

HTML Injection

Description:

This server is vulnerable to HTML injection which occurs when an attacker is able to control an input point and is able to inject arbitrary HTML code into a vulnerable web page using metacharacters. This may lead to consequences like disclosure of a user's session cookies or it can allow the attacker to modify the page content seen by the victims.

Solution

Properly validate meta-characters from user's inputs.

Occurrence:

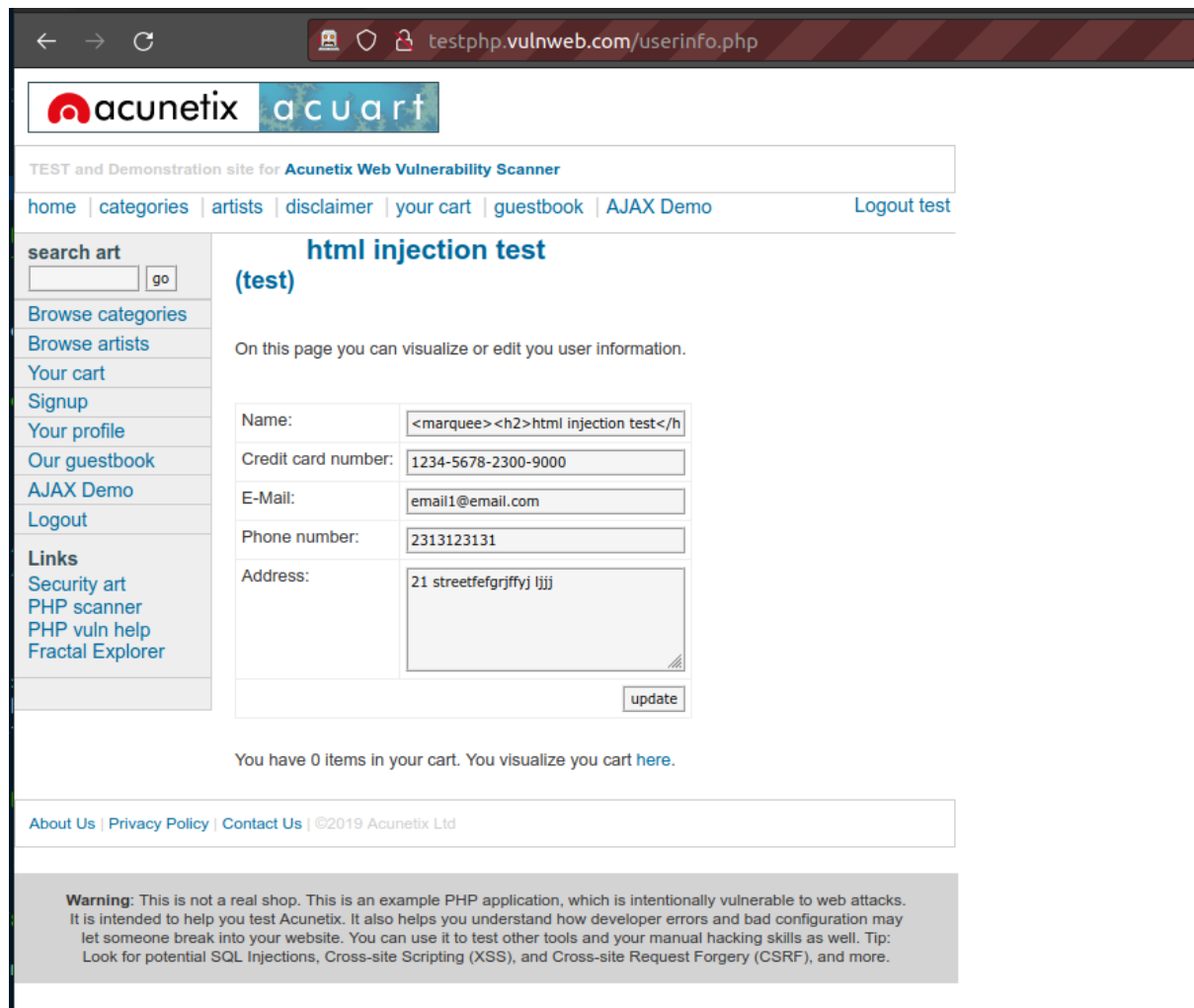
Occurrence: 1

URL: <http://testphp.vulnweb.com/userinfo.php>

Parameter: uname

Payload: `<marquee><h2>html injection test</h2></marquee>`

Images:



Header: Text

Body: Text

POST http://testphp.vulnweb.com/userinfo.php HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,
image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 191
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Referer: http://testphp.vulnweb.com/userinfo.php
Cookie: login=test%2Ftest
Upgrade-Insecure-Requests: 1
Host: testphp.vulnweb.com

username=%3Cmarquee%3E%3Ch2%3Ehtml+injection+
test%3C%2Fh2%3E%3C%2Fmarquee%3E&ucc=1234-5678-2300-9000&uemail=
email1%40email.com&uphone=2313123131&uaddress=21+streetfefgrjffj+
ljjj&update=update

Header: Text

Body: Text

HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Wed, 13 Jul 2022 10:18:28 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional
a//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<!-- InstanceBegin template="/Templates/main_dynamic_te
mplate.dwt.php" codeOutsideHTMIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content=
"text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" --
>
<title>user info</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css"
>
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->

Occurrence: 2

URL: http://testphp.vulnweb.com/search.php?test=query

Parameter: searchFor

Payload: <marquee><h2>html injection test</h2></marquee>

Images:

← → ↺

testphp.vulnweb.com/search.php?test=query

acunetix

acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

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

search art

go

searched for:

html injection test

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo

Logout

Links

Security art

PHP scanner

PHP vuln help

Fractal Explorer

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 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.

Header: Text

Body: Text

POST http://testphp.vulnweb.com/search.php?test=query HTTP/1.1

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Content-Type: application/x-www-form-urlencoded

Content-Length: 89

Origin: http://testphp.vulnweb.com

Connection: keep-alive

Referer: http://testphp.vulnweb.com/userinfo.php

Cookie: login=test%2Ftest

Upgrade-Insecure-Requests: 1

Host: testphp.vulnweb.com

searchFor=%3Cmarquee%3E%3Ch2%3Ehtml+injection+test%3C%2Fh2%3E%3C%2Fmarquee%3E%3CgoButton=go

Header: Text

Body: Text

HTTP/1.1 200 OK

Server: nginx/1.19.0

Date: Wed, 13 Jul 2022 10:28:11 GMT

Content-Type: text/html; charset=UTF-8

Connection: keep-alive

X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional/EN"

"http://www.w3.org/TR/html4/loose.dtd">

<html>

<!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMlIsLocked="false" -->

<head>

<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->

<title>search</title>

<!-- InstanceEndEditable -->

<link rel="stylesheet" href="style.css" type="text/css">

<!-- InstanceBeginEditable name="headers_rgn" -->

<!-- here goes headers headers -->