

RP Advanced Canaries

99% is not good enough for you? At RP enterprises, we do the extra %1 to keep our customers satisfied until their mouth drops to the floor. We are not just banging rocks together here. We implement advanced canaries so prevent the hacker from guessing the canary's values.

We have 3 types of Canaries

1. **Random Seed Canary** – as described earlier in the document
2. **Terminal Canary** – the canary value is 0 to stop shellcode injection
3. **XOR Canary** – the seeded canary value is XOR'ed with its memory address. Since canary value is now execution dependent, and this provides an extra layer of security such that attacker cannot guess the value.

The 3 types of canaries can be randomly inserted at any time in the program. The seed is first terminated or XOR'ed, then the seed value is always increased by 9.

High Memory Address		Description
 V 100	Function Parameters	
	Return Address	
	Previous Frame Pointer	
	Canary1	1000
	Local Variables	
	...	
	Canary2	100 XOR 1000 (next seed is this plus 9)
	Local Variables	
Low Memory Address		