**MEMORANDUM**

**TO: WHITE TEAM**

**FROM: TEAM ##**

**SUBJECT:**

**INJECT #:**

**DATE & TIME:**

**Memo should not have any indentation. Preferably double spaces text in the paragraphs. Font size 11 for the body of the memo. Only title should be bolded.** Remember the following when it comes to injects:

* Injects are similar to business tasks you may receive in a corporate environment. The Blue Team should use the quickest, most efficient, and secure way of addressing the inject. Team Captains should be prepared to defend the team choices to the CEO.
* Points from injects can be the deciding factor as to whether a team wins or not.
* Decide which injects are most important and prioritize according to time, ability, and personnel available.
* Follow directions and procedures; this attention to detail will be rewarded.
* Avoid technical jargon when communicating with the CEO – he/she will not understand it.
* Write well in your reports and include a summary of important information. This will allow the CEO to can scan the document quickly and still understand 1) what you have accomplished, 2) what has not been accomplished, 3) the business impact of any inject tasks not completed; and 3) what you have planned to address what has yet to be completed.
* If completing the inject was influenced by a Red Team action, you should provide solutions that will minimize the impact of the Red Team’s action, or your service failure in the future.
* Stay calm even when the CEO is not
  + If you know that the CEO is asking for a policy change that will compromise the security of a system, or perhaps violate competition policies/rules, you need to educate him/her with concrete examples. You need to prove to the CEO, in non-technical terms, how his/her decision could be costly to the business; and why your solution is cost effective and worth the inconvenience.

If you suspect an incursion by the Red Team, please submit an Incident Report with as much detail as possible. Up to 50% of the points lost due to Red Team activity can be recouped through diligent, thorough, and complete reporting of known and suspected attacks. Please submit one report for each incident; be as detailed as possible.

Include the following information:

* \* date/time the attack started (if known) \* date/time the attack was discovered \* attacker source address \* target system name / address
* \* target port / service \* type of attack (virus, hacking, DoS, etc) \* result of attack \* vulnerability that allowed the attack \* how discovered \* how contained \* remediation actions / controls \* result of remediation