Logging needs to be enabled for \*X\* because using \*X\* malicious users can cause \*Y\* attack as reported by \*Z\* et al. (\*DOI of paper Z\*)

1. Logging needs to be enabled for \*data load-related methods\* because using \*data load-related methods\* malicious users can cause \*poisoning\* attack as reported by \*Papernot\* et al. (\*DOI: [https://doi.org/10.1109/EuroSP.2018.00035\*](https://doi.org/10.1109/EuroSP.2018.00035*))
2. Logging needs to be enabled for \*Training and Prediction\* because using \* Training and Prediction\* malicious users can cause \*Exploratory\* attack as reported by \*Papernot\* et al. (\*DOI: [https://doi.org/10.1109/EuroSP.2018.00035\*](https://doi.org/10.1109/EuroSP.2018.00035*))
3. Logging needs to be enabled for \*Model Parameters\* because using \*Model Parameters\* malicious users can cause \*Confidentiality\* attack as reported by \*Papernot\* et al. (\*DOI: [https://doi.org/10.1109/EuroSP.2018.00035\*](https://doi.org/10.1109/EuroSP.2018.00035*))
4. Logging needs to be enabled for \*Model Output\* because using \*Model Output\* malicious users can cause \*Integrity \* attack as reported by \*Papernot\* et al. (\*DOI: [https://doi.org/10.1109/EuroSP.2018.00035\*](https://doi.org/10.1109/EuroSP.2018.00035*))
5. Logging needs to be enabled for \*Model Input\* because using \*Model Input\* malicious users can cause \*Integrity\* attack as reported by \*Papernot\* et al. (\*DOI: [https://doi.org/10.1109/EuroSP.2018.00035\*](https://doi.org/10.1109/EuroSP.2018.00035*))
6. Logging needs to be enabled for \*Training Data\* because using \*Training Data\* malicious users can cause \*Integrity\* attack as reported by \*Papernot\* et al. (\*DOI: [https://doi.org/10.1109/EuroSP.2018.00035\*](https://doi.org/10.1109/EuroSP.2018.00035*))
7. Logging needs to be enabled for \*Model Output\* because using \*Model Output\* malicious users can cause \*Availability\* attack as reported by \*Papernot\* et al. (\*DOI: [https://doi.org/10.1109/EuroSP.2018.00035\*](https://doi.org/10.1109/EuroSP.2018.00035*))
8. Logging needs to be enabled for \*Model Input/Training Data\* because using \* Model Input/Training Data\* malicious users can cause \*Confidence Reduction\* attack as reported by \*Papernot\* et al. (\*DOI: [https://doi.org/10.1109/EuroSP.2018.00035\*](https://doi.org/10.1109/EuroSP.2018.00035*))
9. Logging needs to be enabled for \*Input Features\* because using \*Input Features\* malicious users can cause \*Denial of Service\* attack as reported by \*Papernot\* et al. (\*DOI: [https://doi.org/10.1109/EuroSP.2018.00035\*](https://doi.org/10.1109/EuroSP.2018.00035*))
10. Logging needs to be enabled for \*ML model queries\* because using \*ML model queries\* malicious users can cause \*Oracle\* attack as reported by \*Papernot\* et al. (\*DOI: [https://doi.org/10.1109/EuroSP.2018.00035\*](https://doi.org/10.1109/EuroSP.2018.00035*))
11. Logging needs to be enabled for \*Model Training\* because using \* Model Training\* malicious users can cause \*Model Substitution\* attack as reported by \*Papernot\* et al. (\*DOI: [https://doi.org/10.1109/EuroSP.2018.00035\*](https://doi.org/10.1109/EuroSP.2018.00035*))
12. Logging needs to be enabled for \*Training Data\* because using \* Training Data\* malicious users can cause \*Data Injection\* attack as reported by \*Papernot\* et al. (\*DOI: [https://doi.org/10.1109/EuroSP.2018.00035\*](https://doi.org/10.1109/EuroSP.2018.00035*))
13. Logging needs to be enabled for \* Training Data\* because using \* Training Data\* malicious users can cause \*Data Modification\* attack as reported by \*Papernot\* et al. (\*DOI: [https://doi.org/10.1109/EuroSP.2018.00035\*](https://doi.org/10.1109/EuroSP.2018.00035*))
14. Logging needs to be enabled for \*Environment in RL\* because using \* Environment in RL\* malicious users can cause \*Environment Modification\* attack as reported by \*Papernot\* et al. (\*DOI: [https://doi.org/10.1109/EuroSP.2018.00035\*](https://doi.org/10.1109/EuroSP.2018.00035*))
15. Logging needs to be enabled for \*Learning Algorithm\* because using \* Learning Algorithm\* malicious users can cause \*Logic Corruption\* attack as reported by \*Papernot\* et al. (\*DOI: [https://doi.org/10.1109/EuroSP.2018.00035\*](https://doi.org/10.1109/EuroSP.2018.00035*))
16. Logging needs to be enabled for \*Model Inputs/Feature Values\* because using \*Model Inputs/Feature Values\* malicious users can cause \*Source-Target Misclassification\* attack as reported by \*Papernot\* et al. (\*DOI: [https://doi.org/10.1109/EuroSP.2018.00035\*](https://doi.org/10.1109/EuroSP.2018.00035*))
17. Logging needs to be enabled for \*Data Pipelines\* because using \*Data pipelines\* malicious users can cause \*physical domain\* attack as reported by \*Papernot\* et al. (\*DOI: [https://doi.org/10.1109/EuroSP.2018.00035\*](https://doi.org/10.1109/EuroSP.2018.00035*))
18. Logging needs to be enabled for \* Model Prediction\* because using \* Model Prediction\* malicious users can cause \*Adversarial Example Transferability\* attack as reported by \*Papernot\* et al. (\*DOI: [https://doi.org/10.1109/EuroSP.2018.00035\*](https://doi.org/10.1109/EuroSP.2018.00035*))
19. Logging needs to be enabled for \*Model Training\* because using \*Model Training\* malicious users can cause \*Membership\* attack as reported by \*Papernot\* et al. (\*DOI: [https://doi.org/10.1109/EuroSP.2018.00035\*](https://doi.org/10.1109/EuroSP.2018.00035*))
20. Logging needs to be enabled for \*Model Prediction\* because using \*Model Prediction\* malicious users can cause \*Model Inversion\* attack as reported by \*Papernot\* et al. (\*DOI: [https://doi.org/10.1109/EuroSP.2018.00035\*](https://doi.org/10.1109/EuroSP.2018.00035*))
21. Logging needs to be enabled for \*Model Prediction\* because using \*Model Prediction\* malicious users can cause \*Model Extraction\* attack as reported by \*Papernot\* et al. (\*DOI: [https://doi.org/10.1109/EuroSP.2018.00035\*](https://doi.org/10.1109/EuroSP.2018.00035*))
22. Logging needs to be enabled for \*Model Training\* because using \* Model Training \* malicious users can cause \*Causative\* attack as reported by \*Barreno\* et al. (\*DOI: [https://doi.org/10.1145/1128817.1128824\*](https://doi.org/10.1145/1128817.1128824*))
23. Logging needs to be enabled for \*Feedback\* because using \*Feedback\* malicious users can cause \*Probing\* attack as reported by \*Barreno\* et al. (\*DOI: [https://doi.org/10.1145/1128817.1128824\*](https://doi.org/10.1145/1128817.1128824*))
24. Logging needs to be enabled for \*X\* because using \*X\* malicious users can cause \*Targeted\* attack as reported by \*Barreno\* et al. (\*DOI: [https://doi.org/10.1145/1128817.1128824\*](https://doi.org/10.1145/1128817.1128824*))
25. Logging needs to be enabled for \*X\* because using \*X\* malicious users can cause \*Indiscriminate\* attack as reported by \*Barreno\* et al. (\*DOI: [https://doi.org/10.1145/1128817.1128824\*](https://doi.org/10.1145/1128817.1128824*))
26. Logging needs to be enabled for \*X\* because using \*X\* malicious users can cause \*Backdoor\* attack as reported by \*Islam\* et al. (\*DOI: https://doi.org/10.1145/3377811.3380378 \*)
27. Logging needs to be enabled for \*Training/Model Architecture & Parameter\* because using \*Training/Model Architecture & Parameter\* malicious users can cause \*Inference\* attack as reported by \*Mireshghallah \* et al. (\*DOI: \*)
28. Logging needs to be enabled for \*Model Architecture\* because using \*Model Architecture\* malicious users can cause \*Neural-level Trojan\* attack as reported by \*Shafique\* et al. (\*DOI: <https://doi.org/10.1109/mdat.2020.2971217>\*)
29. Logging needs to be enabled for \*X\* because using \*X\* malicious users can cause \*Hardware\* attack as reported by \*Shafique\* et al. (\*DOI: <https://doi.org/10.1109/mdat.2020.2971217>\*)
30. Logging needs to be enabled for \*X\* because using \*X\* malicious users can cause \*Side-channel\* attack as reported by \*Shafique\* et al. (\*DOI: <https://doi.org/10.1109/mdat.2020.2971217>\*)
31. Logging needs to be enabled for \*Model\* because using \*Model\* malicious users can cause \*Model-stealing\* attack as reported by \*Shafique\* et al. (\*DOI: <https://doi.org/10.1109/mdat.2020.2971217>\*)
32. Logging needs to be enabled for \*Model\* because using \*Model\* malicious users can cause \*Data-stealing\* attack as reported by \*Shafique\* et al. (\*DOI: <https://doi.org/10.1109/mdat.2020.2971217>\*)

Evasion Attack