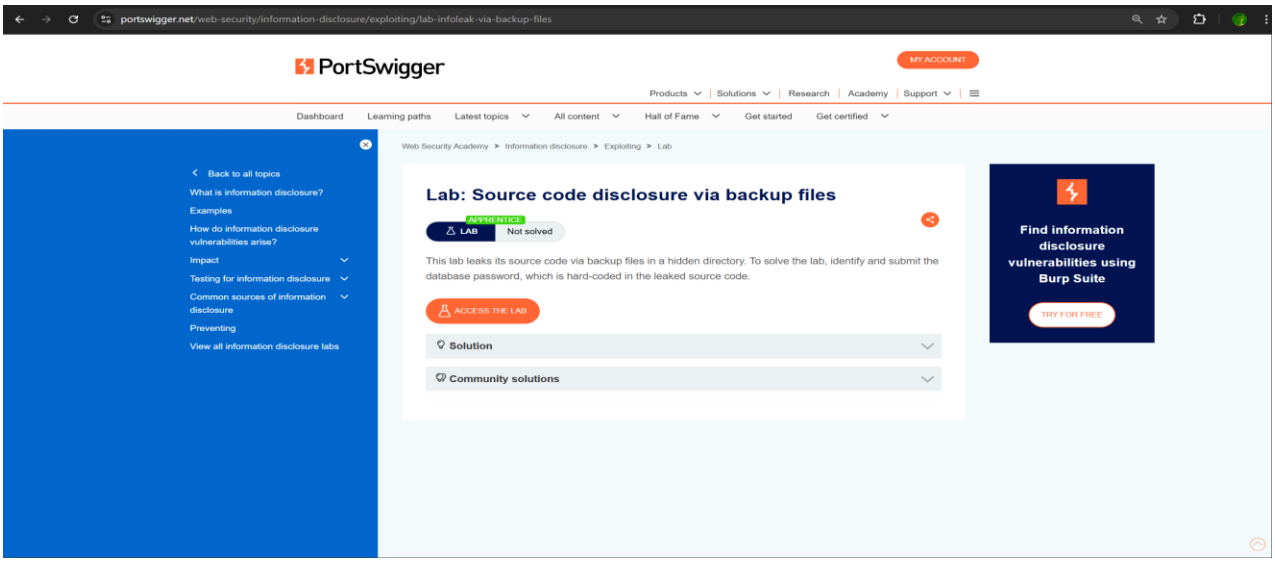
Lab 2: Information Disclosure Vulnerabilities

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

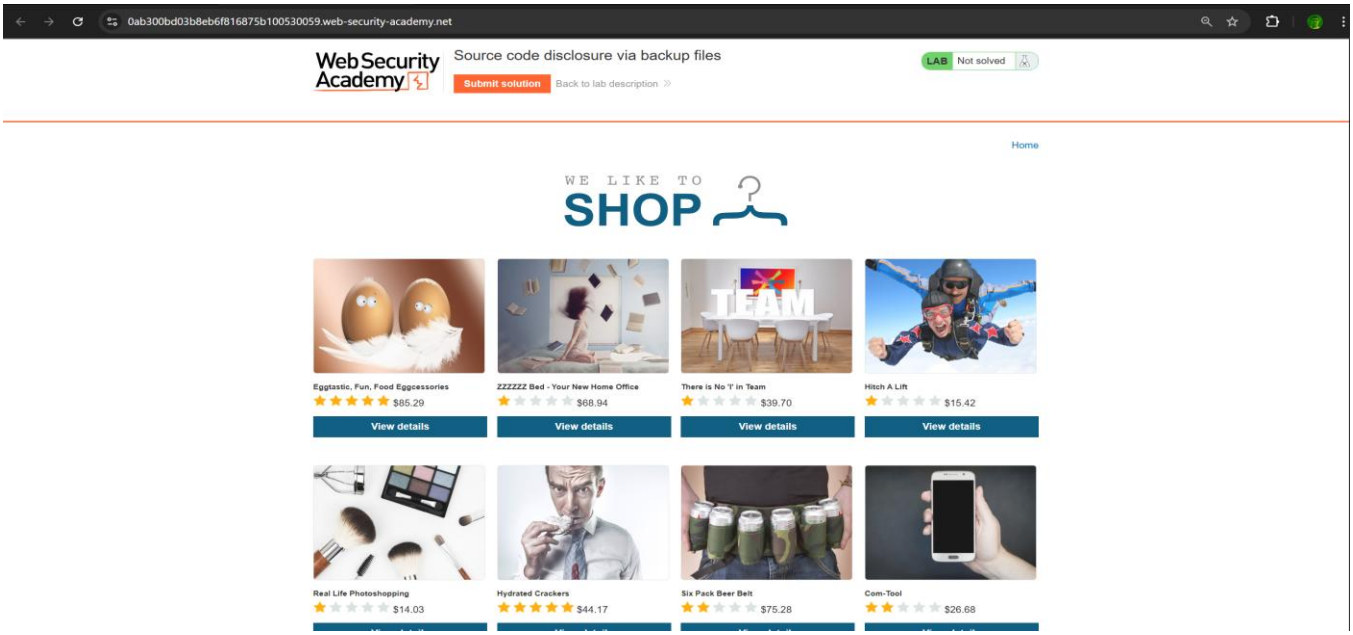
1. Browse to /robots.txt and notice that it reveals the existence of a /backup directory. Browse to /backup to find the file ProductTemplate.java.bak. Alternatively, right-click on the lab in the site map and go to "Engagement tools" > "Discover content". Then, launch a content discovery session to discover 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

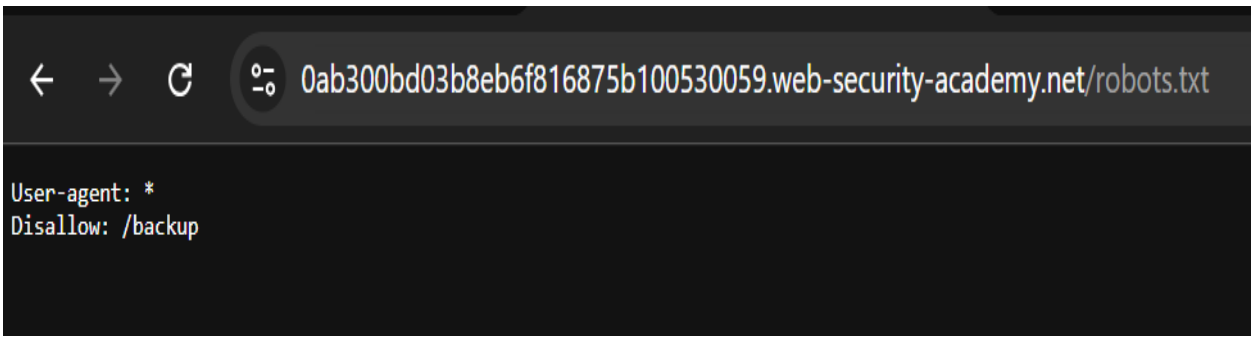
Step 1: Access the target application

- **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".



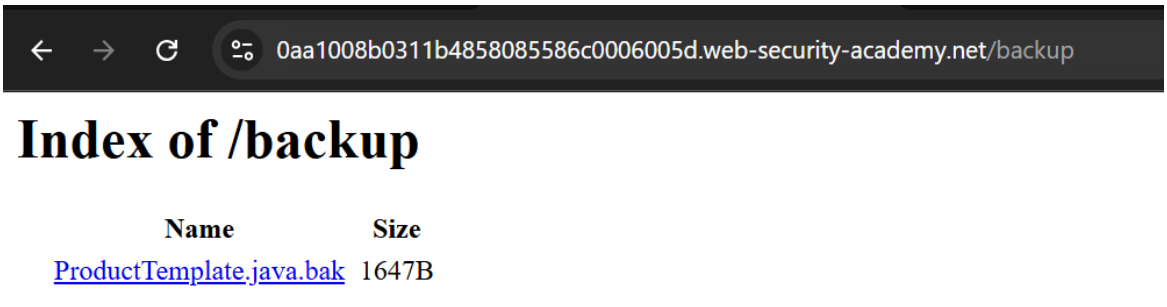
Step 2: Reconnaissance via robots.txt

- **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.



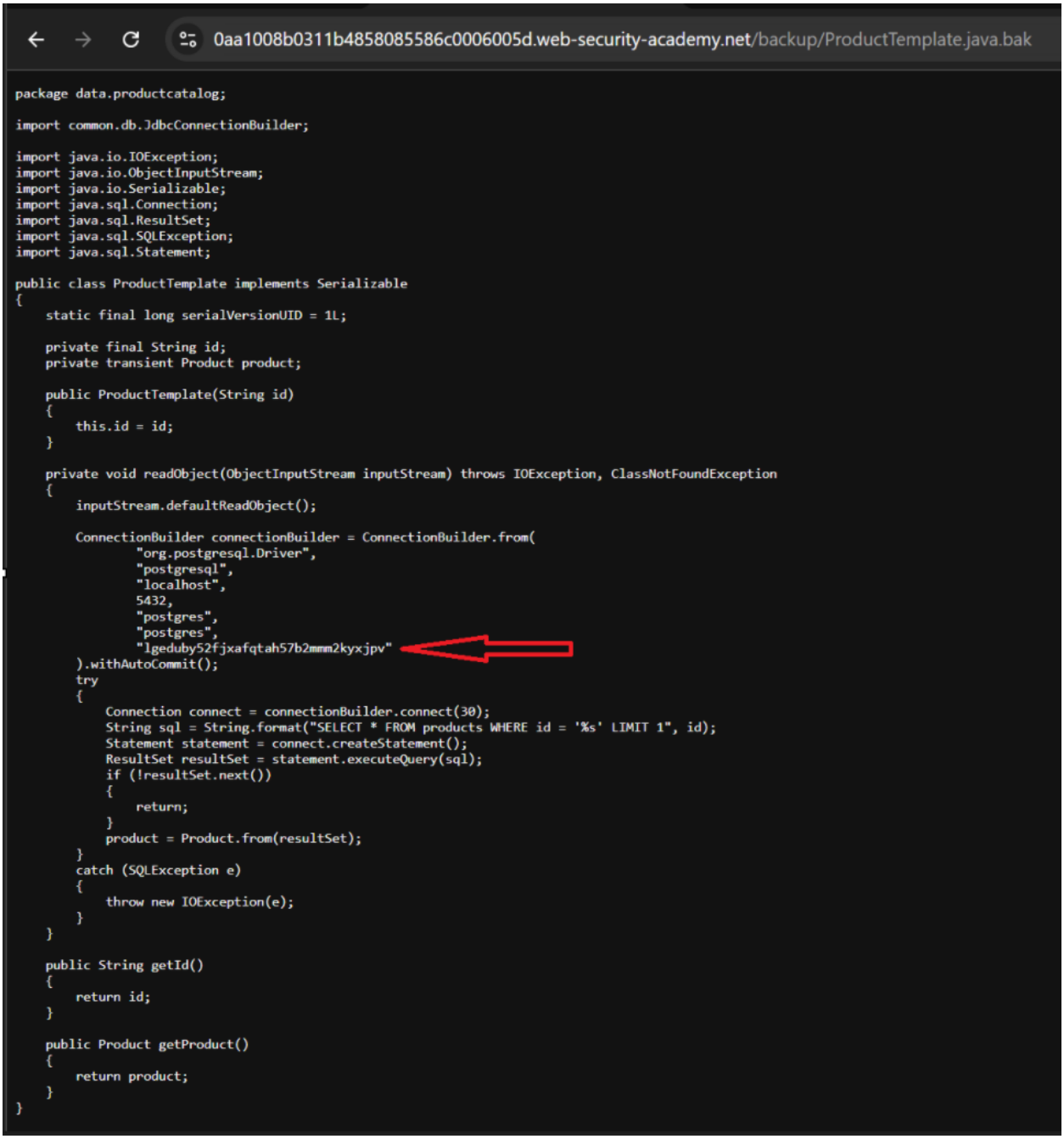
Step 3: Access the hidden directory

- **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.



Step 4: Analyze source code for sensitive data

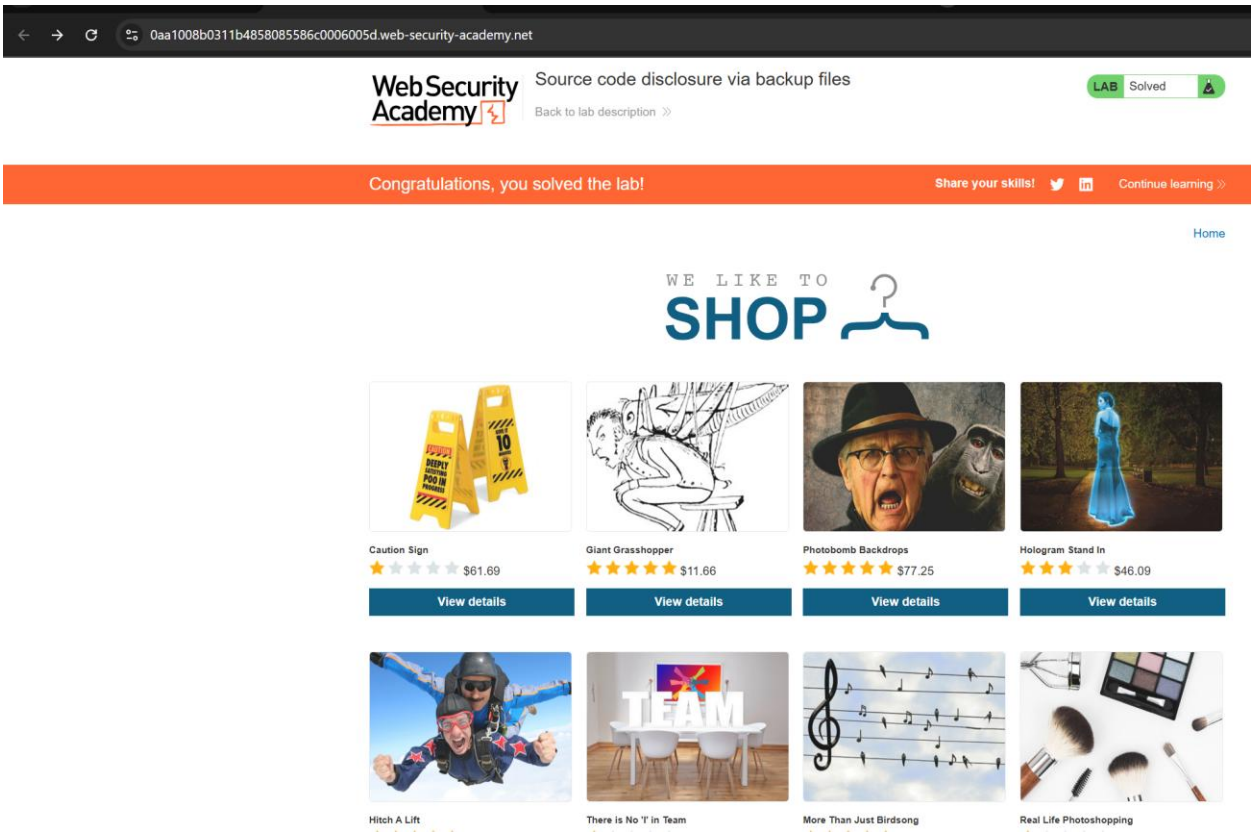
- **Action:** Opened the ProductTemplate.java.bak file to review its content.
- **Result:** The file contains Java source code responsible for database connections (ConnectionBuilder). Upon inspection, a hard-coded database password was found in the connection string configuration.
- Extracted Data:
    - **User:** postgres
    - **Password:** lgeduby52fjxafqtah57b2mmm2kyxjpv



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.

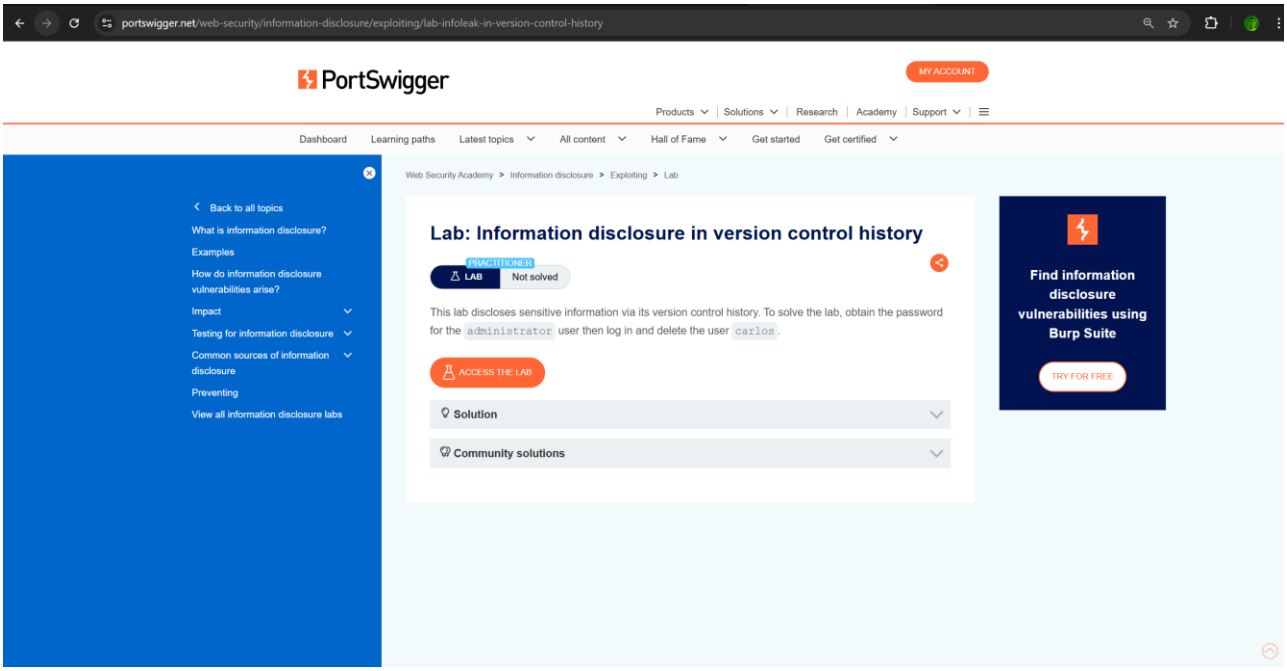


Information disclosure in version control history

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

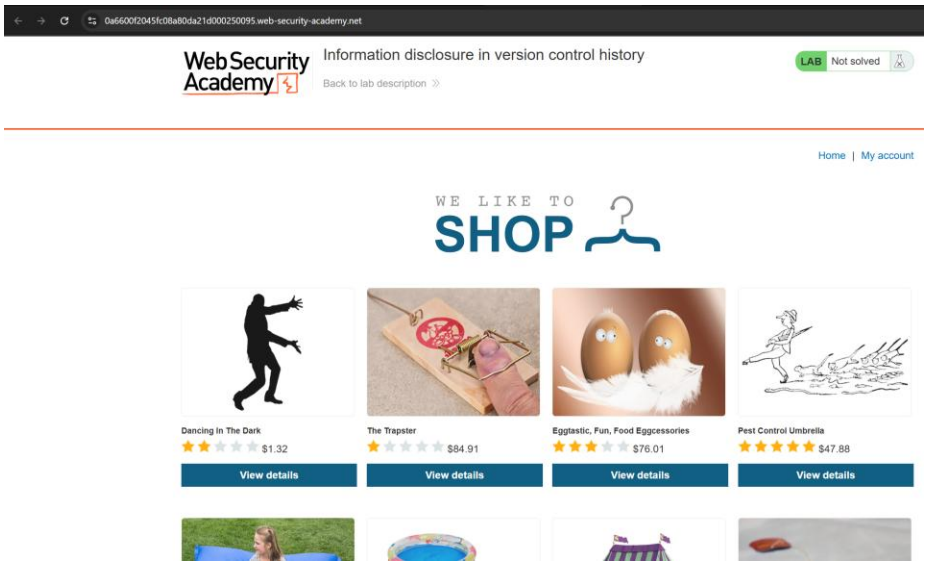
1. Open the lab and browse to /.git to reveal the lab's Git version control data.
2. Download a copy of this entire directory. For Linux users, the easiest way to do this is using the command:
   wget -r https://YOUR-LAB-ID.web-security-academy.net/.git/
   Windows users will need to find an alternative 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

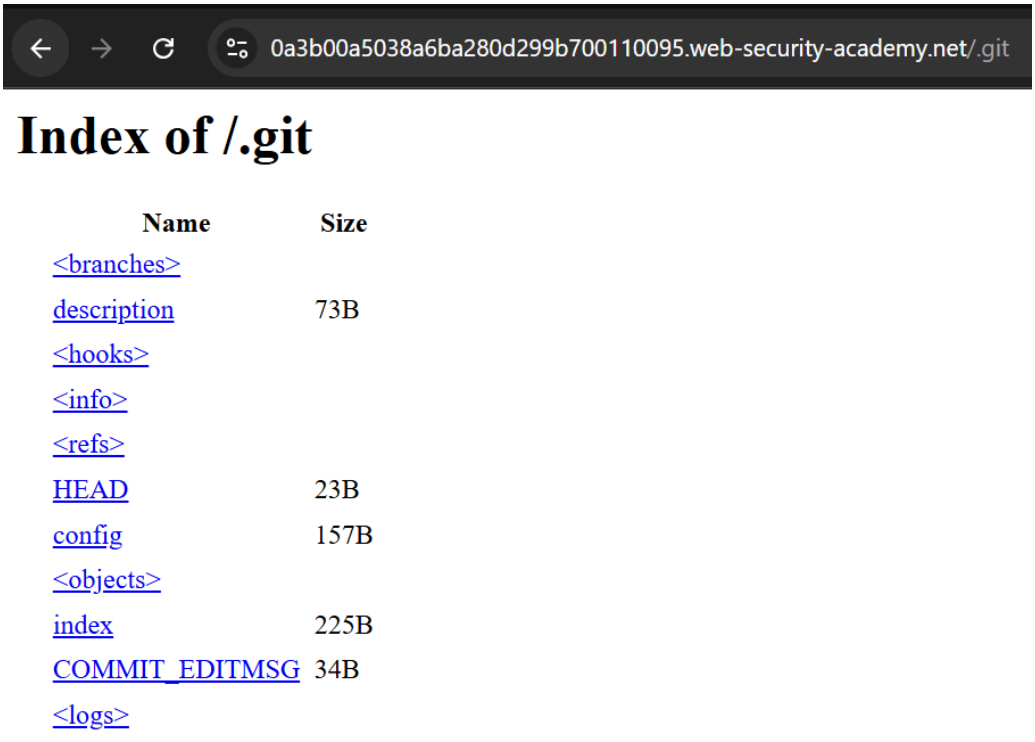
- **Action:** Accessed the lab instance to view the main application.

- **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.



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-JRQSJ0C MINGW64 ~/lab
$ wget -r -np -nc https://0a3b00a5038a6ba280d299b700110095.web-security-academy.
net/.git/
--2025-12-31 23:08:51--  https://0a3b00a5038a6ba280d299b700110095.web-security-a
cademy.net/.git/
```

```
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-JRQSJ0C MINGW64 ~/lab
$ cd 0a3b00a5038a6ba280d299b700110095.web-security-academy.net

main@DESKTOP-JRQSJ0C 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-JRQSJ0C 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:** onh1u8evabuoxpy8ubw9

```
main@DESKTOP-JRQSJ0C 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=onh1u8evabuoxpy8ubw9
+ADMIN_PASSWORD=env('ADMIN_PASSWORD')

main@DESKTOP-JRQSJ0C 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 / onh1u8evabuoxpy8ubw9).
    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".