**TEAM : ANONYMOUS**

* ***CHALLENGE: PASSWORD INTEGRITY VULNERABILITY***

1. **TARGET -I**

**DESCRIPTION:** Password integrity vulnerability refers to the vulnerability where the data confidentiality and integrity is compromised and that data can be seen by any one in unauthorized way also

**VULNERABLE TARGET:** WWW.ISSUU.COM

**STEPS TO PROVE THE PASSWORD INTEGRITY VULNERABILITY:**

**Step1:** Open the firefox and burpsuit

**Step2:** Now **OFF** the intercept in burpsuit

**Step3:** Search the target website and try to login with the login credentials

**Step4:** Before sending the login details to the server **ON** the intercept in burpsuit and click on login/signup button

**Step5:** Now click “forward” button until you see the service request of the issuu website

**Step6:** If you see the password in plain text format then the password integrity vulnerability exists

**IMPACT:**

If the password integrity vulnerability exists then the user confidentiality is compromised

**MITIGATION:**

Use encryption algorithms to encrypt the data in the unreadable format so that no data confidentiality is compromised.

**PROOF OF CONCEPT:**

Graphical user interface, text, application, email

Description automatically generated

**2. TARGET -II**

**DESCRIPTION:** Password integrity vulnerability refers to the vulnerability where the data confidentiality and integrity is compromised and that data can be seen by any one in unauthorized way also

**VULNERABLE TARGET:** <http://103.15.62.229/results/mlrit-login/>

**STEPS TO PROVE THE PASSWORD INTEGRITY VULNERABILITY:**

**Step1:** Open the firefox and burpsuit

**Step2:** Now **OFF** the intercept in burpsuit

**Step3:** Search the target website and try to login with the login credentials

**Step4:** Before sending the login details to the server **ON** the intercept in burpsuit and click on login/signup button

**Step5:** Now click “forward” button until you see the service request of the mlrit website

**Step6:** If you see the password in plain text format then the password integrity vulnerability exists

**IMPACT:**

If the password integrity vulnerability exists then the user confidentiality is compromised

**MITIGATION:**

Use encryption algorithms to encrypt the data in the unreadable format so that no data confidentiality is compromised.

**PROOF OF CONCEPT:**

Graphical user interface, text, application, email

Description automatically generated

**3. TARGET -III**

**DESCRIPTION:** Password integrity vulnerability refers to the vulnerability where the data confidentiality and integrity is compromised and that data can be seen by any one in unauthorized way also

**VULNERABLE TARGET:** <https://www.seamless.ai/>

**STEPS TO PROVE THE PASSWORD INTEGRITY VULNERABILITY:**

**Step1:** Open the firefox and burpsuit

**Step2:** Now **OFF** the intercept in burpsuit

**Step3:** Search the target website and try to login with the login credentials

**Step4:** Before sending the login details to the server **ON** the intercept in burpsuit and click on login/signup button

**Step5:** Now click “forward” button until you see the service request of the mlrit website

**Step6:** If you see the password in plain text format then the password integrity vulnerability exists

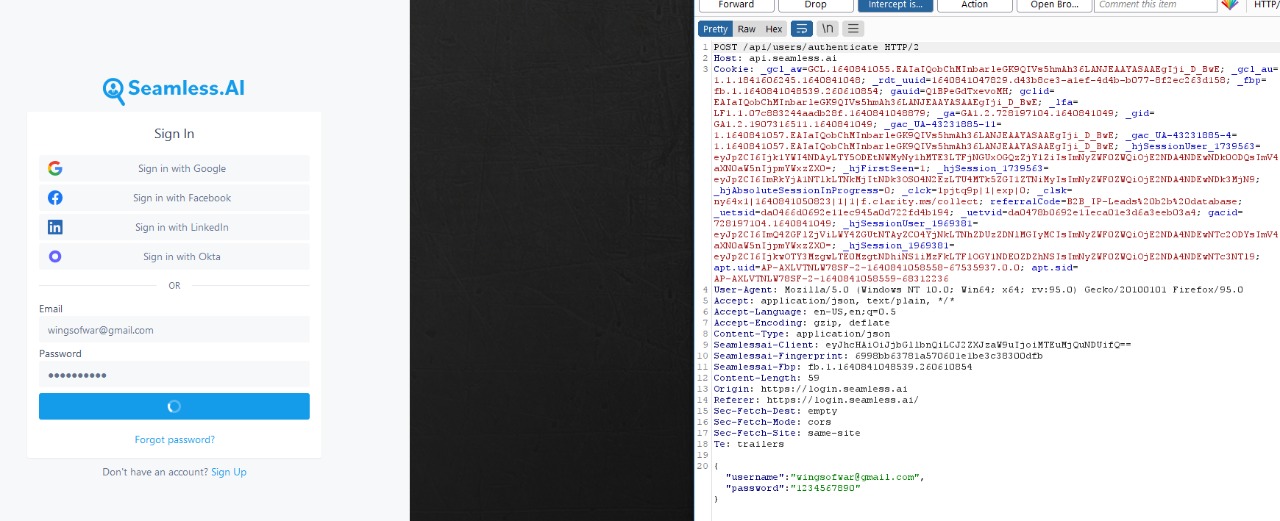
**IMPACT:**

If the password integrity vulnerability exists then the user confidentiality is compromised

**MITIGATION:**

Use encryption algorithms to encrypt the data in the unreadable format so that no data confidentiality is compromised.

**PROOF OF CONCEPT:**

****

**4. TARGET -IV**

**DESCRIPTION:** Password integrity vulnerability refers to the vulnerability where the data confidentiality and integrity is compromised and that data can be seen by any one in unauthorized way also.

**VULNERABLE TARGET:** https://www.chegg.com/auth?action=login&redirect=https%3A%2F%2Fwww.chegg.com%2Fpromo%2Fsohp

**STEPS TO PROVE THE PASSWORD INTEGRITY VULNERABILITY:**

**Step1:** Open the firefox and burpsuit

**Step2:** Now **OFF** the intercept in burpsuit

**Step3:** Search the target website and try to login with the login credentials

**Step4:** Before sending the login details to the server **ON** the intercept in burpsuit and click on login/signup button

**Step5:** Now click “forward” button until you see the service request of the CHEGG website

**Step6:** If you see the password in plain text format then the password integrity vulnerability exists

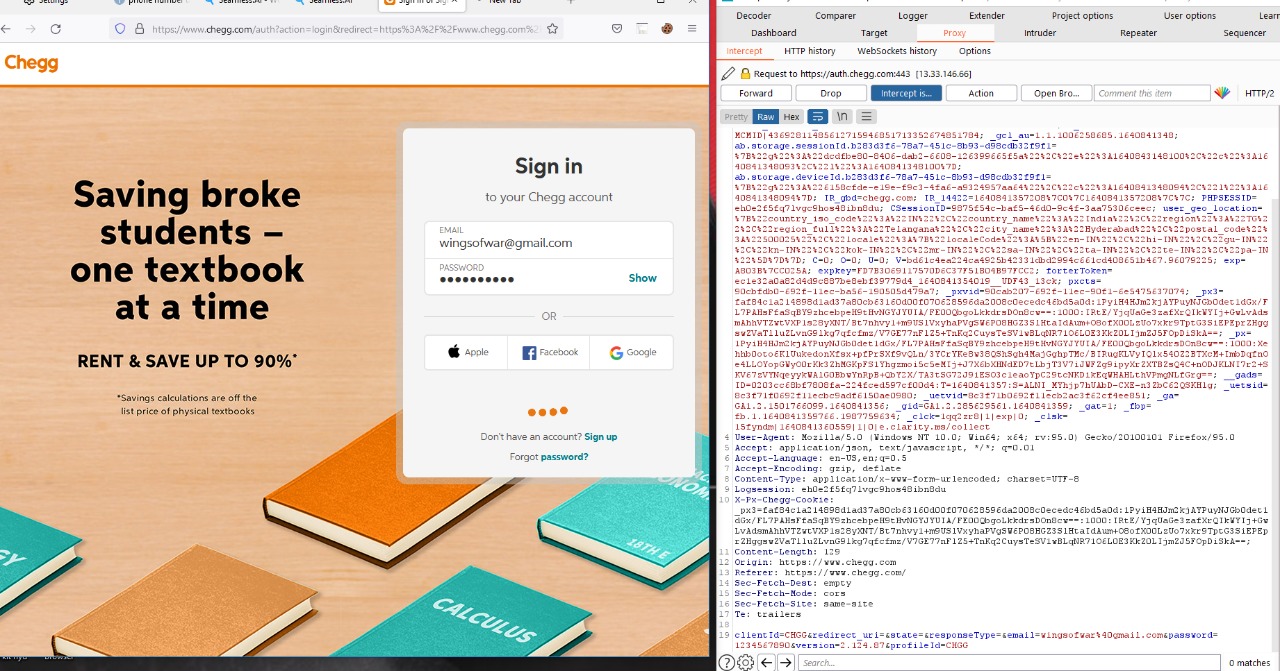
**IMPACT:**

If the password integrity vulnerability exists then the user confidentiality is compromised

**MITIGATION:**

Use encryption algorithms to encrypt the data in the unreadable format so that no data confidentiality is compromised.

**PROOF OF CONCEPT:**

****

**5. TARGET -V**

**DESCRIPTION:** Password integrity vulnerability refers to the vulnerability where the data confidentiality and integrity is compromised and that data can be seen by any one in unauthorized way also

**VULNERABLE TARGET:** https://everpress.com/login

**STEPS TO PROVE THE PASSWORD INTEGRITY VULNERABILITY:**

**Step1:** Open the firefox and burpsuit

**Step2:** Now **OFF** the intercept in burpsuit

**Step3:** Search the target website and try to login with the login credentials

**Step4:** Before sending the login details to the server **ON** the intercept in burpsuit and click on login/signup button

**Step5:** Now click “forward” button until you see the service request of the EVERPRESS website

**Step6:** If you see the password in plain text format then the password integrity vulnerability exists

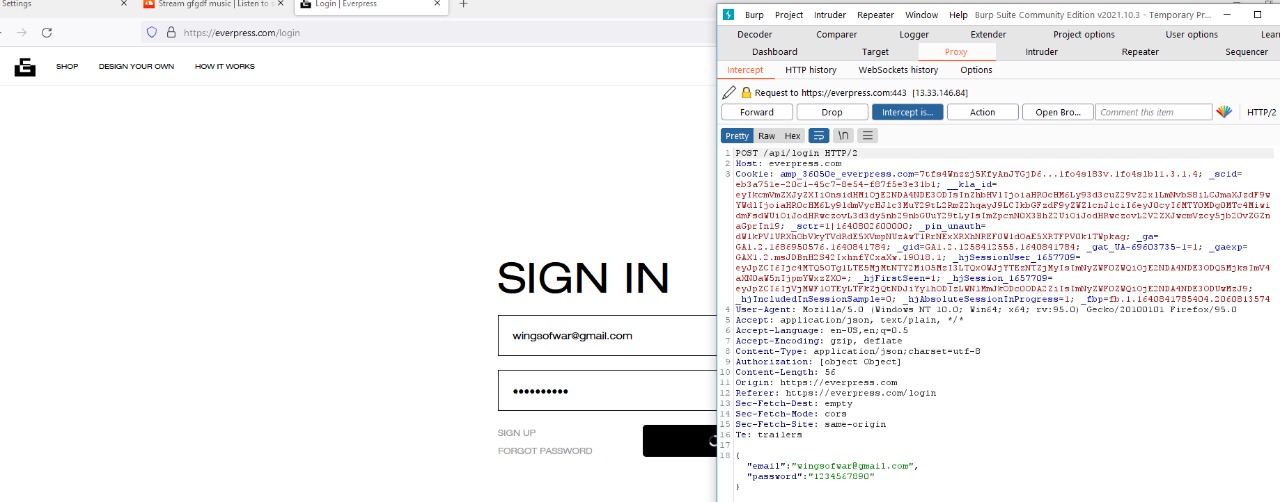
**IMPACT:**

If the password integrity vulnerability exists then the user confidentiality is compromised

**MITIGATION:**

Use encryption algorithms to encrypt the data in the unreadable format so that no data confidentiality is compromised.

**PROOF OF CONCEPT:**

****

**THANK YOU**

**BY :**

**M.VUJWALA (CSE BTECH-II)**

**B.SAI TEJA (CSE-CS BTECH-I)**

**A.VAMSHI (CSE-CS BTECH-I)**

**SRI NIKHIL.C (CSE-CS BTECH-I)**