ОНЛАЙН-ОБРАЗОВАНИЕ

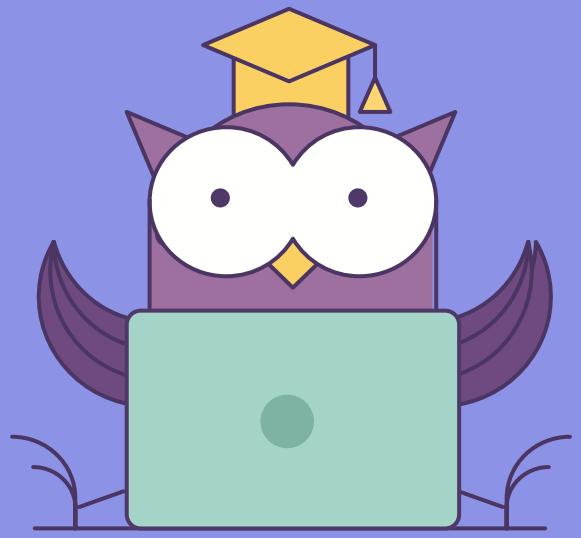
OTUS

Классификация уязвимостей веб-приложений.

Способы эксплуатации.

Колесников Александр Александрович

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

Содержание

- Классификации уязвимостей
  - CWE
  - OWASP
  - WASC
- Эксплуатация и поиск:
  - Command Injection
  - Server Misconfiguration
  - LFI

01

WASC

Классификация угроз или ничего не меняется уже 10 лет

- Open Source проект, который давно не обновляется
- Содержит в себе названия распространенных уязвимостей Web
- Достаточное подробное объяснение каждой их атак - главное отличие от других списков и классификаций.
- Есть как уязвимости так и реализации атак

Attacks	Weaknesses
Abuse of Functionality	Application Misconfiguration
Brute Force	Directory Indexing
Buffer Overflow	Improper Filesystem Permissions
Content Spoofing	Improper Input Handling
Credential/Session Prediction	Improper Output Handling
Cross-Site Scripting	Information Leakage
Cross-Site Request Forgery	Insecure Indexing
Denial of Service	Insufficient Anti-automation
Fingerprinting	Insufficient Authentication
Format String	Insufficient Authorization
HTTP Response Smuggling	Insufficient Password Recovery
HTTP Response Splitting	Insufficient Process Validation
HTTP Request Smuggling	Insufficient Session Expiration
HTTP Request Splitting	Insufficient Transport Layer Protection
Integer Overflows	Server Misconfiguration

01

CWE

- Список уязвимостей ранжированных по встречаемости in the wild
- Есть перечень примеров
- Обновляется, по отношению к другим спискам более оперативно (последнее обновление 2019 год)

01

OWASP

TOP 10

- Список уязвимостей, который формируется раз в несколько лет
- Имеет самый полный список подходов к тестированию приложений
- Единственный проект, который описывает не только веб, но и мобильные платформы

Тестирование сервисов

Колесников Александр

Спасибо
за внимание!