Team ID: Team-593490 **Team Size:** 4

Team Leader: Mohamed Naveed **Team member:** Dharun Ramesh

Team member: Madhuri Santhosh Srinivasan **Team member:** Aravind. S

Project: AI-enhanced intrusion detection system

Vulnerabilities in Practice Website

Practice Website: https://google-gruyere.appspot.com/

Vulnerability Name: Unrestricted Upload of File with Dangerous Type

CWE : CWE - 434

OWASP Category: A04:2021 – Insecure Design

Description: The product allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment.

Business Impact:Lack of effective security controls in the design phase often results in an application being susceptible to many weaknesses, collectively known as insecure design vulnerabilities.

Vulnerability Path : https://google-gruyere.appspot.com/upload.gtl

Vulnerability Parameter: HTML File

Steps To Reproduce

Step 1: Access the URL

Step 2: Create account and then login with your credentials

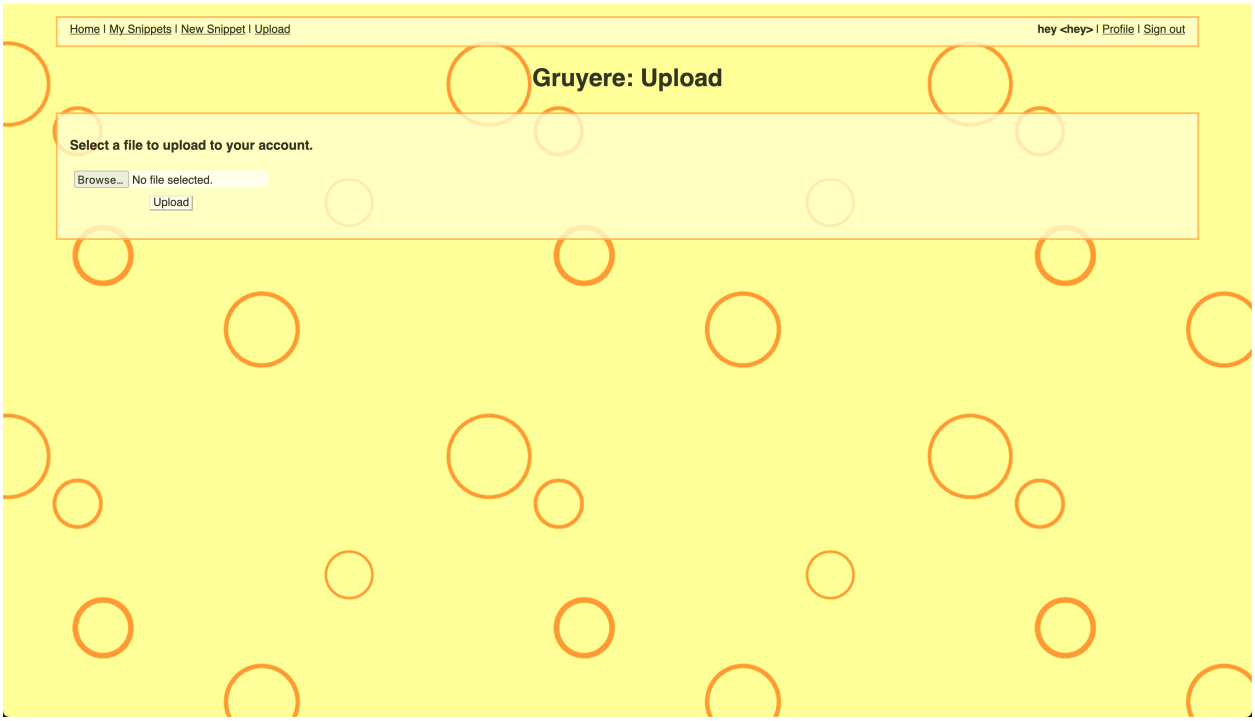
Step 3: Upload a HTML file with script

Team ID: Team-593490 **Team Size:** 4

Team Leader: Mohamed Naveed **Team member:** Dharun Ramesh

Team member: Madhuri Santhosh Srinivasan **Team member:** Aravind. S

Project: AI-enhanced intrusion detection system




```html
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <title>Document</title>
  </head>
  <body>
    <script>
      alert("File Upload XSS");
    </script>
  </body>
</html>
```

Step 4: Upload

Step 5: Visit the given link

Team ID: Team-593490

Team Size: 4

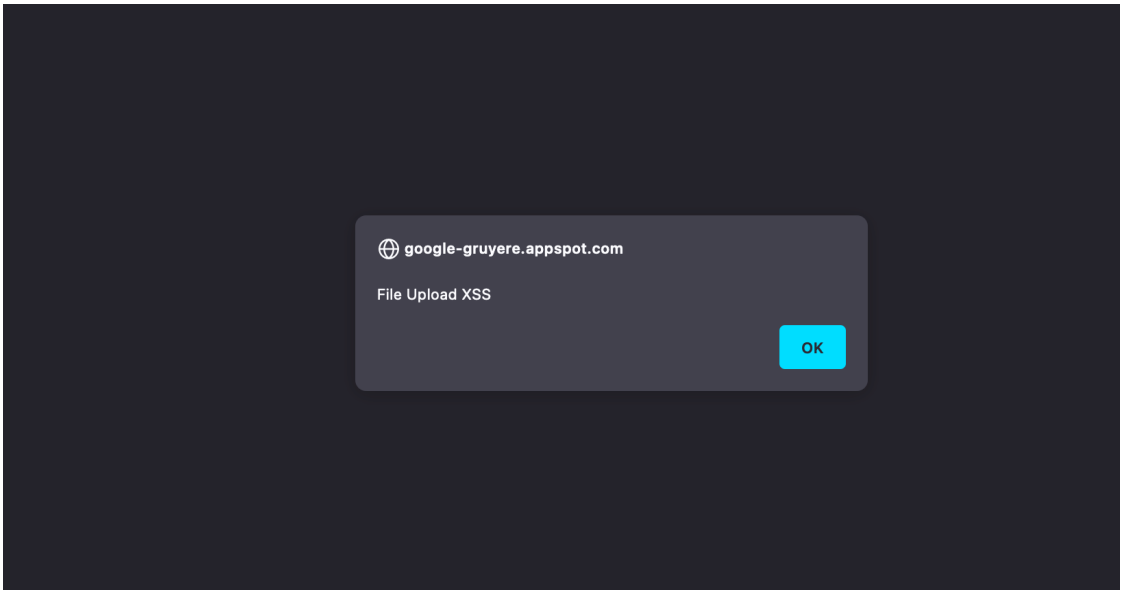
Team Leader: Mohamed Naveed

Team member: Dharun Ramesh

Team member: Madhuri Santhosh Srinivasan

Team member: Aravind. S

Project: AI-enhanced intrusion detection system



Team ID: Team-593490 **Team Size:** 4

Team Leader: Mohamed Naveed **Team member:** Dharun Ramesh

Team member: Madhuri Santhosh Srinivasan **Team member:** Aravind. S

Project: AI-enhanced intrusion detection system

Vulnerability Name: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CWE : CWE - 79

OWASP Category: A03:2021 – Injection

Description: The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.

Business Impact: Cross-site scripting (XSS) can lead to unauthorized access to user data, damaging trust and reputation, and exposing businesses to legal and financial repercussions.

Vulnerability Path : https://google-gruyere.appspot.com/

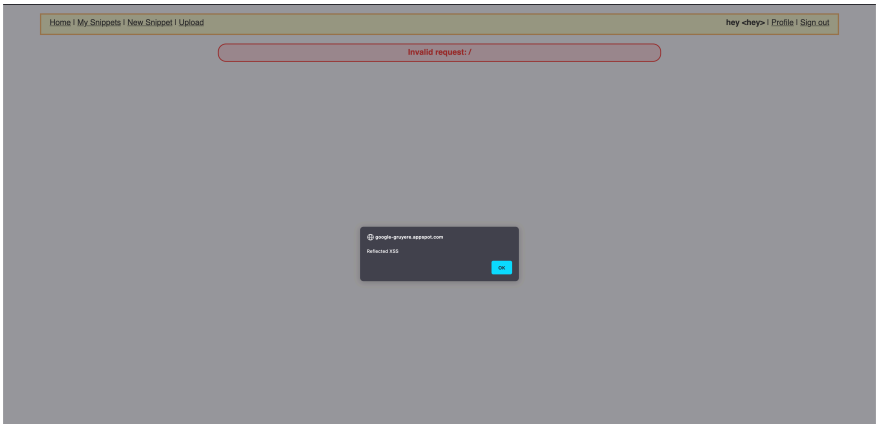
Vulnerability Parameter: https://google-gruyere.appspot.com//%3Cscript%3Ealert(%22Reflected%20XSS%22)%3C/script%3E

Steps To Reproduce

Step 1: Access the URL

Step 2: Create account and then login with your credentials

Step 3: Enter a HTML code in the URL



Team ID: Team-593490 **Team Size:** 4

Team Leader: Mohamed Naveed **Team member:** Dharun Ramesh

Team member: Madhuri Santhosh Srinivasan **Team member:** Aravind. S

Project: AI-enhanced intrusion detection system

Vulnerability Name: Improper Privilege management

CWE : CWE - 269

OWASP Category: A04:2021 – Insecure Design

Description: The product does not properly assign, modify, track, or check privileges for an actor, creating an unintended sphere of control for that actor.

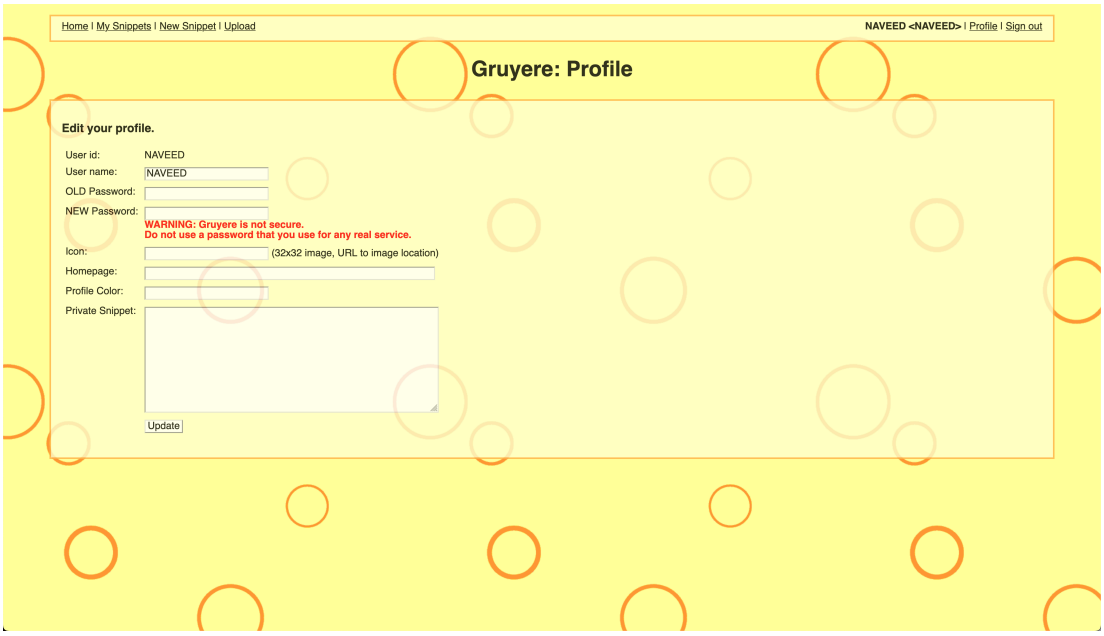
Business Impact:Lack of effective security controls in the design phase often results in an application being susceptible to many weaknesses, collectively known as insecure design vulnerabilities.

Vulnerability Path : https://google-gruyere.appspot.com/editprofile.gtl

Vulnerability Parameter: https://google-gruyere.appspot.com/saveprofile?action=update&is_admin=True

Steps To Reproduce

Step 1: Access the URL



Team ID: Team-593490 **Team Size:** 4

Team Leader: Mohamed Naveed **Team member:** Dharun Ramesh

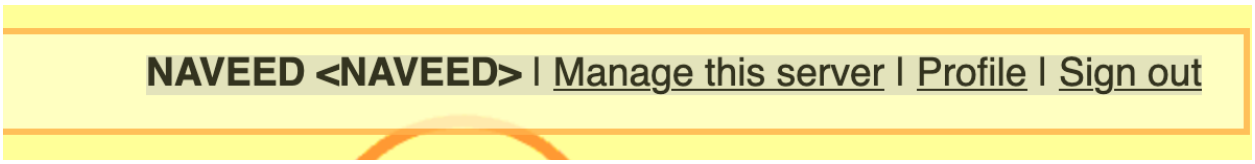
Team member: Madhuri Santhosh Srinivasan **Team member:** Aravind. S

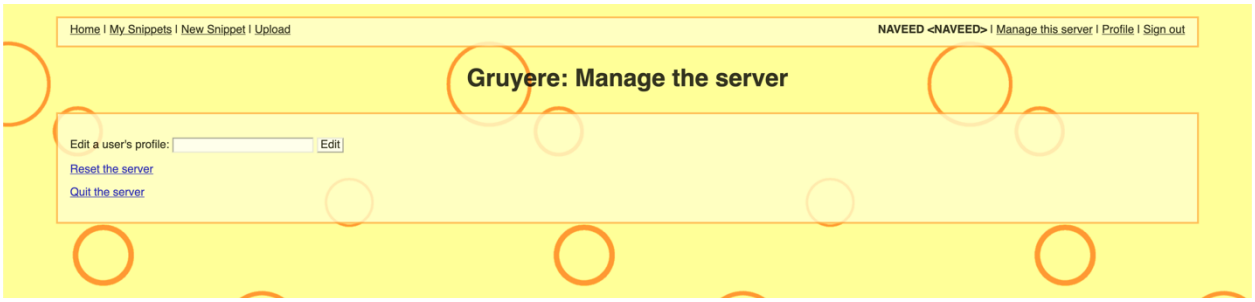
Project: AI-enhanced intrusion detection system

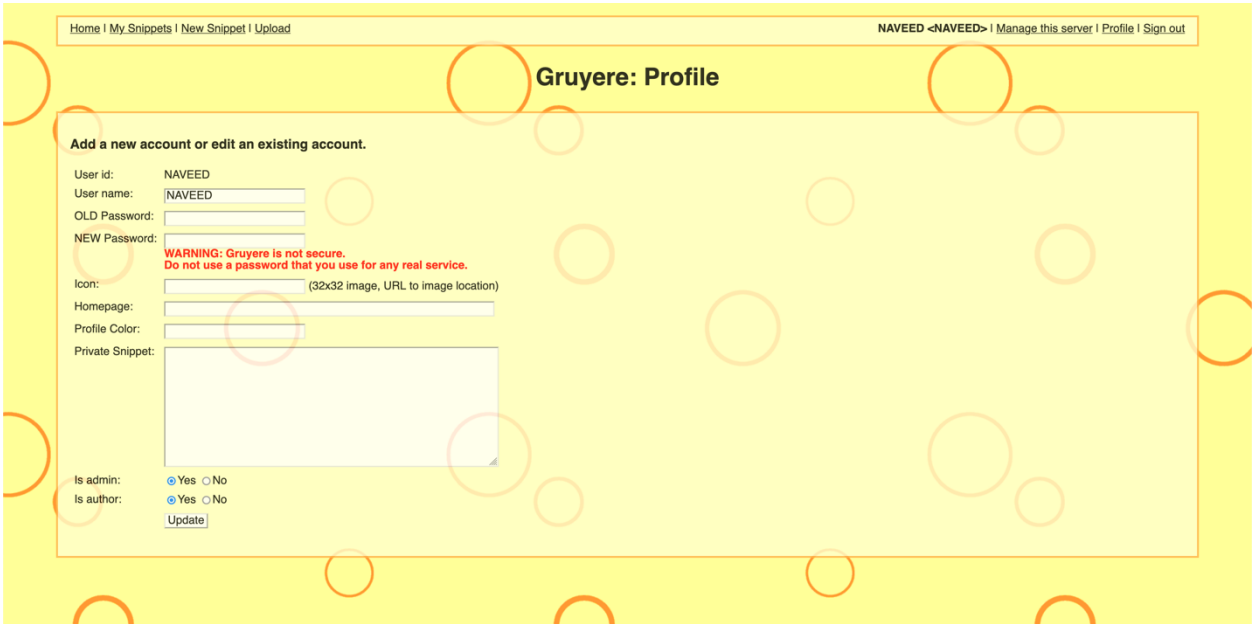
Step 2: Create account and then login with your credentials

Step 3: Enter the given parameters

Step 4: Sign-out and Sign back in







Team ID: Team-593490 **Team Size:** 4

Team Leader: Mohamed Naveed **Team member:** Dharun Ramesh

Team member: Madhuri Santhosh Srinivasan **Team member:** Aravind. S

Project: AI-enhanced intrusion detection system

Vulnerability Name: Reliance on Cookies without Validation and Integrity Checking

CWE : CWE - 565

OWASP Category: A08:2021 - Software and Data Integrity Failures

Description: The product relies on the existence or values of cookies when performing security-critical operations, but it does not properly ensure that the setting is valid for the associated user.

Business Impact: Software and data integrity failures can lead to data corruption, system crashes, and unauthorized access, causing business disruptions, financial losses, and damage to reputation.

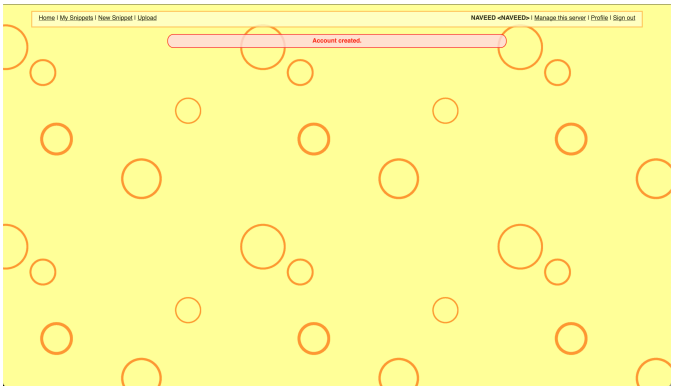
Vulnerability Path : https://google-gruyere.appspot.com/

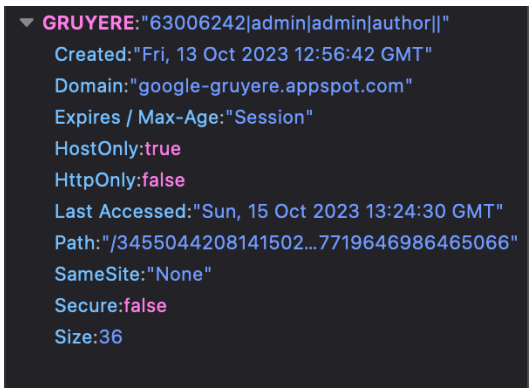
Vulnerability Parameter: https://google-gruyere.appspot.com/saveprofile?action=new&uid=admin|admin|author&pw=12345

Steps To Reproduce

Step 1: Access the URL

Step 2: Enter the parameter





Found the admin|admin|author pattern in the cookie stored

Team ID: Team-593490 **Team Size:** 4

Team Leader: Mohamed Naveed **Team member:** Dharun Ramesh

Team member: Madhuri Santhosh Srinivasan **Team member:** Aravind. S

Project: AI-enhanced intrusion detection system

Vulnerability Name: Cross-Site Request Forgery (CSRF)

CWE : CWE - 352

OWASP Category: A01:2021 – Broken Access Control

Description: The web application does not, or can not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request.

Business Impact: CSRF attacks can lead to unauthorized actions on a user's behalf, potentially causing financial losses and reputation damage, impacting a business's trust and bottom line.

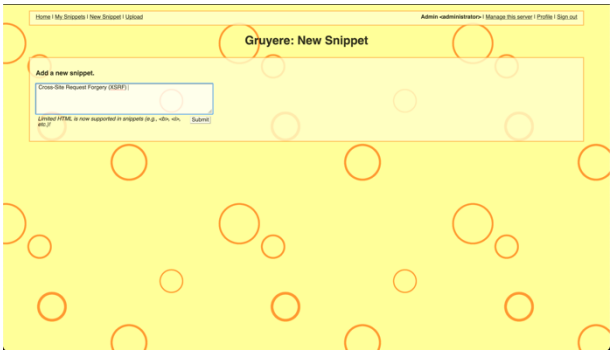
Vulnerability Path : https://google-gruyere.appspot.com/newsnippet.gtl

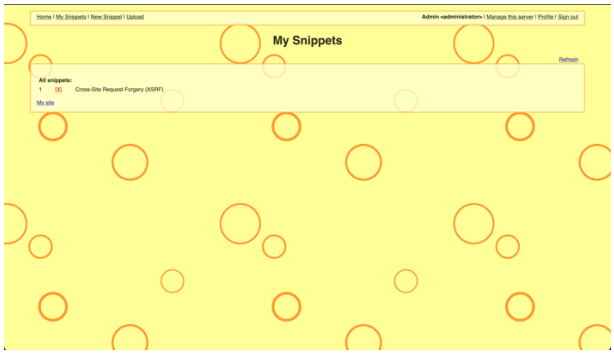
Vulnerability Parameter: https://google-gruyere.appspot.com/deletesnippet?index=0

Steps To Reproduce

Step 1: Access the URL

Step 2: Create a snippet





Step 3: Enter the parameter

Team ID: Team-593490 **Team Size:** 4

Team Leader: Mohamed Naveed **Team member:** Dharun Ramesh

Team member: Madhuri Santhosh Srinivasan **Team member:** Aravind. S

Project: AI-enhanced intrusion detection system

Vulnerability Name: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CWE : CWE - 22

OWASP Category: A01:2021 – Broken Access Control

Description: The product uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the product does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory.

Business Impact: Improper limitation of a pathname can allow unauthorized access to sensitive files, risking data breaches and damaging a company's reputation and legal compliance.

Vulnerability Path : https://google-gruyere.appspot.com/

Vulnerability Parameter: https://google-gruyere.appspot.com/../%2fsecret.txt

Steps To Reproduce

Step 1: Access the URL

Step 2: Enter the parameters

Team ID: Team-593490 **Team Size:** 4

Team Leader: Mohamed Naveed **Team member:** Dharun Ramesh

Team member: Madhuri Santhosh Srinivasan **Team member:** Aravind. S

Project: AI-enhanced intrusion detection system

Vulnerability Name: Uncontrolled Resources Consumption

CWE : CWE - 400

OWASP Category: A09:2004 – Denial Of Service

Description: The product does not properly control the allocation and maintenance of a limited resource, thereby enabling an actor to influence the amount of resources consumed, eventually leading to the exhaustion of available resources.

Business Impact: Uncontrolled resource consumption can lead to system outages, degradation of user experience, and increased operational costs, potentially causing revenue losses and customer dissatisfaction.

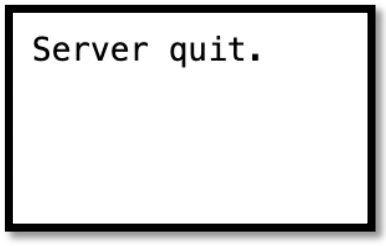
Vulnerability Path : https://google-gruyere.appspot.com/

Vulnerability Parameter: https://google-gruyere.appspot.com/quitserver

Steps To Reproduce

Step 1: Access the URL

Step 2: Enter the parameters



Team ID: Team-593490 **Team Size:** 4

Team Leader: Mohamed Naveed **Team member:** Dharun Ramesh

Team member: Madhuri Santhosh Srinivasan **Team member:** Aravind. S

Project: AI-enhanced intrusion detection system

Vulnerability Name: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CWE : CWE - 79

OWASP Category: A03:2021 – Injection

Description: The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.

Business Impact: Cross-site scripting (XSS) can lead to unauthorized access to user data, damaging trust and reputation, and exposing businesses to legal and financial repercussions.

Vulnerability Path : https://google-gruyere.appspot.com/

Vulnerability Parameter: https://google-gruyere.appspot.com/feed.gtl

Steps To Reproduce

Step 1: Create a HTML file with the below code

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <title>Document</title>
  </head>
  <body>
    <h1 id="snip"></h1>
    <script>
      function _feed(s) {
        document.getElementById("snip").innerHTML = JSON.stringify(s);
      }
    </script>
    <script src="https://google-
gruyere.appspot.com/345504420814150224321947719646986465066/feed.gtl"></script>
  </body>
</html>
```

Team ID: Team-593490

Team Size: 4

Team Leader: Mohamed Naveed

Team member: Dharun Ramesh

Team member: Madhuri Santhosh Srinivasan

Team member: Aravind. S

Project: AI-enhanced intrusion detection system

{"private_snippet":"","cheddar":"Gruyere is the cheesiest application on the web.","brie":"Brie is the queen of the cheeses!!!"}

Team ID: Team-593490 **Team Size:** 4

Team Leader: Mohamed Naveed **Team member:** Dharun Ramesh

Team member: Madhuri Santhosh Srinivasan **Team member:** Aravind. S

Project: AI-enhanced intrusion detection system

Vulnerability Name: Exposure of Sensitive Information to an Unauthorized Actor

CWE : CWE - 200

OWASP Category: A01:2021 – Broken Access Control

Description: The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.

Business Impact: Exposure of sensitive information to an unauthorized actor can result in data breaches, leading to legal consequences, reputation damage, and loss of customer trust.

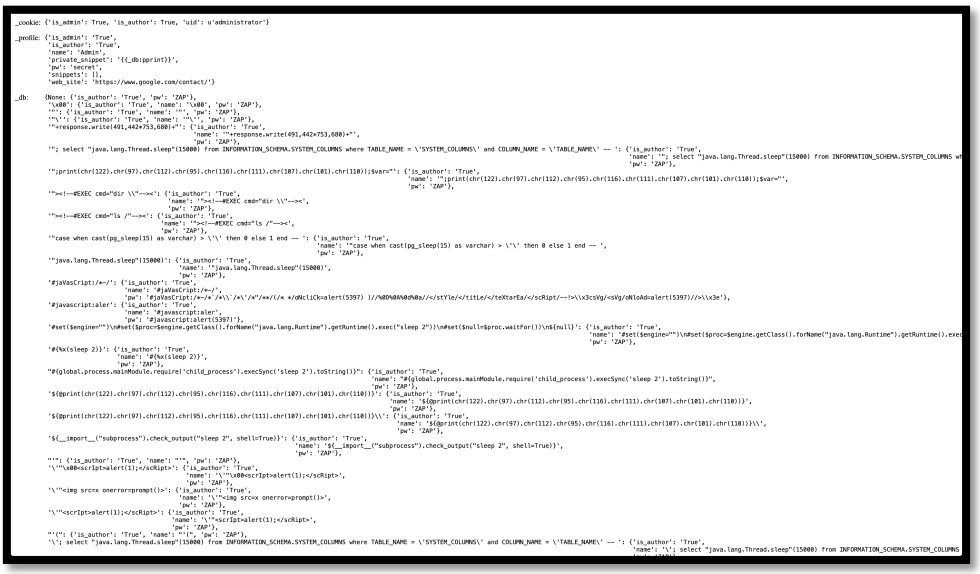
Vulnerability Path : https://google-gruyere.appspot.com/

Vulnerability Parameter: https://google-gruyere.appspot.com/dump.gtl

Steps To Reproduce

Step 1: Access the URL

Step 2: Enter The parameters



Team ID: Team-593490 **Team Size:** 4

Team Leader: Mohamed Naveed **Team member:** Dharun Ramesh

Team member: Madhuri Santhosh Srinivasan **Team member:** Aravind. S

Project: AI-enhanced intrusion detection system

Vulnerability Name: Exposure of Sensitive Information to an Unauthorized Actor

CWE : CWE - 200

OWASP Category: A01:2021 – Broken Access Control

Description: The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.

Business Impact: Exposure of sensitive information to an unauthorized actor can result in data breaches, leading to legal consequences, reputation damage, and loss of customer trust.

Vulnerability Path : https://google-gruyere.appspot.com/editprofile.gtl

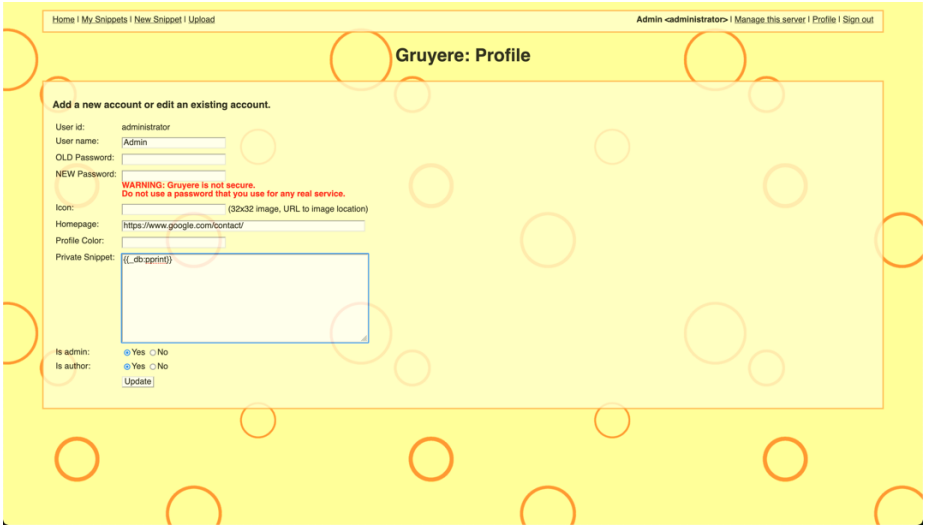
Vulnerability Parameter: {{_db:pprint}}

Steps To Reproduce

Step 1: Access the URL

Step 2: Enter the parameter in My private snippet

Step 3: view your private snippet



Team ID: Team-593490 **Team Size:** 4

Team Leader: Mohamed Naveed **Team member:** Dharun Ramesh

Team member: Madhuri Santhosh Srinivasan **Team member:** Aravind. S

Project: AI-enhanced intrusion detection system