Team 4 attack findings

Target Team Details:

URL: https://neu-csye6225-spring2017-team-4.me/

1. The victim's web application accepts all types of files in their file upload section.

Uploaded files represent a significant risk to applications. The first step in many attacks is to get some code to the system to be attacked. Then the attack only needs to find a way to get the code executed. Using a file upload helps the attacker accomplish the first step.

The consequences of unrestricted file upload can vary, including complete system takeover, an overloaded file system or database, forwarding attacks to back-end systems, client-side attacks, or simple defacement. It depends on what the application does with the uploaded file and especially where it is stored.

There are really two classes of problems here. The first is with the file metadata, like the path and file name. These are generally provided by the transport, such as HTTP multi-part encoding. This data may trick the application into overwriting a critical file or storing the file in a bad location. They must validate the metadata extremely carefully before using it.

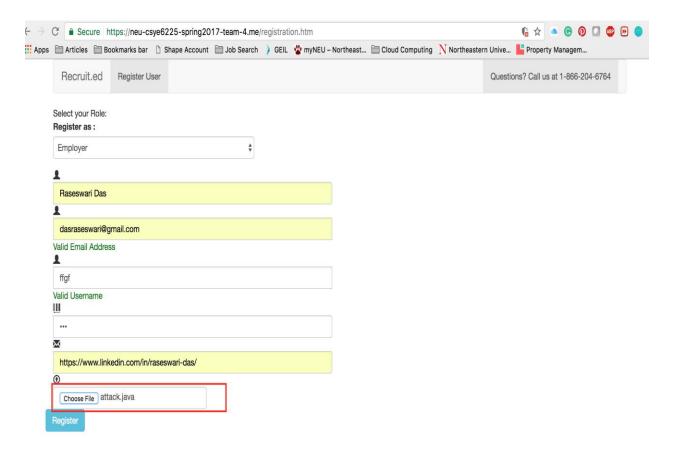
Tool used: w3af (Kali Linux)

The page is written in: "en".

The remote Web server sent a strange HTTP reasonmessage "", manual inspection is recommended. This information was found in the request with id 18.

The URL: "https://neu-csye6225-spring2017-team-4.me/login" has a "<form>" element with auto-complete enabled. This information was found in the request with id 43. "https://neu-csye6225-spring2017-team-4.me/login" has a "<form>" element with auto-complete enabled. This information was found in

A form which allows file uploads was found at "https://neu-csye6225-spring2017-team-4.me/registration.htm". This information was found in the erequest with id 68.



2. Using W3af, we found several injection points, where a SQL injection attack was launched using "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system.

```
The following is a list of broken links that were found by the web spider plugin:
https://neu-csye6225-spring2017-team-4.me/login.htm [ referenced from: https://neu-csye6225-spring2017-team-4.me/registration.htm ]
ound 4 URLs and 11 different injections points.
The URL list is:
 https://neu-csye6225-spring2017-team-4.me/ Gloub com Mebus cupp by Mebus from
 https://neu-csye6225-spring2017-team-4.me/forgot password.htm
 https://neu-csye6225-spring2017-team-4.me/login
 https://neu-csye6225-spring2017-team-4.me/registration.htm
The list of fuzzable requests is:
 Method: GET | https://neu-csye6225-spring2017-team-4.me/
 Method: GET | https://neu-csye6225-spring2017-team-4.me/
 Method: GET | https://neu-csye6225-spring2017-team-4.me/forgot password.htm
 Method: GET | https://neu-csye6225-spring2017-team-4.me/login
 Method: GET | https://neu-csye6225-spring2017-team-4.me/login | Query string: (error)
 Method: GET | https://neu-csye6225-spring2017-team-4.me/registration.htm
 Method: POST | https://neu-csye6225-spring2017-team-4.me/forgot password.htm | URL encoded form: (emailaddress)
 Method: POST | https://neu-csye6225-spring2017-team-4.me/login | URL encoded form: (username, password)
 Method: POST | https://neu-csye6225-spring2017-team-4.me/login | URL encoded form: (username, password)
 Method: POST | https://neu-csye6225-spring2017-team-4.me/registration.htm | Multipart/post: (role, name, email, gpa, univName, username, p
assword, linkedInUrl, image)
 Method: POST | https://neu-csye6225-spring2017-team-4.me/registration.htm | Multipart/post: (role, name, email, gpa, univName, username, p
assword, linkedİnUrl, image)
```

3. Discovered open ports. An open port is an attack surface. The daemon that is listing on a port, could be vulnerable to a buffer overflow, or another remotely exploitable vulnerability.

This report can assist analysts in identifying SSH server versions within the organization. Once analysts identify the different versions of SSH installed on hosts, they can update vulnerable SSH servers and clients.

An important principle in security is reducing your attack surface, and ensure that servers have the minimum number of exposed services.

