ZAP SCAN REPORT – GOOGLE GRUYERE

https://www.google-gruyere.appspot.com

APRIL 16, 2024

TYLER PROVENCHER
www.linkedin.com/in/tyler-provencher/
www.provenchermultimedia.com

Table of Contents

Section 1: Executive Summary

The OWASP ZAP scan conducted on the Google Gruyere web application revealed several key findings regarding security vulnerabilities. The scan primarily focused on identifying potential risks within the application's functionality and architecture.

1.1: Key Findings

The following vulnerabilities were identified during the OWASP ZAP scan of the Google Gruyere web application, categorized by their corresponding risk severity levels:

High Severity Vulnerabilities Found:

- Cross Site Scripting (Reflected)

Medium Severity Vulnerabilities Found:

- Absence of Anti-CSRF Tokens
- Content Security Policy (CSP) Header Not Set
- Missing Anti-clickjacking Header

Low Severity Vulnerabilities Found:

- Cookie No HttpOnly Flag
- Cookie without SameSite Attribute
- Cross-Domain JavaScript Source File Inclusion
- Strict-Transport-Security Header Not Set
- X-Content-Type-Options Header Missing

Informational Risk Severity Level Vulnerabilities Found:

- Charset Mismatch (Header Versus Meta Content-Type Charset)
- Cookie Poisoning
- Information Disclosure - Suspicious Comments
- Modern Web Application
- Re-examine Cache-control Directives
- Retrieved from Cache
- Session Management Response Identified

- User Agent Fuzzer

The detailed analysis and explanations for the identified vulnerabilities will be provided in Sections 5 of this report. Additionally, actionable recommendations and mitigation strategies to address these vulnerabilities effectively will be outlined in Sections 6.

Section 2: Introduction

The purpose of this scan is twofold: to serve as an academic research endeavor aimed at gaining hands-on experience with web application scanning, report writing, and cybersecurity best practices, and to contribute to a portfolio-building cybersecurity project. This report is my first attempt at conducting a comprehensive web application security scan and compiling a detailed vulnerability assessment report.

2.1: Target Application: Google Gruyere

Google Gruyere (https://google-gruyere.appspot.com) is a deliberately vulnerable web application designed by Google to illustrate common web security vulnerabilities and serve as an educational platform for cybersecurity enthusiasts. It features a range of vulnerabilities, including but not limited to cross-site scripting (XSS) and insecure configuration settings.

The objective of scanning Google Gruyere is to identify and analyze these vulnerabilities using OWASP ZAP, a widely recognized security testing tool, and to document the findings in a structured report format. This project will hopefully enhance my understanding of web application security principles.

As this is my first scan and report in a professional capacity, I approach this endeavor with a commitment to professionalism, accuracy, and thoroughness. The insights gained from this scan will strengthen my capabilities as a cybersecurity professional.

Section 3: Scope of Scan

The scope of the OWASP ZAP scan conducted on the Google Gruyere website (https://google-gruyere.appspot.com) encompassed the following:

1. **URLs:**

   All publicly accessible URLs within the Google Gruyere domain were included in the scan. This includes:

   - https://google-gruyere.appspot.com/
   - Any additional paths and pages within the domain structure.
   - 223 total URLs scanned.

2. **Parameters:**

   The scan targeted all parameters within the URLs, including query parameters, form inputs, and any other user-supplied inputs processed by the web application.

3. **Technologies Tested:**

   The scan covered a range of technologies commonly used in web applications, including but not limited to:

   - Front-end programming languages: HTML, CSS, JavaScript
   - Server-side scripting languages (e.g., Python, Java)
   - Web application frameworks and libraries

Section 4: Methodology

4.1: Scanning Environment

The OWASP ZAP scan was conducted using a dedicated scanning environment configured as follows:

- **Operating System:** Kali Linux 2024.1 (Debian 64-bit)
- **Virtualization Platform:** Oracle VM VirtualBox
- **Virtual Machine Configuration:**
  - **OS:** Kali Linux 2024.1 (Debian 64-bit)
  - **CPU:** AMD64 architecture
  - **Memory:** 4096 MB
  - **Disk Space:** 25 GB

The use of Kali Linux provides a comprehensive suite of security tools and utilities, including OWASP ZAP, for conducting thorough web application security assessments. Oracle VM VirtualBox was selected as the virtualization platform to create an isolated and controlled scanning environment without impacting the host system.

Additional Configuration Details:

- **OWASP ZAP version:** 2.14.0
- **Proxy Settings:** OWASP ZAP configured as a proxy for intercepting and analyzing HTTP(S) traffic during the scan.

This scanning environment ensured a controlled and secure testing environment for conducting the OWASP ZAP scan of the Google Gruyere web application, allowing for accurate vulnerability identification and analysis.

4.2: Testing Approach

The testing approach for the OWASP ZAP scan conducted on the Google Gruyere web application involved utilizing automated scans for all vulnerability categories outlined in the comprehensive scan policy (section 4.3). This approach involved configuring OWASP ZAP to perform automated scans targeting a wide range of vulnerabilities, including but not limited to injection vulnerabilities, information disclosure, server security issues, and miscellaneous attack vectors.

The automated testing approach included the following steps for each vulnerability category:

- **Automated Scans:**
  - OWASP ZAP's active scanning capabilities were leveraged to automatically identify and test for vulnerabilities across multiple categories, including injections (SQL

injection, XSS), information disclosure, server-side vulnerabilities, and miscellaneous attack vectors.

- **Policy-Based Scanning:**
  - The scan policy settings (section 4.4) were applied to ensure comprehensive coverage of potential security weaknesses and vulnerabilities within the Google Gruyere application.
- **Detection and Analysis:**
  - OWASP ZAP automatically detected and analyzed HTTP(S) requests and responses, looking for pattern's indicative of known vulnerabilities such as SQL injection, XSS, path traversal, and more.
- **Reporting and Analysis:**
  - Upon completion of the automated scans, OWASP ZAP generated a detailed report highlighting the identified vulnerabilities, including severity levels, affected URLs, and potential impact.

This testing approach facilitated a comprehensive evaluation of the Google Gruyere web application's security posture, leveraging automated scans across diverse vulnerability categories to identify and prioritize potential security weaknesses and vulnerabilities.

4.3: Scan Depth

The OWASP ZAP scan conducted on the Google Gruyere web application was a surface-level scan focused on accessible URLs and parameters. This approach targeted the publicly available and commonly accessed areas of the application without delving into hidden or restricted areas.

Key Focus Areas:

- The scan prioritized scanning URLs and parameters accessible to regular users without requiring privileged access or specific authentication credentials.
- Commonly used functionalities and features of the Google Gruyere application were thoroughly scanned for potential security vulnerabilities.

Exclusion of Hidden or Restricted Areas:

- The scan did not include deep scanning of hidden or restricted areas of the application that would typically require specialized permissions or authentication beyond standard user access.

By focusing on surface-level scanning, the objective was to identify and analyze security vulnerabilities and weaknesses in the publicly accessible components of the Google Gruyere web application, providing insights into potential risks that could affect regular users interacting with the application.

4.4: Scan Policies

The OWASP ZAP scan was conducted with a comprehensive scan policy designed to cover a wide range of security vulnerabilities and attack vectors. The scan policy settings used for this assessment are outlined below:

- **Client-Browser:**
  - Cross Site Scripting (DOM Based)

- **Information Gathering:**
  - .env Information Leak
  - .htaccess Information Leak
  - Directory Browsing
  - ELMAH Information Leak
  - Heartbleed OpenSSL Vulnerability
  - Hidden File Finder
  - Remote Code Execution - CVE-2012-1823
  - Source Code Disclosure - /WEB-INF Folder
  - Source Code Disclosure - CVE-2012-1823
  - Spring Actuator Information Leak
  - Trace.axd Information Leak
  - User Agent Fuzzer

- **Injection:**

- Buffer Overflow
- Cloud Metadata Potentially Exposed
- CRLF Injection
- Cross Site Scripting (Persistent)
- Cross Site Scripting (Persistent) – Prime
- Cross Site Scripting (Persistent) – Spider
- Cross Site Scripting (Reflected)
- Format String Error
- Parameter Tampering
- Remote OS Command Injection
- Server Side Code Injection
- Server Side Include
- Server Side Template Injection
- Server Side Template Injection (Blind)
- Spring4Shell
- SQL Injection
- SQL Injection - Hypersonic SQL
- SQL Injection – MsSQL
- SQL Injection – MySQL
- SQL Injection – Oracle
- SQL Injection – PostgreSQL
- SQL Injection – SQLite
- XML External Entity Attack
- XPath Injection
- XSLT Injection

- **Miscellaneous:**
  - External Redirect
  - Generic Padding Oracle
  - GET for POST
  - Log4Shell
  - Script Active Scan Rules
  - SOAP Action Spoofing (Beta)
  - SOAP XML Injection (Beta)

- **Server Security:**
  - Path Traversal
  - Remote File Inclusion

Each vulnerability category was scanned using default thresholds and strengths, with a focus on identifying potential security weaknesses and vulnerabilities within the Google Gruyere web application.

Section 5: Scan Findings

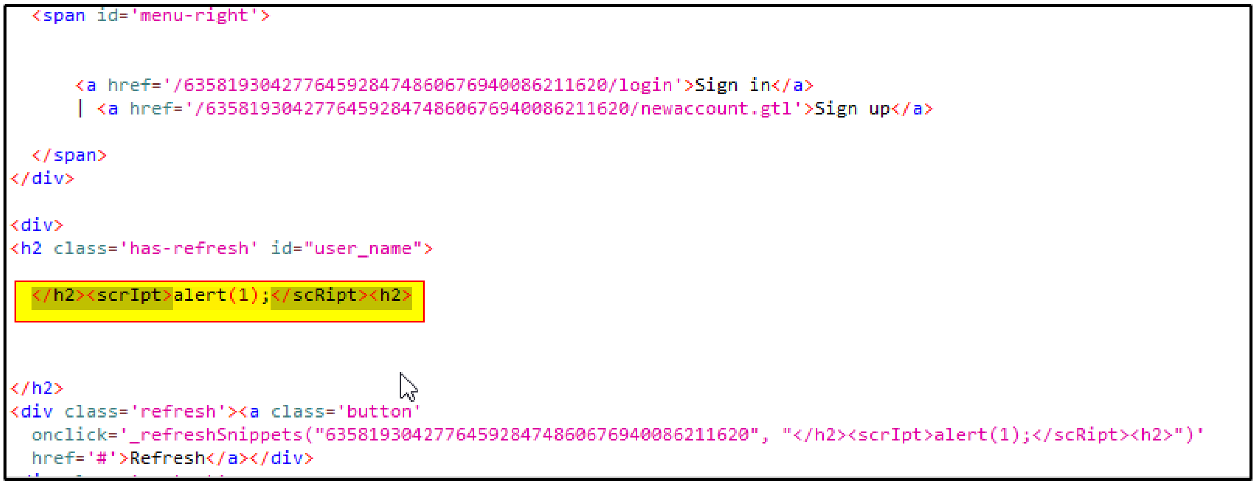
This section delves into an in-depth examination of vulnerabilities unearthed during the OWASP ZAP scan of the Google Gruyere web application. The vulnerabilities are classified based on their severity levels, ranging from high-risk vulnerabilities necessitating immediate attention to lower-risk issues that still merit mitigation measures. Each vulnerability is elaborated on with specific details, including the affected URL (a full list of the affected URLs for each vulnerability will be provided in section 8.1: Affected URLs), parameters, potential impacts, and the consequences if not addressed. The insights provided here aim to illuminate the security posture of the application and underline the importance of enhancing its resilience against potential threats.

5.1: High Severity Vulnerabilities

These vulnerabilities are categorized as high severity due to their potential to cause significant harm or compromise to the system. They require immediate attention and remediation to prevent exploitation by malicious actors.

1. **Cross Site Scripting (Reflected)**
   - **URL:** http://google-gruyere.appspot.com/635819304277645928474860676940086211620/snippets.gtl?uid=%3C%2Fh2%3E%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E%3Ch2%3E
   - **Risk:** High
   - **Confidence:** Medium
   - **Parameter:** uid

- **Description:** Cross-Site Scripting (XSS) is a high-risk vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users. In this case, the absence of input sanitization in the URL parameter 'uid' of the snippets page exposes users to potential script execution attacks. This vulnerability could allow an attacker to execute arbitrary code in a user's browser instance.



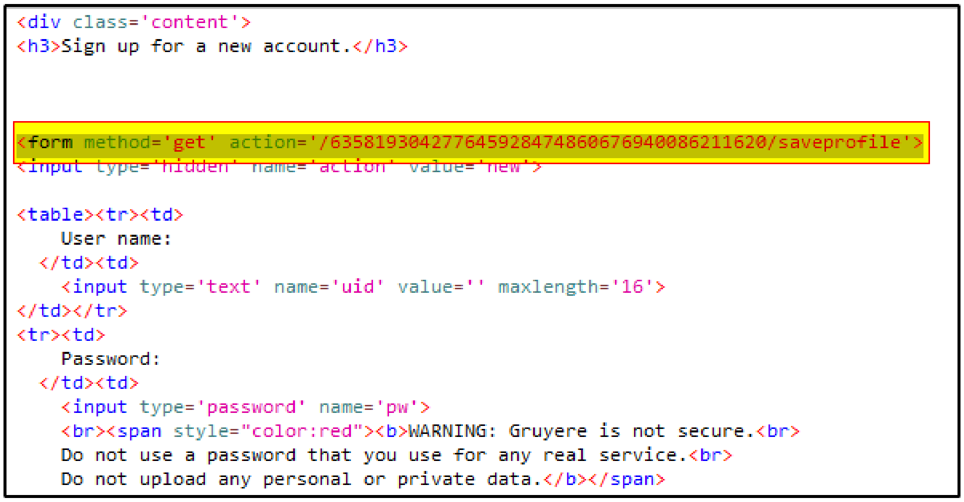
```
  <span id='menu-right'>


      <a href='/635819304277645928474860676940086211620/login'>Sign in</a>
      | <a href='/635819304277645928474860676940086211620/newaccount.gtl'>Sign up</a>

  </span>
</div>

<div>
<h2 class='has-refresh' id="user_name">

  </h2><scrIpt>alert(1);</scRipt><h2>



</h2>
<div class='refresh'><a class='button'
  onclick='_refreshSnippets("635819304277645928474860676940086211620", "</h2><scrIpt>alert(1);</scRipt><h2>")'
  href='#'>Refresh</a></div>
```

5.2: Medium Severity Vulnerabilities

These vulnerabilities are considered medium severity as they pose a moderate risk to the system's security and functionality. While not as critical as high severity vulnerabilities, they still need to be addressed promptly to minimize potential threats.

2. Absence of Anti-CSRF Tokens

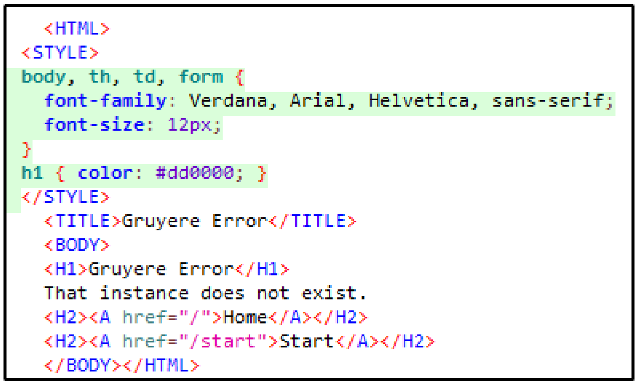
- **URL:** http://google-gruyere.appspot.com/635819304277645928474860676940086211620/newaccount.gtl
- **Risk:** Medium
- **Confidence:** Low
- **Description:** The absence of Anti-CSRF Tokens in HTML forms leaves the application vulnerable to Cross-Site Request Forgery (CSRF) attacks. Without proper token validation, attackers could forge requests on behalf of authenticated users, leading to unauthorized actions. No Anti-CSRF tokens found in a HTML submission form, exposing the application to Cross-Site Request Forgery (CSRF) attacks.



```
<div class='content'>
<h3>Sign up for a new account.</h3>


<form method='get' action='/635819304277645928474860676940086211620/saveprofile'>
<input type='hidden' name='action' value='new'>

<table><tr><td>
    User name:
  </td><td>
    <input type='text' name='uid' value='' maxlength='16'>
</td></tr>
<tr><td>
    Password:
  </td><td>
    <input type='password' name='pw'>
    <br><span style="color:red"><b>WARNING: Gruyere is not secure.<br>
    Do not use a password that you use for any real service.<br>
    Do not upload any personal or private data.</b></span>
```

3. Content Security Policy (CSP) Header Not Set

- **URL:** https://google-gruyere.appspot.com/7
- **Risk:** Medium
- **Confidence:** High
- **Description:** The absence of Anti-clickjacking headers makes the application susceptible to ClickJacking attacks, urging the implementation of X-Frame-Options or Content-Security-Policy headers for protection against such threats.

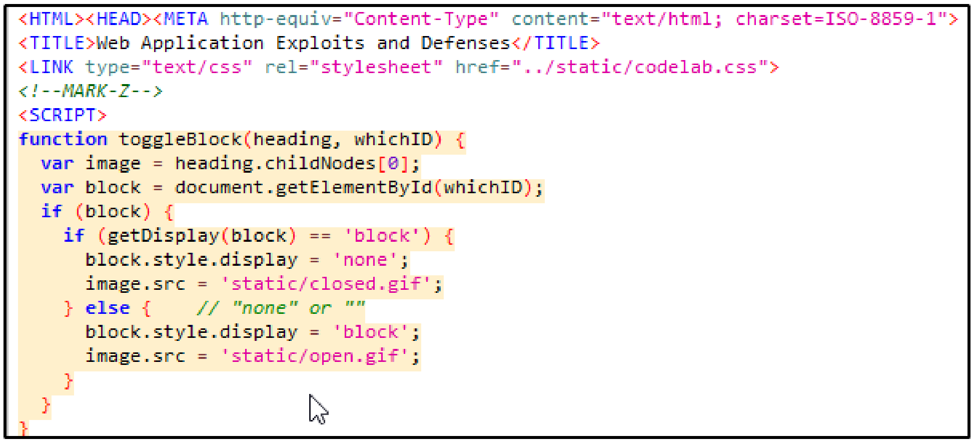


```
  <HTML>
<STYLE>
body, th, td, form {
  font-family: Verdana, Arial, Helvetica, sans-serif;
  font-size: 12px;
}
h1 { color: #dd0000; }
</STYLE>
  <TITLE>Gruyere Error</TITLE>
  <BODY>
  <H1>Gruyere Error</H1>
  That instance does not exist.
  <H2><A href="/">Home</A></H2>
  <H2><A href="/start">Start</A></H2>
  </BODY></HTML>
```

4. Missing Anti-clickjacking Header

- **URL:** http://google-gruyere.appspot.com/2 & 111 other URLs.
- **Risk:** Medium

- **Confidence:** Medium
- **Description:** Absence of Anti-clickjacking headers exposes the application to ClickJacking attacks, where malicious entities can trick users into interacting with hidden or disguised elements.



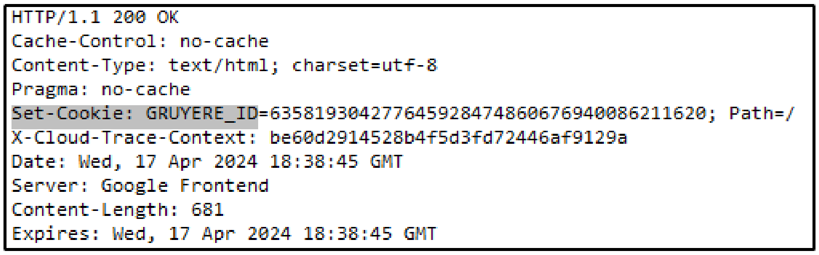
```
<HTML><HEAD><META http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<TITLE>Web Application Exploits and Defenses</TITLE>
<LINK type="text/css" rel="stylesheet" href="../static/codelab.css">
<!--MARK-Z-->
<SCRIPT>
function toggleBlock(heading, whichID) {
  var image = heading.childNodes[0];
  var block = document.getElementById(whichID);
  if (block) {
    if (getDisplay(block) == 'block') {
      block.style.display = 'none';
      image.src = 'static/closed.gif';
    } else {    // "none" or ""
      block.style.display = 'block';
      image.src = 'static/open.gif';
    }
  }
}
```

5.3: Low Severity Vulnerabilities

Low severity vulnerabilities are typically less urgent but still require attention and mitigation measures. Although they may not pose an immediate threat, addressing them helps improve overall system security and resilience against potential attacks.

5. Cookie No HttpOnly Flag

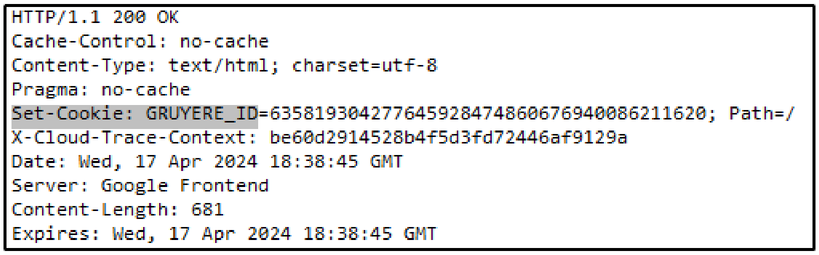
- **URL:** http://google-gruyere.appspot.com/start
- **Risk:** Low
- **Confidence:** Medium
- **Parameter:** GRUYERE_ID
- **Description:** A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page, then the cookie will be accessible and can be transmitted to another site. If this is a session cookie, then session hijacking may be possible.



```
HTTP/1.1 200 OK
Cache-Control: no-cache
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Set-Cookie: GRUYERE_ID=635819304277645928474860676940086211620; Path=/
X-Cloud-Trace-Context: be60d2914528b4f5d3fd72446af9129a
Date: Wed, 17 Apr 2024 18:38:45 GMT
Server: Google Frontend
Content-Length: 681
Expires: Wed, 17 Apr 2024 18:38:45 GMT
```

6. Cookie without SameSite Attribute

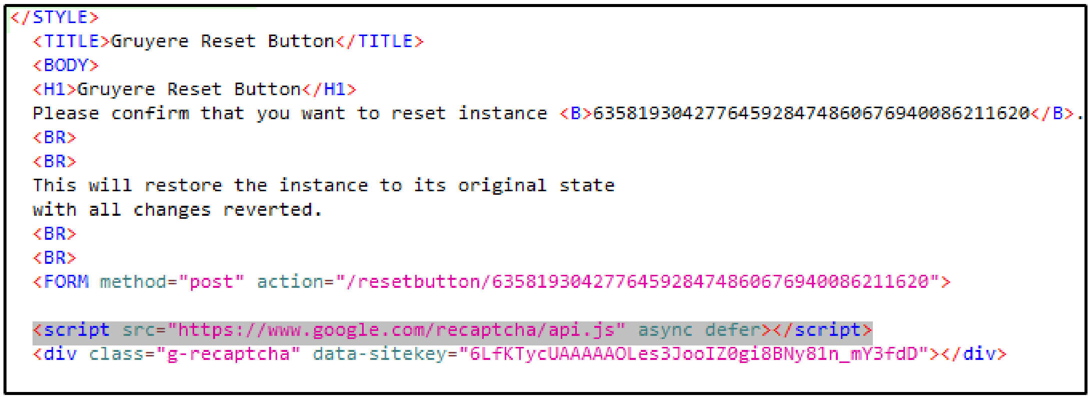
- **URL:** http://google-gruyere.appspot.com/start
- **Risk:** Low
- **Confidence:** Medium
- **Parameter:** GRUYERE_ID
- **Description:** A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective countermeasure to cross-site request forgery, cross-site script inclusion, and timing attacks.



```
HTTP/1.1 200 OK
Cache-Control: no-cache
Content-Type: text/html; charset=utf-8
Pragma: no-cache
Set-Cookie: GRUYERE_ID=635819304277645928474860676940086211620; Path=/
X-Cloud-Trace-Context: be60d2914528b4f5d3fd72446af9129a
Date: Wed, 17 Apr 2024 18:38:45 GMT
Server: Google Frontend
Content-Length: 681
Expires: Wed, 17 Apr 2024 18:38:45 GMT
```

7. Cross-Domain JavaScript Source File Inclusion

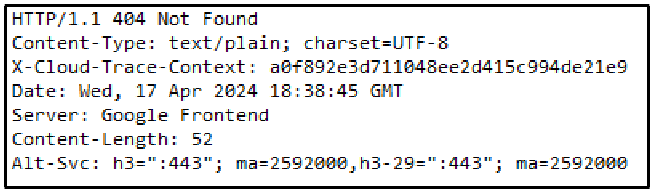
- **URL:** https://google-gruyere.appspot.com/resetbutton/635819304277645928474860676940086211620
- **Risk:** Low
- **Confidence:** Medium
- **Parameter:** https://www.google.com/recaptcha/api.js
- **Description:** The page includes one or more script files from a third-party domain, potentially introducing security risks such as script injection and data leakage.



```
</STYLE>
  <TITLE>Gruyere Reset Button</TITLE>
  <BODY>
  <H1>Gruyere Reset Button</H1>
  Please confirm that you want to reset instance <B>635819304277645928474860676940086211620</B>.
  <BR>
  <BR>
  This will restore the instance to its original state
  with all changes reverted.
  <BR>
  <BR>
  <FORM method="post" action="/resetbutton/635819304277645928474860676940086211620">

  <script src="https://www.google.com/recaptcha/api.js" async defer></script>
  <div class="g-recaptcha" data-sitekey="6LfKTycUAAAAAOLes3JooIZ0gi8BNy81n_mY3fdD"></div>
```

8. Strict-Transport-Security Header Not Set

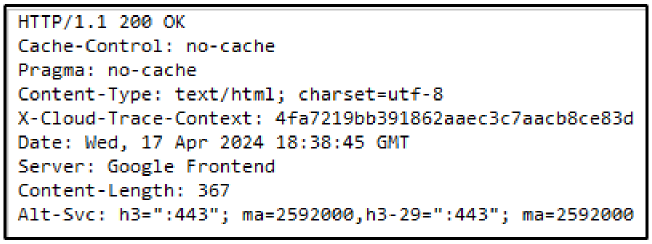
- **URL:** https://google-gruyere.appspot.com/start.
- **Risk:** Low
- **Confidence:** High
- **Description:** HTTP Strict Transport Security (HSTS) header is not set, leaving the application vulnerable to downgrade attacks and protocol downgrade risks.



```
HTTP/1.1 404 Not Found
Content-Type: text/plain; charset=UTF-8
X-Cloud-Trace-Context: a0f892e3d711048ee2d415c994de21e9
Date: Wed, 17 Apr 2024 18:38:45 GMT
Server: Google Frontend
Content-Length: 52
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

9. X-Content-Type-Options Header Missing

- **URL:** http://google-gruyere.appspot.com/static/codelab.css
- **Risk:** Low
- **Confidence:** Medium
- **Description:** The X-Content-Type-Options header is missing, allowing older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body. This could lead to misinterpretation and display of the response body as a content type other than the declared one, potentially exposing security vulnerabilities.



```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: text/html; charset=utf-8
X-Cloud-Trace-Context: 4fa7219bb391862aaec3c7aacb8ce83d
Date: Wed, 17 Apr 2024 18:38:45 GMT
Server: Google Frontend
Content-Length: 367
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
```

5.4: Informational Severity Vulnerabilities

Informational severity level vulnerabilities, while not posing an immediate threat, provide valuable insights and recommendations to enhance system security and reduce potential risks.

10. Charset Mismatch (Header Versus Meta Content-Type Charset)

- **URL:** http://google-gruyere.appspot.com/part2
- **Risk:** Informational
- **Confidence:** Low
- **Description:** The charset mismatch between the HTTP Content-Type header and the content body's charset declaration can lead to content-sniffing vulnerabilities, potentially allowing attackers to manipulate content encoding and execute script injections.

11. Cookie Poisoning

- **URL:** http://google-gruyere.appspot.com/635819304277645928474860676940086211620/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
- **Risk:** Informational
- **Confidence:** Low
- **Description:** Detects potential cookie poisoning attacks where user-controlled inputs influence cookie parameters. Such issues may not be directly exploitable but indicate a security oversight.

12. Information Disclosure - Suspicious Comments

- **URL:** http://google-gruyere.appspot.com/code/resources/lib.js
- **Risk:** Informational
- **Confidence:** Low

- **Description:** Identifies suspicious comments in responses that may inadvertently leak information useful to attackers. While not directly exploitable, it suggests areas for code refinement.

13. Modern Web Application

- **URL:** http://google-gruyere.appspot.com/part1
- **Risk:** Informational
- **Confidence:** Medium
- **Description:** Flags the application as a modern web app, indicating potential differences in testing approach compared to traditional web apps.

14. Re-examine Cache-control Directives

- **URL:** https://google-gruyere.appspot.com/
- **Risk:** Informational
- **Confidence:** Low
- **Description:** Highlights issues with cache-control headers, potentially leading to unintended caching of sensitive content.

15. Retrieved from Cache

- **URL:** http://google-gruyere.appspot.com/static/codelab.css
- **Risk:** Informational
- **Confidence:** Medium
- **Description:** Notes content retrieved from cache, highlighting potential information leakage risks.

16. Session Management Response Identified

- **URL:** http://google-gruyere.appspot.com/start
- **Risk:** Informational
- **Confidence:** Medium
- **Description:** Identifies a response containing session management tokens, suggesting potential session management methods.

17. User Agent Fuzzer

- **URL:** http://google-gruyere.appspot.com/635819304277645928474860676940086211620/login?pw=ZAP&uid=ZAP
- **Risk:** Informational
- **Confidence:** Medium
- **Description:** Tests for response variations based on different User-Agent headers, aiding in understanding site behavior under different user contexts.

Section 6: Recommended Actions

This section includes recommended actions to mitigate the vulnerabilities found from the ZAP scan.

6.1: Cross Site Scripting (Reflected)

- **Priority:** High
- **Immediate Action**:
  - Implement input validation and output encoding to prevent XSS attacks.
  - Use vetted libraries/frameworks like Microsoft's Anti-XSS library or OWASP ESAPI Encoding module.
  - Set HttpOnly flag for session cookies to mitigate cookie theft.
- **Reference:**
  - OWASP XSS Prevention Cheat Sheet: https://owasp.org/www-community/attacks/xss/
  - CWE-79: https://cwe.mitre.org/data/definitions/79.html

6.2: Absence of Anti-CSRF Tokens

- **Priority:** Medium
- **Action:**
  - Implement Anti-CSRF tokens in HTML forms to prevent CSRF attacks.
- **Reference:**
  - OWASP CSRF Prevention Cheat Sheet**:** https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

- CWE-352: https://cwe.mitre.org/data/definitions/352.html

6.3: Content Security Policy (CSP) Header Not Set

- **Priority:** Medium
- **Action**:
  - Configure the web server/application to set the Content-Security-Policy header.
- **Reference:**
  - Mozilla CSP Documentation: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
  - OWASP Content Security Policy Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

6.4: Missing Anti-clickjacking Header

- **Priority:** Medium
- **Action:**
  - Set X-Frame-Options or Content-Security-Policy header to prevent clickjacking attacks.
- **Reference:**
  - Mozilla X-Frame-Options Documentation: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
  - OWASP Clickjacking Prevention Cheat Sheet: https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking

6.5: Cookie No HttpOnly Flag

- **Priority:** Low
- **Action:**
  - Set the HttpOnly flag for all cookies to prevent access by JavaScript.
- **Reference:**
  - OWASP HttpOnly Flag: https://owasp.org/www-community/HttpOnly

6.6: Cookie without Same Site Attribute

- **Priority:** Low
- **Action:**
  - Set the SameSite attribute to 'Lax' or 'Strict' for all cookies.
- **Reference:**
  - IETF SameSite Attribute: https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-cookie-same-site

6.7: Cross-Domain JavaScript Source File Inclusion

- **Priority:** Low
- **Action:**
  - Load JavaScript source files only from trusted sources.
- **Reference:**
  - OWASP 2021 A08: https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/

6.8: Strict-Transport-Security Header Not Set

- **Priority:** Low
- **Action:**
  - Configure the server to enforce Strict-Transport-Security.
- **Reference:**
  - OWASP Security Headers: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

6.9: X-Content-Type-Options Header Missing

- **Priority:** Low
- **Action:**
  - Set X-Content-Type-Options header to 'nosniff' for all web pages.
- **Reference:**
  - Mozilla X-Content-Type-Options Documentation: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

6.10: Charset Mismatch (Header Versus Meta Content-Type Charset)

- **Priority: Informational**
- **Action:**
  - Ensure consistency between HTTP Content-Type header and HTML body charset declaration.
- **Reference:**
  - Browser Security Part 2: https://code.google.com/archive/p/browsersec/wikis/Part2.wiki#Character_set_handling_and_detection

6.11: Cookie Poisoning:

- **Priority:** Informational
- **Action:**
  - Avoid allowing user input to control cookie names and values.
- **Reference:**
  - OWASP 2021 A03: https://owasp.org/Top10/A03_2021-Injection/

6.12: Information Disclosure - Suspicious Comments

- **Priority:** Informational
- **Action:**
  - Remove suspicious comments that may aid attackers.
- **Reference:**
  - OWASP 2021 A01: https://owasp.org/Top10/A01_2021-Broken_Access_Control/

6.13: Modern Web Application

- **Priority:** Informational
- **Action:**
- No specific action required; informational alert about the application type.

6.14: Re-examine Cache-control Directives:

- **Priority:** Informational
- **Action:**
  - Review and set cache-control directives appropriately.
- **Reference:**
  - OWASP Web Content Caching: https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching

6.15: Retrieved from Cache

- **Priority**: Informational
- **Action:**
  - Validate responses to ensure sensitive information is not cached.
- **Reference:**
  - RFC7234: https://datatracker.ietf.org/doc/html/rfc7234

6.16: Session Management Response Identified

- **Priority:** Informational
- **Action:**
  - No action required; informational alert about session management.
- **Reference:** No action needed.

6.16: User Agent Fuzzer

- **Priority:** Informational
- **Action:**
  - Check for differences in response based on fuzzed User Agent.
- **Reference:**
  - OWASP User Agent Fuzzer: https://owasp.org/www-project-web-security-testing-guide/

Section 7: Conclusion

The OWASP ZAP scan conducted on the Google Gruyere web application has unveiled a spectrum of vulnerabilities across various severity levels, ranging from high-risk cross-site scripting (XSS) vulnerabilities to informational findings such as Charset Mismatch and cookie poisoning alerts. These findings underscore the critical importance of promptly addressing vulnerabilities to enhance the overall security posture of the application, mitigate potential risks associated with data breaches and unauthorized access, and demonstrate a proactive approach to cybersecurity best practices. This comprehensive scan not only serves as an invaluable academic research endeavor, providing hands-on experience with web application scanning, report writing, and vulnerability assessment, but also contributes significantly to a portfolio-building cybersecurity project, marking a pivotal milestone in my professional development and proficiency in the field of cybersecurity.

7.1: Key Findings

- ❖ **High Severity Vulnerabilities:**
  - ➢ The presence of Cross-Site Scripting (XSS) vulnerabilities, especially the reflected XSS found in the 'uid' parameter of the snippets page, poses a significant risk of code execution in users' browsers. Immediate action is imperative to mitigate this threat.
- ❖ **Medium Severity Vulnerabilities:**
  - ➢ Absence of Anti-CSRF Tokens in HTML forms and the lack of Content Security Policy (CSP) headers and Anti-clickjacking headers are notable vulnerabilities that require prompt attention to prevent CSRF attacks and Clickjacking exploits.
- ❖ **Low Severity Vulnerabilities:**
  - ➢ Low severity issues such as missing HttpOnly flag for cookies, absence of the SameSite attribute, and Cross-Domain JavaScript Source File Inclusion may not be as critical but still demand mitigation to bolster the application's defense against potential threats.
- ❖ **Informational Severity Vulnerabilities:**
  - ➢ Informational findings like Charset Mismatch, Cookie Poisoning potential, and Information Disclosure in comments offer insights for refining security measures and best practices.

8.2: Importance of Addressing Vulnerabilities:

Addressing vulnerabilities promptly is paramount to enhance security for several reasons:

- **Risk Mitigation**: Timely mitigation reduces the window of opportunity for attackers to exploit vulnerabilities, mitigating potential risks and minimizing the impact of security breaches.
- **Compliance:** Promptly addressing vulnerabilities aligns with regulatory compliance requirements, ensuring the application meets industry standards and legal obligations.
- **User Trust:** Proactive security measures demonstrate a commitment to user safety and trust, enhancing the reputation of the application and its brand.
- **Cost Efficiency:** Resolving vulnerabilities early in the development lifecycle is more cost-effective than dealing with the repercussions of a security incident later, including potential legal, financial, and reputational consequences.

In conclusion, the OWASP ZAP scan findings underscore the critical need for proactive security measures and prompt vulnerability remediation to fortify the Google Gruyere web application against evolving cyber threats and ensure a resilient and secure user experience.

Section 8: Appendix

8.1 Affected URLs:

This section includes all the affected URLs of the web application separated by the vulnerability.

8.1.1: OWASP XSS Prevention Cheat Sheet:

- GET: http://google-gruyere.appspot.com/635819304277645928474860676940086211620/snippets.gtl?uid=%3C%2Fh2%3E%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E%3Ch2%3E

8.1.2: Absence of Anti-CSRF Tokens:

- GET: http://google-gruyere.appspot.com/635819304277645928474860676940086211620/login
- GET: http://google-gruyere.appspot.com/635819304277645928474860676940086211620/login?pw=ZAP&uid=ZAP

- GET: http://google-gruyere.appspot.com/635819304277645928474860676940086211620/newaccount.gtl
- GET: https://google-gruyere.appspot.com/635819304277645928474860676940086211620/login
- GET: https://google-gruyere.appspot.com/635819304277645928474860676940086211620/newaccount.gtl
- GET: https://google-gruyere.appspot.com/resetbutton/635819304277645928474860676940086211620

8.1.3: Content Security Policy (CSP) Header Not Set:

- GET: http://google-gruyere.appspot.com
- GET: http://google-gruyere.appspot.com/
- GET: http://google-gruyere.appspot.com/0
- GET: http://google-gruyere.appspot.com/1
- GET: http://google-gruyere.appspot.com/2
- GET: http://google-gruyere.appspot.com/3
- GET: http://google-gruyere.appspot.com/4
- GET: http://google-gruyere.appspot.com/5
- GET: http://google-gruyere.appspot.com/6
- GET: http://google-gruyere.appspot.com/635819304277645928474860676940086211620/
- GET: http://google-gruyere.appspot.com/635819304277645928474860676940086211620/login
- GET: http://google-gruyere.appspot.com/635819304277645928474860676940086211620/login?pw=ZAP&uid=ZAP
- GET: http://google-gruyere.appspot.com/635819304277645928474860676940086211620/newaccount.gtl
- GET: http://google-gruyere.appspot.com/635819304277645928474860676940086211620/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
- GET: http://google-gruyere.appspot.com/635819304277645928474860676940086211620/snippets.gtl?uid=brie
- GET: http://google-gruyere.appspot.com/635819304277645928474860676940086211620/snippets.gtl?uid=cheddar
- GET: http://google-gruyere.appspot.com/7
- GET: http://google-gruyere.appspot.com/8
- GET: http://google-gruyere.appspot.com/9
- GET: http://google-gruyere.appspot.com/code/
- GET: http://google-gruyere.appspot.com/code/?data.py
- GET: http://google-gruyere.appspot.com/code/?gruyere.py
- GET: http://google-gruyere.appspot.com/code/?gtl.py
- GET: http://google-gruyere.appspot.com/code/?resoources/dump.gtl
- GET: http://google-gruyere.appspot.com/code/?resources/dump.gtl
- GET: http://google-gruyere.appspot.com/code/?resources/editprofile.gtl
- GET: http://google-gruyere.appspot.com/code/?resources/error.gtl
- GET: http://google-gruyere.appspot.com/code/?resources/feed.gtl
- GET: http://google-gruyere.appspot.com/code/?resources/home.gtl
- GET: http://google-gruyere.appspot.com/code/?resources/manage.gtl
- GET: http://google-gruyere.appspot.com/code/?resources/menubar.gtl
- GET: http://google-gruyere.appspot.com/code/?sanitize.py
- GET: http://google-gruyere.appspot.com/code/data.py
- GET: http://google-gruyere.appspot.com/code/gruyere.py
- GET: http://google-gruyere.appspot.com/code/gtl.py
- GET: http://google-gruyere.appspot.com/code/resources/base.css
- GET: http://google-gruyere.appspot.com/code/resources/dump.gtl
- GET: http://google-gruyere.appspot.com/code/resources/editprofile.gtl
- GET: http://google-gruyere.appspot.com/code/resources/error.gtl
- GET: http://google-gruyere.appspot.com/code/resources/feed.gtl

- GET: http://google-gruyere.appspot.com/code/resources/home.gtl
- GET: http://google-gruyere.appspot.com/code/resources/lib.js
- GET: http://google-gruyere.appspot.com/code/resources/login.gtl
- GET: http://google-gruyere.appspot.com/code/resources/manage.gtl
- GET: http://google-gruyere.appspot.com/code/resources/menubar.gtl
- GET: http://google-gruyere.appspot.com/code/resources/newaccount.gtl
- GET: http://google-gruyere.appspot.com/code/resources/newsnippet.gtl
- GET: http://google-gruyere.appspot.com/code/resources/showprofile.gtl
- GET: http://google-gruyere.appspot.com/code/resources/snippets.gtl
- GET: http://google-gruyere.appspot.com/code/resources/upload.gtl
- GET: http://google-gruyere.appspot.com/code/resources/upload2.gtl
- GET: http://google-gruyere.appspot.com/code/sanitize.py
- GET: http://google-gruyere.appspot.com/code/secret.txt
- GET: http://google-gruyere.appspot.com/part1
- GET: http://google-gruyere.appspot.com/part2
- GET: http://google-gruyere.appspot.com/part3
- GET: http://google-gruyere.appspot.com/part4
- GET: http://google-gruyere.appspot.com/part5
- GET: http://google-gruyere.appspot.com/start
- GET: http://google-gruyere.appspot.com/static/codeindex.html
- GET: http://google-gruyere.appspot.com/static/codeindex/html
- GET: https://google-gruyere.appspot.com/
- GET: https://google-gruyere.appspot.com/635819304277645928474860676940086211620/
- GET: https://google-gruyere.appspot.com/635819304277645928474860676940086211620/feed.gtl
- GET: https://google-gruyere.appspot.com/635819304277645928474860676940086211620/login
- GET: https://google-gruyere.appspot.com/635819304277645928474860676940086211620/newaccount.gtl
- GET: https://google-gruyere.appspot.com/635819304277645928474860676940086211620/quitserver.
- GET: https://google-gruyere.appspot.com/635819304277645928474860676940086211620/RESET.
- GET: https://google-gruyere.appspot.com/635819304277645928474860676940086211620/saveprofile?action=update&is_admin=True
- GET: https://google-gruyere.appspot.com/635819304277645928474860676940086211620/saveprofile?action=update&is_admin=True&uid=username
- GET: https://google-gruyere.appspot.com/code/
- GET: https://google-gruyere.appspot.com/code/?data.py
- GET: https://google-gruyere.appspot.com/code/?gruyere.py
- GET: https://google-gruyere.appspot.com/code/?gtl.py
- GET: https://google-gruyere.appspot.com/code/?resoources/dump.gtl
- GET: https://google-gruyere.appspot.com/code/?resources/dump.gtl
- GET: https://google-gruyere.appspot.com/code/?resources/editprofile.gtl
- GET: https://google-gruyere.appspot.com/code/?resources/error.gtl
- GET: https://google-gruyere.appspot.com/code/?resources/feed.gtl
- GET: https://google-gruyere.appspot.com/code/?resources/home.gtl
- GET: https://google-gruyere.appspot.com/code/?resources/manage.gtl
- GET: https://google-gruyere.appspot.com/code/?resources/menubar.gtl
- GET: https://google-gruyere.appspot.com/code/?sanitize.py
- GET: https://google-gruyere.appspot.com/code/data.py
- GET: https://google-gruyere.appspot.com/code/gruyere.py
- GET: https://google-gruyere.appspot.com/code/gtl.py
- GET: https://google-gruyere.appspot.com/code/resources/base.css
- GET: https://google-gruyere.appspot.com/code/resources/dump.gtl
- GET: https://google-gruyere.appspot.com/code/resources/editprofile.gtl

- GET: https://google-gruyere.appspot.com/code/resources/error.gtl
- GET: https://google-gruyere.appspot.com/code/resources/feed.gtl
- GET: https://google-gruyere.appspot.com/code/resources/home.gtl
- GET: https://google-gruyere.appspot.com/code/resources/lib.js
- GET: https://google-gruyere.appspot.com/code/resources/login.gtl
- GET: https://google-gruyere.appspot.com/code/resources/manage.gtl
- GET: https://google-gruyere.appspot.com/code/resources/menubar.gtl
- GET: https://google-gruyere.appspot.com/code/resources/newaccount.gtl
- GET: https://google-gruyere.appspot.com/code/resources/newsnippet.gtl
- GET: https://google-gruyere.appspot.com/code/resources/showprofile.gtl
- GET: https://google-gruyere.appspot.com/code/resources/snippets.gtl
- GET: https://google-gruyere.appspot.com/code/resources/upload.gtl
- GET: https://google-gruyere.appspot.com/code/resources/upload2.gtl
- GET: https://google-gruyere.appspot.com/code/sanitize.py
- GET: https://google-gruyere.appspot.com/code/secret.txt
- GET: https://google-gruyere.appspot.com/part1
- GET: https://google-gruyere.appspot.com/part2
- GET: https://google-gruyere.appspot.com/part3
- GET: https://google-gruyere.appspot.com/part4
- GET: https://google-gruyere.appspot.com/part5
- GET: https://google-gruyere.appspot.com/resetbutton/635819304277645928474860676940086211620
- GET: https://google-gruyere.appspot.com/start
- GET: https://google-gruyere.appspot.com/static/codeindex.html
- GET: https://google-gruyere.appspot.com/static/codeindex/html
- POST: https://google-gruyere.appspot.com/resetbutton/635819304277645928474860676940086211620

8.1.4: Missing Anti-clickjacking Header:

- GET: http://google-gruyere.appspot.com
- GET: http://google-gruyere.appspot.com/
- GET: http://google-gruyere.appspot.com/0
- GET: http://google-gruyere.appspot.com/1
- GET: http://google-gruyere.appspot.com/2
- GET: http://google-gruyere.appspot.com/3
- GET: http://google-gruyere.appspot.com/4
- GET: http://google-gruyere.appspot.com/5
- GET: http://google-gruyere.appspot.com/6
- GET: http://google-gruyere.appspot.com/635819304277645928474860676940086211620/
- GET: http://google-gruyere.appspot.com/635819304277645928474860676940086211620/login
- GET: http://google-gruyere.appspot.com/635819304277645928474860676940086211620/login?pw=ZAP&uid=ZAP
- GET: http://google-gruyere.appspot.com/635819304277645928474860676940086211620/newaccount.gtl
- GET: http://google-gruyere.appspot.com/635819304277645928474860676940086211620/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
- GET: http://google-gruyere.appspot.com/635819304277645928474860676940086211620/snippets.gtl?uid=brie
- GET: http://google-gruyere.appspot.com/635819304277645928474860676940086211620/snippets.gtl?uid=cheddar
- GET: http://google-gruyere.appspot.com/7

- GET: http://google-gruyere.appspot.com/8
- GET: http://google-gruyere.appspot.com/9
- GET: http://google-gruyere.appspot.com/code/
- GET: http://google-gruyere.appspot.com/code/?data.py
- GET: http://google-gruyere.appspot.com/code/?gruyere.py
- GET: http://google-gruyere.appspot.com/code/?gtl.py
- GET: http://google-gruyere.appspot.com/code/?resoources/dump.gtl
- GET: http://google-gruyere.appspot.com/code/?resources/dump.gtl
- GET: http://google-gruyere.appspot.com/code/?resources/editprofile.gtl
- GET: http://google-gruyere.appspot.com/code/?resources/error.gtl
- GET: http://google-gruyere.appspot.com/code/?resources/feed.gtl
- GET: http://google-gruyere.appspot.com/code/?resources/home.gtl
- GET: http://google-gruyere.appspot.com/code/?resources/manage.gtl
- GET: http://google-gruyere.appspot.com/code/?resources/menubar.gtl
- GET: http://google-gruyere.appspot.com/code/?sanitize.py
- GET: http://google-gruyere.appspot.com/code/data.py
- GET: http://google-gruyere.appspot.com/code/gruyere.py
- GET: http://google-gruyere.appspot.com/code/gtl.py
- GET: http://google-gruyere.appspot.com/code/resources/base.css
- GET: http://google-gruyere.appspot.com/code/resources/dump.gtl
- GET: http://google-gruyere.appspot.com/code/resources/editprofile.gtl
- GET: http://google-gruyere.appspot.com/code/resources/error.gtl
- GET: http://google-gruyere.appspot.com/code/resources/feed.gtl
- GET: http://google-gruyere.appspot.com/code/resources/home.gtl
- GET: http://google-gruyere.appspot.com/code/resources/lib.js
- GET: http://google-gruyere.appspot.com/code/resources/login.gtl
- GET: http://google-gruyere.appspot.com/code/resources/manage.gtl
- GET: http://google-gruyere.appspot.com/code/resources/menubar.gtl
- GET: http://google-gruyere.appspot.com/code/resources/newaccount.gtl
- GET: http://google-gruyere.appspot.com/code/resources/newsnippet.gtl
- GET: http://google-gruyere.appspot.com/code/resources/showprofile.gtl
- GET: http://google-gruyere.appspot.com/code/resources/snippets.gtl
- GET: http://google-gruyere.appspot.com/code/resources/upload.gtl
- GET: http://google-gruyere.appspot.com/code/resources/upload2.gtl
- GET: http://google-gruyere.appspot.com/code/sanitize.py
- GET: http://google-gruyere.appspot.com/code/secret.txt
- GET: http://google-gruyere.appspot.com/part1
- GET: http://google-gruyere.appspot.com/part2
- GET: http://google-gruyere.appspot.com/part3
- GET: http://google-gruyere.appspot.com/part4
- GET: http://google-gruyere.appspot.com/part5
- GET: http://google-gruyere.appspot.com/start
- GET: http://google-gruyere.appspot.com/static/codeindex.html
- GET: https://google-gruyere.appspot.com/
- GET: https://google-gruyere.appspot.com/635819304277645928474860676940086211620/
- GET: https://google-gruyere.appspot.com/635819304277645928474860676940086211620/feed.gtl
- GET: https://google-gruyere.appspot.com/635819304277645928474860676940086211620/login
- GET: https://google-gruyere.appspot.com/635819304277645928474860676940086211620/newaccount.gtl

- GET: https://google-gruyere.appspot.com/635819304277645928474860676940086211620/quitserver.
- GET: https://google-gruyere.appspot.com/635819304277645928474860676940086211620/RESET.
- GET: https://google-gruyere.appspot.com/635819304277645928474860676940086211620/saveprofile?action=update&is_admin=True
- GET: https://google-gruyere.appspot.com/635819304277645928474860676940086211620/saveprofile?action=update&is_admin=True&uid=username
- GET: https://google-gruyere.appspot.com/code/
- GET: https://google-gruyere.appspot.com/code/?data.py
- GET: https://google-gruyere.appspot.com/code/?gruyere.py
- GET: https://google-gruyere.appspot.com/code/?gtl.py
- GET: https://google-gruyere.appspot.com/code/?resoources/dump.gtl
- GET: https://google-gruyere.appspot.com/code/?resources/dump.gtl
- GET: https://google-gruyere.appspot.com/code/?resources/editprofile.gtl
- GET: https://google-gruyere.appspot.com/code/?resources/error.gtl
- GET: https://google-gruyere.appspot.com/code/?resources/feed.gtl
- GET: https://google-gruyere.appspot.com/code/?resources/home.gtl
- GET: https://google-gruyere.appspot.com/code/?resources/manage.gtl
- GET: https://google-gruyere.appspot.com/code/?resources/menubar.gtl
- GET: https://google-gruyere.appspot.com/code/?sanitize.py
- GET: https://google-gruyere.appspot.com/code/data.py
- GET: https://google-gruyere.appspot.com/code/gruyere.py
- GET: https://google-gruyere.appspot.com/code/gtl.py
- GET: https://google-gruyere.appspot.com/code/resources/base.css
- GET: https://google-gruyere.appspot.com/code/resources/dump.gtl
- GET: https://google-gruyere.appspot.com/code/resources/editprofile.gtl
- GET: https://google-gruyere.appspot.com/code/resources/error.gtl
- GET: https://google-gruyere.appspot.com/code/resources/feed.gtl
- GET: https://google-gruyere.appspot.com/code/resources/home.gtl
- GET: https://google-gruyere.appspot.com/code/resources/lib.js
- GET: https://google-gruyere.appspot.com/code/resources/login.gtl
- GET: https://google-gruyere.appspot.com/code/resources/manage.gtl
- GET: https://google-gruyere.appspot.com/code/resources/menubar.gtl
- GET: https://google-gruyere.appspot.com/code/resources/newaccount.gtl
- GET: https://google-gruyere.appspot.com/code/resources/newsnippet.gtl
- GET: https://google-gruyere.appspot.com/code/resources/showprofile.gtl
- GET: https://google-gruyere.appspot.com/code/resources/snippets.gtl
- GET: https://google-gruyere.appspot.com/code/resources/upload.gtl
- GET: https://google-gruyere.appspot.com/code/resources/upload2.gtl
- GET: https://google-gruyere.appspot.com/code/sanitize.py
- GET: https://google-gruyere.appspot.com/code/secret.txt
- GET: https://google-gruyere.appspot.com/part1
- GET: https://google-gruyere.appspot.com/part2
- GET: https://google-gruyere.appspot.com/part3
- GET: https://google-gruyere.appspot.com/part4
- GET: https://google-gruyere.appspot.com/part5
- GET: https://google-gruyere.appspot.com/resetbutton/635819304277645928474860676940086211620

- GET: https://google-gruyere.appspot.com/start
- GET: https://google-gruyere.appspot.com/static/codeindex.html
- POST: https://google-gruyere.appspot.com/resetbutton/635819304277645928474860676940086211620

8.1.5: Cookie No HttpOnly Flag

- GET: http://www.google-gruyere.appspot.com/601593815671992150146832323098486527403/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
- GET: http://www.google-gruyere.appspot.com/start
- GET: https://www.google-gruyere.appspot.com/start

8.1.6: Cookie without SameSite Attribute

- GET: http://www.google-gruyere.appspot.com/601593815671992150146832323098486527403/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
- GET: http://www.google-gruyere.appspot.com/start
- GET: https://www.google-gruyere.appspot.com/start

8.1.7: Cross-Domain JavaScript Source File Inclusion

- GET: https://google-gruyere.appspot.com/resetbutton/635819304277645928474860676940086211620

8.1.8: Strict-Transport-Security Header Not Set

- GET: https://www.google-gruyere.appspot.com/
- GET: https://www.google-gruyere.appspot.com/%C9%A1ru%CB%90%CB%88j%C9%9B%C9%99r/
- GET: https://www.google-gruyere.appspot.com/*
- GET: https://www.google-gruyere.appspot.com/,
- GET: https://www.google-gruyere.appspot.com/0
- GET: https://www.google-gruyere.appspot.com/1
- GET: https://www.google-gruyere.appspot.com/2
- GET: https://www.google-gruyere.appspot.com/3
- GET: https://www.google-gruyere.appspot.com/4
- GET: https://www.google-gruyere.appspot.com/5
- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/
- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/lib.js
- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/login

- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/newaccount.gtl
- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/snippets.gtl?uid=brie
- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/snippets.gtl?uid=cheddar
- GET: https://www.google-gruyere.appspot.com/6
- GET: https://www.google-gruyere.appspot.com/7
- GET: https://www.google-gruyere.appspot.com/8
- GET: https://www.google-gruyere.appspot.com/9
- GET: https://www.google-gruyere.appspot.com/Applications/Google%5C
- GET: https://www.google-gruyere.appspot.com/code/
- GET: https://www.google-gruyere.appspot.com/code/?data.py
- GET: https://www.google-gruyere.appspot.com/code/?gruyere.py
- GET: https://www.google-gruyere.appspot.com/code/?gtl.py
- GET: https://www.google-gruyere.appspot.com/code/?resoources/dump.gtl
- GET: https://www.google-gruyere.appspot.com/code/?resources/dump.gtl
- GET: https://www.google-gruyere.appspot.com/code/?resources/editprofile.gtl
- GET: https://www.google-gruyere.appspot.com/code/?resources/error.gtl
- GET: https://www.google-gruyere.appspot.com/code/?resources/feed.gtl
- GET: https://www.google-gruyere.appspot.com/code/?resources/home.gtl
- GET: https://www.google-gruyere.appspot.com/code/?resources/manage.gtl
- GET: https://www.google-gruyere.appspot.com/code/?resources/menubar.gtl
- GET: https://www.google-gruyere.appspot.com/code/?sanitize.py
- GET: https://www.google-gruyere.appspot.com/code/data.py
- GET: https://www.google-gruyere.appspot.com/code/gruyere.py
- GET: https://www.google-gruyere.appspot.com/code/gtl.py
- GET: https://www.google-gruyere.appspot.com/code/resources/base.css
- GET: https://www.google-gruyere.appspot.com/code/resources/dump.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/editprofile.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/error.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/feed.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/home.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/lib.js
- GET: https://www.google-gruyere.appspot.com/code/resources/login.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/manage.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/menubar.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/newaccount.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/newsnippet.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/showprofile.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/snippets.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/upload.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/upload2.gtl
- GET: https://www.google-gruyere.appspot.com/code/sanitize.py

- GET: https://www.google-gruyere.appspot.com/code/secret.txt
- GET: https://www.google-gruyere.appspot.com/deletesnippet
- GET: https://www.google-gruyere.appspot.com/etc.
- GET: https://www.google-gruyere.appspot.com/gruyere-code.zip
- GET: https://www.google-gruyere.appspot.com/gtl.py
- GET: https://www.google-gruyere.appspot.com/opt/google/chrome/google-chrome
- GET: https://www.google-gruyere.appspot.com/part1
- GET: https://www.google-gruyere.appspot.com/part2
- GET: https://www.google-gruyere.appspot.com/part3
- GET: https://www.google-gruyere.appspot.com/part4
- GET: https://www.google-gruyere.appspot.com/part5
- GET: https://www.google-gruyere.appspot.com/quit
- GET: https://www.google-gruyere.appspot.com/quitserver
- GET: https://www.google-gruyere.appspot.com/quitserver.
- GET: https://www.google-gruyere.appspot.com/resetbutton
- GET: https://www.google-gruyere.appspot.com/robots.txt
- GET: https://www.google-gruyere.appspot.com/secret.txt
- GET: https://www.google-gruyere.appspot.com/secret.txt.
- GET: https://www.google-gruyere.appspot.com/sitemap.xml
- GET: https://www.google-gruyere.appspot.com/start
- GET: https://www.google-gruyere.appspot.com/static/cheese_b.png
- GET: https://www.google-gruyere.appspot.com/static/cheese_bw.png
- GET: https://www.google-gruyere.appspot.com/static/cheese_w.png
- GET: https://www.google-gruyere.appspot.com/static/closed.gif
- GET: https://www.google-gruyere.appspot.com/static/codeindex.html
- GET: https://www.google-gruyere.appspot.com/static/codeindex/html
- GET: https://www.google-gruyere.appspot.com/static/codelab.css
- GET: https://www.google-gruyere.appspot.com/static/gruyere-40.png
- GET: https://www.google-gruyere.appspot.com/static/gruyere-78.png
- GET: https://www.google-gruyere.appspot.com/static/gruyere-badge.png
- GET: https://www.google-gruyere.appspot.com/static/gruyere.png
- GET: https://www.google-gruyere.appspot.com/x

8.1.9: X-Content-Type-Options Header Missing

- GET: http://www.google-gruyere.appspot.com/
- GET: http://www.google-gruyere.appspot.com/0
- GET: http://www.google-gruyere.appspot.com/1
- GET: http://www.google-gruyere.appspot.com/2
- GET: http://www.google-gruyere.appspot.com/3
- GET: http://www.google-gruyere.appspot.com/4
- GET: http://www.google-gruyere.appspot.com/5
- GET: http://www.google-gruyere.appspot.com/6
- GET: http://www.google-gruyere.appspot.com/601593815671992150146832323098486527403/

- GET: http://www.google-gruyere.appspot.com/601593815671992150146832323098486527403/lib.js
- GET: http://www.google-gruyere.appspot.com/601593815671992150146832323098486527403/login
- GET: http://www.google-gruyere.appspot.com/601593815671992150146832323098486527403/login?pw=ZAP&uid=ZAP
- GET: http://www.google-gruyere.appspot.com/601593815671992150146832323098486527403/newaccount.gtl
- GET: http://www.google-gruyere.appspot.com/601593815671992150146832323098486527403/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
- GET: http://www.google-gruyere.appspot.com/601593815671992150146832323098486527403/snippets.gtl?uid=brie
- GET: http://www.google-gruyere.appspot.com/601593815671992150146832323098486527403/snippets.gtl?uid=cheddar
- GET: http://www.google-gruyere.appspot.com/7
- GET: http://www.google-gruyere.appspot.com/8
- GET: http://www.google-gruyere.appspot.com/9
- GET: http://www.google-gruyere.appspot.com/code/
- GET: http://www.google-gruyere.appspot.com/code/?data.py
- GET: http://www.google-gruyere.appspot.com/code/?gruyere.py
- GET: http://www.google-gruyere.appspot.com/code/?gtl.py
- GET: http://www.google-gruyere.appspot.com/code/?resoources/dump.gtl
- GET: http://www.google-gruyere.appspot.com/code/?resources/dump.gtl
- GET: http://www.google-gruyere.appspot.com/code/?resources/editprofile.gtl
- GET: http://www.google-gruyere.appspot.com/code/?resources/error.gtl
- GET: http://www.google-gruyere.appspot.com/code/?resources/feed.gtl
- GET: http://www.google-gruyere.appspot.com/code/?resources/home.gtl
- GET: http://www.google-gruyere.appspot.com/code/?resources/manage.gtl
- GET: http://www.google-gruyere.appspot.com/code/?resources/menubar.gtl
- GET: http://www.google-gruyere.appspot.com/code/?sanitize.py
- GET: http://www.google-gruyere.appspot.com/code/data.py
- GET: http://www.google-gruyere.appspot.com/code/gruyere.py
- GET: http://www.google-gruyere.appspot.com/code/gtl.py
- GET: http://www.google-gruyere.appspot.com/code/resources/base.css
- GET: http://www.google-gruyere.appspot.com/code/resources/dump.gtl
- GET: http://www.google-gruyere.appspot.com/code/resources/editprofile.gtl
- GET: http://www.google-gruyere.appspot.com/code/resources/error.gtl
- GET: http://www.google-gruyere.appspot.com/code/resources/feed.gtl
- GET: http://www.google-gruyere.appspot.com/code/resources/home.gtl
- GET: http://www.google-gruyere.appspot.com/code/resources/lib.js
- GET: http://www.google-gruyere.appspot.com/code/resources/login.gtl
- GET: http://www.google-gruyere.appspot.com/code/resources/manage.gtl
- GET: http://www.google-gruyere.appspot.com/code/resources/menubar.gtl

- GET: http://www.google-gruyere.appspot.com/code/resources/newaccount.gtl
- GET: http://www.google-gruyere.appspot.com/code/resources/newsnippet.gtl
- GET: http://www.google-gruyere.appspot.com/code/resources/showprofile.gtl
- GET: http://www.google-gruyere.appspot.com/code/resources/snippets.gtl
- GET: http://www.google-gruyere.appspot.com/code/resources/upload.gtl
- GET: http://www.google-gruyere.appspot.com/code/resources/upload2.gtl
- GET: http://www.google-gruyere.appspot.com/code/sanitize.py
- GET: http://www.google-gruyere.appspot.com/code/secret.txt
- GET: http://www.google-gruyere.appspot.com/gruyere-code.zip
- GET: http://www.google-gruyere.appspot.com/part1
- GET: http://www.google-gruyere.appspot.com/part2
- GET: http://www.google-gruyere.appspot.com/part3
- GET: http://www.google-gruyere.appspot.com/part4
- GET: http://www.google-gruyere.appspot.com/part5
- GET: http://www.google-gruyere.appspot.com/robots.txt
- GET: http://www.google-gruyere.appspot.com/start
- GET: http://www.google-gruyere.appspot.com/static/cheese_b.png
- GET: http://www.google-gruyere.appspot.com/static/cheese_bw.png
- GET: http://www.google-gruyere.appspot.com/static/cheese_w.png
- GET: http://www.google-gruyere.appspot.com/static/closed.gif
- GET: http://www.google-gruyere.appspot.com/static/codeindex.html
- GET: http://www.google-gruyere.appspot.com/static/codelab.css
- GET: http://www.google-gruyere.appspot.com/static/gruyere-40.png
- GET: http://www.google-gruyere.appspot.com/static/gruyere-78.png
- GET: http://www.google-gruyere.appspot.com/static/gruyere-badge.png
- GET: http://www.google-gruyere.appspot.com/static/gruyere.png
- GET: https://www.google-gruyere.appspot.com/
- GET: https://www.google-gruyere.appspot.com/0
- GET: https://www.google-gruyere.appspot.com/1
- GET: https://www.google-gruyere.appspot.com/2
- GET: https://www.google-gruyere.appspot.com/3
- GET: https://www.google-gruyere.appspot.com/4
- GET: https://www.google-gruyere.appspot.com/5
- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/
- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/lib.js
- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/login
- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/newaccount.gtl
- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/snippets.gtl?uid=brie
- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/snippets.gtl?uid=cheddar

- GET: https://www.google-gruyere.appspot.com/6
- GET: https://www.google-gruyere.appspot.com/7
- GET: https://www.google-gruyere.appspot.com/8
- GET: https://www.google-gruyere.appspot.com/9
- GET: https://www.google-gruyere.appspot.com/code/
- GET: https://www.google-gruyere.appspot.com/code/?data.py
- GET: https://www.google-gruyere.appspot.com/code/?gruyere.py
- GET: https://www.google-gruyere.appspot.com/code/?gtl.py
- GET: https://www.google-gruyere.appspot.com/code/?resoources/dump.gtl
- GET: https://www.google-gruyere.appspot.com/code/?resources/dump.gtl
- GET: https://www.google-gruyere.appspot.com/code/?resources/editprofile.gtl
- GET: https://www.google-gruyere.appspot.com/code/?resources/error.gtl
- GET: https://www.google-gruyere.appspot.com/code/?resources/feed.gtl
- GET: https://www.google-gruyere.appspot.com/code/?resources/home.gtl
- GET: https://www.google-gruyere.appspot.com/code/?resources/manage.gtl
- GET: https://www.google-gruyere.appspot.com/code/?resources/menubar.gtl
- GET: https://www.google-gruyere.appspot.com/code/?sanitize.py
- GET: https://www.google-gruyere.appspot.com/code/data.py
- GET: https://www.google-gruyere.appspot.com/code/gruyere.py
- GET: https://www.google-gruyere.appspot.com/code/gtl.py
- GET: https://www.google-gruyere.appspot.com/code/resources/base.css
- GET: https://www.google-gruyere.appspot.com/code/resources/dump.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/editprofile.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/error.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/feed.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/home.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/lib.js
- GET: https://www.google-gruyere.appspot.com/code/resources/login.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/manage.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/menubar.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/newaccount.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/newsnippet.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/showprofile.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/snippets.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/upload.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/upload2.gtl
- GET: https://www.google-gruyere.appspot.com/code/sanitize.py
- GET: https://www.google-gruyere.appspot.com/code/secret.txt
- GET: https://www.google-gruyere.appspot.com/gruyere-code.zip
- GET: https://www.google-gruyere.appspot.com/part1
- GET: https://www.google-gruyere.appspot.com/part2
- GET: https://www.google-gruyere.appspot.com/part3
- GET: https://www.google-gruyere.appspot.com/part4

- GET: https://www.google-gruyere.appspot.com/part5
- GET: https://www.google-gruyere.appspot.com/robots.txt
- GET: https://www.google-gruyere.appspot.com/start
- GET: https://www.google-gruyere.appspot.com/static/cheese_b.png
- GET: https://www.google-gruyere.appspot.com/static/cheese_bw.png
- GET: https://www.google-gruyere.appspot.com/static/cheese_w.png
- GET: https://www.google-gruyere.appspot.com/static/closed.gif
- GET: https://www.google-gruyere.appspot.com/static/codeindex.html
- GET: https://www.google-gruyere.appspot.com/static/codelab.css
- GET: https://www.google-gruyere.appspot.com/static/gruyere-40.png
- GET: https://www.google-gruyere.appspot.com/static/gruyere-78.png
- GET: https://www.google-gruyere.appspot.com/static/gruyere-badge.png
- GET: https://www.google-gruyere.appspot.com/static/gruyere.png

8.1.10: Charset Mismatch (Header Versus Meta Content-Type Charset)

- GET: http://www.google-gruyere.appspot.com/
- GET: http://www.google-gruyere.appspot.com/part1
- GET: http://www.google-gruyere.appspot.com/part2
- GET: http://www.google-gruyere.appspot.com/part3
- GET: http://www.google-gruyere.appspot.com/part4
- GET: http://www.google-gruyere.appspot.com/part5
- GET: https://www.google-gruyere.appspot.com/
- GET: https://www.google-gruyere.appspot.com/part1
- GET: https://www.google-gruyere.appspot.com/part2
- GET: https://www.google-gruyere.appspot.com/part3
- GET: https://www.google-gruyere.appspot.com/part4
- GET: https://www.google-gruyere.appspot.com/part5

8.1.11: Cookie Poisoning

- GET: http://www.google-gruyere.appspot.com/601593815671992150146832323098486527403/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
- GET: http://www.google-gruyere.appspot.com/601593815671992150146832323098486527403/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP

8.1.12: Information Disclosure - Suspicious Comments

- GET: http://www.google-gruyere.appspot.com/601593815671992150146832323098486527403/lib.js
- GET: http://www.google-gruyere.appspot.com/code/resources/lib.js

- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/lib.js
- GET: https://www.google-gruyere.appspot.com/code/resources/lib.js

8.1.13: Modern Web Application

- GET: http://www.google-gruyere.appspot.com/
- GET: http://www.google-gruyere.appspot.com/601593815671992150146832323098486527403/
- GET: http://www.google-gruyere.appspot.com/601593815671992150146832323098486527403/snippets.gtl?uid=brie
- GET: http://www.google-gruyere.appspot.com/601593815671992150146832323098486527403/snippets.gtl?uid=cheddar
- GET: http://www.google-gruyere.appspot.com/part1
- GET: http://www.google-gruyere.appspot.com/part2
- GET: http://www.google-gruyere.appspot.com/part3
- GET: http://www.google-gruyere.appspot.com/part4
- GET: http://www.google-gruyere.appspot.com/part5
- GET: https://www.google-gruyere.appspot.com/
- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/
- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/snippets.gtl?uid=brie
- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/snippets.gtl?uid=cheddar
- GET: https://www.google-gruyere.appspot.com/part1
- GET: https://www.google-gruyere.appspot.com/part2
- GET: https://www.google-gruyere.appspot.com/part3
- GET: https://www.google-gruyere.appspot.com/part4
- GET: https://www.google-gruyere.appspot.com/part5

8.1.14: Re-examine Cache-control Directives

- GET: https://www.google-gruyere.appspot.com/
- GET: https://www.google-gruyere.appspot.com/0
- GET: https://www.google-gruyere.appspot.com/1
- GET: https://www.google-gruyere.appspot.com/2
- GET: https://www.google-gruyere.appspot.com/3
- GET: https://www.google-gruyere.appspot.com/4
- GET: https://www.google-gruyere.appspot.com/5
- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/
- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/login
- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/newaccount.gtl
- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/snippets.gtl?uid=brie

- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/snippets.gtl?uid=cheddar
- GET: https://www.google-gruyere.appspot.com/6
- GET: https://www.google-gruyere.appspot.com/7
- GET: https://www.google-gruyere.appspot.com/8
- GET: https://www.google-gruyere.appspot.com/9
- GET: https://www.google-gruyere.appspot.com/code/
- GET: https://www.google-gruyere.appspot.com/code/?data.py
- GET: https://www.google-gruyere.appspot.com/code/?gruyere.py
- GET: https://www.google-gruyere.appspot.com/code/?gtl.py
- GET: https://www.google-gruyere.appspot.com/code/?resoources/dump.gtl
- GET: https://www.google-gruyere.appspot.com/code/?resources/dump.gtl
- GET: https://www.google-gruyere.appspot.com/code/?resources/editprofile.gtl
- GET: https://www.google-gruyere.appspot.com/code/?resources/error.gtl
- GET: https://www.google-gruyere.appspot.com/code/?resources/feed.gtl
- GET: https://www.google-gruyere.appspot.com/code/?resources/home.gtl
- GET: https://www.google-gruyere.appspot.com/code/?resources/manage.gtl
- GET: https://www.google-gruyere.appspot.com/code/?resources/menubar.gtl
- GET: https://www.google-gruyere.appspot.com/code/?sanitize.py
- GET: https://www.google-gruyere.appspot.com/code/data.py
- GET: https://www.google-gruyere.appspot.com/code/gruyere.py
- GET: https://www.google-gruyere.appspot.com/code/gtl.py
- GET: https://www.google-gruyere.appspot.com/code/resources/dump.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/editprofile.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/error.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/feed.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/home.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/login.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/manage.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/menubar.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/newaccount.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/newsnippet.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/showprofile.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/snippets.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/upload.gtl
- GET: https://www.google-gruyere.appspot.com/code/resources/upload2.gtl
- GET: https://www.google-gruyere.appspot.com/code/sanitize.py
- GET: https://www.google-gruyere.appspot.com/code/secret.txt
- GET: https://www.google-gruyere.appspot.com/part1
- GET: https://www.google-gruyere.appspot.com/part2
- GET: https://www.google-gruyere.appspot.com/part3
- GET: https://www.google-gruyere.appspot.com/part4
- GET: https://www.google-gruyere.appspot.com/part5

- GET: https://www.google-gruyere.appspot.com/robots.txt
- GET: https://www.google-gruyere.appspot.com/start
- GET: https://www.google-gruyere.appspot.com/static/codeindex.html

8.1.15: Retrieved from Cache

- GET: http://google-gruyere.appspot.com/static/codelab.css

8.1.16: Session Management Response Identified

- GET: http://www.google-gruyere.appspot.com/601593815671992150146832323098486527403/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
- GET: http://www.google-gruyere.appspot.com/start
- GET: https://www.google-gruyere.appspot.com/start
- GET: http://www.google-gruyere.appspot.com/601593815671992150146832323098486527403/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
- GET: https://www.google-gruyere.appspot.com/515732668486819412692813186130642687171/newaccount.gtl

8.2: Reference Sites

- www.owasp.org
- www.cheatsheetseries.owasp.org
- www.cwe.mitre.org
- www.datatracker.ietf.org
- www.developer.mozilla.org
- www.code.google.com