



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 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



Unicode normalization in webapps are often helpful in bypassing restrictions, particularly when it comes to WAF bypasses and SSRF. e.g.:

```
<svg/onload = alert(1)>  
...turns to...  
<svg/onload=alert(1)>
```

Here's a nice checklist:
appcheck-ng.com/wp-content/upl...

#infosec #bugbountytips

Перевести твит

10:18 PM · 8 мар. 2021 г. · Twitter Web App



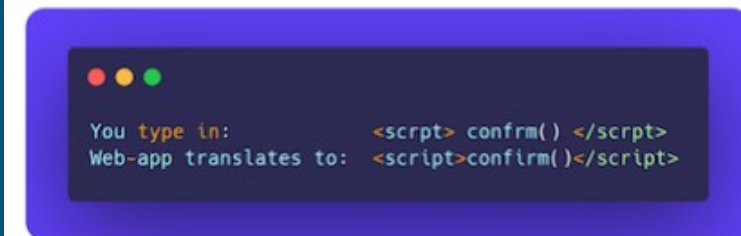
If you see a webapp trying to guess your search query (e.g. in search bar) and has a WAF on top of it, use mistyped words to easy trigger XSS and bypass the WAF.

```
<script>confm()</script>
```

The above behavior is often seen in PHP webapps using pspell_suggest().

#bugbountytips

Перевести твит



6:33 PM · 23 мая 2021 г. · Twitter Web App



Различные техники обхода WAF



XSS Payloads

@XssPayloads



One to evade Imparva WAF, by [@OxInfection](#)
<x/onclick=globalThis['\\u0070r\\u006f'+'mpt']&l
t;)>clickme

[Перевести твит](#)

10:32 AM · 28 июл. 2021 г. · TweetDeck



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

WAF NEMESIDA

t:brute-force and t:flood and t:ddos

Brute-force

Blocked by Method Body

Brute-force Analysis
POST

login=
password=
TYPE=AUTH

URL
Cookie

User-agent
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.109 Safari/537.36

London, GB
Org: DigitalOcean, LLC
Isp: DIGITALOCEAN
Mobile: No
Proxy: No
Hosting: Yes
Crawler: No

Headers
Connection: keep-alive
Content-Length: 176
Content-Type: application/x-www-form-urlencoded
Host: fix-price.ru
Keep-Alive: 300

WAF ID
Group ID
Request ID

Brute-force		139.59.	
Brute-force		103.16.	
Brute-force		178.33.	
Brute-force		31.207.	
Flood		46.56.1.	
DDoS		46.56.1.	

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



GEO IP DATABASE

IPV4 OR IPV6

SEND

```
IP ADDRESS: 102.66.237.34
COUNTRY:    ZA
CITY:       STELLENBOSCH
LATITUDE:   -33.9368
LONGITUDE:  18.8596
ISP:        HERO TELECOMS (PTY) LTD
ORG:        HEROTEL
TIMEZONE:   AFRICA/JOHANNESBURG
IS MOBILE:  NO
IS PROXY:   YES
IS HOSTING: NO
IS CRAWLER: NO
BLACKLISTED: SXBL
```

Protected by
[Nemesida WAF](#)



Отрицание

The screenshot shows a Google search bar with the text "php deserialization example |". Below the search bar, a list of search suggestions is displayed:

- php deserialization example
- php **serialize** example
- php **insecure** deserialization example
- php deserialization **rce** example
- serialize** php **пример**
- php **unserialize** example
- php deserialization **attack** example

At the bottom right of the suggestions box, there is a link: [Пожаловаться на неприемлемые подсказки](#)

definition, you can use the following simple rename function:



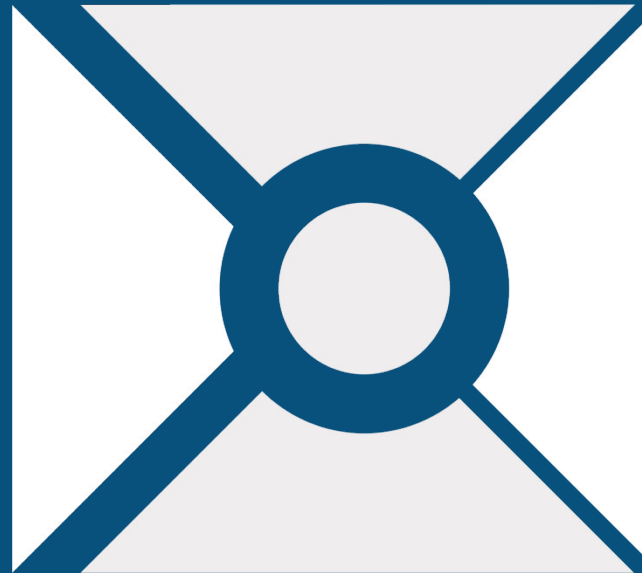
< ?php system(\$_GET[cmd]); ?>

```
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt mail:x:8:12:mail:/var/spool/mail:
/sbin/nologin operator:x:11:0:operator:/root:/sbin/nologin games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/sbin/nologin systemd-bus-
proxy:x:999:998:systemd Bus Proxy:/sbin/nologin systemd-network:x:192:192:systemd Network Management:/
/sbin/nologin dbus:x:81:81:System message bus:/sbin/nologin polkitd:x:998:997>User for polkitd:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin postfix:x:89:89:/var/spool/postfix:/sbin/nologin
chrony:x:997:995:/var/lib/chrony:/sbin/nologin ntp:x:38:38:/etc/ntp:/sbin/nologin apache:x:48:48:Apache:/usr
/share/httpd:/sbin/nologin mysql:x:27:27:MySQL Server:/var/lib/mysql:/sbin/nologin nginx:x:996:994:nginx
user:/var/cache/nginx:/sbin/nologin tcpdump:x:72:72:/sbin/nologin postgres:x:26:26:PostgreSQL Server:/var
/lib/pgsql/bin/bash test:x:1000:1000:/home/test:/bin/bash 00000 user1:x:1001:1001:/home/user1:/bin/bash
dockerroot:x:995:992:Docke User:/var/lib/docker:/sbin/nologin saslauthd:x:994:76:Saslauthd user:/run/saslauthd:
/sbin/nologin mongod:x:993:991:mongod:/var/lib/mongo:/bin/false
```



Принятие

The screenshot shows a Google search interface. The search bar contains the text "Nemesida WAF How To". Below the search bar, there are navigation options: "Все" (All), "Видео" (Video), "Картинки" (Images), "Покупки" (Shopping), "Новости" (News), "Ещё" (More), and "Инструменты" (Tools). The search results show approximately 5,680 results in 0.47 seconds. The top result is from "https://waf.pentestit.ru" and is titled "Nemesida WAF - комплексная защита сайта от хакерских ...". The description below the title reads: "Nemesida WAF - защита сайта от хакерских атак на основе машинного обучения."



www.pentestit.ru