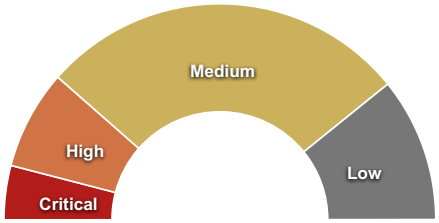
Executive Summary

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	41
Low	16



Server Information

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

Table of Contents

1.Blind OS Command Injection

Issue Background

An OS command injection attack occurs when an attacker attempts to execute system level commands through a vulnerable application. Applications are considered vulnerable to the OS command injection attack if they utilize user input in a system level command.

Issue Remediation

Minimize use of OS commands in web applications, as they are always a security risk. When it is necessary to use an OS command that includes user input, comprehensively scrub all user input for malicious characters prior to running the command.

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	Critical	Likely	Active

Details

The field `filename` was submitted with the value `& sleep 10 &` . The response times seen were 10.14 and 10.12. The field was then submitted with the value `& sleep 4 &` . The response times seen were 4.07 and 4.07. The difference between these times suggests that the injected command was executed, and therefore that OS command injection is possible.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

2.Blind SQL Injection

Issue Background

SQL Injection enables attackers to gain control over your database and, through it, compromise your data and potentially your entire application. A blind SQL injection is one in which the results of the statement are not shown to the user, but are executed nonetheless.

Issue Remediation

Preventing injection requires keeping untrusted data separate from commands and queries.

The preferred option is to use a safe API which avoids the use of the interpreter entirely or provides a parameterized interface. Be careful with APIs, such as stored procedures, that are parameterized, but can still introduce injection under the hood.

If a parameterized API is not available, you should carefully escape special characters using the specific escape syntax for that interpreter.

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

Details

The field `cityid` was submitted with the value `3499 and sleep(10)` . The response times seen were 10.13 and 10.07. The field was then submitted with the value `3499 and sleep(4)` . The response times seen were 4.09 and 4.09. The difference between these times suggests that the server is executing the injected SQL statement.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

The field `search` was submitted with the value `Kabul' and sleep(10)='`. The response times seen were 10.07 and 10.07. The field was then submitted with the value `Kabul' and sleep(4)='`. The response times seen were 4.07 and 4.07. The difference between these times suggests that the server is executing the injected SQL statement.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

3.OS Command Injection

Issue Background

An OS command injection attack occurs when an attacker attempts to execute system level commands through a vulnerable application. Applications are considered vulnerable to the OS command injection attack if they utilize user input in a system level command.

Issue Remediation

Minimize use of OS commands in web applications, as they are always a security risk. When it is necessary to use an OS command that includes user input, comprehensively scrub all user input for malicious characters prior to running the command.

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	Active

Details

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 11/01/2017 20:13:10` was found in the response, suggesting that the injected command was executed, and therefore that OS command injection is possible.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

4.SQL Injection

Issue Background

SQL Injection enables attackers to gain control over your database and, through it, compromise your data and potentially your entire application.

Issue Remediation

Preventing injection requires keeping untrusted data separate from commands and queries.

The preferred option is to use a safe API which avoids the use of the interpreter entirely or provides a parameterized interface. Be careful with APIs, such as stored procedures, that are parameterized, but can still introduce injection under the hood.

If a parameterized API is not available, you should carefully escape special characters using the specific escape syntax for that interpreter.

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	Active

Details

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.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

5.Directory Traversal

Issue Background

Directory Traversal, also known as Path Traversal, "dot-dot-slash" and "backtracking", is when a misconfigured server or code error allows an attacker access to files outside the web root folder. These files may contain source code, configuration, and critical system files, including password files.

Issue Remediation

Do not use user input that is not properly sanitized as any part of a path component. It is even more advisable to never use user input in a path component at all.

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/dirtrav.php	High	Certain	New

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

6.Known Vulnerable Web Server

Issue Background

None

Issue Remediation

Upgrade to the latest version of your web server.

List of Pages

This vulnerability was found on the following pages:

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

7.Reflected Cross-Site Scripting

Issue Background

XSS (Cross-site scripting) enables attackers to inject client-side script into Web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same origin policy

Issue Remediation

Sanitize all user input to remove HTML markup (such as < and > signs). Escape all values that come from user input before outputting them to the resulting page.

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_parsing_test.php	High	Certain	New

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

The `q` parameter was submitted with the value `<script>prompt(12345)</script>zOJ8e`, and the string was echoed verbatim in the output, showing that there is a reflected XSS vulnerability.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

The `lname` parameter was submitted with the value `<script>prompt(12345)</script>0zdH6`, and the string was echoed verbatim in the output, showing that there is a reflected XSS vulnerability.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

The `color` parameter was submitted with the value `<script>prompt(12345)</script>q3iVX`, and the string was echoed verbatim in the output, showing that there is a reflected XSS vulnerability.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

8.Stored Cross-Site Scripting

Issue Background

Stored attacks are those where the injected script is permanently storedon the target servers, such as in a database, in a message forum, visitor log, comment field, etc. The victim then retrieves the malicious script from the server when it requests the stored information. Stored XSS is also sometimes referred to as Persistent or Type-I XSS.

Issue Remediation

Sanitize all user input to remove HTML markup (such as < and > signs). Escape all values that come from user input before outputting them to the resulting page, .

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/page_header_inject.php	High	Certain	New

Details

The `fname` parameter was submitted with the value `<script>prompt(12345)</script>a5s15`, and then the page was requested again without submitting the form. The string `<script>prompt(12345)</script>a5s15` was echoed verbatim in the output of the page - even when not submitting the form - showing that there is a stored XSS vulnerability.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

The `lname` parameter was submitted with the value `<script>prompt(12345)</script>xtdtf`, and then the page was requested again without submitting the form. The string `<script>prompt(12345)</script>xtdtf` was echoed verbatim in the output of the page - even when not submitting the form - showing that there is a stored XSS vulnerability.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

9.Unvalidated Redirect

Issue Background

Unvalidated redirects and forwards are possible when a web application accepts untrusted input that could cause the web application to redirect the request to a URL contained within untrusted input. By modifying untrusted URL input to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials. Because the server name in the modified link is identical to the original site, phishing attempts may have a more trustworthy appearance. Unvalidated redirect and forward attacks can also be used to maliciously craft a URL that would pass the application's access control check and then forward the attacker to privileged functions that they would normally not be able to access.

Issue Remediation

It is recommended to avoid using redirects and forwards where not necessary. Where necessary, instead of passing in the URL itself as user input, pass in an identifier that is internally converted into a URL. If even this is not possible, comprehensively validate that the input URL is a URL that makes sense for this application and that the user is authorized to redirect to.

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

10.Blacklisted Domain

Issue Background

Barracuda Threat Intelligence monitors IP addresses and domain names for malicious or questionable activity. One or more of the domain names or IPs associated with this web application were detected by Barracuda Threat Intelligence as malicious or questionable. See below for more information.

Issue Remediation

If you are linking to a blacklisted IP or domain - remove the link, to prevent search engines from penalizing your application or blacklisting it by association. If your own domain or IP is blacklisted - perform a thorough audit to ensure your site is not hosting any malware or sending any spam email.

List of Pages

This vulnerability was found on the following pages:

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

11.Clickjacking: Missing X-Frame-Options Header

Issue Background

Clickjacking, also known as a "UI redress attack", is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the the top level page.

Issue Remediation

Sending the proper X-Frame-Options HTTP response header instructs the browser to not allow framing from other domains.

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

12.Directory Indexing

Issue Background

When the web server is configured appropriately, it will show a directory listing when a client requests a directory instead of a file, and that directory does not have a index file (such as index.html or index.php). Such a directory listing provides an attacker with an inventory of files on the server, which makes the attack surface clearer and could include sensitive information.

Issue Remediation

Consult your web server's user guide for information on how to disable directory indexes. For example, in Apache, add the directive "Options -Indexes" to the server's configuration file.

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/sqli/	Medium	Likely	New

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

13.FrontPage Server Extensions Found

Issue Background

FrontPage is an old content publishing platform. It is commonly regarded as insecure, and rarely in use today; however, it is installed by default in some configurations.

Issue Remediation

If the FrontPage server extensions are not in use, remove them to minimize security risk.

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

14.HTML Injection

Issue Background

Hypertext Markup Language (HTML) injection is an attack on a user made possible by an injection vulnerability in a web application. When an application does not properly handle user supplied data, an attacker can supply valid HTML,typically via a parameter value, and inject their own content into the page.

Issue Remediation

Sanitize all user input to remove HTML markup (such as < and > signs). Escape all values that come from user input before outputting them to the resulting page.

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

Details

The `q` parameter was submitted with the value `<h1>f1mea</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.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

The `url` parameter was submitted with the value `<h1>cywwx</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.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

The `search` parameter was submitted with the value `<h1>gyyjl</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.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

The `fname` parameter was submitted with the value `<h1>lharf</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.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

The `lname` parameter was submitted with the value `<h1>yxtkc</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.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

The `color` parameter was submitted with the value `<h1>s9nvv</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.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

15.HTTP Header Injection

Issue Background

HTTP Header Injection/HTTP Request Splitting allows attackers to forge pages and alter browser behavior by directly controlling HTTPheaders returned by the server.

Issue Remediation

Sanitize and escape all user input before using it in code that affects HTTP headers. Also, sanitize and escape all strings before using them to generate an HTTP response header.

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

16.HTTP OPTIONS Method Enabled

Your web server allows the HTTP OPTIONS method, which can provide information to an attacker to help mount an attack.

Threat Details

HTTP, the protocol used by browsers to talk to web servers, defines eight methods (or verbs), which a client browser may request from the server. GET and POST are the most commonly used methods. The OPTIONS method returns information on which HTTP methods the server supports. This is not in itself a security vulnerability; however, it tells potential attackers which (potentially uncommon) methods are supported and allows the attacker to then probe those methods for unanticipated functionality. The OPTIONS method is necessary for a limited set of applications (such as REST APIs or applications supporting CORS pre-flight requests); however, in the vast majority of circumstances, it should be disabled.

Remediation on the Barracuda Web Application Firewall

The Web Application Firewall always restricts HTTP methods to only those that are explicitly allowed. Any others are blocked.

For More Information

 See the OWASP page on testing HTTP methods for technical information on the possible security vulnerabilities created by HTTP methods.

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

Details

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.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

17.Malicious File Upload

Issue Background

A malicious file upload occurs when users are allowed to upload files to the server, and these files are not checked for malicious content such as viruses. Allowing a user to upload files without virus scanning can allow attackers to infect the server and/or other clients with malicious code that can provide the attacker unauthorized access to data and code.

Issue Remediation

All files uploaded to the server should be scanned for viruses before being processed. This can be done by the application code itself, or by a web application firewall (WAF) in front of the application.

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

Details

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.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

18.Password is Sent Unencrypted

Issue Background

A form containing a password field is configured to submit using HTTP, instead of encrypted HTTPS. This could allow malicious users to intercept passwords.

Issue Remediation

Forms containing sensitive information such as passwords should always submit using HTTPS.

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

19.Remote File Inclusion

Issue Background

The File Inclusion vulnerability allows an attacker to include a file, usually exploiting a "dynamic file inclusion" mechanisms implemented in the target application. The vulnerability occurs due to the use of user-supplied input without proper validation. This could allow an attacker torelay attacks to other sites, or execute arbitrary code on the web server.

Issue Remediation

Do not use user input that is not properly sanitized as any part of a path component. It is even more advisable to never use user input in a path component at all.

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/dirtrav.php	Medium	Certain	New

Details

The field `fname` was submitted with the value `http://s3.amazonaws.com/hashedfiles/f.txt`. The contents of the remote URL ,85ZvACUNhP6xUkKUCyRn, were included in the response, showing that the remote file was successfully included..

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

The field `color` was submitted with the value `http://s3.amazonaws.com/hashedfiles/f.txt`. The contents of the remote URL ,85ZvACUNhP6xUkKUCyRn, were included in the response, showing that the remote file was successfully included..

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

20.Sensitive File Found

Issue Background

Attackers commonly start their attack by looking for commonly named files, such as backup files, on the server. Any such files may contain information on the server or platforms being used, configuration, or even sensitive information such as passwords.

Issue Remediation

All common files should be either removed from the server (as in the case of backup files) or renamed to a non-common name.

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/web.config	Medium	Likely	New

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

21.Server Error on Page

Issue Background

A page returned from the server has an error message generated by server-side code. This error message leaks information about your environment which can be used by an attacker to improve an attack.

Issue Remediation

1. Configure your server to never show error messages to the user. Consult the documentation for your server-side environment for information on how to do this. For example, for PHP you would need to set show_errors to Off in php.ini.
2. Investigate the cause of the error and eliminate it. For example, if you are not sanitizing input properly, add the relevant sanitizing code.

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_1.php	Medium	Certain	New

Details

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.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

The following error message was returned by the server: `Fatal error: Cannot divide 1493197 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.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

22.Server-Side Source Code Found

Issue Background

Content appearing to be server-side source code was found in the web page. Disclosing server-side code to the user provides information that is very useful in mounting another attack, and in some cases can even disclose credentials that can easily be used to gain unauthorized access. However, due to overlap between server-side languages (e.g. PHP) and client-side languages (e.g. Javascript), it is possible that the code detected as server-side is actually valid, secure client-side code. All instances of this vulnerability should be manually checked.

Issue Remediation

Manually check to see if the code in question is indeed server-side code; if so, remove it from the 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/cgi-bin/header_inj.cgi	Medium	Possible	New

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

23.Social Security Number Found

Issue Background

One or more numbers that appear to be valid US social security numbers were found on this page. This may indicate an information leak

Issue Remediation

Check and remove any US social security numbers from the 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/rfi.php?color=red	Medium	Possible	New

Details

- `078-05-1120`

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

24.Vulnerable Flash Cross-Domain Policy

Issue Background

Flash's default security model enforces the "same origin policy," similar to contemporary browsers, and does not allow cross domain data read operations. However, it can make an exception to this rule and disregard its default security model if a web application hosts a cross-domain policy file (named crossdomain.xml) to allow data access from other domains. Insecurely written cross-domain policy files can expose critical application data over the internet.

Issue Remediation

Restrict cross-domain access by removing or editing the crossdomain.xml file. If your web application is not accessed by Flash, remove the file altogether to restrict all cross-domain access. If your web application is accessed by Flash, change the file to allow only the specific domains you would like to have access to your web application via Flash. For more information, see the Cross-domain policy file specification on Adobe's web site.

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

25.Vulnerable Silverlight Cross-Domain Policy

Issue Background

Silverlight's default security model enforces the "same origin policy," similar to contemporary browsers, and does not allow cross domain data read operations. However, it can make an exception to this rule and disregard its default security model if a web application hosts a cross-domain policy file (named clientaccesspolicy.xml) to allow data access from other domains. Insecurely written cross-domain policy files can expose critical application data over the internet.

Issue Remediation

Restrict cross-domain access by removing or editing the clientaccesspolicy.xml file. If your web application is not accessed by Silverlight, remove the file altogether to restrict all cross-domain access. If your web application is accessed by Silverlight, change the file to allow only the specific domains you would like to have access to your web application via Silverlight. For more information, see "Making a Service Available Across Domain Boundaries" in the Microsoft Developer Network (MSDN).

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

26.Autocomplete Enabled on Password Field

Issue Background

Enabling autocomplete on a password field could allow the browser to store a user's password in plain text and show it to anyone using the same computer.

Issue Remediation

Add 'autocomplete=off' to every password field or login form on the site.

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

Details

The password input named `pass1` has autocomplete enabled.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

The password input named `password` has autocomplete enabled.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

27.Credit Card Found

Issue Background

One or more numbers that appear to be valid credit card numbers were found on this page. This may indicate an information leak

Issue Remediation

Check and remove any credit card numbers from the 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/frames/deeptree/start_3.php	Low	Possible	New

Details

- `5473421717821222`

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

28.Email Address Found

Issue Background

One or more email addresses were found on this page. Spambots (automated scripts written by spammers) can harvest this information and use it to send you spam email.

Issue Remediation

Use contact forms (protected with Captchas) rather than posting email addresses when possible. When not possible, obfuscate the email address using a Javascript framework or use a honeypot solution to confuse spambots.

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

Details

- `superdude@barracuda.com`: encountered 43 times, for example on http://test.blorpazort.com/
- `megasponsor@cudacuda.com`: encountered 1 time, for example on http://test.blorpazort.com/redirects.php

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

29.HTML Form Without CSRF Protection

Issue Background

Cross Site Request Forgery enables attackers to make your users perform potentially destructive actions on your site when they are visiting an attacker's site

Issue Remediation

Check if this form could perform any destructive actions; if so, implement CSRF protection, for example using a CSRF token or nonce.

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

Details

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

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

30.Open TCP/UDP Port Found

Issue Background

Background: A connection to your web server on a non-web TCP/UDP port was successful. This typically indicates that there is another service running on the web server which is not related to web traffic. Additional services running on the web server expose it to a whole set of attacks on that service, and should be avoided.

Issue Remediation

Use a software or hardware firewall to block access to all ports except those required for web traffic (typically 80 and/or 443). If you require administration access to the web server, use a VPN or IP whitelisting to allow authorized users access while blocking unauthenticated users. If the other services must be publicly accessible, move them to a non-web server so that a compromise in that service does not affect the web server as well.

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

Details

A connection to test.blorpazort.com on UDP port 53 was successful.

Your DNS server is accessible to the world. In most cases, you will not want to expose a DNS 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 53 on your web server from outside your internal network.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

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

Details

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.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

31.Outdated Version of Web Server

Issue Background

Older versions of web servers frequently have known vulnerabilities. Running these old versions exposes you to hackers using pre-built exploits to attack your server, with potentially severe results depending on the nature of the known vulnerability.

Issue Remediation

Upgrade to the latest version of your 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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

32.Session Cookie Does Not Have HttpOnly Flag Set

Issue Background

The application's session cookie should always have the HttpOnly flag set. This prevents the cookie from being stolen or manipulated by client-side code (e.g. Javascript), and greatly reduces the attack surface for session-related attacks such as Cross-Site Scripting.

Issue Remediation

Configure your web server to send the HttpOnly flag with all session cookies.

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

Details

Cookies
- `PHPSESSID`

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

33.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

Details

The following problems were found with the certificate chain supplied by the server:
- **Depth zero self-signed cert**
  Subject: `/C=IL/ST=Some-State/CN=10.8.120.11/O=Internet Widgits Pty Ltd`
  Issuer: `/C=IL/ST=Some-State/CN=10.8.120.11/O=Internet Widgits Pty Ltd`
  Certificate depth: 0

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

34.SSL Certificate Ownership Is Invalid

Issue Background

Every SSL certificate specifies which web servers it is valid for. Trying to use an SSL certificate which is not valid for the server it is used on will cause client browsers to issue a warning, and in some cases deny users access to the site.

Issue Remediation

Contact your certification authority (CA) - the body that generated your original SSL certificate - and obtain a new certificate that is valid for all domains being used by your application. A single certificate can be valid for multiple domains.

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

Details

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'.

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

35.Uncommon HTTP Method Enabled

Your web server allows one or more uncommon HTTP methods, which can expose unanticipated functionality to an attacker.

Threat Details

HTTP, the protocol used by browsers to talk to web servers, defines eight methods (or verbs), which a client browser may request from the server. GET and POST are the most commonly used methods. Most applications do not handle the less common HTTP methods. However, they are still active, and in some cases may expose functionality that was not intended. For example: <ul> In some configurations, the PUT and DELETE methods may be used by users to create and delete files on the web server. The TRACE method may be used to mount a Cross-Site Tracing (XST) attack. The DEBUG method may expose information about the debugging configuration for the application. Uncommon HTTP methods are necessary for a limited set of applications (such as REST APIs); however, in the vast majority of circumstances, they should be disabled.

Remediation on the Barracuda Web Application Firewall

The Web Application Firewall always restricts HTTP methods to only those that are explicitly allowed. Any others are blocked.

For More Information

 See the OWASP page on testing HTTP methods for technical information on the possible security vulnerabilities created by HTTP methods.

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

Details

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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

36.Weak SSL Cipher

Issue Background

HTTPS (HTTP secured via an SSL/TLS tunnel) allows a number of different ciphers to be used. Even if high grade ciphers are today supported and normally used, some misconfiguration in the server can be used to force the use of a weak cipher - or at worst no encryption. This could permit an attacker to read encrypted communications, or even change encrypted data using a man-in-the-middle attack. Other misconfiguration can be used for a Denial of Service attack.

Issue Remediation

Configure your web server to reject weak ciphers. See the attack detail for the specific ciphers to disable.

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	Certain	New

Details

The following weak SSL ciphers were detected:

- **('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_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_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

Recent Scans

The status of this vulnerability in the ten most recent scans of this web application:

Scan Date	Configuration	Type	Status
2017-01-12	Default	Max depth 3, N/A	Found

37.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/sqli_form_1.php
- http://test.blorpazort.com/pages/error_page_2.php
- http://test.blorpazort.com/frames/frameset.php
- http://test.blorpazort.com/pages/dirtrav.php
- http://test.blorpazort.com/pages/infi_loop.php.bad
- http://test.blorpazort.com/frames/deeptree/start_1.php
- http://test.blorpazort.com/frames/db_error.php
- http://test.blorpazort.com/pages/redirect_301.php
- http://test.blorpazort.com/pages/xss_form_get.php?action=search&q=Kabul1111
- http://test.blorpazort.com/frames/deeptree/start_2.php
- http://test.blorpazort.com/pages/targets/target-utf8.php
- http://test.blorpazort.com/frames/frame_c.php
- http://test.blorpazort.com/cgi-bin/header_inj.cgi
- http://test.blorpazort.com/pages/os_injection_2.php?filename=pavel.txt&securetoken=1234
- http://test.blorpazort.com/frames/frame_iframe.php
- http://test.blorpazort.com/pages/page_insecure_part.php
- http://test.blorpazort.com/pages/os_injection_1.php?cmd=whoami11&securetoken=1234
- http://test.blorpazort.com/cgi-bin/header_inj_csrf_ssn.cgi?hdn1=abc&hdn2=def&userdata=11
- http://test.blorpazort.com/pages/sqli/sqli_blind_only.php
- https://test.blorpazort.com/pages/page_must_be_https.php
- http://test.blorpazort.com/pages/error_page_1.php
- http://test.blorpazort.com/pages/rfi.php?color=red
- http://test.blorpazort.com/pages/targets/redirect_meta_target.php
- http://test.blorpazort.com/pages/redirect_unvalidated_form_1.php?url=http://badstorevm1.bvs.scl.cudaops.com
- http://test.blorpazort.com/pages/xss_form_get.php?action=search&q=Kabul11
- http://test.blorpazort.com/pages/sqli_form_1.php?region=Australia+and+New+Zealand
- http://test.blorpazort.com/pages/dirtrav.php?fname=inf.txt11
- http://test.blorpazort.com/frames/frame_sample_link_in_center.php
- http://test.blorpazort.com/frames/frame_b.php

- http://test.blorpazort.com/pages/os_injection_1.php
- http://test.blorpazort.com/pages/sqli/sqli_blind_only.php?cityname=11
- http://test.blorpazort.com/pages/xss_form_get.php
- http://test.blorpazort.com/frames/deeptree/start_3.php
- http://test.blorpazort.com/pages/xss_parsing_test.php?url=http%3A%2F%2Fblorpazort.com%2F
- http://test.blorpazort.com/frames/frame_a.php
- http://test.blorpazort.com/pages/sqli_blind_form_1.php?search=Kabulblorpazort
- http://test.blorpazort.com/members/members.php
- http://test.blorpazort.com/cgi-bin/header_inj_csrf_ssn.cgi
- http://test.blorpazort.com/pages/sqli_showcity.php?cityid=3499
- http://test.blorpazort.com/pages/sqli/sqli_with_errors.php
- http://test.blorpazort.com/pages/redirect_302.php
- http://test.blorpazort.com/pages/sqli/sqli_boolean_only.php
- http://test.blorpazort.com/pages/page_header_inject.php
- http://test.blorpazort.com/members/denied.php
- http://test.blorpazort.com/pages/os_injection_2.php
- http://test.blorpazort.com/pages/rfi.php
- http://test.blorpazort.com/pages/sqli/sqli_with_errors.php?search=Amsterdamblorpazort
- http://test.blorpazort.com/pages/sqli_showcity.php?cityid=2317
- http://test.blorpazort.com/pages/sqli_showcity.php?cityid=2806
- http://test.blorpazort.com/frames/php_error.php
- http://test.blorpazort.com/pages/redirect_meta.php
- http://test.blorpazort.com/pages/targets/redirect_dynamicjs_target.php
- http://test.blorpazort.com/pages/error_500.php
- http://test.blorpazort.com/pages/targets/redirect_onload_target.php
- http://test.blorpazort.com/pages/sqli_blind_form_1.php
- http://test.blorpazort.com/pages/page_iso_8859_1.php
- http://test.blorpazort.com/pages/page_utf16.html
- http://test.blorpazort.com/pages/xss_dom.php
- http://test.blorpazort.com/members/login.php
- http://test.blorpazort.com/cgi-bin/banner.cgi
- http://test.blorpazort.com/pages/sqli_blind_form_2.php
- http://test.blorpazort.com/pages/page_must_be_https.php
- http://test.blorpazort.com/redirects.php
- http://test.blorpazort.com/pages/redirect_dynamicjs.php
- http://test.blorpazort.com/pages/redirect_onload.php
- http://test.blorpazort.com/cgi-bin/header_inj.cgi?userdata=11
- http://test.blorpazort.com/
- http://test.blorpazort.com/pages/sqli/sqli_boolean_only.php?id=11
- http://test.blorpazort.com/register.php
- http://test.blorpazort.com/pages/targets/target-8859.php
- http://test.blorpazort.com/pages/xss_parsing_test.php
- http://test.blorpazort.com/pages/xss_form_post.php
- 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/pages/upload.php
- http://test.blorpazort.com/pages/sqli_showcity.php?cityid=1791
- http://test.blorpazort.com/pages/sqli_showcity.php?cityid=135