document 对象的常用属性

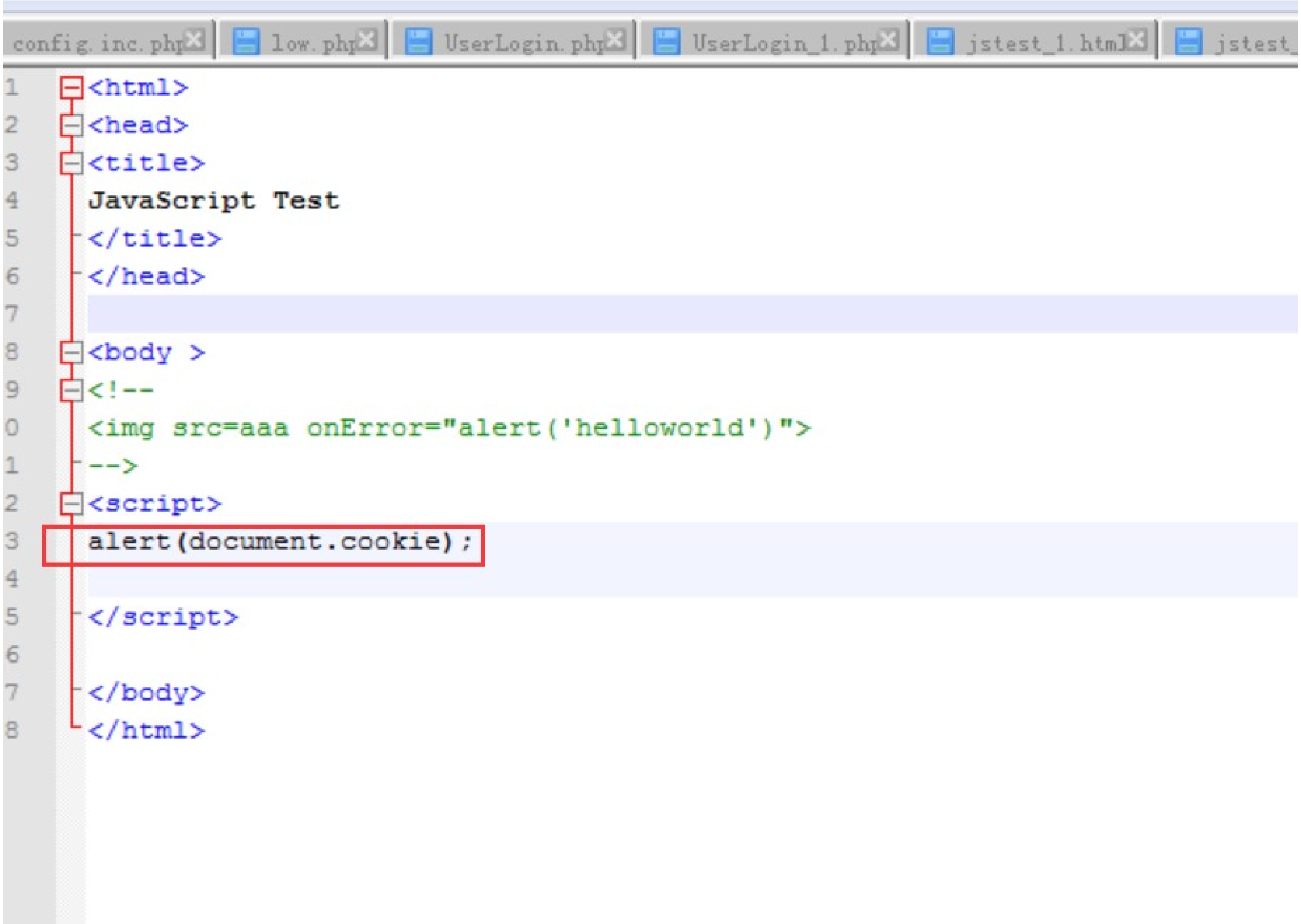
- document.cookie,显示当前页面的cookie(访问当前页面的cookie)

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

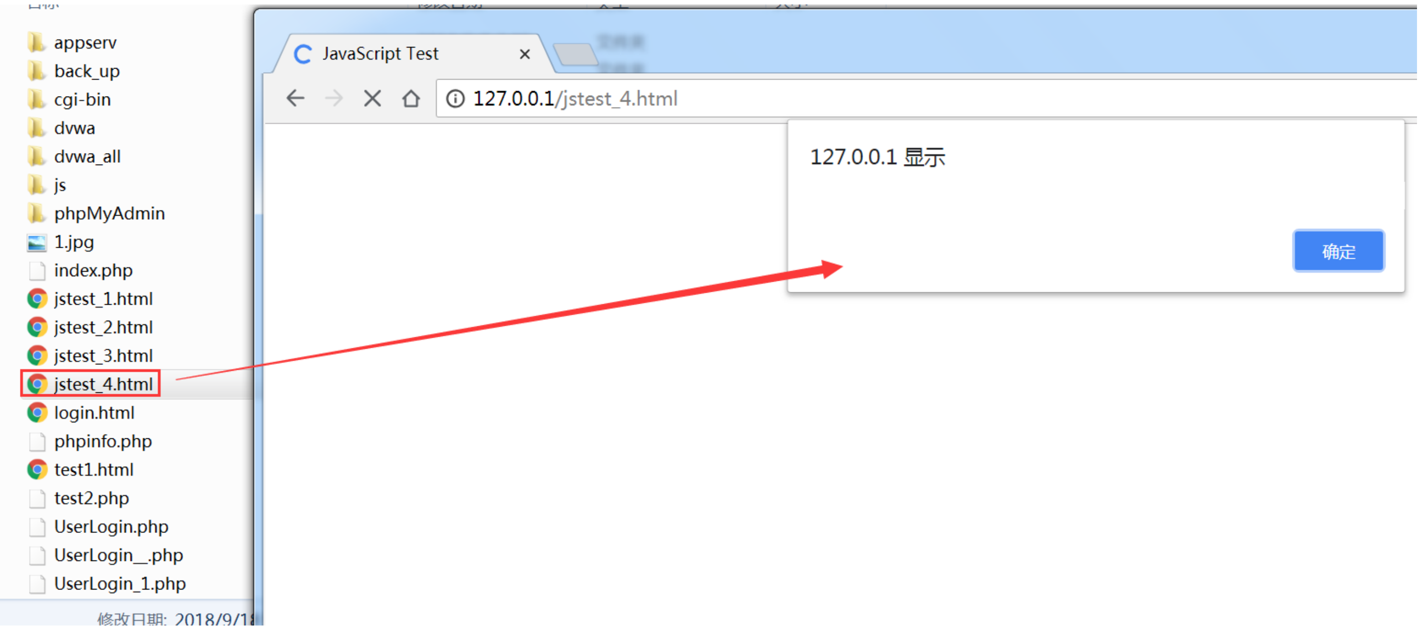
- document.location,显示当前页面的URL

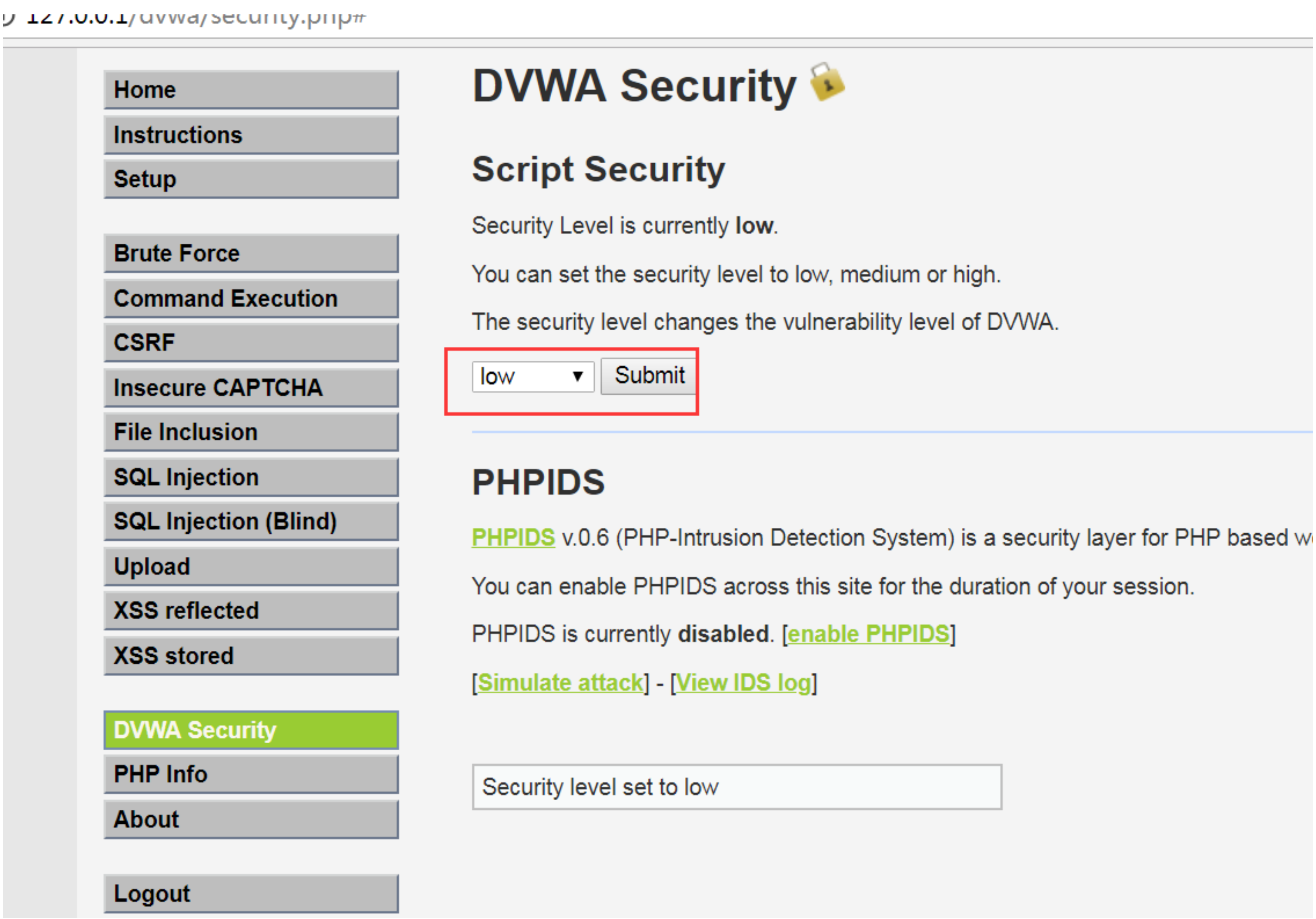
```
<script>alert(document.location);
    </script>
```

这里由于没有登录所以没有显示cookie!



```
<html>
<head>
<title>
JavaScript Test
</title>
</head>

<body >
<!--
<img src=aaa onError="alert('helloworld')">
-->
<script>
alert(document.cookie);

</script>

</body>
</html>
```





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.

PHPIDS

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

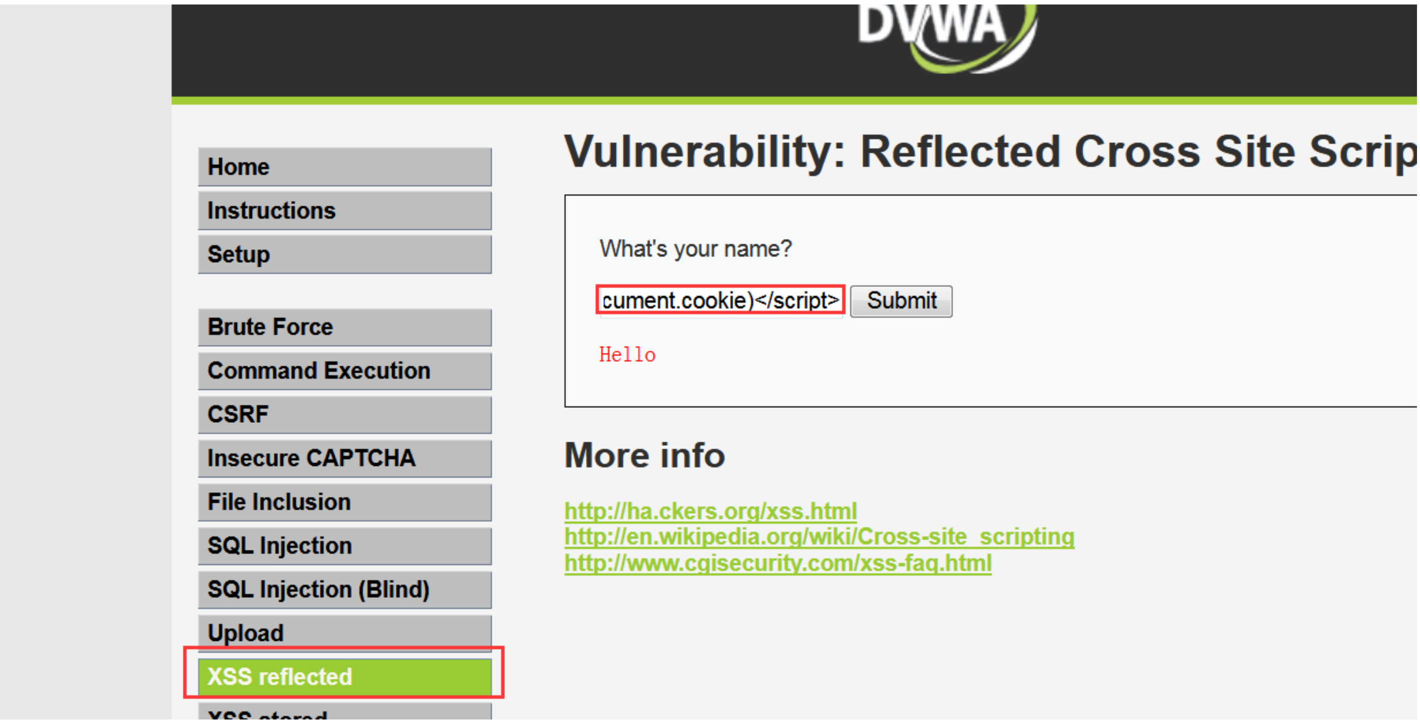
You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]

Security level set to low

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



Vulnerability: Reflected Cross Site Scrip

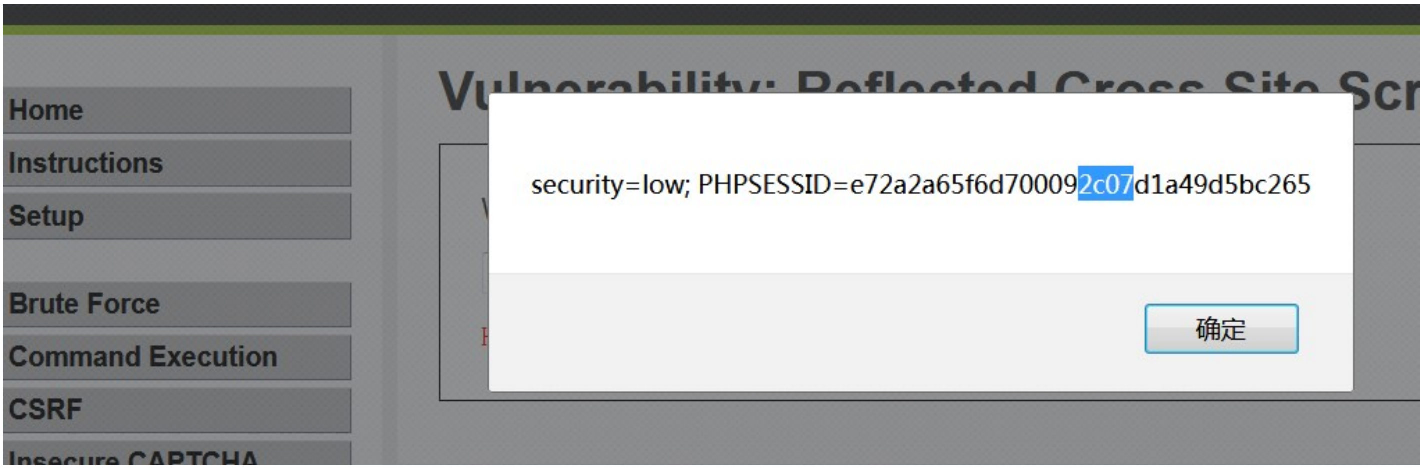
What's your name?

cument.cookie)</script> Submit

Hello

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html



security=low; PHPSESSID=e72a2a65f6d700092c07d1a49d5bc265

```
<html>
<head>
<title>
JavaScript Test
</title>
</head>

<body >
<!--
<img src=aaa onError="alert('helloworld')">
-->
<script>
document.write(document.cookie);

</script>

</body>
</html>
```

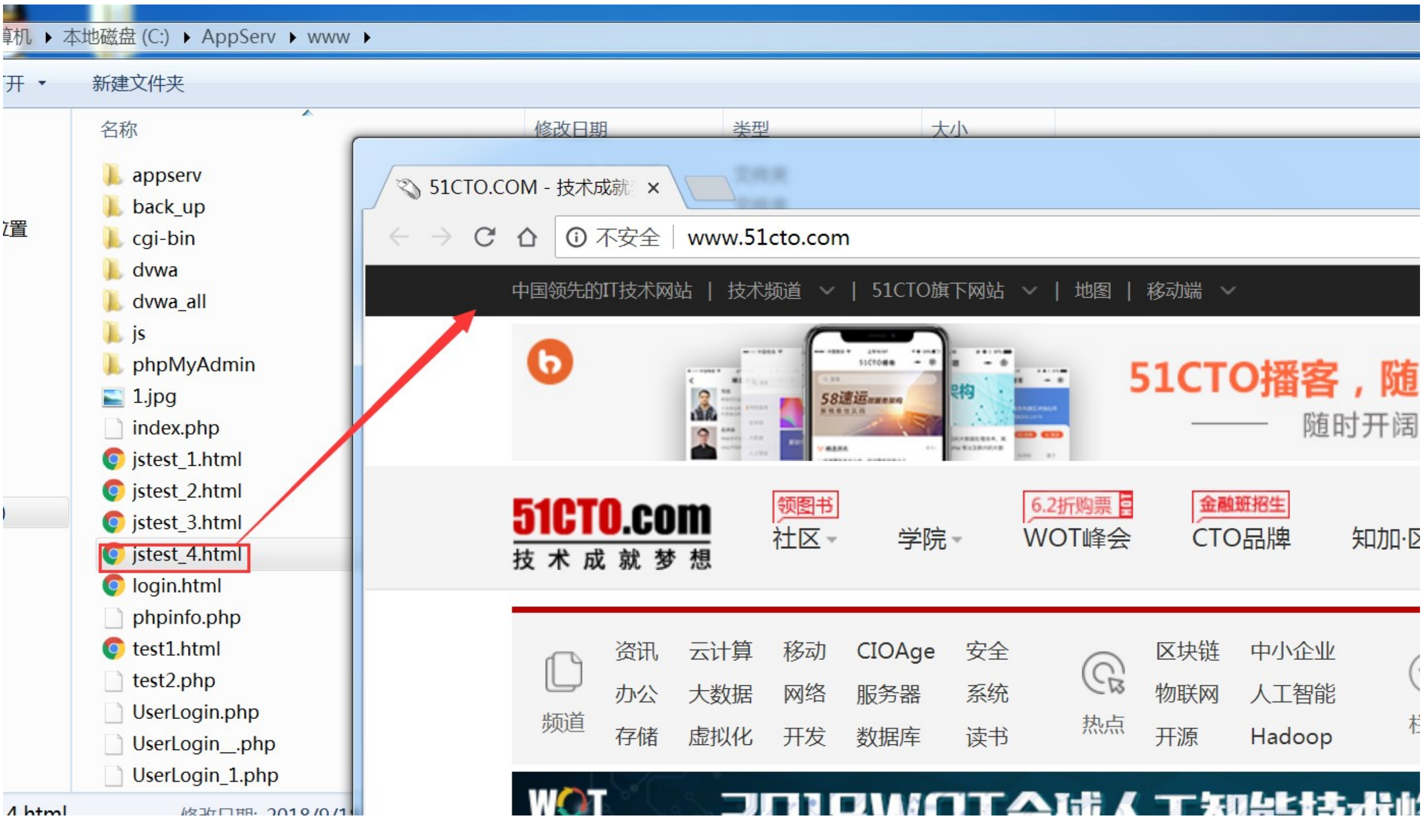
locatio.href实现页面跳转

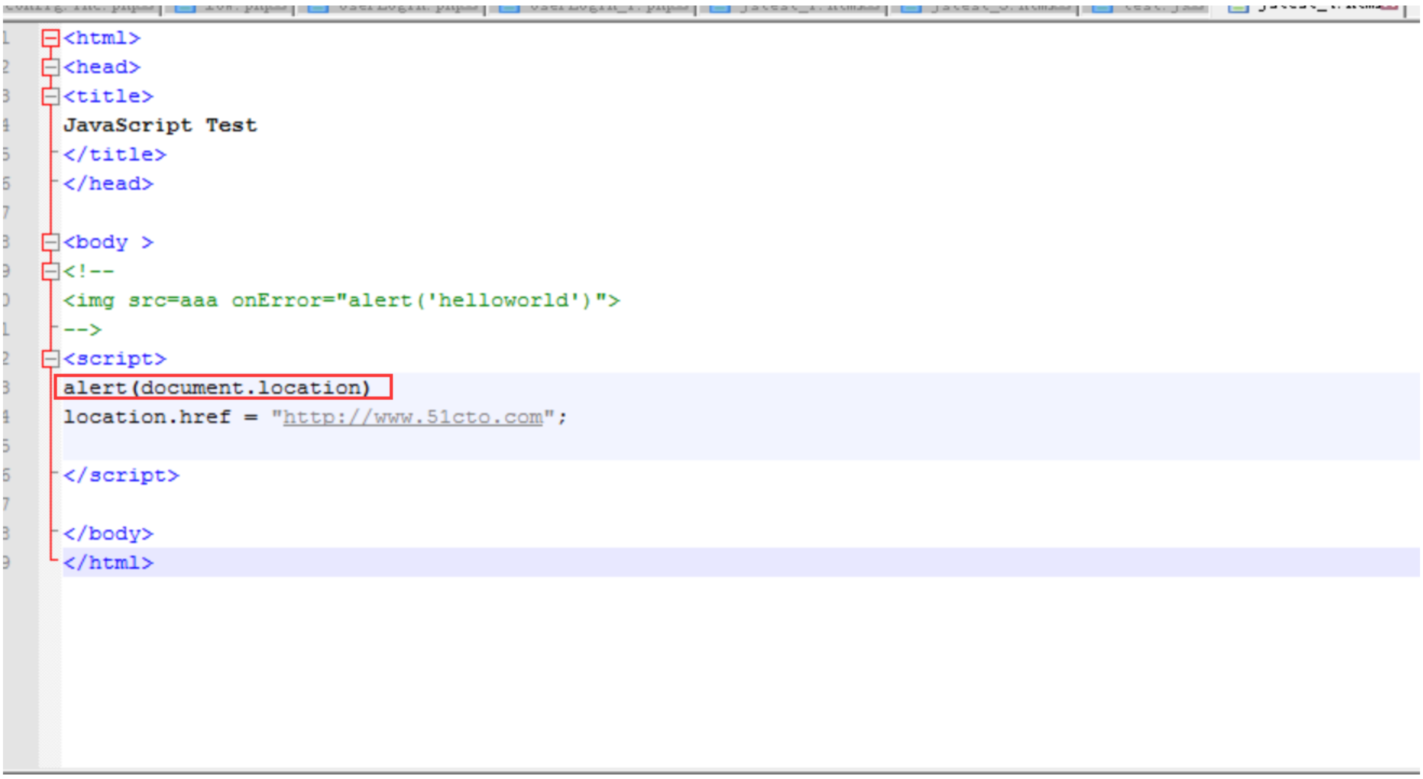
- 当页面整体跳转至另外一个页面上去

```
<script>
alert(document.location);
location.href = "www.51cto.com";
</script>

```

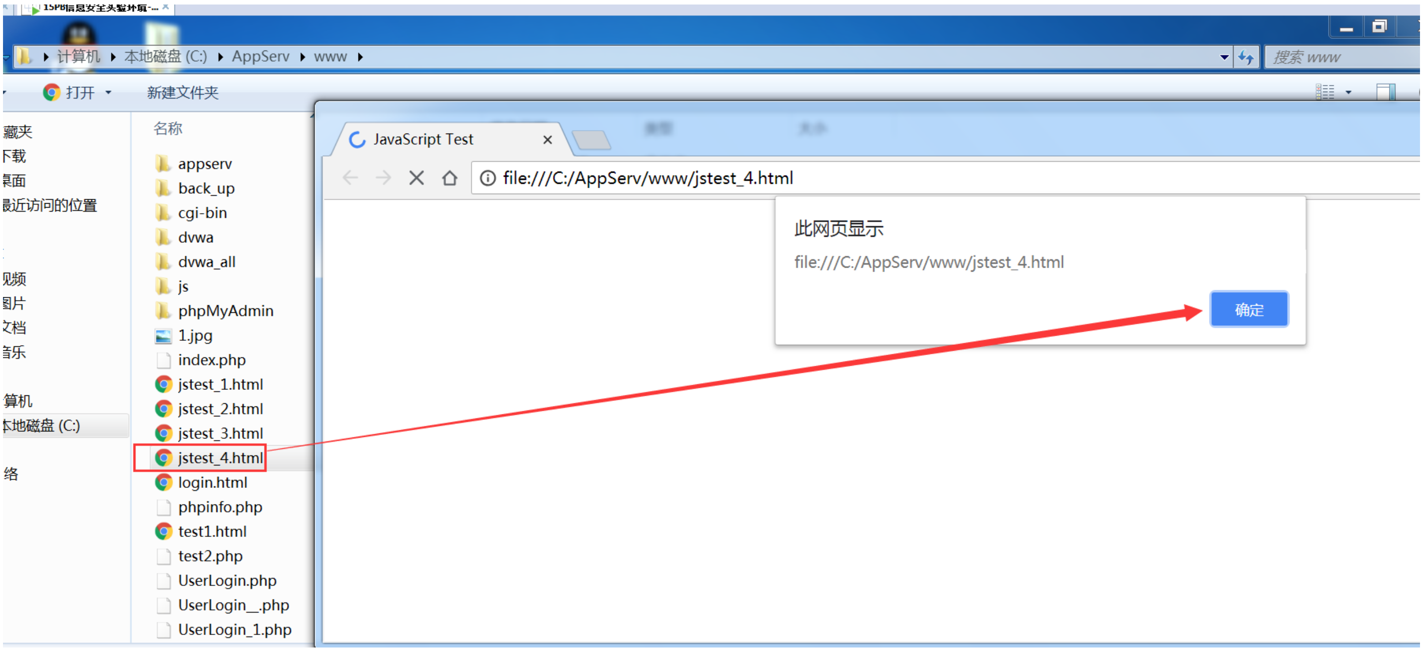
location.href可以简写成location

```
<html>
<head>
<title>
JavaScript Test
</title>
</head>

<body >
<!--
<img src=aaa onError="alert('helloworld')">
-->
<script>
document.write(document.location)
location.href = "http://www.51cto.com";

</script>

</body>
</html>

```



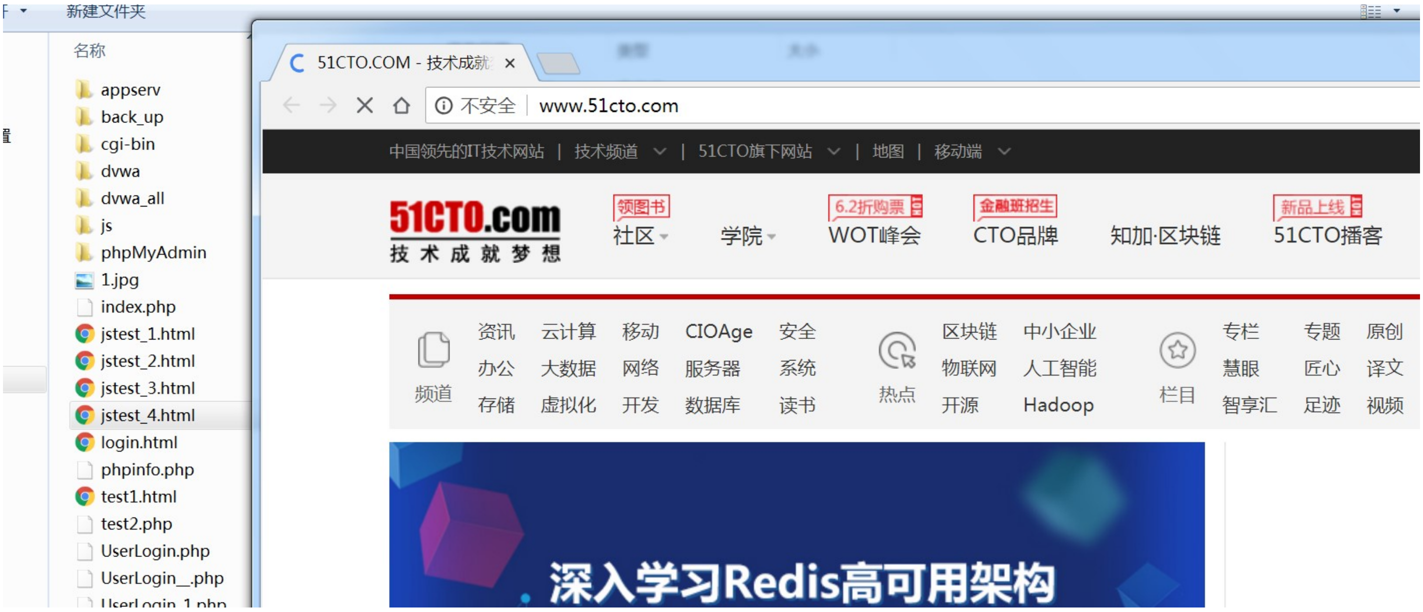


```
<html>
<head>
<title>
JavaScript Test
</title>
</head>

<body >
<!--
<img src=aaa onError="alert('helloworld')">
-->
<script>
alert(document.location)
location.href = "http://www.51cto.com";

</script>

</body>
</html>
```



此网页显示

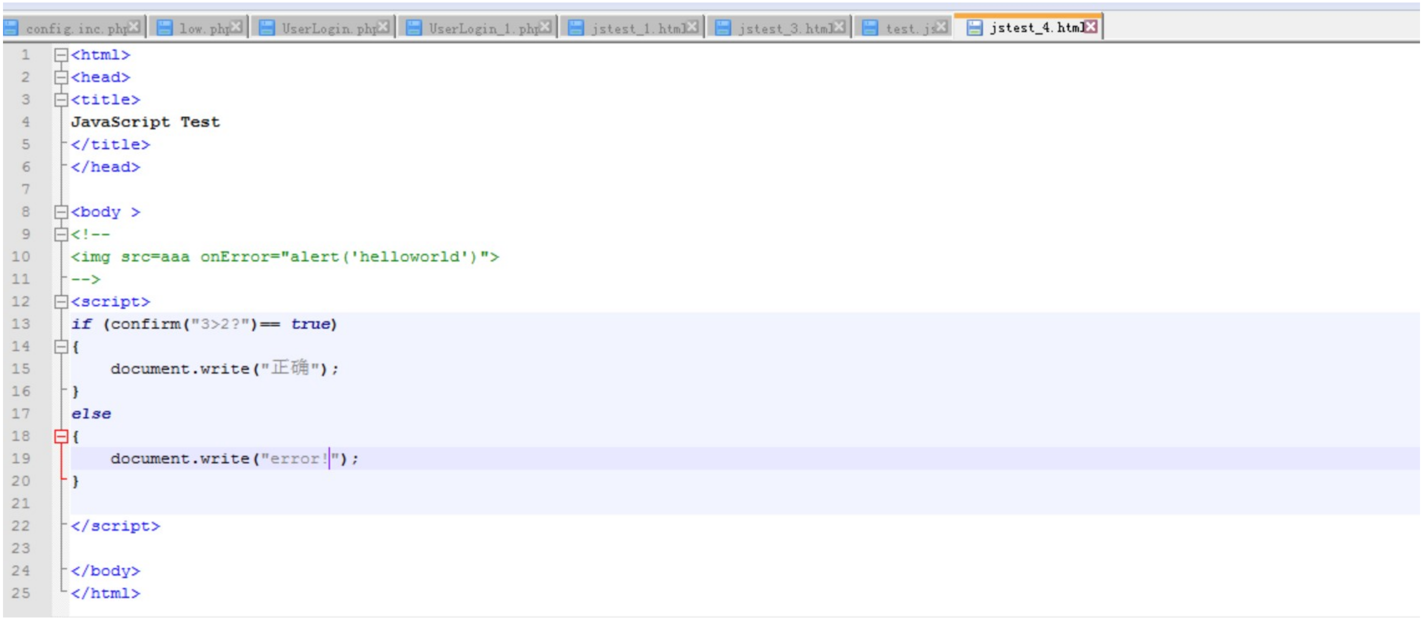
file:///C:/AppServ/www/jstest_4.html



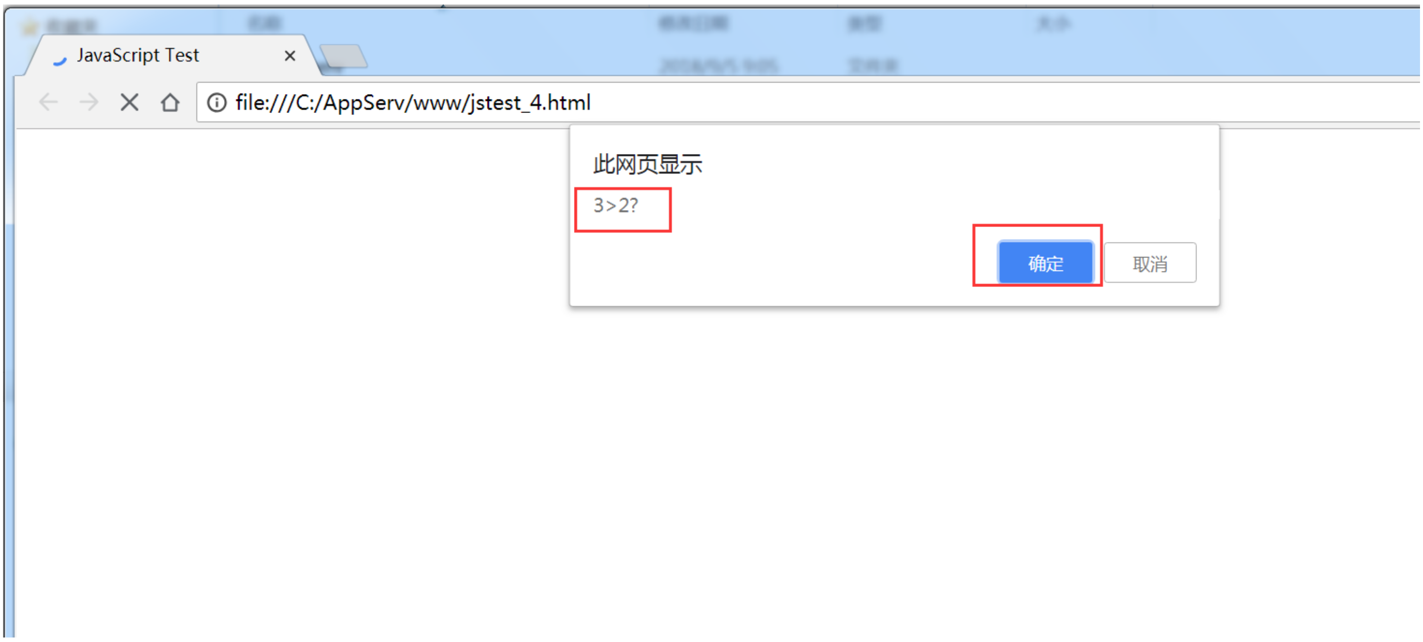
confirm语句

- 显示确认选择对话框,返回true或者false

```
<script>
    if(confirm("3>2? ")==true)
    {
    document.write("正确");
    }
    else
    {
        document.write("错误");
    }
</script>

```

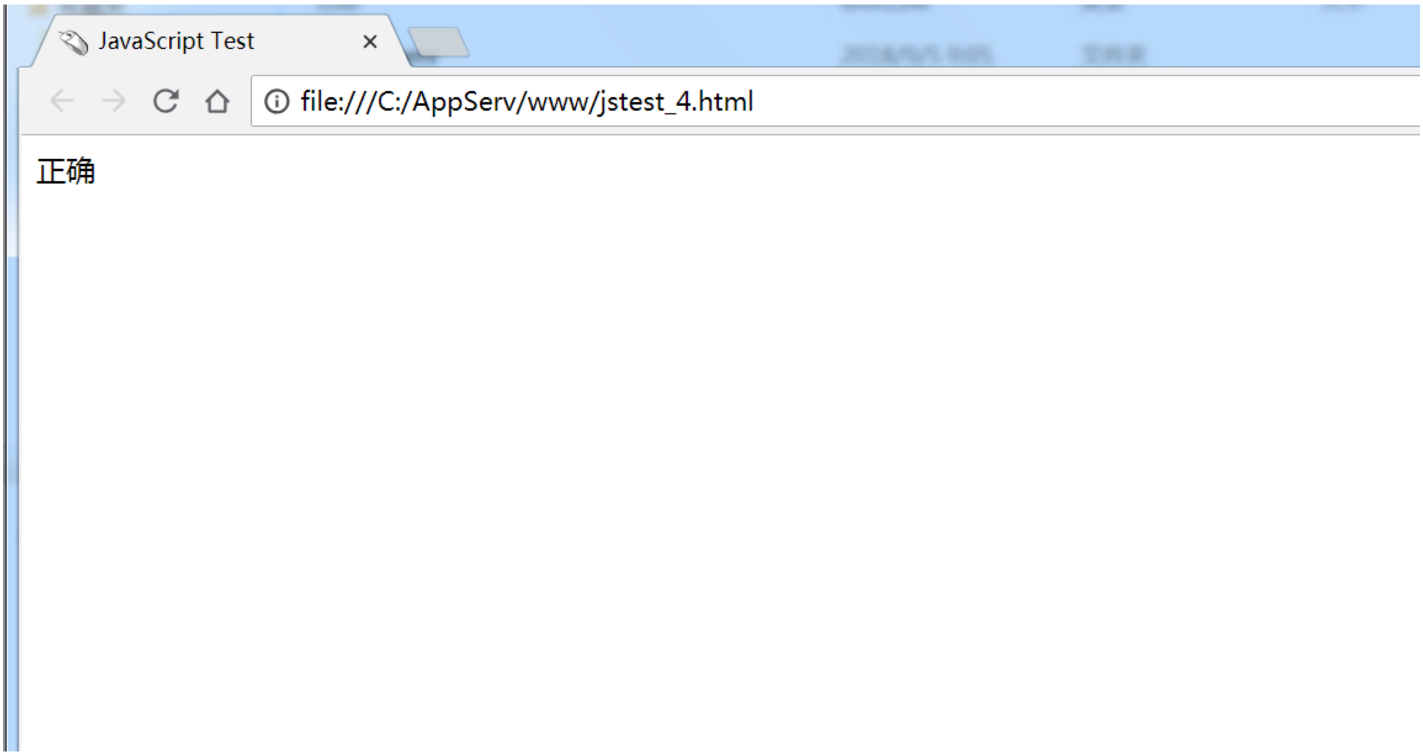


```
<html>
<head>
<title>
JavaScript Test
</title>
</head>

<body >
<!--
<img src=aaa onError="alert('helloworld')">
-->
<script>
if (confirm("3>2?")== true)
{
    document.write("正确");
}
else
{
    document.write("error!");
}

</script>

</body>
</html>
```



此网页显示

3>2?



正确