Evan Parton (eparto01)			COMP116				
11/19/2015			Technical Risk Analysis				
Risk ID	**Technical Risk**	**Techical Risk Indicators**	**Related CVE, CWE, or OSVDB IDs**	**Impact Rating**	**Impact**	**Mitigation**	**Validation Steps**
1	SQL Injection (covers ctf 5,6,7,8; and via sqlmapper, exposes all 1-12)	Any modification done to ANY data/file; repeated login attempts (esp. w/ single char. change => brute force)	CVE-2014-7137 (MANY related IDs, grouped by similarities)	H	Access allowed to ENTIRE filesystem, all databases, all files (via sqlmapper)	Sanitize input to text boxes to disallow commands	Run static analysis tool such as veracode to check all SQL usages
2	WordPress Vulnerabilities (covers 9,10,11)	Any modification to Word Press files	CVE-2015-7683 (MANY related IDs, grouped by similarities)	H	Access allowed to content directory	Use proper Word Press mechanisms to secure site	Consult Word Press documentation for best practices and security measures
3	Hiding Strings in gif/image (1)	Any amount of data (strings, keys, otherwise) stored and hidden in image files	N/A	L	Allows for hiding (potentially sensitive) data inside other files	Use media format that does not allow hiding; use checksums	Compare checksums for all known media to ensure no data hiding
4	FTP Anonymous login enabled (2)	Upon nmap scan or FTP login, anonymous login enabled clearly displayed	CVE-1999-0497	L	Could allow unauthenticated access to FTP server	Block FTP anonymous login	nmap / test FTP login
5	Social Engineering (hug Ming...) (4)	Communication with person that was breeched / engineered	N/A	H	Could allow access to keys to kingdom!, if done properly	Train employees to hide their secrets better	Test employees on social engineering training; 3rd party audit
6	Data/Media in PCAP file (3)	Anaylsis of file types in all data files	N/A	M	Allows for hiding of media or other data	Pattern match for different types of files embedded within other files	Static scan of all media files for containing unauthorized data