

**Finding Name:** Brute Force Attack

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Team** | **Role** | **Project** | **Quality Assurance** | **Is this a re-tested Finding?** |
| Natalia Khobotova | PT | Junior SCR lead | Ontrack | Oliver Power | No |
|  |  |  |  |  |  |

|  |
| --- |
| **Was this Finding Successful?** |
| Yes |

**Finding Description**

It is a potential security risk related to brute-force attacks and automated password guessing against an API endpoint (http://localhost:3000/api/auth). By systematically testing multiple combinations of usernames and passwords from provided lists (usernames.txt and passwords.txt), the script exploits weak or reused credentials to gain unauthorised access to the system.

**Risk Rating**  
Impact: Severe

Likelihood: High

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact values** | | | | |
| **Very Minor** | **Minor** | **Significant** | **Major** | **Severe** |
| Risk that holds little to no impact. Will not cause damage and regular activity can continue. | Risk that holds minor form of impact, but not significant enough to be of threat. Can cause some damage but not enough to impede regular activity. | Risk that holds enough impact to be somewhat of a threat. Will cause damage that can impede regular activity but will be able to run normally. | Risk that holds major impact to be of threat. Will cause damage that will impede regular activity and will not be able to run normally. | Risk that holds severe impact and is a threat. Will cause critical damage that can cease activity to be run. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Likelihood** | | | | |
| **Rare** | **Unlikely** | **Moderate** | **High** | **Certain** |
| Event may occur and/or if it did, it happens in specific circumstances. | Event could occur occasionally and/or could happen (at some point) | Event may occur and/or happens. | Event occurs at times and/or probably happens a lot. | Event is occurring now and/or happens frequently. |

**Business Impact**  
***Data Breach and Unauthorised Access:***

Successful brute force attacks may result in intrusion into the application that accessed confidential data, customer information, and proprietary business information.

***Reputational Damage:***

A successful attack exploiting this vulnerability can severely damage the company's reputation and trust among customers, partners, and stakeholders.

***Operational Disruption:***

Business operations can be interrupted by unauthorised access and data breaches thereby leading to downtime, service interruptions, and operational inefficiencies.

**Affected Assets**

***Data:***

* Customer Information: Personal and sensitive customer data, including names, addresses, contact details, payment information, and account credentials
* Business Data: intellectual property, financial records, operational data

***Business Operations:***

* Workflows
* Functions supported by an application

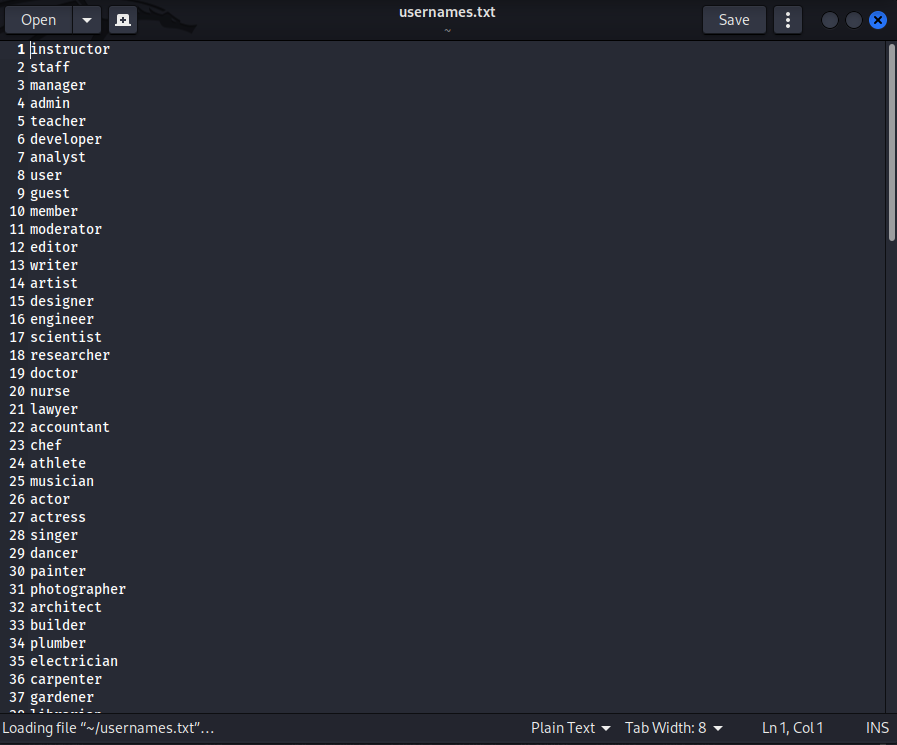
***Reputation:***

The vulnerability exploitation can lead to a loss of customer faith, damage to the brand name, and reputational harm, thus affecting its reputation, image and the general public’s opinion.

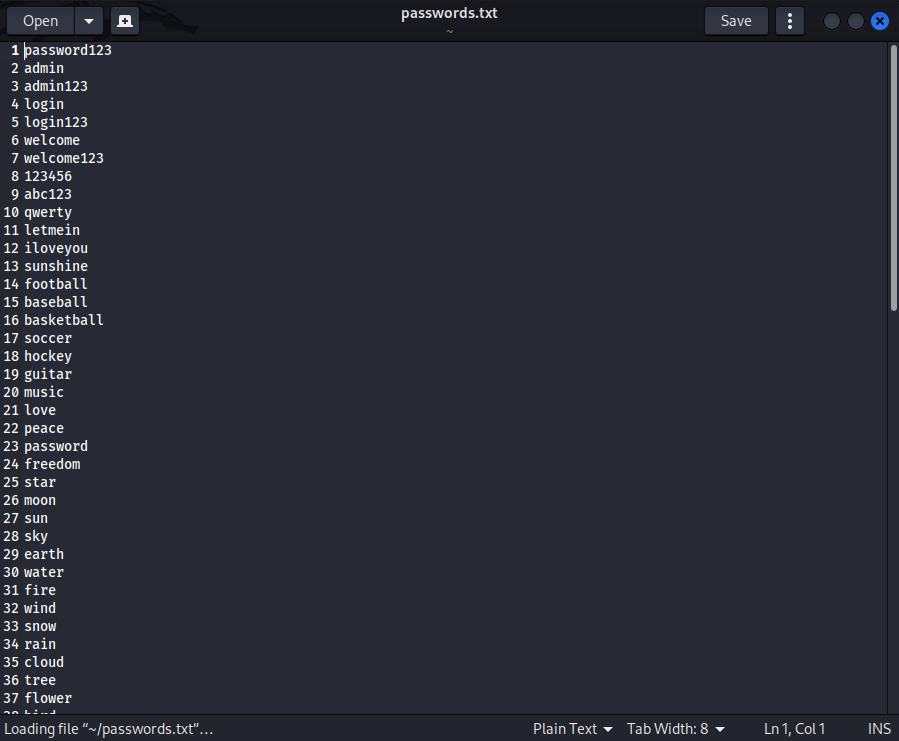
**Evidence**

**Step 1.**   
Create a txt file with usernames and name it username.txt, as this name is used in my script. If the name is changed, the script will need to be changed (a copy of the file I used is located [here](https://deakin365-my.sharepoint.com/:t:/g/personal/s223011356_deakin_edu_au/EXcH12yyTl1Bkz9kIfL_1PEBJ4L8BCqTccW8dLwSfG_4Eg?e=Zeza8a)). Both files include usernames and password for a successful attempt to prove that there are no controls to prevent it. You can use nano or gedit command

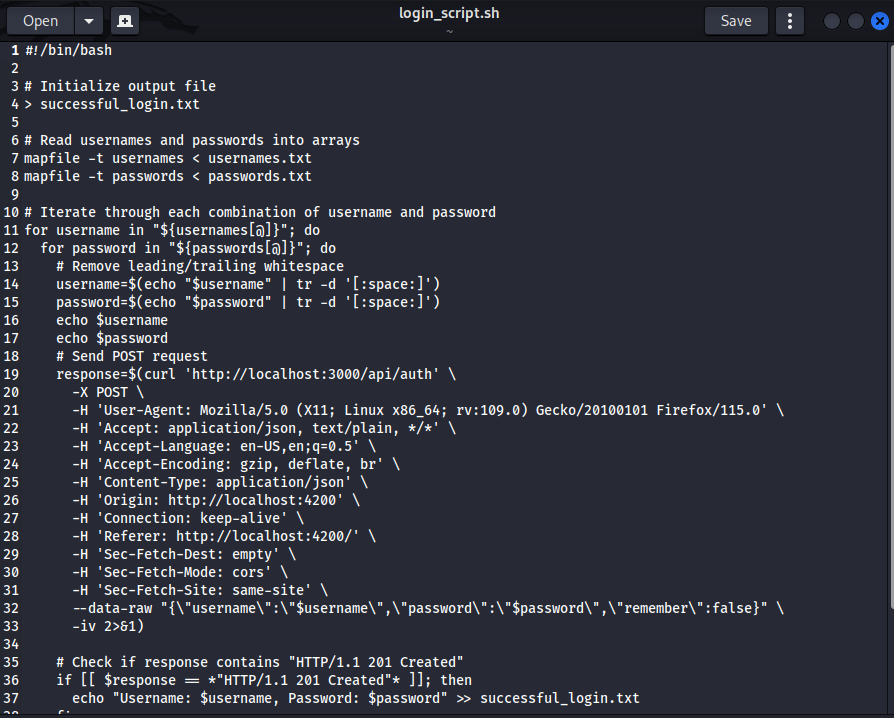
**gedit usernames.txt**   
copy the usernames from provided file or generate your own

  
save and close

**Step 2.** Create a txt file with passwords and name it passwords.txt t, as this name is used in my script. If the name is changed, the script will need to be changed (a copy of the file I used is located [here](https://deakin365-my.sharepoint.com/:t:/g/personal/s223011356_deakin_edu_au/EfVEO7oEHOFJkmhiegwW0tsBRnc2xwscay0ATx_TxZmiwg?e=nxckBu))  
gedit passwords.txt   
copy the passwords from provided file or generate your own



save and close

**Step 3.** Create login\_script.sh file  
gedit login\_script.sh and paste the content from [this file](https://deakin365-my.sharepoint.com/:u:/g/personal/s223011356_deakin_edu_au/EQK--brHMthKoVTbpweYUCUBwBRWzuED9QyHYFuiFzTcrw?e=ag9gSu)

Save and close

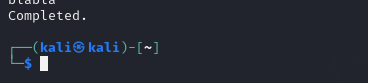
Make the script executable by running chmod +x login\_script.sh.

Place your usernames.txt and passwords.txt files in the same directory as the script, with each username and password on a new line.

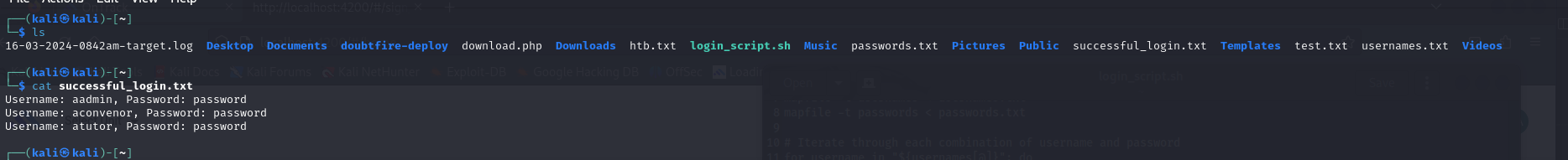
Run the script by executing ./login\_script.sh.

While the script is running it will display the username and the password it is currently trying to log in with, if you want to stop you need to comment out line 16 and 17 by inserting # symbol at the front of the line   
#echo $username

#echo $password

When the script ends you will see a line saying completed  
  
if any pair of username and password was used to successfully login, they will be saved into a file called successful\_login.txt

**PLEASE NOTE THE SCRIPT RUNS ABOUT 40 MINS!** If you want to make it shorter make the usernames.txt and passwords.txt shorter   
Here’s the results from my run:



**Remediation Advice**

* implement server-side rate limiting to block or throttle users who make too many unsuccessful login attempts. This can be done by tracking the number of failed login attempts for each user and blocking or throttling their requests when a certain threshold is reached.
* use HTTP headers and response codes to handle unsuccessful login attempts. For example, you can set specific HTTP response codes (e.g., 429 Too Many Requests) and headers to indicate rate limiting or temporary blocks
* Implementing authentication tokens or CAPTCHA challenges

**References**

* <https://www.fortinet.com/resources/cyberglossary/brute-force-attack>
* https://sosafe-awareness.com/glossary/brute-force-attack/

**Contact Details**

* Natalia Khobotova
* s223011356@deakin.edu.au

**Pentest Leader Feedback.**

Thanks Natalia. I would recommend that the impact be severe due to the compromise of the account and therefore sensitive information.