



REPORTE DE INFORMES

VULNERABILIDADES

GISELLE MATA

MARIANO FURLONG

BRYAN HERRERA

1. RESUMEN

Se encontraron vulnerabilidades usando las técnicas de Cross-Site Scripting y SQL injection en las siguientes páginas Web:

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

Se logró acceder al login en ambas páginas con los siguientes comandos SQL

```
SELECT firstname FROM users where username='admin'--' and password='admin'

SELECT firstname FROM users where username='admin'--'

' OR '1'='1'
```

login user info

No es seguro | testaspnet.vulnweb.com/login.aspx

acunetix acublog Test Website for Acunetix Web Vulnerability Scanner

about news login signup network scanner network vuln help RSS

Username: admin--

Password:

☒ Remember me

Login

Get RSS feed

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.

Browser address bar: No es seguro | testaspnet.vulnweb.com/Default.aspx

 **acublog**

Test Website for **Acunetix Web Vulnerability Scanner**

[about](#) [news](#) [logout admin](#) [post news](#) [network scanner](#) [network vuln help](#) [RSS](#)

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

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/>.

[Get RSS feed](#)

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.

<

August 2023


>

Sun	Mon	Tue	Wed	Thu	Fri	Sat
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	31	1	2
3	4	5	6	7	8	9

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.

Browser tabs: Bienvenido, Aviso de priv, FoxyProxy, FoxyProxy, GitHub - fo, ¿Cómo hac, user info, Advertencia, acublog news

Browser address bar: testphp.vulnweb.com/userinfo.php

 **acuart**

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](#)

John Smith (test)

On this page you can visualize or edit you user information.

Name:

Credit card number:

E-Mail:

Phone number:

Address:

update

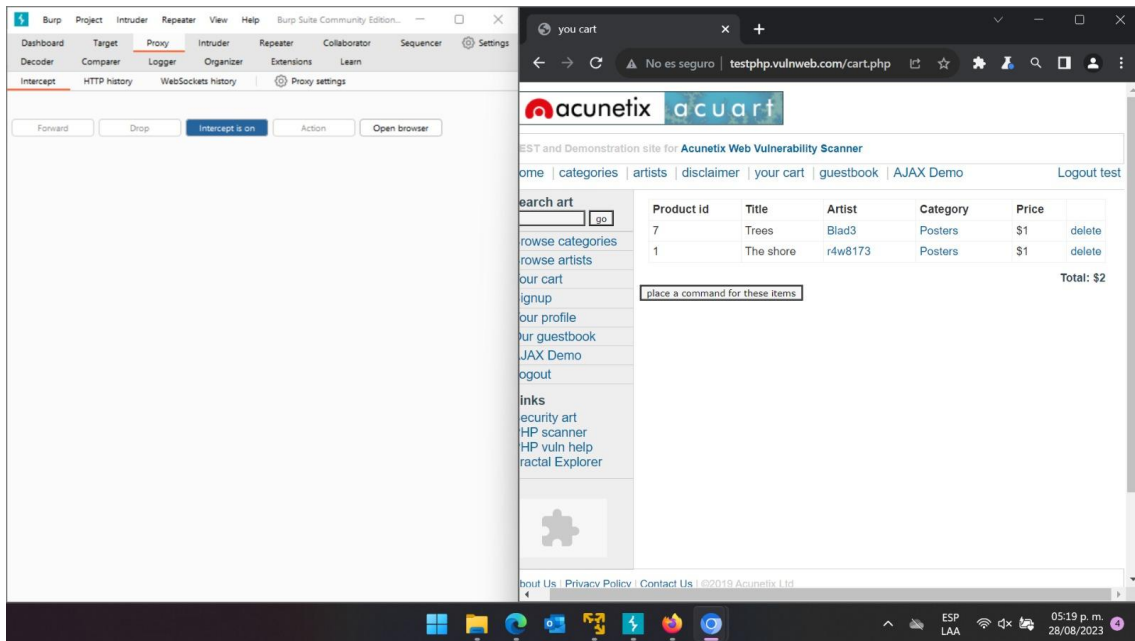
You have 0 items in your cart. You visualize you cart [here](#).

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

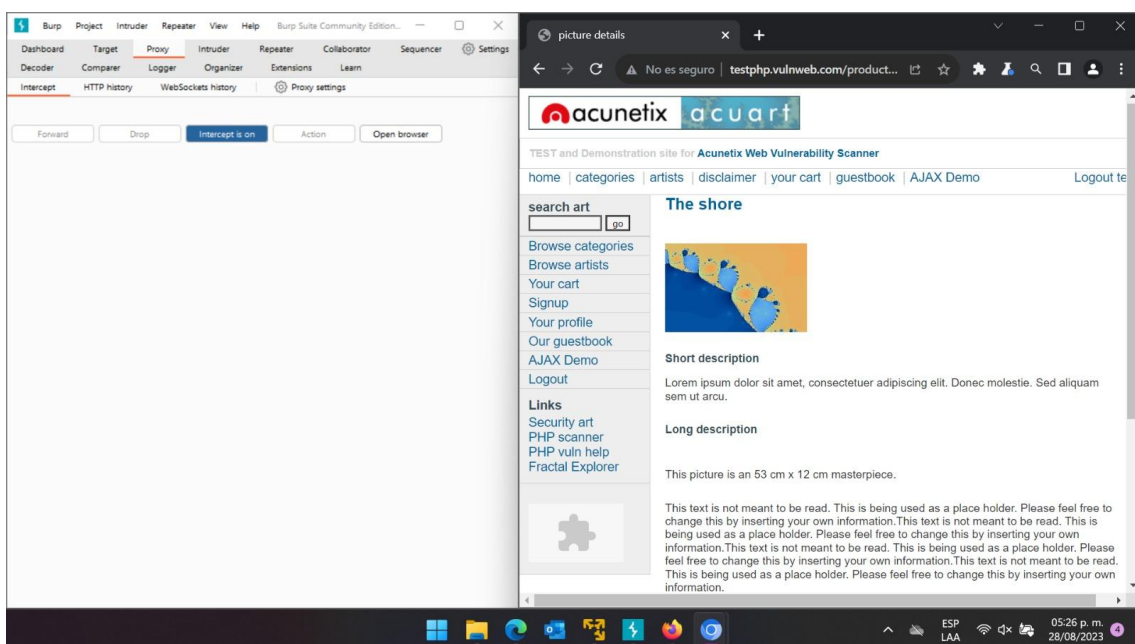
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developers expose web-based configuration errors.

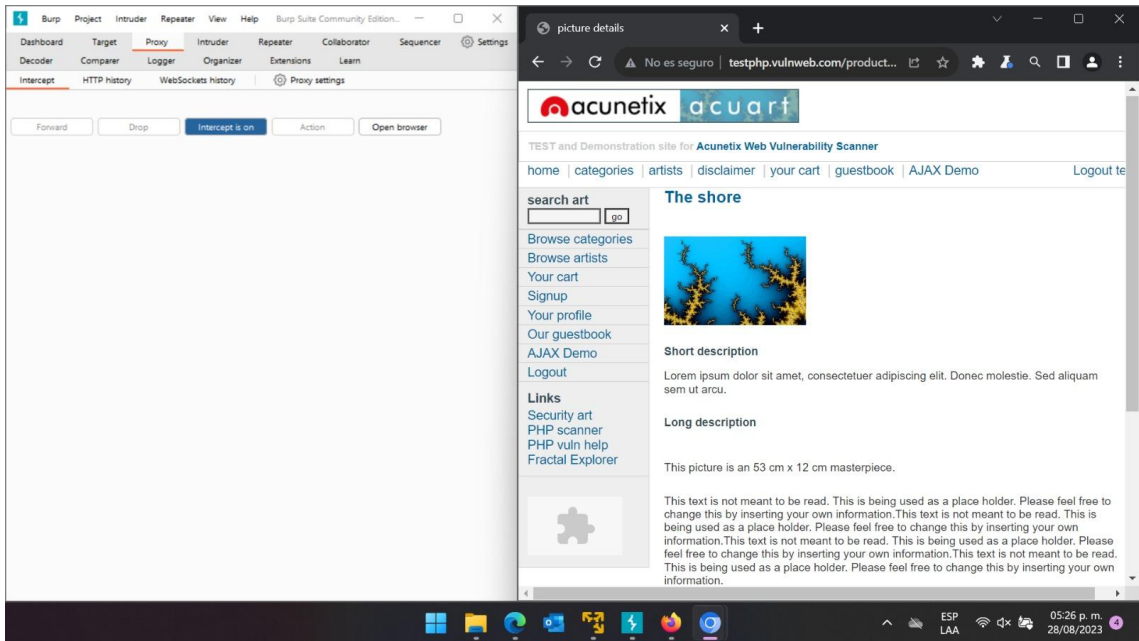
Windows taskbar: 04:33 p.m. 28/08/2023

Se logró cambiar de precio los productos con burp suite y poder ajustar el precio al valor deseado



También se pudo acceder cambiar las imágenes del sitio web en los productos deseados





Se logró acceder a sus directorios y credenciales del sitio web

