Find\_vuln6.py

Уязвимости

1) OS command injection

2) Debug-enabled

заключается в том, что при включённой отладке злоумышленник может отправить отладочные операторы в удалённые сценарии ASP. С их помощью он может изменить время выполнения удалённых сценариев и получить конфиденциальную информацию о веб-сервере и приложении ASP.NET

Find\_vuln7.js

**1)detect-child-process**

связана с модулем child\_process в Node.js, который позволяет напрямую выполнять команды оболочки. Если входные данные для этого модуля не санитизированы должным образом, это может привести к атакам внедрения команды (command injection). В результате злоумышленники могут ввести вредоносные команды, которые при исполнении скомпрометируют целостность системы или приведут к утечке данных.

Find-vuln8.php

1)tainted-exec

 возникает, когда для оценки динамического контента используется exec или eval. Это может быть опасно, если контент может быть введён извне программы. В таком случае возникает угроза инъекции кода.

2)exec-use