CSYE6225 – PENETRATION TESTING REPORT

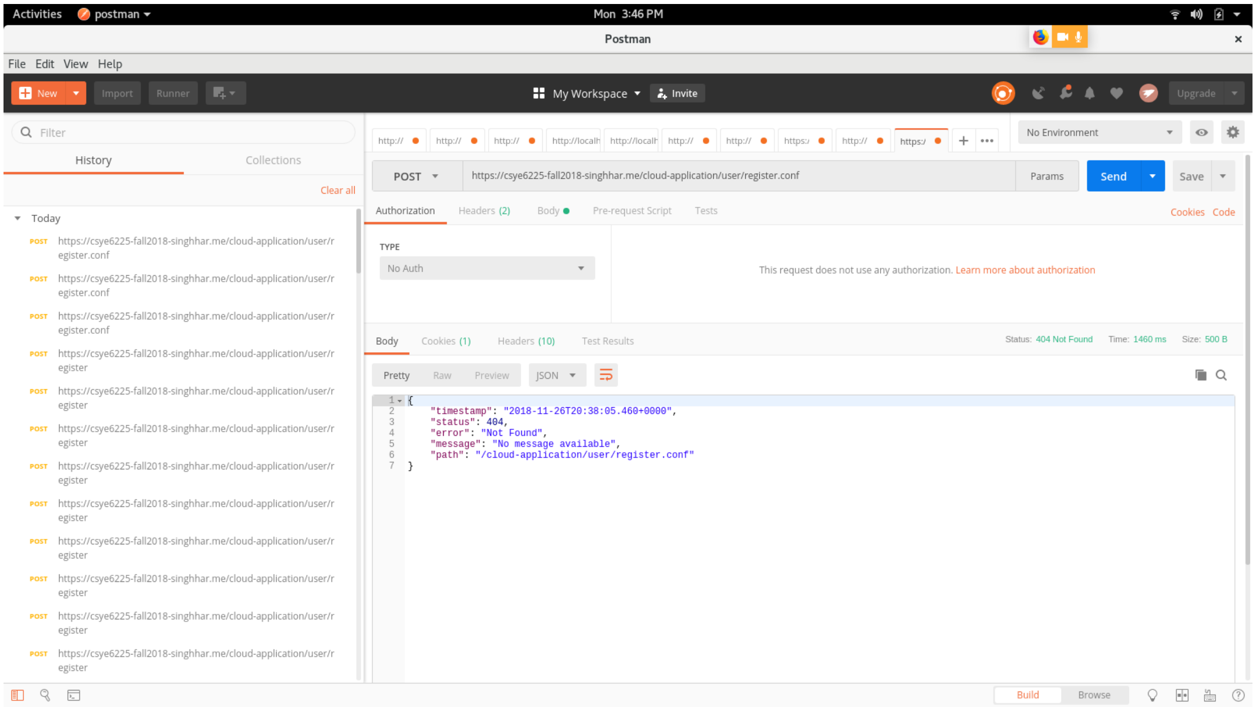
1. Attack Vector 1: Using Components with Known Vulnerabilities

Reason

Known vulnerabilities are vulnerabilities that were discovered in open source components and published. From the moment of publication , a vulnerability can be exploited by hackers who find the documentation. The conceivable effect of open source vulnerabilities ranges from minor to the absolute biggest breaks known. These are files which are loaded at runtime to collect the HTTP response. Its recommended that these components aren't placed on the public web path else accessing them might expose internal application information or provide vectors of attack.

1.1 Result

Before



POST https://csye6225-fall2018-singhhar.me/cloud-application/user/register.conf

TYPE: No Auth

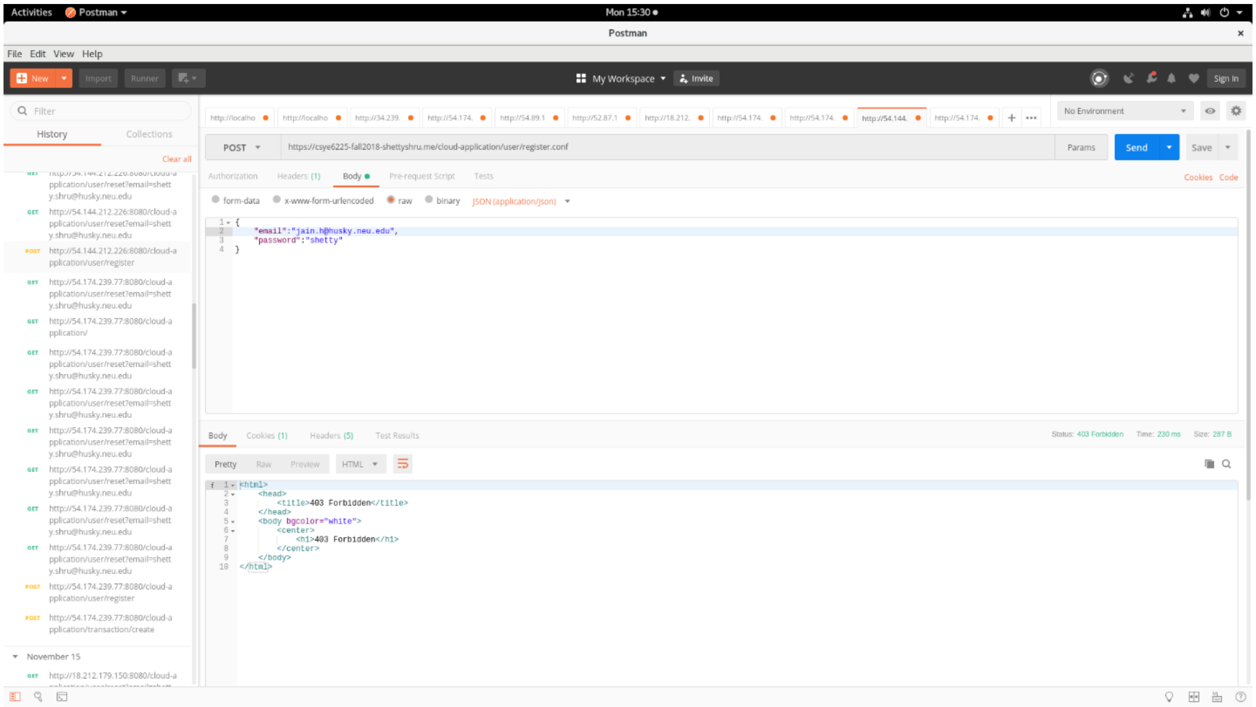
This request does not use any authorization. Learn more about authorization

POST https://csye6225-fall2018-singhhar.me/cloud-application/user/register.conf
POST https://csye6225-fall2018-singhhar.me/cloud-application/user/register.conf
POST https://csye6225-fall2018-singhhar.me/cloud-application/user/register.conf
POST https://csye6225-fall2018-singhhar.me/cloud-application/user/register
POST https://csye6225-fall2018-singhhar.me/cloud-application/user/register
POST https://csye6225-fall2018-singhhar.me/cloud-application/user/register
POST https://csye6225-fall2018-singhhar.me/cloud-application/user/register
POST https://csye6225-fall2018-singhhar.me/cloud-application/user/register
POST https://csye6225-fall2018-singhhar.me/cloud-application/user/register
POST https://csye6225-fall2018-singhhar.me/cloud-application/user/register
POST https://csye6225-fall2018-singhhar.me/cloud-application/user/register
POST https://csye6225-fall2018-singhhar.me/cloud-application/user/register

Status: 404 Not Found Time: 1460 ms Size: 500 B

```
{
    "timestamp": "2018-11-26T20:38:05.460+0000",
    "status": 404,
    "error": "Not Found",
    "message": "No message available",
    "path": "/cloud-application/user/register.conf"
}
```

After



GET http://54.144.212.226:8080/cloud-application/user/reset?email=shetty.shru@husky.neu.edu
GET http://54.144.212.226:8080/cloud-application/user/reset?email=shetty.shru@husky.neu.edu
POST http://54.144.212.226:8080/cloud-application/user/register
GET http://54.174.239.77:8080/cloud-application/user/reset?email=shetty.shru@husky.neu.edu
GET http://54.174.239.77:8080/cloud-application/
GET http://54.174.239.77:8080/cloud-application/user/reset?email=shetty.shru@husky.neu.edu
GET http://54.174.239.77:8080/cloud-application/user/reset?email=shetty.shru@husky.neu.edu
GET http://54.174.239.77:8080/cloud-application/user/reset?email=shetty.shru@husky.neu.edu
GET http://54.174.239.77:8080/cloud-application/user/reset?email=shetty.shru@husky.neu.edu
GET http://54.174.239.77:8080/cloud-application/user/reset?email=shetty.shru@husky.neu.edu
GET http://54.174.239.77:8080/cloud-application/user/reset?email=shetty.shru@husky.neu.edu
POST http://54.174.239.77:8080/cloud-application/user/register
POST http://54.174.239.77:8080/cloud-application/transaction/create

November 15

GET http://18.212.179.150:8080/cloud-a

http://localho | http://localho | http://34.239. | http://54.174. | http://54.89.1 | http://52.87.1 | http://18.212. | http://54.174. | http://54.174. | http://54.144. | http://54.174.

```
POST https://csye6225-fall2018-shettyshru.me/cloud-application/user/register.conf
```

```
{
    "email":"jain.h@husky.neu.edu",
    "password":"shetty"
}
```

Status: 403 Forbidden Time: 230 ms Size: 287 B

```
<html>
    <head>
        <title>403 Forbidden</title>
    </head>
    <body bgcolor="white">
        <center>
            <h1>403 Forbidden</h1>
        </center>
    </body>
</html>
```

2. Attack Vector 2: Insufficient Attack Protection

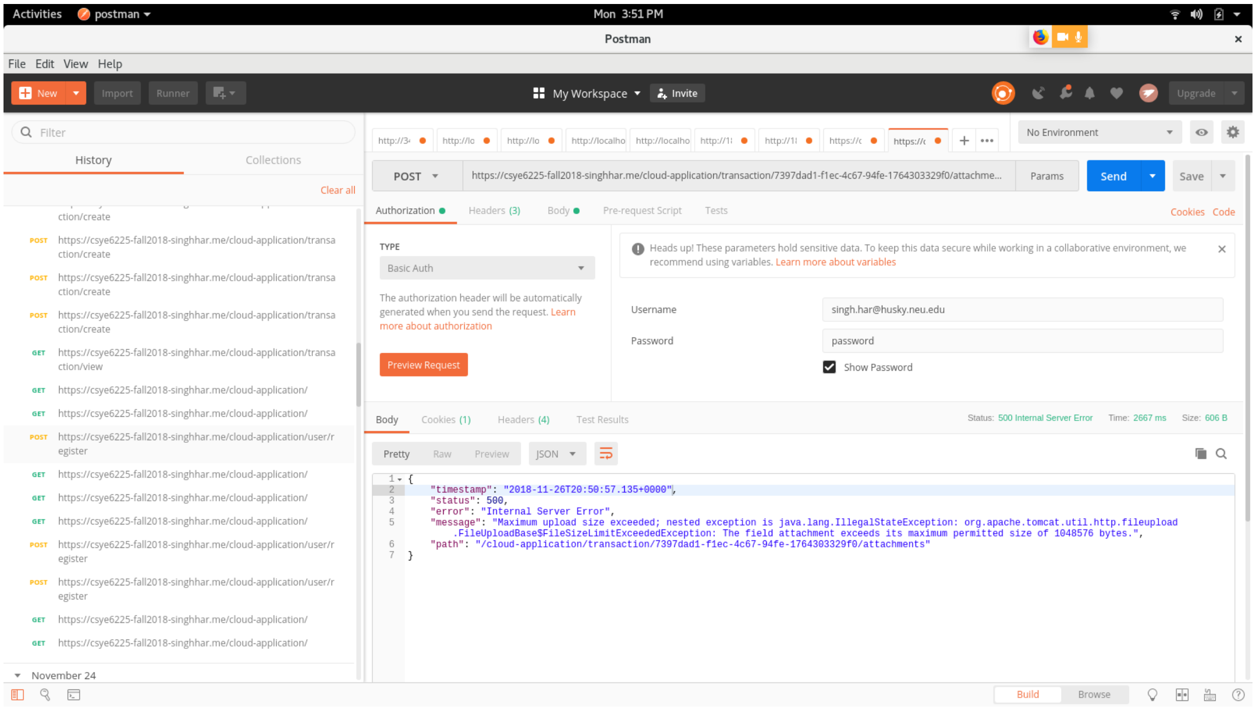
Reason

These attacks are when your application is targeted with unusual requests pattern or high volumes. Here we are limiting the file size that can be uploaded.

2.1 Result

Before

CSYE6225 – PENETRATION TESTING REPORT



POST https://csye6225-fall2018-singhhar.me/cloud-application/transaction/7397dad1-f1ec-4c67-94fe-1764303329f0/attachme...

Authorization — TYPE: Basic Auth

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. Learn more about variables

Username: singh.har@husky.neu.edu

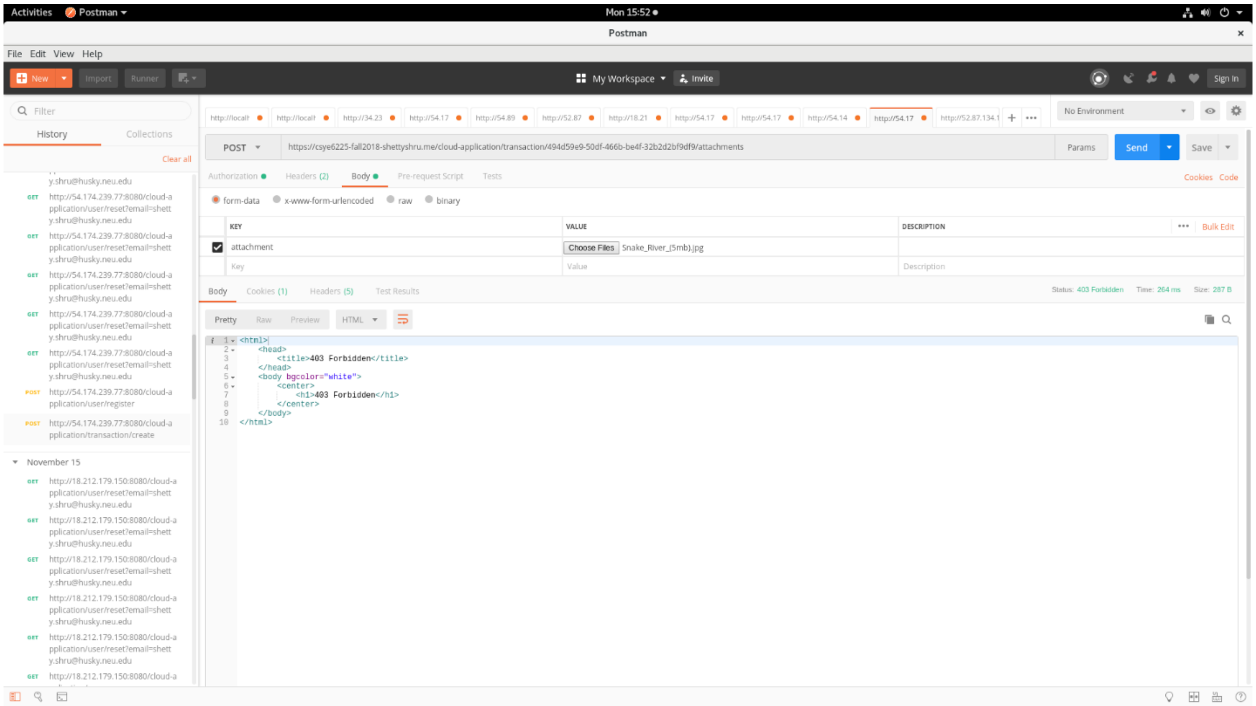
Password: password

☑ Show Password

Status: 500 Internal Server Error Time: 2667 ms Size: 606 B

```
{
    "timestamp": "2018-11-26T20:50:57.135+0000",
    "status": 500,
    "error": "Internal Server Error",
    "message": "Maximum upload size exceeded; nested exception is java.lang.IllegalStateException: org.apache.tomcat.util.http.fileupload
        .FileUploadBase$FileSizeLimitExceededException: The field attachment exceeds its maximum permitted size of 1048576 bytes.",
    "path": "/cloud-application/transaction/7397dad1-f1ec-4c67-94fe-1764303329f0/attachments"
}
```

After



POST https://csye6225-fall2018-shettyshru.me/cloud-application/transaction/494d59e9-50df-466b-be4f-32b2d2bf9df9/attachments

Body: ● form-data ○ x-www-form-urlencoded ○ raw ○ binary

	KEY	VALUE	DESCRIPTION
☑	attachment	Choose Files Snake_River_(5mb).jpg	

Status: 403 Forbidden Time: 264 ms Size: 287 B

```
<html>
    <head>
        <title>403 Forbidden</title>
    </head>
    <body bgcolor="white">
        <center>
            <h1>403 Forbidden</h1>
        </center>
    </body>
</html>
```

3. Attack Vector 3: Broken Access Control

3.1 Reason

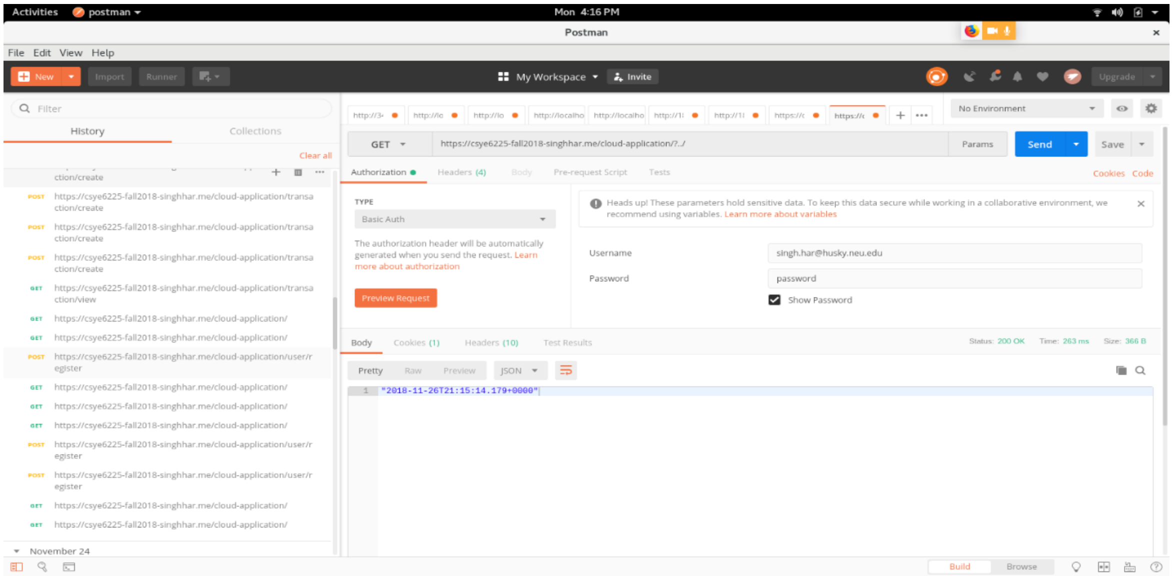
Access control is the means by which web applications control what functionalities and features ought to be open to various clients.

An appropriately application would basically redirect the client to the login page if it is not authorized to use a particular feature. Assuming, not withstanding, this technique enables access to those pages, it is a type of broken access control. Even a simple assault like this can cause disturbing harm if client information is put away inappropriately.

In our application when a query string with ?../ is provided before using the WAF rules we do get the current date and time but on applying WAF rules we get a 403 Forbidden

3.2 Result

Before



POST https://csye6225-fall2018-singhhar.me/cloud-application/transaction/create
POST https://csye6225-fall2018-singhhar.me/cloud-application/transaction/create
POST https://csye6225-fall2018-singhhar.me/cloud-application/transaction/create
GET https://csye6225-fall2018-singhhar.me/cloud-application/transaction/view
GET https://csye6225-fall2018-singhhar.me/cloud-application/
GET https://csye6225-fall2018-singhhar.me/cloud-application/
POST https://csye6225-fall2018-singhhar.me/cloud-application/user/register
GET https://csye6225-fall2018-singhhar.me/cloud-application/
GET https://csye6225-fall2018-singhhar.me/cloud-application/
GET https://csye6225-fall2018-singhhar.me/cloud-application/
POST https://csye6225-fall2018-singhhar.me/cloud-application/user/register
POST https://csye6225-fall2018-singhhar.me/cloud-application/user/register
GET https://csye6225-fall2018-singhhar.me/cloud-application/
GET https://csye6225-fall2018-singhhar.me/cloud-application/

GET https://csye6225-fall2018-singhhar.me/cloud-application/?../

TYPE: Basic Auth

The authorization header will be automatically generated when you send the request. Learn more about authorization

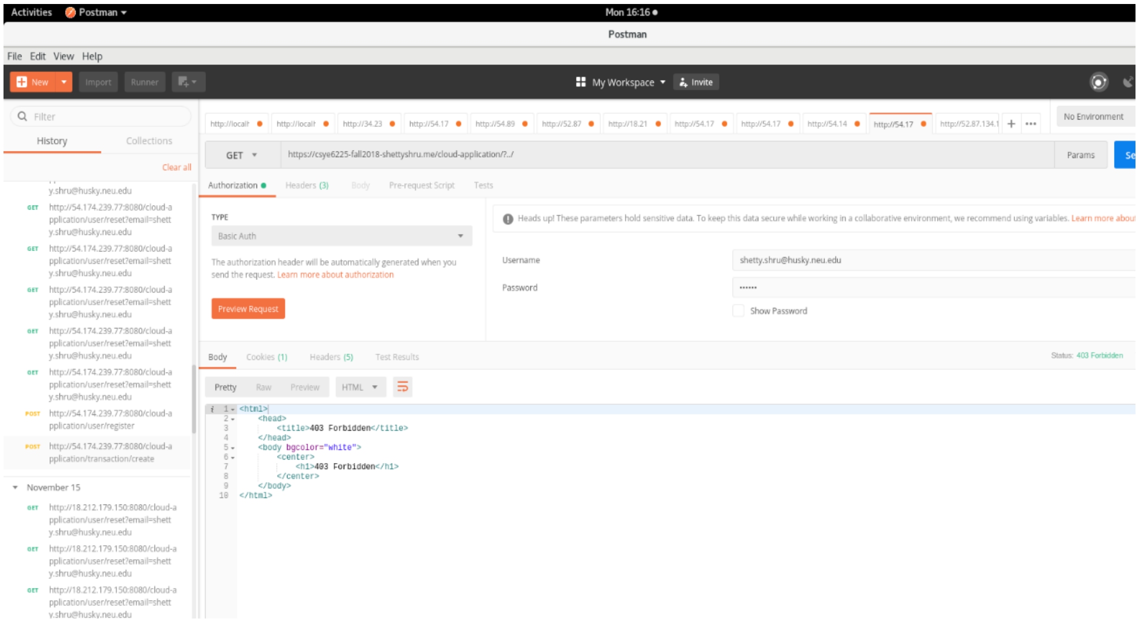
Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. Learn more about variables

Username: singh.har@husky.neu.edu
Password: password
☑ Show Password

Status: 200 OK Time: 263 ms Size: 366 B

```
"2018-11-26T21:15:14.179+0000"
```

After



y.shru@husky.neu.edu

GET http://54.174.239.77:8080/cloud-application/user/reset?email=shetty.shru@husky.neu.edu

GET http://54.174.239.77:8080/cloud-application/user/reset?email=shetty.shru@husky.neu.edu

GET http://54.174.239.77:8080/cloud-application/user/reset?email=shetty.shru@husky.neu.edu

GET http://54.174.239.77:8080/cloud-application/user/reset?email=shetty.shru@husky.neu.edu

GET http://54.174.239.77:8080/cloud-application/user/reset?email=shetty.shru@husky.neu.edu

POST http://54.174.239.77:8080/cloud-application/user/register

POST http://54.174.239.77:8080/cloud-application/transaction/create

November 15

GET http://18.212.179.150:8080/cloud-application/user/reset?email=shetty.shru@husky.neu.edu

GET http://18.212.179.150:8080/cloud-application/user/reset?email=shetty.shru@husky.neu.edu

GET http://18.212.179.150:8080/cloud-application/user/reset?email=shetty.shru@husky.neu.edu

GET https://csye6225-fall2018-shettyshru.me/cloud-application/?../

TYPE: Basic Auth

The authorization header will be automatically generated when you send the request. Learn more about authorization

Heads up! These parameters hold sensitive data. To keep this data secure while working in a collaborative environment, we recommend using variables. Learn more about

Username: shetty.shru@husky.neu.edu

Password: ••••••

□ Show Password

Status: 403 Forbidden

```html
<html>
    <head>
        <title>403 Forbidden</title>
    </head>
    <body bgcolor="white">
        <center>
            <h1>403 Forbidden</h1>
        </center>
    </body>
</html>
```