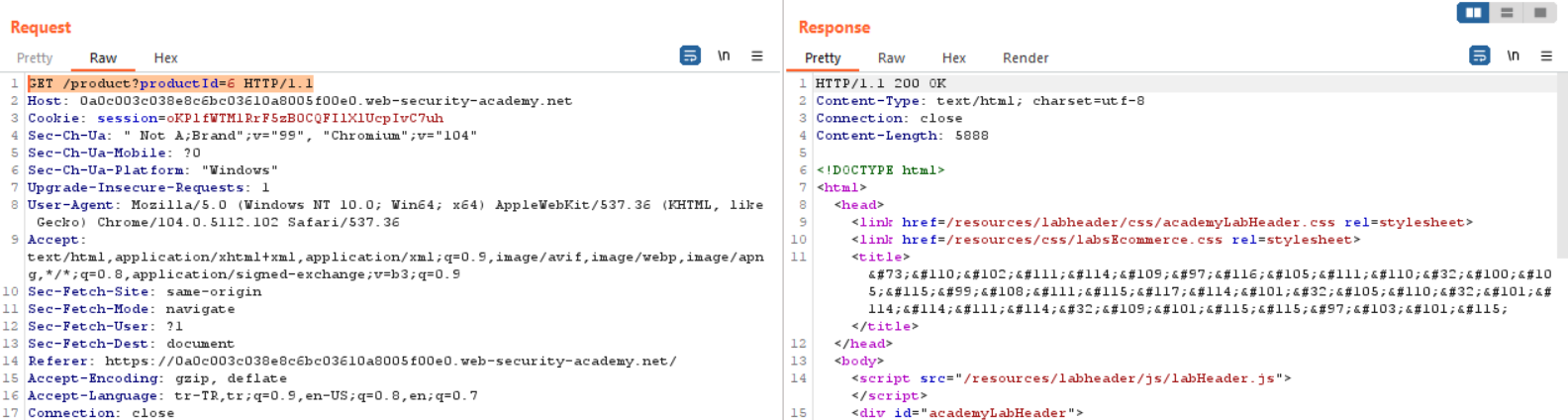
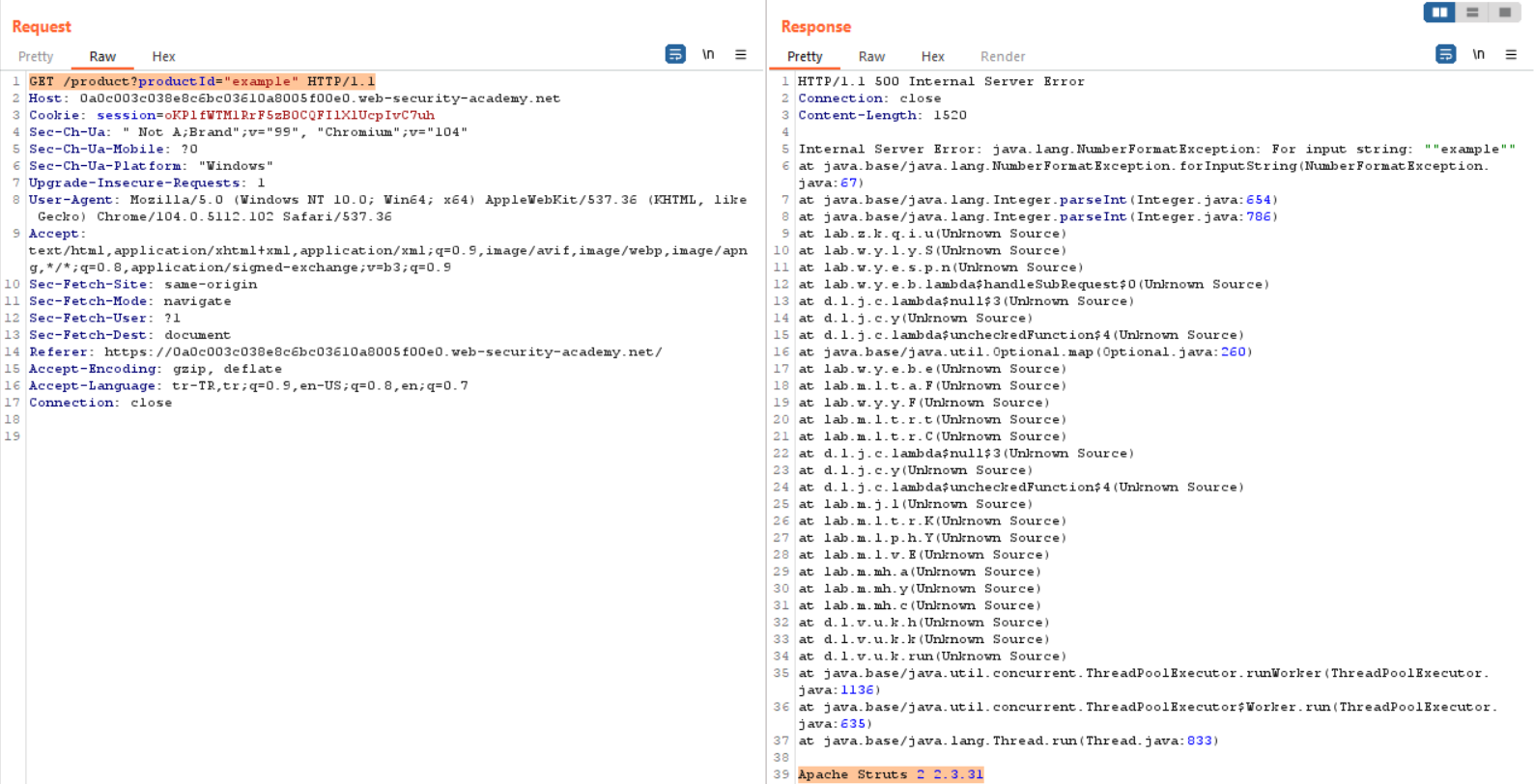
Lab: Information disclosure in error messages

GET /product?productId=2 HTTP/1.1

GET /product?productId=”example” HTTP/1.1

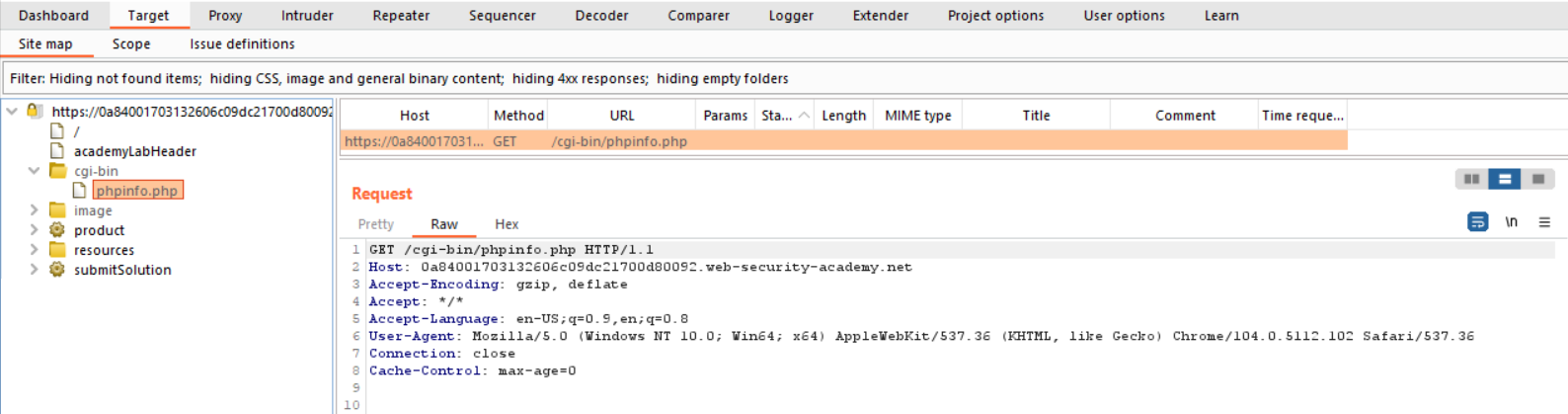


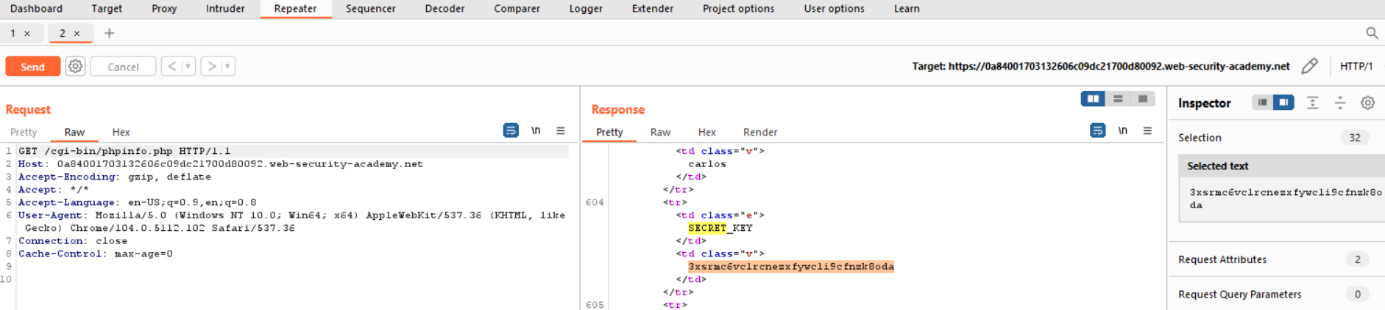


Lab: Information disclosure on debug page

**APPRENTICE**

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.





Lab: Source code disclosure via backup files

**APPRENTICE**

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.

Backup lı 2. Linkten source koda erişim var. Olmaması gereken bir durum yani.

https://0a200065030930c6c03a395d006e00c1.web-security-academy.net/

https://0a200065030930c6c03a395d006e00c1.web-security-academy.net/backup

https://0a200065030930c6c03a395d006e00c1.web-security-academy.net/backup/ProductTemplate.java.bak

**Lab 4: Authentication bypass via information disclosure**

APPRENTICE

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

**Solution**

1. In Burp Repeater, browse to GET /admin. The response discloses that the admin panel is only accessible if logged in as an administrator, or if requested from a local IP.
2. Send the request again, but this time use the TRACE method:

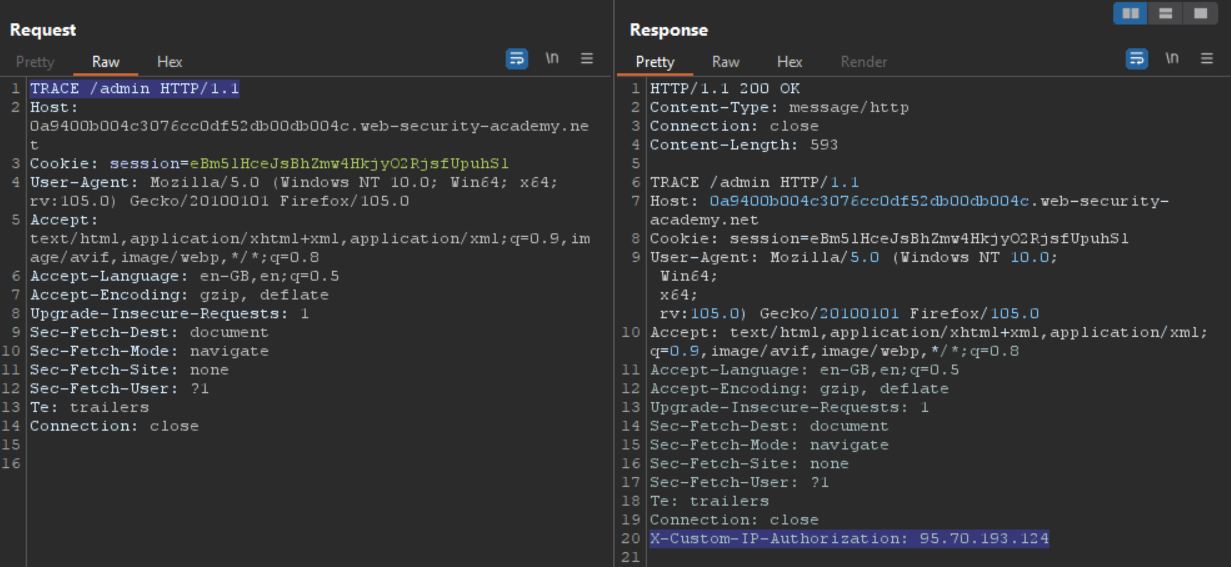
TRACE /admin

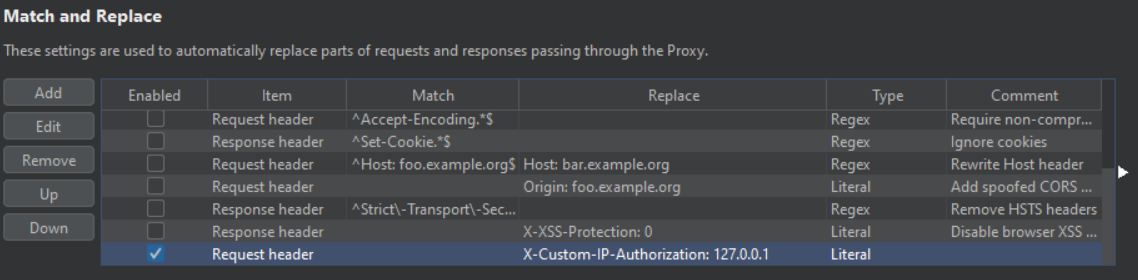
1. Study the response. Notice that the X-Custom-IP-Authorization header, containing your IP address, was automatically appended to your request. This is used to determine whether or not the request came from the localhost IP address.
2. Go to "Proxy" > "Options", scroll down to the "Match and Replace" section, and click "Add". Leave the match condition blank, but in the "Replace" field, enter:

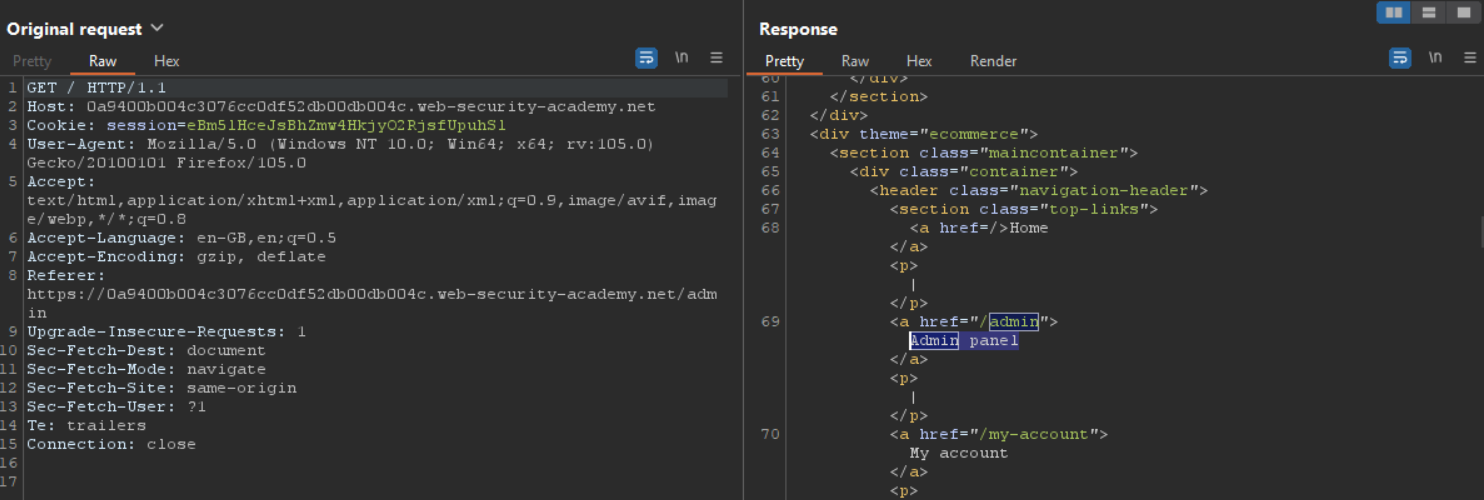
X-Custom-IP-Authorization: 127.0.0.1

Burp Proxy will now add this header to every request you send.

1. Browse to the home page. Notice that you now have access to the admin panel, where you can delete Carlos.







GET /admin HTTP/1.1

TRACE /admin HTTP/1.1

* X-Custom-IP-Authorization: 95.70.193.124

Proxy 🡪 Match and Replace 🡪 Add 🡪 X-Custom-IP-Authorization: 127.0.0.1

**Lab: Information disclosure in version control history**

PRACTITIONER

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.

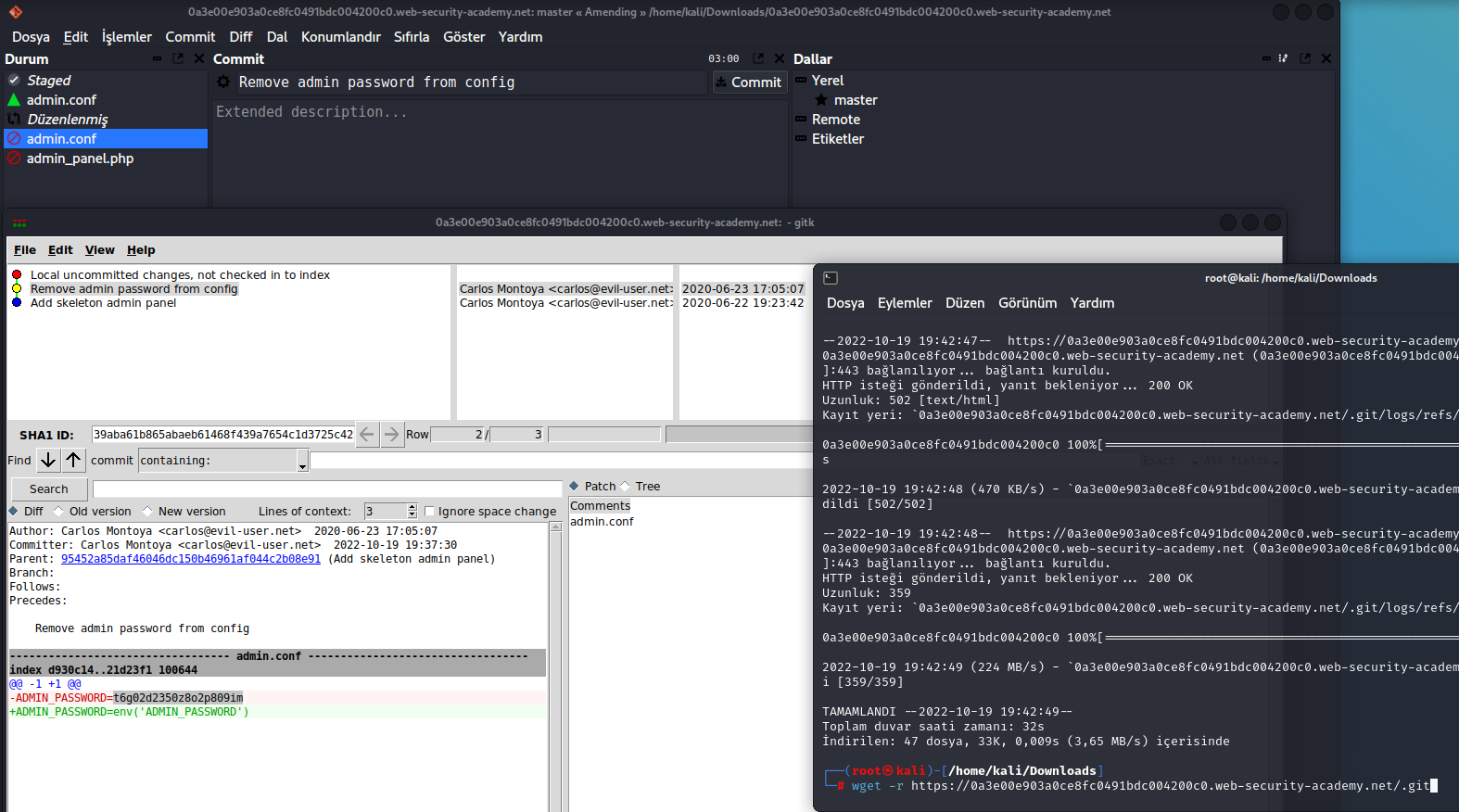
**Solution**

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.

1. Explore the downloaded directory using your local Git installation. Notice that there is a commit with the message "Remove admin password from config".
2. 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.
3. Go back to the lab and log in to the administrator account using the leaked password.
4. To solve the lab, open the admin interface and delete Carlos's account.



https://0a3e00e903a0ce8fc0491bdc004200c0.web-security-academy.net/.git

wget –r https://0a3e00e903a0ce8fc0491bdc004200c0.web-security-academy.net/.git

budan git ile admin bilgileri gözüküyor.

https://0a3e00e903a0ce8fc0491bdc004200c0.web-security-academy.net/admin