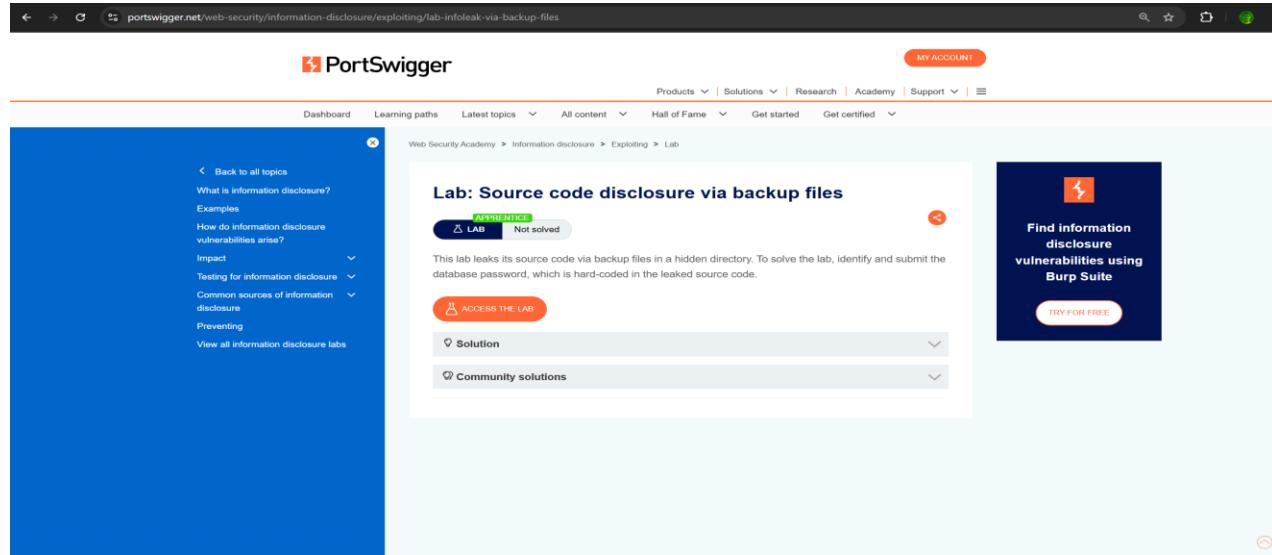


Lab 2: Information Disclosure Vulnerabilities

Source code disclosure via backup files

Description: This lab exposes its source code via backup files. An attacker can use these files to reveal sensitive information about the application's logic and configuration.

Objective: To solve the lab, identify and access the backup files in the hidden directory. Analyze the exposed source code to retrieve the hard-coded database password, then submit it to solve the lab.



1. Solution

1. Browse to `/robots.txt` and notice that it reveals the existence of a `/backup` directory. Browse to `/backup` to find the file `ProductTemplate.java.bak`. Alternatively, right-click on the lab in the site map and go to "Engagement tools" > "Discover content". Then, launch a content discovery session to discover the `/backup` directory and its contents.
2. Browse to `/backup/ProductTemplate.java.bak` to access the source code.
3. In the source code, notice that the connection builder contains the hard-coded password for a Postgres database.
4. Go back to the lab, click "Submit solution", and enter the database password to solve the lab.

2. Walkthrough / Proof of Concept

Step 1: Access the target application

- **Action:** Click the "Access the Lab" button to open the lab instance.
- **Observation:** The application is an e-commerce site titled "We Like To Shop".

The screenshot shows a web browser window with the URL `0ab300bd03b8eb6f816875b100530059.web-security-academy.net`. The page title is "WebSecurity Academy" with a red exclamation mark icon. Below it, a banner reads "Source code disclosure via backup files" with a "Submit solution" button and a link to "Back to lab description". A green "LAB" badge with "Not solved" and a refresh icon is visible. The main content area features a logo with the text "WE LIKE TO SHOP" and a hanger icon. Below the logo are four product cards: "Eggstastic, Fun, Food Eggssories" (rating 4.5/5, \$85.29), "ZZZZZZ Bed - Your New Home Office" (rating 3.5/5, \$68.94), "There Is No 'T' In Team" (rating 3.5/5, \$39.70), and "Hitch A Lift" (rating 4.5/5, \$16.42). Each card has a "View details" button. Below these are four more products: "Real Life Photoshopping" (rating 3.5/5, \$14.03), "Hydrated Crackers" (rating 4.5/5, \$44.17), "Six Pack Beer Belt" (rating 3.5/5, \$75.28), and "Com-Tool" (rating 3.5/5, \$26.68). Each of these also has a "View details" button.

Step 2: Reconnaissance via robots.txt

- **Action:** Append `/robots.txt` to the base URL to identify any paths hidden from search engine crawlers
- **Result:** The robots.txt file reveals a disallowed entry: `Disallow: /backup`. This indicates a potentially sensitive directory exists.

The screenshot shows a web browser window with the URL `0ab300bd03b8eb6f816875b100530059.web-security-academy.net/robots.txt`. The page displays the contents of the robots.txt file:
User-agent: *
Disallow: /backup

Step 3: Access the hidden directory

- **Action:** Navigated to the /backup directory identified in the robots.txt file.
- **Result:** The directory listing is enabled and exposes a backup source code file named ProductTemplate.java.bak.



Index of /backup

Name	Size
ProductTemplate.java.bak	1647B

Step 4: Analyze source code for sensitive data

- **Action:** Opened the ProductTemplate.java.bak file to review its content.
- **Result:** The file contains Java source code responsible for database connections (ConnectionBuilder). Upon inspection, a hard-coded database password was found in the connection string configuration.
- Extracted Data:
 - **User:** postgres
 - **Password:** lgeduby52fxafqtah57b2mmm2kyxjpv

```

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",
            "lgeduby52fjxafqtah57b2mmm2kyxjpv" <----->
        ).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);
        }
        catch (SQLException e)
        {
            throw new IOException(e);
        }
    }

    public String getId()
    {
        return id;
    }

    public Product getProduct()
    {
        return product;
    }
}

```

Step 5. Result / Conclusion

Submission:

- Action:** Clicked the "Submit solution" button and entered the database password extracted from the source code: lgeduby52fjxafqtah57b2mmm2kyxjpv.
- Result:** The application verified the password and marked the lab as "Solved". This confirms that the information leaked via the backup file was valid and critical.

The screenshot shows a web browser window for 'WebSecurity Academy'. The URL in the address bar is '0aa1008b0311b4858085586c0006005d.web-security-academy.net'. The page title is 'Source code disclosure via backup files'. A green button in the top right corner says 'LAB Solved' with a small icon. Below the title, there's a link 'Back to lab description >'. A prominent orange banner at the top says 'Congratulations, you solved the lab!'. To the right of the banner are links 'Share your skills!', 'Continue learning >', and 'Home'. The main content area features a large logo 'WE LIKE TO SHOP' with a hanger icon. Below the logo are eight product cards arranged in two rows of four. The products are:

- Caution Sign**: A yellow 'DANGER' sign with 'DIEPLY RECOMMENDED POO IN PROGRESS' written on it. Rating: ★★★★☆ \$61.69. [View details](#)
- Giant Grasshopper**: A black and white illustration of a giant grasshopper. Rating: ★★★★★ \$11.66. [View details](#)
- Photobomb Backdrops**: A photo of an older man with a shocked expression superimposed over a background of two cartoonish faces. Rating: ★★★★★ \$77.25. [View details](#)
- Hologram Stand In**: An image of a woman in a blue dress standing in a park-like setting. Rating: ★★★★☆ \$46.09. [View details](#)

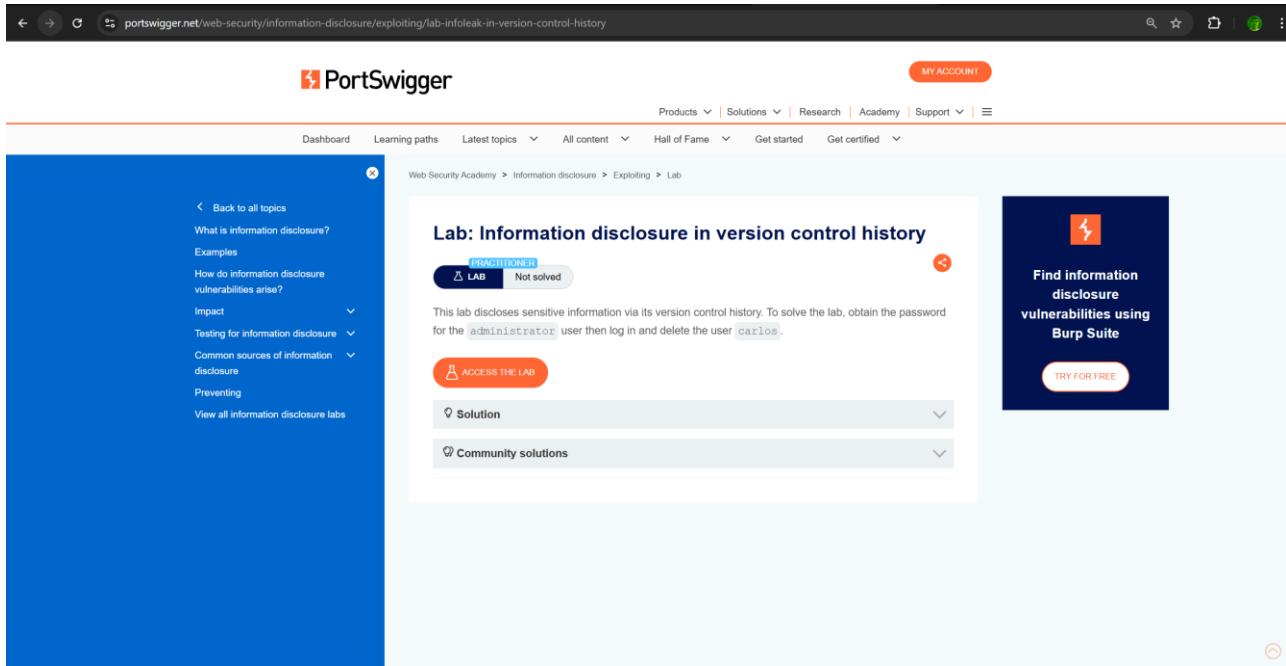
- Hitch A Lift**: Two people skydiving together. [View details](#)
- There is No 'I' in Team**: A team of people around a table with a 'TEAM' banner. [View details](#)
- More Than Just Birdsong**: A wire with musical notes and a treble clef. [View details](#)
- Real Life Photoshopping**: Various makeup and cosmetic products. [View details](#)

Information disclosure in version control history

Description: This lab discloses sensitive information via its version control history. The application is running a Git repository, and the .git directory has been left exposed.

Objective: To solve the lab, you must:

1. Download the exposed .git directory.
2. Analyze the Git history to find a commit that removed the administrator password.
3. Recover the password, log in as administrator, and delete the user carlos.



1. Solution

1. Open the lab and browse to `./.git` to reveal the lab's Git version control data.
2. Download a copy of this entire directory. For Linux users, the easiest way to do this is using the command:
`wget -r https://YOUR-LAB-ID.web-security-academy.net/.git/`
Windows users will need to find an alternative method, or install a UNIX-like environment, such as Cygwin, in order to use this command.
3. Explore the downloaded directory using your local Git installation. Notice that there is a commit with the message "Remove admin password from config".
4. Look closer at the diff for the changed `admin.conf` file. Notice that the commit replaced the hard-coded admin password with an environment variable `ADMIN_PASSWORD` instead. However, the hard-coded password is still clearly visible in the diff.
5. Go back to the lab and log in to the administrator account using the leaked password.
6. To solve the lab, open the admin interface and delete `carlos`.

2. Walkthrough / Proof of Concept

Step 1: Access the target application

- **Action:** Accessed the lab instance to view the main application.

- **Observation:** The application is an e-commerce site titled "We Like To Shop". At first glance, there are no obvious errors or leaks on the homepage.

Step 2: Reconnaissance via /.git

- **Action:** Appended /.git to the base URL to check for exposed version control directories.
- **Result:** The server returned a full directory listing of the .git folder, exposing critical repository metadata such as config, HEAD, and objects. This confirms the vulnerability.

Index of /.git

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

Step 3: Download the Git repository

- **Action:** Used the wget command in a terminal (Git Bash) to recursively download the entire exposed .git directory from the server to the local machine.
 - Command used: wget -r -np -nc <https://.../.git/>
- **Result:** The repository files (objects, refs, logs) were successfully downloaded.

```
main@DESKTOP-JRQSJOC MINGW64 ~/lab
$ wget -r -np -nc https://0a3b00a5038a6ba280d299b700110095.web-security-academy.net/.git/
--2025-12-31 23:08:51--  https://0a3b00a5038a6ba280d299b700110095.web-security-academy.net/.git/
[downloaded 369/369]
2025-12-31 23:09:35 (126 MB/s) - '0a3b00a5038a6ba280d299b700110095.web-security-academy.net/.git/logs/refs/heads/master' saved [369/369]
FINISHED --2025-12-31 23:09:35--
Total wall clock time: 44s
Downloaded: 47 files, 33K in 0s (99.7 MB/s)
```

Step 4: Analyze Git History

- **Action:** Navigated into the downloaded directory and executed the git log command to inspect the commit history.
- **Observation:** The log revealed a commit by author "Carlos Montoya" with a suspicious message: "*Remove admin password from config*".
- **Vulnerable Commit Hash:** 444c84370a2c3413ad78280b000d3e78d2eb0f1e

```
main@DESKTOP-JRQSJOC MINGW64 ~/lab
$ cd 0a3b00a5038a6ba280d299b700110095.web-security-academy.net

main@DESKTOP-JRQSJOC MINGW64 ~/lab/0a3b00a5038a6ba280d299b700110095.web-security-academy.net (master)
$ git log
commit 444c84370a2c3413ad78280b000d3e78d2eb0f1e (HEAD -> master)
Author: Carlos Montoya <carlos@carlos-montoya.net>
Date:   Tue Jun 23 14:05:07 2020 +0000

    Remove admin password from config

commit f4a314b7198c9d1dc9e2978555de176cb67c58a4
Author: Carlos Montoya <carlos@carlos-montoya.net>
Date:   Mon Jun 22 16:23:42 2020 +0000

    Add skeleton admin panel

main@DESKTOP-JRQSJOC MINGW64 ~/lab/0a3b00a5038a6ba280d299b700110095.web-security-academy.net (master)
$ |
```

Step 5: Recover the Password

- **Action:** Executed the git show command with the identified commit hash to view the specific changes made in that commit.
git show 444c84370a2c3413ad78280b000d3e78d2eb0f1e
- **Result:** The diff output displayed the admin.conf file changes. The line prefixed with a minus sign (-) revealed the hard-coded administrator password that was removed.
- Extracted Credentials:
 - **Username:** administrator
 - **Password:** onh1u8evabuoxy8ubw9

```

main@DESKTOP-JRQSJOC MINGW64 ~/lab/0a3b00a5038a6ba280d299b700110095.web-security-academy.net (master)
$ git show 444c84370a2c3413ad78280b000d3e78d2eb0f1e
commit 444c84370a2c3413ad78280b000d3e78d2eb0f1e (HEAD -> master)
Author: Carlos Montoya <carlos@carlos-montoya.net>
Date:   Tue Jun 23 14:05:07 2020 +0000

    Remove admin password from config

diff --git a/admin.conf b/admin.conf
index a9ba0d3..21d23f1 100644
--- a/admin.conf
+++ b/admin.conf
@@ -1 +1 @@
-ADMIN_PASSWORD=onh1u8evabuoxy8ubw9
+ADMIN_PASSWORD=env('ADMIN_PASSWORD')

main@DESKTOP-JRQSJOC MINGW64 ~/lab/0a3b00a5038a6ba280d299b700110095.web-security-academy.net (master)
$ |

```

Step 6: Exploitation & Conclusion

- Action:
 1. Logged into the application's "My account" page using the recovered credentials (administrator / onh1u8evabuoxy8ubw9).
 2. Navigated to the "Admin panel".
 3. Deleted the user carlos.
- **Result:** The user carlos was successfully deleted, and the lab was marked as "Solved".

The screenshot shows the WebSecurity Academy interface. At the top, there is a navigation bar with icons for back, forward, and search. The URL in the address bar is `0a3b00a5038a6ba280d299b700110095.web-security-academy.net/admin`. Below the address bar, the WebSecurity Academy logo is displayed. To the right of the logo, it says "Information disclosure in version control history" and "Back to lab description >". On the far right, there is a green button labeled "LAB Solved" with a checkmark icon. In the main content area, there is an orange banner at the top with the text "Congratulations, you solved the lab!". To the right of the banner are links for "Share your skills!" (with icons for Twitter and LinkedIn) and "Continue learning >". Below the banner, a message says "User deleted successfully!". The main content area has a heading "Users" and a sub-section "wiener - Delete". At the bottom right of the page, there are links for "Home | Admin panel | My account".