



Score Card

Microsoft Security Development Lifecycle



Name	Points	Card	Component(s)	Notes on Threat
	0	10		
	0	3 IO		
	1	J IO		
	1	4 IO	Between browsers	Possible threat if wifi
	0	5 IO		
	1+1	K S	Between Web page & admin	Spoofer poses as admin
		J S		
		Q S		
	1	9 S	A → WPA	Possible to reuse password when you have it
		10 S		
	1+1	K R	A → LS	No way to see changes being made
		3 R		
		4 R		
		10 R		
		2 R		
		6 DoS		
		9 DoS		
		K DoS		
		7 DoS		
	1	8 DoS		
		Q R	T → Web-page	Can't doing anything against that
		6 R		
		2 R		
		5 R		
		J R		
		5 DoS		
	1	Q DoS		
		K DoS		
		J DoS		
		4 DoS		

Score Card



Name	Points	Card	Component(s)	Notes on Threat
	1	13	V	Secure err msg in validation
		12	None	NA
		1J	None	None
	1	1K	None	None
		1 IO	None	None
		14	None	None
		D3	None	None
		D4	None	None
	1	KD	None	None
		D2	None	None
		D5	-11-	-11-
		D6	-11-	-11-
	1	1Q	-11-	-11-
		16	-11-	-11-
		19	-11-	-11-
	1	D9	V	If we get a corrupted image, might have
		107	-	-
		18	none	none
		D7	-11-	-11-
		Df	-11-	-11-
		D8	-11-	-11-
	1	D10	V	corrupted on large image as input
		15	-	-
	1	D10Q	none	none

Score Card

Microsoft Security Development Lifecycle



Name	Points	Card	Component(s)	Notes on Threat
	1	5T	Backend	Reply document
	1	6T	Config DB	Internal attacker
	1	3ID	Backend	Internal attacker
	0	4DoS	External	Not applicable because problem still persists after attacker stops
	1	3DoS	Frontend	Internal attacker
	1	7T		Not applicable
	0	10S		Spoofing doesn't matter
	1	4ID	Frontend	Does unencrypted in frontend
	1	8ID		Not applicable
	1	7ID	Frontend	Man-in-the-middle
	1	6ID	DBs	Database backups
	0	8EP		Not relevant