Nemesida WAF

Комплексная защита веб-приложений и API от хакерских атак

Romanov Roman
Pentestit, 2021

Какие проблемы решает

- Простая установка и настройка
- Минимум времени на обслуживание
- Блокирование попыток поиска и эксплуатации уязвимостей
- Выявление сложных и неизвестных атак
- Выявление веб-уязвимостей
- Защита от DDoS L7 / подбора паролей / прочего паразитного бот-трафика

Некорректная фильтрация данных

Запрос:
http://example.com/index.php?id=1

Пример кода:

```
$id = $_GET['id'];
$query = "SELECT * FROM %some_table% WHERE id=$id";
```

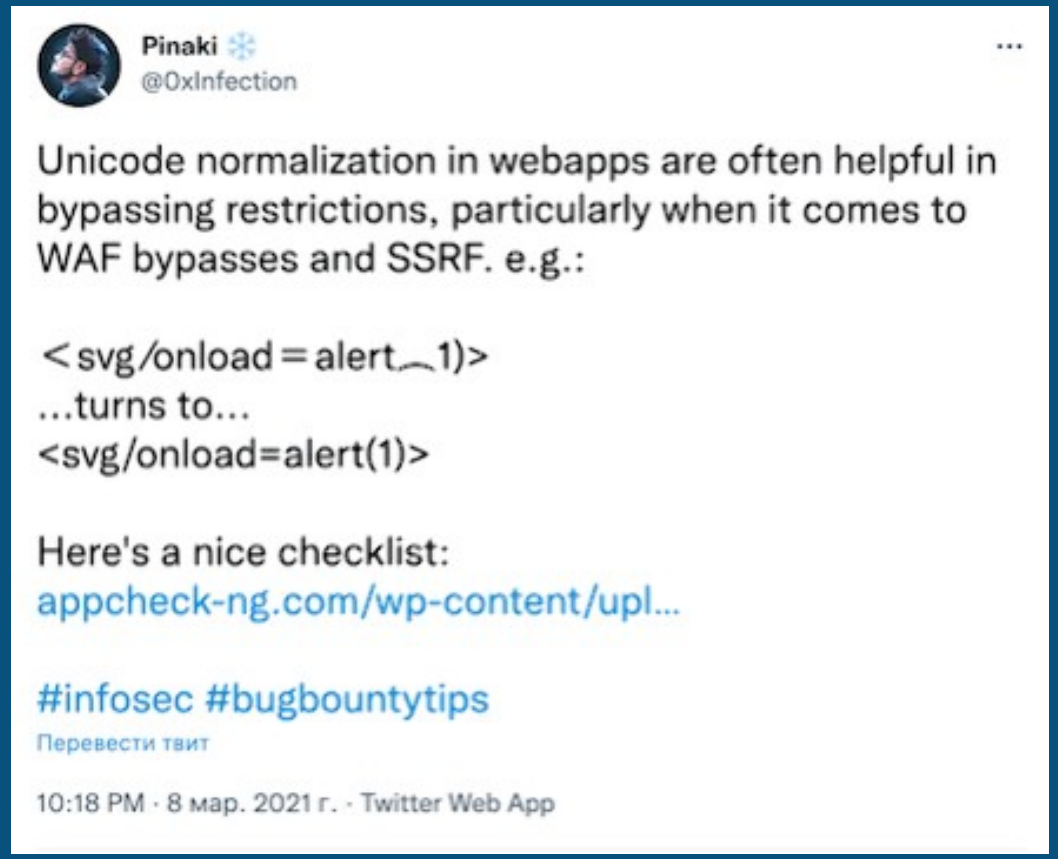
Результат запроса в БД:
SELECT * FROM %some_table% WHERE id=%данные из запроса%

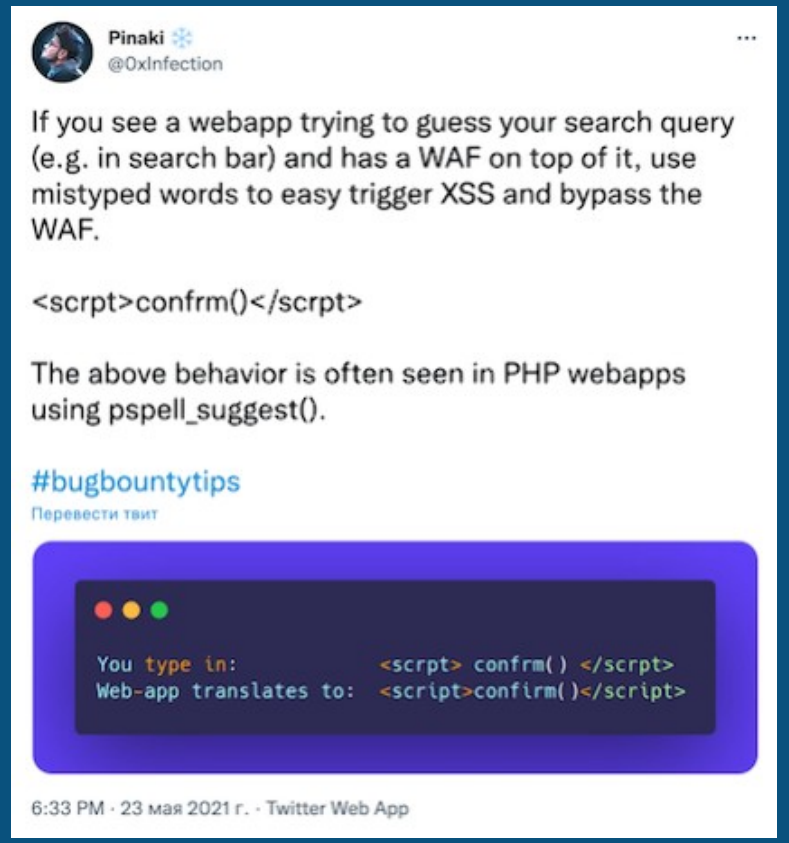
Различные техники обхода WAF

- Различные кодировки (HTTP Entity Encode, URL encode, UTF-16/32, Halfwidth and Fullwidth Forms и другие)
- Расщепление полезной нагрузки (un","ion se","lect)
- Особенности нормализации запроса (/???/??t /???/p??s??)

и другие

Различные техники обхода WAF



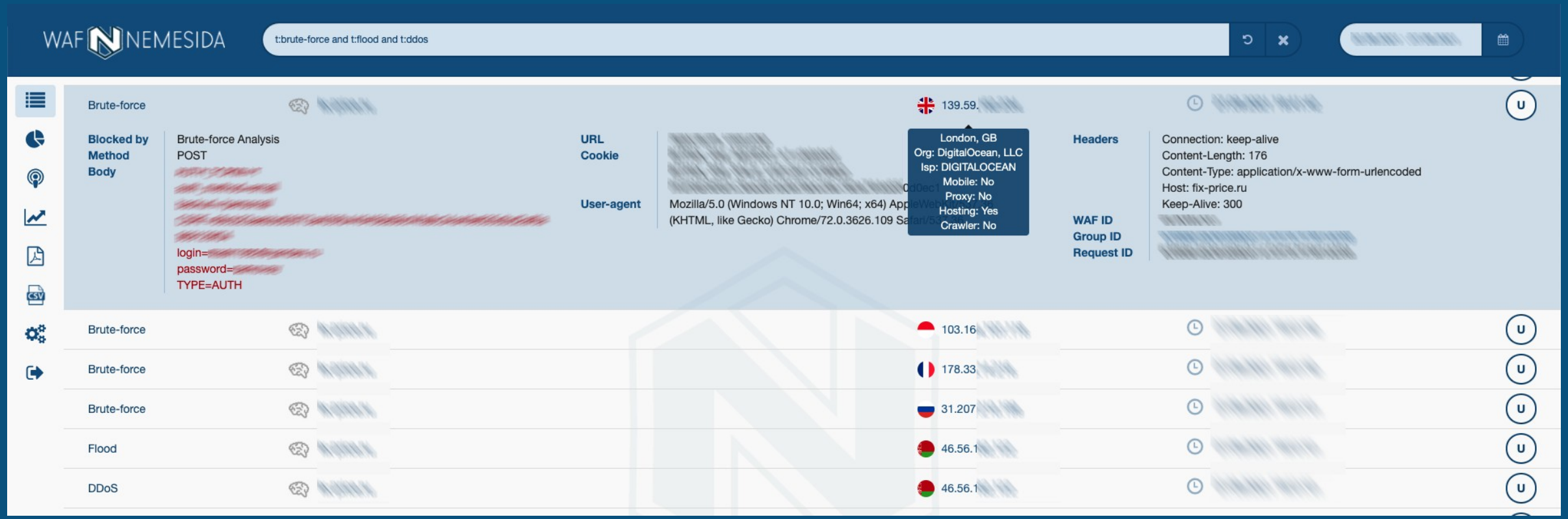


Различные техники обхода WAF

Сигнатурный анализ VS машинное обучение

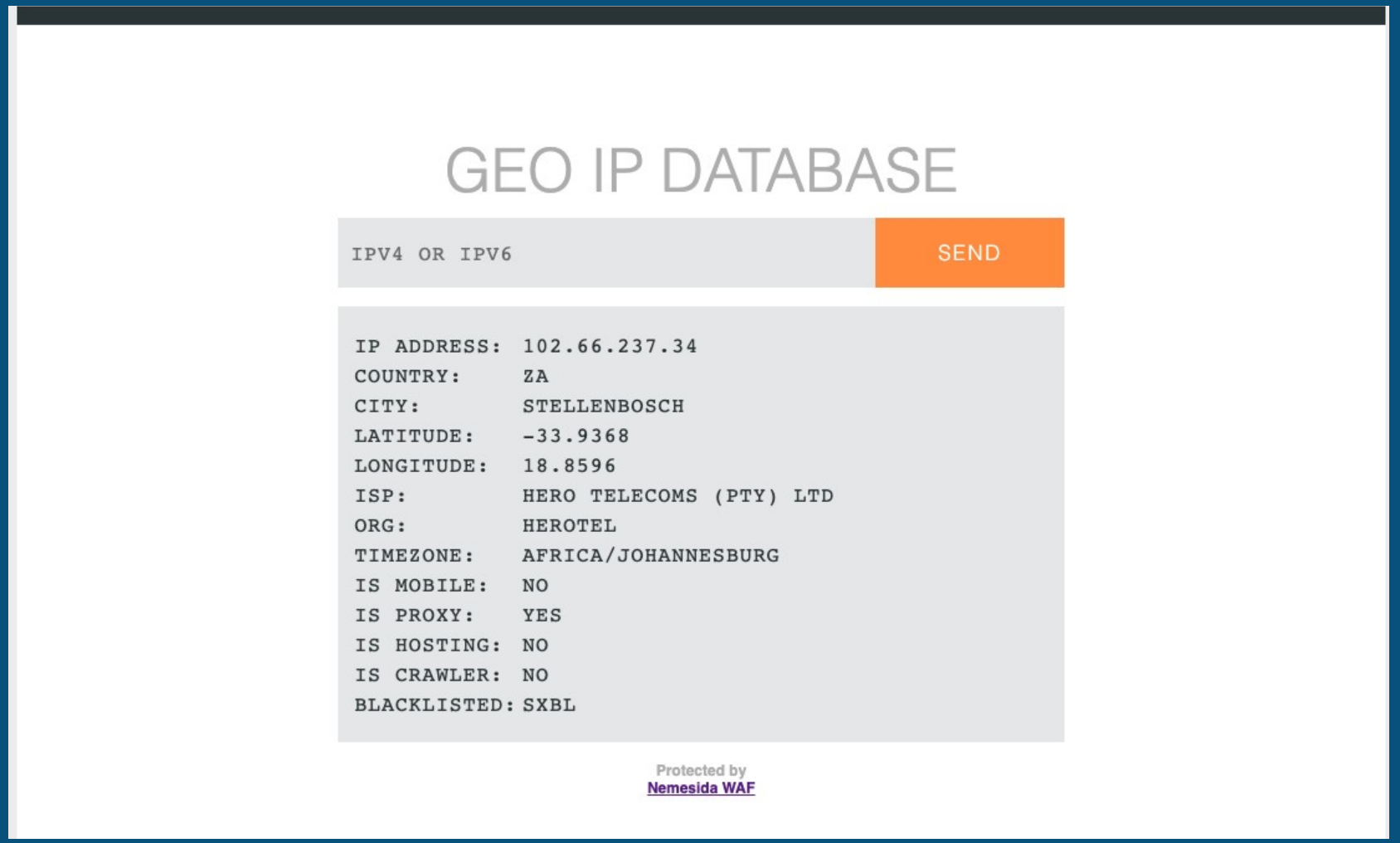
- Какой тип анализа имеет меньше пропусков и ложных срабатываний
- Почему мы используем комбинированный анализ
- Получаем 99.98 — 99.99 % точности на обычном «железе»

Защита от DDoS L7, атаки методом перебора и флуда



Расширенные алгоритмы определения атак с использованием поведенческих признаков и специальных меток — GeoIP-данные в сочетании с коэффициентами значимости и надежности.

Собственная GeoIP-база

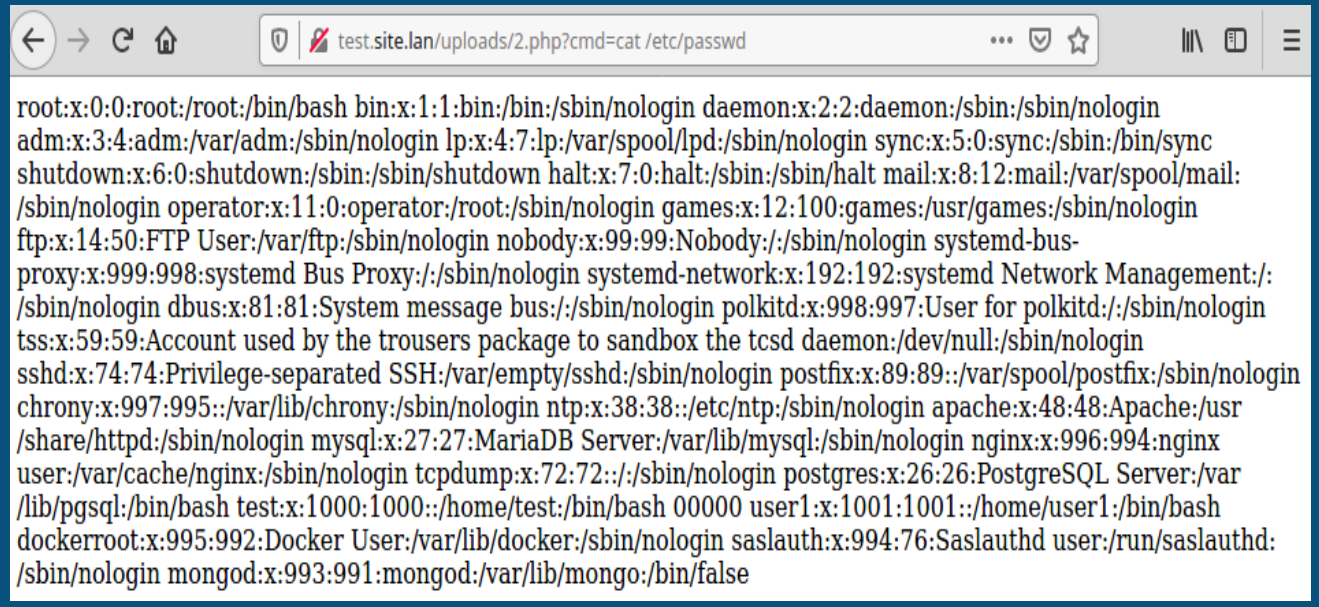


Отрицание

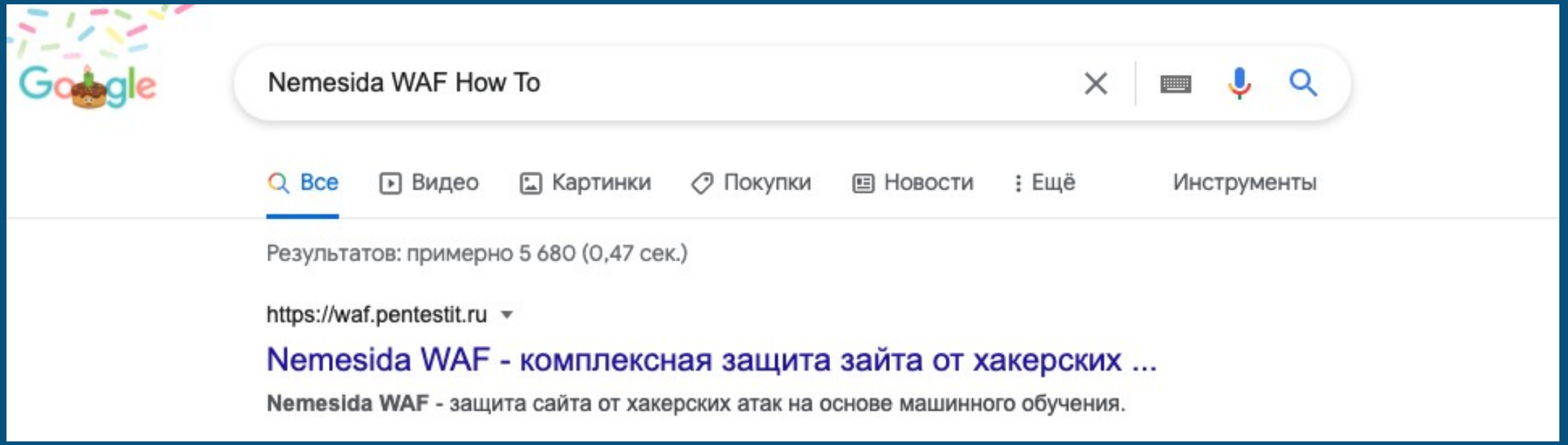

Google
php deserialization example
php deserialization example
php serialize example
php insecure deserialization example
php deserialization rce example
serialize php пример
php unserialize example
php deserialization attack example
Пожаловаться на неприемлемые подсказки
definition, you can use the following simple rename function:

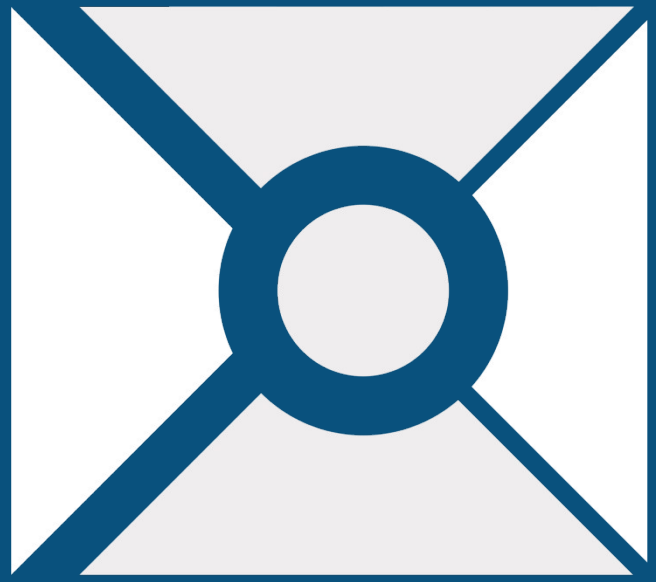
Депрессия

< ?php system($_GET[cmd]); ?>



Принятие


Google
Nemesida WAF How To
Все
Видео
Картинки
Покупки
Новости
Ещё
Инструменты
Результатов: примерно 5 680 (0,47 сек.)
https://waf.pentestit.ru
Nemesida WAF - комплексная защита зайта от хакерских ...
Nemesida WAF - защита сайта от хакерских атак на основе машинного обучения.



www.pentestit.ru