

**Негосударственное образовательное
учреждение
высшего образования
Московский технологический институт**

ДИПЛОМНАЯ РАБОТА

на тему:

**Анализ уязвимостей web-приложений и способы
защиты с использованием Java-технологий на
примере организации**

Выполнил:

ф.и.о.

Научный руководитель:

ф.и.о.

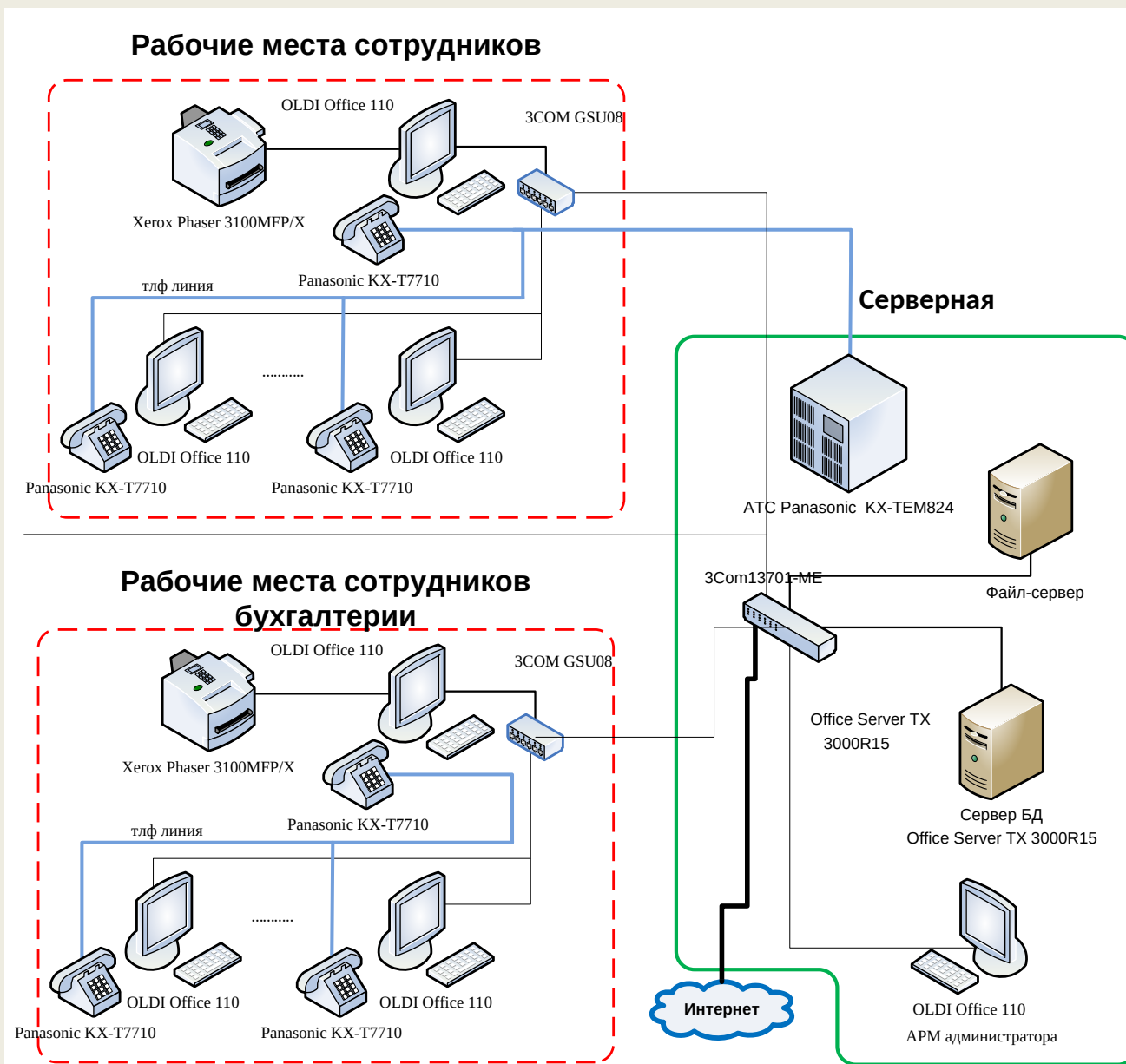
Цель и задачи

Цель - анализ уязвимостей web-приложений и способы защиты с использованием Java-технологий на примере организации.

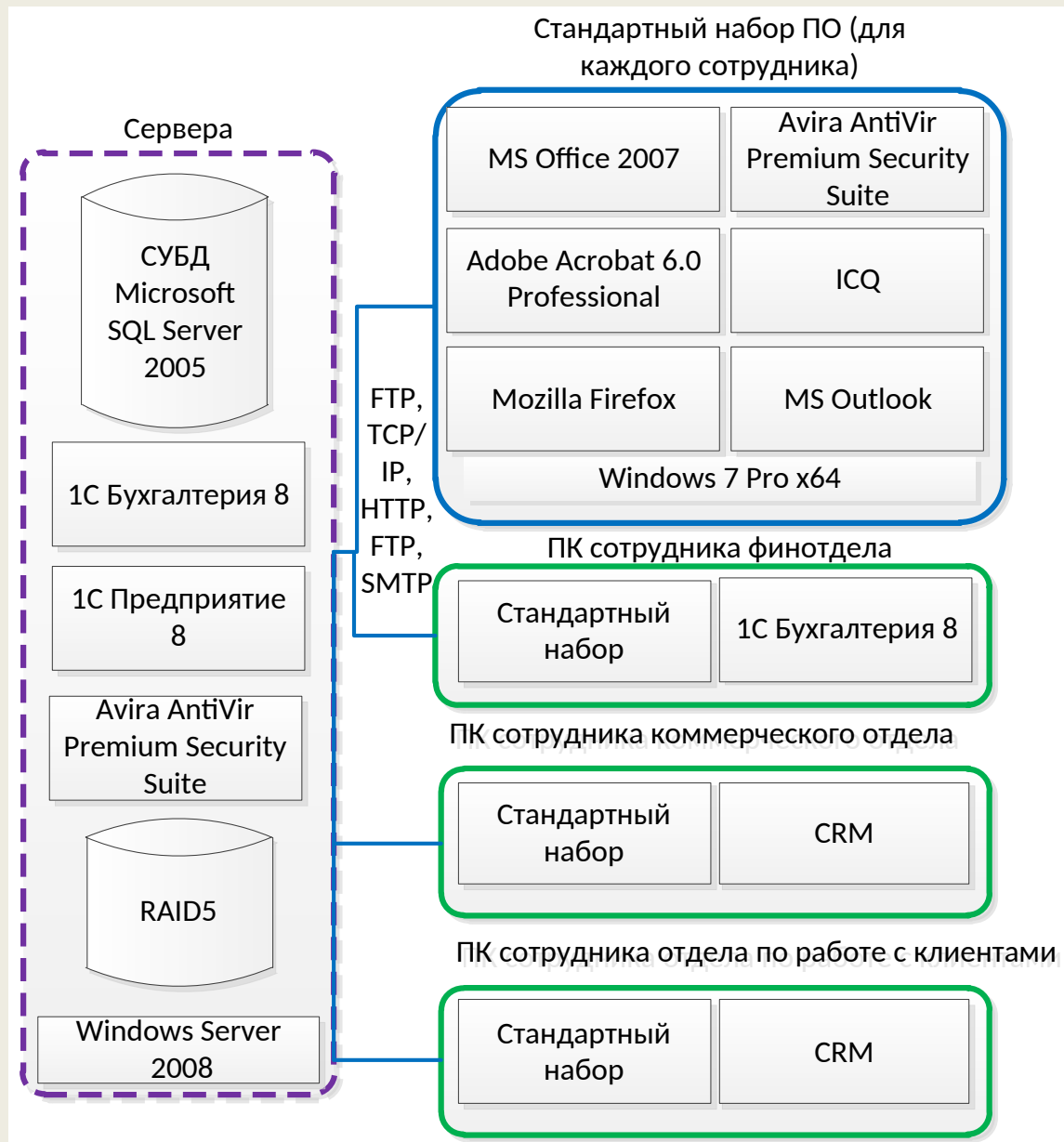
Задачи:

1. разработать критерии для сравнения технологий поиска веб-уязвимостей, критерии сравнения обеспечения безопасности интегрированных средств тестирования;
2. провести обзор и анализ современных технологий тестирования веб-уязвимостей;
3. провести анализ современных веб-уязвимостей и рассмотреть варианты их реализации и способы защиты;
4. провести сравнение интегрированных сред тестирования веб-уязвимостей;
5. усовершенствовать интегрированное средство тестирования веб-уязвимостей путем разработки нового сценария тестирования.

Схема технической архитектуры предприятия



Программная архитектура предприятия



Итоги сканирования Metasploid Framework

Тип уязвимости	Найдено	Ложно найдено	Время
Инъекции	6	5	3ч18м
Вопросы аутентификации и проверки сессий	11	2	
XSS	1	1	
Вопросы контроля доступа	3	2	
Неправильная конфигурация	128	0	

Итоги сканирования OneSQL

Тип уязвимости	Найдено	Ложно найдено	Время
Инъекции	14	0	4ч27м
Вопросы аутентификации и проверки сессий	—	—	
XSS	—	—	
Вопросы контроля доступа	—	—	
Неправильная конфигурация	—	—	

Итоги сканирования BDD-Security

Тип уязвимости	Найдено	Ложно найдено	Время
Инъекции	1	0	2ч 13м
Вопросы аутентификации и проверки сессий	31	0	
XSS	19	0	
Вопросы контроля доступа	4	3	
Неправильная конфигурация	231	0	

Итоги сканирования w3af

Тип уязвимости	Найдено	Ложно найдено	Время
Инъекции	4	2	2ч57м
Вопросы аутентификации и проверки сессий	3	1	
XSS	25	0	
Вопросы контроля доступа	4	3	
Неправильная конфигурация	17	0	

Сравнение по критериям

№	Средство тестирования \ Критерий сравнения	Metasploit Framework	OneSQL	BDD-Security	W3AF
1.	Сопоставление стоимости продукта относительно оценкам критериев.	1	1	0	1
2.	Универсальность использования средств тестирования уязвимостей.	1	0	0	1
3.	Число поддерживаемых векторов атаки: тип и число активных плагинов средства тестирования уязвимостей.	1	0	0	1
4.	Точность выявления CSS.	0	1	0	1
5.	Точность выявления SQL-инъекций.	0	1	1	1
6.	Точность обхода структуры веб-приложения и выявления локальных файлов.	1	0	1	0
7.	Удаленное применение файлов, XSS, фишинг посредством RFI.	1	0	1	0
8.	WIVET-сравнение.	1	0	0	1
9.	Адаптивность технологии.	0	1	0	1
10.	Сопоставление особенностей аутентификации.	1	0	0	1
11.	Число дополнительных возможностей сканирования и интегрированных механизмов.	1	0	0	1
12.	Общее представление о работе ключевой функции сканирования.	0	1	0	1
Итого		8	5	3	10

Результат работы сканера Metasploit Framework

```
root@kaliTest:~# nmap -A -T4 scanme.nmap.org

Starting Nmap 7.40 ( https://nmap.org ) at 2018-01-09 22:37 EET
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.18s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 closed ports
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
25/tcp    filtered  smtp
80/tcp    open      http         Apache httpd 2.4.7 ((Ubuntu))
|_ http-title: Go ahead and ScanMe!
139/tcp   filtered  netbios-ssn
9929/tcp  open      nping-echo   Nping echo
Aggressive OS guesses: Linux 3.2 - 4.6 (97%), Linux 3.10 - 4.2 (94%), Linux 3.13 (94%), Linux 3.13 - 3.16 (94%), Android 5.0 - 5.1 (93%), Linux 3.10 (93%), Linux 3.2 - 3.10 (93%), Linux 3.2 - 3.16 (93%), Linux 4.5 (93%), Linux 4.2 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 14 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux kernel
```

Результат работы утилиты searchsploit

```
root@kaliTest: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
root@kaliTest:~# searchsploit apache
```

Exploit Title	Path (/usr/share/exploitdb/platforms/)
Apache 2.x - Memory Leak Exploit	windows/dos/9.c
Apache 2.0.44 (Linux) - Remote Denial of Ser	linux/dos/11.c
Apache - Arbitrary Long HTTP Headers Denial	multiple/dos/360.pl
Apache - Arbitrary Long HTTP Headers Denial	linux/dos/371.c
Apache 2.0.52 - HTTP GET request Denial of S	multiple/dos/855.pl
Apache 2.0.49 - Arbitrary Long HTTP Headers	multiple/dos/1056.pl
Apache (mod_rewrite) < 1.3.37 / 2.0.59 / 2.2	multiple/dos/2237.sh
Apache mod_dav / svn - Remote Denial of Serv	multiple/dos/8842.pl
Apache 2.2 (Windows) - Local Denial of Servi	windows/dos/15319.pl
Apache - Remote Denial of Service (Memory Ex	multiple/dos/17696.pl

Результат работы Metasploit Framework по поиску модулей, описывающих уязвимости WordPress

```
Matching Modules
=====

```

Name	Description	Disclosure Date
auxiliary/admin/http/wp_custom_contact_forms	WordPress custom-contact-forms Plugin SQL Upload	2014-08-07
normal		
auxiliary/dos/http/wordpress_long_password_dos	WordPress Long Password DoS	2014-11-20
normal		
auxiliary/dos/http/wordpress_xmlrpc_dos	WordPress XMLRPC DoS	2014-08-06
normal		
auxiliary/gather/wp_ultimate_csv_importer_user_extract	WordPress Ultimate CSV Importer User Table Extract	2015-02-02
normal		
auxiliary/gather/wp_w3_total_cache_hash_extract	W3-Total-Cache Wordpress-plugin 0.9.2.4 (or before) Username and Password Hash Extract	
normal		
auxiliary/scanner/http/wordpress_ghost_scanner	WordPress XMLRPC GHOST Vulnerability Scanner	
normal		
auxiliary/scanner/http/wordpress_login_enum	WordPress Brute Force and User Enumeration Utility	
normal		
auxiliary/scanner/http/wordpress_pingback_access		

Процесс перебора паролей по словарю при помощи Metasploit Framework

```
[*] / - WordPress Brute Force - Trying username:'admin' with password:'steven'
[-] / - WordPress Brute Force - Failed to login as 'admin'
[*] / - WordPress Brute Force - Trying username:'admin' with password:'fender'
[-] / - WordPress Brute Force - Failed to login as 'admin'
[*] / - WordPress Brute Force - Trying username:'admin' with password:'john'
[-] / - WordPress Brute Force - Failed to login as 'admin'
[*] / - WordPress Brute Force - Trying username:'admin' with password:'yamaha'
[-] / - WordPress Brute Force - Failed to login as 'admin'
[*] / - WordPress Brute Force - Trying username:'admin' with password:'diablo'
[-] / - WordPress Brute Force - Failed to login as 'admin'
[*] / - WordPress Brute Force - Trying username:'admin' with password:'chris'
```

Информация о найденном пароле способом перебора по словарю

```
msf auxiliary(wordpress_login_enum) > run

[*] / - WordPress Version 4.2.2 detected
[+] / - Found user 'admin' with id 1
[*] / - Usernames stored in: /root/.msf4/loot/20150601134638_default_192.168.33.10_
wordpress.users_187286.txt
[*] / - WordPress User-Validation - Checking Username:''
[*] / - Brute-forcing previously found accounts...
[+] / - WordPress Brute Force - SUCCESSFUL login for 'admin' : 'admin'
[-] *** auxiliary/scanner/http/wordpress_login_enum is still calling the deprecated
report_auth_info method! This needs to be updated!
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(wordpress_login_enum) > 
```

Пример работы Burp Proху по анализу HTTP - запросов

125	http://www.google-analytic...	GET	/ga.js	☐	☐	200
144	http://www.google-analytic...	GET	/ga.js	☐	☐	200
129	http://forum.portswigger.net	GET	/board/5/news	☐	☐	200
109	http://portswigger.net	GET	/burp/help/contents.html	☐	☐	200
122	http://cdn.viglink.com	GET	/api/vglnk.js	☐	☐	200
167	http://portswigger.net	GET	/js/jquery.js	☐	☐	200
124	http://ads.pro-market.net	GET	/ads/scripts/dda3-6-2pt2.js	☐	☐	200
152	http://ads.pro-market.net	GET	/ads/scripts/dda3-6-2pt2.js	☐	☐	200
115	http://ajax.googleapis.com	GET	/ajax/libs/jquery/1.7.2/jquery.mi...	☐	☐	200
112	http://d.storage.proboards....	GET	/f/forum_201.js	☐	☐	200

Request

Response

Raw

Headers

Hex

Name	Value
HTTP/1.1	200 OK
Content-Type	text/javascript
Content-Length	61565
Connection	keep-alive
Date	Thu, 06 Nov 2014 11:48:39 GMT
Cache-Control	max-age=15, must-revalidate
Last-Modified	Tue, 04 Nov 2014 17:41:36 GMT
ETag	"0bb928b65488e416e330799a613e791f"

Пример сканирования портов

```
$ nmap -sV --reason -PN -n --top-ports 100 www.example.com
Starting Nmap 6.25 ( http://nmap.org ) at 2013-01-01 00:00 CEST
Nmap scan report for www.example.com (127.0.0.1)
Host is up, received user-set (0.20s latency).
Not shown: 89 filtered ports
Reason: 89 no-responses
```

PORT	STATE	SERVICE	REASON	VERSION
21/tcp	open	ftp	syn-ack	Pure-FTPd
22/tcp	open	ssh	syn-ack	OpenSSH 5.3 (protocol 2.0)
25/tcp	open	smtp	syn-ack	Exim smtpd 4.80
26/tcp	open	smtp	syn-ack	Exim smtpd 4.80
80/tcp	open	http	syn-ack	
110/tcp	open	pop3	syn-ack	Dovecot pop3d
143/tcp	open	imap	syn-ack	Dovecot imapd
443/tcp	open	ssl/http	syn-ack	Apache
465/tcp	open	ssl/smtp	syn-ack	Exim smtpd 4.80
993/tcp	open	ssl/imap	syn-ack	Dovecot imapd
995/tcp	open	ssl/pop3	syn-ack	Dovecot pop3d

```
Service Info: Hosts: example.com
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 131.38 seconds
```

Фрагмент результата сканирования алгоритмов, поддерживаемых SSL / HTTP - службой на порту 443

```
PORT      STATE SERVICE REASON
443/tcp   open  https  syn-ack
|  ssl-enum-ciphers:
|    TLSv1.0:
|      ciphers:
|        TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|        TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|        TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|        TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|        TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
|        TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
|        TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|        TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (secp256r1) - C
|        TLS_ECDHE_RSA_WITH_RC4_128_SHA (secp256r1) - C
|        TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
|        TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
|      compressors:
|        NULL
|      cipher preference: server
|      warnings:
|        64-bit block cipher 3DES vulnerable to SWEET32 attack
|        Broken cipher RC4 is deprecated by RFC 7465
|        Ciphersuite uses MD5 for message integrity
|        Weak certificate signature: SHA1
```

БЛАГОДАРЮ ЗА ВНИМАНИЕ!