Изучаем Exploit-db

The condition of a given task:

```
Давным давно в продукте vsFTPd нашли бэкдор. Он открывал шелл при попытке авторизации с любым паролем и логином, оканчивающимся на особую строку.
Введите эту особенную строку в качестве ответа
```

Solution:

exploit is https://www.exploit-db.com/exploits/49757 bypass characters is `:)` at the end of username

---

Hello, bash

The condition of a given task:

```
Необходимо подключиться к серверу. Флаг ждёт вас в файле /home/flag.txt
```

Solution:

the answer inside of the `/home/flag.txt` you can check it with `cat /home/flag.txt`

Hello,Telnet

The condition of a given task:

```
Необходимо подключиться к серверу используя telnet. Флаг ждёт вас в файле /home/flag.txt
Логин/пароль для подключения: user:user
Для подключения вам понадобится ваш личный VPN конфиг: https://lms.itmo.xyz/vpn
```

Solution:

the import the vpn-config into vpn-client wireguard and in terminal paste: `telnet 10.10.10.10 YOUR-PORT` with credentials `user:user` then use `cat /home/flag.txt` to find flag

---

Выйти из Vim

The condition of a given task:

```
Нужно не просто выйти из Vim, а прочитать флаг в /home/flag.txt
```

Solution:

at first you can open flag.txt through `:view <filename>` or tryna `:! cat /home/flag.txt` it's args for ==/bin/bash -c==

Анализ УК РФ

The condition of a given task:

```
Исследуйте правоприменительную практику по статье УК РФ 272 или 273 за последние 5 лет.
Оцените общее количество возбужденных дел, число обвинительных приговоров.
Выделите общие черты действий, которые могут привести к привлечению к ответственности по
статье. Приведите несколько примеров дел с указанием приговора.
Ваш ответ должен включать:
Динамику количества возбужденных уголовных дел по статье 272 и 273 УК РФ, а также число
обвинительных приговоров. В виде нумерованного списка или графика.Основные черты
действий, которые могут привести к судебному преследованию. Почему вы так считаете?
Приведите 2-3 примера дел с указанием: сути дела и вердикта
```

Solution:

2022 год - *179* обвинительных приговоров и *1* оправдательных

2021 год - *133* обвинительных приговора

2020 год - *133* обвинительных приговоров

2019 год - *85* обвинительных приговоров

2018 год - *50* обвинительных приговоров и 1 оправдательных

273 УК РФ - Создание, использование и распространение вредоносных компьютерных программ

2022 год - *90* обвинительных приговоров

2021 год - *153* обвинительных приговора

2020 год - *90* обвинительных приговоров

2019 год - *195* обвинительных приговоров и 2 оправдательных

2018 год - *157* обвинительных приговоров и 1 оправдательный

Источник: https://stat.апи-пресс.рф/stats/ug/t/14/s/17 Основными чертами, на мой взгляд, могут служить **неотвратимость**, **непосредственный урон бизнес-процессу** или **репутационные риски компании**.

CVSS Score

The condition of a given task:

```
Посчитайте CVSSv3 и CVSSv4 score для уязвимости в веб-приложении, эксплуатируемой путем
отправки запроса от имени непривилегированного пользователя, которая позволит атакующему
получить доступ к чтению и изменению данных всех пользователей данного приложения.
В качестве ответа пришлите вашу оценку и вектор, например:
Оценка v4: 5.8 / Medium Вектор v4:
CVSS:4.0/AV:A/AC:H/AT:N/PR:L/UI:A/VC:L/VI:H/VA:N/SC:L/SI:L/SA:H
```

```
Оценка v3: ... / ... Вектор v3: ...
У меня получились такие векторы, потому что ...
Не забудьте написать обоснование, почему именно такой компонент в векторе написали.
Литература:
https://www.first.org/cvss/v4-0/https://www.first.org/cvss/v3.1/examples
```

Solution:

Оценка v3: *9.1* / Critical

Вектор v3: `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N`

Оценка v4: *8.2* / High

Вектор v4: `CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N`

Вектор v3 указывает на возможную уязвимость типа SQL инъекции, которая эксплуатируется удаленно. Для ее использования не требуется сложной предварительной настройки, особых привилегий или взаимодействия с пользователем. Уязвимость ограничивается конкретным сервисом или приложением, и, вероятно, не влияет на другие системы или сервисы. Главными последствиями эксплуатации являются **потеря конфиденциальности** и **целостности данных**, в то время как *доступность системы остается неизменной*.

Вектор v4 в целом соответствует v3, но включает в себя дополнительные метрики, характерные для этой версии системы оценки.

Отчет по уязвимости

The condition of a given task:

```
Выберите известную современную уязвимость и укажите для нее следующее:
CVE CVSS (подробно) CWE Подходящие техники MITRE ATT&CK Статус наличия эксплойта
Перечень диапазонов уязвимых версий
При выборе CWE используйте наиболее точную классификацию. CWE-20 – экстренный вариант,
если совсем ничего не подходит. Ответы без перечисления всех 6 пунктов приниматься не
будут.
```

Solution:

Давайте рассмотрим уязвимость "**Zerologon**", обнаруженную в 2020 году, которая затрагивает Windows Server.

CVE: **CVE-2020-1472**

CVSS (подробно):

Версия CVSS: 3.0 Вектор атаки (AV): Сеть (Network) Сложность атаки (AC): Низкая (Low) Требования к привилегиям (PR): Ни одного (None) Вектор взаимодействия пользователя (UI): Не требуется (None) Воздействие на конфиденциальность (C): Высокое (High) Воздействие на целостность (I): Высокое (High)

Воздействие на доступность (A): Высокое (High) Баллы CVSS: **10.0** (из 10) CWE: CWE-311: *Отсутствие аутентификации*

Подходящие техники MITRE ATT&CK:

```
Exploitation for Privilege Escalation
Exploitation for Credential Access
Forge Web Credentials
```

Статус наличия эксплойта: Доступен

Перечень диапазонов уязвимых версий:

```
Windows Server 2008 R2 для 64-битных систем
Windows Server 2012
Windows Server 2012 R2
Windows Server 2016
Windows Server 2019
Windows Server, версия 1903 (сервер с рабочей станцией)
Windows Server, версия 1909 (сервер с рабочей станцией)
Windows Server, версия 2004 (сервер с рабочей станцией)
```
