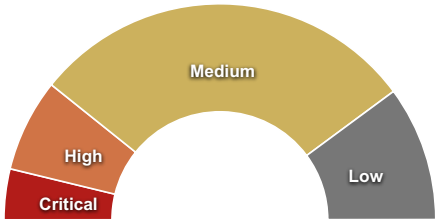
Executive Summary

Your application is at **high risk** of being compromised due to the vulnerabilities found by this scan. You should take immediate action to remediate these issues.

Results by severity level

Critical	6
High	11
Medium	46
Low	16



Server Information

Server Responsive	**Yes**
Server Banner	**Apache/2.2.22 (Ubuntu)**
Server OS	**Linux**
Server Technologies	**Apache**

Table of Contents

Critical

1. Blind SQL Injection (2 instances)
2. OS Command Injection (1 instance)
3. SQL Injection (3 instances)

High

4. Blind OS Command Injection (1 instance)
5. Directory Traversal (2 instances)
6. Known Vulnerable Web Server (1 instance)
7. Reflected Cross-Site Scripting (6 instances)
8. Unvalidated Redirect (1 instance)

Medium

9. Blacklisted Domain (1 instance)
10. Clickjacking: Missing X-Frame-Options Header (1 instance)
11. Directory Indexing (3 instances)
12. FrontPage Server Extensions Found (1 instance)
13. HTML Injection (7 instances)
14. HTTP Header Injection (2 instances)
15. HTTP OPTIONS Method Enabled (1 instance)
16. Insecure Login Page (1 instance)
17. Malicious File Upload (1 instance)
18. Password is Sent Unencrypted (2 instances)
19. Remote File Inclusion (3 instances)
20. Sensitive File Found (10 instances)
21. Server Error on Page (4 instances)
22. Server-Side Source Code Found (4 instances)
23. Social Security Number Found (2 instances)
24. Vulnerable Flash Cross-Domain Policy (1 instance)
25. Vulnerable Silverlight Cross-Domain Policy (1 instance)
26. Weak SSL Cipher (1 instance)

Low

27. Autocomplete Enabled on Password Field (2 instances)
28. Credit Card Found (1 instance)
29. Email Address Found (1 instance)
30. HTML Form Without CSRF Protection (3 instances)
31. Insufficient Session Expiration (1 instance)
32. Open TCP/UDP Port Found (2 instances)
33. Outdated Version of Web Server (1 instance)
34. Session Cookie Does Not Have HttpOnly Flag Set (1 instance)
35. Session Fixation (1 instance)
36. SSL Certificate Is Untrusted (1 instance)
37. SSL Certificate Ownership Is Invalid (1 instance)
38. Uncommon HTTP Method Enabled (1 instance)

Crawler

39. Crawler Database (95 instances)

1.Blind SQL Injection

CVSS

Score: 6.8
Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/sqli_showcity.php	Critical	Likely	New

The field `cityid` was submitted with the value `2806 and sleep(10)`. The response times seen were 10.14 and 10.09. The field was then submitted with the value `2806 and sleep(4)`. The response times seen were 4.08 and 4.08. The difference between these times suggests that the server is executing the injected SQL statement.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/sqli_blind_form_1.php	Critical	Likely	New

The field `search` was submitted with the value `Kabul' and sleep(10)='`. The response times seen were 10.07 and 10.01. The field was then submitted with the value `Kabul' and sleep(4)='`. The response times seen were 4.01 and 4.01. The difference between these times suggests that the server is executing the injected SQL statement.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

2.OS Command Injection

CVSS

Score: 7.5
Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/os_injection_1.php	Critical	Certain	Manual

The field `cmd` was submitted with the value `/bin/cat /etc/passwd`. The marker `root:x:0:0:root:/root:/bin/bash [1] => daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin [2] => bin:x:2:2:bin:/bin:/usr/sbin/nologin [3] => sys:x:3:3:sys:/dev:/usr/sbin/nologin [4] => sync:x:4:65534:sync:/bin:/bin/sync [5] => games:x:5:60:games:/usr/games:/usr/sbin/nologin [6] => man:x:6:12:man:/var/cache/man:/usr/sbin/nologin [7] => lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin [8] => mail:x:8:8:mail:/var/mail:/usr/sbin/nologin [9] => news:x:9:9:news:/var/spool/news:/usr/sbin/nologin [10] => uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin [11] => proxy:x:13:13:proxy:/bin:/usr/sbin/nologin [12] => www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin [13] => backup:x:34:34:backup:/var/backups:/usr/sbin/nologin [14] => list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin [15] => irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin [16] => gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin [17] => nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin [18] => libuuid:x:100:101::/var/lib/libuuid: [19] => syslog:x:101:104::/home/syslog:/bin/false [20] => messagebus:x:102:106::/var/run/dbus:/bin/false [21] => landscape:x:103:109::/var/lib/landscape:/bin/false [22] => sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin [23] => dave:x:1000:1000:dave,,,:/home/dave:/bin/bash [24] => mysql:x:105:113:MySQL Server,,,:/nonexistent:/bin/false [25] => snmp:x:106:114::/var/lib/snmp:/bin/false [26] => proftpd:x:107:65534::/var/run/proftpd:/bin/false [27] => ftp:x:108:65534::/srv/ftp:/bin/false [28] => colord:x:109:116:colord colour management daemon,,,:/var/lib/colord:/bin/false) </pre> <!-- FOOTER --> <div style="background:#eee; border:1px solid #666; bottom:0; height:60px; left:0; position:fixed; width:100%;"> <div style="line-height:60px; margin:0 auto; width:100%; text-align:center;"> Footer: Generated at 28/09/2016 11:54:00` was found in the response, suggesting that the injected command was executed, and therefore that OS command injection is possible.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

3.SQL Injection

CVSS

Score: 6.8
Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/sqli_form_1.php	Critical	Likely	New

The field `region` was submitted with the value `1'"`. The string `You have an error in your SQL syntax;` was found in the response, which is similar to errors typically shown by the mysql database system. This suggests that the `region` field is vulnerable to SQL injection.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/sqli/sqli_with_errors.php	Critical	Likely	New

The field `search` was submitted with the value `1'"`. The string `You have an error in your SQL syntax;` was found in the response, which is similar to errors typically shown by the mysql database system. This suggests that the `search` field is vulnerable to SQL injection.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/members/profile.php	Critical	Likely	New

The field `about` was submitted with the value `1'"`. The string `You have an error in your SQL syntax;` was found in the response, which is similar to errors typically shown by the mysql database system. This suggests that the `about` field is vulnerable to SQL injection.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Not found
2016-09-23	Test Scan	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Not found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

4.Blind OS Command Injection

CVSS

Score: 7.5
Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/os_injection_2.php	High	Likely	New

The field `filename` was submitted with the value `& sleep 10 &`. The response times seen were 10.07 and 10.01. The field was then submitted with the value `& sleep 4 &`. The response times seen were 4.01 and 4.01. The difference between these times suggests that the injected command was executed, and therefore that OS command injection is possible.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

5.Directory Traversal

CVSS

Score: 6.8
Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/dirtrav.php	High	Certain	New

The `fname` parameter was submitted with the value `../../../../../../etc/passwd`, and the response contained the value `root:x:0:0:`.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/members/file_show.php	High	Certain	New

The `fname` parameter was submitted with the value `/etc/passwd`, and the response contained the value `root:x:0:0:`.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Not found
2016-09-23	Test Scan	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Not found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

6.Known Vulnerable Web Server

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/	High	Possible	New

The following webserver vulnerabilities were detected (Highest severity found: High)

- **Apache2 mod_proxy_balancer CSRF, XSS, Memory Corruption and DoS Vulnerability**
  - Details: Apache2 mod_proxy_balancer CSRF, XSS, Memory Corruption and DoS Vulnerability
  - CVE: CVE-2007-6423
- **Apache envvars privilege escalation**
  - Details: envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.
  - CVE: CVE-2012-0883
- **Apache mod_status race condition denial of service/code execution**

- Details: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_workerfunction in modules/lua/lua_request.c.
- CVE: CVE-2014-0226

- **Apache mod_rewrite remote command execution**
  - Details: mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.
  - CVE: CVE-2013-1862
- **Apache lua_websocket_read denial of service**
  - Details: The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.
  - CVE: CVE-2015-0228
- **Apache mod_cgid denial of service**
  - Details: The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.
  - CVE: CVE-2014-0231
- **Apache mod_log_config denial-of-service**
  - Details: The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.
  - CVE: CVE-2014-0098
- **Apache mod_dav denial of service**
  - Details: The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.
  - CVE: CVE-2013-6438
- **Apache mod_headers RequestHeader bypass**
  - Details: The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass "RequestHeader unset" directives by placing a header in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states "this is not a security issue in httpd as such."
  - CVE: CVE-2013-5704

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

7.Reflected Cross-Site Scripting

CVSS

Score: 4.3
Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/xss_form_get.php	High	Certain	New

The `q` parameter was submitted with the value `"--><script>prompt(12345)</script>KrMNG<!--`, and the string was echoed verbatim in the output, showing that there is a reflected XSS vulnerability.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/xss_parsing_test.php	High	Certain	New

The `url` parameter was submitted with the value `"--><script>prompt(12345)</script>fZ5iu<!--`, and the string was echoed verbatim in the output, showing that there is a reflected XSS vulnerability.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/page_header_inject.php	High	Certain	New

The `fname` parameter was submitted with the value `"--><script>prompt(12345)</script>kmlvo<!--`, and the string was echoed verbatim in the output, showing that there is a reflected XSS vulnerability.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/page_header_inject.php	High	Certain	New

The `lname` parameter was submitted with the value `"--><script>prompt(12345)</script>WkpQ7<!--`, and the string was echoed verbatim in the output, showing that there is a reflected XSS vulnerability.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/xss_form_post.php	High	Certain	New

The `search` parameter was submitted with the value `"--><script>prompt(12345)</script>T17Gq<!--`, and the string was echoed verbatim in the output, showing that there is a reflected XSS vulnerability.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/rfi.php	High	Certain	New

The `color` parameter was submitted with the value `"--><script>prompt(12345)</script>B5knH<!--`, and the string was echoed verbatim in the output, showing that there is a reflected XSS vulnerability.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

8.Unvalidated Redirect

CVSS

Score: 6.4
Vector: AV:N/AC:L/Au:N/C:P/I:P/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/redirect_unvalidated_form_1.php?url=http://badstorevm1.bvs.scl.cudaops.com	High	Possible	New

The query parameter `url` was set to an arbitrary URL, and the client browser was redirected to that URL.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

9.Blacklisted Domain

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/	Medium	Possible	New

The following domains were associated with malicious or questionable activity by Barracuda Threat Intelligence:

- **Pornography:** www.sex.com, www.porn.com
- **Gambling:** wwww.poker.com, wwww.888.com

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

10.Clickjacking: Missing X-Frame-Options Header

CVSS

Score: 6.8
Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/	Medium	Certain	New

The server did not return the X-Frame-Options header.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

11.Directory Indexing

CVSS

Score: 5.0
Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
https://test.blorpazort.com/pages/	Medium	Likely	New

A request to the server yielded the following pattern, which suggests a directory index page: `<a href="\?C=[NMSD];O=[AD]">Name</a>`.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/sqli/	Medium	Likely	New

A request to the server yielded the following pattern, which suggests a directory index page: `<a href="\?C=[NMSD];O=[AD]">Name</a>`.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/	Medium	Likely	New

A request to the server yielded the following pattern, which suggests a directory index page: `<a href="\?C=[NMSD];O=[AD]">Name</a>`.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

12.FrontPage Server Extensions Found

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/_vti_inf.html	Medium	Certain	New

The *_vti_inf.html* file exists on the site, and contains strings known to be associated with FrontPage server extensions.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

13.HTML Injection

CVSS

Score: 5.0
Vector: AV:N/AC:L/Au:N/C:N/I:P/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/xss_form_get.php	Medium	Certain	New

The `q` parameter was submitted with the value `<h1>buttt</h1>`, and this value was echoed back verbatim in the resulting page.

Note: Due to the non-invasive way Vulnerability Manager tests for HTML Injection vulnerabilities, this vulnerability may be reported even if you have a Web Application Firewall protecting the application. If you are using a Barracuda Web Application Firewall, you can disregard this vulnerability. If you are using a different Web Application Firewall, you should manually check to ensure that your protection is adequate for this vulnerability.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/xss_parsing_test.php	Medium	Certain	New

The `url` parameter was submitted with the value `<h1>xadl8</h1>`, and this value was echoed back verbatim in the resulting page.

Note: Due to the non-invasive way Vulnerability Manager tests for HTML Injection vulnerabilities, this vulnerability may be reported even if you have a Web Application Firewall protecting the application. If you are using a Barracuda Web Application Firewall, you can disregard this vulnerability. If you are using a different Web Application Firewall, you should manually check to ensure that your protection is adequate for this vulnerability.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/page_header_inject.php	Medium	Certain	New

The `fname` parameter was submitted with the value `<h1>74ukg</h1>`, and this value was echoed back verbatim in the resulting page.

Note: Due to the non-invasive way Vulnerability Manager tests for HTML Injection vulnerabilities, this vulnerability may be reported even if you have a Web Application Firewall protecting the application. If you are using a Barracuda Web Application Firewall, you can disregard this vulnerability. If you are using a different Web Application Firewall, you should manually check to ensure that your protection is adequate for this vulnerability.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/page_header_inject.php	Medium	Certain	New

The `lname` parameter was submitted with the value `<h1>olxna</h1>`, and this value was echoed back verbatim in the resulting page.

Note: Due to the non-invasive way Vulnerability Manager tests for HTML Injection vulnerabilities, this vulnerability may be reported even if you have a Web Application Firewall protecting the application. If you are using a Barracuda Web Application Firewall, you can disregard this vulnerability. If you are using a different Web Application Firewall, you should manually check to ensure that your protection is adequate for this vulnerability.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/xss_form_post.php	Medium	Certain	New

The `search` parameter was submitted with the value `<h1>zcujx</h1>`, and this value was echoed back verbatim in the resulting page.

Note: Due to the non-invasive way Vulnerability Manager tests for HTML Injection vulnerabilities, this vulnerability may be reported even if you have a Web Application Firewall protecting the application. If you are using a Barracuda Web Application Firewall, you can disregard this vulnerability. If you are using a different Web Application Firewall, you should manually check to ensure that your protection is adequate for this vulnerability.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/rfi.php	Medium	Certain	New

The `color` parameter was submitted with the value `<h1>h1zi2</h1>`, and this value was echoed back verbatim in the resulting page.

Note: Due to the non-invasive way Vulnerability Manager tests for HTML Injection vulnerabilities, this vulnerability may be reported even if you have a Web Application Firewall protecting the application. If you are using a Barracuda Web Application Firewall, you can disregard this vulnerability. If you are using a different Web Application Firewall, you should manually check to ensure that your protection is adequate for this vulnerability.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/members/profile.php	Medium	Certain	New

The `about` parameter was submitted with the value `<h1>c6rti</h1>`, and this value was echoed back verbatim in the resulting page.

Note: Due to the non-invasive way Vulnerability Manager tests for HTML Injection vulnerabilities, this vulnerability may be reported even if you have a Web Application Firewall protecting the application. If you are using a Barracuda Web Application Firewall, you can disregard this vulnerability. If you are using a different Web Application Firewall, you should manually check to ensure that your protection is adequate for this vulnerability.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Not found
2016-09-23	Test Scan	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Not found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

14.HTTP Header Injection

CVSS

Score: 5.0
Vector: AV:N/AC:L/Au:N/C:N/I:P/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/cgi-bin/header_inj.cgi	Medium	Certain	New

The `userdata` parameter was submitted with the value `ValueOne\nInjected-Header:ValueTwo`, and the resulting page had the `Injected-Header` header set.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Not found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Not found

Path	Severity	Confidence	Status
http://test.blorpazort.com/cgi-bin/header_inj_csrf_ssn.cgi	Medium	Certain	New

The `userdata` parameter was submitted with the value `ValueOne\nInjected-Header:ValueTwo`, and the resulting page had the `Injected-Header` header set.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Not found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Not found

15.HTTP OPTIONS Method Enabled

CVSS

Score: 5.0
Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/	Medium	Certain	New

A request to the site using the OPTIONS method returned successfully, but did not report any allowed HTTP methods. This typically means the server is treating the OPTIONS request like a GET request, and indicates a misconfiguration. Under certain circumstances, this misconfiguration could allow attackers to bypass path access restrictions, so it is recommended to disable the OPTIONS method.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

16.Insecure Login Page

CVSS

Score: 5.0
Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/members/login.php	Medium	Certain	New

The login form's action is a URL with an 'http' scheme, meaning form values will be submitted unencrypted.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Not found
2016-09-23	Test Scan	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Not found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

17.Malicious File Upload

CVSS

Score: 7.5
Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/upload.php	Medium	Possible	New

The `uploadedfile` file upload field was populated with the EICAR Test Virus. The server accepted the file and did not return any errors that the scanner detected.

Note: it is possible that the server is performing virus scanning but does not show the result of the scan to the user in any way. This vulnerability should be validated manually.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

18.Password is Sent Unencrypted

CVSS

Score: 5.0
Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/register.php	Medium	Certain	New

Form name: `registerform`
Form method: `POST`
Form action: *http://test.blorpazort.com/register.php*
Input name: `pass1`
Input type: `password`

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/	Medium	Certain	New

Form method: `POST`
Form action: *http://test.blorpazort.com/members/login.php*
Input name: `password`
Input type: `password`

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

19.Remote File Inclusion

CVSS

Score: 7.5
Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/rfi.php	Medium	Certain	New

The field `color` was submitted with the value `http://s3.amazonaws.com/hashedfiles/f.txt`. The contents of the remote URL, `<Response [200]>`, were included in the response, showing that the remote file was successfully included..

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/dirtrav.php	Medium	Certain	New

The field `fname` was submitted with the value `http://s3.amazonaws.com/hashedfiles/f.txt`. The contents of the remote URL, `<Response [200]>`, were included in the response, showing that the remote file was successfully included..

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/members/file_show.php	Medium	Certain	New

The field `fname` was submitted with the value `http://s3.amazonaws.com/hashedfiles/f.txt`. The contents of the remote URL, `<Response [200]>`, were included in the response, showing that the remote file was successfully included..

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Not found
2016-09-23	Test Scan	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Not found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

20.Sensitive File Found

CVSS

Score: 5.0
Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
https://test.blorpazort.com/pages/phpinfo.php	Medium	Likely	New

File *https://test.blorpazort.com/pages/phpinfo.php* may contain sensitive information.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
https://test.blorpazort.com/pages/backup/	Medium	Likely	New

Directory *https://test.blorpazort.com/pages/backup/* may exist and contain sensitive information.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/mail/	Medium	Likely	New

Directory *http://test.blorpazort.com/mail/* may exist and contain sensitive information.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/web.config	Medium	Likely	New

File *http://test.blorpazort.com/web.config* may contain sensitive information.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/members/members.zip	Medium	Likely	New

File *http://test.blorpazort.com/members/members.zip* may contain sensitive information.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/phpinfo.php	Medium	Likely	New

File *http://test.blorpazort.com/pages/phpinfo.php* may contain sensitive information.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/backup/	Medium	Likely	New

Directory *http://test.blorpazort.com/pages/backup/* may exist and contain sensitive information.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/frames.tar.gz	Medium	Likely	New

File *http://test.blorpazort.com/frames.tar.gz* may contain sensitive information.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/.idea/	Medium	Likely	New

Directory *http://test.blorpazort.com/pages/.idea/* may exist and contain sensitive information.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
https://test.blorpazort.com/pages/.idea/	Medium	Likely	New

Directory *https://test.blorpazort.com/pages/.idea/* may exist and contain sensitive information.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

21.Server Error on Page

CVSS

Score: 5.0
Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/error_page_2.php	Medium	Certain	New

The following error message was returned by the server: `Fatal error: Cannot divide 3946196 by zero in /opt/StashProjects/vulnerability_scanner_ci/testplatform/www/pages/error_page_2.php on line` . This is an error message associated with PHP code.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/error_page_1.php	Medium	Certain	New

The following error message was returned by the server: `Notice: Use of undefined constant adjfkj - assumed 'adjfkj' in /opt/StashProjects/vulnerability_scanner_ci/testplatform/www/pages/error_page_1.php on line` . This is an error message associated with PHP code.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/frames/db_error.php	Medium	Certain	New

The following error message was returned by the server: `Warning: mysql_connect(): Access denied for user 'root'@'localhost' (using password: YES) in /opt/StashProjects/vulnerability_scanner_ci/testplatform/www/frames/db_error.php on line` . This is an error message associated with PHP code.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/frames/php_error.php	Medium	Certain	New

The following error message was returned by the server: `Notice: Undefined variable: dave_test_parameter in /opt/StashProjects/vulnerability_scanner_ci/testplatform/www/frames/php_error.php on line` . This is an error message associated with PHP code.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

22.Server-Side Source Code Found

CVSS

Score: 5.0
Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/cgi-bin/header_inj.cgi	Medium	Possible	New

PHP code was detected in content: `<?php include("../tsfooter.php"); ?>`.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Not found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Not found

Path	Severity	Confidence	Status
http://test.blorpazort.com/cgi-bin/header_inj_csrf_ssn.cgi	Medium	Possible	New

PHP code was detected in content: `<?php include("../tsfooter.php"); ?>`.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Not found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Not found

Path	Severity	Confidence	Status
http://test.blorpazort.com/cgi-bin/header_inj_csrf_ssn.cgi?hdn1=abc&hdn2=def&userdata=11	Medium	Possible	New

PHP code was detected in content: `<?php include("../tsfooter.php"); ?>`.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Not found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Not found

Path	Severity	Confidence	Status
http://test.blorpazort.com/cgi-bin/header_inj.cgi?userdata=11	Medium	Possible	New

PHP code was detected in content: `<?php include("../tsfooter.php"); ?>`.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Not found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Not found

23.Social Security Number Found

CVSS

Score: 5.0
Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/frames/deeptree/start_31.php	Medium	Possible	New

- `078-05-1120`
- `532-14-6066`

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Not found
2016-09-23	Test Scan	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Not found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/rfi.php?color=red	Medium	Possible	New

- `078-05-1120`

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

24.Vulnerable Flash Cross-Domain Policy

CVSS

Score: 5.0
Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/crossdomain.xml	Medium	Certain	New

The file at *http://test.blorpazort.com/crossdomain.xml* contains `allow-access-from domain=*`.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

25.Vulnerable Silverlight Cross-Domain Policy

CVSS

Score: 5.0
Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/clientaccesspolicy.xml	Medium	Certain	New

The file at *http://test.blorpazort.com/clientaccesspolicy.xml* contains `domain uri=*`.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

26.Weak SSL Cipher

CVSS

Score: 5.0
Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com	Medium	Certain	New

The following weak SSL ciphers were detected:

- **('TLS_ECDHE_RSA_WITH_RC4_128_SHA', 'SSLv3, TLSv1.0', '128')**:
  - Uses the RC4 cipher, which is insecure and vulnerable to various attacks as described in CVE-2013-2566
- **('TLS_RSA_WITH_RC4_128_SHA', 'SSLv3, TLSv1.0', '128')**:
  - Uses the RC4 cipher, which is insecure and vulnerable to various attacks as described in CVE-2013-2566
- **SSLv3**:
  - Uses SSL3, which is insecure and vulnerable to man-in-the-middle (MITM) attacks such as POODLE. More information can be found at US-CERT
- **('TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA', 'SSLv3, TLSv1.0', '112')**:
  - Encryption key size is below the minimum of 128 bits
- **('TLS_RSA_WITH_3DES_EDE_CBC_SHA', 'SSLv3, TLSv1.0', '112')**:
  - Encryption key size is below the minimum of 128 bits
- **('TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA', 'SSLv3, TLSv1.0', '112')**:
  - Encryption key size is below the minimum of 128 bits

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

27.Autocomplete Enabled on Password Field

CVSS

Score: 0.0
Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/register.php	Low	Certain	New

The password input named `pass1` has autocomplete enabled.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/	Low	Certain	New

The password input named `password` has autocomplete enabled.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

28.Credit Card Found

CVSS

Score: 5.0
Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/frames/deeptree/start_3.php	Low	Possible	New

- `5473421717821222`

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

29.Email Address Found

CVSS

Score: 5.0
Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/	↓ Low	Likely	New

- `superdude@barracuda.com`: encountered 43 times, for example on http://test.blorpazort.com/

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

30.HTML Form Without CSRF Protection

CVSS

Score: 2.6
Vector: AV:N/AC:H/Au:N/C:N/I:P/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/register.php	↓ Low	Possible	New

The form named `registerform` with the following fields does not appear to have a CSRF token:

- `user (type text)`
- `pass1 (type password)`

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/		Possible	New

Path	Severity	Confidence	Status
	Low		

The form with the following fields does not appear to have a CSRF token:

- `password (type password)`
- `username (type TEXT)`
- `submit (type submit)`

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/pages/sqli_blind_form_2.php	Low	Possible	New

The form named `test_from_2` with the following fields does not appear to have a CSRF token:

- `q (type text)`
- `Submit (type submit)`
- `col (type radio)`
- `reset (type reset)`

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

31.Insufficient Session Expiration

CVSS

Score: 0.0
Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/	Low	Likely	New

A session was maintained idle for 5 minutes, and it was still authenticated (according to the authentication configuration provided to the scan).

Note: depending on your application's security requirements, it may be acceptable to allow idle sessions to persist for longer than 5 minutes.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Not found
2016-09-23	Test Scan	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Not found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

32.Open TCP/UDP Port Found

CVSS

Score: 0.0
Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/	Low	Certain	New

A connection to test.blorpazort.com on TCP port 22 was successful.

Your SSH server is open to the world. This is not a recommended configuration, as anyone can connect to your server and attempt to guess your password using a brute-force attack; if successful, the attacker would have full access to your server. It is highly recommended not block access to port 22 except to authorized IP addresses, or better yet, to block access entirely and use a VPN or other method to access the server.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

Path	Severity	Confidence	Status
http://test.blorpazort.com/	Low	Certain	New

A connection to test.blorpazort.com on UDP port 161 was successful.

An SNMP server running on your web server is accessible to the world. In most cases, you will not want to expose an SNMP server on your web server to the world. Unless you have a specific reason to need this configuration, you should use your network firewall to block access to port 161 on your web server from outside your internal network.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

33.Outdated Version of Web Server

CVSS

Score: 0.0
Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/	Low	Possible	New

Your server reports itself as "Apache/2.2.22 (Ubuntu)"; version 2.4.20 of this server is available.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

34.Session Cookie Does Not Have HttpOnly Flag Set

CVSS

Score: 0.0
Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/	Low	Possible	New

Cookies
- PHPSESSID

, which seems to be session cookies, do not have the HttpOnly flag set.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

35.Session Fixation

CVSS

Score: 0.0
Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/	Low	Likely	New

The scanner visited *http://test.blorpazort.com/* and received the following session cookies: `PHPSESSID=a0ud3rgns9nb0i6lbo17lt4423`. After successfully authenticating, the same session cookies were still being used, indicating a session fixation vulnerability.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Not found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Not found
2016-09-23	Test Scan	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Not found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

36.SSL Certificate Is Untrusted

CVSS

Score: 6.4
Vector: AV:N/AC:L/Au:N/C:P/I:P/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com	Low	Certain	New

The following problems were found with the certificate chain supplied by the server:

- **Depth zero self-signed cert**
  Subject: `/O=Internet Widgits Pty Ltd/ST=Some-State/CN=10.8.120.11/C=IL`
  Issuer: `/O=Internet Widgits Pty Ltd/ST=Some-State/CN=10.8.120.11/C=IL`
  Certificate depth: 0

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Not found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

37.SSL Certificate Ownership Is Invalid

CVSS

Score: 0.0
Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com	Low	Certain	New

Although you did not scan an HTTPS application, the application you scanned is accessible via HTTPS as well. When accessing the application via HTTPS, its hostname 'test.blorpazort.com' doesn't match any of the allowed hosts in the certificate: '10.8.120.11'.

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

38.Uncommon HTTP Method Enabled

CVSS

Score: 0.0
Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

List of Pages

This vulnerability was found on the following pages:

Path	Severity	Confidence	Status
http://test.blorpazort.com/	Low	Certain	New

The following HTTP methods resulted in a successful response from the server: TRACK, DEBUG, PUT, DELETE

This vulnerability was found in the following recent scans:

Scan Date	Configuration	Type	Status
2016-09-28	Test Scan	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-27	test pav222	Max depth 3, N/A	Found
2016-09-27	Test Scan	Max depth 3, N/A	Not found
2016-09-26	Test Scan	Max depth 3, N/A	Found
2016-09-23	Test Scan	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 33	Max depth 3, N/A	Found
2016-09-11	testing blorpazort 22	Max depth 3, N/A	Found
2016-09-11	testing blorpazort	Max depth 3, N/A	Found
2016-08-16	qa scan with + auth + sched	Max depth 5, HTML form	Found

39.Crawler Database

Crawling started from **http://test.blorpazort.com/** with a maximum depth of links

List of all URLs crawled

- http://test.blorpazort.com/pages/upload.php
- http://test.blorpazort.com/pages/xss_form_get.php?action=search&q=Kabul11111111
- http://test.blorpazort.com/pages/sqli_blind_form_1.php?search=Kabulblorpazort
- http://test.blorpazort.com/pages/redirect_onload.php
- http://test.blorpazort.com/members/profile.php
- http://test.blorpazort.com/pages/page_header_inject.php
- http://test.blorpazort.com/pages/sqli/sqli_blind_only.php?cityname=11
- http://test.blorpazort.com/frames/frame_a.php

- http://test.blorpazort.com/pages/targets/target-8859.php
- http://test.blorpazort.com/members/file_show.php
- http://test.blorpazort.com/pages/sqli/sqli_boolean_only.php?id=11
- http://test.blorpazort.com/frames/frame_sample_link_in_center.php
- http://test.blorpazort.com/frames/deeptree/start_13.php
- http://test.blorpazort.com/pages/error_500.php
- http://test.blorpazort.com/pages/page_must_be_https.php
- http://test.blorpazort.com/frames/deeptree/start_33.php
- http://test.blorpazort.com/frames/deeptree/start_12.php
- http://test.blorpazort.com/frames/deeptree/start_1.php
- http://test.blorpazort.com/pages/sqli_form_1.php?region=Australia+and+New+Zealand
- http://test.blorpazort.com/pages/page_utf16.html
- http://test.blorpazort.com/pages/xss_form_get.php?action=search&q=Kabul111111
- http://test.blorpazort.com/frames/deeptree/start_32.php
- http://test.blorpazort.com/frames/deeptree/start_22.php
- http://test.blorpazort.com/frames/frame_iframe.php
- http://test.blorpazort.com/pages/sqli/sqli_boolean_only.php
- http://test.blorpazort.com/frames/deeptree/start_21.php
- http://test.blorpazort.com/
- http://test.blorpazort.com/pages/os_injection_2.php
- http://test.blorpazort.com/pages/redirect_unvalidated_form_1.php?url=http://badstorevm1.bvs.scl.cudaops.com
- http://test.blorpazort.com/redirects.php
- http://test.blorpazort.com/cgi-bin/header_inj.cgi?userdata=11
- http://test.blorpazort.com/pages/redirect_302.php
- http://test.blorpazort.com/pages/redirect_dynamicjs.php
- http://test.blorpazort.com/pages/sqli_showcity.php?cityid=3499
- http://test.blorpazort.com/pages/sqli_showcity.php?cityid=1791
- http://test.blorpazort.com/frames/deeptree/start_2.php
- http://test.blorpazort.com/pages/sqli_showcity.php?cityid=2806
- http://test.blorpazort.com/members/login.php
- http://test.blorpazort.com/pages/xss_dom.php
- http://test.blorpazort.com/pages/xss_parsing_test.php
- http://test.blorpazort.com/members/
- http://test.blorpazort.com/pages/redirect_301.php
- http://test.blorpazort.com/pages/targets/target-utf8.php
- http://test.blorpazort.com/pages/page_insecure_part.php
- http://test.blorpazort.com/pages/rfi.php
- http://test.blorpazort.com/pages/sqli/sqli_with_errors.php?search=Amsterdamblorpazort
- http://test.blorpazort.com/frames/deeptree/start_23.php
- http://test.blorpazort.com/pages/targets/redirect_dynamicjs_target.php
- http://test.blorpazort.com/pages/xss_parsing_test.php?url=http%3A%2F%2Fblorpazort.com%2Fhttp%3A%2F%2Fblorpazort.com%2Fhttp%3A%2F%2Fblorpazort.com%2F
- http://test.blorpazort.com/pages/xss_parsing_test.php?url=http%3A%2F%2Fblorpazort.com%2Fhttp%3A%2F%2Fblorpazort.com%2F
- http://test.blorpazort.com/frames/php_error.php
- http://test.blorpazort.com/pages/rfi.php?color=red
- http://test.blorpazort.com/pages/xss_form_post.php
- https://test.blorpazort.com/pages/page_must_be_https.php
- http://test.blorpazort.com/pages/dirtrav.php?fname=inf.txt11
- http://test.blorpazort.com/frames/frame_b_after_link.php
- http://test.blorpazort.com/pages/redirect_meta.php
- http://test.blorpazort.com/pages/sqli_blind_form_1.php
- http://test.blorpazort.com/members/denied.php
- http://test.blorpazort.com/frames/frameset.php
- http://test.blorpazort.com/cgi-bin/header_inj.cgi
- http://test.blorpazort.com/pages/sqli/sqli_with_errors.php
- http://test.blorpazort.com/pages/sqli/sqli_blind_only.php
- http://test.blorpazort.com/pages/page_iso_8859_1.php
- http://test.blorpazort.com/pages/infi_loop.php.bad
- http://test.blorpazort.com/pages/error_page_2.php
- http://test.blorpazort.com/cgi-bin/banner.cgi
- http://test.blorpazort.com/private.php
- http://test.blorpazort.com/pages/os_injection_2.php?filename=pavel.txt&securetoken=1234
- http://test.blorpazort.com/register.php
- http://test.blorpazort.com/pages/xss_form_get.php?action=search&q=Kabul11
- http://test.blorpazort.com/pages/xss_parsing_test.php?url=http%3A%2F%2Fblorpazort.com%2Fhttp%3A%2F%2Fblorpazort.com%2Fhttp%3A%2F%2Fblorpazort.com%2F
- http://test.blorpazort.com/frames/frame_c.php
- http://test.blorpazort.com/pages/sqli_form_1.php
- http://test.blorpazort.com/members/members.php
- http://test.blorpazort.com/pages/sqli_showcity.php?cityid=2317
- http://test.blorpazort.com/cgi-bin/header_inj_csrf_ssn.cgi?hdn1=abc&hdn2=def&userdata=11
- http://test.blorpazort.com/frames/deeptree/start_3.php
- http://test.blorpazort.com/cgi-bin/header_inj_csrf_ssn.cgi
- http://test.blorpazort.com/pages/sqli_showcity.php?cityid=135
- http://test.blorpazort.com/pages/xss_form_get.php
- http://test.blorpazort.com/pages/sqli_blind_form_2.php
- http://test.blorpazort.com/pages/xss_form_get.php?action=search&q=Kabul1111
- http://test.blorpazort.com/pages/error_page_1.php

- http://test.blorpazort.com/pages/targets/redirect_meta_target.php
- http://test.blorpazort.com/frames/frame_b.php
- http://test.blorpazort.com/pages/xss_parsing_test.php?url=http%3A%2F%2Fblorpazort.com%2F
- http://test.blorpazort.com/pages/targets/redirect_onload_target.php
- http://test.blorpazort.com/pages/os_injection_1.php?cmd=whoami11&securetoken=1234
- http://test.blorpazort.com/members/forum.php
- http://test.blorpazort.com/frames/deeptree/start_31.php
- http://test.blorpazort.com/frames/db_error.php
- http://test.blorpazort.com/pages/dirtrav.php
- http://test.blorpazort.com/frames/deeptree/start_11.php
- http://test.blorpazort.com/pages/os_injection_1.php