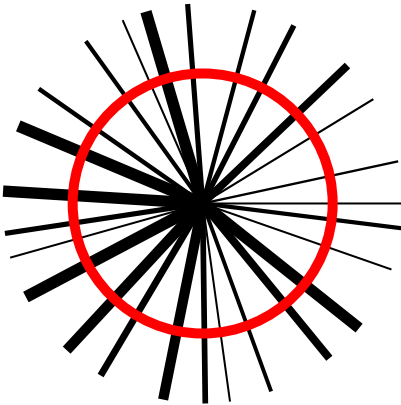


█	1000	fe010113	add sp,sp,-32	int main(void) {
█	1004	00112e23	sw ra,28(sp)	// 12(sp)
█	1008	00100793	li a5,1	int run = 1;
█	1012	00f12623	sw a5,12(sp)	do {
█	1016	???00793	li a5,🔪	// 8(sp)
█	1020	00f12423	sw a5,8(sp)	int choice = 98;
█	1024	00012783	lw a5,8(sp)	if (choice) {
█	1028	00070653	beqz a5,1040	exploit();
█	1032	04c000ef	jal 1108	} else {
█	1036	0000006f	j 1044	bug();
█	1040	c71ff0ef	jal 128	}
█	1044	00c12783	lw a5,12(sp)	} while(run);
█	1048	fe0790e3	bnez a5,1016	
█	1052	00000793	li a5,0	return 0;
█	1056	00070513	mv a0,a5	}
█	1060	01c12083	lw ra,28(sp)	
█	1064	02010113	add sp,sp,32	
█	1068	00000057	ret	
█	1072	00000000		
█	1076	00000000		
█	1080	00000000		
█	1084	00000000		
█	1088	00000000		
█	1092	00000000		
█	1096	00000000		
█	1100	00000000		
█	1104	00000000		
█	1108	fe010113	add sp,sp,-32	
█	1112	00112e23	sw ra,28(sp)	void exploit(void) {
█	1116	00c12783	lw a5,12(sp)	// 12(sp)
█	1120	00070853	beqz a5,1136	int should_set_trap;
█	1124	02c000ef	jal 1168	if (should_set_trap) {
█	1128	00012623	sw zero,12(sp)	set_trap();
█	1132	00c0006f	j 1144	should_set_trap = 0;
█	1136	c8dff0ef	jal 252	} else {
█	1140	c09ff0ef	jal 252	copy();
█	1144	00000013	nop	copy();
█	1148	01c12083	lw ra,28(sp)	}
█	1152	02010113	add sp,sp,32	}
█	1156	00000057	ret	void set_trap(void) {
█	1160	00000000		asm("li a4, 98");
█	1164	00000000		asm("csrc mtvec, a4");
█	1168	???00713	li a4,🔪	}
█	1172	30571073	csrc mtvec,a4	
█	1176	00000013	nop	
█	1180	00000057	ret	
█	1184	00000000		
█	1188	00000000		



PROJEKT: OVERFLOW
https://punkx.org/overflow
version: 0.0.5
license: CC BY 4.0
copyright: jackdoe 2023