Information Disclosure

Information disclosure, also known as information leakage, is when a website unintentionally reveals sensitive information to its users. Depending on the context, websites may leak all kinds of information to a potential attacker, including:

- Data about other users, such as usernames or financial information
- Sensitive commercial or business data
- Technical details about the website and its infrastructure

Some basic examples of information disclosure are as follows:

- Revealing the names of hidden directories, their structure, and their contents via a robots.txt file or directory listing
- Providing access to source code files via temporary backups
- Explicitly mentioning database table or column names in error messages
- Unnecessarily exposing highly sensitive information, such as credit card details
- Hard-coding API keys, IP addresses, database credentials, and so on in the source code
- Hinting at the existence or absence of resources, usernames, and so on via subtle differences in application behavior

Mitigations for Information Disclosure:

- Make sure that everyone involved in producing the website is fully aware of what information is considered sensitive.
- Audit any code for potential information disclosure as part of your QA or build processes.
- Use generic error messages as much as possible. Don't provide attackers with clues about application behavior unnecessarily.

- Double-check that any debugging or diagnostic features are disabled in the production environment.
- Make sure you fully understand the configuration settings, and security implications, of any third-party technology that you implement.

Common sources of Information Disclosure:

- Files for web crawlers (robots.txt and sitemap.xml)
- Directory listings
- Developer comments
- Error messages
- Debugging data
- User account pages
- Backup files
- Insecure configuration
- Version control history

★ Information Disclosure in Error Message: (Portswigger Labs)

Send burp proxy to repeater and change the url parameter

Eg. GET /product?productId=1 here, change the productID to non integer value

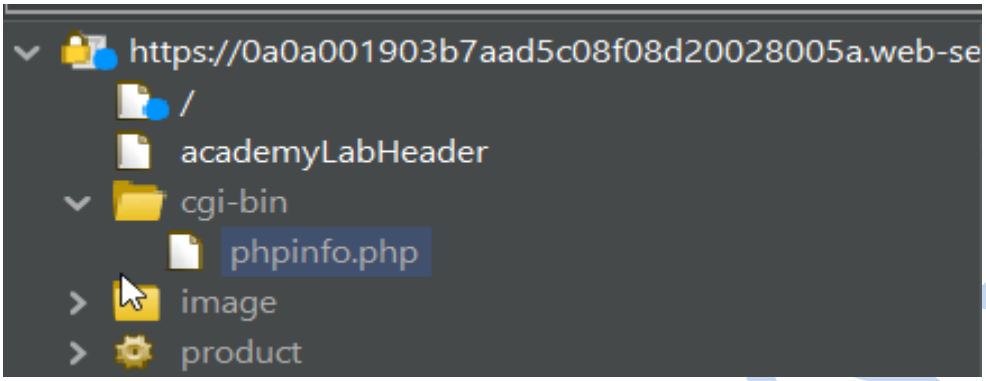
Eg. GET /product?productId=abcd HTTP/1.1 and check the response.

```
at lab.s.l.p(Unknown Source)
at lab.s.l.X(Unknown Source)
at lab.s.l.I(Unknown Source)
at m.k.e.u.p.m(Unknown Source)
at m.k.e.u.p.M(Unknown Source)
at m.k.e.u.p.run(Unknown Source)
at java.base/java.util.concurrent.ThreadPoolExec
at java.base/java.util.concurrent.ThreadPoolExec
at java.base/java.lang.Thread.run(Thread.java:83

Apache Struts 2 2.3.31
```

★ **Information Disclosure on Debug Page: (Portswigger Labs)**

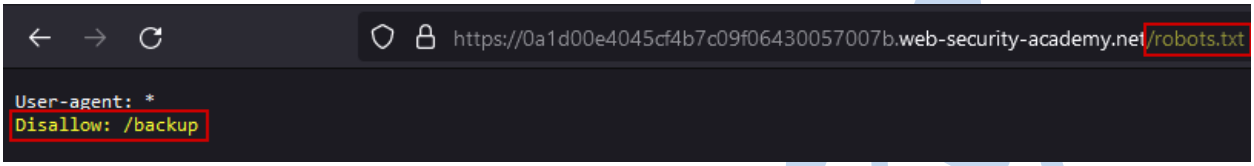
Go to target, and try to check for /cgi-bin/phpinfo.php file and then send it to the repeater and then check the response.

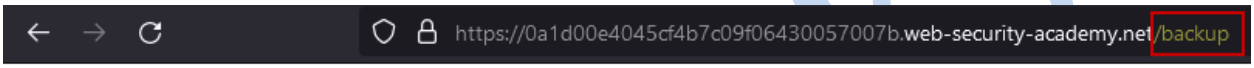



```
    </td>
  </tr>
  <tr>
    <td class="e">
      SECRET_KEY
    </td>
    <td class="v">
      zo8lk0fhogvs30jrbbbef58gyuoyxpcr
    </td>
  </tr>
  <tr>
    <td class="e">
```

★ Source Code Disclosure via Backup Files: (Portswigger Labs)

Browse to url/robots.txt , it reveals the existence of /backup directory. Then go to url/backup you'll find the file ProductTemplate.java.bak , Click on that file to access the source code. Here we find a hard-coded password for Postgres database.





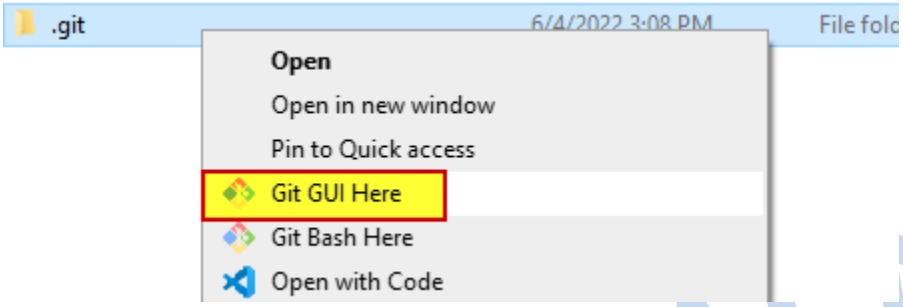

```
        ConnectionBuilder connectionBuilder = ConnectionBuilder.from(
                "org.postgresql.Driver",
                "postgresql",
                "localhost",
                5432,
                "postgres",
                "postgres",
                "icl9cbn95isr3v4ww1rpcim6cppvh1w0"
        ).withAutoCommit();
```

★ Information Disclosure in Version Control History: (Portswigger Labs)

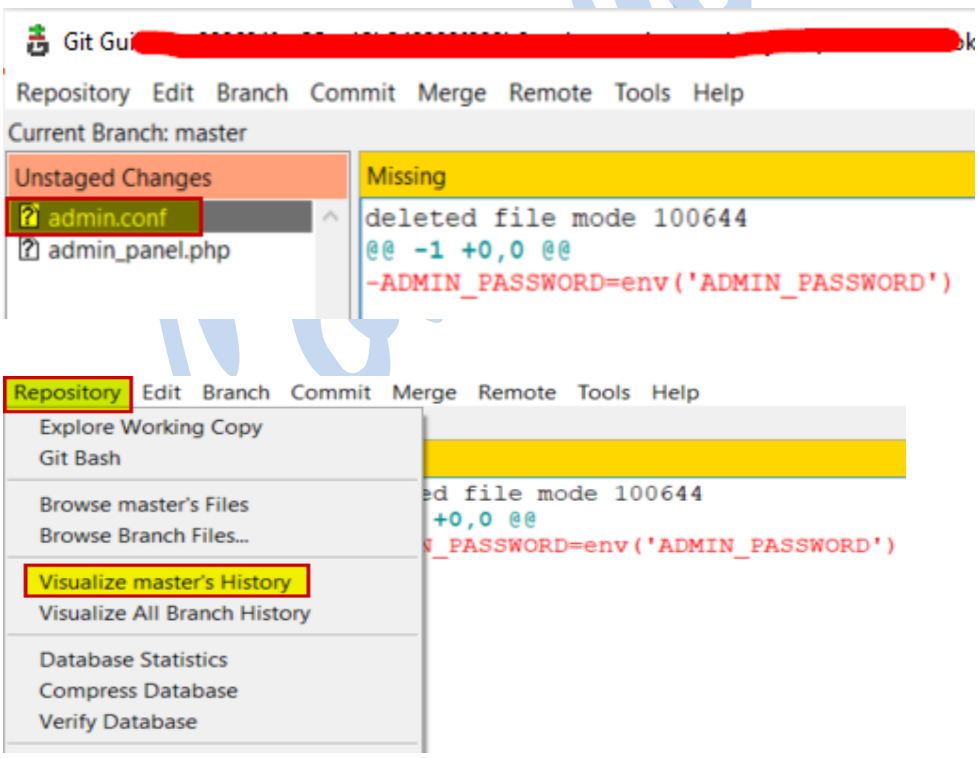
Open the url with /.git in the end. Download a copy of entire directory using the following command in cmd:

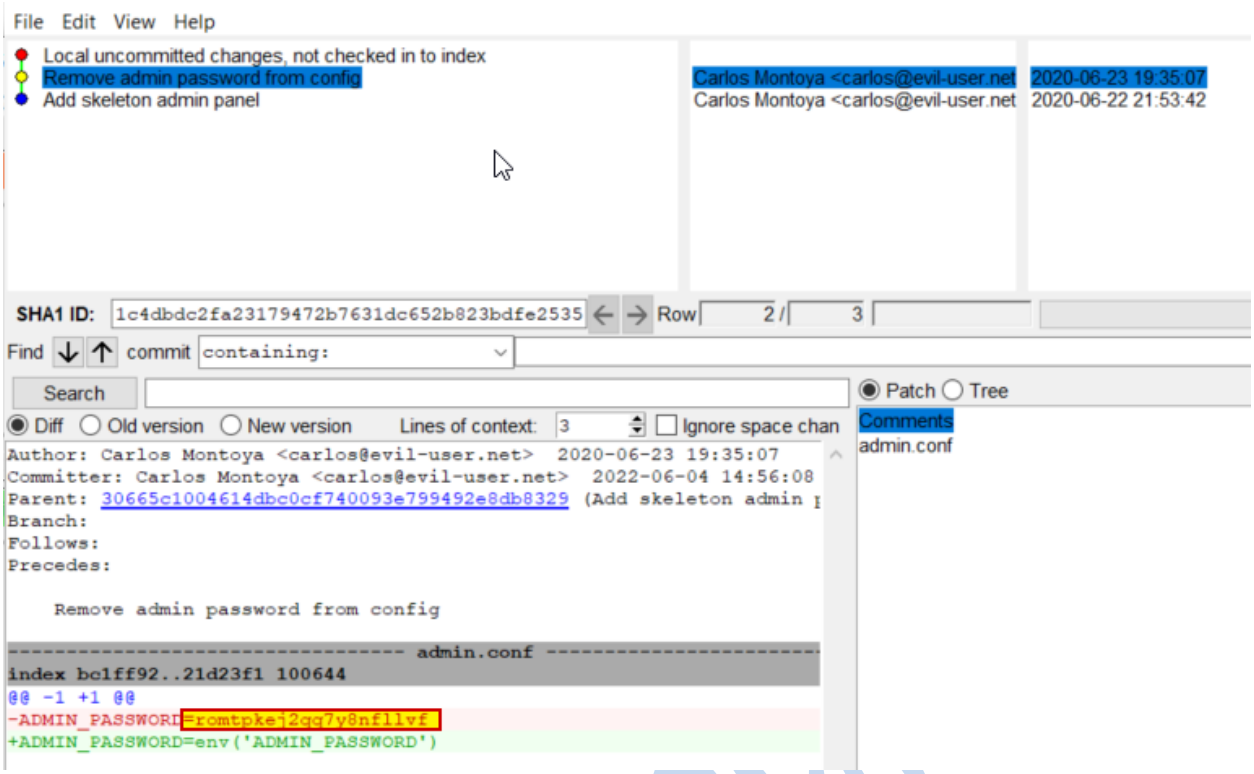
wget -r https://your-lab-id.web-security-academy.net/.git/

Then using file explorer in windows, go to the downloaded path, my path was the user folder, then open the folder, you'll find the .git folder inside it. Then right click on .git folder and select Git GUI Here



Then you'll find the admin.conf file. Click on admin.conf file the go to Repository option and click on Visualize Master's History .





These are some techniques you can try for Information Disclosure.