

Практическая работа «Поиск уязвимостей в CMS (системе управления контентом) сайта аэропорта Сокол, г. Магадан»

Выполнил студент 1-го курса группы
Кибербезопасность (09.04.01 информатика и вычислительная техника)

Чейвелхут Анатолий Васильевич.

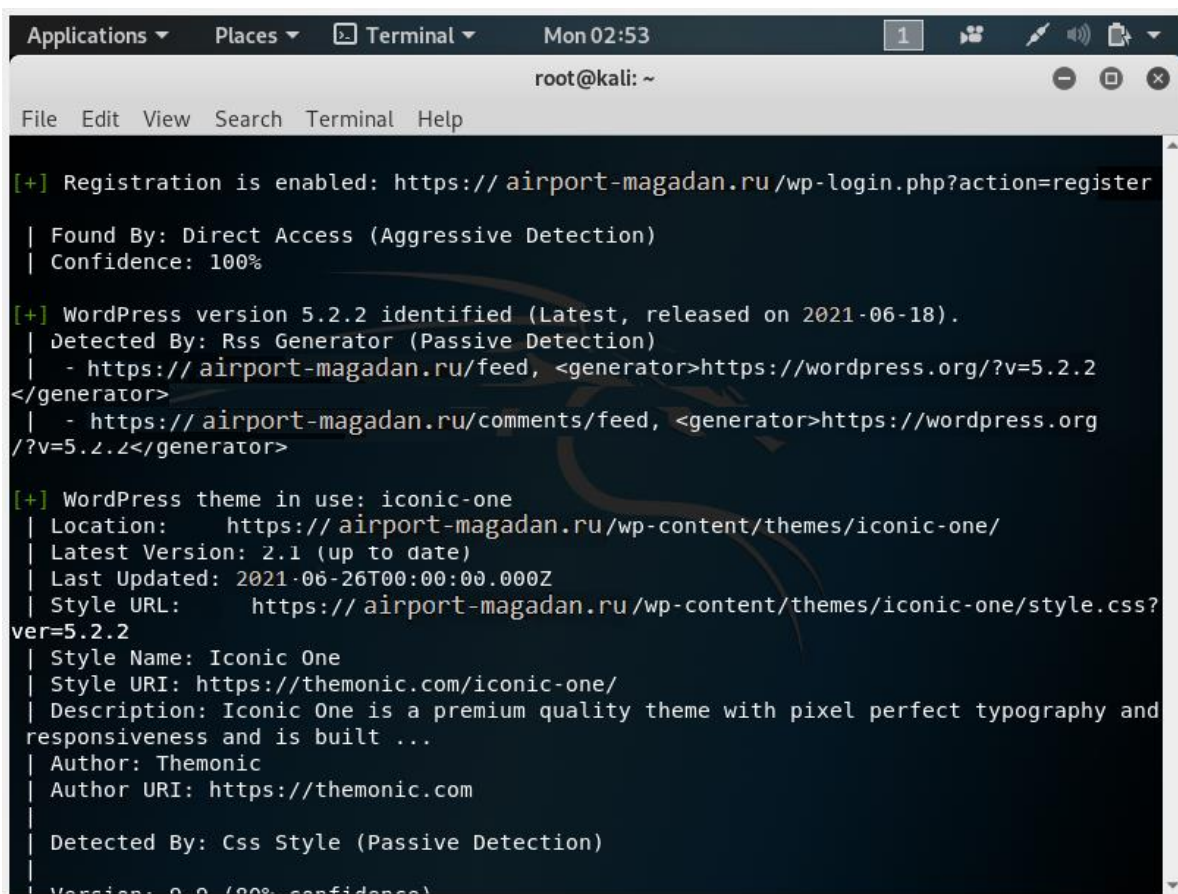
Руководитель практики: Зотов Сергей Сергеевич

Описание инструментов реализации практического задания

Для поиска уязвимостей была использована программа KaliLinux, установленная на виртуальной машине VirtualBox. Так как в ходе поверхностного анализа сайта было определено, что движок сайта написан с помощью WordPress, соответственно для анализа уязвимостей был использован WPScan. Эта программа может определить старые версии WordPress, тему оформления, установленные плагины, показать известные уязвимости в плагинах и темах оформления WordPress.

Пошаговое описание реализации задания

- 1) В первую очередь необходимо обновить инструменты WPScan (иначе некоторые инструменты могут быть неактуальными): `wpscan --update`
- 2) Затем проверить систему управления сайтом (CMS) airport-magadan.ru, для этого в консоли KaliLinux печатаем следующую команду: `wpscan --url airport-magadan.ru -e p,v,t,u`



```
Applications ▾ Places ▾ Terminal ▾ Mon 02:53 1
root@kali: ~
File Edit View Search Terminal Help

[+] Registration is enabled: https://airport-magadan.ru/wp-login.php?action=register
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] WordPress version 5.2.2 identified (Latest, released on 2021-06-18).
| Detected By: Rss Generator (Passive Detection)
| - https://airport-magadan.ru/feed, <generator>https://wordpress.org/?v=5.2.2
</generator>
| - https://airport-magadan.ru/comments/feed, <generator>https://wordpress.org
/?v=5.2.2</generator>

[+] WordPress theme in use: iconic-one
| Location: https://airport-magadan.ru/wp-content/themes/iconic-one/
| Latest Version: 2.1 (up to date)
| Last Updated: 2021-06-26T00:00:00.000Z
| Style URL: https://airport-magadan.ru/wp-content/themes/iconic-one/style.css?
ver=5.2.2
| Style Name: Iconic One
| Style URI: https://themonic.com/iconic-one/
| Description: Iconic One is a premium quality theme with pixel perfect typography and
responsiveness and is built ...
| Author: Themonic
| Author URI: https://themonic.com
|
| Detected By: Css Style (Passive Detection)
|
| Version: 0.0 (00% confidence)
```

Найдено много уязвимостей в установленных плагинах WordPress:

```
Applications ▾ Places ▾ Terminal ▾ Mon 02:54 1
root@kali: ~
File Edit View Search Terminal Help

[+] gd-bbpress-attachments
/
| Latest Version: 3.1
| Last Updated: 2021-03-10T18:50:00.000Z
|
| Detected By: Urls In Homepage (Passive Detection)
|
| [!] 3 vulnerabilities identified:
|
| [!] Title: GD bbPress Attachments <= 2.2 - Local File Inclusion
| Fixed in: 2.3
| References:
|   - https://wpvulndb.com/vulnerabilities/8087
|   - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5482
|   - https://security.dxw.com/advisories/local-file-include-vulnerability-in-gd-bb
| press-attachments-allows-attackers-to-include-arbitrary-php-files/
|   - http://packetstormsecurity.com/files/132656/
|
| [!] Title: GD bbPress Attachments <= 2.2 - Authenticated Reflected Cross-Site Script
| ing (XSS)
| Fixed in: 2.3
| References:
|   - https://wpvulndb.com/vulnerabilities/8088
|   - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5481
|   - https://security.dxw.com/advisories/reflected-xss-in-gd-bbpress-attachments-a
| llows-an-attacker-to-do-almost-everything-an-admin-can/
|   - http://packetstormsecurity.com/files/132657/
```

```
Applications ▾ Places ▾ Terminal ▾ Mon 02:54 1
root@kali: ~
File Edit View Search Terminal Help

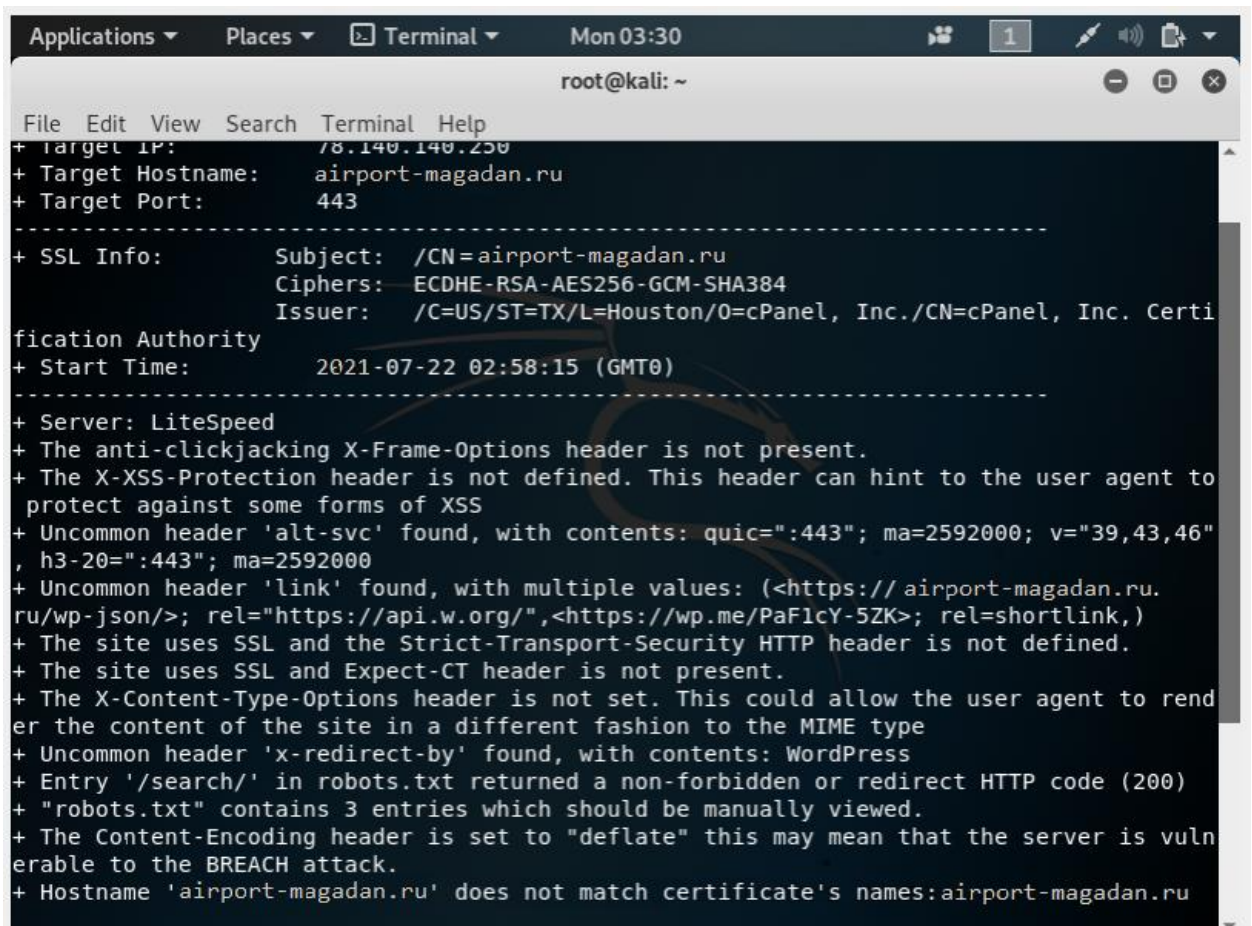
[+] simple-ads-manager
| Latest Version: 2.9.8.125
| Last Updated: 2021-05-03T19:28:00.000Z
|
| Detected By: Urls In Homepage (Passive Detection)
|
| [!] 4 vulnerabilities identified:
|
| [!] Title: Simple Ads Manager <= 2.5.94 - Arbitrary File Upload & SQL Injection
| Fixed in: 2.7.102
| References:
|   - https://wpvulndb.com/vulnerabilities/7882
|   - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2824
|   - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2825
|   - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2826
|   - https://www.exploit-db.com/exploits/36613/
|   - https://www.exploit-db.com/exploits/36614/
|   - https://www.exploit-db.com/exploits/36615/
|   - http://seclists.org/bugtraq/2015/Apr/10
|   - http://packetstormsecurity.com/files/131280/
|   - http://packetstormsecurity.com/files/131281/
|   - http://packetstormsecurity.com/files/131282/
|
| [!] Title: Simple Ads Manager <= 2.9.3.114 - Unauthenticated Denial of Service (DoS)
| Fixed in: 2.9.4.116
| References:
|   - https://wpvulndb.com/vulnerabilities/8060
```

Использование Nikto для оценки и сканирования дефолтных и небезопасных файлов, конфигураций и программ на веб-серверах любого типа

Для сканирования сайта запустим в консоли команду

```
nikto -h https://www.forum.comp-web-pro.ru/
```

Показываемая информация может говорить как о серьезных ошибках, так и о менее важных недочетах (например, не установлены заголовки безопасности HTTP протокола)

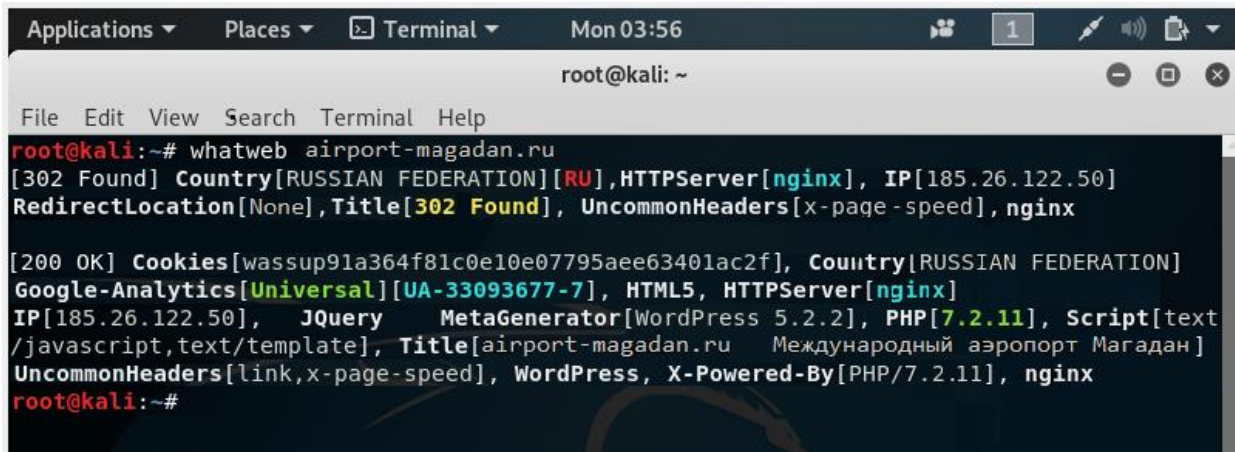


```
Applications ▾ Places ▾ Terminal ▾ Mon 03:30
root@kali: ~
File Edit View Search Terminal Help
+ Target IP: 78.140.140.250
+ Target Hostname: airport-magadan.ru
+ Target Port: 443
-----
+ SSL Info: Subject: /CN=airport-magadan.ru
Ciphers: ECDHE-RSA-AES256-GCM-SHA384
Issuer: /C=US/ST=TX/L=Houston/O=cPanel, Inc./CN=cPanel, Inc. Certi
fication Authority
+ Start Time: 2021-07-22 02:58:15 (GMT0)
-----
+ Server: LiteSpeed
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to
protect against some forms of XSS
+ Uncommon header 'alt-svc' found, with contents: quic=":443"; ma=2592000; v="39,43,46"
, h3-20=":443"; ma=2592000
+ Uncommon header 'link' found, with multiple values: (<https://airport-magadan.ru.
ru/wp-json/>; rel="https://api.w.org/",<https://wp.me/PaFlcY-5ZK>; rel=shortlink,)
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to rend
er the content of the site in a different fashion to the MIME type
+ Uncommon header 'x-redirect-by' found, with contents: WordPress
+ Entry '/search/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ "robots.txt" contains 3 entries which should be manually viewed.
+ The Content-Encoding header is set to "deflate" this may mean that the server is vuln
erable to the BREACH attack.
+ Hostname 'airport-magadan.ru' does not match certificate's names:airport-magadan.ru
```


Сбор информации об используемых веб-технологиях

Для сбора информации будет использована команда WhatWeb:

```
whatweb airport-magadan.ru
```



```
Applications ▾ Places ▾ Terminal ▾ Mon 03:56
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# whatweb airport-magadan.ru
[302 Found] Country[RUSSIAN FEDERATION][RU],HTTPServer[nginx], IP[185.26.122.50]
RedirectLocation[None],Title[302 Found], UncommonHeaders[x-page-speed], nginx

[200 OK] Cookies[wassup91a364f81c0e10e07795aee63401ac2f], Country[RUSSIAN FEDERATION]
Google-Analytics[Universal][UA-33093677-7], HTML5, HTTPServer[nginx]
IP[185.26.122.50], JQuery MetaGenerator[WordPress 5.2.2], PHP[7.2.11], Script[text
/javascript,text/template], Title[airport-magadan.ru Международный аэропорт Магадан]
UncommonHeaders[link,x-page-speed], WordPress, X-Powered-By[PHP/7.2.11], nginx
root@kali:~#
```

Как видно из результатов сканирования сайта сертификаты шифрования устарели. Пользователи, использующие учетные записи сайта через зараженные WI-FI, могут невольно передать свои данные злоумышленнику.

Оценка полученных результатов

Сайт аэропорта Сокол не является критически важным объектом инфраструктуры, т.к. является обычным информационным сайтом для пассажиров и не содержит в себе конфиденциальной информации, от которой зависит работоспособность всего предприятия. Однако с учебной точки зрения были отработаны навыки по поиску уязвимостей сайта. В итоге необходимо выделить следующие моменты:

- 1) Программное обеспечение в системе управления сайта необходимо постоянно обновлять, т.к. в старом программном обеспечении при желании легко эксплуатировать уязвимости, например есть специализированная для этого программа Metasploit.
- 2) На сайте используется протокол HTTP, однако более безопасным является HTTPS. Это создает потенциальную угрозу для кражи данных через зараженные WI-FI сети.