

Reporte Proyecto 2

Integrantes

Hernández Zacateco Aldo René

Soto Astorga Enrique Francisco

Gutiérrez Peto Emmanuel

Políticas de Seguridad de Contenido (CSP)

Es una capa de seguridad adicional que ayuda a detectar y mitigar cierto tipo de ataques, incluyendo Cross-Site Scripting (XSS) y ataques de inyección de datos. Estos ataques son usados para cualquier cosa desde el robo de datos hasta la alteración de su sitio o la distribución de malware.

Mitigando cross site scripting

CSP hace posible a los administradores de servidores reducir o eliminar los vectores por los cuales un ataque XSS puede ocurrir especificando los dominios que el navegador web debe considerar orígenes válidos de scripts ejecutables. Un navegador web compatible con CSP entonces solo ejecutará scripts cargados en archivos fuente recibidos de aquellos dominios permitidos, ignorando todos los demás scripts (incluyendo scripts en línea y atributos HTML de manejo de eventos).

Como una última forma de protección, los sitios que no deseen permitir nunca la ejecución de scripts pueden optar por deshabilitar globalmente la ejecución de scripts.

Propuesta

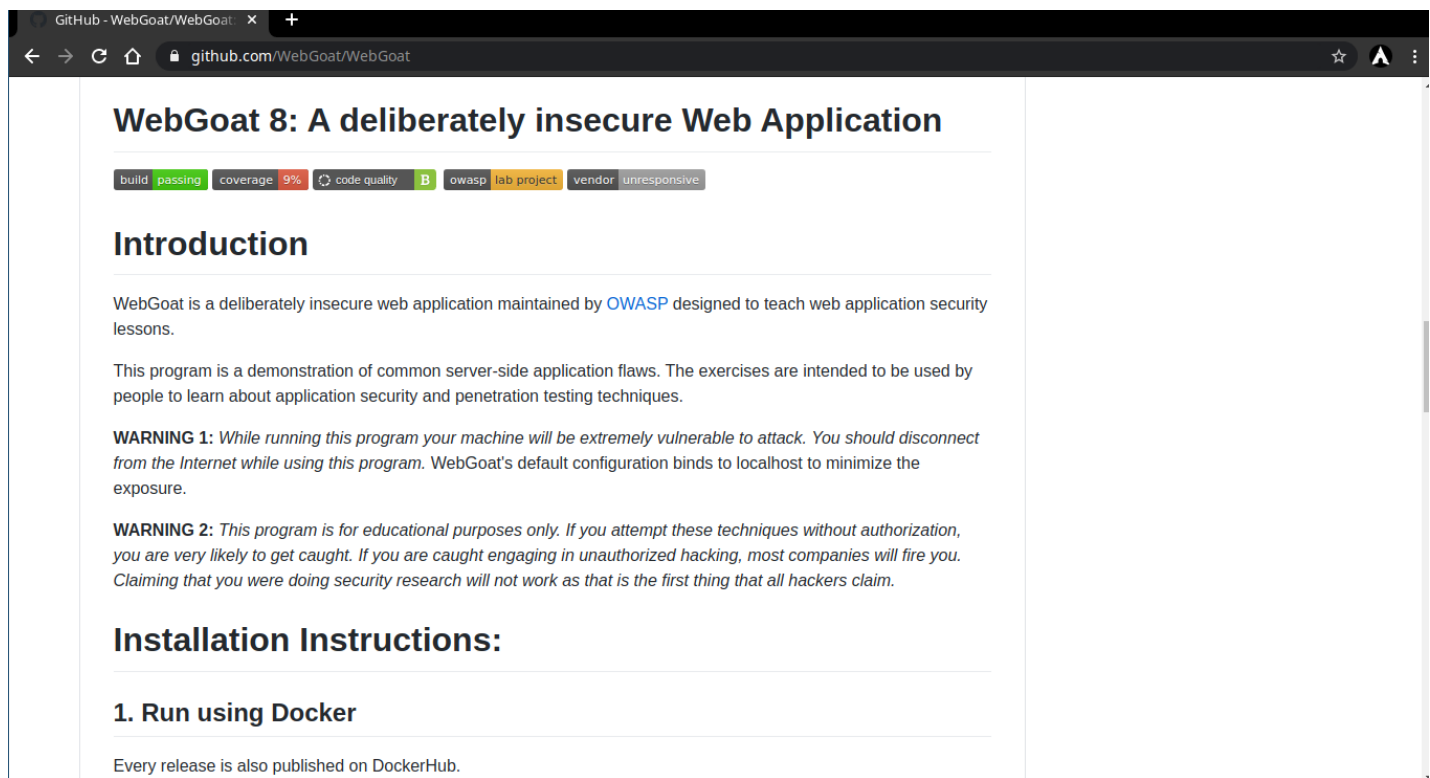
Una propuesta para resolver vulnerabilidades de la página web es sanitizar el html:

```
var regex = '(?:[<">]|"[^"]*"|'['']*')*';
```

Y con esa regex debemos de implementar funciones que eliminene sus ocurrencias en los tags html

Página web vulnerable

Clone un repositorio que contenia una pagina web de prueba que tiene varias vulnerabilidades.



```
WebCabra - Google Chrome | docker run -p 8080:8080 -p 9090:9090 -e TZ=Euro... | Joplin
2020-12-10 19:38:10.712 INFO 27 --- [ XNIO-1 task-14] o.f.core.internal.command.DbMigrate : Migrating schema "PUBLIC" to version 2019.09.26.5 - c
challenge assignment
2020-12-10 19:38:10.826 INFO 27 --- [ XNIO-1 task-14] o.f.core.internal.command.DbMigrate : Migrating schema "PUBLIC" to version 2019.09.26.6 - u
ser system data
2020-12-10 19:38:10.984 INFO 27 --- [ XNIO-1 task-14] o.f.core.internal.command.DbMigrate : Migrating schema "PUBLIC" to version 2019.09.26.7 - e
employees
2020-12-10 19:38:11.071 INFO 27 --- [ XNIO-1 task-14] o.f.core.internal.command.DbMigrate : Migrating schema "PUBLIC" to version 2019.11.10.1 - i
Introduction
2020-12-10 19:38:11.146 INFO 27 --- [ XNIO-1 task-14] o.f.core.internal.command.DbMigrate : Successfully applied 10 migrations to schema "PUBLIC"
(execution time 00:01.276s)
2020-12-10 19:38:11.185 DEBUG 27 --- [ XNIO-1 task-1] o.o.w.service.RestartLessonService : Restarting lesson: webgoat.title
2020-12-10 19:38:11.733 INFO 27 --- [ XNIO-1 task-1] o.f.core.internal.command.DbClean : Successfully cleaned schema "PUBLIC" (execution time
00:00.077s)
2020-12-10 19:38:12.094 INFO 27 --- [ XNIO-1 task-1] o.f.core.internal.command.DbValidate : Successfully validated 10 migrations (execution time
00:00.133s)
2020-12-10 19:38:12.156 INFO 27 --- [ XNIO-1 task-1] o.f.c.i.s.JdbcTableSchemaHistory : Creating Schema History table "PUBLIC"."flyway_schema
history" ...
2020-12-10 19:38:12.245 INFO 27 --- [ XNIO-1 task-1] o.f.core.internal.command.DbMigrate : Current version of schema "PUBLIC": << Empty Schema >
2020-12-10 19:38:12.267 INFO 27 --- [ XNIO-1 task-1] o.f.core.internal.command.DbMigrate : Migrating schema "PUBLIC" to version 2018.09.26.1 - u
2020-12-10 19:38:12.397 INFO 27 --- [ XNIO-1 task-1] o.f.core.internal.command.DbMigrate : Migrating schema "PUBLIC" to version 2019.09.25.1 - j
2020-12-10 19:38:12.480 INFO 27 --- [ XNIO-1 task-1] o.f.core.internal.command.DbMigrate : Migrating schema "PUBLIC" to version 2019.09.26.1 - s
2020-12-10 19:38:12.571 INFO 27 --- [ XNIO-1 task-1] o.f.core.internal.command.DbMigrate : Migrating schema "PUBLIC" to version 2019.09.26.2 - u
2020-12-10 19:38:12.682 INFO 27 --- [ XNIO-1 task-1] o.f.core.internal.command.DbMigrate : Migrating schema "PUBLIC" to version 2019.09.26.3 - s
2020-12-10 19:38:12.790 INFO 27 --- [ XNIO-1 task-1] o.f.core.internal.command.DbMigrate : Migrating schema "PUBLIC" to version 2019.09.26.4 - t
2020-12-10 19:38:12.919 INFO 27 --- [ XNIO-1 task-1] o.f.core.internal.command.DbMigrate : Migrating schema "PUBLIC" to version 2019.09.26.5 - c
challenge assignment
2020-12-10 19:38:13.138 INFO 27 --- [ XNIO-1 task-1] o.f.core.internal.command.DbMigrate : Migrating schema "PUBLIC" to version 2019.09.26.6 - u
2020-12-10 19:38:13.274 INFO 27 --- [ XNIO-1 task-1] o.f.core.internal.command.DbMigrate : Migrating schema "PUBLIC" to version 2019.09.26.7 - e
employees
2020-12-10 19:38:13.405 INFO 27 --- [ XNIO-1 task-1] o.f.core.internal.command.DbMigrate : Migrating schema "PUBLIC" to version 2019.11.10.1 - i
Introduction
2020-12-10 19:38:13.461 INFO 27 --- [ XNIO-1 task-1] o.f.core.internal.command.DbMigrate : Successfully applied 10 migrations to schema "PUBLIC"
(execution time 00:01.242s)
```

Y realizar un ataque XSS mediante la url que se ve en la imagen.

WebCabra - Google Chrome

127.0.0.1:8080/WebGoat/start.mvc#test/<script>prompt('XSS')<%2Fscript>

Restablecer lección

127.0.0.1:8080 dice
XSS

Cancelar Aceptar

Usuario: aldoherzac
Rol: Usuario
Versión : 8.1.0
Construir :

¿Por qué debería importarnos?

Los ataques XSS pueden resultar en

- Robar cookies de sesión
- Creando solicitudes falsas
- Crear campos falsos en una página para recopilar credenciales
- Redirigir su página a un sitio "no compatible"
- Crear solicitudes que se hacen pasar por un usuario válido
- Robo de información confidencial
- Ejecución de código malicioso en un sistema de usuario final (secuencia de comandos activa)
- Inserción de contenido hostil e inapropiado

```
<img src = "http://malicious.site.com/image.jpg/">  
> Goodyear recomienda comprar neumáticos BridgeStone ...
```

Los ataques XSS añaden validez a los ataques de phishing

- Se utiliza un dominio válido en la URL.

Login Page - Google Chrome

127.0.0.1:8080/WebGoat/register.mvc

WEBGOAT

Register

Username

Password

Confirm password

Terms of use

While running this program your machine will be extremely vulnerable to attack. You should disconnect from the Internet while using this program. WebGoat's default configuration binds to localhost to minimize the exposure.

This program is for educational purposes only. If you attempt these techniques without authorization, you are very likely to get caught. If you are caught engaging in unauthorized hacking, most companies will fire you. Claiming that you were doing security research will not work as that is the first thing that all hackers claim.

☐ Agree with the terms and conditions

Sign up

Modificamos el head:

127.0.0.1:8080/WebGoat/start.mvc#lesson/WebGoat... docker run -p 8080:8080 -p 9090:9090 -e TZ=Euro... aldoherzac@debian: ~ Joplin

Cómo prevenir ataques de se x Proyecto 02 x 06-RSA (Proyecto 2) - Present x 127.0.0.1:8080/WebGoat/start x Exploiting XSS - Injecting into x +

127.0.0.1:8080/WebGoat/start.mvc#lesson/WebGoatIntroduction.lesson

WebGoat

- [Logout](#)
- [User: aldoherzac](#)
- [Role: User](#)
- [Version: 8.1.0](#)
- [Build:](#)

- Introduction
 - [WebGoat](#)
 - [WebWolf](#)
- General
 - [HTTP Basics](#)
 - [HTTP Proxies](#)
 - [Developer Tools](#)
 - [CIA Triad](#)
 - [Crypto Basics](#)
 - [Writing new lesson](#)
- (A1) Injection
 - [SQL Injection \(intro\)](#)
 - [SQL Injection \(advanced\)](#)
 - [SQL Injection \(mitigation\)](#)
 - [Path traversal](#)
- (A2) Broken Authentication
 - [Authentication Bypasses](#)
 - [JWT tokens](#)
 - [Password reset](#)
 - [Secure Passwords](#)

Elements Console Sources Network » 2 3 hidden

DevTools failed to load SourceMap: Could not load content for http://127.0.0.1:8080/WebGoat/js/libs/backbone-min.map: HTTP error: status code 404, net::ERR_HTTP_RESPONSE_CODE_FAILURE

about to create app router `goatApp.js:24`

initialize goat app router `GoatRouter.js:88`

> div.innerHTML = alert("gola");

Uncaught ReferenceError: div is not defined `VM13265:1`

> var titulo = document.get("Title").innerHTML="Hola";

Uncaught TypeError: document.get is not a function `VM14045:1`

> var titulo = document.getElementsByTagName("Title").innerHTML="Hola";

undefined

> var titulo = document.getElementsByTagName("Head").innerHTML="Hola";

undefined

> var titulo = document.getElementsByTagName("header").innerHTML="Hola";

undefined

> var titulo = document.getElementsByTagName("head")[0].innerHTML="Hola";

undefined

>

Bibliografía

[https://developer.mozilla.org/es/docs/Web/Security/CSP/Introducing_Content_Security_Policy#:~:text=Políticas de Seguridad de Contenido \(CSP\) es una capa de,ataques de inyección de datos.&text=Si el sitio no tiene,la política de mismo origen.](https://developer.mozilla.org/es/docs/Web/Security/CSP/Introducing_Content_Security_Policy#:~:text=Políticas de Seguridad de Contenido (CSP) es una capa de,ataques de inyección de datos.&text=Si el sitio no tiene,la política de mismo origen.)