极客学院
jikexueyuan.com

XSS测试与防御

XSS测试与防御 — **课程概要**

- XSS辅助工具使用介绍
- XSS漏洞挖掘实例讲解
- XSS的防御

XSS辅助工具使用介绍

XSS辅助工具使用介绍

HackBar与TamperData的使用

- 使用HackBar模拟请求
- 使用TamperData修改提交的数据
- Fiddler(Watcher/x5s)

XSS漏洞挖掘实例讲解

XSS漏洞挖掘实例讲解

XSS实例

https://xss-game.appspot.com/

答案:http://www.freebuf.com/articles/web/36072.html

XSS的防御

XSS的防御

XSS的一些基本转义

- html_escape
- javascript_string_escape
- url_escape
- css_string_escape
- 推荐：《给开发者的终极XSS防御备忘录》

XSS的防御

设置字符编码和content-type

- 字符编码：避免如utf-7 XSS等问题
- Conent-type：避免如Json的XSS等问题

XSS的防御

HTTP响应头的一些XSS防护指令

HTTP 响应头	描述
X-XSS-Protection: 1; mode=block	该响应头会开启浏览器的防 XSS 过滤器。
X-Frame-Options: deny	该响应头会禁止页面被加载到框架。
X-Content-Type-Options: nosniff	该响应头会阻止浏览器做 MIMEtype（译者
	注:Multipurpose Internet Mail Extensions，代表互联网媒体类型）嗅探。.
Content-Security-Policy: default-src 'self'	该响应头是防止 XSS 最有效的解决方案之一。它允许我们定义从 URLS 或内容中加载和执行对象的策略
Set-Cookie: key=value; HttpOnly	Set-Cookie 响应头通过 HttpOnly 标签的设置将限制 JavaScript 访问你的 Cookie。
Content-Type: type/subtype; charset=utf-8	始终设置响应的内容类型和字符集. 例如: 返回 json 格式应该使用 application/json, 纯文本使用 text/plain, HTML 使用 text/html 等等，以及设置字符集为 utf-8。

XSS的防御

PHP的XSS防护

```
echo htmlspecialchars($string, ENT_QUOTES | ENT_XHTML, 'UTF-8');
```

XSS的防御

JAVA的XSS防护

使用WASP Java Encoder

XSS的防御

Coverity Security Library(CSL)

转义方法	描述
cov:htmlEscape(string)	执行 HTML 编码
cov:jsStringEscape(string)	执行 JavaScript 字符串编码
cov:asURL(string)	执行 URL 编码和净化危险的 scheme，如javascript:
cov:cssStringEscape(string)	执行 CSS 字符串编码
cov:asNumber(string)	检查输入额字符串是一个数值，默认值为 0
cov:asCssColor(string)	允许将颜色字符串指定为文本或者十六进制并且防止注入
cov:uriEncode(name)	执行 URL 编码

XSS的防御

OWASP ESAPI(The OWASP Enterprise Security API)

Method	Description
ESAPI.encoder().encodeForHTML()	转义 HTML
ESAPI.encoder().encodeForHTMLAttribute()	转义 HTML 属性
ESAPI.encoder().encodeForJavaScript()	转义 JavaScript 字符串
ESAPI.encoder().encodeForCSS()	转义 CSS 字符串
ESAPI.encoder().encodeForURL()	转义 URL

XSS的防御

.NET的XSS防护

HttpUtility Class(System.Web.HttpUtility)

Methods	Description
HtmlEncode()	HTML 编码。
HtmlAttributeEncode()	基础 HTML 编码，它只编码 (" & < \ )。
UrlEncode()	URL 编码。
JavaScriptStringEncode()	JavaScript 字符串编码。

XSS的防御

AntiXSSencoder类(System.Web.Security.AntiXssEncoder于.NET 4.5)

方法	描述
HtmlEncode()	HTML 编码，并且可选指定是否使用 HTML 4.0 的命名实体。
HtmlAttributeEncode()	编码 HTML 属性中反射的数据。
HeaderNameValueEncode()	编码 header 的名称和值为可以用用于 HTTP header 的字符串。
HtmlFormUrlEncode()	编码用于表单提交的 MIME 类型为 "application/x-www-formurlencoded" 的数据，并选择指定的字符串编码。
JavaScriptStringEncode()	JavaScript 字符串编码。
UrlEncode()	URL 编码并选择指定的字符串编码。
UrlPathEncode()	编码 URL 中使用的路径。
XmlAttributeEncode() & XmlEncode()	编码 XML 属性中使用的数据。

XSS的防御

Ruby on Rails 框架中的XSS防护

Method	Description
sanitize()	这个方法可以用来清洁/HTML 编码用户指定的数据，由白名单提供支持。它也可以分别清洁无效协议的 href/src 标签, 像javascript: 。它会尽可能的应对任何技巧的使用，比如输入 unicode/ascii/hex 值来通过javascript: 过滤器的技巧。
sanitize_css()	该方法将会清洁字符串，你可以在 CSS 中安全的使用它。
strip_links()	该方法将清除一个字符串中的所有链接标签。
h() or html_escape()	这个方法将分别编码 (& < > " ') 为 (& < > " ') 。
html_escape_once()	该方法类似于 html_escape() 。一个不同的地方在于它将编码之前没有编码过的任何东西。
json_escape()	该方法将分别编码 (& > < \u2028 \u2029) 为 (\u0026 \u003e \u003c \u2028 \u2029) 。同时也要记住，这个方法只能用于有效的 JSON。无效 JSON 值使用可以导致 XSS。

XSS的防御

Python Django框架中的XSS防护

函数	描述
{{ string }}	django 有自动转义功能，这将转义字符串。
escape()	该函数将转义（&"'<>）。
conditional_escape()	该函数类似于 escape() 函数, 除了它不能转义转义过的字符串，所以它不能进行双重转义。
urlencode()	该函数可以用于 URL 编码。

XSS测试与防御

本课程我们主要进行XSS相关测试与防御的讲解，主要包含：

- 使用辅助工具模拟和修改数据请求
- XSS实例测试
- XSS的防御

XSS是一门很深的课程，特别是涉及到编码等问题的处理还有XSS绕过的艺术等，有兴趣大家可以深入的去了解。

极客学院
jikexueyuan.com

中国最大的IT职业在线教育平台