??????????

Способы атаки

- Как ведет приложение при запросах отсутствующих страниц?
- Список существующих endpoint (Фаззинг)
- Категории уязвимостей, которые возможно эксплуатировать в endpoint

Категории типовых уязвимостей
Типовые уязвимости по механизмам, где они происходят:

- Уязвимости механизмов аутентификации (Authentication Bypass)
- Уязвимости механизмов авторизации (Vulnerabilities of authorization)
- Уязвимости загрузки файлов (File upload vulnerabilities)
- Уязвимости раскрытия информации (Coordinated Vulnerability Disclosure)
- Уязвимости в системах криптографии (Vulnerabilities in cryptography systems) и др.

Типовые уязвимости по характеру их эксплуатации:

- Уязвимости состояния гонки (race condition)
- Уязвимости некорректной нейтрализации управляющих конструкций при генерации веб-страниц (атаки межсайтового скриптинга) (XSS)
- Уязвимости подделки запроса со стороны сервера (SSRF)
- Уязвимости подделки запроса со стороны клиента (CSRF) и др.

Типовые уязвимости по технологиям, в которых они происходят:

- Уязвимости SQL инъекций (SQL injection)
- Уязвимости внедрения внешних сущностей в XML-документы (XXE)
- Уязвимости инъекций в ORM-запросах (ORM injection)
- Уязвимости инъекций в LDAP-запросах (LDAP Injection)
- Уязвимости инъекции команд или аргументов в запросах к терминальной оболочке ОС (Command Injection)

Revision #11
Created 20 September 2025 13:05:48 by Admin
Updated 29 September 2025 15:37:37 by Admin