

UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA

ESCUELA PROFESIONAL DE CIENCIA DE LA
COMPUTACIÓN
INGENIERA DE SOFTWARE II



Laboratorio 6

Presentado por:

Fiorela Villarroel Ramos

Juan Manuel Soto Begazo

Docente :

Edgar Sarmiento Calisaya



Laboratorio 6 : Pruebas de Seguridad con OWASP - ZAP

1. Objetivo

Automatizar pruebas de seguridad de aplicaciones web utilizando OWASP ZAP

2. Actividades

1. Configurar Proxies: <https://github.com/zaproxy/zap-core-help/wiki/HelpStartProxies>
2. Implementar Pruebas de Penetración sobre una aplicación web apropiada con propósito de investigación en seguridad!
 - a) Implementar los casos de prueba [reglas]
 - b) Ejecutar los casos de prueba [ejecutar ataques]
 - c) Reportar los resultados de la ejecución (Alertas - alarmas)

2.1. Pre-requisitos

- maven

```
C:\Users\juan>mvn --version
Apache Maven 3.8.6 (84538c9988a25aec085021c365c560670ad80f63)
Maven home: C:\Program Files\apache-maven-3.8.6
Java version: 17.0.4.1, vendor: Oracle Corporation, runtime: C:\Program Files\Java\jdk-17.0.4.1
Default locale: es_PE, platform encoding: Cp1252
OS name: "windows 11", version: "10.0", arch: "amd64", family: "windows"
```

- java +8

```
C:\Users\juan>java --version
java 17.0.4.1 2022-08-18 LTS
Java(TM) SE Runtime Environment (build 17.0.4.1+1-LTS-2)
Java HotSpot(TM) 64-Bit Server VM (build 17.0.4.1+1-LTS-2, mixed mode, sharing)
```

- docker

```
***** Setting docker container name as simple-blog-demo *****
***** Set docker image name as simple-blog-demo:dev *****
***** Set docker image PORT to 8080 *****
***** Create target jar *****
[INFO] Scanning for projects...
Downloading from central: https://repo.maven.apache.org/maven2/org/springframework/boot/spring-boot-starter-parent/2.2.2.RELEASE/spring-boot-starter-parent-2.2.2.RELEASE.pom
Downloaded from central: https://repo.maven.apache.org/maven2/org/springframework/boot/spring-boot-starter-parent/2.2.2.RELEASE/spring-boot-starter-parent-2.2.2.RELEASE.pom (8.1 kB at 5.6 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/org/springframework/boot/spring-boot-dependencies/2.2.2.RELEASE/spring-boot-dependencies-2.2.2.RELEASE.pom
Downloaded from central: https://repo.maven.apache.org/maven2/org/springframework/boot/spring-boot-dependencies/2.2.2.RELEASE/spring-boot-dependencies-2.2.2.RELEASE.pom (127 kB at 280 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/com/fasterxml/jackson/jackson-bom/2.10.1/jackson-bom-2.10.1.pom
Downloaded from central: https://repo.maven.apache.org/maven2/com/fasterxml/jackson/jackson-bom/2.10.1/jackson-bom-2.10.1.pom (13 kB at 42 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/com/fasterxml/jackson/jackson-parent/2.10/jackson-parent-2.10.pom
Downloaded from central: https://repo.maven.apache.org/maven2/com/fasterxml/jackson/jackson-parent/2.10/jackson-parent-2.10.pom
```

2.2. Ejecución de la aplicación springBootDemo

- Creación del archivo SimpleBlogDemo-0.0.1-SNAPSHOT.jar con docker

```
[INFO] Scanning for projects...
[WARNING]
[WARNING] Some problems were encountered while building the effective model for com.barry.home:
[WARNING] 'dependencies.dependency.(groupId:artifactId:type:classifier)' must be unique: org.sp
5, column 15
[WARNING]
[WARNING] It is highly recommended to fix these problems because they threaten the stability of
[WARNING]
[WARNING] For this reason, future Maven versions might no longer support building such malforme
[WARNING]
[INFO]
[INFO] -----< com.barry.home:SimpleBlogDemo >-----
[INFO] Building SimpleBlogDemo 0.0.1-SNAPSHOT
[INFO] -----[ jar ]-----
[INFO]
[INFO] --- maven-clean-plugin:3.1.0:clean (default-clean) @ SimpleBlogDemo ---
[INFO] Deleting E:\Universidad\Ciencias de la Computacion\4to AÑO\Semestre B\Ingenieria de Soft
[INFO]
[INFO] --- maven-resources-plugin:3.1.0:resources (default-resources) @ SimpleBlogDemo ---
[INFO] Using 'UTF-8' encoding to copy filtered resources.
[INFO] Copying 1 resource
[INFO] Copying 9 resources
[INFO]
[INFO] --- maven-compiler-plugin:3.8.1:compile (default-compile) @ SimpleBlogDemo ---
[INFO] Changes detected - recompiling the module!
[INFO] Compiling 14 source files to E:\Universidad\Ciencias de la Computacion\4to AÑO\Semestre
[INFO]
[INFO] --- maven-resources-plugin:3.1.0:testResources (default-testResources) @ SimpleBlogDemo
[INFO] Using 'UTF-8' encoding to copy filtered resources.
[INFO] skip non existing resourceDirectory E:\Universidad\Ciencias de la Computacion\4to AÑO\Se
[INFO]
[INFO] --- maven-compiler-plugin:3.8.1:testCompile (default-testCompile) @ SimpleBlogDemo ---
[INFO] Changes detected - recompiling the module!
[INFO] Compiling 3 source files to E:\Universidad\Ciencias de la Computacion\4to AÑO\Semestre B
[INFO]
[INFO] --- maven-surefire-plugin:2.22.2:test (default-test) @ SimpleBlogDemo ---
[INFO]
```

- Ejecución del punto jar con el comando `java -jar SimpleBlogDemo-0.0.1-SNAPSHOT.jar`

```
C:\Windows\System32\cmd.exe - java -jar SimpleBlogDemo-0.0.1-SNAPSHOT.jar
Microsoft Windows [Versión 10.0.22000.1098]
(c) Microsoft Corporation. Todos los derechos reservados.

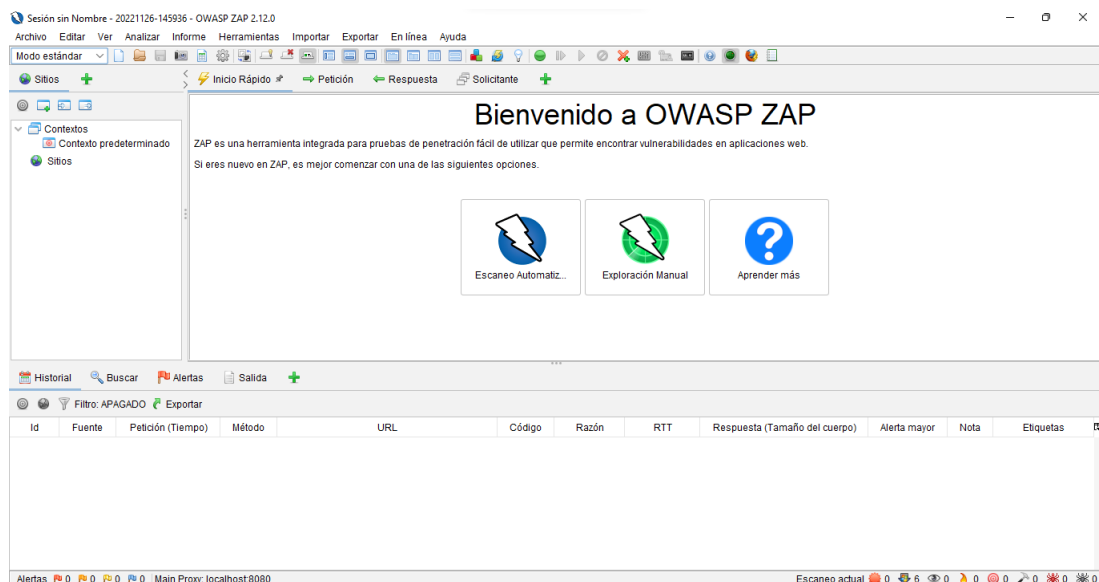
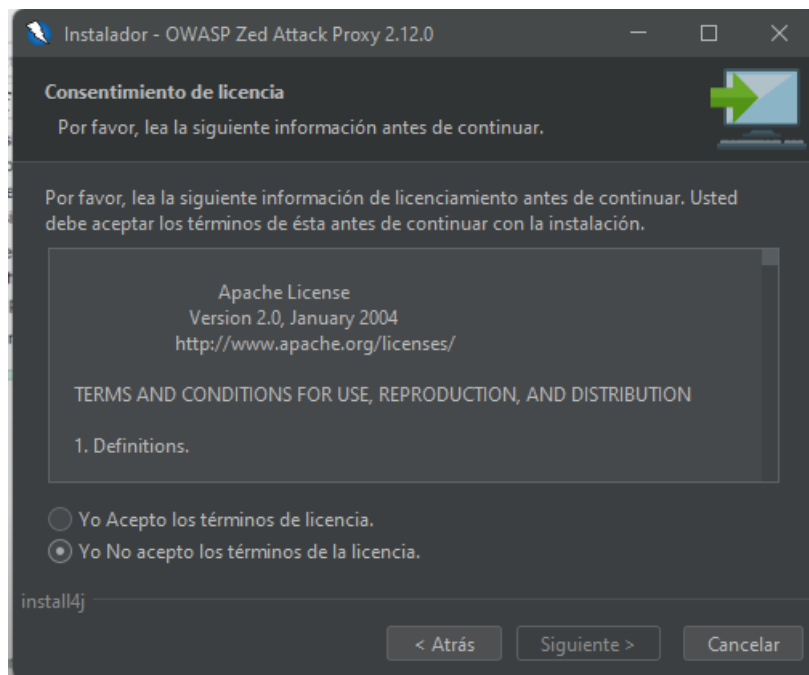
E:\Universidad\Ciencias de la Computacion\4to Año\Semestre B\Ingenieria de Software II\Practica06\SimpleBlogDemo-master\target>java -jar SimpleBlogDemo-0.0.1-SNAPSHOT.jar
22:14:18,177 |-INFO in ch.qos.logback.classic.LoggerContext[default] - Could NOT find resource [logback-test.xml]
22:14:18,179 |-INFO in ch.qos.logback.classic.LoggerContext[default] - Could NOT find resource [logback.groovy]
22:14:18,180 |-INFO in ch.qos.logback.classic.LoggerContext[default] - Found resource [logback.xml] at [jar:file:/E:/Universidad/Ciencias%20de%20la%20Computacion/4to%20Año/Semestre%20B/Ingenieria%20de%20Software%20II/Practica06/SimpleBlogDemo-master/target/SimpleBlogDemo-0.0.1-SNAPSHOT.jar!/BOOT-INF/classes!/logback.xml]
22:14:18,245 |-INFO in ch.qos.logback.core.joran.spi.ConfigurationWatchList@7f560810 - URL [jar:file:/E:/Universidad/Ciencias%20de%20la%20Computacion/4to%20Año/Semestre%20B/Ingenieria%20de%20Software%20II/Practica06/SimpleBlogDemo-master/target/SimpleBlogDemo-0.0.1-SNAPSHOT.jar!/BOOT-INF/classes!/logback.xml] is not of type file
22:14:18,446 |-INFO in ch.qos.logback.classic.joran.action.ConfigurationAction - debug attribute not set
22:14:18,462 |-INFO in ch.qos.logback.classic.joran.action.LoggerAction - Setting level of logger [com.barry.home.SimpleBlogDemo.service.implementation.CommentServiceImpl] to DEBUG
22:14:18,465 |-WARN in ch.qos.logback.classic.joran.action.IncludeAction - Could not find resource corresponding to [org.springframework.boot/logging/logback/defaults.xml]
22:14:18,465 |-INFO in ch.qos.logback.classic.joran.action.AppenderAction - About to instantiate appender of type [ch.qos.logback.core.ConsoleAppender]
22:14:18,475 |-INFO in ch.qos.logback.classic.joran.action.AppenderAction - Naming appender as [STDOUT]
22:14:18,628 |-INFO in ch.qos.logback.classic.joran.action.RootLoggerAction - Setting level of ROOT logger to INFO
22:14:18,629 |-INFO in ch.qos.logback.classic.joran.action.AppenderRefAction - Attaching appender named [STDOUT] to Logger[ROOT]
22:14:18,631 |-INFO in ch.qos.logback.classic.joran.action.ConfigurationAction - End of configuration.
22:14:18,634 |-INFO in ch.qos.logback.classic.joran.JoranConfigurator@69d9c55 - Registering current configuration as safe fallback point

:: Spring Boot ::
(v2.2.2.RELEASE)

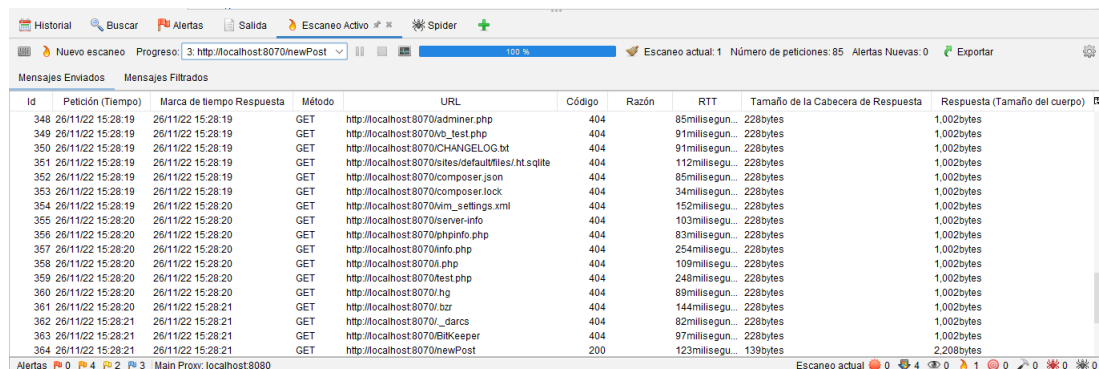
2022-11-25 22:14:19.629 [main] INFO c.b.h.s.SimpleBlogDemoApplication - Starting SimpleBlogDemoApplication v0.0.1-SNAPSHOT on DESKTOP-4F6EK0M with PID 14180 (E:\Universidad\Ciencias de la Computacion\4to Año\Semestre B\Ingenieria de Software II\Practica06\SimpleBlogDemo-master\target\SimpleBlogDemo-0.0.1-SNAPSHOT.jar started by juanm in E:\Universidad\Ciencias de la Computacion\4to Año\Semestre B\Ingenieria de Software II\Practica06\SimpleBlogDemo-master\target)
2022-11-25 22:14:19.636 [main] INFO c.b.h.s.SimpleBlogDemoApplication - No active profile set, falling back to default profiles: default
2022-11-25 22:14:21.619 [main] INFO o.s.d.r.c.RepositoryConfigurationDelegate - Bootstrapping Spring Data JPA repositories in DEFAULT mode.
2022-11-25 22:14:21.815 [main] INFO o.s.d.r.c.RepositoryConfigurationDelegate - Finished Spring Data repository scanning in 166ms. Found 2 JPA repository interfaces.
2022-11-25 22:14:22.978 [main] INFO o.s.c.s.PostProcessorRegistrationDelegate$BeanPostProcessorChecker - Bean 'org.springframework.transaction.annotation.ProxyTransactionManagementConfiguration' of type [org.springframework.transaction.annotation.ProxyTransactionManagementConfiguration] is not eligible for getting processed by all BeanPostProcessors (for example: not eligible for auto-proxying)
2022-11-25 22:14:23.818 [main] INFO o.s.b.w.e.tomcat.TomcatWebServer - Tomcat initialized with port(s): 8070 (http)
2022-11-25 22:14:23.854 [main] INFO o.a.coyote.http11.Http11NioProtocol - Initializing ProtocolHandler ["http-nio-8070"]
```

2.3. Desarrollo

1. Configurar Proxies: <https://github.com/zaproxy/zap-core-help/wiki/HelpStartProxies>

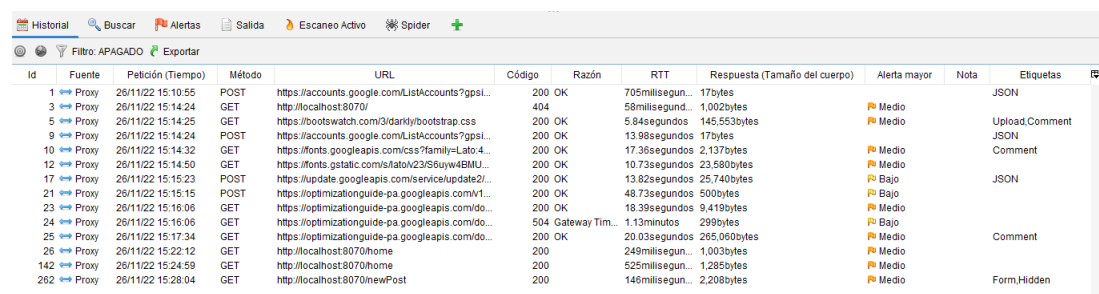


2. Implementar Pruebas de Penetración sobre una aplicación web apropiada con propósito de investigación en seguridad!:
 - a) Implementar los casos de prueba [reglas]
 - b) Ejecutar los casos de prueba [ejecutar ataques]
 - c) Reportar los resultados de la ejecución (Alertas - alarmas)



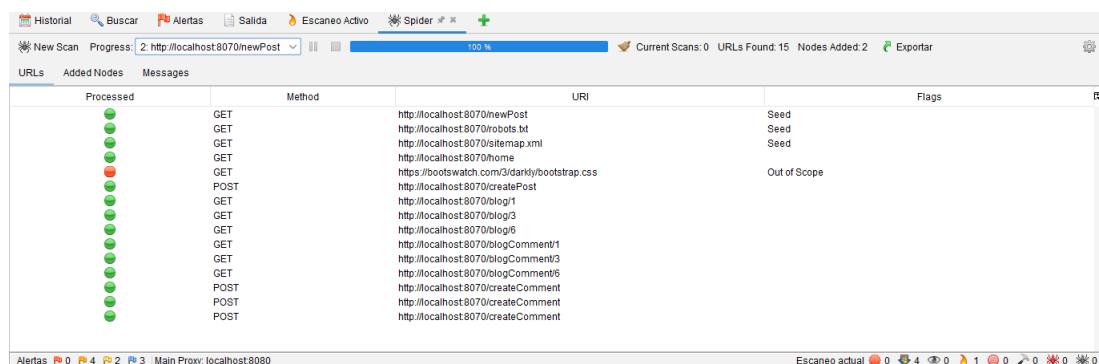
Id	Petición (Tiempo)	Marca de tiempo Respuesta	Método	URL	Código	Razón	RTT	Tamaño de la Cabecera de Respuesta	Respuesta (Tamaño del cuerpo)
348	26/11/22 15:28:19	26/11/22 15:28:19	GET	http://localhost:8070/adminer.php	404		85milisegun...	228bytes	1,002bytes
349	26/11/22 15:28:19	26/11/22 15:28:19	GET	http://localhost:8070/vb_test.php	404		91milisegun...	228bytes	1,002bytes
350	26/11/22 15:28:19	26/11/22 15:28:19	GET	http://localhost:8070/CHANGELOG.txt	404		91milisegun...	228bytes	1,002bytes
351	26/11/22 15:28:19	26/11/22 15:28:19	GET	http://localhost:8070/sites/default/files/ht.sqlite	404		112milisegu...	228bytes	1,002bytes
352	26/11/22 15:28:19	26/11/22 15:28:19	GET	http://localhost:8070/composer.json	404		85milisegun...	228bytes	1,002bytes
353	26/11/22 15:28:19	26/11/22 15:28:19	GET	http://localhost:8070/composer.lock	404		34milisegun...	228bytes	1,002bytes
354	26/11/22 15:28:19	26/11/22 15:28:20	GET	http://localhost:8070/vm_settings.xml	404		152milisegu...	228bytes	1,002bytes
355	26/11/22 15:28:20	26/11/22 15:28:20	GET	http://localhost:8070/server-info	404		103milisegu...	228bytes	1,002bytes
356	26/11/22 15:28:20	26/11/22 15:28:20	GET	http://localhost:8070/phpinfo.php	404		83milisegun...	228bytes	1,002bytes
357	26/11/22 15:28:20	26/11/22 15:28:20	GET	http://localhost:8070/info.php	404		254milisegu...	228bytes	1,002bytes
358	26/11/22 15:28:20	26/11/22 15:28:20	GET	http://localhost:8070/i.php	404		109milisegu...	228bytes	1,002bytes
359	26/11/22 15:28:20	26/11/22 15:28:20	GET	http://localhost:8070/test.php	404		248milisegu...	228bytes	1,002bytes
360	26/11/22 15:28:20	26/11/22 15:28:20	GET	http://localhost:8070/hg	404		89milisegun...	228bytes	1,002bytes
361	26/11/22 15:28:20	26/11/22 15:28:21	GET	http://localhost:8070/bzr	404		144milisegu...	228bytes	1,002bytes
362	26/11/22 15:28:21	26/11/22 15:28:21	GET	http://localhost:8070/_darcs	404		82milisegun...	228bytes	1,002bytes
363	26/11/22 15:28:21	26/11/22 15:28:21	GET	http://localhost:8070/BlkKeeper	404		97milisegun...	228bytes	1,002bytes
364	26/11/22 15:28:21	26/11/22 15:28:21	GET	http://localhost:8070/newPost	200		123milisegu...	139bytes	2,208bytes

Figura 1: Ejecutando Ataques



Id	Fuente	Petición (Tiempo)	Método	URL	Código	Razón	RTT	Respuesta (Tamaño del cuerpo)	Alerta mayor	Nota	Etiquetas
1	Proxy	26/11/22 15:10:55	POST	https://accounts.google.com/ListAccounts?gpsi...	200	OK	705milisegun...	17bytes			JSON
3	Proxy	26/11/22 15:14:24	GET	http://localhost:8070/	404		58milisegund...	1,002bytes	Medio		
5	Proxy	26/11/22 15:14:25	GET	https://bootswatch.com/3/darkly/bootstrap.css	200	OK	5.84segundos	145,553bytes	Medio		Upload,Comment
9	Proxy	26/11/22 15:14:24	POST	https://accounts.google.com/ListAccounts?gpsi...	200	OK	13.98segundos	17bytes			JSON
10	Proxy	26/11/22 15:14:32	GET	https://fonts.googleapis.com/css?family=Lato:4...	200	OK	17.36segundos	2,137bytes	Medio		Comment
12	Proxy	26/11/22 15:14:50	GET	https://fonts.gstatic.com/s/fato/v23/56uyw46MU...	200	OK	10.73segundos	23,580bytes	Medio		
17	Proxy	26/11/22 15:15:23	POST	https://update.googleapis.com/service/update2/...	200	OK	13.82segundos	25,740bytes	Bajo		JSON
21	Proxy	26/11/22 15:15:15	POST	https://optimizationguide-pa.googleapis.com/v1...	200	OK	48.73segundos	500bytes	Bajo		
23	Proxy	26/11/22 15:16:06	GET	https://optimizationguide-pa.googleapis.com/do...	200	OK	18.39segundos	9,419bytes	Medio		
24	Proxy	26/11/22 15:16:06	GET	https://optimizationguide-pa.googleapis.com/do...	504	Gateway Tim...	1.13minutos	299bytes	Bajo		
25	Proxy	26/11/22 15:17:34	GET	https://optimizationguide-pa.googleapis.com/do...	200	OK	20.03segundos	265,060bytes	Medio		Comment
26	Proxy	26/11/22 15:22:12	GET	http://localhost:8070/home	200		249milisegun...	1,003bytes	Medio		
142	Proxy	26/11/22 15:24:59	GET	http://localhost:8070/home	200		525milisegun...	1,285bytes	Medio		
262	Proxy	26/11/22 15:28:04	GET	http://localhost:8070/newPost	200		146milisegun...	2,208bytes	Medio		Form.Hidden

Figura 2: Historial de Ataques



URLs	Added Nodes	Messages
Processed		
●	GET	http://localhost:8070/newPost
●	GET	http://localhost:8070/robots.txt
●	GET	http://localhost:8070/sitemap.xml
●	GET	http://localhost:8070/home
●	GET	https://bootswatch.com/3/darkly/bootstrap.css
●	POST	http://localhost:8070/createPost
●	GET	http://localhost:8070/blog/1
●	GET	http://localhost:8070/blog/3
●	GET	http://localhost:8070/blog/6
●	GET	http://localhost:8070/blogComment/1
●	GET	http://localhost:8070/blogComment/3
●	GET	http://localhost:8070/blogComment/6
●	POST	http://localhost:8070/createComment
●	POST	http://localhost:8070/createComment
●	POST	http://localhost:8070/createComment

Figura 3: Spider del Ataque

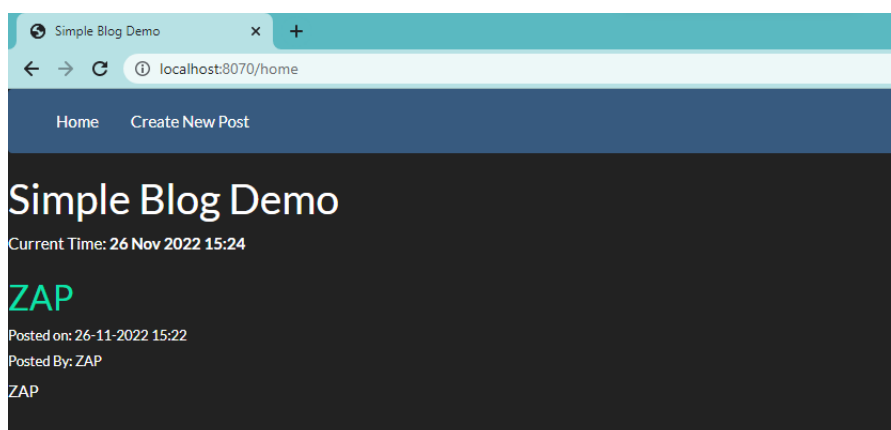


Figura 4: Resultado de los Ataques

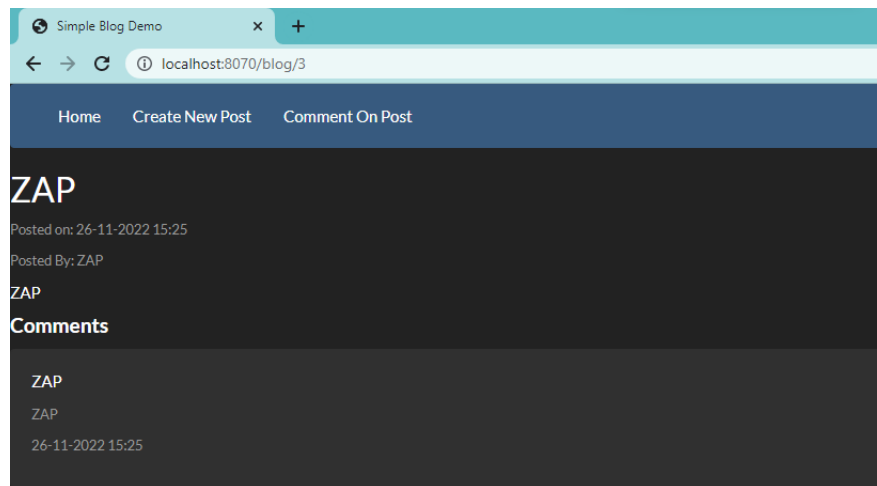


Figura 5: Resultado de los Ataques

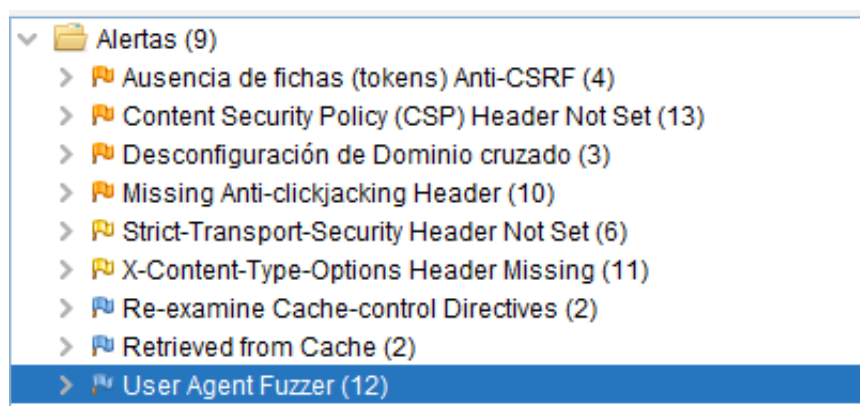


Figura 6: Alarmas , resultado como ejecución del programa


2.3.1. Descripción de las alertas y posibles soluciones

En las siguientes imágenes se observan las alertas producidas después de la ejecución del programa, las cuales son:

2.3.1.1. Alerta 1 Descripción y solución

Ausencia de fichas (tokens) Anti-CSRF

URL: <http://localhost:8070/newPost>

Riesgo:  Medium

Confianza: Low

Parámetro:

Ataque:

Evidencia: `<form autocomplete="off" action="/createPost" method="post" class="form-horizontal" role="form">`

CWE ID: 352

WASC ID: 9

Origen: Pasivo (10202 - Ausencia de fichas (tokens) Anti-CSRF)

Input Vector:

Descripción:

recientes para difundir información al obtener el acceso a la respuesta. El riesgo de divulgación de información aumenta de forma drástica cuando el sitio de destino se encuentra vulnerable a XSS, porque XSS se puede utilizar como una plataforma para CSRF, lo que le permite al atacante que opere desde adentro de los límites de la misma política de origen.

Otra info:

Ninguna ficha (token) Anti-CSRF [anticsrf, CSRFTOKEN, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, __csrf_secret, __csrf_magic, CSRF_token, csrf_token] fue encontrada en los siguientes formularios HTML: [Form 1: "bodyError" "id" "titleError" "usernameError"].

Figura 7: Descripción

Solución:

Frase: Arquitectura y Diseño

Utilice una biblioteca o marco comprobado que no acepte que ocurra esta debilidad o que proporcione construcciones que permitan que esta debilidad sea mas sencilla de evitar.

Referencia:

<http://projects.webappsec.org/Cross-Site-Request-Forgery>

<http://cwe.mitre.org/data/definitions/352.html>

Etiquetas de Alerta:


Clave	Valor
OWASP_2021_A01	https://owasp.org/Top10/A01_2021-Broken_Access_Control/
WSTG-v42-SESS-05	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application...
OWASP_2017_A05	https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html

Figura 8: Soluciones

2.3.1.2. Alerta 2 Descripción y solución

Content Security Policy (CSP) Header Not Set

URL: <http://localhost:8070/>

Riesgo:  Medium

Confianza: High

Parámetro:

Ataque:

Evidencia:

CWE ID: 693

WASC ID: 15

Origen: Pasivo (10038 - Content Security Policy (CSP) Header Not Set)

Input Vector:

Descripción:

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames,

Figura 9: Descripción

Solución:

Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.

Referencia:

https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
<http://www.w3.org/TR/CSP/>

Etiquetas de Alerta:


Clave	Valor
OWASP_2021_A05	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
OWASP_2017_A06	https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.ht...

Figura 10: Soluciones

2.3.1.3. Alerta 3 Descripción y solución

Desconfiguración de Dominio cruzado

URL: <https://bootswatch.com/3/darkly/bootstrap.css>

Riesgo:  Medium

Confianza: Medium

Parámetro:

Ataque:

Evidencia: Access-Control-Allow-Origin: *

CWE ID: 264

WASC ID: 14

Origen: Pasivo (10098 - Desconfiguración de Dominio cruzado)

Input Vector:

Descripción:

Descargas de datos del navegador web podría ser posible, debido a una desconfiguración del intercambio de recursos cruzados de origen (CORS) en el servidor web

Otra info:

La desconfiguración CORS en el servidor web permite a dominios cruzados leer peticiones de dominios de terceros arbitrariamente, usando APIs sin autenticación en este dominio. Las implementaciones de navegador web no permiten a terceros arbitrarios leer la respuesta de APIs autenticados, de todas formas. Esto reduce el riesgo de alguna forma. Esta desconfiguración podría ser usada por un atacante para acceder a datos que está disponible en una manera sin autenticación, pero que

Figura 11: Descripción

Solución:

Asegúrese que los datos sensibles no están disponibles de manera no autenticada (usando dirección IP listado-blanco, por ejemplo). Configurar el encabezado HTTP "Access-Control-Allow-Origin" a un conjunto de dominios más restrictivo, o remover completamente todos los encabezados CORS, para permitir que el navegador web refuerce la política de mismo origen (SOP) en una manera mas restrictiva.

Referencia:

https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Etiquetas de Alerta:


Clave	Valor
OWASP_2021_A01	https://owasp.org/Top10/A01_2021-Broken_Access_Control/
OWASP_2017_A05	https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html

Figura 12: Soluciones

2.3.1.4. Alerta 4 Descripción y solución

Missing Anti-clickjacking Header

URL: https://optimizationguide-pa.googleapis.com/downloads?name=2202180000&target=OPTIMIZATION_TARGET_SEGMENTATION_CHROME_LOW_USER_ENGA

Riesgo:  Medium

Confianza: Medium

Parámetro: X-Frame-Options

Ataque:

Evidencia:

CWE ID: 1021

WASC ID: 15

Origen: Pasivo (10020 - Anti-clickjacking Header)

Input Vector:

Descripción:

The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.

Figura 13: Descripción

Solución:

Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.

Referencia:

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

Etiquetas de Alerta:


Clave	Valor
OWASP_2021_A05	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
WSTG-v42-CLNT-09	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application...
OWASP_2017_A06	https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.ht...

Figura 14: Soluciones

2.3.1.5. Alerta 5 Descripción y solución

Strict-Transport-Security Header Not Set

URL: <https://bootswatch.com/3/darkly/bootstrap.css>

Riesgo:  Low

Confianza: High

Parámetro:

Ataque:

Evidencia:

CWE ID: 319

WASC ID: 15

Origen: Pasivo (10035 - Strict-Transport-Security Header)

Input Vector:

Descripción:

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

Figura 15: Descripción

Solución:

Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Referencia:

https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

<https://owasp.org/www-community/Security-Headers>

http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security

Etiquetas de Alerta:

Clave	Valor
OWASP_2021_A05	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
OWASP_2017_A06	https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.ht...

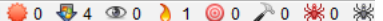

Escaneo actual 

Figura 16: Soluciones

2.3.1.6. Alerta 6 Descripción y solución

X-Content-Type-Options Header Missing

URL: <https://bootswatch.com/3/darkly/bootstrap.css>

Riesgo:  Low

Confianza: Medium

Parámetro: X-Content-Type-Options

Ataque:

Evidencia:

CWE ID: 693

WASC ID: 15

Origen: Pasivo (10021 - X-Content-Type-Options Header Missing)

Input Vector:

Descripción:

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

Otra info:

This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scan rule will not alert on client or server error responses.

Figura 17: Descripción

Solución:

Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

Referencia:

<http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx>
<https://owasp.org/www-community/Security-Headers>

Etiquetas de Alerta:


Clave	Valor
OWASP_2021_A05	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
OWASP_2017_A06	https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.ht...

Figura 18: Soluciones

2.3.1.7. Alerta 7 Descripción y solución

Re-examine Cache-control Directives

URL: https://optimizationguide-pa.googleapis.com/downloads?name=2202180000&target=OPTIMIZATION_TARGET_SEGMENTATION_CHROME_LOW_USER_ENGAGEMENT

Riesgo:  Informational

Confianza: Low

Parámetro: Cache-Control

Ataque:

Evidencia: public, max-age=86400

CWE ID: 525

WASC ID: 13

Origen: Pasivo (10015 - Re-examine Cache-control Directives)

Input Vector:

Descripción:

The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

Figura 19: Descripción

Solución:

For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".

Referencia:

https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control>
<https://grayduck.mn/2021/09/13/cache-control-recommendations/>

Etiquetas de Alerta:

Clave	Valor
WSTG-v42-ATHN-06	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application...

Figura 20: Soluciones

2.3.1.8. Alerta 8 Descripción y solución


Retrieved from Cache
 URL: <https://bootswatch.com/3/darkly/bootstrap.css>
 Riesgo:  Informational
 Confianza: Medium
 Parámetro:
 Ataque:
 Evidencia: Age: 74
 CWE ID:
 WASC ID:
 Origen: Pasivo (10050 - Retrieved from Cache)
 Input Vector:
Descripción:
 The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in
Otra info:
 The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.

Figura 21: Descripción

Solución:
 Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user:
 Cache-Control: no-cache, no-store, must-revalidate, private

Referencia:
<https://tools.ietf.org/html/rfc7234>
<https://tools.ietf.org/html/rfc7231>
<http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html> (obsoleted by rfc7234)

Etiquetas de Alerta:


Clave	Valor
WSTG-v42-ATHN-06	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application...

Figura 22: Soluciones

2.3.1.9. Alerta 9 Descripción y solución

User Agent Fuzzer

URL: http://localhost:8070/home

Riesgo:  Informational

Confianza: Medium

Parámetro: Header User-Agent

Ataque: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)

Evidencia:

CWE ID: 0

WASC ID: 0

Origen: Activo (10104 - User Agent Fuzzer)

Input Vector:

Descripción:

Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

Figura 23: Descripción