



CAPTURE THE FLAG

Что такое CTF?

CTF (Capture the flag, Захват флага) — командные соревнования по компьютерной безопасности, в которых участники исследуют заранее заложенные уязвимости предоставленных сервисов, обеспечивают безопасность своих ресурсов и пытаются атаковать ресурсы противников, захватывая «флаги» скомпрометированных сервисов.

Варианты соревнований

- Attack-defense(classic)
- Loopardy(tool based)



Категории task-based CTF

- admin — задачи на администрирование, настройку сети
- joy — различные развлекательные задачи вроде коллективной фотографии или игры в какую-нибудь мини-игру
- ppc — задачи на программирование (professional programming and coding)

Reverse Engineering

The screenshot displays the IDA Pro interface for a debugger session. The main window shows assembly code for a function named `WinMain(x,x,x,x)+35`. The instruction at address `00431219` is highlighted: `jnz short loc_43124E`. The instruction pointer (EIP) is shown pointing to this instruction. The stack view (IDA View-ESP) shows the current stack frame, with the return address `retaddr` at `0012FF38` pointing to `43CC53h`. The general registers window shows the state of various registers, including `EAX` (00000001), `EBX` (7FFDF000), `ECX` (00000065), `EDX` (77FD0170), `ESI` (00000000), `EDI` (0012D9C4), `EBP` (0012FF34), `ESP` (0012FF34), `EIP` (00431219), and `EFL` (00000206).

Debugger: Library loaded: C:\WINNT\system32\NTDLL.DLL
Debugger: Library loaded: C:\WINNT\system32\ADVAPI32.dll
Debugger: Library loaded: C:\WINNT\system32\KERNEL32.DLL

ALU: idle Down Disk: 103GB 00031219 00431219: WinMain(x,x,x,x)+35

Threads: 00000350 (Line 1 of 1)

IDA View-EIP:

```
.text:00431207 call ds:InitCommonControls
.text:0043120D call sub_4300A1
.text:00431212 call sub_437607
.text:00431217 test eax, eax
.text:00431219 jnz short loc_43124E
.text:0043121B push ds:lpSt_eax=00000001
.text:00431221 push offset aSFatalError
.text:00431226 call sub_406B06
.text:0043122B pop ecx
.text:0043122C mov esi, eax
.text:0043122E pop ecx
.text:0043122F push 30h
.text:00431231 push esi
.text:00431232 push offset Text
.text:00431237 push 0
.text:00431239 call ds:MessageBoxA
.text:0043123F push esi
.text:00431240 call sub_406E7E
.text:00431245 pop ecx
.text:00431246 push 1
.text:00431248 pop eax
.text:00431249 jmp loc_43204E
.text:0043124E ;
.text:0043124E loc_43124E:
.text:0043124E mov eax, dword_45A1C4
```

IDA View-ESP:

```
EBP 0012FF30 var_4 dd 65h
ESP 0012FF34 dd 12FFC0h ; Stack[000000
0012FF38 retaddr dd 43CC53h ; sta
0012FF3C hInstance dd offset unk_400
0012FF40 hMenu dd 0
0012FF44 uIDEvent dd offset unk_132D
0012FF48 nCmdShow dd 0Ah
0012FF48 ; [END OF STACK FRAME_WinM
0012FF4C dd 12D9C4h ; Stack_PAGE_
0012FF50 dd 200h
0012FF54 dd 7FFDF000h
```

General registers:

EAX	00000001		CF	0
EBX	7FFDF000	debug013:7FFDF000	PF	1
ECX	00000065		AF	0
EDX	77FD0170	NTDLL.DLL:77FD0170	ZF	0
ESI	00000000		SF	0
EDI	0012D9C4	Stack_PAGE_GUARD[0000035	TF	0
EBP	0012FF34	Stack[00000350]:0012FF34	IF	1
ESP	0012FF34	Stack[00000350]:0012FF34	DF	0
EIP	00431219	WinMain(x,x,x,x)+35	OF	0
EFL	00000206			

Web

- SQL injection
- XSS
- CSRF
- Directory traversal

WEB SECURITY: SQL INJECTION

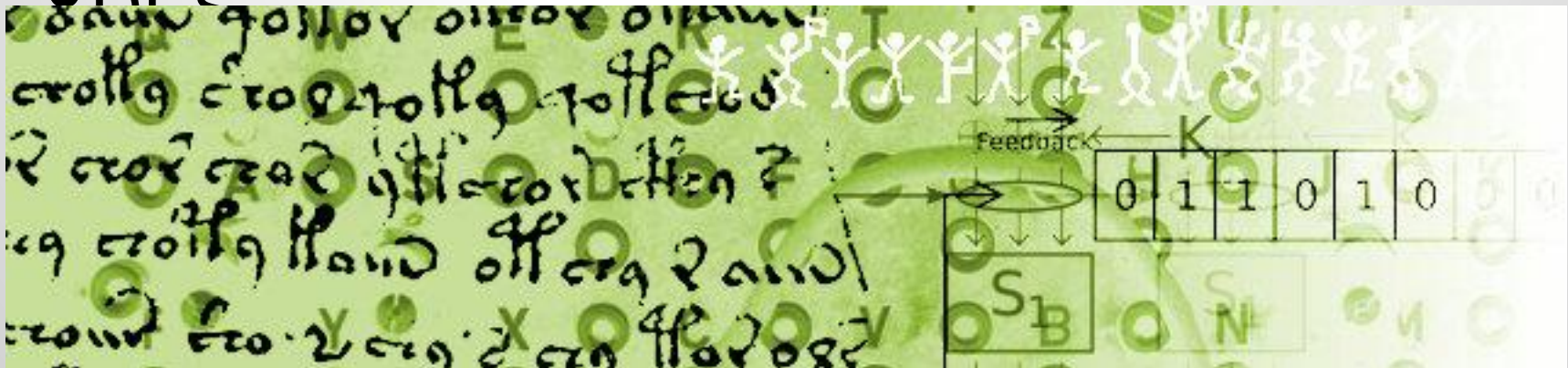


```
<?
if(is_numeric($_GET['show'])&&isset($_GET['ver'])){
    if($_GET['ver']==phpversion()){
        if(!is_numeric($_REQUEST['show'])&&is_numeric($_REQUEST['ver'])){
            die('Flag: FLAGISHERE');
        }
        die("<script>alert('Failed #2')</script>");
    }
    die("<script>alert('Failed #1')</script>");
}
die("<script>alert('Failed #0')</script>");
?>
```

Crypto

- AES
- RSA
- ГОСТ 28147-89

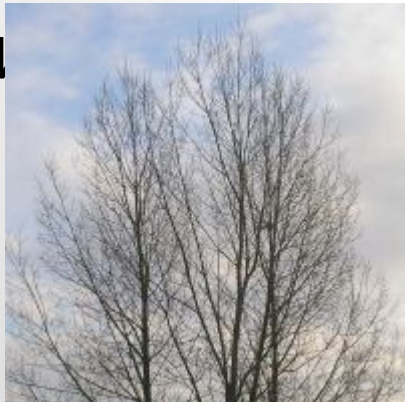
- DES



Steganography

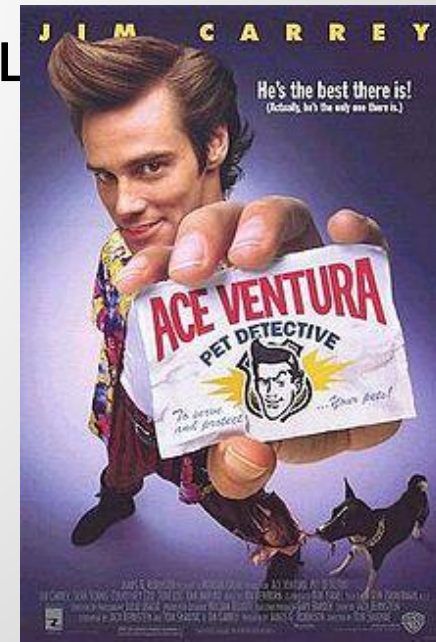
- Стеганография - это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи.
- Преимущество – сообщение не привлекает к себе внимания.

- Отличительная особенность – не привлекает к себе внимания кри...



Forensics

- Ответвление криминалистики, сочетающее в себе восстановление и расследование материалов, найденных на электронных носителях.
- Криминалистика – наука, исследующая закономерности приготовления, совершения и раскрытия преступлений.



Exploit

- **Эксплойт, эксплоит, спloit** (англ. *exploit*, эксплуатировать) — компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение её функционирования (DoS-атака).

Capture The Flag!

