Лабораторная работа 1

Защита разработчика программного обеспечения

Панченко Денис 1132229056

Савурская Полина 1132222827

Кочарян Никита 1132221541

Норсоян Шушаник 1132221545

Сухальская Ксения 1132229052

Умярова Камилла 1132229051

Содержание

# 1. Цель работы

Злоумышленник решает предпринять атаку на инфраструктуру небольшой IT-компании, занимающейся веб-разработкой. Просканировав сеть организации, он обнаруживает уязвимость на веб-сайте компании. Закрепившись в системе, нарушитель атакует один из узлов внутренней инфраструктуры разработчика. Нужно защитить разработчика программного обеспечения.

# 2. Обнаружение атаки

Событие 1: Выполнение XXE-инъекции на узле Webmarket ([рис. 1](#fig-001)).

|  |
| --- |
| Рисунок 1: Событие 1 |

Событие 2: Обход аутентификации и выполнение удаленного кода в TeamCity ([рис. 2](#fig-002)).

|  |
| --- |
| Рисунок 2: Событие 2 |

Событие 3: Атака на песочницу NodeJS Sandbox ([рис. 3](#fig-003)).

|  |
| --- |
| Рисунок 3: Событие 3 |

# 3. Выполнение лабораторной работы

## 3.1 Уязвимость XML Injection и последствие Webmarket PHP backdoor

Обнаруживаем вредоносную сессию ([рис. 4](#fig-004)).

|  |
| --- |
| Рисунок 4: Сканирование файловой системы |

|  |
| --- |
| Рисунок 5: Сканирование файловой системы |

|  |
| --- |
| Рисунок 6: Сканирование файловой системы |

Изменяем исполняемы файл ([рис. 7](#fig-007)).

|  |
| --- |
| Рисунок 7: Изменение файла |

|  |
| --- |
| Рисунок 8: изменения файла |

Удаляем вредоносный файл ([рис. 9](#fig-009)).

|  |
| --- |
| Рисунок 9: Удаление вредоносного файла |

Завершаем вредоносную сессию ([рис. 10](#fig-010)).

|  |
| --- |
| Рисунок 10: Завершение вредоносной сессии |

Удаляем вредоносный исполняемый файл ([рис. 11](#fig-011)).

|  |
| --- |
| Рисунок 11: Удаление вредоносного файла |

Уязвимость устранена ([рис. 12](#fig-012)).

|  |
| --- |
| Рисунок 12: Устранение уязвимости |

## 3.2 Уязвимость TeamCity RCE и последствие TeamCity DB Deleter

На TeamCity совершена атака ([рис. 13](#fig-013)).

|  |
| --- |
| Рисунок 13: Атака на TeamCity |

Восстанавливаем TeamCity из резервной копии ([рис. 14](#fig-014)).

|  |
| --- |
| Рисунок 14: Восстанавление |

Перезапускаем TeamCity ([рис. 15](#fig-015)).

|  |
| --- |
| Рисунок 15: Перезапуск |

Входим в TeamCity ([рис. 16](#fig-016)).

|  |
| --- |
| Рисунок 16: Авторизация |

Устанавливаем плагин для устранения уязвимости ([рис. 17](#fig-017)).

|  |
| --- |
| Рисунок 17: Загрузка плагина |

|  |
| --- |
| Рисунок 18: Загрузка плагина |

Уязвимость устранена ([рис. 19](#fig-019)).

|  |
| --- |
| Рисунок 19: Устранение уязвимости |

## 3.3 Уязвимость JS Sandbox escape и последствие Node DOS

Сканируем файлы ([рис. 20](#fig-020)).

|  |
| --- |
| Рисунок 20: Сканирование файлов |

|  |
| --- |
| Рисунок 21: Сканирование файлов |

Редактируем исполняемый файл ([рис. 22](#fig-022)).

|  |
| --- |
| Рисунок 22: Редактирование файла |

|  |
| --- |
| Рисунок 23: Редактирование файла |

Редактируем следующий исполняемый файл ([рис. 24](#fig-024)).

|  |
| --- |
| Рисунок 24: Редактирование файла |

|  |
| --- |
| Рисунок 25: Редактирование файла |

|  |
| --- |
| Рисунок 26: Редактирование файла |

Завершаем вредоносную сессию ([рис. 27](#fig-027)).

|  |
| --- |
| Рисунок 27: Завершение вредоносной сессии |

Удаляем вредоносный файл ([рис. 28](#fig-028)).

|  |
| --- |
| Рисунок 28: Удаление вредоносного файла |

Уязвимость устранена ([рис. 29](#fig-029)).

|  |
| --- |
| Рисунок 29: Устранение уязвимости |

# 4. Выводы

В результате выполнения работы мы успешно устранили все уязвимости и их последствия: Webmarket XML Injection → Webmarket PHP backdoor; TeamCity RCE → TeamCity DB Deleter; JS Sandbox escape → Node DOS.