أخذوها ظلماً. فاستراح عمر لهذا الرأي وقام يرد المظالم إلى أهلها. استمرت خلافته فترة قصيرة جداً، فلم تطل مدة خلافته سوى عامين ونصف ثم حضره أجله ولاقى ربه عادلاً في الرعية قائماً فيها بأمر الله تعالى.

Outroduction :

I hope you learned something new...writing olly scripts is not that hard as you saw. anyway it's just for fun :) .

as usual , suggestions ,criticisms ,etc are welcomed at www.alalame.net/vb forums.

Greetings :

DiDi
Dahaka
Dj-Siba
Sqr2002
Cold-Fever
E3 for his wonderful plug In : OllyScript
and all 'programming and protection' forums members

June 2006