

???????????? ???? ???? ????
??

Инъекция команд ОС (shell инъекция) позволяет выполнять произвольные команды ОС на сервере, и обычно дает возможность полностью скомпрометировать приложение и все его данные. Возможно использовать также для компрометации других частей инфраструктуры, используя доверительные отношения для перенаправления атаки на другие системы в организации.

Обычно эксплуатация затруднена и требует поиска возможностей выполнения кода через другие уязвимости:

- Уязвимости небезопасной десериализации
- Уязвимости внедрения шаблонов на стороне сервера SSTI
- Уязвимости SQL инъекции
- Уязвимости переполнения буфера / кучи / стека
- Множественные случаи проблем и ошибок реализации, возникающих при работе с запуском процессов и работе с терминальной оболочкой

Здесь нужно понимать что искать.

Revision #1

Created 27 September 2025 17:34:20 by Admin

Updated 27 September 2025 17:47:55 by Admin