Cílem práce je prozkoumat zranitelnost hlubokých klasifikátorů obrazu v realistických scénářích. Prozkoumali jsme několik operací augmentací a navrhli kombinace vhodných metod útoků black-box a white-box. Výsledkem práce je implementovaný systém, který úspěšně napadá Google Cloud Vision API.