OWASP TOP 10 2021

Description

The primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risk problem areas - and also provides guidance on where to go from here.

Disclaimer

This document or any of its content cannot account for, or be included in any form of legal advice. The outcome of a vulnerability scan (or security evaluation) should be utilized to ensure that diligent measures are taken to lower the risk of potential exploits carried out to compromise data.

Legal advice must be supplied according to its legal context. All laws and the environments in which they are applied, are constantly changed and revised. Therefore no information provided in this document may ever be used as an alternative to a qualified legal body or representative.

A portion of this report is taken from OWASP's Top Ten 2021 Project document, that can be found at http://www.owasp.org.

Scan Detail

Target	http://192.168.27.1/
Scan Type	Full Scan
Start Time	Oct 17, 2025, 4:14:08 PM GMT
Scan Duration	5 minutes
Requests	26244
Average Response Time	1ms
Maximum Response Time	30040ms
Application Build	v24.6.240626115
Authentication Profile	-

Compliance at a Glance

CATEGORY	
8	A01 Broken Access Control
9	A02 Cryptographic Failures
7	A03 Injection
2	A04 Insecure Design
6	A05 Security Misconfiguration
13	A06 Vulnerable and Outdated Components
1	A07 Identification and Authentication Failures
0	A08 Software and Data Integrity Failures
0	A09 Security Logging and Monitoring Failures
0	A10 Server-Side Request Forgery

Detailed Compliance Report by Category

This section is a detailed report that explains each vulnerability found according to individual compliance categories.

A01 Broken Access Control

Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.

[Possible] Internal IP Address Disclosure

One or more strings matching an internal IPv4 address were found. These IPv4 addresses may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

The significance of this finding should be confirmed manually.

CWE
CWE-200

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible sensitive information disclosure.

http://192.168.27.1/

Pages with internal IPs:

- http://192.168.27.1/usage/usage_200909.html
  192.168.1.200
- http://192.168.27.1/mrtg/cfgmaker.html
  10.10.0.18
- http://192.168.27.1/mrtg/mibhelp.html
  10.32.2.1
- http://192.168.27.1/mrtg/nt-guide.html
  10.10.10.1
- http://192.168.27.1/manual/mod/mod_ssl/ssl_howto.html
  192.168.1.0

Request

```
GET /usage/usage_200909.html HTTP/1.1
Referer: http://192.168.27.1/usage/index.html
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
```

```
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

CWE
CWE-200

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

http://192.168.27.1/

Possible sensitive files:

- http://192.168.27.1/**test.php**

Request

```
GET /test.php HTTP/1.1
Accept: eyipcxkf/viqc
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

Restrict access to this file or remove it from the website.

References

Web Server Security and Database Server Security
https://www.acunetix.com/websitesecurity/webserver-security/

[Possible] Internal Path Disclosure (*nix)

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

CWE
CWE-200

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible sensitive information disclosure.

http://192.168.27.1/

Pages with paths being disclosed:

- http://192.168.27.1/
  >/etc/httpd/conf/httpd.conf
- http://192.168.27.1/index.html
  >/etc/httpd/conf/httpd.conf
- http://192.168.27.1/mrtg/mrtg-rrd.html
  /usr/local/rrdtool/bin/
- http://192.168.27.1/mrtg/reference.html
  /usr/tardis/pub/www/stats/mrtg
- http://192.168.27.1/mrtg/unix-guide.html
  /usr/local/src
- http://192.168.27.1/manual/mod/mod_ssl/ssl_howto.html
  /usr/local/apache/htdocs
- http://192.168.27.1/manual/mod/mod_ssl/ssl_reference.html
  :/usr/local/apache/sbin/pp

Request

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

References

Full Path Disclosure
https://www.owasp.org/index.php/Full_Path_Disclosure

[Possible] Internal Path Disclosure (Windows)

One or more fully qualified path names were been found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

CWE
CWE-200

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible sensitive information disclosure.

http://192.168.27.1/

Pages with paths being disclosed:

- http://192.168.27.1/mrtg/nt-guide.html
  c:\www\mrtg

Request

```
GET /mrtg/nt-guide.html HTTP/1.1
Referer: http://192.168.27.1/mrtg/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

References

Full Path Disclosure
https://www.owasp.org/index.php/Full_Path_Disclosure

Generic Email Address Disclosure

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

CWE
CWE-200

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Email addresses posted on Web sites may attract spam.

http://192.168.27.1/

Emails found:

- http://192.168.27.1/usage/index.html
  brad@mrunix.net
- http://192.168.27.1/usage/
  brad@mrunix.net
- http://192.168.27.1/usage/usage_200909.html
  brad@mrunix.net
- http://192.168.27.1/mrtg/
  oetiker@ee.ethz.ch
- http://192.168.27.1/mrtg/
  dlr@bungi.com
- http://192.168.27.1/mrtg/
  mirror@vinnie.ksu.ksu.edu
- http://192.168.27.1/mrtg/
  seror@agarik.com
- http://192.168.27.1/mrtg/
  ayamura@ayamura.org
- http://192.168.27.1/mrtg/
  steve@hdl.com
- http://192.168.27.1/mrtg/
  martin.och@cs-compex.cz
- http://192.168.27.1/mrtg/
  gaiser@matrix.com.br
- http://192.168.27.1/mrtg/
  freitas@dcc.ufmg.br
- http://192.168.27.1/mrtg/
  hiroyuki@nucba.ac.jp
- http://192.168.27.1/mrtg/
  keith@nol.net
- http://192.168.27.1/mrtg/
  levine@yoyo.org
- http://192.168.27.1/mrtg/
  web@std.siamu.ac.th
- http://192.168.27.1/mrtg/
  --trond.kandal@itea.ntnu.no
- http://192.168.27.1/mrtg/
  dima@chg.ru
- http://192.168.27.1/mrtg/
  brian@ou.edu
- http://192.168.27.1/mrtg/
  stefano@unipi.it
- http://192.168.27.1/mrtg/
  ijliao@ccca.nctu.edu.tw

Request

```
GET /usage/index.html HTTP/1.1
Referer: http://192.168.27.1/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

Check references for details on how to solve this problem.

References

Anti-spam techniques
https://en.wikipedia.org/wiki/Anti-spam_techniques

Apache version older than 1.3.31

This alert was generated using only banner information. It may be a false positive.

Multiple vulnerabilities have been found in this version of Apache. You should upgrade to the latest version of Apache.

Affected Apache versions (up to 1.3.30).

CWE
CWE-264

CVSS2
AV:N/AC:L/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	Partial
Exploitability	Proof of concept code
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Base Score	7.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	Low
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Multiple. Check references for details about every vulnerability.

http://192.168.27.1/

Version detected: Apache/1.3.20 .

Recommendation

Upgrade Apache to the latest version.

References

CAN-2003-0987
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0987

CAN-2003-0020
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0020

CAN-2004-0174
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0174

CAN-2003-0993
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0993

Apache homepage
http://httpd.apache.org

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

CWE
CWE-538

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

http://192.168.27.1/ Verified

Folders with directory listing enabled:

- http://192.168.27.1/manual/
- http://192.168.27.1/manual/mod/
- http://192.168.27.1/icons/
- http://192.168.27.1/icons/small/
- http://192.168.27.1/manual/mod/mod_perl/

Request

```
GET /manual/ HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

References

CWE-548: Exposure of Information Through Directory Listing
https://cwe.mitre.org/data/definitions/548.html

Webalizer script

The Webalizer is a fast, free web server log file analysis program. It produces highly detailed, easily configurable usage reports in HTML format, for viewing with a standard web browser.

It's recommended to restrict access to this directory as it may contain sensitive information (test scripts, administrative interfaces, session tokens sent via GET, ...). This kind of information may help an attacker to learn more about the structure of your website and can be used to conduct further attacks.

CWE
CWE-538

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

Base Score	5.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	Low
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible sensitive information disclosure.

http://192.168.27.1/usage/index.html

Request

```
GET /usage/index.html HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

Restrict (or password protect) the access to directory or make it accessible only on the local interface.

References

Wikipedia: Webalizer
https://en.wikipedia.org/wiki/Webalizer

A02 Cryptographic Failures

The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws, e.g., EU's General Data Protection Regulation (GDPR), or regulations, e.g., financial data protection such as PCI Data Security Standard (PCI DSS).

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

CWE
CWE-538

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

http://192.168.27.1/ Verified

Folders with directory listing enabled:

- http://192.168.27.1/manual/
- http://192.168.27.1/manual/mod/
- http://192.168.27.1/icons/
- http://192.168.27.1/icons/small/
- http://192.168.27.1/manual/mod/mod_perl/

Request

```
GET /manual/ HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

References

CWE-548: Exposure of Information Through Directory Listing
https://cwe.mitre.org/data/definitions/548.html

Webalizer script

The Webalizer is a fast, free web server log file analysis program. It produces highly detailed, easily configurable usage reports in HTML format, for viewing with a standard web browser.

It's recommended to restrict access to this directory as it may contain sensitive information (test scripts, administrative interfaces, session tokens sent via GET, ...). This kind of information may help an attacker to learn more about the structure of your website and can be used to conduct further attacks.

CWE
CWE-538

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

Base Score	5.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	Low
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible sensitive information disclosure.

http://192.168.27.1/usage/index.html

Request

```
GET /usage/index.html HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

Restrict (or password protect) the access to directory or make it accessible only on the local interface.

References

Wikipedia: Webalizer
https://en.wikipedia.org/wiki/Webalizer

[Possible] Internal IP Address Disclosure

One or more strings matching an internal IPv4 address were found. These IPv4 addresses may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

The significance of this finding should be confirmed manually.

CWE
CWE-200

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None

Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible sensitive information disclosure.

http://192.168.27.1/

Pages with internal IPs:

- http://192.168.27.1/usage/usage_200909.html
  192.168.1.200
- http://192.168.27.1/mrtg/cfgmaker.html
  10.10.0.18
- http://192.168.27.1/mrtg/mibhelp.html
  10.32.2.1
- http://192.168.27.1/mrtg/nt-guide.html
  10.10.10.1
- http://192.168.27.1/manual/mod/mod_ssl/ssl_howto.html
  192.168.1.0

Request

```
GET /usage/usage_200909.html HTTP/1.1
Referer: http://192.168.27.1/usage/index.html
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

Possible sensitive files

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

CWE

CWE-200

CVSS2

AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

http://192.168.27.1/

Possible sensitive files:

- http://192.168.27.1/**test.php**

Request

```
GET /test.php HTTP/1.1
Accept: eyipcxkf/viqc
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

Restrict access to this file or remove it from the website.

References

Web Server Security and Database Server Security
https://www.acunetix.com/websitesecurity/webserver-security/

TRACE/TRACK Method Detected

HTTP TRACE method is enabled on this web server. In the presence of other cross-domain vulnerabilities in web browsers, sensitive header information could be read from any domains that support the HTTP TRACE method.

CWE
CWE-489

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Attackers may abuse HTTP TRACE functionality to gain access to information in HTTP headers such as cookies and authentication data.

http://192.168.27.1/

Request

```
TRACE /BxSWbRBuW7 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

Disable TRACE Method on the web server.

References

W3C - RFC 2616
http://www.w3.org/Protocols/rfc2616/rfc2616-sec9.html

US-CERT VU#867593
https://www.kb.cert.org/vuls/id/867593/

Cross-site tracing (XST)
https://www.cgisecurity.com/lib/WH-WhitePaper_XST_ebook.pdf

[Possible] Internal Path Disclosure (*nix)

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

CWE
CWE-200

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible sensitive information disclosure.

http://192.168.27.1/

Pages with paths being disclosed:

- http://192.168.27.1/
  >/etc/httpd/conf/httpd.conf
- http://192.168.27.1/index.html
  >/etc/httpd/conf/httpd.conf
- http://192.168.27.1/mrtg/mrtg-rrd.html
  /usr/local/rrdtool/bin/
- http://192.168.27.1/mrtg/reference.html
  /usr/tardis/pub/www/stats/mrtg
- http://192.168.27.1/mrtg/unix-guide.html
  /usr/local/src
- http://192.168.27.1/manual/mod/mod_ssl/ssl_howto.html
  /usr/local/apache/htdocs
- http://192.168.27.1/manual/mod/mod_ssl/ssl_reference.html
  :/usr/local/apache/sbin/pp

Request

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

References

Full Path Disclosure
https://www.owasp.org/index.php/Full_Path_Disclosure

[Possible] Internal Path Disclosure (Windows)

One or more fully qualified path names were been found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

CWE
CWE-200

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible sensitive information disclosure.

http://192.168.27.1/

Pages with paths being disclosed:

- http://192.168.27.1/mrtg/nt-guide.html
  c:\www\mrtg

Request

```
GET /mrtg/nt-guide.html HTTP/1.1
Referer: http://192.168.27.1/mrtg/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

References

Full Path Disclosure
https://www.owasp.org/index.php/Full_Path_Disclosure

Generic Email Address Disclosure

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

CWE
CWE-200

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Email addresses posted on Web sites may attract spam.

http://192.168.27.1/

Emails found:

- http://192.168.27.1/usage/index.html
  brad@mrunix.net
- http://192.168.27.1/usage/
  brad@mrunix.net
- http://192.168.27.1/usage/usage_200909.html
  brad@mrunix.net
- http://192.168.27.1/mrtg/
  oetiker@ee.ethz.ch
- http://192.168.27.1/mrtg/
  dlr@bungi.com
- http://192.168.27.1/mrtg/
  mirror@vinnie.ksu.ksu.edu
- http://192.168.27.1/mrtg/
  seror@agarik.com
- http://192.168.27.1/mrtg/
  ayamura@ayamura.org
- http://192.168.27.1/mrtg/
  steve@hdl.com
- http://192.168.27.1/mrtg/
  martin.och@cs-compex.cz
- http://192.168.27.1/mrtg/
  gaiser@matrix.com.br

- http://192.168.27.1/mrtg/ **freitas@dcc.ufmg.br**
- http://192.168.27.1/mrtg/ **hiroyuki@nucba.ac.jp**
- http://192.168.27.1/mrtg/ **keith@nol.net**
- http://192.168.27.1/mrtg/ **levine@yoyo.org**
- http://192.168.27.1/mrtg/ **web@std.siamu.ac.th**
- http://192.168.27.1/mrtg/ **--trond.kandal@itea.ntnu.no**
- http://192.168.27.1/mrtg/ **dima@chg.ru**
- http://192.168.27.1/mrtg/ **brian@ou.edu**
- http://192.168.27.1/mrtg/ **stefano@unipi.it**
- http://192.168.27.1/mrtg/ **ijliao@ccca.nctu.edu.tw**

Request

```
GET /usage/index.html HTTP/1.1
Referer: http://192.168.27.1/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

Check references for details on how to solve this problem.

References

Anti-spam techniques
https://en.wikipedia.org/wiki/Anti-spam_techniques

SSL/TLS Not Implemented

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE
CWE-319

CVSS2
AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible information disclosure.

http://192.168.27.1/ Verified

Request

```
GET / HTTP/1.1
Referer: http://192.168.27.1/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

A03 Injection

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

Check for apache versions up to 1.3.25, 2.0.38

This alert was generated using only banner information. It may be a false positive.

Apache does not properly calculate buffer size when processing request encoded as 'Chunked'. It's possible to exploit this flaw resulting execution of arbitrary code.

Affected Apache versions (up to 2.0.38 for Apache 2.x and up to 1.3.25 for Apache 1.x).

CWE
CWE-119

CVSS2
AV:N/AC:L/Au:N/C:P/I:P/A:P/E:F/RL:OF/RC:C

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	Partial
Exploitability	Functional exploit exists
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L

Base Score	8.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/S

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	Low
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Code execution.

http://192.168.27.1/

Version detected: Apache/1.3.20 .

Recommendation

Upgrade Apache to the latest version.

References

BID 5033
https://www.securityfocus.com/bid/5033

Apache homepage
http://httpd.apache.org

Apache version older than 1.3.39

This alert was generated using only banner information. It may be a false positive.

Security fixes in Apache version 1.3.39:

- CVE-2006-5752 (cve.mitre.org) mod_status: Fix a possible XSS attack against a site with a public server-status page and ExtendedStatus enabled, for browsers which perform charset "detection". Reported by Stefan Esser. [Joe Orton]
- CVE-2007-3304 (cve.mitre.org) Ensure that the parent process cannot be forced to kill non-child processes by checking scoreboard PID data with parent process privately stored PID data. [Jim Jagielski]

Affected Apache versions (up to 1.3.38).

CWE
CWE-79

CVSS2
AV:N/AC:M/Au:N/C:N/I:P/A:N/E:H/RL:OF/RC:C

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	None
Integrity Impact	Partial
Availability Impact	None
Exploitability	High
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Passive
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Check references for details about each vulnerability.

http://192.168.27.1/

Version detected: Apache/1.3.20 .

Recommendation

Upgrade Apache to the latest version.

References

Apache HTTP Server 1.x announcement
http://archive.apache.org/dist/httpd/CHANGES_1.3.39

Apache homepage
http://httpd.apache.org

Apache version older than 1.3.41

This alert was generated using only banner information. It may be a false positive.

Security fixes in Apache version 1.3.41:

- CVE-2007-6388 (cve.mitre.org) mod_status: Ensure refresh parameter is numeric to prevent a possible XSS attack caused by redirecting to other URLs. Reported by SecurityReason. [Mark Cox]

Security fixes in Apache version 1.3.40:

- CVE-2007-5000 (cve.mitre.org) mod_imap: Fix cross-site scripting issue. Reported by JPCERT. [Joe Orton]
- CVE-2007-3847 (cve.mitre.org) mod_proxy: Prevent reading past the end of a buffer when parsing date-related headers. PR 41144. With Apache 1.3, the denial of service vulnerability applies only to the Windows and NetWare platforms. [Jeff Trawick]

Affected Apache versions (up to 1.3.39).

CWE
CWE-79

CVSS2
AV:N/AC:M/Au:N/C:N/I:P/A:N/E:H/RL:OF/RC:C

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	None
Integrity Impact	Partial
Availability Impact	None
Exploitability	High
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Passive
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Check references for details about each vulnerability.

http://192.168.27.1/

Version detected: Apache/1.3.20 .

Recommendation

Upgrade Apache to the latest version.

References

Apache HTTP Server 1.x announcement
http://archive.apache.org/dist/httpd/CHANGES_1.3.41

Apache homepage
http://httpd.apache.org

Unfiltered header injection in Apache 1.3.34/2.0.57/2.2.1

This version of Apache is vulnerable to HTML injection (including malicious Javascript code) through "Expect" header. Until now it was not classified as a security vulnerability, since an attacker has no way to influence the Expect header to send the victim to a target website. However, according to Amit Klein's paper: "Forging HTTP request headers with Flash" there is a working cross site scripting (XSS) attack against Apache 1.3.34, 2.0.57 and 2.2.1 (as long as the client browser is IE or Firefox, and it supports Flash 6/7+).

Affected Apache versions (up to 1.3.34/2.0.57/2.2.1).

CWE
CWE-79

CVSS2
AV:N/AC:M/Au:N/C:N/I:P/A:N/E:POC/RL:OF/RC:C

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	None
Integrity Impact	Partial
Availability Impact	None
Exploitability	Proof of concept code
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Passive
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user. It is also possible to modify the content of the page presented to the user.

http://192.168.27.1/

Pattern found:

```
<script>alert(12345)</script>
```

Request

```
GET / HTTP/1.1
Expect: <script>alert(12345)</script>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

Upgrade to the latest Apache versions. This flaw has been corrected in Apache versions (1.3.35/2.0.58/2.2.2)

References

Unfiltered Header Injection in Apache 1.3.34/2.0.57/2.2.1
https://www.securityfocus.com/archive/1/433280

Forging HTTP request headers with Flash
https://www.securityfocus.com/archive/1/441014/30/0/threaded

Apache homepage
http://httpd.apache.org/

Apache error log escape sequence injection vulnerability

This alert was generated using only banner information. It may be a false positive.

This version of Apache is vulnerable to escape character sequences injection into error log.This problem may be exploited when a vulnerable terminal emulator is used.

Affected Apache versions (up to 2.0.48 for Apache 2.x and up to 1.3.29 for Apache 1.x).

CWE
CWE-20

CVSS2
AV:N/AC:L/Au:N/C:N/I:P/A:N/E:U/RL:OF/RC:C

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	Partial
Availability Impact	None
Exploitability	Unproven that exploit exists
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N

Base Score	4.7
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible file creation and/or code execution (if vulnerable terminal emulator is present)

http://192.168.27.1/

Version detected: Apache/1.3.20.

Recommendation

Upgrade to the latest version of Apache.

References

BID 9930
https://www.securityfocus.com/bid/9930/

Apache homepage
http://httpd.apache.org

Apache version older than 1.3.28

This alert was generated using only banner information. It may be a false positive.

Multiple vulnerabilities have been found in this version of Apache. You should upgrade to the latest version of Apache.

Affected Apache versions (up to 1.3.27).

CWE
CWE-20

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:P/E:H/RL:OF/RC:C

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	Partial
Exploitability	High
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	Low

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:I

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	Low
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Multiple. Check references for details about every vulnerability.

http://192.168.27.1/

Version detected: Apache/1.3.20 .

Recommendation

Upgrade Apache to the latest version.

References

BID 8226
https://www.securityfocus.com/bid/8226

Apache homepage
http://httpd.apache.org

Apache version older than 1.3.34

This alert was generated using only banner information. It may be a false positive.

Two potential security issues have been fixed in Apache version 1.3.34:

- If a request contains both Transfer-Encoding and Content-Length headers, remove the Content-Length, mitigating some HTTP Request Splitting/Spoofing attacks.
- Added TraceEnable [on|off|extended] per-server directive to alter the behavior of the TRACE method.

Affected Apache versions (up to 1.3.33).

CWE
CWE-20

CVSS2
AV:N/AC:M/Au:N/C:N/I:P/A:N/E:H/RL:OF/RC:C

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	None
Integrity Impact	Partial
Availability Impact	None
Exploitability	High
Remediation Level	Official Fix

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	Low

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI:I

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Passive
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low

Report Confidence	Confirmed

Availability Impact	None

Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Multiple. Check references for details about every vulnerability.

http://192.168.27.1/

Version detected: Apache/1.3.20 .

Recommendation

Upgrade Apache to the latest version.

References

Apache HTTP Server 1.x announcement
http://archive.apache.org/dist/httpd/Announcement1.3.html

Apache homepage
http://httpd.apache.org

A04 Insecure Design

Insecure design is a broad category representing different weaknesses, expressed as "missing or ineffective control design." Insecure design is not the source for all other Top 10 risk categories. There is a difference between insecure design and insecure implementation. We differentiate between design flaws and implementation defects for a reason, they have different root causes and remediation. A secure design can still have implementation defects leading to vulnerabilities that may be exploited. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks. One of the factors that contribute to insecure design is the lack of business risk profiling inherent in the software or system being developed, and thus the failure to determine what level of security design is required.

Content Security Policy (CSP) Not Implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

CWE
CWE-1021

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None

Integrity Impact	None
Availability Impact	None

Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

http://192.168.27.1/

Paths without CSP header:

- http://192.168.27.1/
- http://192.168.27.1/manual/mod/core.html
- http://192.168.27.1/usage/index.html
- http://192.168.27.1/icons/
- http://192.168.27.1/index.html
- http://192.168.27.1/manual/index.html
- http://192.168.27.1/usage/
- http://192.168.27.1/manual/mod/
- http://192.168.27.1/usage/usage_200909.html
- http://192.168.27.1/manual/
- http://192.168.27.1/icons/small/
- http://192.168.27.1/manual/mod/mod_perl/
- http://192.168.27.1/mrtg/
- http://192.168.27.1/manual/mod/mod_ssl/
- http://192.168.27.1/mrtg/es/
- http://192.168.27.1/mrtg/cfgmaker.html
- http://192.168.27.1/mrtg/contrib.html
- http://192.168.27.1/mrtg/faq.html
- http://192.168.27.1/mrtg/forum.html
- http://192.168.27.1/mrtg/indexmaker.html
- http://192.168.27.1/manual/mod/mod_ssl/ssl_overview.html

Request

```
GET / HTTP/1.1
Referer: http://192.168.27.1/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
```

```
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

Content Security Policy (CSP)
https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

Implementing Content Security Policy
https://hacks.mozilla.org/2016/02/implementing-content-security-policy/

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

CWE
CWE-1021

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

http://192.168.27.1/

Locations without Permissions-Policy header:

- http://192.168.27.1/
- http://192.168.27.1/manual/mod/core.html
- http://192.168.27.1/usage/index.html
- http://192.168.27.1/icons/
- http://192.168.27.1/index.html
- http://192.168.27.1/manual/index.html
- http://192.168.27.1/usage/
- http://192.168.27.1/manual/mod/
- http://192.168.27.1/usage/usage_200909.html
- http://192.168.27.1/manual/
- http://192.168.27.1/icons/small/
- http://192.168.27.1/manual/mod/mod_perl/
- http://192.168.27.1/mrtg/
- http://192.168.27.1/manual/mod/mod_ssl/
- http://192.168.27.1/mrtg/es/
- http://192.168.27.1/mrtg/cfgmaker.html
- http://192.168.27.1/mrtg/contrib.html
- http://192.168.27.1/mrtg/faq.html
- http://192.168.27.1/mrtg/forum.html

- http://192.168.27.1/mrtg/indexmaker.html
- http://192.168.27.1/manual/mod/mod_ssl/ssl_overview.html

Request

```
GET / HTTP/1.1
Referer: http://192.168.27.1/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

References

Permissions-Policy / Feature-Policy (MDN)
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Permissions Policy (W3C)
https://www.w3.org/TR/permissions-policy-1/

A05 Security Misconfiguration

Security misconfiguration is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securly configured, but they must be patched and upgraded in a timely fashion.

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

CWE
CWE-538

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

http://192.168.27.1/ Verified

Folders with directory listing enabled:

- http://192.168.27.1/manual/
- http://192.168.27.1/manual/mod/
- http://192.168.27.1/icons/

- http://192.168.27.1/icons/small/
- http://192.168.27.1/manual/mod/mod_perl/

Request

```
GET /manual/ HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

References

CWE-548: Exposure of Information Through Directory Listing
https://cwe.mitre.org/data/definitions/548.html

Webalizer script

The Webalizer is a fast, free web server log file analysis program. It produces highly detailed, easily configurable usage reports in HTML format, for viewing with a standard web browser.

It's recommended to restrict access to this directory as it may contain sensitive information (test scripts, administrative interfaces, session tokens sent via GET, ...). This kind of information may help an attacker to learn more about the structure of your website and can be used to conduct further attacks.

CWE
CWE-538

CVSS2
AV:N/AC:L/Au:N/C:P/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

Base Score	5.8
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	Low
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible sensitive information disclosure.

http://192.168.27.1/usage/index.html

Request

```
GET /usage/index.html HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

Restrict (or password protect) the access to directory or make it accessible only on the local interface.

References

Wikipedia: Webalizer
https://en.wikipedia.org/wiki/Webalizer

TRACE/TRACK Method Detected

HTTP TRACE method is enabled on this web server. In the presence of other cross-domain vulnerabilities in web browsers, sensitive header information could be read from any domains that support the HTTP TRACE method.

CWE
CWE-489

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Attackers may abuse HTTP TRACE functionality to gain access to information in HTTP headers such as cookies and authentication data.

http://192.168.27.1/

Request

```
TRACE /BxSWbRBuW7 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

Disable TRACE Method on the web server.

References

W3C - RFC 2616
http://www.w3.org/Protocols/rfc2616/rfc2616-sec9.html

US-CERT VU#867593
https://www.kb.cert.org/vuls/id/867593/

Cross-site tracing (XST)
https://www.cgisecurity.com/lib/WH-WhitePaper_XST_ebook.pdf

Content Security Policy (CSP) Not Implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

CWE
CWE-1021

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

http://192.168.27.1/

Paths without CSP header:

- http://192.168.27.1/
- http://192.168.27.1/manual/mod/core.html
- http://192.168.27.1/usage/index.html
- http://192.168.27.1/icons/
- http://192.168.27.1/index.html
- http://192.168.27.1/manual/index.html
- http://192.168.27.1/usage/
- http://192.168.27.1/manual/mod/
- http://192.168.27.1/usage/usage_200909.html
- http://192.168.27.1/manual/
- http://192.168.27.1/icons/small/

- http://192.168.27.1/manual/mod/mod_perl/
- http://192.168.27.1/mrtg/
- http://192.168.27.1/manual/mod/mod_ssl/
- http://192.168.27.1/mrtg/es/
- http://192.168.27.1/mrtg/cfgmaker.html
- http://192.168.27.1/mrtg/contrib.html
- http://192.168.27.1/mrtg/faq.html
- http://192.168.27.1/mrtg/forum.html
- http://192.168.27.1/mrtg/indexmaker.html
- http://192.168.27.1/manual/mod/mod_ssl/ssl_overview.html

Request

```
GET / HTTP/1.1
Referer: http://192.168.27.1/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

Content Security Policy (CSP)
https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

Implementing Content Security Policy
https://hacks.mozilla.org/2016/02/implementing-content-security-policy/

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

CWE
CWE-1021

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None

Availability Impact to the Subsequent System	None

Impact

http://192.168.27.1/

Locations without Permissions-Policy header:

- http://192.168.27.1/
- http://192.168.27.1/manual/mod/core.html
- http://192.168.27.1/usage/index.html
- http://192.168.27.1/icons/
- http://192.168.27.1/index.html
- http://192.168.27.1/manual/index.html
- http://192.168.27.1/usage/
- http://192.168.27.1/manual/mod/
- http://192.168.27.1/usage/usage_200909.html
- http://192.168.27.1/manual/
- http://192.168.27.1/icons/small/
- http://192.168.27.1/manual/mod/mod_perl/
- http://192.168.27.1/mrtg/
- http://192.168.27.1/manual/mod/mod_ssl/
- http://192.168.27.1/mrtg/es/
- http://192.168.27.1/mrtg/cfgmaker.html
- http://192.168.27.1/mrtg/contrib.html
- http://192.168.27.1/mrtg/faq.html
- http://192.168.27.1/mrtg/forum.html
- http://192.168.27.1/mrtg/indexmaker.html
- http://192.168.27.1/manual/mod/mod_ssl/ssl_overview.html

Request

```
GET / HTTP/1.1
Referer: http://192.168.27.1/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

References

Permissions-Policy / Feature-Policy (MDN)
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Permissions Policy (W3C)
https://www.w3.org/TR/permissions-policy-1/

Insecure HTTP Usage

It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.

CWE

CWE-16

CVSS2

AV:N/AC:L/Au:N/C:N/I:N/A:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None

CVSS3

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

Base Score	0.0
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None

Availability Impact	None

Integrity Impact	None
Availability Impact	None

Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

In some circumstances, it could be used for a man-in-the-middle (MitM) attack

http://192.168.27.1/

Request

```
GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information

References

HTTP Redirections
https://infosec.mozilla.org/guidelines/web_security#http-redirections

A06 Vulnerable and Outdated Components

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

Check for apache versions up to 1.3.25, 2.0.38

This alert was generated using only banner information. It may be a false positive.

Apache does not properly calculate buffer size when processing request encoded as 'Chunked'. It's possible to exploit this flaw resulting execution of arbitrary code.

Affected Apache versions (up to 2.0.38 for Apache 2.x and up to 1.3.25 for Apache 1.x).

CWE
CWE-119

CVSS2
AV:N/AC:L/Au:N/C:P/I:P/A:P/E:F/RL:OF/RC:C

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	Partial
Exploitability	Functional exploit exists

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L

Base Score	8.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/S

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	Low

Remediation Level	Official Fix
Report Confidence	Confirmed

Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Code execution.

http://192.168.27.1/

Version detected: Apache/1.3.20 .

Recommendation

Upgrade Apache to the latest version.

References

BID 5033
https://www.securityfocus.com/bid/5033

Apache homepage
http://httpd.apache.org

Apache error log escape sequence injection vulnerability

This alert was generated using only banner information. It may be a false positive.

This version of Apache is vulnerable to escape character sequences injection into error log.This problem may be exploited when a vulnerable terminal emulator is used.

Affected Apache versions (up to 2.0.48 for Apache 2.x and up to 1.3.29 for Apache 1.x).

CWE
CWE-20

CVSS2
AV:N/AC:L/Au:N/C:N/I:P/A:N/E:U/RL:OF/RC:C

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	Partial
Availability Impact	None
Exploitability	Unproven that exploit exists
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N

Base Score	4.7
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible file creation and/or code execution (if vulnerable terminal emulator is present)

http://192.168.27.1/

Version detected: Apache/1.3.20.

Recommendation

Upgrade to the latest version of Apache.

References

BID 9930
https://www.securityfocus.com/bid/9930/

Apache homepage
http://httpd.apache.org

Apache httpd remote denial of service

A denial of service vulnerability has been found in the way the multiple overlapping ranges are handled by the Apache HTTPD server:

http://seclists.org/fulldisclosure/2011/Aug/175

An attack tool is circulating in the wild. Active use of this tools has been observed. The attack can be done remotely and with a modest number of requests can cause very significant memory and CPU usage on the server.

This alert was generated using only banner information. It may be a false positive.

Affected Apache versions (1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19).

CWE
CWE-399

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	Complete
Exploitability	Functional exploit exists
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	Low

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI

Base Score	8.7
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	High
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Remote Denial of Service

http://192.168.27.1/

Version detected: Apache/1.3.20 .

Recommendation

Upgrade to the latest version of Apache HTTP Server (2.2.20 or later), available from the Apache HTTP Server Project Web site.

References

CVE-2011-3192
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192

Apache HTTPD Security ADVISORY
http://mail-archives.apache.org/mod_mbox/httpd-announce/201108.mbox/%3C20110824161640.122D387DD@minotaur.apache.org%3E

Apache httpd Remote Denial of Service (memory exhaustion)
https://www.exploit-db.com/exploits/17696

Apache version older than 1.3.27

This alert was generated using only banner information. It may be a false positive.

Multiple vulnerabilities have been found in this version of Apache. You should upgrade to the latest version of Apache.

Affected Apache versions (up to 1.3.26).

CWE
CWE-119

CVSS2
AV:N/AC:L/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	Partial
Exploitability	Proof of concept code
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Base Score	7.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	Low
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Multiple. Check references for details about every vulnerability.

http://192.168.27.1/

Version detected: Apache/1.3.20 .

Recommendation

Upgrade Apache to the latest version.

References

BID 5847
https://www.securityfocus.com/bid/5847

BID 5884
https://www.securityfocus.com/bid/5884

BID 5995
https://www.securityfocus.com/bid/5995

BID 5996
https://www.securityfocus.com/bid/5996

Apache homepage
http://httpd.apache.org

Apache version older than 1.3.28

This alert was generated using only banner information. It may be a false positive.

Multiple vulnerabilities have been found in this version of Apache. You should upgrade to the latest version of Apache.

Affected Apache versions (up to 1.3.27).

CWE
CWE-20

CVSS2
AV:N/AC:L/Au:N/C:N/I:N/A:P/E:H/RL:OF/RC:C

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	None
Integrity Impact	None
Availability Impact	Partial
Exploitability	High
Remediation Level	Official Fix
Report Confidence	Confirmed

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	Low

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	None
Availability Impact to the Vulnerable System	Low
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Multiple. Check references for details about every vulnerability.

http://192.168.27.1/

Version detected: Apache/1.3.20 .

Recommendation

Upgrade Apache to the latest version.

References

BID 8226
https://www.securityfocus.com/bid/8226

Apache homepage
http://httpd.apache.org

Apache version older than 1.3.29

This alert was generated using only banner information. It may be a false positive.

Multiple vulnerabilities have been found in this version of Apache. You should upgrade to the latest version of Apache.

Affected Apache versions (up to 1.3.28).

CWE

CWE-119

CVSS2

AV:L/AC:L/Au:N/C:C/I:C/A:C/E:POC/RL:OF/RC:C

Access Vector	Local
Access Complexity	Low
Authentication	None
Confidentiality	Complete
Integrity Impact	Complete
Availability Impact	Complete
Exploitability	Proof of concept code
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Base Score	8.4
Attack Vector	Local
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity Impact	High
Availability Impact	High

CVSS4

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/S

Base Score	8.6
Attack Vector	Local
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	High
Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	High
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Multiple. Check references for details about every vulnerability.

http://192.168.27.1/

Version detected: Apache/1.3.20 .

Recommendation

Upgrade Apache to the latest version.

References

CAN-2003-0542
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0542

Apache homepage
http://httpd.apache.org

Apache version older than 1.3.31

This alert was generated using only banner information. It may be a false positive.

Multiple vulnerabilities have been found in this version of Apache. You should upgrade to the latest version of Apache.

Affected Apache versions (up to 1.3.30).

CWE
CWE-264

CVSS2
AV:N/AC:L/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	Partial
Exploitability	Proof of concept code
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Base Score	7.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	Low

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N

Base Score	6.9
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	None
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	Low
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Multiple. Check references for details about every vulnerability.

http://192.168.27.1/

Version detected: Apache/1.3.20 .

Recommendation

Upgrade Apache to the latest version.

References

CAN-2003-0987
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0987

CAN-2003-0020
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0020

CAN-2004-0174
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0174

CAN-2003-0993
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0993

Apache homepage
http://httpd.apache.org

Apache version older than 1.3.34

This alert was generated using only banner information. It may be a false positive.

Two potential security issues have been fixed in Apache version 1.3.34:

- If a request contains both Transfer-Encoding and Content-Length headers, remove the Content-Length, mitigating some HTTP Request Splitting/Spoofing attacks.
- Added TraceEnable [on|off|extended] per-server directive to alter the behavior of the TRACE method.

Affected Apache versions (up to 1.3.33).

CWE
CWE-20

CVSS2
AV:N/AC:M/Au:N/C:N/I:P/A:N/E:H/RL:OF/RC:C

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	None
Integrity Impact	Partial
Availability Impact	None
Exploitability	High
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI:I

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Passive
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Multiple. Check references for details about every vulnerability.

http://192.168.27.1/

Version detected: Apache/1.3.20 .

Recommendation

Upgrade Apache to the latest version.

References

Apache HTTP Server 1.x announcement
http://archive.apache.org/dist/httpd/Announcement1.3.html

Apache homepage
http://httpd.apache.org

Apache version older than 1.3.37

This alert was generated using only banner information. It may be a false positive.

Security fixes in Apache version 1.3.37:

- CVE-2006-3747 (cve.mitre.org) mod_rewrite: Fix an off-by-one security problem in the ldap scheme handling. For some RewriteRules this could lead to a pointer being written out of bounds. Reported by Mark Dowd of McAfee. [Mark Cox]

Affected Apache versions (up to 1.3.36).

CWE
CWE-189

CVSS2
AV:N/AC:H/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C

Access Vector	Network
Access Complexity	High
Authentication	None
Confidentiality	Complete
Integrity Impact	Complete
Availability Impact	Complete
Exploitability	Functional exploit exists
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3
CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Base Score	7.5
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	High
Integrity Impact	High
Availability Impact	High

CVSS4
CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:

Base Score	7.5
Attack Vector	Network
Attack Complexity	High
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	High
Integrity Impact to the Vulnerable System	High
Availability Impact to the Vulnerable System	High
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Check references for details about each vulnerability.

http://192.168.27.1/

Version detected: Apache/1.3.20 .

Recommendation

Upgrade Apache to the latest version.

References

Apache HTTP Server 1.x announcement
http://archive.apache.org/dist/httpd/CHANGES_1.3.37

Apache homepage
http://httpd.apache.org

Apache version older than 1.3.39

This alert was generated using only banner information. It may be a false positive.

Security fixes in Apache version 1.3.39:

- CVE-2006-5752 (cve.mitre.org) mod_status: Fix a possible XSS attack against a site with a public server-status page and ExtendedStatus enabled, for browsers which perform charset "detection". Reported by Stefan Esser. [Joe Orton]
- CVE-2007-3304 (cve.mitre.org) Ensure that the parent process cannot be forced to kill non-child processes by checking scoreboard PID data with parent process privately stored PID data. [Jim Jagielski]

Affected Apache versions (up to 1.3.38).

CWE
CWE-79

CVSS2
AV:N/AC:M/Au:N/C:N/I:P/A:N/E:H/RL:OF/RC:C

Access Vector	Network

CVSS3
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Base Score	5.3

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI:

Base Score	5.3

Access Complexity	Medium
Authentication	None
Confidentiality	None
Integrity Impact	Partial
Availability Impact	None
Exploitability	High
Remediation Level	Official Fix
Report Confidence	Confirmed

Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Passive
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Check references for details about each vulnerability.

http://192.168.27.1/

Version detected: Apache/1.3.20 .

Recommendation

Upgrade Apache to the latest version.

References

Apache HTTP Server 1.x announcement
http://archive.apache.org/dist/httpd/CHANGES_1.3.39

Apache homepage
http://httpd.apache.org

Apache version older than 1.3.41

This alert was generated using only banner information. It may be a false positive.

Security fixes in Apache version 1.3.41:

- CVE-2007-6388 (cve.mitre.org) mod_status: Ensure refresh parameter is numeric to prevent a possible XSS attack caused by redirecting to other URLs. Reported by SecurityReason. [Mark Cox]

Security fixes in Apache version 1.3.40:

- CVE-2007-5000 (cve.mitre.org) mod_imap: Fix cross-site scripting issue. Reported by JPCERT. [Joe Orton]
- CVE-2007-3847 (cve.mitre.org) mod_proxy: Prevent reading past the end of a buffer when parsing date-related headers. PR 41144. With Apache 1.3, the denial of service vulnerability applies only to the Windows and NetWare platforms. [Jeff Trawick]

Affected Apache versions (up to 1.3.39).

CWE

CWE-79

CVSS2

AV:N/AC:M/Au:N/C:N/I:P/A:N/E:H/RL:OF/RC:C

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	None
Integrity Impact	Partial
Availability Impact	None
Exploitability	High

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N/SI

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Passive
Confidentiality Impact to the Vulnerable System	None

Remediation Level	Official Fix
Report Confidence	Confirmed

Integrity Impact	Low
Availability Impact	None

Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Check references for details about each vulnerability.

http://192.168.27.1/

Version detected: Apache/1.3.20 .

Recommendation

Upgrade Apache to the latest version.

References

Apache HTTP Server 1.x announcement
http://archive.apache.org/dist/httpd/CHANGES_1.3.41

Apache homepage
http://httpd.apache.org

Apache version up to 1.3.33 htpasswd local overflow

This alert was generated using only banner information. It may be a false positive.

A buffer overflow vulnerability exists in the htpasswd utility included with Apache. The vulnerability is due to improper bounds checking when copying user-supplied 'user' data into local buffers.

Affected Apache versions (up to 1.3.33).

CWE

CWE-119

CVSS2

AV:L/AC:L/Au:N/C:C/I:C/A:C/E:POC/RL:OF/RC:C

Access Vector	Local
Access Complexity	Low
Authentication	None
Confidentiality	Complete
Integrity Impact	Complete
Availability Impact	Complete
Exploitability	Proof of concept code
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N

Base Score	6.1
Attack Vector	Local
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	High
Integrity Impact	Low
Availability Impact	None

CVSS4

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:L/VA:N/SC:N/SI

Base Score	6.8
Attack Vector	Local
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	High
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Since the program is not setuid, this vulnerability does not have a local impact. However, this may be an issue if the software is called from a CGI script. An attacker may be able to supply malformed data to the program which will cause the overflow to occur.

http://192.168.27.1/

Version detected: Apache/1.3.20 .

Recommendation

Make sure htpasswd does not run setuid and is not accessible through any CGI scripts.

References

BID 13777
https://www.securityfocus.com/bid/13777

BID 13778
https://www.securityfocus.com/bid/13778

FlowSecurity.org: Local Stack Overflow on htpasswd apache 1.3.31 advisory
https://seclists.org/fulldisclosure/2004/Sep/565

Unfiltered header injection in Apache 1.3.34/2.0.57/2.2.1

This version of Apache is vulnerable to HTML injection (including malicious Javascript code) through "Expect" header. Until now it was not classified as a security vulnerability, since an attacker has no way to influence the Expect header to send the victim to a target website. However, according to Amit Klein's paper: "Forging HTTP request headers with Flash" there is a working cross site scripting (XSS) attack against Apache 1.3.34, 2.0.57 and 2.2.1 (as long as the client browser is IE or Firefox, and it supports Flash 6/7+).

Affected Apache versions (up to 1.3.34/2.0.57/2.2.1).

CWE

CWE-79

CVSS2

AV:N/AC:M/Au:N/C:N/I:P/A:N/E:POC/RL:OF/RC:C

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	None
Integrity Impact	Partial
Availability Impact	None
Exploitability	Proof of concept code
Remediation Level	Official Fix
Report Confidence	Confirmed

CVSS3

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

CVSS4

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:N/VI:L/VA:N/SC:N

Base Score	5.3
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Passive
Confidentiality Impact to the Vulnerable System	None
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Malicious users may inject JavaScript, VBScript, ActiveX, HTML or Flash to fool a user in order to gather data from them. An attacker can steal the session cookie and take over the account, impersonating the user. It is also possible to modify the content of the page presented to the user.

http://192.168.27.1/

Pattern found:

```
<script>alert(12345)</script>
```

Request

```
GET / HTTP/1.1
Expect: <script>alert(12345)</script>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

Upgrade to the latest Apache versions. This flaw has been corrected in Apache versions (1.3.35/2.0.58/2.2.2)

References

Unfiltered Header Injection in Apache 1.3.34/2.0.57/2.2.1
https://www.securityfocus.com/archive/1/433280

Forging HTTP request headers with Flash
https://www.securityfocus.com/archive/1/441014/30/0/threaded

Apache homepage
http://httpd.apache.org/

A07 Identification and Authentication Failures

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

SSL/TLS Not Implemented

This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.

CWE
CWE-319

CVSS2
AV:N/AC:M/Au:N/C:P/I:P/A:N

Access Vector	Network
Access Complexity	Medium
Authentication	None
Confidentiality	Partial
Integrity Impact	Partial
Availability Impact	None

CVSS3
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

Base Score	5.4
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	Low
Availability Impact	None

CVSS4
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

Base Score	5.1
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	None
User Interaction	Active
Confidentiality Impact to the Vulnerable System	Low
Integrity Impact to the Vulnerable System	Low
Availability Impact to the Vulnerable System	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

Possible information disclosure.

http://192.168.27.1/ Verified

Request

```
GET / HTTP/1.1
Referer: http://192.168.27.1/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.27.1
Connection: Keep-alive
```

Recommendation

The site should send and receive data over a secure (HTTPS) connection.

A08 Software and Data Integrity Failures

Software and data integrity failures relate to code and infrastructure that does not protect against integrity violations. An example of this is where an application relies upon plugins, libraries, or modules from untrusted sources, repositories, and content delivery networks (CDNs). An insecure CI/CD pipeline can introduce the potential for unauthorized access, malicious code, or system compromise. Lastly, many applications now include auto-update functionality, where updates are downloaded without sufficient integrity verification and applied to the previously trusted application. Attackers could potentially upload their own updates to be distributed and run on all installations. Another example is where objects or data are encoded or serialized into a structure that an attacker can see and modify is vulnerable to insecure deserialization.

No alerts in this category

A09 Security Logging and Monitoring Failures

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systesm, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

No alerts in this category

A10 Server-Side Request Forgery

SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control list (ACL).

No alerts in this category

Coverage

- http://192.168.27.1
  - icons
    - Inputs
      - GET D, S, M, N
    - small
      - Inputs
        - GET D, S, M, N
  - manual
    - Inputs
      - GET D, S, M, N
    - images
    - mod
      - Inputs
        - GET D, S, M, N
      - mod_perl
      - mod_ssl
        - index.html
        - ssl_compat.html
          - #fragments
            - ToC1
            - ToC2
            - ToC3
            - table1
            - table2
            - table3
        - ssl_faq.html
          - #fragments
            - ToC1
            - ToC10
            - ToC11
            - ToC12
            - ToC13
            - ToC14
            - ToC15
            - ToC16
            - ToC17
            - ToC18
            - ToC19
            - ToC2
            - ToC20
            - ToC21
            - ToC22
            - ToC23
            - ToC24
            - ToC25
            - ToC26
            - ToC27

ToC28
ToC29
ToC3
ToC30
ToC31
ToC32
ToC33
ToC34
ToC35
ToC36
ToC37
ToC38
ToC39
ToC4
ToC40
ToC41
ToC42
ToC43
ToC44
ToC45
ToC46
ToC47
ToC48
ToC49
ToC5
ToC50
ToC51
ToC52
ToC53
ToC54
ToC55
ToC56
ToC6
ToC7
ToC8
ToC9
ssl_glossary.html
ssl_howto.html
#fragments
ToC1
ToC10
ToC2
ToC3
ToC4
ToC5
ToC6
ToC7
ToC8
ToC9

- ssl_intro.html
  - #fragments
    - AC96
    - MIME
    - PKCS
    - SSL2
    - SSL3
    - TLS1
    - ToC1
    - ToC10
    - ToC11
    - ToC12
    - ToC13
    - ToC14
    - ToC15
    - ToC16
    - ToC17
    - ToC18
    - ToC19
    - ToC2
    - ToC3
    - ToC4
    - ToC5
    - ToC6
    - ToC7
    - ToC8
    - ToC9
    - X208
    - X509
    - figure1
    - figure2
    - figure3
    - table1
    - table2
    - table3
    - table4
- ssl_overview.html
  - #fragments
    - figure1
- ssl_reference.html
  - #fragments
    - SSLCACertificatePath
    - SSLCARevocationPath
    - SSLCertificateFile
    - SSLCertificateKeyFile
    - ToC1
    - ToC10
    - ToC11
    - ToC12

- ToC13
- ToC14
- ToC15
- ToC16
- ToC17
- ToC18
- ToC19
- ToC2
- ToC20
- ToC21
- ToC22
- ToC23
- ToC24
- ToC25
- ToC26
- ToC3
- ToC4
- ToC5
- ToC6
- ToC7
- ToC8
- ToC9
- table1
- table2
- table3
- table4

core.html
- #fragments
  - documentroot

directive-dict.html
- #fragments
  - Compatibility
  - Context
  - Default
  - Module
  - Override
  - PerlSyntax
  - Status
  - Syntax

mod_log_config.html
- #fragments
  - formats

mod_perl.html
- #fragments
  - ./Perl.
  - .Perl.
  - =cut
  - =pod
  - PerlAccessHandler

- PerlAuthenHandler
- PerlAuthzHandler
- PerlChildExitHandler
- PerlChildInitHandler
- PerlCleanupHandler
- PerlDispatchHandler
- PerlFixupHandler
- PerlFreshRestart
- PerlHandler
- PerlHeaderParserHandler
- PerlInitHandler
- PerlLogHandler
- PerlModule
- PerlPassEnv
- PerlPostReadRequestHandler
- PerlRequire
- PerlRestartHandler
- PerlScript
- PerlSendHeader
- PerlSetEnv
- PerlSetVar
- PerlSetupEnv
- PerlTaintCheck
- PerlTransHandler
- PerlTypeHandler
- PerlWarn
- __END__

- index.html

- mrtg
  - es
  - cfgmaker.html
  - contrib.html
  - faq.html
  - forum.html
  - indexmaker.html
  - logfile.html
  - mibhelp.html
  - mrtg-rrd.html
  - mrtg.html
  - mrtglib.html
  - nt-guide.html
  - reference.html
  - squid.html
  - unix-guide.html
  - webserver.html
- usage
  - index.html
  - usage_200909.html
    - #fragments

- DAYSTATS
- HOURSTATS
- TOPAGENTS
- TOPCTRYS
- TOPENTRY
- TOPEXIT
- TOPREFS
- TOPSEARCH
- TOPSITES
- TOPURLS

index.html