CRLF injection

HTTP Response Splitting

Plit00

2018-08-12

PrL

- Web Sever
  - Root-me CRLF 20 Point

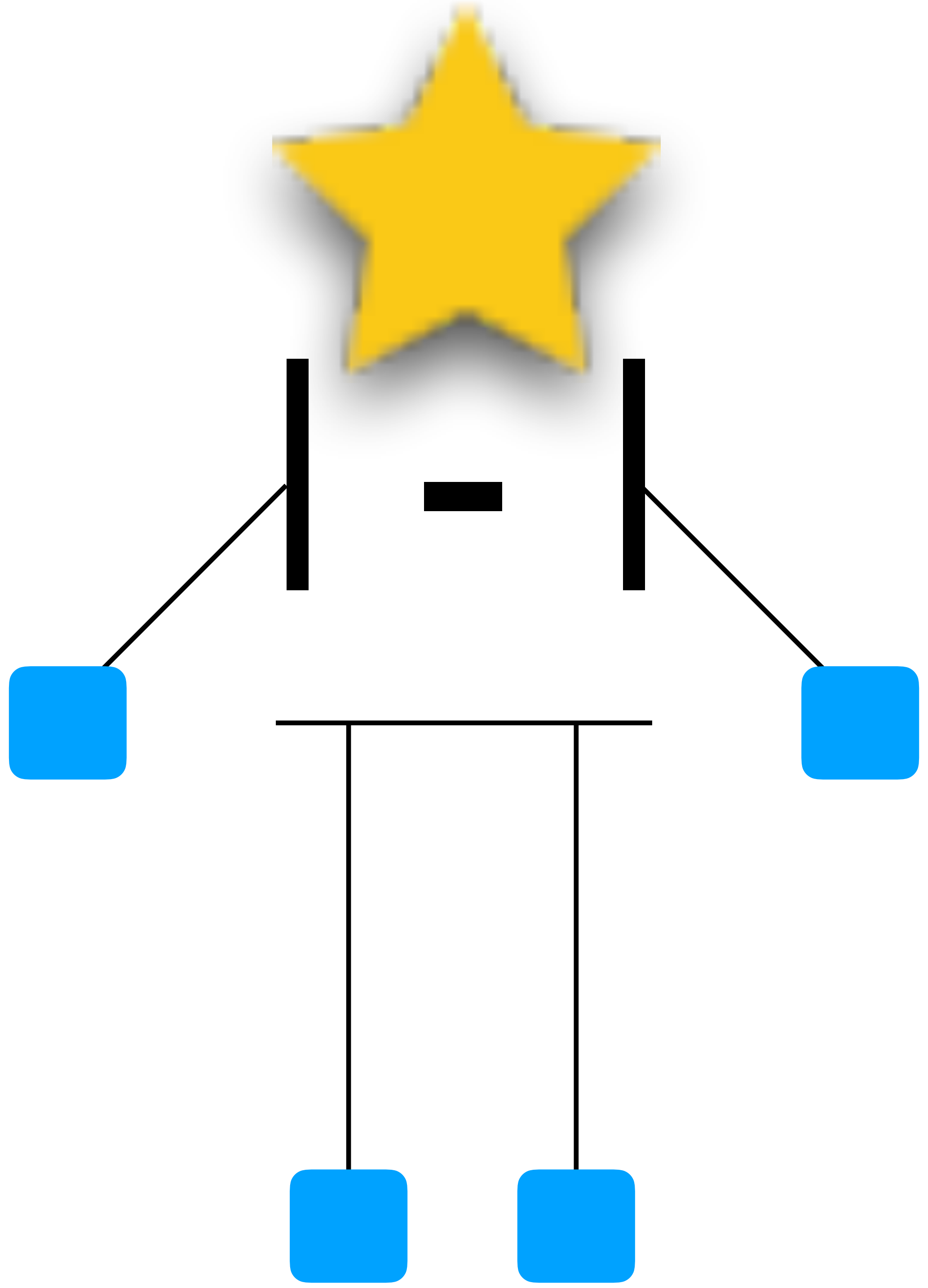
- CRLF _/ HTTP Response Splitting

Analysis

- Line breaks can be inserted in the input field
- Inject unexpected headers when processing forms if dat entered is not verified

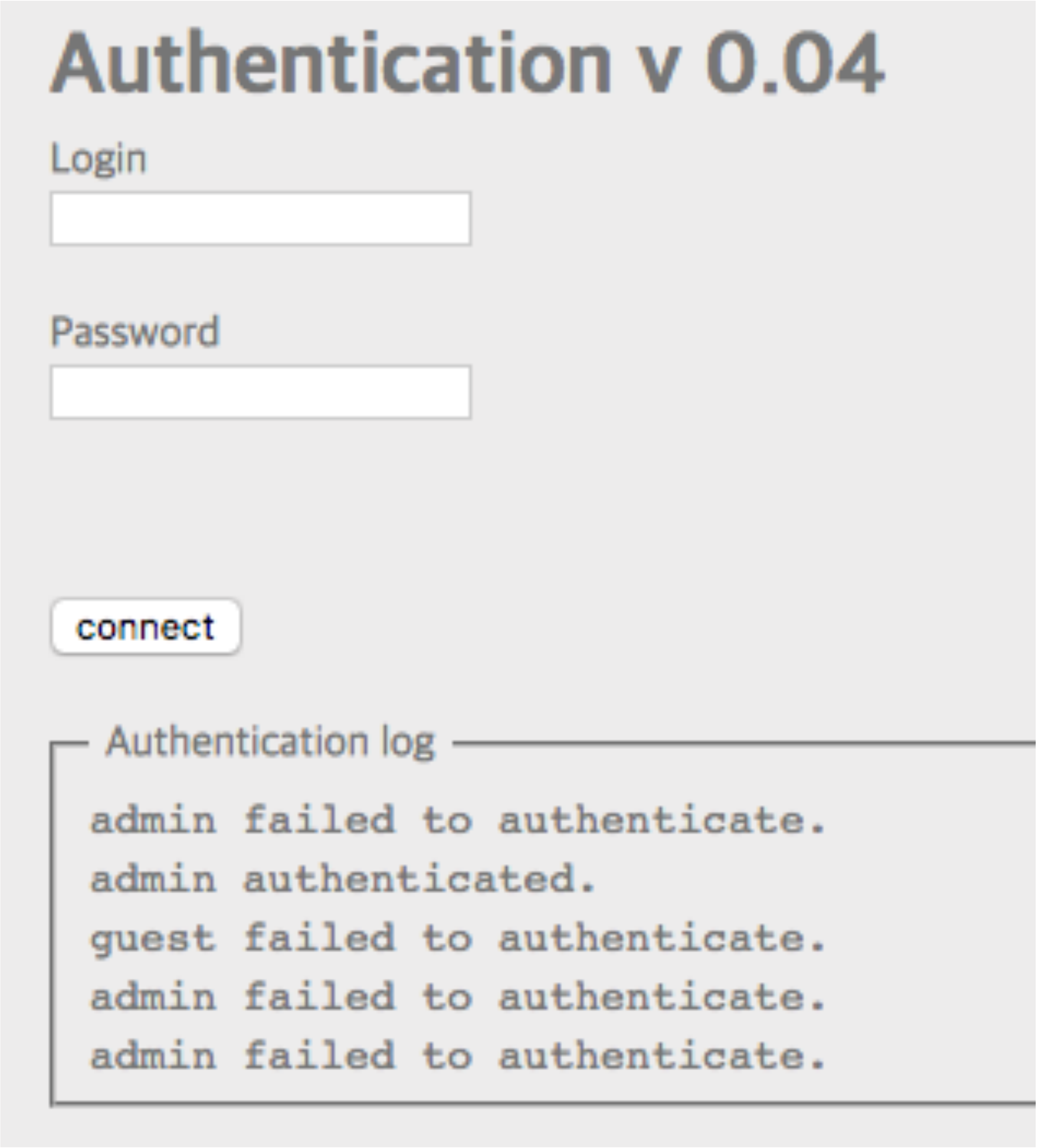
HTTP Vulnerability

- XSS
- Proxy and Web sever Cache poisoning
- Hijacking the client's Session
- Client Web browser poisoning



PrL

Inject false data in the journalisation log.

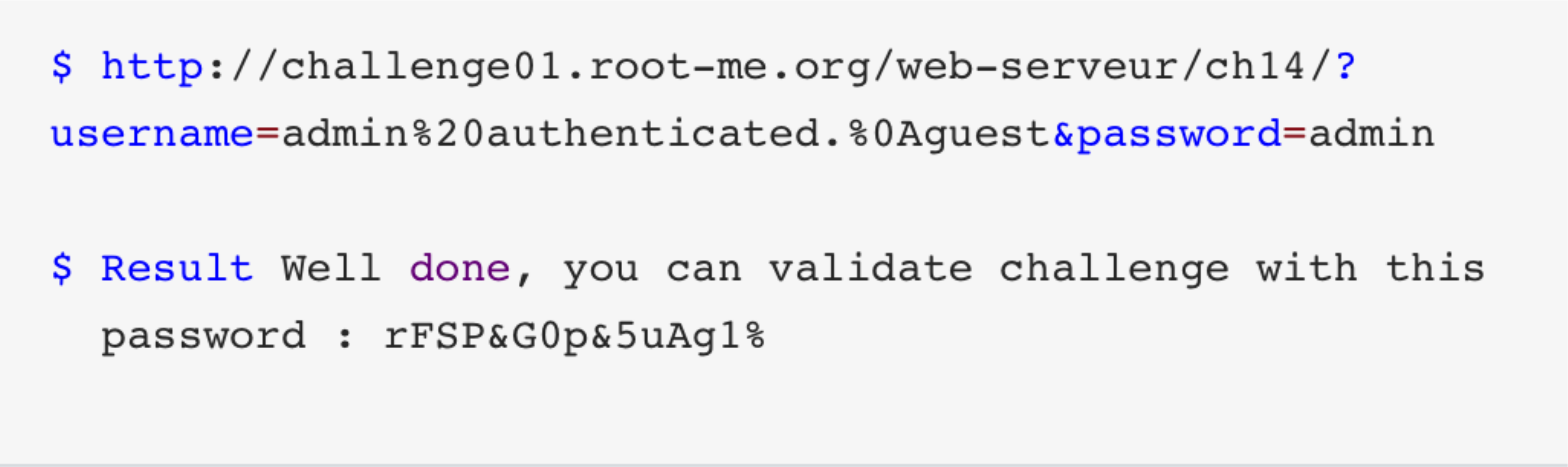


Authentication v 0.04

```
admin failed to authenticate.
admin authenticated.
guest failed to authenticate.
admin failed to authenticate.
admin failed to authenticate.
```

- String test = test.replaceAll(“₩r”.””).replaceAll(“₩n”,””);

- %0D%0A%20+New_Header+%0D%0A



```
$ http://challenge01.root-me.org/web-serveur/ch14/?
username=admin%20authenticated.%0Aguest&password=admin

$ Result Well done, you can validate challenge with this
  password : rFSP&G0p&5uAg1%
```

“QnA”

–plit00