

document 对象的常用属性

location.href实现页面跳转

confirm语句

document 对象的常用属性

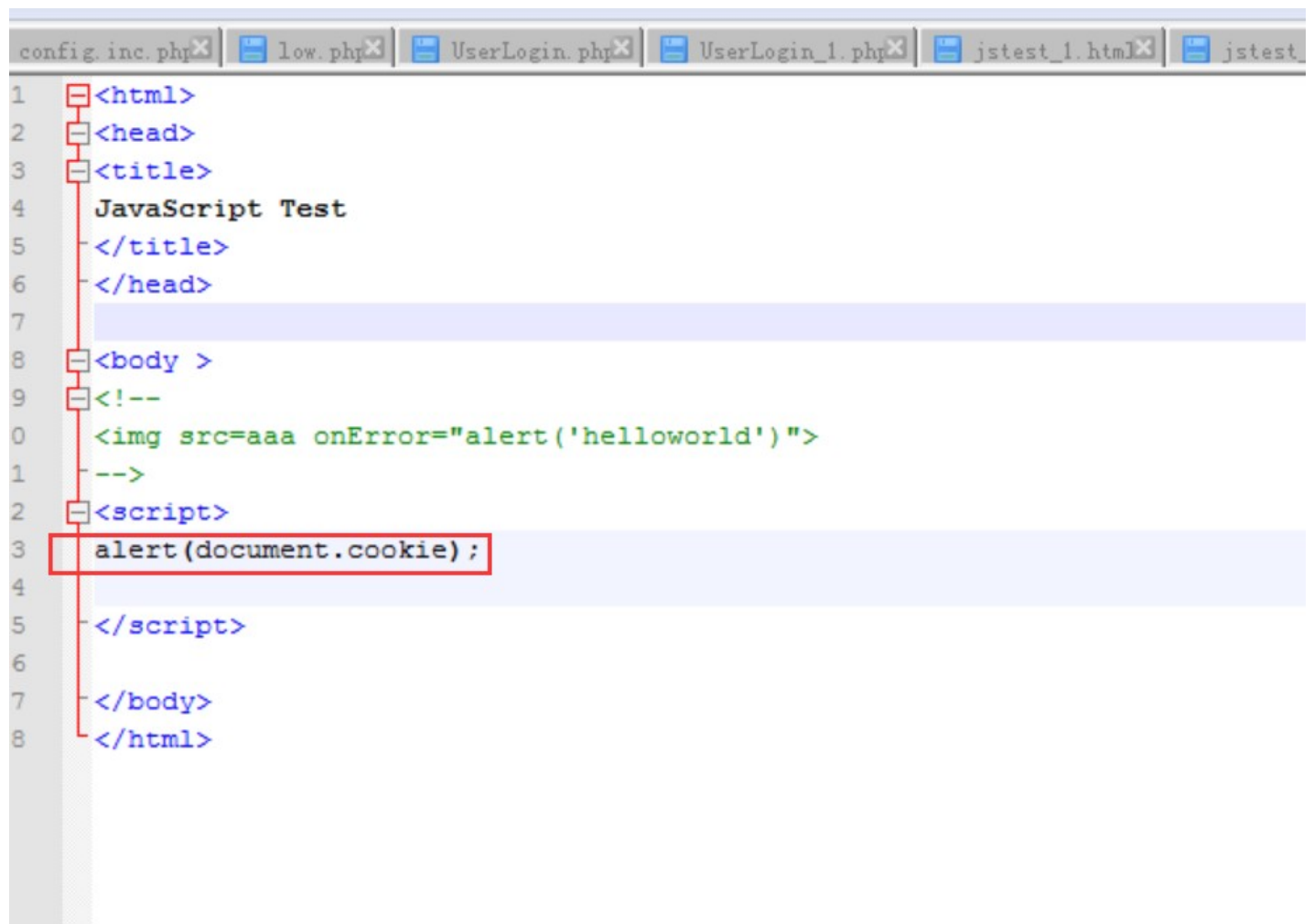
- document.cookie,显示当前页面的cookie(访问当前页面的cookie)

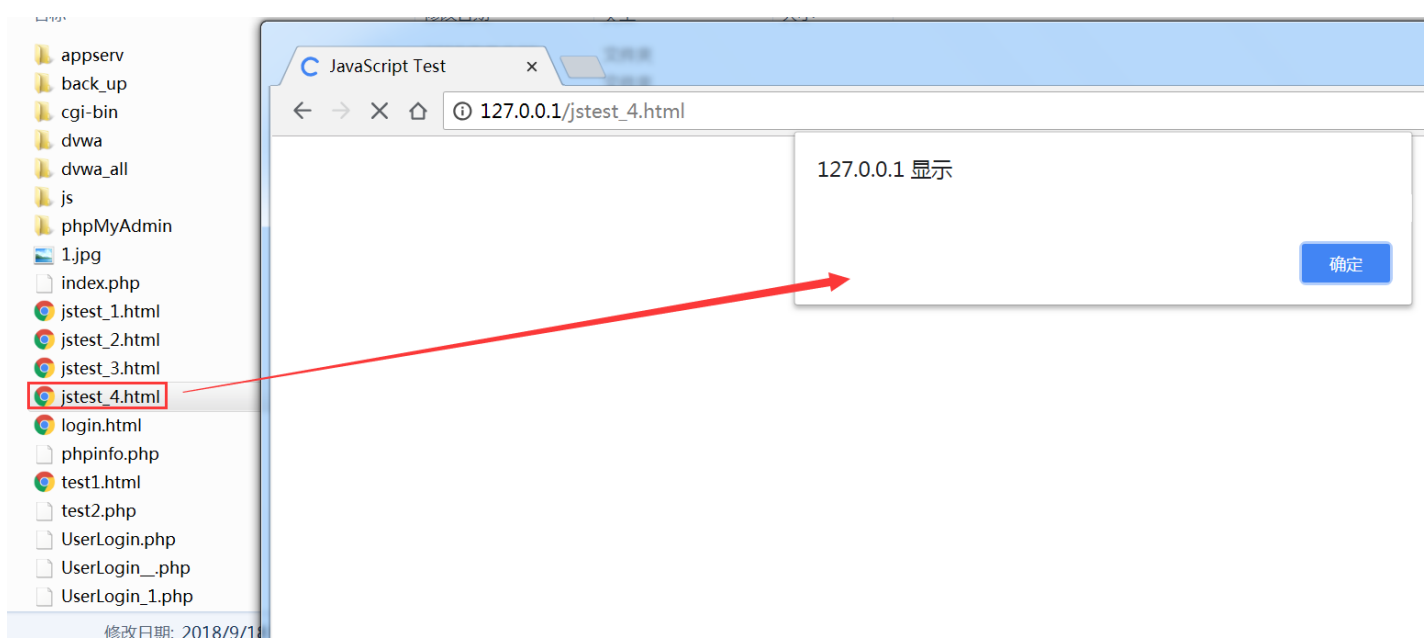
```
1 <script>alert(document.cookie);  
2     </script>
```

- document.location,显示当前页面的URL

```
1 <script>alert(document.location);  
2     </script>
```

这里由于没有登录所以没有显示cookie!





127.0.0.1/dvwa/security.php#

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low

Submit

PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based w

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Security level set to low

```
1 <script>alert(document.cookie)</script>
```

Vulnerability: Reflected Cross Site Script

[Home](#)[Instructions](#)[Setup](#)[Brute Force](#)[Command Execution](#)[CSRF](#)[Insecure CAPTCHA](#)[File Inclusion](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Upload](#)[XSS reflected](#)[XSS stored](#)

What's your name?

Hello

More info

<http://ha.ckers.org/xss.html>http://en.wikipedia.org/wiki/Cross-site_scripting<http://www.cgisecurity.com/xss-faq.html>[Home](#)[Instructions](#)[Setup](#)[Brute Force](#)[Command Execution](#)[CSRF](#)[Insecure CAPTCHA](#)

Vulnerability: Reflected Cross Site Script

security=low; PHPSESSID=e72a2a65f6d700092c07d1a49d5bc265

```
1 <html>
2 <head>
3 <title>
4 JavaScript Test
5 </title>
6 </head>
7
8 <body >
9 <!--
10 <img src=aaa onError="alert('helloworld')">
11 -->
12 <script>
13 document.write(document.cookie);
14
15 </script>
16
17 </body>
18 </html>
```

location.href实现页面跳转

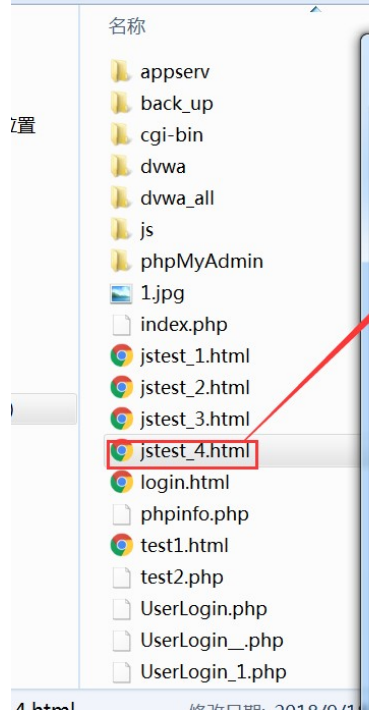
- 当页面整体跳转至另外一个页面上去

```
1 <script>
2 alert(document.location);
3 location.href = "www.51cto.com";
4 </script>
5
```

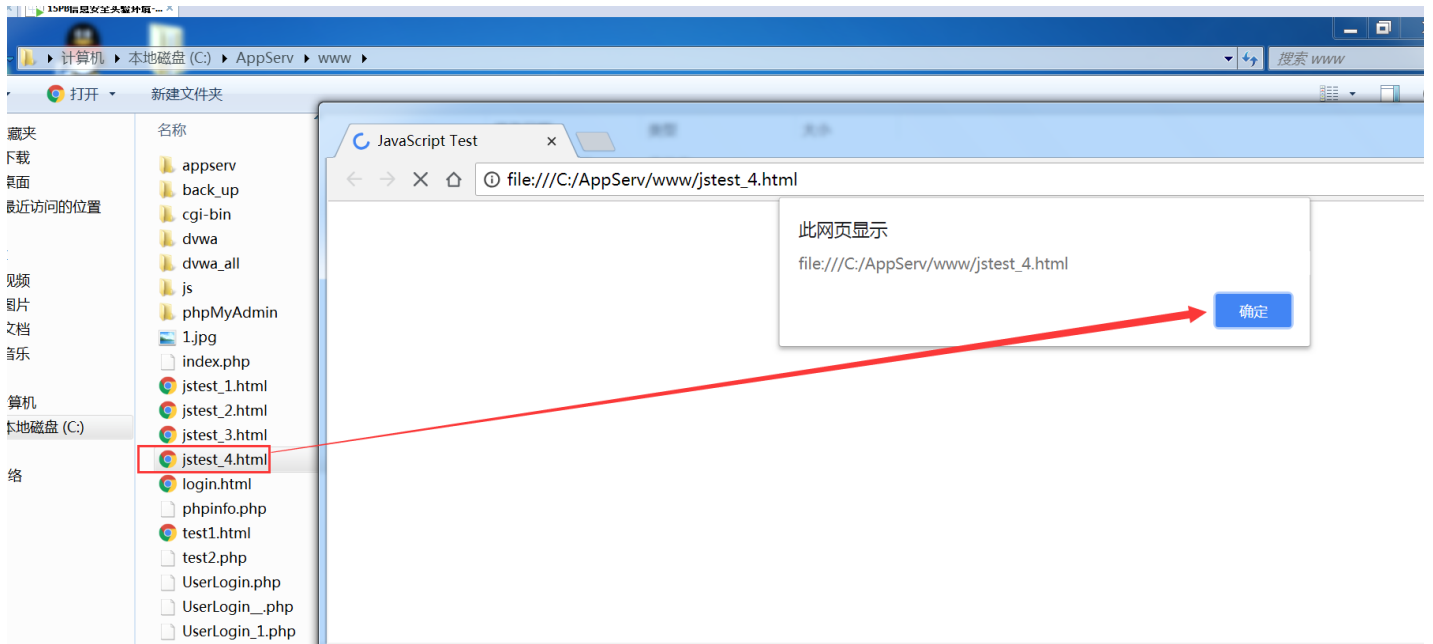
location.href可以简写成location

```
1 <html>
2 <head>
3 <title>
4 JavaScript Test
5 </title>
6 </head>
7
8 <body >
9 <!--
10 <img src=aaa onError="alert('helloworld')">
11 -->
12 <script>
13 document.write(document.location)
14 location.href = "http://www.51cto.com";
15
16 </script>
17
18 </body>
19 </html>
20
```

开 > 新建文件夹



```
1 <html>
2 <head>
3 <title>
4 JavaScript Test
5 </title>
6 </head>
7
8 <body >
9 <!--
10 <img src=aaa onError="alert('helloworld')">
11 -->
12
13 <script>
14 alert(document.location)
15 location.href = "http://www.51cto.com";
16 </script>
17
18 </body>
19 </html>
```



confirm语句

- 显示确认选择对话框,返回true或者false

```
1 <script>
2     if(confirm("3>2? ")==true)
3     {
4         document.write("正确");
5     }
6     else
7     {
8         document.write("错误");
9     }
10 </script>
11
```

```
config.inc.php | low.php | UserLogin.php | UserLogin_1.php | jstest_1.htm | jstest_3.htm | test.js | jstest_4.htm
1 <html>
2 <head>
3 <title>
4 JavaScript Test
5 </title>
6 </head>
7
8 <body>
9 <!--
10 <img src=aaa onError="alert('helloworld')">
11 -->
12 <script>
13 if (confirm("3>2?")== true)
14 {
15     document.write("正确");
16 }
17 else
18 {
19     document.write("error!");
20 }
21
22 </script>
23
24 </body>
25 </html>
```

