**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ»**

**Факультет безопасности информационных технологий**

**Дисциплина:**

**«*Теория информационной безопасности и методология защиты информации*»**

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №1**

**“**Исследование баз данных угроз и уязвимостей. Калькулятор уязвимостей**”**

**Выполнил:**

Студент гр. P32141

*Полуянов Александр Михайлович*

**Проверила:**

*Коржук Виктория Михайловна*

Санкт-Петербург

2023 г.

**Цель работы:**

получить знания и навыки работы с различными базами данных угроз и уязвимостей. Работа индивидуальная.  
  
**Объекты:**

1. Обязательный материал для ознакомления:
   1. <https://habr.com/ru/company/pt/blog/266485/>
   2. <https://habr.com/ru/company/ic-dv/blog/453756/>
   3. [https://xakep.ru/2009/05/15/48221/#toc01.](https://xakep.ru/2009/05/15/48221/#toc01)
   4. <https://habr.com/ru/company/xakep/blog/305262/>
2. БД угроз и уязвимостей (описываем 5 БД и прикладываем пару скриншотов):
   1. ФСТЭК
   2. Vulners
   3. CVE (NVD)
   4. cert/cc
   5. secunia
   6. exploit in
   7. X-Force
   8. SecurityFocus
   9. CNNVD
   10. JVN
   11. https://www.exploit-db.com
3. Калькулятор CVSS. Метрики. Выбрать один вариант задачи из каждого блока метрик (задачи а / задачи б и т.д.) и посчитать. (Задачи ниже в текущем документе)

# **Ход работы:**

БД угроз и уязвимостей:

1. **ФСТЭК**

Аббревиатура расшифровывается как Федеральная служба по техническому и экспортному контролю. Это крупнейшая и наиболее значимая база уязвимостей на русском языке.Банк угроз ФСТЭК содержит, помимо названия и кода угрозы, её краткое описание, вероятные источники, объекты воздействия и, конечно, последствия, которые повлечёт за собой реализация угрозы.

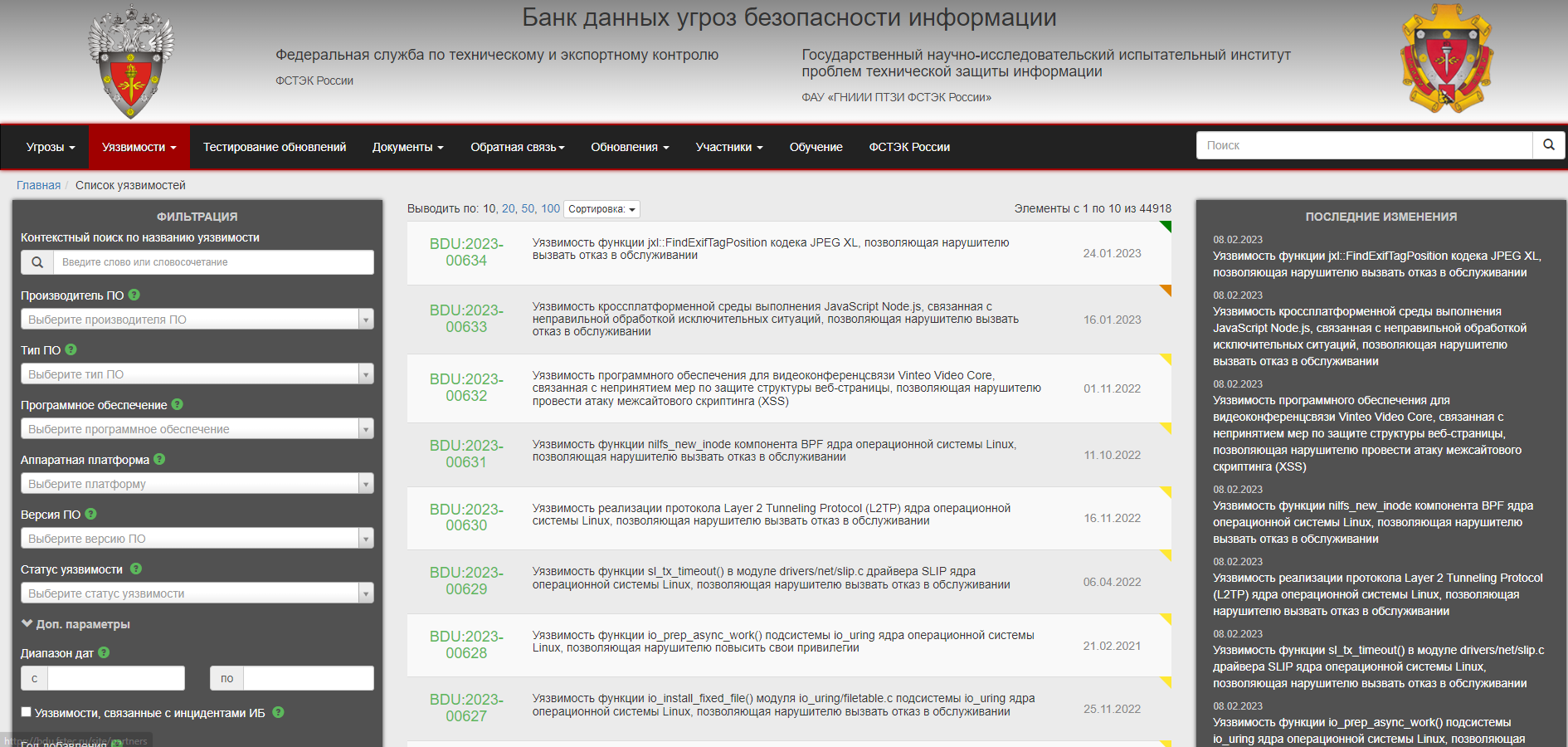


Рисунок 1 - Список уязвимостей по данным ФСТЭК

1. **Vulners**

Vulners — это очень большая и непрерывно обновляемая база данных ИБ-контента. Сайт позволяет искать уязвимости, эксплоиты, патчи, результаты bug bounty так же, как обычный поисковик ищет сайты. Vulners агрегирует и представляет в удобном виде шесть основных типов данных: популярные базы уязвимостей, вендорские бюллетени безопасности, эксплоиты из Exploit-DB и Metasploit, Nessus-плагины для детекта уязвимостей, дисклозы багов с сайтов bug bounty программ, публикации на тематических ресурсах.

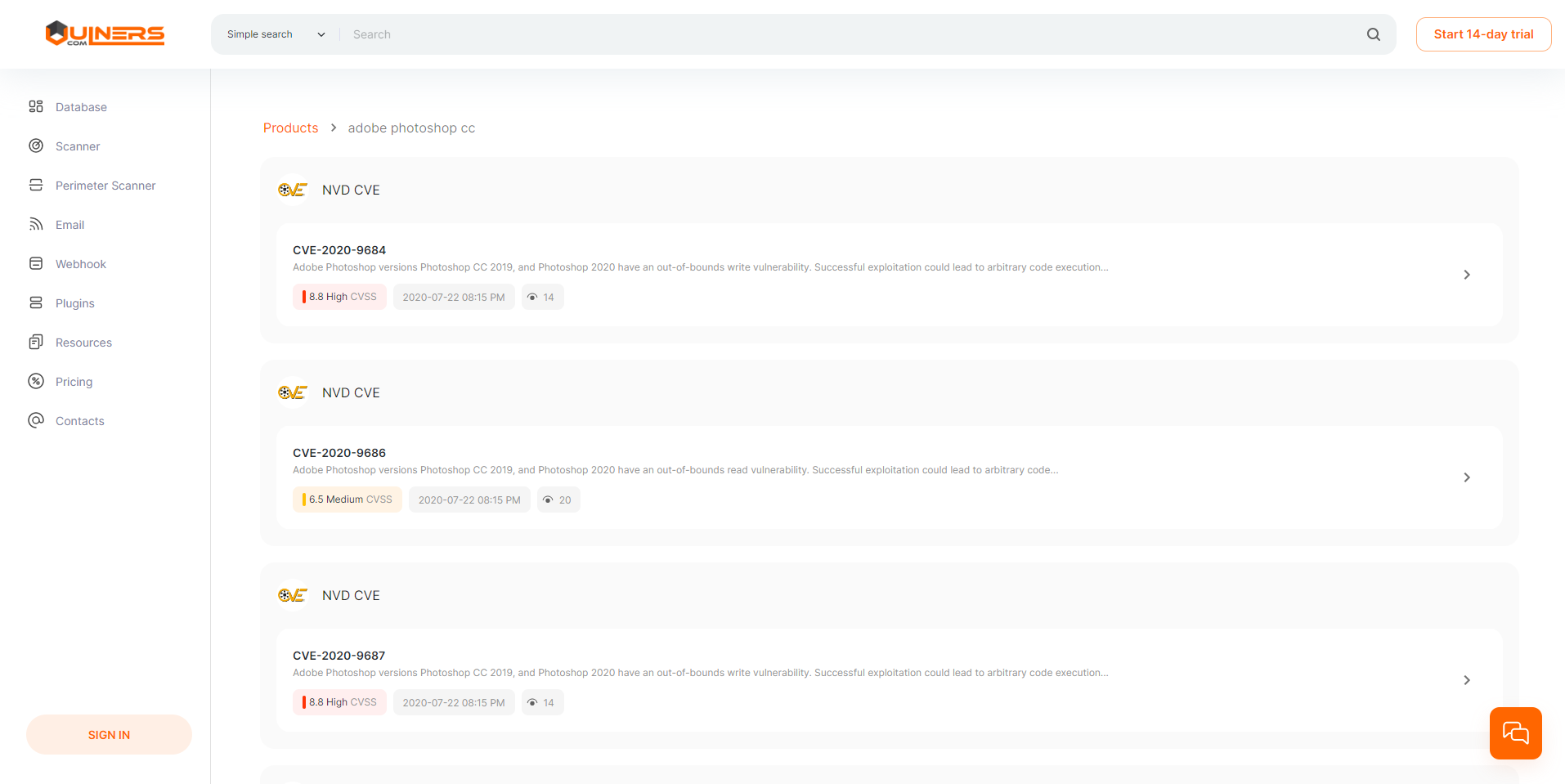


Рисунок 2 - Пример поиска уязвимостей в программе Adobe Photoshop

1. **CERT Coordination Center (CERT/CC)** Наряду с проведением независимых исследований и решением различных задач по обеспечению безопасности глобальной информационной инфраструктуры, эта организация обеспечивает централизованный сбор сведений обо всех уязвимостях в различных информационных системах и поддержание актуальной базы знаний об уязвимостях в информационных системах. Сведения о вновь выявляемых уязвимостях, вредоносных программах и способах нарушения информационной безопасности рассылаются по электронной почте: подписчиками этого бюллетеня являются более 161000 специалистов во всем мире.

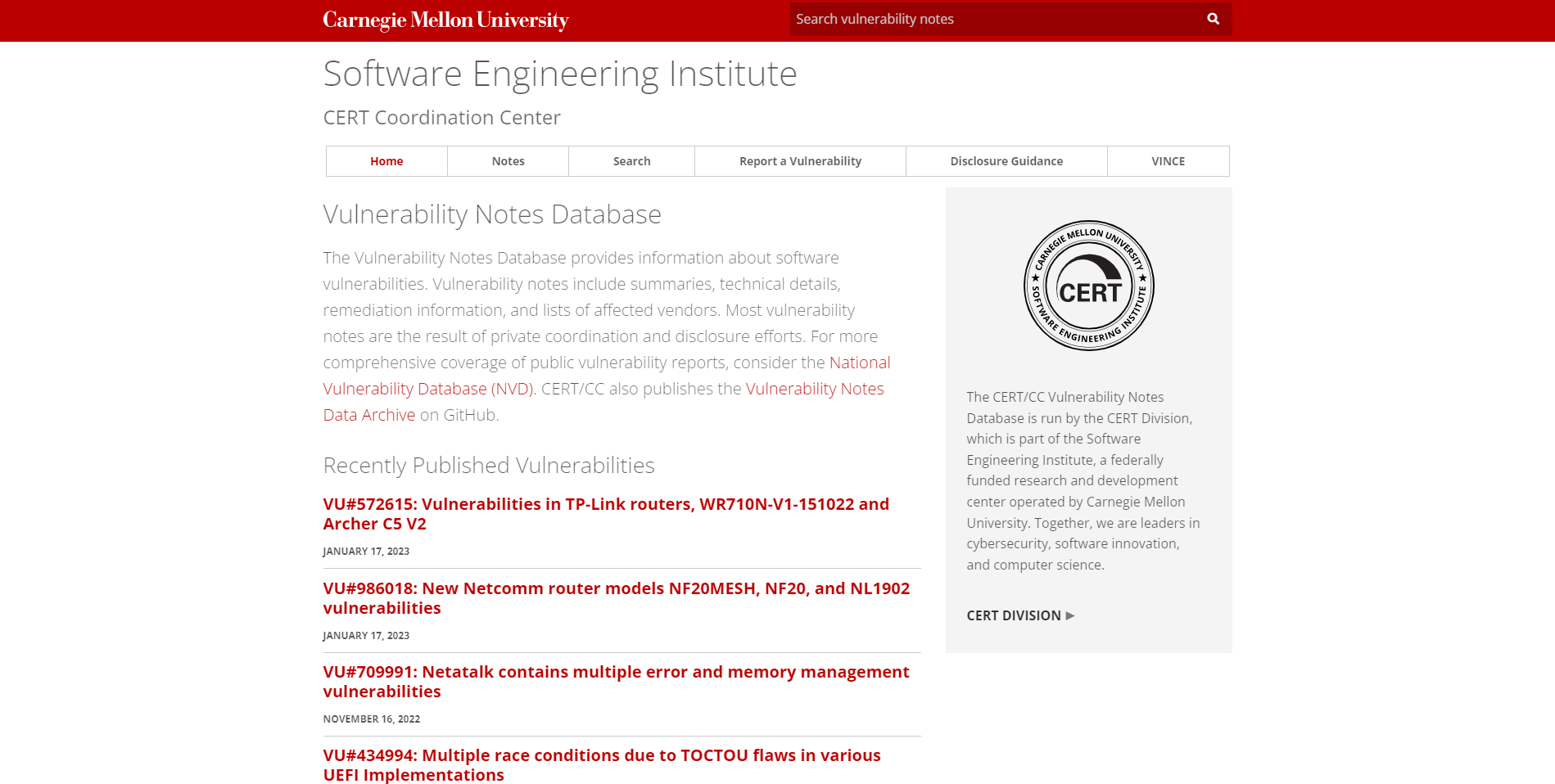


Рисунок 3 - Вид главной страницы сайта CERT/CC

1. **Secunia**Secunia - датская компания, специализирующаяся на компьютерной и сетевой безопасности. Наибольшую известность приобрела благодаря своим тестам на наличие уязвимостей. Эти тесты прошли более 12400 программных продуктов и ОС.

15 сентября 2015 года компания Flexera Software объявила о приобретении компании Secunia. Условия сделки не разглашаются.

По мнению Питера Колстеда (Peter Colsted), CEO компании Secunia, приобретение позволит предприятиям "проактивно противостоять кибер-угрозам безопасности в рамках своей основной деятельности по управлению использованием приложений".

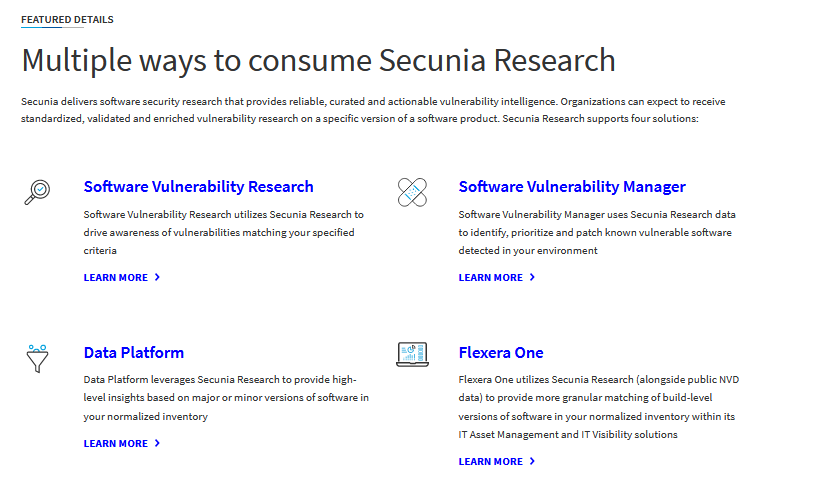


Рисунок 4 - Описание Secunia с сайта flexera.com

1. **Exploit Data Base**

База данных Exploit – это архив публичных эксплойтов и соответствующего уязвимого программного обеспечения, разработанный для использования тестировщиками проникновения и исследователями уязвимостей. Его цель – служить наиболее полным набором эксплойтов, шелкодека и документов, собранных с помощью прямых представлений, списков рассылки и других общедоступных источников, и представлять их в свободно доступной и простой для навигации базе данных. База данных Exploit – это хранилище эксплойтов и доказательств концепций, а не советов, что делает его ценным ресурсом для тех, кто нуждается в действительных данных сразу.

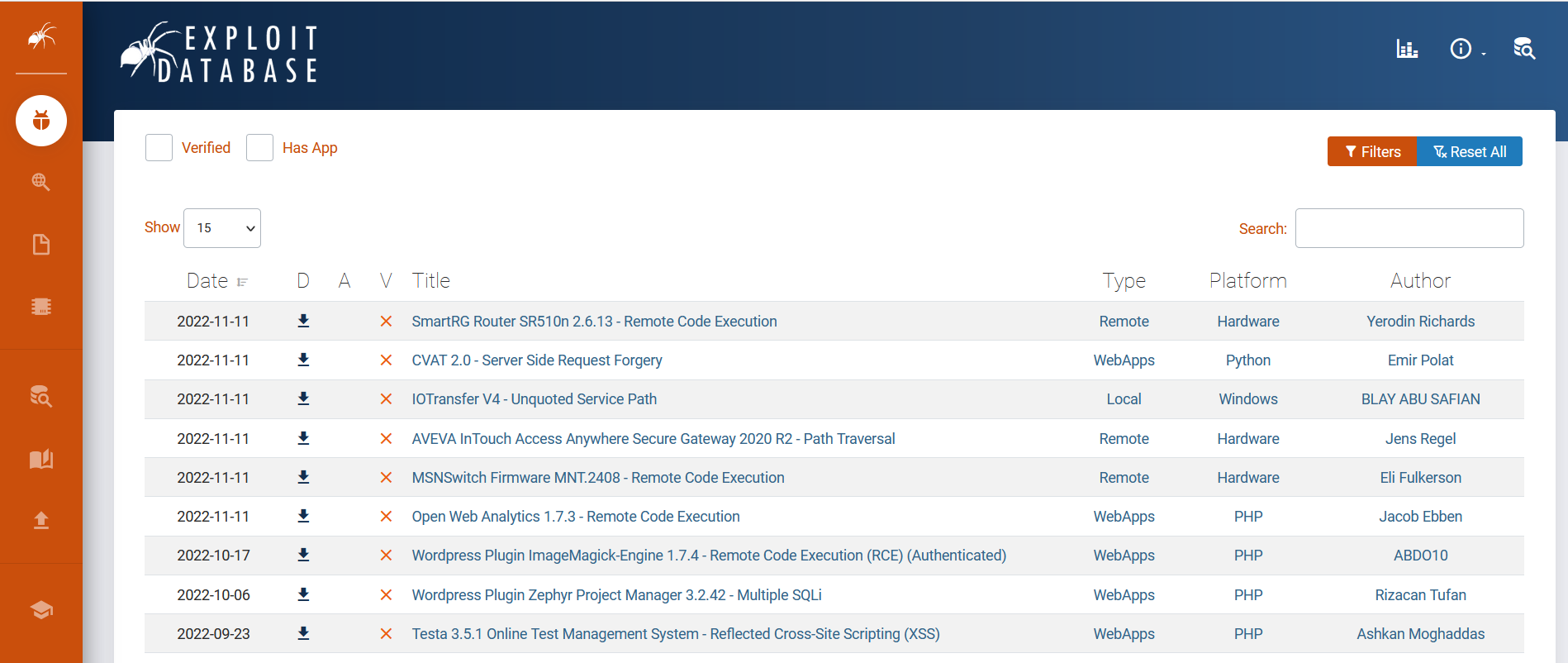


Рисунок 5 - Список эксплойтов с официального сайта

1. **Оцените уязвимости по базовым метрикам для ситуации при следующих условиях:**

а) атака высокой сложности будет проводится на физический уровень

системы, при этом оказывается влияние на другие компоненты системы.

Однако атака приводит только к нарушению целостности высокого уровня.

Взаимодействие с пользователем не требуется, а уровень привилегий -

низкий.

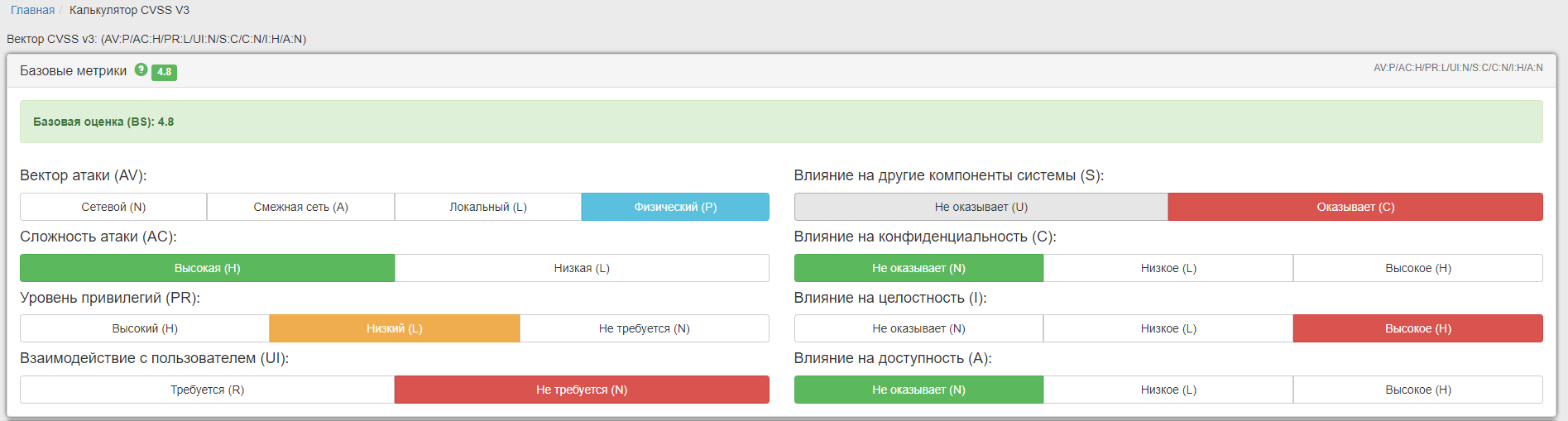


Рис 6. Оценка по базовым метрикам

Базовая оценка (BS): **4.8**Вектор CVSS v3: **(AV:P/AC:H/PR:L/UI:N/S:C/C:N/I:H/A:N)**

1. **Оцените уязвимости по временным метрикам для ситуации при следующих условиях:**

в) Предполагается, что есть PoC-код для средств эксплуатации, не определена доступность средств устранения и подтверждена степень доверия к источнику информации об уязвимости.

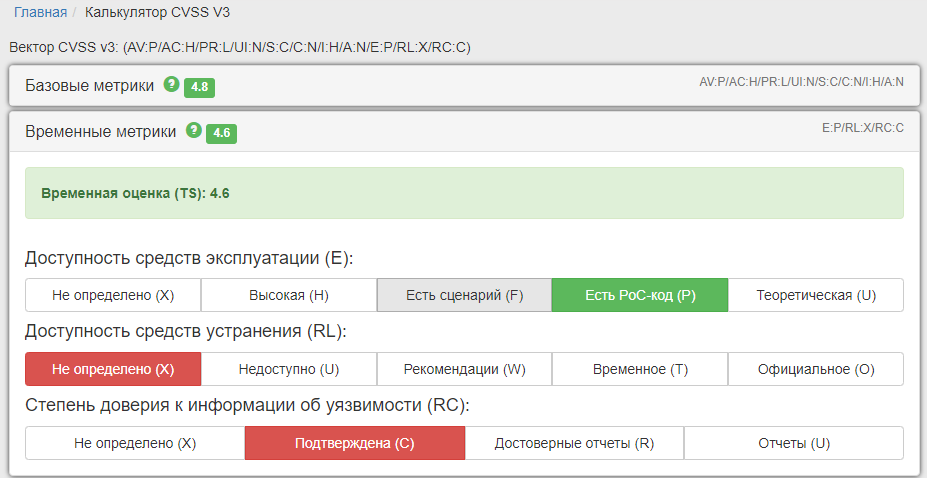


Рисунок 7 - Оценка по временным метрикам

Временная оценка (TS): **4.6**

1. **Оцените уязвимости по контекстным метрикам для ситуации при следующих условиях:**

е) К уровню обеспечения КЦД заданы высокие требования, однако влияние оказывается низким. При этом проводится атака неопределенной сложности на сетевой уровень системы. Уровень привилегий в данном случае - низкий, взаимодействия с пользователем не происходит. Также оказывается влияние на другие компоненты системы.

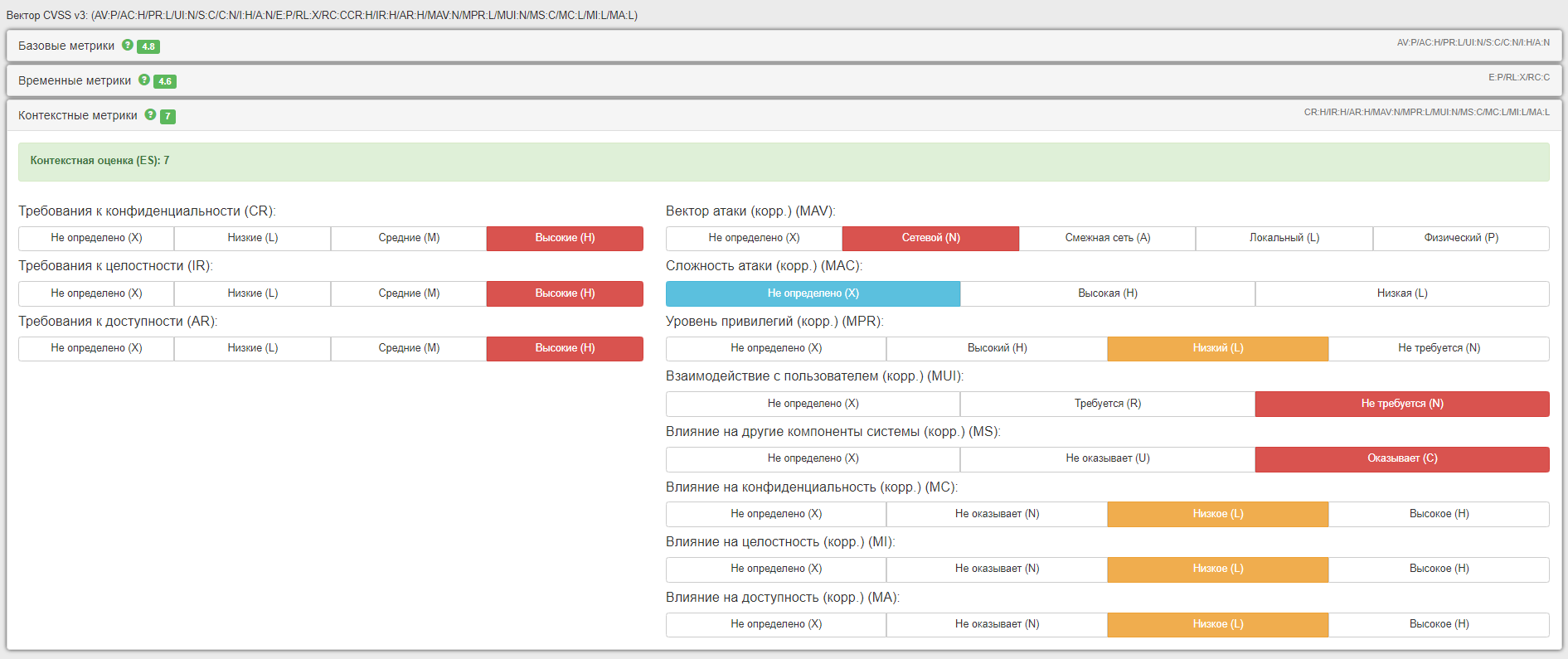


Рисунок 8 - Оценка по контекстным метрикам

Контекстная оценка (ES): **7**Вектор CVSS v3: **(AV:P/AC:H/PR:L/UI:N/S:C/C:N/I:H/A:N/E:P/RL:X/RC:CCR:H/IR:H/AR:H/MAV:N/MPR:L/MUI:N/MS:C/MC:L/MI:L/MA:L)**

**Вывод:**

В ходе работы мною были изучены различные базы данных уязвимостей и получены навыки по работе с ними. Во второй части лабораторной работы получен опыт работы с калькулятором CVSS v3.