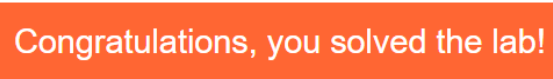


Here is the content of phpinfo.php:

```
576 <tr class="n"><td>Zlib Support</td><td>enabled</td></tr>
577 <tr><td class="e">Stream Wrapper </td><td class="v">compress.zlib:// </td></tr>
578 <tr><td class="e">HTTP SEC_FETCH_USER </td><td class="v">zlib.inflate, zlib.deflate </td></tr>
579 <tr><td class="e">Compiled Version </td><td class="v">1.2.11 </td></tr>
580 <tr><td class="e">Linked Version </td><td class="v">1.2.11 </td></tr>
581 </table>
582 <table>
583 <tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
584 <tr><td class="e">zlib.output_compression</td><td class="v">Off</td><td class="v">Off</td></tr>
585 <tr><td class="e">zlib.output_compression_level</td><td class="v">-1</td><td class="v">-1</td></tr>
586 <tr><td class="e">zlib.output_handler</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
587 </table>
588 <h2>Additional Modules</h2>
589 <table>
590 <tr class="h"><th>Module Name</th></tr>
591 </table>
592 <h2>Environment</h2>
593 <table>
594 <tr class="h"><th>Variable</th><th>Value</th></tr>
595 <tr><td class="e">GATEWAY_INTERFACE </td><td class="v">CGI/1.1 </td></tr>
596 <tr><td class="e">SUPO_ID </td><td class="v">10000 </td></tr>
597 <tr><td class="e">REMOTE_HOST </td><td class="v">194.29.137.21 </td></tr>
598 <tr><td class="e">USER </td><td class="v">carlos </td></tr>
599 <tr><td class="e">HTTP_SEC_CH-UA </td><td class="v">Not A Brand&quot;;v=&quot;8&quot;; &quot;;Chromium&quot;;v=&quot;120&quot;; </td></tr>
600 <tr><td class="e">SECRET_KEY </td><td class="v">bq4fqtnkrqt2cs1d0ys6rdsxm4fzsb1 </td></tr>
601 <tr><td class="e">HTTP_SEC_CH-UA_PLATFORM </td><td class="v">?1 </td></tr>
602 <tr><td class="e">QUERY_STRING </td><td class="v"><i>no value</i> </td></tr>
603 <tr><td class="e">HOME </td><td class="v">/home/carlos </td></tr>
604 <tr><td class="e">HTTP_USER_AGENT </td><td class="v">Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.199 Safari/537.36 </td></tr>
605 <tr><td class="e">HTTP_SEC_CH-UA_PLATFORM </td><td class="v">&quot;;Windows&quot;; </td></tr>
606 <tr><td class="e">HTTP_UPGRADE_INSECURE_REQUESTS </td><td class="v">1 </td></tr>
607 <tr><td class="e">HTTP_ACCEPT </td><td class="v">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 </td></tr>
608 <tr><td class="e">SCRIPT_FILENAME </td><td class="v">/home/carlos/cgi-bin/phpinfo.php </td></tr>
609 <tr><td class="e">HTTP_HOST </td><td class="v">0ac6002b0320a8b0808062b7e0000009e.web-security-academy.net </td></tr>
610 <tr><td class="e">SUPO_ID </td><td class="v">10000 </td></tr>
611 <tr><td class="e">LOGNAME </td><td class="v">carlos </td></tr>
612 <tr><td class="e">SERVER_SOFTWARE </td><td class="v">PortSwiggerHttpServer/1.0 </td></tr>
613 <tr><td class="e">HTTP_SEC_FETCH_MODE </td><td class="v">navigate </td></tr>
614 <tr><td class="e">TERM </td><td class="v">unknown </td></tr>
615 <tr><td class="e">HTTP_COOKIE </td><td class="v">session=KjkZaUG2PCHMghRZ0WxRLttCHG8o5 </td></tr>
616 <tr><td class="e">PATH </td><td class="v">/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin/snap/bin </td></tr>
617 <tr><td class="e">HTTP_ACCEPT_LANGUAGE </td><td class="v">en-US,en;q=0.9 </td></tr>
618 <tr><td class="e">SERVER_PROTOCOL </td><td class="v">HTTP/1.1 </td></tr>
619 <tr><td class="e">HTTP_PRIORITY </td><td class="v">u=0, i </td></tr>
620 <tr><td class="e">HTTP_ACCEPT_ENCODING </td><td class="v">gzip, deflate, br </td></tr>
621 <tr><td class="e">SUDO_COMMAND </td><td class="v">/usr/bin/sh -c /usr/bin/php-cgi </td></tr>
622 <tr><td class="e">SHELL </td><td class="v">/bin/bash </td></tr>
623 <tr><td class="e">BDTRFFFT_KTATIN </td><td class="v"><i>no value</i> </td></tr>
```

This file exposes a lot of information about environment variables that are used for debugging, including secret key:

bq4fqtnkrqt2cs1d0ys6rdsxm4fzsb1



LAB 58 [Source code disclosure via backup files](#)

Contents of robots.txt:

```
User-agent: *
Disallow: /backup
```

/backup keeps the backup file of the service, so the source code is free to read:

```
package data.productcatalog;

import common.db.JdbcConnectionBuilder;

import java.io.IOException;
import java.io.ObjectInputStream;
import java.io.Serializable;
import java.sql.Connection;
import java.sql.ResultSet;
import java.sql.SQLException;
import java.sql.Statement;

public class ProductTemplate implements Serializable
{
    static final long serialVersionUID = 1L;

    private final String id;
    private transient Product product;

    public ProductTemplate(String id)
    {
        this.id = id;
    }

    private void readObject(ObjectInputStream inputStream) throws IOException, ClassNotFoundException
    {
        inputStream.defaultReadObject();

        ConnectionBuilder connectionBuilder = ConnectionBuilder.from(
            "org.postgresql.Driver",
            "postgresql",
            "localhost",
            5432,
            "postgres",
            "postgres",
            "9rv10ndq157jt77ukama16srzhgl6s3"
        ).withAutoCommit();

        try
        {
            Connection connect = connectionBuilder.connect(30);
            String sql = String.format("SELECT * FROM products WHERE id = '%s' LIMIT 1", id);
            Statement statement = connect.createStatement();
            ResultSet resultSet = statement.executeQuery(sql);
            if (!resultSet.next())
            {
                return;
            }
            product = Product.from(resultSet);
        }
    }
}
```

Hard coded password from the database: 9rvl0ndq157jt77ukamal66srzhgl6s3

Congratulations, you solved the lab!

LAB 59 Authentication bypass via information disclosure

/admin contents:

Admin interface only available to local users

I have sent GET /admin request to Burp Repeater but changed HTTP GET with HTTP TRACE method and got a response successfully:

The screenshot displays the Burp Suite interface with a request and response for an HTTP TRACE method. The request is sent to the host 0af4003603c707a1857ec2a200a3000d.web-security-academy.net. The response is a 200 OK status with a Content-Type of message/http. The response body contains the raw HTTP request details, including the Host, Cookie, User-Agent, and Accept headers, confirming that the TRACE method successfully reflected the request back to the client.

X-Custom-IP-Authorization: 194.29.137.21

This header was appended to my request automatically and it is used to check whether the request came from localhost 127.0.0.1 request. Therefore, I can this header in match/replace rules to localhost IP and trick the host:

The screenshot shows the 'Match and replace rules' configuration window in Burp Suite. The 'Add match/replace rule' dialog is open, showing the configuration for a new rule. The 'Type' is set to 'Request header', the 'Match' is set to 'Regex condition to match - leave blank to add a new header', and the 'Replace' is set to 'X-Custom-IP-Authorization: 127.0.0.1'. The 'Comment' field is empty. The 'Regex match' checkbox is unchecked. The background shows the 'Match and replace rules' table with various rules for request and response headers.

Enabled	Item	Match	Replace	Type	Comment
<input type="checkbox"/>	Request header	^If-None-Match.*\$		Regex	Require non-cached respon...
<input type="checkbox"/>	Request header	^Referer.*\$		Regex	Hide Referer header
<input type="checkbox"/>	Request header	^Accept-Encoding.*\$		Regex	Require non-compressed re...
<input type="checkbox"/>	Response header	^Set-Cookie.*\$		Regex	Ignore cookies
<input type="checkbox"/>	Request header	^Host: foo.example.org\$	Host: bar.example.org	Regex	Rewrite Host header
<input type="checkbox"/>	Request header		Origin: foo.example.org	Literal	Add spoofed CORS origin
<input type="checkbox"/>	Response header	^Strict-Transport\-\Sec...		Regex	Remove HSTS headers
<input type="checkbox"/>	Response header		X-XSS-Protection: 0	Literal	Disable browser XSS protec...

Once done, I can see that Admin Panel is now available and list of users to delete is showed:

WebSecurity Academy

Authentication bypass via information disclosure

LAB Not solved

Back to lab description >>

Home | [Admin panel](#) | My account

WE LIKE TO SHOP

Users

wiener - [Delete](#)
carlos - [Delete](#)

Congratulations, you solved the lab!

LAB 60 [Information disclosure in version control history](#)

/.git contents:

Index of /.git

Name	Size
<branches>	
description	73B
<hooks>	
<info>	
<refs>	
HEAD	23B
config	157B
<objects>	
index	225B
COMMIT_EDITMSG	34B
<logs>	

I downloaded the repository with wget and started to inspect it from my Linux environment:

```
(urals@kali) - [~/0a4f001f032c32cd81b6cae300340006.web-security-academy.net/.git]
$ git log
commit 13609e3af68fdf17f19fb59fadd22da790d44ef8 (HEAD -> master)
Author: Carlos Montoya <carlos@carlos-montoya.net>
Date: Tue Jun 23 14:05:07 2020 +0000

    Remove admin password from config

commit c7e972229907f82bf22f7d3dd74783ee39ad7390
Author: Carlos Montoya <carlos@carlos-montoya.net>
Date: Mon Jun 22 16:23:42 2020 +0000

    Add skeleton admin panel

(urals@kali) - [~/0a4f001f032c32cd81b6cae300340006.web-security-academy.net/.git]
$
```

Above is contents of git logs: there is 2 commits. Their diff:

```
(urals@kali) - [~/0a4f001f032c32cd81b6cae300340006.web-security-academy.net/.git]
$ git diff c7e972229907f82bf22f7d3dd74783ee39ad7390 13609e3af68fdf17f19fb59fadd22da790d44ef8
diff --git a/admin.conf b/admin.conf
index 2c8a4c2..21d23f1 100644
--- a/admin.conf
+++ b/admin.conf
@@ -1,1 +1 @@
-ADMIN_PASSWORD=lvr7labhmfaz2zhx44rh6
+ADMIN_PASSWORD=env('ADMIN_PASSWORD')
```

As the message in log file said, the admin password was deleted from configuration file, and commits were done at admin.conf and I can find the password that was deleted (red log):

lvr7labhmfa2zhx44rh6

Let's try this:

Home | Admin panel | My account | Log out

My Account

Your username is: administrator

Email

Update email

Great! The log in was successful and Admin panel is now available:

Congratulations, you solved the lab!

User deleted successfully!

Users

wiener - Delete