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://10.136.108.237/
Scan Type	Full Scan
Start Time	Nov 12, 2025, 5:51:17 PM GMT
Scan Duration	57 minutes
Requests	122147
Average Response Time	1ms
Maximum Response Time	38340ms
Application Build	v24.6.240626115
Authentication Profile	-

Compliance at a Glance

CATEGORY	
9	A01 Broken Access Control
10	A02 Cryptographic Failures
7	A03 Injection
2	A04 Insecure Design
6	A05 Security Misconfiguration
6	A06 Vulnerable and Outdated Components
3	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.

Database User Has Admin Privileges

Acunetix detected the Database User Has Admin Privileges.
This issue has been confirmed by checking the connection privileges via an identified SQL injection vulnerability in the application.

CWE
CWE-267

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

Access Vector	Network
Access Complexity	High
Authentication	None
Confidentiality	Complete
Integrity Impact	Complete
Availability Impact	Complete

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

Base Score	9
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	High
Integrity Impact	High
Availability Impact	High

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

Base Score	9.2
Attack Vector	Network
Attack Complexity	High
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

This can allow an attacker to gain extra privileges via SQL injection attacks. Here is the list of attacks that the attacker might carry out:

- Gain full access to the database server.
- Gain a reverse shell to the database server and execute commands on the underlying operating system.
- Access the database with full permissions, where it may be possible to read, update or delete arbitrary data from the database.
- Depending on the platform and the database system user, an attacker might carry out a privilege escalation attack to gain administrator access to the target system.

http://10.136.108.237/index.php

Database name: **webapp**

Request

```
POST /index.php HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://10.136.108.237/
Content-Type: application/x-www-form-urlencoded
Content-Length: 82
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: 10.136.108.237
Connection: Keep-alive

btnLogin=Login&psw=-1'%20OR%203*2*1=6%20AND%20000693=000693%20--%20&uname=RDFYjolf
```

http://10.136.108.237/index.php

Database name: **webapp**

Request

```
POST /index.php HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://10.136.108.237/
Content-Type: application/x-www-form-urlencoded
Content-Length: 90
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: 10.136.108.237
Connection: Keep-alive

btnLogin=Login&psw=u]H[ww6KrA9F.x-F&uname=-1'%20OR%203*2*1=6%20AND%20000549=000549%20--%20
```

Recommendation

Create a database user with the least possible permissions for your application and connect to the database with that user. Always follow the principle of providing the least privileges for all users and applications.

References

Authorization and Permissions in SQL Server (ADO.NET)
https://msdn.microsoft.com/en-us/library/bb669084.aspx

Wikipedia - Principle of Least Privilege
https://en.wikipedia.org/wiki/Principle_of_least_privilege

How to Use MySQL GRANT to Grant Privileges to Account
http://www.mysqltutorial.org/mysql-grant.aspx

[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://10.136.108.237/

Pages with internal IPs:

- http://10.136.108.237/manual/ssl/ssl_faq.html
  192.168.1.1

Request

```
GET /manual/ssl/ssl_faq.html HTTP/1.1
Referer: http://10.136.108.237/manual/ssl/
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: 10.136.108.237
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

[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://10.136.108.237/

Pages with paths being disclosed:

- http://10.136.108.237/manual/howto/auth.html
  >/usr/local/apache/htdocs

Request

```
GET /manual/howto/auth.html HTTP/1.1
Referer: http://10.136.108.237/manual/
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: 10.136.108.237
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://10.136.108.237/

Pages with paths being disclosed:

- http://10.136.108.237/manual/platform/netware.html
  S:\APACHE2

Request

```
GET /manual/platform/netware.html HTTP/1.1
Referer: http://10.136.108.237/manual/
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: 10.136.108.237
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

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

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

Error messages information about an application's internal workings may be used to escalate attacks.

http://10.136.108.237/

Request

```
GET /PAsRNR5VaB 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: 10.136.108.237
Connection: Keep-alive
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

Custom Error Responses (Apache HTTP Server)
https://httpd.apache.org/docs/current/custom-error.html

server_tokens (Nginx)
http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

Remove Unwanted HTTP Response Headers (Microsoft IIS)
https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/

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://10.136.108.237/

Emails found:

- http://10.136.108.237/manual/ssl/ssl_faq.html
  modssl-users@modssl.org
- http://10.136.108.237/manual/ssl/ssl_faq.html
  rse@engelschall.com
- http://10.136.108.237/manual/ssl/ssl_faq.html
  ben@algroup.co.uk

Request

```
GET /manual/ssl/ssl_faq.html HTTP/1.1
Referer: http://10.136.108.237/manual/ssl/
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: 10.136.108.237
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 httpOnly cookie disclosure

Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.

Affected Apache versions (up to 2.0.21).

CWE
CWE-264

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

Access Vector	Network
Access Complexity	Medium

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

Base Score	4.3
Attack Vector	Network

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

Base Score	5.1
Attack Vector	Network

Authentication	None
Confidentiality	Partial
Integrity Impact	None
Availability Impact	None
Exploitability	Functional exploit exists
Remediation Level	Official Fix
Report Confidence	Confirmed

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

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	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

Information disclosure.

http://10.136.108.237/

Pattern found:

```
<pre>
Cookie: testingCookie=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Request

```
GET / HTTP/1.1
Cookie:
testingCookie=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAA
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: 10.136.108.237
Connection: Keep-alive
```

Recommendation

Upgrade Apache 2.x to the latest version. Apache 2.2.22 is the first version that fixed this issue.

References

[Fixed in Apache httpd 2.2.22](http://httpd.apache.org/security/vulnerabilities_22.html)
http://httpd.apache.org/security/vulnerabilities_22.html

[Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability](https://www.securityfocus.com/bid/51706)
https://www.securityfocus.com/bid/51706

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://10.136.108.237/ Verified

Folders with directory listing enabled:

- http://10.136.108.237/manual/style/css/

Request

```
GET /manual/style/css/ 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: 10.136.108.237
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

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).

Apache httpOnly cookie disclosure

Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.

Affected Apache versions (up to 2.0.21).

CWE
CWE-264

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

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

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

Base Score	4.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

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

Information disclosure.

http://10.136.108.237/

Pattern found:

```
<pre>
Cookie: testingCookie=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Request

```
GET / HTTP/1.1
Cookie:
testingCookie=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAA
```

```
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: 10.136.108.237
Connection: Keep-alive
```

Recommendation

Upgrade Apache 2.x to the latest version. Apache 2.2.22 is the first version that fixed this issue.

References

Fixed in Apache httpd 2.2.22
http://httpd.apache.org/security/vulnerabilities_22.html

Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
https://www.securityfocus.com/bid/51706

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://10.136.108.237/ Verified

Folders with directory listing enabled:

- http://10.136.108.237/manual/style/css/

Request

```
GET /manual/style/css/ 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: 10.136.108.237
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

[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://10.136.108.237/

Pages with internal IPs:

- http://10.136.108.237/manual/ssl/ssl_faq.html
  192.168.1.1

Request

```
GET /manual/ssl/ssl_faq.html HTTP/1.1
Referer: http://10.136.108.237/manual/ssl/
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: 10.136.108.237
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

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://10.136.108.237/

Request

```
TRACE /q06im521jZ 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: 10.136.108.237
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

Version Disclosure (PHP)

The web server is sending the X-Powered-By: response headers, revealing the PHP version.

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: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

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/E:P

Base Score	5.5
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	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

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

http://10.136.108.237/

Version detected: **PHP/4.3.9**.

Recommendation

Configure your web server to prevent information leakage from its HTTP response.

References

PHP Documentation: header_remove()
https://www.php.net/manual/en/function.header-remove.php

PHP Documentation: php.ini directive expose_php
https://www.php.net/manual/en/ini.core.php#ini.expose-php

[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://10.136.108.237/

Pages with paths being disclosed:

- http://10.136.108.237/manual/howto/auth.html
  >/usr/local/apache/htdocs

Request

```
GET /manual/howto/auth.html HTTP/1.1
Referer: http://10.136.108.237/manual/
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: 10.136.108.237
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://10.136.108.237/

Pages with paths being disclosed:

- http://10.136.108.237/manual/platform/netware.html
  S:\APACHE2

Request

```
GET /manual/platform/netware.html HTTP/1.1
Referer: http://10.136.108.237/manual/
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: 10.136.108.237
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

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

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

Error messages information about an application's internal workings may be used to escalate attacks.

http://10.136.108.237/

Request

```
GET /PAsRNR5VaB 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: 10.136.108.237
Connection: Keep-alive
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

Custom Error Responses (Apache HTTP Server)
https://httpd.apache.org/docs/current/custom-error.html

server_tokens (Nginx)
http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

Remove Unwanted HTTP Response Headers (Microsoft IIS)

https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/

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://10.136.108.237/

Emails found:

- http://10.136.108.237/manual/ssl/ssl_faq.html
  modssl-users@modssl.org
- http://10.136.108.237/manual/ssl/ssl_faq.html
  rse@engelschall.com
- http://10.136.108.237/manual/ssl/ssl_faq.html
  ben@algroup.co.uk

Request

```
GET /manual/ssl/ssl_faq.html HTTP/1.1
Referer: http://10.136.108.237/manual/ssl/
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: 10.136.108.237
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://10.136.108.237/ Verified

Request

```
GET / HTTP/1.1
Referer: http://10.136.108.237/
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: 10.136.108.237
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.

Apache mod_rewrite off-by-one buffer overflow vulnerability

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

Apache mod_rewrite is prone to an off-by-one buffer-overflow condition. The vulnerability arising in the mod_rewrite module's ldap scheme handling allows for potential memory corruption when an attacker exploits certain rewrite rules.

Affected Apache versions:

- Apache 1.3.28 - 1.3.36 with mod_rewrite
- Apache 2.2.0 - 2.2.2 with mod_rewrite
- Apache 2.0.46 - 2.0.58 with mod_rewrite

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:N/S:C/C:H/I:H/A:H

Base Score	9
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	High
Integrity Impact	High
Availability Impact	High

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

Base Score	9.2
Attack Vector	Network
Attack Complexity	High
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

An attacker may exploit this issue to trigger a denial-of-service condition. Reportedly, arbitrary code execution may also be possible.

http://10.136.108.237/

Version detected: Apache/2.0.52 .

Recommendation

Upgrade Apache to the latest version.

References

BID 19204
https://www.securityfocus.com/bid/19204

Apache homepage
http://httpd.apache.org

VU#395412
https://www.kb.cert.org/vuls/id/395412/

Database User Has Admin Privileges

Acunetix detected the Database User Has Admin Privileges.
This issue has been confirmed by checking the connection privileges via an identified SQL injection vulnerability in the application.

CWE
CWE-267

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

Access Vector	Network
Access Complexity	High
Authentication	None
Confidentiality	Complete
Integrity Impact	Complete
Availability Impact	Complete

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

Base Score	9
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	High
Integrity Impact	High
Availability Impact	High

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

Base Score	9.2
Attack Vector	Network
Attack Complexity	High
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

This can allow an attacker to gain extra privileges via SQL injection attacks. Here is the list of attacks that the attacker might carry out:

- Gain full access to the database server.
- Gain a reverse shell to the database server and execute commands on the underlying operating system.
- Access the database with full permissions, where it may be possible to read, update or delete arbitrary data from the database.
- Depending on the platform and the database system user, an attacker might carry out a privilege escalation attack to gain administrator access to the target system.

http://10.136.108.237/index.php

Database name: **webapp**

Request

```
POST /index.php HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://10.136.108.237/
Content-Type: application/x-www-form-urlencoded
Content-Length: 82
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: 10.136.108.237
Connection: Keep-alive

btnLogin=Login&psw=-1'%20OR%203*2*1=6%20AND%20000693=000693%20--%20&uname=RDFYjolf
```

http://10.136.108.237/index.php

Database name: **webapp**

Request

```
POST /index.php HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://10.136.108.237/
Content-Type: application/x-www-form-urlencoded
Content-Length: 90
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: 10.136.108.237
Connection: Keep-alive

btnLogin=Login&psw=u]H[ww6KrA9F.x-F&uname=-1'%20OR%203*2*1=6%20AND%20000549=000549%20--%20
```

Recommendation

Create a database user with the least possible permissions for your application and connect to the database with that user. Always follow the principle of providing the least privileges for all users and applications.

References

Authorization and Permissions in SQL Server (ADO.NET)
https://msdn.microsoft.com/en-us/library/bb669084.aspx

Wikipedia - Principle of Least Privilege
https://en.wikipedia.org/wiki/Principle_of_least_privilege

How to Use MySQL GRANT to Grant Privileges to Account
http://www.mysqltutorial.org/mysql-grant.aspx

SQL Injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

CWE
CWE-89

CVSS2

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

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

CVSS3

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

Base Score	10
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	High
Integrity Impact	High
Availability Impact	None

CVSS4

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

Base Score	9.3
Attack Vector	Network
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	None
Confidentiality Impact to the Subsequent System	None
Integrity Impact to the Subsequent System	None
Availability Impact to the Subsequent System	None

Impact

An attacker can use SQL injection to bypass a web application's authentication and authorization mechanisms and retrieve the contents of an entire database. SQLi can also be used to add, modify and delete records in a database, affecting data integrity. Under the right circumstances, SQLi can also be used by an attacker to execute OS commands, which may then be used to escalate an attack even further.

http://10.136.108.237/index.php Verified

URL encoded POST input **psw** was set to **-1' OR 3*2*1=6 AND 000693=000693 --**

Tests performed:

- -1' OR 2+693-693-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+693-693-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+693-693) -- => **FALSE**
- -1' OR 3*2>(0+5+693-693) -- => **FALSE**
- -1' OR 2+1-1+1=1 AND 000693=000693 -- => **FALSE**
- -1' OR 3*2=5 AND 000693=000693 -- => **FALSE**
- -1' OR 3*2=6 AND 000693=000693 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000693=000693 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000693=000693 -- => **TRUE**

Original value: **u]H[ww6KrA9F.x-F**

Proof of Exploit

SQL query - SELECT database()

```
webapp
```

Request

```
POST /index.php HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://10.136.108.237/
Content-Type: application/x-www-form-urlencoded
Content-Length: 82
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: 10.136.108.237
Connection: Keep-alive

btnLogin=Login&psw=-1'%20OR%203*2*1=6%20AND%20000693=000693%20--%20&uname=RDFYjolf
```

http://10.136.108.237/index.php Verified

URL encoded POST input **uname** was set to **-1' OR 3*2*1=6 AND 000549=000549 --**

Tests performed:

- -1' OR 2+549-549-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+549-549-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+549-549) -- => **FALSE**
- -1' OR 3*2>(0+5+549-549) -- => **FALSE**
- -1' OR 2+1-1+1=1 AND 000549=000549 -- => **FALSE**
- -1' OR 3*2=5 AND 000549=000549 -- => **FALSE**
- -1' OR 3*2=6 AND 000549=000549 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000549=000549 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000549=000549 -- => **TRUE**

Original value: **RDFYjolf**

Proof of Exploit

SQL query - SELECT database()

```
webapp
```

Request

```
POST /index.php HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://10.136.108.237/
Content-Type: application/x-www-form-urlencoded
Content-Length: 90
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: 10.136.108.237
Connection: Keep-alive

btnLogin=Login&psw=u]H[ww6KrA9F.x-F&uname=-1'%20OR%203*2*1=6%20AND%20000549=000549%20--%20
```

Recommendation

Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.

References

SQL Injection (SQLi) - Acunetix
https://www.acunetix.com/websitesecurity/sql-injection/

Types of SQL Injection (SQLi) - Acunetix
https://www.acunetix.com/websitesecurity/sql-injection2/

Prevent SQL injection vulnerabilities in PHP applications and fix them - Acunetix
https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/

SQL Injection - OWASP
https://www.owasp.org/index.php/SQL_Injection

Bobby Tables: A guide to preventing SQL injection
https://bobby-tables.com/

SQL Injection Cheet Sheets - Pentestmonkey
http://pentestmonkey.net/category/cheat-sheet/sql-injection

Apache 2.x version older than 2.0.61

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

Fixed in Apache httpd 2.0.61:

- **moderate**: mod_proxy crash CVE-2007-3847
  A flaw was found in the Apache HTTP Server mod_proxy module. On sites where a reverse proxy is configured, a remote attacker could send a carefully crafted request that would cause the Apache child process handling that request to crash. On sites where a forward proxy is configured,

an attacker could cause a similar crash if a user could be persuaded to visit a malicious site using the proxy. This could lead to a denial of service if using a threaded Multi-Processing Module.

- **moderate**: mod_status cross-site scripting CVE-2006-5752
  A flaw was found in the mod_status module. On sites where the server-status page is publicly accessible and ExtendedStatus is enabled this could lead to a cross-site scripting attack. Note that the server-status page is not enabled by default and it is best practice to not make this publicly available.
- **moderate**: Signals to arbitrary processes CVE-2007-3304
  The Apache HTTP server did not verify that a process was an Apache child process before sending it signals. A local attacker with the ability to run scripts on the HTTP server could manipulate the scoreboard and cause arbitrary processes to be terminated which could lead to a denial of service.
- **moderate**: mod_cache proxy DoS CVE-2007-1863
  A bug was found in the mod_cache module. On sites where caching is enabled, a remote attacker could send a carefully crafted request that would cause the Apache child process handling that request to crash. This could lead to a denial of service if using a threaded Multi-Processing Module.

Affected Apache versions (up to 2.0.60).

CWE
CWE-701

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

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

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

Base Score	5.1
Attack Vector	Local
Attack Complexity	High
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	High

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

Base Score	5.9
Attack Vector	Local
Attack Complexity	High
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

Check references for details about every vulnerability.

http://10.136.108.237/

Version detected: Apache/2.0.52 .

Recommendation

Upgrade Apache 2.x to the latest version.

References

Apache homepage
http://httpd.apache.org

Apache HTTP Server 2.x announcement
https://archive.apache.org/dist/httpd/CHANGES_2.0

Apache 2.x version older than 2.0.63

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

Fixed in Apache httpd 2.0.63:

- **low**: mod_proxy_ftp UTF-7 XSS CVE-2008-0005
  A workaround was added in the mod_proxy_ftp module. On sites where mod_proxy_ftp is enabled and a forward proxy is configured, a cross-site scripting attack is possible against Web browsers which do not correctly derive the response character set following the rules in RFC 2616.

- **moderate**: mod_status XSS CVE-2007-6388
  A flaw was found in the mod_status module. On sites where mod_status is enabled and the status pages were publicly accessible, a cross-site scripting attack is possible. Note that the server-status page is not enabled by default and it is best practice to not make this publicly available.
- **moderate**: mod_imap XSS CVE-2007-5000
  A flaw was found in the mod_imap module. On sites where mod_imap is enabled and an imagemap file is publicly available, a cross-site scripting attack is possible.

Affected Apache versions (up to 2.0.62).

CWE
CWE-79

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

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

CVSS3
CVSS:3.0/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 every vulnerability.

http://10.136.108.237/

Version detected: Apache/2.0.52 .

Recommendation

Upgrade Apache 2.x to the latest version.

References

Apache homepage
http://httpd.apache.org

Apache HTTP Server 2.x announcement
http://archive.apache.org/dist/httpd/CHANGES_2.0

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
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://10.136.108.237/

Paths without CSP header:

- http://10.136.108.237/

Request

```
GET / HTTP/1.1
Referer: http://10.136.108.237/
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: 10.136.108.237
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://10.136.108.237/

Locations without Permissions-Policy header:

- http://10.136.108.237/

Request

```
GET / HTTP/1.1
Referer: http://10.136.108.237/
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: 10.136.108.237
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://10.136.108.237/ Verified

Folders with directory listing enabled:

- http://10.136.108.237/manual/style/css/

Request

```
GET /manual/style/css/ 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: 10.136.108.237
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

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

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

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	Unchanged
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

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

http://10.136.108.237/

Request

```
TRACE /q06im521jZ 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: 10.136.108.237
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

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

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

Confidentiality	None
Integrity Impact	None
Availability Impact	None

Privileges Required	None
User Interaction	Required
Scope	Changed
Confidentiality	None
Integrity Impact	None
Availability Impact	None

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://10.136.108.237/

Paths without CSP header:

- http://10.136.108.237/

Request

```
GET / HTTP/1.1
Referer: http://10.136.108.237/
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: 10.136.108.237
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/

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

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

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

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

Availability Impact	None

Confidentiality	Low
Integrity Impact	None
Availability Impact	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

Error messages information about an application's internal workings may be used to escalate attacks.

http://10.136.108.237/

Request

```
GET /PAsRNR5VaB 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: 10.136.108.237
Connection: Keep-alive
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

Custom Error Responses (Apache HTTP Server)
https://httpd.apache.org/docs/current/custom-error.html

server_tokens (Nginx)
http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

Remove Unwanted HTTP Response Headers (Microsoft IIS)
https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/

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://10.136.108.237/

Locations without Permissions-Policy header:

- http://10.136.108.237/

Request

```
GET / HTTP/1.1
Referer: http://10.136.108.237/
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: 10.136.108.237
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
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

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

http://10.136.108.237/

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: 10.136.108.237
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.

Apache mod_rewrite off-by-one buffer overflow vulnerability

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

Apache mod_rewrite is prone to an off-by-one buffer-overflow condition. The vulnerability arising in the mod_rewrite module's ldap scheme handling allows for potential memory corruption when an attacker exploits certain rewrite rules.

Affected Apache versions:

- Apache 1.3.28 - 1.3.36 with mod_rewrite
- Apache 2.2.0 - 2.2.2 with mod_rewrite
- Apache 2.0.46 - 2.0.58 with mod_rewrite

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:N/S:C/C:H/I:H/A:H

Base Score	9
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	High
Integrity Impact	High
Availability Impact	High

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

Base Score	9.2
Attack Vector	Network
Attack Complexity	High
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

An attacker may exploit this issue to trigger a denial-of-service condition. Reportedly, arbitrary code execution may also be possible.

http://10.136.108.237/

Version detected: Apache/2.0.52 .

Recommendation

Upgrade Apache to the latest version.

References

BID 19204

https://www.securityfocus.com/bid/19204
Apache homepage
http://httpd.apache.org

VU#395412
https://www.kb.cert.org/vuls/id/395412/

Apache 2.x version older than 2.0.55

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 2.0.55).

CWE
CWE-119

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

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

Multiple. Check references for details about every vulnerability.

http://10.136.108.237/

Version detected: Apache/2.0.52 .

Recommendation

Upgrade Apache 2.x to the latest version.

References

CAN-2005-2088
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2088

CAN-2005-2700
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2700

CAN-2005-2491
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2491

CAN-2005-2728
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2728

CAN-2005-1268
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1268

Apache homepage
http://httpd.apache.org

Apache HTTP Server 2.x announcement
https://archive.apache.org/dist/httpd/Announcement2.0.html

Apache 2.x version older than 2.0.61

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

Fixed in Apache httpd 2.0.61:

- **moderate**: mod_proxy crash CVE-2007-3847
  A flaw was found in the Apache HTTP Server mod_proxy module. On sites where a reverse proxy is configured, a remote attacker could send a carefully crafted request that would cause the Apache child process handling that request to crash. On sites where a forward proxy is configured, an attacker could cause a similar crash if a user could be persuaded to visit a malicious site using the proxy. This could lead to a denial of service if using a threaded Multi-Processing Module.
- **moderate**: mod_status cross-site scripting CVE-2006-5752
  A flaw was found in the mod_status module. On sites where the server-status page is publicly accessible and ExtendedStatus is enabled this could lead to a cross-site scripting attack. Note that the server-status page is not enabled by default and it is best practice to not make this publicly available.
- **moderate**: Signals to arbitrary processes CVE-2007-3304
  The Apache HTTP server did not verify that a process was an Apache child process before sending it signals. A local attacker with the ability to run scripts on the HTTP server could manipulate the scoreboard and cause arbitrary processes to be terminated which could lead to a denial of service.
- **moderate**: mod_cache proxy DoS CVE-2007-1863
  A bug was found in the mod_cache module. On sites where caching is enabled, a remote attacker could send a carefully crafted request that would cause the Apache child process handling that request to crash. This could lead to a denial of service if using a threaded Multi-Processing Module.

Affected Apache versions (up to 2.0.60).

CWE
CWE-701

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

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

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

Base Score	5.1
Attack Vector	Local
Attack Complexity	High
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	None
Availability Impact	High

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

Base Score	5.9
Attack Vector	Local
Attack Complexity	High
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

Check references for details about every vulnerability.

http://10.136.108.237/

Version detected: Apache/2.0.52 .

Recommendation

Upgrade Apache 2.x to the latest version.

References

Apache homepage
http://httpd.apache.org

Apache HTTP Server 2.x announcement
https://archive.apache.org/dist/httpd/CHANGES_2.0

Apache 2.x version older than 2.0.63

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

Fixed in Apache httpd 2.0.63:

- **low**: mod_proxy_ftp UTF-7 XSS CVE-2008-0005
  A workaround was added in the mod_proxy_ftp module. On sites where mod_proxy_ftp is enabled and a forward proxy is configured, a cross-site scripting attack is possible against Web browsers which do not correctly derive the response character set following the rules in RFC 2616.
- **moderate**: mod_status XSS CVE-2007-6388
  A flaw was found in the mod_status module. On sites where mod_status is enabled and the status pages were publicly accessible, a cross-site scripting attack is possible. Note that the server-status page is not enabled by default and it is best practice to not make this publicly available.
- **moderate**: mod_imap XSS CVE-2007-5000
  A flaw was found in the mod_imap module. On sites where mod_imap is enabled and an imagemap file is publicly available, a cross-site scripting attack is possible.

Affected Apache versions (up to 2.0.62).

CWE
CWE-79

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

Access Vector	Network
Access Complexity	Medium
Authentication	None

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

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

Confidentiality	None
Integrity Impact	Partial
Availability Impact	None
Exploitability	Unproven that exploit exists
Remediation Level	Official Fix
Report Confidence	Confirmed

Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	None
Integrity Impact	Low
Availability Impact	None

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 every vulnerability.

http://10.136.108.237/

Version detected: Apache/2.0.52 .

Recommendation

Upgrade Apache 2.x to the latest version.

References

Apache homepage
http://httpd.apache.org

Apache HTTP Server 2.x announcement
http://archive.apache.org/dist/httpd/CHANGES_2.0

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://10.136.108.237/

Version detected: Apache/2.0.52.

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 httpOnly cookie disclosure

Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.

Affected Apache versions (up to 2.0.21).

CWE
CWE-264

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

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

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

Base Score	4.3
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity Impact	None
Availability Impact	None

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

Information disclosure.

http://10.136.108.237/

Pattern found:

```
<pre>
Cookie: testingCookie=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Request

```
GET / HTTP/1.1
Cookie:
testingCookie=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAA
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: 10.136.108.237
Connection: Keep-alive
```

Recommendation

Upgrade Apache 2.x to the latest version. Apache 2.2.22 is the first version that fixed this issue.

References

Fixed in Apache httpd 2.2.22
http://httpd.apache.org/security/vulnerabilities_22.html

Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
https://www.securityfocus.com/bid/51706

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://10.136.108.237/ Verified

Request

```
GET / HTTP/1.1
Referer: http://10.136.108.237/
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: 10.136.108.237
Connection: Keep-alive
```

Recommendation

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

Database User Has Admin Privileges

Acunetix detected the Database User Has Admin Privileges.
This issue has been confirmed by checking the connection privileges via an identified SQL injection vulnerability in the application.

CWE
CWE-267

CVSS2

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

Access Vector	Network
Access Complexity	High
Authentication	None
Confidentiality	Complete
Integrity Impact	Complete
Availability Impact	Complete

CVSS3

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

Base Score	9
Attack Vector	Network
Attack Complexity	High
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality	High
Integrity Impact	High
Availability Impact	High

CVSS4

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

Base Score	9.2
Attack Vector	Network
Attack Complexity	High
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

This can allow an attacker to gain extra privileges via SQL injection attacks. Here is the list of attacks that the attacker might carry out:

- Gain full access to the database server.
- Gain a reverse shell to the database server and execute commands on the underlying operating system.
- Access the database with full permissions, where it may be possible to read, update or delete arbitrary data from the database.
- Depending on the platform and the database system user, an attacker might carry out a privilege escalation attack to gain administrator access to the target system.

http://10.136.108.237/index.php

Database name: **webapp**

Request

```
POST /index.php HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://10.136.108.237/
Content-Type: application/x-www-form-urlencoded
Content-Length: 82
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: 10.136.108.237
Connection: Keep-alive

btnLogin=Login&psw=-1'%20OR%203*2*1=6%20AND%20000693=000693%20--%20&uname=RDFYjolf
```

http://10.136.108.237/index.php

Database name: **webapp**

Request

```
POST /index.php HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: http://10.136.108.237/
Content-Type: application/x-www-form-urlencoded
Content-Length: 90
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: 10.136.108.237
Connection: Keep-alive

btnLogin=Login&psw=u]H[ww6KrA9F.x-F&uname=-1'%20OR%203*2*1=6%20AND%20000549=000549%20--%20
```

Recommendation

Create a database user with the least possible permissions for your application and connect to the database with that user. Always follow the principle of providing the least privileges for all users and applications.

References

Authorization and Permissions in SQL Server (ADO.NET)
https://msdn.microsoft.com/en-us/library/bb669084.aspx

Wikipedia - Principle of Least Privilege
https://en.wikipedia.org/wiki/Principle_of_least_privilege

How to Use MySQL GRANT to Grant Privileges to Account
http://www.mysqltutorial.org/mysql-grant.aspx

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://10.136.108.237
  - icons
    - small
  - manual
    - de
      - de
        - mod
          - directives.html
        - vhosts
      - developer
      - en
        - mod
          - directives.html
        - vhosts
      - es
        - mod
          - directives.html
        - vhosts
      - faq
      - howto
        - auth.html
        - auth.html.en
        - auth.html.ja.euc-jp
        - auth.html.ko.euc-kr
        - cgi.html
        - cgi.html.en
        - cgi.html.ja.euc-jp
        - cgi.html.ko.euc-kr
        - htaccess.html
        - htaccess.html.en
        - htaccess.html.ja.euc-jp
        - htaccess.html.ko.euc-kr
        - public_html.html
        - public_html.html.en
        - public_html.html.ja.euc-jp
        - public_html.html.ko.euc-kr
        - ssi.html
        - ssi.html.en
        - ssi.html.ja.euc-jp
        - ssi.html.ko.euc-kr
      - images
      - ja
        - mod
          - directives.html
        - vhosts
      - ko
        - mod

- directives.html
- vhosts
- misc
  - perf-tuning.html
  - perf-tuning.html.en
  - perf-tuning.html.ko.euc-kr
  - rewriteguide.html
  - rewriteguide.html.en
  - rewriteguide.html.ko.euc-kr
  - security_tips.html
  - security_tips.html.en
  - security_tips.html.ko.euc-kr
- mod
  - beos.html
  - core.html
    - #fragments
      - namevirtualhost
      - serveralias
      - servername
      - serverpath
      - virtualhost
  - directive-dict.html
  - directives.html
    - #fragments
      - A
      - B
      - C
      - D
      - E
      - F
      - G
      - H
      - I
      - K
      - L
      - M
      - N
      - O
      - P
      - R
      - S
      - T
      - U
      - V
      - W
      - X
  - directives.html.de
    - #fragments
      - A

- B
- C
- D
- E
- F
- G
- H
- I
- K
- L
- M
- N
- O
- P
- R
- S
- T
- U
- V
- W
- X

directives.html.en

- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G
  - H
  - I
  - K
  - L
  - M
  - N
  - O
  - P
  - R
  - S
  - T
  - U
  - V
  - W
  - X

directives.html.ja.euc-jp

- #fragments
  - A
  - B

- C
- D
- E
- F
- G
- H
- I
- K
- L
- M
- N
- O
- P
- R
- S
- T
- U
- V
- W
- X

directives.html.ko.euc-kr

- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G
  - H
  - I
  - K
  - L
  - M
  - N
  - O
  - P
  - R
  - S
  - T
  - U
  - V
  - W
  - X

directives.html.ru.koi8-r

- #fragments
  - A
  - B
  - C

- D
- E
- F
- G
- H
- I
- K
- L
- M
- N
- O
- P
- R
- S
- T
- U
- V
- W
- X

leader.html

mod_access.html
- #fragments
  - allow
  - deny
  - order

mod_actions.html
- #fragments
  - action
  - script

mod_alias.html
- #fragments
  - alias
  - aliasmatch
  - redirect
  - redirectmatch
  - redirectpermanent
  - redirecttemp
  - scriptalias
  - scriptaliasmatch

mod_auth_anon.html
- #fragments
  - anonymous
  - anonymous_authoritative
  - anonymous_logemail
  - anonymous_mustgiveemail
  - anonymous_nouserid
  - anonymous_verifyemail

mod_auth_dbm.html
- #fragments

- authdbmauthoritative
- authdbmgroupfile
- authdbmtype
- authdbmuserfile

mod_auth_digest.html
- #fragments
  - authdigestalgorithm
  - authdigestdomain
  - authdigestfile
  - authdigestgroupfile
  - authdigestnccheck
  - authdigestnonceformat
  - authdigestnoncelifetime
  - authdigestqop
  - authdigestshmemsize

mod_auth_ldap.html
- #fragments
  - authldapauthoritative
  - authldapbinddn
  - authldapbindpassword
  - authldapcharsetconfig
  - authldapcomparednonserver
  - authldapdereferencealiases
  - authldapenabled
  - authldapfrontpagehack
  - authldapgroupattribute
  - authldapgroupattributeisdn
  - authldapremoteuserisdn
  - authldapurl

mod_auth.html
- #fragments
  - authauthoritative
  - authgroupfile
  - authuserfile

mod_autoindex.html
- #fragments
  - addalt
  - addaltbyencoding
  - addaltbytype
  - adddescription
  - addicon
  - addiconbyencoding
  - addiconbytype
  - defaulticon
  - headername
  - indexignore
  - indexoptions
  - indexorderdefault
  - readmename

- mod_cache.html
  - #fragments
    - cachedefaultexpire
    - cachedisable
    - cacheenable
    - cacheforcecompletion
    - cacheignorecachecontrol
    - cacheignorenolastmod
    - cachelastmodifiedfactor
    - cachemaxexpire
- mod_cern_meta.html
  - #fragments
    - metadir
    - metafiles
    - metasuffix
- mod_cgi.html
  - #fragments
    - scriptlog
    - scriptlogbuffer
    - scriptloglength
- mod_cgid.html
  - #fragments
    - scriptsock
- mod_charset_lite.html
  - #fragments
    - charsetdefault
    - charsetoptions
    - charsetsourceenc
- mod_dav_fs.html
  - #fragments
    - davlockdb
- mod_dav.html
  - #fragments
    - dav
    - davdepthinfinity
    - davmintimeout
- mod_deflate.html
  - #fragments
    - deflatebuffersize
    - deflatecompressionlevel
    - deflatefilternote
    - deflatememlevel
    - deflatewindowsize
- mod_dir.html
  - #fragments
    - directoryindex
    - directoryslash
- mod_disk_cache.html
  - #fragments
    - cachedirlength

- cachedirlevels
- cacheexpirycheck
- cachegcclean
- cachegcdaily
- cachegcinterval
- cachegcmemusage
- cachegcunused
- cachemaxfilesize
- cacheminfilesize
- cacheroot
- cachesize
- cachetimemargin

mod_echo.html
- #fragments
  - protocolecho

mod_env.html
- #fragments
  - passenv
  - setenv
  - unsetenv

mod_example.html
- #fragments
  - example

mod_expires.html
- #fragments
  - expiresactive
  - expiresbytype
  - expiresdefault

mod_ext_filter.html
- #fragments
  - extfilterdefine
  - extfilteroptions

mod_file_cache.html
- #fragments
  - cachefile
  - mmapfile

mod_headers.html
- #fragments
  - header
  - requestheader

mod_imap.html
- #fragments
  - imapbase
  - imapdefault
  - imapmenu

mod_include.html
- #fragments
  - ssiendtag
  - ssierrormsg

- ssistarttag
- ssitimeformat
- ssiundefinedecho
- xbithack

mod_info.html
- #fragments
  - addmoduleinfo

mod_isapi.html
- #fragments
  - isapiappendlogtoerrors
  - isapiappendlogtoquery
  - isapicachefile
  - isapifakeasync
  - isapilognotsupported
  - isapireadaheadbuffer

mod_ldap.html
- #fragments
  - ldapcacheentries
  - ldapcachettl
  - ldapopcacheentries
  - ldapopcachettl
  - ldapsharedcachefile
  - ldapsharedcachesize
  - ldaptrustedca
  - ldaptrustedcatype

mod_log_config.html
- #fragments
  - cookielog
  - customlog
  - logformat
  - transferlog

mod_log_forensic.html
- #fragments
  - forensiclog

mod_mem_cache.html
- #fragments
  - mcachemaxobjectcount
  - mcachemaxobjectsize
  - mcachemaxstreamingbuffer
  - mcacheminobjectsize
  - mcacheremovalalgorithm
  - mcachesize

mod_mime_magic.html
- #fragments
  - mimemagicfile

mod_mime.html
- #fragments
  - addcharset
  - addencoding

- addhandler
- addinputfilter
- addlanguage
- addoutputfilter
- addtype
- defaultlanguage
- modmimeusepathinfo
- multiviewsmatch
- removecharset
- removeencoding
- removehandler
- removeinputfilter
- removelanguage
- removeoutputfilter
- removetype
- typesconfig

mod_negotiation.html

- #fragments
  - cachenegotiateddocs
  - forcelanguagepriority
  - languagepriority

mod_nw_ssl.html

- #fragments
  - nwssltrustedcerts
  - nwsslupgradeable
  - securelisten

mod_proxy.html

- #fragments
  - allowconnect
  - noproxy
  - proxy
  - proxybadheader
  - proxyblock
  - proxydomain
  - proxyerroroverride
  - proxyiobuffersize
  - proxymatch
  - proxymaxforwards
  - proxypass
  - proxypassreverse
  - proxypreservehost
  - proxyreceivebuffersize
  - proxyremote
  - proxyremotematch
  - proxyrequests
  - proxytimeout
  - proxyvia

mod_rewrite.html

- #fragments

- rewritebase
- rewritecond
- rewriteengine
- rewritelock
- rewritelog
- rewriteloglevel
- rewritemap
- rewriteoptions
- rewriterule

mod_setenvif.html
- #fragments
  - browsermatch
  - browsermatchnocase
  - setenvif
  - setenvifnocase

mod_so.html
- #fragments
  - loadfile
  - loadmodule

mod_speling.html
- #fragments
  - checkspelling

mod_ssl.html
- #fragments
  - sslcacertificatefile
  - sslcacertificatepath
  - sslcarevocationfile
  - sslcarevocationpath
  - sslcertificatechainfile
  - sslcertificatefile
  - sslcertificatekeyfile
  - sslciphersuite
  - sslengine
  - sslmutex
  - ssloptions
  - sslpassphrasedialog
  - sslprotocol
  - sslproxycacertificatefile
  - sslproxycacertificatepath
  - sslproxycarevocationfile
  - sslproxycarevocationpath
  - sslproxyciphersuite
  - sslproxyengine
  - sslproxymachinecertificatefile
  - sslproxymachinecertificatepath
  - sslproxyprotocol
  - sslproxyverify
  - sslproxyverifydepth
  - sslrandomseed

- sslrequire
- sslrequiressl
- sslsessioncache
- sslsessioncachetimeout
- sslverifyclient
- sslverifydepth

mod_status.html
- #fragments
  - extendedstatus

mod_suexec.html
- #fragments
  - suexecusergroup

mod_userdir.html
- #fragments
  - userdir

mod_usertrack.html
- #fragments
  - cookiedomain
  - cookieexpires
  - cookiename
  - cookiestyle
  - cookietracking

mod_vhost_alias.html

mpm_common.html

mpm_netware.html
- #fragments
  - maxthreads
  - threadstacksize

mpm_winnt.html
- #fragments
  - win32disableacceptex

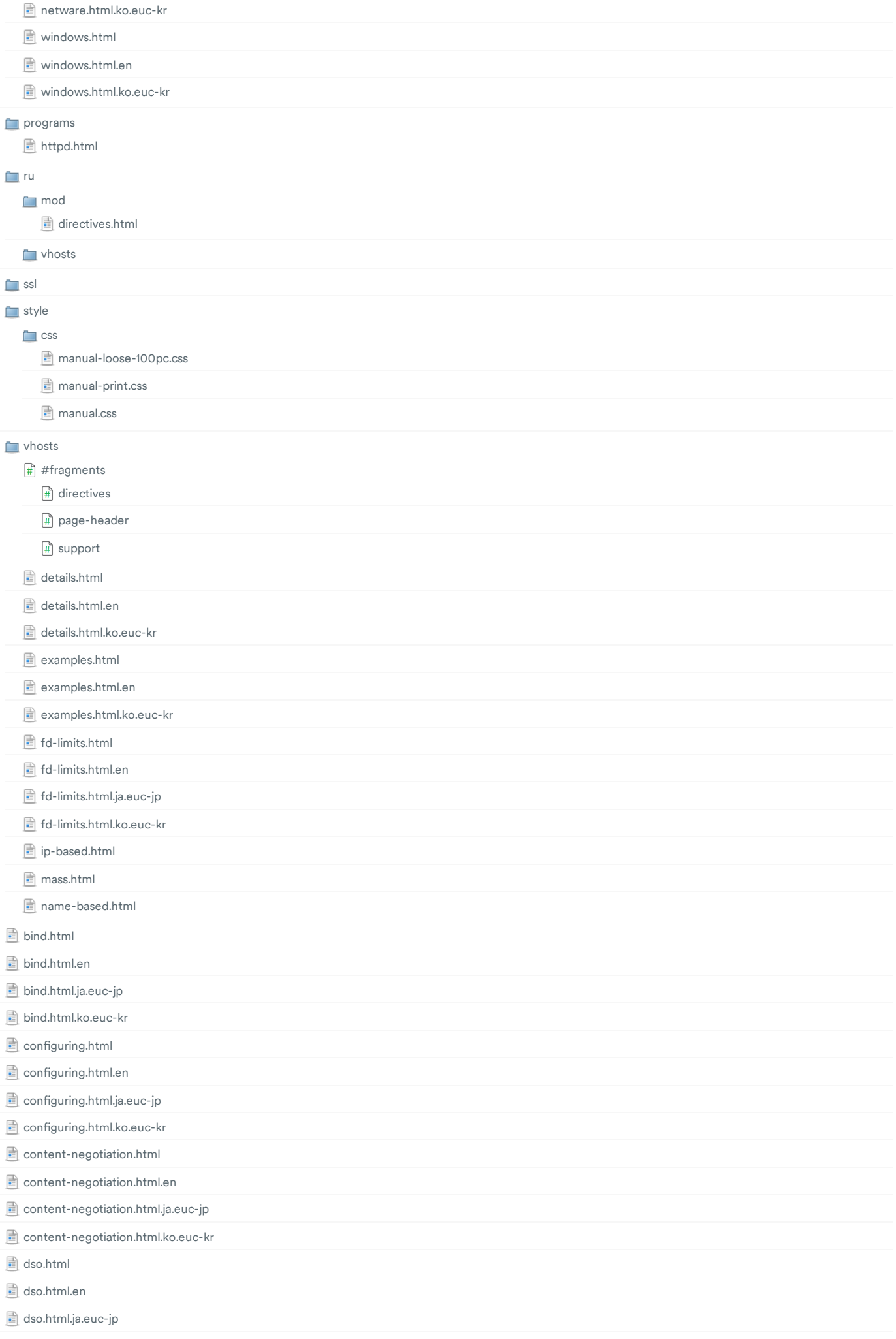
perchild.html
- #fragments
  - assignuserid
  - childperuserid
  - maxthreadsperchild
  - numservers

prefork.html
- #fragments
  - maxspareservers
  - minspareservers

quickreference.html

worker.html

platform
- ebcdic.html
- ebcdic.html.en
- ebcdic.html.ko.euc-kr
- netware.html
- netware.html.en


netware.html.ko.euc-kr
windows.html
windows.html.en
windows.html.ko.euc-kr
programs
httpd.html
ru
mod
directives.html
vhosts
ssl
style
css
manual-loose-100pc.css
manual-print.css
manual.css
vhosts
#fragments
directives
page-header
support
details.html
details.html.en
details.html.ko.euc-kr
examples.html
examples.html.en
examples.html.ko.euc-kr
fd-limits.html
fd-limits.html.en
fd-limits.html.ja.euc-jp
fd-limits.html.ko.euc-kr
ip-based.html
mass.html
name-based.html
bind.html
bind.html.en
bind.html.ja.euc-jp
bind.html.ko.euc-kr
configuring.html
configuring.html.en
configuring.html.ja.euc-jp
configuring.html.ko.euc-kr
content-negotiation.html
content-negotiation.html.en
content-negotiation.html.ja.euc-jp
content-negotiation.html.ko.euc-kr
dso.html
dso.html.en
dso.html.ja.euc-jp

- dso.html.ko.euc-kr
- env.html
- env.html.en
- env.html.ja.euc-jp
- env.html.ko.euc-kr
- filter.html
- filter.html.en
- filter.html.ja.euc-jp
- filter.html.ko.euc-kr
- filter.html.ru.koi8-r
- glossary.html
- glossary.html.en
- glossary.html.ko.euc-kr
- handler.html
- handler.html.en
- handler.html.ja.euc-jp
- handler.html.ko.euc-kr
- handler.html.ru.koi8-r
- index.html.de
- index.html.en
- index.html.ja.euc-jp
- index.html.ko.euc-kr
- index.html.ru.koi8-r
- install.html
- invoking.html
- license.html
- logs.html
- mpm.html
- new_features_2_0.html
- sections.html
- server-wide.html
- sitemap.html
- stopping.html
- suexec.html
- upgrading.html
- urlmapping.html
- developer
  - #fragments
    - external
    - page-header
    - topics
  - API.html
    - #fragments
      - HMR
      - auth_handlers
      - basics
      - commands
      - config
      - handlers

- log_handlers
- moduletour
- page-header
- per-dir
- pool-files
- pools
- req_orig
- req_return
- req_tour
- resp_handlers
- servconf

API.html.en

debugging.html
- #fragments
  - combo
  - howto
  - options
  - page-header

debugging.html.en

documenting.html
- #fragments
  - page-header

documenting.html.en

filters.html
- #fragments
  - asis
  - conclusion
  - howinserted
  - page-header
  - types

filters.html.en

hooks.html
- #fragments
  - create
  - hooking
  - page-header

hooks.html.en

modules.html
- #fragments
  - easy
  - messy
  - page-header

modules.html.en

modules.html.ja.euc-jp
- #fragments
  - easy
  - messy
  - page-header

request.html

- #fragments
  - handler
  - page-header
  - parsing
  - preparation
  - processing
  - security
- request.html.en
- thread_safety.html
  - #fragments
    - commonlibs
    - errno
    - functions
    - liblist
    - page-header
    - variables
- thread_safety.html.en

- en
  - de
    - mod
      - directives.html
  - developer
    - API.html
    - API.html.en
    - debugging.html
    - debugging.html.en
    - documenting.html
    - documenting.html.en
    - filters.html
    - filters.html.en
    - hooks.html
    - hooks.html.en
    - modules.html
    - modules.html.en
    - modules.html.ja.euc-jp
    - request.html
    - request.html.en
    - thread_safety.html
    - thread_safety.html.en
  - en
    - mod
      - directives.html
  - es
    - mod
      - directives.html
  - faq
    - all_in_one.html
    - all_in_one.html.en
    - all_in_one.html.ko.euc-kr

- error.html
- error.html.en
- error.html.ko.euc-kr
- support.html
- support.html.en
- support.html.ko.euc-kr

howto
- auth.html
- auth.html.en
- auth.html.ja.euc-jp
- auth.html.ko.euc-kr
- cgi.html
- cgi.html.en
- cgi.html.ja.euc-jp
- cgi.html.ko.euc-kr
- htaccess.html
- htaccess.html.en
- htaccess.html.ja.euc-jp
- htaccess.html.ko.euc-kr
- public_html.html
- ssi.html

images

ja
- mod
  - directives.html

ko
- mod
  - directives.html

misc
- custom_errordocs.html
- custom_errordocs.html.en
- descriptors.html
- descriptors.html.en
- fin_wait_2.html
- fin_wait_2.html.en
- known_client_problems.html
- known_client_problems.html.en
- perf-tuning.html
- perf-tuning.html.en
- perf-tuning.html.ko.euc-kr
- relevant_standards.html
- relevant_standards.html.en
- relevant_standards.html.ko.euc-kr
- rewriteguide.html
- rewriteguide.html.en
- rewriteguide.html.ko.euc-kr
- security_tips.html
- security_tips.html.en
- security_tips.html.ko.euc-kr

- tutorials.html
- tutorials.html.en

mod

- beos.html
- core.html
- directive-dict.html
- directives.html
  - #fragments
    - A
    - B
    - C
    - D
    - E
    - F
    - G
    - H
    - I
    - K
    - L
    - M
    - N
    - O
    - P
    - R
    - S
    - T
    - U
    - V
    - W
    - X
- directives.html.de
  - #fragments
    - A
    - B
    - C
    - D
    - E
    - F
    - G
    - H
    - I
    - K
    - L
    - M
    - N
    - O
    - P
    - R
    - S

- T
- U
- V
- W
- X

directives.html.en

- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G
  - H
  - I
  - K
  - L
  - M
  - N
  - O
  - P
  - R
  - S
  - T
  - U
  - V
  - W
  - X

directives.html.ja.euc-jp

- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G
  - H
  - I
  - K
  - L
  - M
  - N
  - O
  - P
  - R
  - S
  - T

- U
- V
- W
- X

directives.html.ko.euc-kr

- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G
  - H
  - I
  - K
  - L
  - M
  - N
  - O
  - P
  - R
  - S
  - T
  - U
  - V
  - W
  - X

directives.html.ru.koi8-r

- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G
  - H
  - I
  - K
  - L
  - M
  - N
  - O
  - P
  - R
  - S
  - T
  - U

- V
- W
- X

leader.html
mod_access.html
mod_actions.html
mod_alias.html
mod_asis.html
mod_auth_anon.html
mod_auth_dbm.html
mod_auth_digest.html
mod_auth_ldap.html
mod_auth.html
mod_autoindex.html
mod_cache.html
mod_cern_meta.html
mod_cgi.html
mod_cgid.html
mod_charset_lite.html
mod_dav_fs.html
mod_dav.html
mod_deflate.html
mod_dir.html
mod_disk_cache.html
- #fragments
  - cachedirlength
  - cachedirlevels
  - cacheexpirycheck
  - cachegcclean
  - cachegcdaily
  - cachegcinterval
  - cachegcmemusage
  - cachegcunused
  - cachemaxfilesize
  - cacheminfilesize
  - cacheroot
  - cachesize
  - cachetimemargin

mod_echo.html
- #fragments
  - protocolecho

mod_env.html
- #fragments
  - passenv
  - setenv
  - unsetenv

mod_example.html
- #fragments
  - example

- mod_expires.html
  - #fragments
    - expiresactive
    - expiresbytype
    - expiresdefault
- mod_ext_filter.html
  - #fragments
    - extfilterdefine
    - extfilteroptions
- mod_file_cache.html
  - #fragments
    - cachefile
    - mmapfile
- mod_headers.html
  - #fragments
    - header
    - requestheader
- mod_imap.html
  - #fragments
    - imapbase
    - imapdefault
    - imapmenu
- mod_include.html
  - #fragments
    - ssiendtag
    - ssierrormsg
    - ssistarttag
    - ssitimeformat
    - ssiundefinedecho
    - xbithack
- mod_info.html
  - #fragments
    - addmoduleinfo
- mod_isapi.html
  - #fragments
    - isapiappendlogtoerrors
    - isapiappendlogtoquery
    - isapicachefile
    - isapifakeasync
    - isapilognotsupported
    - isapireadaheadbuffer
- mod_ldap.html
  - #fragments
    - ldapcacheentries
    - ldapcachettl
    - ldapopcacheentries
    - ldapopcachettl
    - ldapsharedcachefile
    - ldapsharedcachesize
    - ldaptrustedca

- ldaptrustedcatype
- mod_log_config.html
- mod_log_forensic.html
  - #fragments
    - forensiclog
- mod_logio.html
- mod_mem_cache.html
  - #fragments
    - mcachemaxobjectcount
    - mcachemaxobjectsize
    - mcachemaxstreamingbuffer
    - mcacheminobjectsize
    - mcacheremovalalgorithm
    - mcachesize
- mod_mime_magic.html
  - #fragments
    - mimemagicfile
- mod_mime.html
- mod_negotiation.html
  - #fragments
    - cachenegotiateddocs
    - forcelanguagepriority
    - languagepriority
- mod_nw_ssl.html
  - #fragments
    - nwssltrustedcerts
    - nwsslupgradeable
    - securelisten
- mod_proxy_connect.html
- mod_proxy_ftp.html
- mod_proxy_http.html
- mod_proxy.html
  - #fragments
    - allowconnect
    - noproxy
    - proxy
    - proxybadheader
    - proxyblock
    - proxydomain
    - proxyerroroverride
    - proxyiobuffersize
    - proxymatch
    - proxymaxforwards
    - proxypass
    - proxypassreverse
    - proxypreservehost
    - proxyreceivebuffersize
    - proxyremote
    - proxyremotematch

- proxyrequests
- proxytimeout
- proxyvia
- mod_rewrite.html
- mod_setenvif.html
  - #fragments
    - browsermatch
    - browsermatchnocase
    - setenvif
    - setenvifnocase
- mod_so.html
- mod_speling.html
  - #fragments
    - checkspelling
- mod_ssl.html
  - #fragments
    - sslcacertificatefile
    - sslcacertificatepath
    - sslcarevocationfile
    - sslcarevocationpath
    - sslcertificatechainfile
    - sslcertificatefile
    - sslcertificatekeyfile
    - sslciphersuite
    - sslengine
    - sslmutex
    - ssloptions
    - sslpassphrasedialog
    - sslprotocol
    - sslproxycacertificatefile
    - sslproxycacertificatepath
    - sslproxycarevocationfile
    - sslproxycarevocationpath
    - sslproxyciphersuite
    - sslproxyengine
    - sslproxymachinecertificatefile
    - sslproxymachinecertificatepath
    - sslproxyprotocol
    - sslproxyverify
    - sslproxyverifydepth
    - sslrandomseed
    - sslrequire
    - sslrequiressl
    - sslsessioncache
    - sslsessioncachetimeout
    - sslverifyclient
    - sslverifydepth
- mod_status.html
- mod_suexec.html

- #fragments
  - suexecusergroup
- mod_userdir.html
- mod_usertrack.html
  - #fragments
    - cookiedomain
    - cookieexpires
    - cookiename
    - cookiestyle
    - cookietracking
- mod_vhost_alias.html
  - #fragments
    - virtualdocumentroot
    - virtualdocumentrootip
    - virtualscriptalias
    - virtualscriptaliasip
- mpm_common.html
- mpm_netware.html
- mpm_winnt.html
- mpmt_os2.html
- perchild.html
  - #fragments
    - assignuserid
    - childperuserid
    - maxthreadsperchild
    - numservers
- prefork.html
- quickreference.html
- worker.html

platform

- ebcdic.html
- ebcdic.html.en
- ebcdic.html.ko.euc-kr
- netware.html
- netware.html.en
- netware.html.ko.euc-kr
- perf-hp.html
- perf-hp.html.en
- perf-hp.html.ko.euc-kr
- win_compiling.html
- win_compiling.html.en
- win_compiling.html.ko.euc-kr
- windows.html
- windows.html.en
- windows.html.ko.euc-kr

programs

- ab.html
- apachectl.html
- apxs.html

- configure.html
- dbmmanage.html
- htdigest.html
- htpasswd.html
- httpd.html
- logresolve.html
- other.html
- rotatelogs.html
- suexec.html

ru
- mod
  - directives.html

ssl
- ssl_compat.html
- ssl_compat.html.en
- ssl_faq.html
- ssl_faq.html.en
- ssl_howto.html
- ssl_howto.html.en
- ssl_intro.html
- ssl_intro.html.en
- ssl_intro.html.ja.euc-jp

style
- css
  - manual-loose-100pc.css
  - manual-print.css
  - manual.css

vhosts
- details.html
- details.html.en
- details.html.ko.euc-kr
- examples.html
- fd-limits.html
- ip-based.html
- mass.html
- name-based.html

- bind.html
- bind.html.en
- bind.html.ja.euc-jp
- bind.html.ko.euc-kr
- configuring.html
- configuring.html.en
- configuring.html.ja.euc-jp
- configuring.html.ko.euc-kr
- content-negotiation.html
- content-negotiation.html.en
- content-negotiation.html.ja.euc-jp
- content-negotiation.html.ko.euc-kr
- custom-error.html

- dns-caveats.html
- dso.html
- env.html
- filter.html
- glossary.html
- handler.html
- index.html.de
- index.html.en
- index.html.ja.euc-jp
- index.html.ko.euc-kr
- index.html.ru.koi8-r
- install.html
- invoking.html
- license.html
- logs.html
- mpm.html
- new_features_2_0.html
- sections.html
- server-wide.html
- sitemap.html
- stopping.html
- suexec.html
- upgrading.html
- urlmapping.html
- es
  - mod
    - beos.html
    - directives.html
    - leader.html
    - mpm_winnt.html
    - prefork.html
    - quickreference.html
    - worker.html
  - programs
  - vhosts
  - filter.html
  - glossary.html
  - handler.html
  - install.html
  - invoking.html
  - mpm.html
  - new_features_2_0.html
  - sitemap.html
  - stopping.html
  - upgrading.html
- faq
  - #fragments
    - page-header
  - all_in_one.html

- #fragments
  - error
  - error.acceptex
  - error.scriptheaders
  - error.sendfile
  - page-header
  - support
  - support.support
  - support.what2do
  - support.what2do.user-support
  - topics
- all_in_one.html.en
- all_in_one.html.ko.euc-kr
  - #fragments
    - error
    - error.acceptex
    - error.scriptheaders
    - error.sendfile
    - page-header
    - support
    - support.support
    - support.what2do
    - support.what2do.user-support
    - topics
- error.html
  - #fragments
    - error.acceptex
    - error.scriptheaders
    - error.sendfile
    - page-header
- error.html.en
- error.html.ko.euc-kr
  - #fragments
    - error.acceptex
    - error.scriptheaders
    - error.sendfile
    - page-header
- support.html
  - #fragments
    - page-header
    - support.support
    - support.what2do
    - support.what2do.user-support
- support.html.en
- support.html.ko.euc-kr
  - #fragments
    - page-header
    - support.support
    - support.what2do

- support.what2do.user-support
- fr
  - de
    - mod
      - core.html
      - directives.html
      - vhosts
        - name-based.html
      - new_features_2_0.html
      - sitemap.html
  - developer
    - API.html
    - API.html.en
    - debugging.html
    - debugging.html.en
    - documenting.html
    - documenting.html.en
    - filters.html
    - filters.html.en
    - hooks.html
    - hooks.html.en
    - modules.html
    - modules.html.en
    - modules.html.ja.euc-jp
    - request.html
  - en
    - mod
      - core.html
      - directives.html
      - vhosts
        - name-based.html
      - new_features_2_0.html
      - sitemap.html
  - es
    - mod
      - directives.html
      - vhosts
        - name-based.html
      - new_features_2_0.html
      - sitemap.html
  - faq
    - error.html
    - error.html.en
    - error.html.ko.euc-kr
    - support.html
    - support.html.en
    - support.html.ko.euc-kr
  - fr
    - new_features_2_0.html

- howto
  - auth.html
  - cgi.html
  - htaccess.html
  - public_html.html
  - ssi.html
- images
- ja
  - mod
    - core.html
    - directives.html
  - vhosts
    - name-based.html
  - new_features_2_0.html
  - sitemap.html
- ko
  - mod
    - directives.html
  - vhosts
    - name-based.html
  - new_features_2_0.html
  - sitemap.html
- misc
  - custom_errordocs.html
  - descriptors.html
  - fin_wait_2.html
  - known_client_problems.html
  - perf-tuning.html
  - relevant_standards.html
  - rewriteguide.html
  - security_tips.html
    - #fragments
      - serverroot
  - security_tips.html.en
  - security_tips.html.ko.euc-kr
  - tutorials.html
- mod
  - beos.html
    - #fragments
      - maxrequestsperthread
  - core.html
    - #fragments
      - %3Cvirtualhost%3E
      - acceptpathinfo
      - accessfilename
      - adddefaultcharset
      - addoutputfilterbytype
      - allowencodedslashes
      - allowoverride
      - authname

- authtype
- cgimapextension
- contentdigest
- defaulttype
- directory
- directorymatch
- documentroot
- enablemmap
- enablesendfile
- errordocument
- errorlog
- fileetag
- files
- filesmatch
- forcetype
- hostnamelookups
- identitycheck
- ifdefine
- ifmodule
- include
- keepalive
- keepalivetimeout
- limit
- limitexcept
- limitinternalrecursion
- limitrequestbody
- limitrequestfields
- limitrequestfieldsize
- limitrequestline
- limitxmlrequestbody
- location
- locationmatch
- loglevel
- maxkeepaliverequests
- namevirtualhost
- options
- page-header
- require
- rlimitcpu
- rlimitmem
- rlimitnproc
- satisfy
- scriptinterpretersource
- serveradmin
- serveralias
- servername
- serverpath
- serverroot
- serversignature

- servertokens
- sethandler
- setinputfilter
- setoutputfilter
- timeout
- usecanonicalname
- virtualhost
- virtualhost%3E

core.html.de

- #fragments
  - acceptpathinfo
  - accessfilename
  - adddefaultcharset
  - addoutputfilterbytype
  - allowencodedslashes
  - allowoverride
  - authname
  - authtype
  - cgimapextension
  - contentdigest
  - defaulttype
  - directory
  - directorymatch
  - documentroot
  - enablemmap
  - enablesendfile
  - errordocument
  - errorlog
  - fileetag
  - files
  - filesmatch
  - forcetype
  - hostnamelookups
  - identitycheck
  - ifdefine
  - ifmodule
  - include
  - keepalive
  - keepalivetimeout
  - limit
  - limitexcept
  - limitinternalrecursion
  - limitrequestbody
  - limitrequestfields
  - limitrequestfieldsize
  - limitrequestline
  - limitxmlrequestbody
  - location
  - locationmatch

- loglevel
- maxkeepaliverequests
- namevirtualhost
- options
- page-header
- require
- rlimitcpu
- rlimitmem
- rlimitnproc
- satisfy
- scriptinterpretersource
- serveradmin
- serveralias
- servername
- serverpath
- serverroot
- serversignature
- servertokens
- sethandler
- setinputfilter
- setoutputfilter
- timeout
- usecanonicalname
- virtualhost

core.html.en

core.html.ja.euc-jp

- #fragments
  - acceptpathinfo
  - accessfilename
  - adddefaultcharset
  - addoutputfilterbytype
  - allowencodedslashes
  - allowoverride
  - authname
  - authtype
  - cgimapextension
  - contentdigest
  - defaulttype
  - directory
  - directorymatch
  - documentroot
  - enablemmap
  - enablesendfile
  - errordocument
  - errorlog
  - fileetag
  - files
  - filesmatch
  - forcetype

- hostnamelookups
- identitycheck
- ifdefine
- ifmodule
- include
- keepalive
- keepalivetimeout
- limit
- limitexcept
- limitinternalrecursion
- limitrequestbody
- limitrequestfields
- limitrequestfieldsize
- limitrequestline
- limitxmlrequestbody
- location
- locationmatch
- loglevel
- maxkeepaliverequests
- namevirtualhost
- options
- page-header
- port
- require
- rlimitcpu
- rlimitmem
- rlimitnproc
- satisfy
- scriptinterpretersource
- serveradmin
- serveralias
- servername
- serverpath
- serverroot
- serversignature
- servertokens
- sethandler
- setinputfilter
- setoutputfilter
- timeout
- usecanonicalname
- virtualhost

directive-dict.html

- #fragments
  - Compatibility
  - Context
  - Default
  - Description
  - Module

- Override
- Status
- Syntax

directive-dist.html
- #fragments
  - context

directives.html
- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G
  - H
  - I
  - K
  - L
  - M
  - N
  - O
  - P
  - R
  - S
  - T
  - U
  - V
  - W
  - X

directives.html.de
- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G
  - H
  - I
  - K
  - L
  - M
  - N
  - O
  - P
  - R
  - S

- T
- U
- V
- W
- X

directives.html.en

- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G
  - H
  - I
  - K
  - L
  - M
  - N
  - O
  - P
  - R
  - S
  - T
  - U
  - V
  - W
  - X

directives.html.ja.euc-jp

- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G
  - H
  - I
  - K
  - L
  - M
  - N
  - O
  - P
  - R
  - S
  - T

- U
- V
- W
- X

directives.html.ko.euc-kr

- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G
  - H
  - I
  - K
  - L
  - M
  - N
  - O
  - P
  - R
  - S
  - T
  - U
  - V
  - W
  - X

directives.html.ru.koi8-r

- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G
  - H
  - I
  - K
  - L
  - M
  - N
  - O
  - P
  - R
  - S
  - T
  - U

- V
- W
- X

leader.html

mod_access.html
- #fragments
  - allow
  - deny
  - order

mod_actions.html
- #fragments
  - action

mod_alias.html
- #fragments
  - alias
  - scriptalias

mod_asis.html

mod_auth_anon.html
- #fragments
  - anonymous
  - anonymous_authoritative
  - anonymous_logemail
  - anonymous_mustgiveemail
  - anonymous_nouserid
  - anonymous_verifyemail

mod_auth_dbm.html
- #fragments
  - authdbmtype

mod_auth_digest.html

mod_auth_ldap.html

mod_auth.html
- #fragments
  - authgroupfile
  - authuserfile

mod_autoindex.html

mod_cache.html
- #fragments
  - cachedefaultexpire
  - cachedisable
  - cacheenable
  - cacheforcecompletion
  - cacheignorecachecontrol
  - cacheignorenolastmod
  - cachelastmodifiedfactor
  - cachemaxexpire

mod_cern_meta.html
- #fragments
  - metadir
  - metafiles

- metasuffix
- mod_cgi.html
- mod_cgid.html
  - #fragments
    - scriptsock
- mod_charset_lite.html
- mod_dav_fs.html
  - #fragments
    - davlockdb
- mod_dav.html
- mod_deflate.html
- mod_dir.html
  - #fragments
    - directoryindex
- mod_disk_cache.html
  - #fragments
    - cachedirlength
    - cachedirlevels
    - cacheexpirycheck
    - cachegcclean
    - cachegcdaily
    - cachegcinterval
    - cachegcmemusage
    - cachegcunused
    - cachemaxfilesize
    - cacheminfilesize
    - cacheroot
    - cachesize
    - cachetimemargin
- mod_echo.html
- mod_env.html
  - #fragments
    - passenv
    - setenv
    - unsetenv
- mod_example.html
  - #fragments
    - example
- mod_expires.html
  - #fragments
    - expiresactive
    - expiresbytype
    - expiresdefault
- mod_ext_filter.html
- mod_file_cache.html
- mod_headers.html
- mod_imap.html
  - #fragments
    - imapbase

- imapdefault
- imapmenu
- mod_include.html
- mod_info.html
- mod_isapi.html
- mod_ldap.html
- mod_log_config.html
  - #fragments
    - cookielog
    - customlog
    - logformat
    - transferlog
- mod_log_forensic.html
  - #fragments
    - forensiclog
- mod_logio.html
- mod_mem_cache.html
  - #fragments
    - mcachemaxobjectcount
    - mcachemaxobjectsize
    - mcachemaxstreamingbuffer
    - mcacheminobjectsize
    - mcacheremovalalgorithm
    - mcachesize
- mod_mime_magic.html
  - #fragments
    - mimemagicfile
- mod_mime.html
  - #fragments
    - addhandler
    - addinputfilter
    - addoutputfilter
    - addtype
- mod_negotiation.html
  - #fragments
    - forcelanguagepriority
- mod_nw_ssl.html
  - #fragments
    - nwssltrustedcerts
    - nwsslupgradeable
    - securelisten
- mod_proxy_connect.html
- mod_proxy_ftp.html
- mod_proxy_http.html
- mod_proxy.html
  - #fragments
    - proxy
- mod_rewrite.html
  - #fragments

- rewritebase
- rewritecond
- rewriteengine
- rewritelock
- rewritelog
- rewriteloglevel
- rewritemap
- rewriteoptions
- rewriterule

mod_setenvif.html
- #fragments
  - browsermatch
  - browsermatchnocase
  - setenvif
  - setenvifnocase

mod_so.html
- #fragments
  - loadmodule

mod_speling.html
- #fragments
  - checkspelling

mod_ssl.html

mod_status.html
- #fragments
  - extendedstatus

mod_suexec.html
- #fragments
  - suexecusergroup

mod_unique_id.html

mod_userdir.html
- #fragments
  - userdir

mod_usertrack.html
- #fragments
  - cookiedomain
  - cookieexpires
  - cookiename
  - cookiestyle
  - cookietracking

mod_vhost_alias.html
- #fragments
  - virtualdocumentroot
  - virtualdocumentrootip
  - virtualscriptalias
  - virtualscriptaliasip

module-dict.html
- #fragments
  - Description
  - Status

- mpm_common.html
  - #fragments
    - listen
- mpm_netware.html
  - #fragments
    - maxthreads
    - threadstacksize
- mpm_winnt.html
  - #fragments
    - win32disableacceptex
- mpmt_os2.html
- perchild.html
  - #fragments
    - assignuserid
    - childperuserid
    - maxthreadsperchild
    - numservers
- prefork.html
  - #fragments
    - maxspareservers
    - minspareservers
- quickreference.html
- threadpool.html
- worker.html

platform

- ebcdic.html
- ebcdic.html.en
- ebcdic.html.ko.euc-kr
- netware.html
- perf-hp.html
- win_compiling.html
- windows.html

programs

- ab.html
- apachectl.html
- apachectl.html.en
- apachectl.html.ko.euc-kr
- apxs.html
- configure.html
- dbmmanage.html
- htdigest.html
- htpasswd.html
- httpd.html
- logresolve.html
- logresolve.html.en
- logresolve.html.ko.euc-kr
- other.html
- rotatelogs.html
- suexec.html

- ru
  - mod
    - directives.html
  - new_features_2_0.html
- ssl
  - ssl_compat.html
  - ssl_compat.html.en
  - ssl_faq.html
  - ssl_faq.html.en
  - ssl_howto.html
  - ssl_howto.html.en
  - ssl_intro.html
  - ssl_intro.html.en
  - ssl_intro.html.ja.euc-jp
- style
  - css
    - manual-loose-100pc.css
    - manual-print.css
    - manual.css
- vhosts
  - details.html
  - details.html.en
  - details.html.ko.euc-kr
  - examples.html
    - #fragments
      - serverpath
  - fd-limits.html
  - ip-based.html
  - mass.html
  - name-based.html
    - #fragments
      - compat
      - namevip
      - page-header
      - using
  - name-based.html.de
    - #fragments
      - compat
      - namevip
      - page-header
      - using
  - name-based.html.en
  - name-based.html.ja.euc-jp
    - #fragments
      - compat
      - namevip
      - page-header
      - using
  - name-based.html.ko.euc-kr
    - #fragments

- compat
- namevip
- page-header
- using

bind.html
configuring.html
content-negotiation.html
custom-error.html
dns-caveats.html
dso.html
env.html
filter.html
glossary.html
glossary.html.en
glossary.html.ko.euc-kr
handler.html
index.html.de
index.html.en
index.html.ja.euc-jp
index.html.ko.euc-kr
index.html.ru.koi8-r
install.html
invoking.html
license.html
logs.html
mpm.html
mpm.html.en
mpm.html.ja.euc-jp
mpm.html.ko.euc-kr
mpm.html.ru.koi8-r
new_features_2_0.html
- #fragments
  - core
  - module

new_features_2_0.html.de
- #fragments
  - core
  - module
  - page-header

new_features_2_0.html.en
new_features_2_0.html.fr
new_features_2_0.html.ja.euc-jp
new_features_2_0.html.ko.euc-kr
new_features_2_0.html.ru.koi8-r
sections.html
- #fragments
  - mergin

server-wide.html
sitemap.html

- sitemap.html.de
  - #fragments
    - developer
    - faq
    - howto
    - index
    - misc
    - modules
    - page-header
    - platform
    - programs
    - release
    - ssl
    - using
    - vhosts
- sitemap.html.en
- sitemap.html.ja.euc-jp
- sitemap.html.ko.euc-kr
- stopping.html
- suexec.html
- upgrading.html
- urlmapping.html
- howto
  - #fragments
    - page-header
  - auth.html
    - #fragments
      - gettingitworking
      - introduction
      - lettingmorethanonepersonin
      - moreinformation
      - page-header
      - possibleproblems
      - related
      - theprerequisites
      - whatotherneatstuffcanido
  - auth.html.en
  - auth.html.ja.euc-jp
  - auth.html.ko.euc-kr
    - #fragments
      - gettingitworking
      - introduction
      - lettingmorethanonepersonin
      - moreinformation
      - page-header
      - possibleproblems
      - related
      - theprerequisites
      - whatotherneatstuffcanido

- cgi.html
  - #fragments
    - behindscenes
    - configuring
    - env
    - errorlogs
    - intro
    - libraries
    - moreinfo
    - page-header
    - pathinformation
    - permissions
    - troubleshoot
    - writing
- cgi.html.en
- cgi.html.ja.euc-jp
  - #fragments
    - behindscenes
    - configuring
    - errorlogs
    - filepermissions
    - intro
    - libraries
    - moreinfo
    - page-header
    - pathinformation
    - troubleshoot
    - writing
- cgi.html.ko.euc-kr
  - #fragments
    - behindscenes
    - configuring
    - env
    - errorlogs
    - intro
    - libraries
    - moreinfo
    - page-header
    - pathinformation
    - permissions
    - troubleshoot
    - writing
- htaccess.html
  - #fragments
    - auth
    - cgi
    - how
    - page-header
    - related

- ssi
- troubleshoot
- what
- when

htaccess.html.en

htaccess.html.ja.euc-jp

htaccess.html.ko.euc-kr

- #fragments
  - auth
  - cgi
  - how
  - page-header
  - related
  - ssi
  - troubleshoot
  - what
  - when

public_html.html

- #fragments
  - cgi
  - enable
  - htaccess
  - page-header
  - related
  - userdir

public_html.html.en

public_html.html.ja.euc-jp

- #fragments
  - cgi
  - enable
  - htaccess
  - page-header
  - related
  - userdir

public_html.html.ko.euc-kr

- #fragments
  - cgi
  - enable
  - htaccess
  - page-header
  - related
  - userdir

ssi.html

- #fragments
  - additionalexamples
  - advanced
  - basic
  - conclusion
  - config

- configuring
- exec
- page-header
- related
- what
- ssi.html.en
- ssi.html.ja.euc-jp
  - #fragments
    - additionalexamples
    - advanced
    - basic
    - conclusion
    - config
    - configuring
    - exec
    - page-header
    - related
    - what
- ssi.html.ko.euc-kr
  - #fragments
    - additionalexamples
    - advanced
    - basic
    - conclusion
    - config
    - configuring
    - exec
    - page-header
    - related
    - what
- images
- ja
  - de
    - mod
      - directives.html
    - vhosts
  - developer
    - modules.html
    - modules.html.ja.euc-jp
  - en
    - howto
      - auth.html
    - mod
      - directives.html
    - ssl
    - vhosts
  - es
    - mod
      - directives.html

- vhosts
- faq
- howto
  - #fragments
    - page-header
  - auth.html
    - #fragments
      - gettingitworking
      - introduction
      - lettingmorethanonepersonin
      - moreinformation
      - page-header
      - possibleproblems
      - related
      - theprerequisites
      - whatotherneatstuffcanido
  - auth.html.ja.euc-jp
  - cgi.html
  - cgi.html.ja.euc-jp
  - htaccess.html
  - htaccess.html.ja.euc-jp
  - public_html.html
  - public_html.html.ja.euc-jp
  - ssi.html
  - ssi.html.ja.euc-jp
- images
- ja
  - howto
    - auth.html
  - mod
    - directives.html
  - ssl
  - vhosts
- ko
  - howto
    - auth.html
  - mod
    - directives.html
  - vhosts
- mod
  - #fragments
    - A
    - C
    - D
    - E
    - F
    - H
    - I
    - L

- M
- N
- P
- R
- S
- U
- V
- core
- other
- page-header

beos.html

core.html

- #fragments
  - acceptpathinfo
  - accessfilename
  - adddefaultcharset
  - addoutputfilterbytype
  - allowencodedslashes
  - allowoverride
  - authname
  - authtype
  - cgimapextension
  - contentdigest
  - defaulttype
  - directory
  - directorymatch
  - documentroot
  - enablemmap
  - enablesendfile
  - errordocument
  - errorlog
  - fileetag
  - files
  - filesmatch
  - forcetype
  - hostnamelookups
  - identitycheck
  - ifdefine
  - ifmodule
  - include
  - keepalive
  - keepalivetimeout
  - limit
  - limitexcept
  - limitinternalrecursion
  - limitrequestbody
  - limitrequestfields
  - limitrequestfieldsize
  - limitrequestline

- limitxmlrequestbody
- location
- locationmatch
- loglevel
- maxkeepaliverequests
- namevirtualhost
- options
- require
- rlimitcpu
- rlimitmem
- rlimitnproc
- satisfy
- scriptinterpretersource
- serveradmin
- serveralias
- servername
- serverpath
- serverroot
- serversignature
- servertokens
- sethandler
- setinputfilter
- setoutputfilter
- timeout
- usecanonicalname
- virtualhost

core.html.ja.euc-jp

directive-dict.html

directives.html

- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G
  - H
  - I
  - K
  - L
  - M
  - N
  - O
  - P
  - R
  - S
  - T
  - U

- V
- W
- X

directives.html.ja.euc-jp
- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G
  - H
  - I
  - K
  - L
  - M
  - N
  - O
  - P
  - R
  - S
  - T
  - U
  - V
  - W
  - X

leader.html

mod_access.html
- #fragments
  - allow
  - deny
  - order

mod_access.html.ja.euc-jp

mod_actions.html

mod_alias.html

mod_asis.html

mod_auth_anon.html

mod_auth_dbm.html
- #fragments
  - authdbmuserfile

mod_auth_dbm.html.en

mod_auth_digest.html

mod_auth_digest.html.en

mod_auth_digest.html.ko.euc-kr

mod_auth_file.html
- #fragments
  - authuserfile

mod_auth_ldap.html

- mod_auth.html
  - #fragments
    - authgroupfile
    - authuserfile
- mod_auth.html.ja.euc-jp
- mod_autoindex.html
- mod_cache.html
- mod_cern_meta.html
- mod_cgi.html
- mod_cgid.html
- mod_charset_lite.html
- mod_dav_fs.html
- mod_dav.html
- mod_deflate.html
- mod_dir.html
- mod_disk_cache.html
- mod_echo.html
- mod_env.html
- mod_example.html
- mod_expires.html
- mod_ext_filter.html
- mod_file_cache.html
- mod_headers.html
- mod_imap.html
- mod_include.html
- mod_info.html
- mod_isapi.html
- mod_ldap.html
- mod_log_config.html
- mod_log_forensic.html
- mod_logio.html
- mod_mem_cache.html
- mod_mime_magic.html
- mod_mime.html
- mod_negotiation.html
- mod_nw_ssl.html
- mod_proxy_connect.html
- mod_proxy_ftp.html
- mod_proxy_http.html
- mod_proxy.html
- mod_rewrite.html
- mod_setenvif.html
- mod_so.html
- mod_speling.html
- mod_ssl.html
- mod_status.html
- mod_suexec.html
- mod_unique_id.html
- mod_userdir.html

- #fragments
  - userdir
- mod_userdir.html.ja.euc-jp
- mod_usertrack.html
- mod_vhost_alias.html
- mpm_common.html
- mpm_netware.html
- mpm_winnt.html
- mpmt_os2.html
- perchild.html
- prefork.html
- quickreference.html
- threadpool.html
- worker.html

programs

- dbmmanage.html
- dbmmanage.html.en
- dbmmanage.html.ko.euc-kr
- htpasswd.html
- htpasswd.html.en
- htpasswd.html.ko.euc-kr
- httpd.html
- httpd.html.en
- httpd.html.ko.euc-kr

ru

- mod
  - directives.html
- vhosts

ssl

- #fragments
  - documentation
  - mod-ssl
  - page-header
- ssl_compat.html
- ssl_compat.html.en
- ssl_faq.html
- ssl_faq.html.en
- ssl_howto.html
- ssl_howto.html.en
- ssl_intro.html
- ssl_intro.html.ja.euc-jp

style

- css
  - manual-loose-100pc.css
  - manual-print.css
  - manual.css

vhosts

- #fragments
  - directives

- page-header
- support
- details.html
- details.html.en
- details.html.ko.euc-kr
- examples.html
- examples.html.en
- examples.html.ko.euc-kr
- fd-limits.html
- fd-limits.html.ja.euc-jp
- ip-based.html
- ip-based.html.en
- ip-based.html.ko.euc-kr
- mass.html
- mass.html.en
- mass.html.ko.euc-kr
- name-based.html
- name-based.html.ja.euc-jp
- bind.html
- bind.html.ja.euc-jp
- configuring.html
- configuring.html.ja.euc-jp
- content-negotiation.html
- content-negotiation.html.ja.euc-jp
- custom-error.html
- dns-caveats.html
- dso.html
- dso.html.ja.euc-jp
- env.html
- env.html.ja.euc-jp
- filter.html
- filter.html.ja.euc-jp
- glossary.html
- glossary.html.en
- glossary.html.ko.euc-kr
- handler.html
- handler.html.ja.euc-jp
- index.html.de
- index.html.en
- index.html.ja.euc-jp
- index.html.ko.euc-kr
- index.html.ru.koi8-r
- install.html
- install.html.ja.euc-jp
- invoking.html
- logs.html
- mpm.html
- new_features_2_0.html
- sections.html

- server-wide.html
- sitemap.html
- sitemap.html.ja.euc-jp
- stopping.html
- suexec.html
- upgrading.html
- urlmapping.html
- ko
  - de
    - mod
      - directives.html
  - en
    - faq
    - howto
    - mod
      - directives.html
    - platform
    - programs
  - es
    - mod
      - directives.html
    - programs
  - faq
    - #fragments
      - page-header
    - all_in_one.html
    - all_in_one.html.ko.euc-kr
    - error.html
    - error.html.ko.euc-kr
    - support.html
    - support.html.ko.euc-kr
  - howto
    - #fragments
      - page-header
    - auth.html
    - auth.html.ko.euc-kr
    - cgi.html
    - cgi.html.ko.euc-kr
    - htaccess.html
    - htaccess.html.ko.euc-kr
    - public_html.html
    - public_html.html.ko.euc-kr
    - ssi.html
    - ssi.html.ko.euc-kr
  - images
  - ja
    - howto
    - mod
      - directives.html

- ko
  - faq
  - howto
  - mod
    - directives.html
  - platform
  - programs
- misc
  - perf-tuning.html
  - perf-tuning.html.ko.euc-kr
  - relevant_standards.html
  - relevant_standards.html.ko.euc-kr
  - rewriteguide.html
  - rewriteguide.html.ko.euc-kr
  - security_tips.html
  - security_tips.html.ko.euc-kr
- mod
  - #fragments
    - A
    - C
    - D
    - E
    - F
    - H
    - I
    - L
    - M
    - N
    - P
    - R
    - S
    - U
    - V
    - core
    - other
    - page-header
  - beos.html
  - beos.html.ko.euc-kr
  - core.html
  - directive-dict.html
  - directives.html
    - #fragments
      - A
      - B
      - C
      - D
      - E
      - F
      - G

- H
- I
- K
- L
- M
- N
- O
- P
- R
- S
- T
- U
- V
- W
- X

directives.html.ko.euc-kr

- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G
  - H
  - I
  - K
  - L
  - M
  - N
  - O
  - P
  - R
  - S
  - T
  - U
  - V
  - W
  - X

leader.html

mod_access.html

mod_actions.html

mod_alias.html

mod_asis.html

mod_auth_anon.html

mod_auth_dbm.html

mod_auth_digest.html

mod_auth_ldap.html

mod_auth.html

mod_autoindex.html
mod_cache.html
mod_cern_meta.html
mod_cgi.html
mod_cgid.html
mod_charset_lite.html
mod_dav_fs.html
mod_dav.html
mod_deflate.html
mod_dir.html
mod_disk_cache.html
mod_echo.html
mod_env.html
mod_example.html
mod_expires.html
mod_ext_filter.html
mod_file_cache.html
mod_headers.html
mod_imap.html
mod_include.html
mod_info.html
mod_isapi.html
mod_ldap.html
mod_log_config.html
mod_log_forensic.html
mod_logio.html
mod_mem_cache.html
mod_mime_magic.html
mod_mime.html
mod_negotiation.html
mod_nw_ssl.html
mod_proxy_connect.html
mod_proxy_ftp.html
mod_proxy_http.html
mod_proxy.html
mod_rewrite.html
mod_setenvif.html
mod_so.html
mod_speling.html
mod_ssl.html
mod_status.html
mod_suexec.html
mod_unique_id.html
mod_userdir.html
mod_usertrack.html
mod_vhost_alias.html
mpm_common.html
mpm_netware.html
mpm_winnt.html

- mpmt_os2.html
- perchild.html
- prefork.html
- quickreference.html
- threadpool.html
- worker.html

platform
- #fragments
  - other
  - page-header
  - win
- ebcdic.html
- ebcdic.html.ko.euc-kr
- netware.html
- netware.html.ko.euc-kr
- perf-hp.html
- perf-hp.html.ko.euc-kr
- win_compiling.html
- win_compiling.html.ko.euc-kr
- windows.html
- windows.html.ko.euc-kr

programs
- #fragments
  - page-header
- ab.html
- ab.html.ko.euc-kr
- apachectl.html
- apachectl.html.ko.euc-kr
- apxs.html
- apxs.html.ko.euc-kr
- configure.html
- configure.html.ko.euc-kr
- dbmmanage.html
- dbmmanage.html.ko.euc-kr
- htdigest.html
- htdigest.html.ko.euc-kr
- htpasswd.html
- htpasswd.html.ko.euc-kr
- httpd.html
- httpd.html.ko.euc-kr
- logresolve.html
- logresolve.html.ko.euc-kr
- other.html
- other.html.ko.euc-kr
- rotatelogs.html
- suexec.html

ru
- mod
  - directives.html

- programs
- style
  - css
    - manual-loose-100pc.css
    - manual-print.css
    - manual.css
- vhosts
  - details.html
  - details.html.ko.euc-kr
  - examples.html
  - examples.html.ko.euc-kr
  - fd-limits.html
  - fd-limits.html.ko.euc-kr
  - ip-based.html
  - ip-based.html.ko.euc-kr
  - mass.html
  - mass.html.ko.euc-kr
  - name-based.html
- bind.html
- bind.html.ko.euc-kr
- configuring.html
- configuring.html.ko.euc-kr
- content-negotiation.html
- content-negotiation.html.ko.euc-kr
- custom-error.html
- dns-caveats.html
- dso.html
- dso.html.ko.euc-kr
- env.html
- env.html.ko.euc-kr
- filter.html
- filter.html.ko.euc-kr
- glossary.html
- glossary.html.ko.euc-kr
- handler.html
- handler.html.ko.euc-kr
- index.html.de
- index.html.en
- index.html.ja.euc-jp
- index.html.ko.euc-kr
- index.html.ru.koi8-r
- install.html
- invoking.html
- logs.html
- mpm.html
- new_features_2_0.html
- sections.html
- server-wide.html
- sitemap.html

- sitemap.html.ko.euc-kr
- stopping.html
- suexec.html
- upgrading.html
- urlmapping.html
- misc
  - custom_errordocs.html
    - #fragments
      - createdir
      - createdocs
      - fallback
      - intro
      - listings
      - page-header
      - proxy
  - custom_errordocs.html.en
  - descriptors.html
    - #fragments
      - AIX
      - bsdi
      - freebsd
      - linux
      - others
      - page-header
      - sco
      - solaris
      - tru64
  - descriptors.html.en
  - fin_wait_2.html
    - #fragments
      - appendix
      - page-header
      - what
      - why
  - fin_wait_2.html.en
  - known_client_problems.html
    - #fragments
      - boundary-string
      - broken-keepalive
      - byte-257
      - byterange-requests
      - content-type-persistent
      - cookie-merge
      - force-response-1.0
      - gif89-expires
      - ie40-vary
      - jdk-12-bugs
      - lynx-negotiate-trans
      - msie-cookie-y2k

- msie4.0b2
- no-content-length
- page-header
- trailing-crlf

known_client_problems.html.en

perf-tuning.html
- #fragments
  - compiletime
  - hardware
  - page-header
  - runtime
  - trace

perf-tuning.html.en

perf-tuning.html.ko.euc-kr
- #fragments
  - compiletime
  - hardware
  - page-header
  - runtime
  - trace

relevant_standards.html
- #fragments
  - authentication
  - html_recommendations
  - http_recommendations
  - language_country_codes
  - page-header

relevant_standards.html.en

relevant_standards.html.ko.euc-kr
- #fragments
  - authentication
  - html_recommendations
  - http_recommendations
  - language_country_codes
  - page-header

rewriteguide.html
- #fragments
  - ToC1
  - ToC2
  - access
  - content
  - other
  - page-header
  - url

rewriteguide.html.en

rewriteguide.html.ko.euc-kr
- #fragments
  - ToC1
  - ToC2

- access
- content
- other
- page-header
- url

security_tips.html
- #fragments
  - cgi
  - dynamic
  - nsaliasedcgi
  - page-header
  - protectserverfiles
  - saliasedcgi
  - serverroot
  - ssi
  - systemsettings
  - uptodate
  - watchyourlogs

security_tips.html.en

security_tips.html.ko.euc-kr
- #fragments
  - cgi
  - dynamic
  - nsaliasedcgi
  - page-header
  - protectserverfiles
  - saliasedcgi
  - serverroot
  - ssi
  - systemsettings
  - uptodate
  - watchyourlogs

tutorials.html
- #fragments
  - basics
  - cgi_ssi
  - logging
  - other
  - page-header
  - security
  - starting

tutorials.html.en

mod
- #fragments
  - A
  - C
  - D
  - E
  - F

- H
- I
- L
- M
- N
- P
- R
- S
- U
- V
- core
- other
- page-header

beos.html
- #fragments
  - maxrequestsperthread
  - page-header

beos.html.de
- #fragments
  - maxrequestsperthread
  - page-header

beos.html.en

beos.html.ko.euc-kr
- #fragments
  - maxrequestsperthread
  - page-header

core.c.html

core.html
- #fragments
  - allowoverride
  - authname
  - authtype
  - directory
  - options
  - require

core.html.de

core.html.en

core.html.ja.euc-jp

directive-dict.html
- #fragments
  - Context

directives.html
- #fragments
  - A
  - B
  - C
  - D
  - E
  - F

- G
- H
- I
- K
- L
- M
- N
- O
- P
- R
- S
- T
- U
- V
- W
- X

directives.html.de

- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G
  - H
  - I
  - K
  - L
  - M
  - N
  - O
  - P
  - R
  - S
  - T
  - U
  - V
  - W
  - X

directives.html.en

- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G

- H
- I
- K
- L
- M
- N
- O
- P
- R
- S
- T
- U
- V
- W
- X

directives.html.ja.euc-jp

- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G
  - H
  - I
  - K
  - L
  - M
  - N
  - O
  - P
  - R
  - S
  - T
  - U
  - V
  - W
  - X

directives.html.ko.euc-kr

- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G
  - H

- I
- K
- L
- M
- N
- O
- P
- R
- S
- T
- U
- V
- W
- X

directives.html.ru.koi8-r

- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G
  - H
  - I
  - K
  - L
  - M
  - N
  - O
  - P
  - R
  - S
  - T
  - U
  - V
  - W
  - X

index.html

leader.html

leader.html.de

leader.html.en

leader.html.ko.euc-kr

mod_access.html

- #fragments
  - allow
  - deny
  - order
  - page-header

- mod_access.html.en
- mod_access.html.ja.euc-jp
  - #fragments
    - allow
    - deny
    - order
    - page-header
- mod_actions.html
  - #fragments
    - action
    - page-header
    - script
- mod_actions.html.en
- mod_actions.html.ja.euc-jp
  - #fragments
    - action
    - page-header
    - script
- mod_actions.html.ko.euc-kr
  - #fragments
    - action
    - page-header
    - script
- mod_alias.html
  - #fragments
    - alias
    - aliasmatch
    - order
    - page-header
    - redirect
    - redirectmatch
    - redirectpermanent
    - redirecttemp
    - scriptalias
    - scriptaliasmatch
- mod_alias.html.en
- mod_alias.html.ja.euc-jp
  - #fragments
    - alias
    - aliasmatch
    - order
    - page-header
    - redirect
    - redirectmatch
    - redirectpermanent
    - redirecttemp
    - scriptalias
    - scriptaliasmatch
- mod_alias.html.ko.euc-kr

- #fragments
  - alias
  - aliasmatch
  - order
  - page-header
  - redirect
  - redirectmatch
  - redirectpermanent
  - redirecttemp
  - scriptalias
  - scriptaliasmatch
- mod_asis.html
  - #fragments
    - page-header
    - usage
- mod_asis.html.en
- mod_auth_anon.html
  - #fragments
    - anonymous
    - anonymous_authoritative
    - anonymous_logemail
    - anonymous_mustgiveemail
    - anonymous_nouserid
    - anonymous_verifyemail
    - example
    - page-header
- mod_auth_dbm.html
  - #fragments
    - authdbmauthoritative
    - authdbmgroupfile
    - authdbmtype
    - authdbmuserfile
    - page-header
- mod_auth_dbm.html.en
- mod_auth_digest.html
  - #fragments
    - authdigestalgorithm
    - authdigestdomain
    - authdigestfile
    - authdigestgroupfile
    - authdigestnccheck
    - authdigestnonceformat
    - authdigestnoncelifetime
    - authdigestqop
    - authdigestshmemsize
    - msie
    - page-header
    - using
- mod_auth_digest.html.en

- mod_auth_digest.html.ko.euc-kr
  - #fragments
    - authdigestalgorithm
    - authdigestdomain
    - authdigestfile
    - authdigestgroupfile
    - authdigestnccheck
    - authdigestnonceformat
    - authdigestnoncelifetime
    - authdigestqop
    - authdigestshmemsize
    - msie
    - page-header
    - using
- mod_auth_ldap.html
  - #fragments
    - authenphase
    - authldapauthoritative
    - authldapbinddn
    - authldapbindpassword
    - authldapcharsetconfig
    - authldapcomparednonserver
    - authldapdereferencealiases
    - authldapenabled
    - authldapfrontpagehack
    - authldapgroupattribute
    - authldapgroupattributeisdn
    - authldapremoteuserisdn
    - authldapurl
    - authorphase
    - contents
    - examples
    - fpcaveats
    - frontpage
    - howitworks
    - operation
    - page-header
    - reqdn
    - reqgroup
    - requiredirectives
    - requser
    - reqvaliduser
    - usingssl
    - usingtls
- mod_auth.html
  - #fragments
    - allow
    - authauthoritative
    - authgroupfile

- authuserfile
- deny
- order
- page-header

mod_auth.html.en

mod_auth.html.ja.euc-jp

- #fragments
  - authauthoritative
  - authgroupfile
  - authuserfile
  - page-header

mod_authn_dbm.html

mod_autoindex.html

- #fragments
  - addalt
  - addaltbyencoding
  - addaltbytype
  - adddescription
  - addicon
  - addiconbyencoding
  - addiconbytype
  - defaulticon
  - headername
  - indexignore
  - indexoptions
  - indexoptions.descriptionwidth
  - indexoptions.fancyindexing
  - indexoptions.ignoreclient
  - indexoptions.suppresscolumnsorting
  - indexoptions.suppresshtmlpreamble
  - indexoptions.suppressicon
  - indexoptions.suppresslastmodified
  - indexoptions.suppresssize
  - indexorderdefault
  - page-header
  - query
  - readmename

mod_cache.html

- #fragments
  - cachedefaultexpire
  - cachedisable
  - cacheenable
  - cacheforcecompletion
  - cacheignorecachecontrol
  - cacheignorenolastmod
  - cachelastmodifiedfactor
  - cachemaxexpire
  - page-header
  - related

- sampleconf
- mod_cache.html.en
- mod_cache.html.ko.euc-kr
  - #fragments
    - cachedefaultexpire
    - cachedisable
    - cacheenable
    - cacheforcecompletion
    - cacheignorecachecontrol
    - cacheignorenolastmod
    - cachelastmodifiedfactor
    - cachemaxexpire
    - page-header
    - related
    - sampleconf
- mod_cern_meta.html
  - #fragments
    - metadir
    - metafiles
    - metasuffix
    - page-header
- mod_cgi.html
  - #fragments
    - cgi-debug
    - env
    - page-header
    - scriptlog
    - scriptlogbuffer
    - scriptloglength
- mod_cgid.html
  - #fragments
    - page-header
    - scriptsock
- mod_charset_lite.html
  - #fragments
    - charsetdefault
    - charsetoptions
    - charsetsourceenc
    - page-header
    - problems
- mod_dav_fs.html
  - #fragments
    - davlockdb
    - page-header
- mod_dav.html
  - #fragments
    - complex
    - dav
    - davdepthinfinity

- davmintimeout
- example
- page-header
- security

mod_deflate.html
- #fragments
  - deflatebuffersize
  - deflatecompressionlevel
  - deflatefilternote
  - deflatememlevel
  - deflatewindowsize
  - enable
  - page-header
  - proxies
  - recommended

mod_dir.html
- #fragments
  - directoryindex
  - directoryslash
  - page-header

mod_dir.html.en

mod_dir.html.ja.euc-jp
- #fragments
  - directoryindex
  - directoryslash
  - page-header

mod_dir.html.ko.euc-kr
- #fragments
  - directoryindex
  - directoryslash
  - page-header

mod_disk_cache.html
- #fragments
  - cachedirlength
  - cachedirlevels
  - cacheexpirycheck
  - cachegcclean
  - cachegcdaily
  - cachegcinterval
  - cachegcmemusage
  - cachegcunused
  - cachemaxfilesize
  - cacheminfilesize
  - cacheroot
  - cachesize
  - cachetimemargin
  - page-header

mod_echo.html
- #fragments

- page-header
- protocolecho

mod_env.html
- #fragments
  - page-header
  - passenv
  - setenv
  - unsetenv

mod_example.html
- #fragments
  - compiling
  - example
  - page-header
  - using

mod_expires.html
- #fragments
  - AltSyn
  - expiresactive
  - expiresbytype
  - expiresdefault
  - page-header

mod_ext_filter.html
- #fragments
  - examples
  - extfilterdefine
  - extfilteroptions
  - page-header

mod_file_cache.html
- #fragments
  - cachefile
  - mmapfile
  - mmapstatic
  - page-header
  - using

mod_headers.html
- #fragments
  - examples
  - header
  - order
  - page-header
  - requestheader

mod_ident.html
- #fragments
  - identitycheck

mod_imap.html
- #fragments
  - example
  - features
  - imapbase

- imapdefault
- imapfile
- imapmenu
- page-header
- referencing

mod_include.html
- #fragments
  - element.config
  - element.echo
  - element.exec
  - element.flastmod
  - element.fsize
  - element.include
  - element.printenv
  - element.set
  - elements
  - enabling
  - flowctrl
  - includevars
  - includevirtual
  - page-header
  - pathinfo
  - ssiendtag
  - ssierrormsg
  - ssistarttag
  - ssitimeformat
  - ssiundefinedecho
  - substitution
  - xbithack

mod_info.html
- #fragments
  - addmoduleinfo
  - page-header

mod_isapi.html
- #fragments
  - isapiappendlogtoerrors
  - isapiappendlogtoquery
  - isapicachefile
  - isapifakeasync
  - isapilognotsupported
  - isapireadaheadbuffer
  - journal
  - notes
  - page-header
  - usage

mod_ldap.html
- #fragments
  - %0A%20%20%20%20ldaptrustedca
  - %0A%20%20%20%20ldaptrustedcatype

- cache
- exampleconfig
- ldapcacheentries
- ldapcachettl
- ldapopcacheentries
- ldapopcachettl
- ldapsharedcachefile
- ldapsharedcachesize
- ldaptrustedca
- ldaptrustedcatype
- page-header
- pool
- usingssltls

mod_log_config.html
- #fragments
  - %0Alogformat
  - %3Ecustomlog
  - %E3%83%95%E3%82%A9%E3%83%BC%E3%83%9E%E3%83%83%E3%83%88%E6%96%87%E5%AD%97%E5%88%97
  - %EC%82%AC%EC%9A%A9%EC%9E%90%EC%A0%95%EC%9D%98%20%EB%A1%9C%EA%B7%B8%ED%98%95%EC%8B%9D
  - cookielog
  - custom%20log%20formats
  - customlog
  - errorlog
  - formats
  - logformat
  - page-header
  - security
  - transferlog

mod_log_config.html.en

mod_log_config.html.ja.euc-jp
- #fragments
  - cookielog
  - customlog
  - formats
  - logformat
  - page-header
  - security
  - transferlog

mod_log_config.html.ko.euc-kr
- #fragments
  - cookielog
  - customlog
  - formats
  - logformat
  - page-header
  - security
  - transferlog

mod_log_forensic.html
- #fragments

- forensiclog
- formats
- page-header
- security

mod_logio.html
- #fragments
  - formats
  - page-header

mod_mem_cache.html
- #fragments
  - mcachemaxobjectcount
  - mcachemaxobjectsize
  - mcachemaxstreamingbuffer
  - mcacheminobjectsize
  - mcacheremovalalgorithm
  - mcachesize
  - page-header

mod_mime_magic.html
- #fragments
  - format
  - mimemagicfile
  - mimemagicfiles
  - notes
  - page-header
  - performance

mod_mime.html
- #fragments
  - addcharset
  - addencoding
  - addhandler
  - addinputfilter
  - addlanguage
  - addoutputfilter
  - addtype
  - charset-lang
  - contentencoding
  - defaultlanguage
  - modmimeusepathinfo
  - multipleext
  - multiviewsmatch
  - page-header
  - removecharset
  - removeencoding
  - removehandler
  - removeinputfilter
  - removelanguage
  - removeoutputfilter
  - removetype
  - typesconfig

- mod_mime.html.en
- mod_mime.html.ja.euc-jp
  - #fragments
    - addcharset
    - addencoding
    - addhandler
    - addinputfilter
    - addlanguage
    - addoutputfilter
    - addtype
    - charset-lang
    - contentencoding
    - defaultlanguage
    - modmimeusepathinfo
    - multipleext
    - multiviewsmatch
    - page-header
    - removecharset
    - removeencoding
    - removehandler
    - removeinputfilter
    - removelanguage
    - removeoutputfilter
    - removetype
    - typesconfig
- mod_negotiation.html
  - #fragments
    - cachenegotiateddocs
    - forcelanguagepriority
    - languagepriority
    - multiviews
    - page-header
    - typemaps
- mod_nw_ssl.html
  - #fragments
    - nwssltrustedcerts
    - nwsslupgradeable
    - page-header
    - securelisten
- mod_proxy_connect.html
- mod_proxy_ftp.html
- mod_proxy_http.html
- mod_proxy.html
  - #fragments
    - access
    - allowconnect
    - domain
    - envsettings
    - examples

- forwardreverse
- ftp-proxy
- hostname
- intranet
- ipaddr
- ipadr
- noproxy
- page-header
- proxy
- proxybadheader
- proxyblock
- proxydomain
- proxyerroroverride
- proxyiobuffersize
- proxymatch
- proxymaxforwards
- proxypass
- proxypassreverse
- proxypreservehost
- proxyreceivebuffersize
- proxyremote
- proxyremotematch
- proxyrequests
- proxytimeout
- proxyvia
- startup

mod_rewrite.html

- #fragments
  - EnvVar
  - Internal
  - Solutions
  - mapfunc
  - mod_rewrite
  - page-header
  - rewritebase
  - rewritecond
  - rewriteengine
  - rewritelock
  - rewritelog
  - rewriteloglevel
  - rewritemap
  - rewritematch
  - rewriteoptions
  - rewriterule

mod_rewrite.html.en

mod_setenvif.html

- #fragments
  - browsermatch
  - browsermatchnocase

- page-header
- setenvif
- setenvifnocase

mod_so.c.html

mod_so.html
- #fragments
  - creating
  - loadfile
  - loadmodule
  - page-header
  - windows

mod_so.html.en

mod_so.html.ja.euc-jp
- #fragments
  - loadfile
  - loadmodule
  - page-header

mod_so.html.ko.euc-kr
- #fragments
  - loadfile
  - loadmodule
  - page-header
  - windows

mod_speling.html

mod_spelling.html

mod_ssl.html

mod_status.html
- #fragments
  - autoupdate
  - enable
  - extendedstatus
  - machinereadable
  - page-header

mod_status.html.en

mod_status.html.ja.euc-jp
- #fragments
  - autoupdate
  - enable
  - extendedstatus
  - machinereadable
  - page-header

mod_status.html.ko.euc-kr
- #fragments
  - autoupdate
  - enable
  - extendedstatus
  - machinereadable
  - page-header

mod_suexec.html

- mod_unique_id.html
- mod_userdir.html
  - #fragments
    - page-header
    - userdir
- mod_userdir.html.en
- mod_userdir.html.ja.euc-jp
  - #fragments
    - page-header
    - userdir
- mod_userdir.html.ko.euc-kr
  - #fragments
    - page-header
    - userdir
- mod_usertrack.html
- mod_vhost_alias.html
- module-dict.html
  - #fragments
    - Status
- mpm_common.html
  - #fragments
    - %0A%20%20%20%20%20%20maxrequestsperchild
    - %0A%20%20%20%20%20%20maxsparethreads
    - %0A%20%20%20%20%20threadsperchild
    - %20maxsparethreads
    - acceptmutex
    - bs2000account
    - coredumpdirectory
    - enableexceptionhook
    - group
    - listen
    - listenbacklog
    - lockfile
    - maxclients
    - maxmemfree
    - maxrequestsperchild
    - maxsparethreads
    - maxthreadsperchild
    - minsparethreads
    - numservers
    - page-header
    - pidfile
    - scoreboardfile
    - sendbuffersize
    - serverlimit
    - startservers
    - startthreads
    - threadlimit
    - threadsperchild

- user
- mpm_common.html.de
  - #fragments
    - acceptmutex
    - bs2000account
    - coredumpdirectory
    - enableexceptionhook
    - group
    - listen
    - listenbacklog
    - lockfile
    - maxclients
    - maxmemfree
    - maxrequestsperchild
    - maxsparethreads
    - minsparethreads
    - page-header
    - pidfile
    - scoreboardfile
    - sendbuffersize
    - serverlimit
    - startservers
    - startthreads
    - threadlimit
    - threadsperchild
    - user
- mpm_common.html.en
- mpm_common.html.ja.euc-jp
  - #fragments
    - coredumpdirectory
    - group
    - listen
    - listenbacklog
    - lockfile
    - maxclients
    - maxmemfree
    - maxrequestsperchild
    - maxsparethreads
    - maxthreadsperchild
    - minsparethreads
    - numservers
    - page-header
    - pidfile
    - scoreboardfile
    - sendbuffersize
    - serverlimit
    - startservers
    - startthreads
    - threadlimit

- threadsperchild
- user
- mpm_netware.html
  - #fragments
    - maxthreads
    - page-header
    - threadstacksize
- mpm_netware.html.en
- mpm_winnt.html
  - #fragments
    - page-header
    - win32disableacceptex
- mpm_winnt.html.de
  - #fragments
    - page-header
    - win32disableacceptex
- mpm_winnt.html.en
- mpm_winnt.html.ja.euc-jp
  - #fragments
    - page-header
    - win32disableacceptex
- mpmt_os2.html
- mpmt_os2.html.en
- perchild.html
- prefork.html
  - #fragments
    - how-it-works
    - maxspareservers
    - minspareservers
    - page-header
- prefork.html.de
  - #fragments
    - how-it-works
    - maxspareservers
    - minspareservers
    - page-header
- prefork.html.en
- prefork.html.ja.euc-jp
- quickreference.html
  - #fragments
    - A
    - B
    - C
    - D
    - E
    - F
    - G
    - H
    - I

- K
- L
- M
- N
- O
- P
- R
- S
- T
- U
- V
- W
- X

quickreference.html.de
quickreference.html.en
quickreference.html.ja.euc-jp
quickreference.html.ko.euc-kr
quickreference.html.ru.koi8-r
threadpool.html
worker.html
- #fragments
  - how-it-works
  - page-header

worker.html.de
- #fragments
  - how-it-works
  - page-header

worker.html.en
worker.html.ja.euc-jp
- #fragments
  - how-it-works
  - page-header

platform
- #fragments
  - other
  - page-header
  - win

ebcdic.html
- #fragments
  - design
  - document
  - modules
  - overview
  - page-header
  - porting
  - technical
  - third-party

ebcdic.html.en
ebcdic.html.ko.euc-kr

- #fragments
  - design
  - document
  - modules
  - overview
  - page-header
  - porting
  - technical
  - third-party
- netware.html
  - #fragments
    - comp
    - down
    - inst
    - page-header
    - req
    - run
    - use
- netware.html.en
- netware.html.ko.euc-kr
  - #fragments
    - comp
    - down
    - inst
    - page-header
    - req
    - run
    - use
- perf-hp.html
- perf-hp.html.en
- perf-hp.html.ko.euc-kr
- win_compiling.html
  - #fragments
    - commandbuild
    - page-header
    - projectcomponents
    - requirements
    - workspacebuild
- win_compiling.html.en
- win_compiling.html.ko.euc-kr
  - #fragments
    - commandbuild
    - page-header
    - projectcomponents
    - requirements
    - workspacebuild
- windows.html
  - #fragments
    - cust

- down
- inst
- page-header
- req
- test
- wincons
- winsvc

windows.html.en

windows.html.ko.euc-kr

- #fragments
  - cust
  - down
  - inst
  - page-header
  - req
  - test
  - wincons
  - winsvc

windows.xml

- #fragments
  - wincons

programs

- #fragments
  - page-header

ab.html

ab.html.en

ab.html.ko.euc-kr

apachectl.html

apachectl.html.en

apachectl.html.ko.euc-kr

apxs.html

apxs.html.en

apxs.html.ko.euc-kr

configure.html

- #fragments
  - configurationoptions
  - env
  - installationdirectories
  - optionalfeatures
  - options
  - page-header
  - suexec
  - supportopt
  - synopsis
  - systemtypes

configure.html.en

configure.html.ko.euc-kr

- #fragments
  - configurationoptions

- directoryfinetuning
- env
- installationdirectories
- optionalfeatures
- options
- page-header
- suexec
- supportopt
- synopsis
- systemtypes

dbmmanage.html
- #fragments
  - bugs
  - options
  - page-header
  - synopsis

dbmmanage.html.en

dbmmanage.html.ko.euc-kr
- #fragments
  - bugs
  - options
  - page-header
  - synopsis

directoryfinetuning

htdigest.html
- #fragments
  - options
  - page-header
  - synopsis

htdigest.html.en

htdigest.html.ko.euc-kr
- #fragments
  - options
  - page-header
  - synopsis

htpasswd.html
- #fragments
  - examples
  - exit
  - options
  - page-header
  - restrictions
  - security
  - synopsis

htpasswd.html.en

htpasswd.html.ko.euc-kr
- #fragments
  - examples
  - exit

- options
- page-header
- restrictions
- security
- synopsis

httpd.html
- #fragments
  - options
  - page-header
  - synopsis

httpd.html.en

httpd.html.ko.euc-kr
- #fragments
  - options
  - page-header
  - synopsis

logresolve.html
- #fragments
  - options
  - page-header
  - synopsis

logresolve.html.en

logresolve.html.ko.euc-kr
- #fragments
  - options
  - page-header
  - synopsis

other.html
- #fragments
  - log_server_status
  - page-header
  - split-logfile

other.html.en

other.html.ko.euc-kr
- #fragments
  - log_server_status
  - page-header
  - split-logfile

rotatelogs.html
- #fragments
  - options
  - page-header
  - portability
  - synopsis

rotatelogs.html.en

rotatelogs.html.ko.euc-kr
- #fragments
  - options
  - page-header

- portability
- synopsis
- suexec.html
  - #fragments
    - install
    - options
    - page-header
    - synopsis
- suexec.html.en
- suexec.html.ko.euc-kr
  - #fragments
    - options
    - page-header
    - synopsis
- ru
  - de
    - mod
      - directives.html
    - vhosts
    - sitemap.html
  - developer
    - API.html
    - API.html.en
    - debugging.html
    - debugging.html.en
    - documenting.html
    - documenting.html.en
    - filters.html
    - filters.html.en
    - hooks.html
    - hooks.html.en
    - modules.html
    - modules.html.en
    - modules.html.ja.euc-jp
    - request.html
    - request.html.en
  - en
    - mod
      - directives.html
    - programs
      - ab.html
      - apachectl.html
      - apxs.html
    - vhosts
    - sitemap.html
  - es
    - mod
      - directives.html
    - programs

- vhosts
- sitemap.html
- faq
  - error.html
  - error.html.en
  - error.html.ko.euc-kr
  - support.html
  - support.html.en
  - support.html.ko.euc-kr
- howto
  - auth.html
  - cgi.html
  - htaccess.html
  - public_html.html
  - ssi.html
- images
- ja
  - mod
    - directives.html
  - vhosts
  - sitemap.html
- ko
  - mod
    - directives.html
  - programs
    - ab.html
    - apachectl.html
    - apxs.html
  - vhosts
  - sitemap.html
- misc
  - custom_errordocs.html
  - custom_errordocs.html.en
  - descriptors.html
  - descriptors.html.en
  - fin_wait_2.html
  - known_client_problems.html
  - perf-tuning.html
  - relevant_standards.html
  - rewriteguide.html
  - security_tips.html
  - tutorials.html
- mod
  - beos.html
    - #fragments
      - maxrequestsperthread
  - core.html
    - #fragments
      - namevirtualhost

- serveralias
- servername
- serverpath
- virtualhost

core.html.de

core.html.en

core.html.ja.euc-jp

directive-dict.html

directives.html

- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G
  - H
  - I
  - K
  - L
  - M
  - N
  - O
  - P
  - R
  - S
  - T
  - U
  - V
  - W
  - X

directives.html.ru.koi8-r

- #fragments
  - A
  - B
  - C
  - D
  - E
  - F
  - G
  - H
  - I
  - K
  - L
  - M
  - N
  - O
  - P

- R
- S
- T
- U
- V
- W
- X

leader.html

mod_access.html
- #fragments
  - allow
  - deny
  - order

mod_actions.html
- #fragments
  - action
  - script

mod_alias.html
- #fragments
  - alias
  - aliasmatch
  - redirect
  - redirectmatch
  - redirectpermanent
  - redirecttemp
  - scriptalias
  - scriptaliasmatch

mod_asis.html

mod_auth_anon.html
- #fragments
  - anonymous
  - anonymous_authoritative
  - anonymous_logemail
  - anonymous_mustgiveemail
  - anonymous_nouserid
  - anonymous_verifyemail

mod_auth_dbm.html
- #fragments
  - authdbmauthoritative
  - authdbmgroupfile
  - authdbmtype
  - authdbmuserfile

mod_auth_digest.html
- #fragments
  - authdigestalgorithm
  - authdigestdomain
  - authdigestfile
  - authdigestgroupfile
  - authdigestnccheck

- authdigestnonceformat
- authdigestnoncelifetime
- authdigestqop
- authdigestshmemsize

mod_auth_ldap.html
- #fragments
  - authldapauthoritative
  - authldapbinddn
  - authldapbindpassword
  - authldapcharsetconfig
  - authldapcomparednonserver
  - authldapdereferencealiases
  - authldapenabled
  - authldapfrontpagehack
  - authldapgroupattribute
  - authldapgroupattributeisdn
  - authldapremoteuserisdn
  - authldapurl

mod_auth.html
- #fragments
  - authauthoritative
  - authgroupfile
  - authuserfile

mod_autoindex.html
- #fragments
  - addalt
  - addaltbyencoding
  - addaltbytype
  - adddescription
  - addicon
  - addiconbyencoding
  - addiconbytype
  - defaulticon
  - headername
  - indexignore
  - indexoptions
  - indexorderdefault
  - readmename

mod_cache.html
- #fragments
  - cachedefaultexpire
  - cachedisable
  - cacheenable
  - cacheforcecompletion
  - cacheignorecachecontrol
  - cacheignorenolastmod
  - cachelastmodifiedfactor
  - cachemaxexpire

mod_cern_meta.html

- #fragments
  - metadir
  - metafiles
  - metasuffix
- mod_cgi.html
  - #fragments
    - scriptlog
    - scriptlogbuffer
    - scriptloglength
- mod_cgid.html
  - #fragments
    - scriptsock
- mod_charset_lite.html
  - #fragments
    - charsetdefault
    - charsetoptions
    - charsetsourceenc
- mod_dav_fs.html
  - #fragments
    - davlockdb
- mod_dav.html
  - #fragments
    - dav
    - davdepthinfinity
    - davmintimeout
- mod_deflate.html
  - #fragments
    - deflatebuffersize
    - deflatecompressionlevel
    - deflatefilternote
    - deflatememlevel
    - deflatewindowsize
- mod_dir.html
  - #fragments
    - directoryindex
    - directoryslash
- mod_disk_cache.html
  - #fragments
    - cachedirlength
    - cachedirlevels
    - cacheexpirycheck
    - cachegcclean
    - cachegcdaily
    - cachegcinterval
    - cachegcmemusage
    - cachegcunused
    - cachemaxfilesize
    - cacheminfilesize
    - cacheroot
    - cachesize

- cachetimemargin
- mod_echo.html
  - #fragments
    - protocolecho
- mod_env.html
  - #fragments
    - passenv
    - setenv
    - unsetenv
- mod_example.html
  - #fragments
    - example
- mod_expires.html
  - #fragments
    - expiresactive
    - expiresbytype
    - expiresdefault
- mod_ext_filter.html
  - #fragments
    - extfilterdefine
    - extfilteroptions
- mod_file_cache.html
  - #fragments
    - cachefile
    - mmapfile
- mod_headers.html
  - #fragments
    - header
    - requestheader
- mod_imap.html
  - #fragments
    - imapbase
    - imapdefault
    - imapmenu
- mod_include.html
  - #fragments
    - ssiendtag
    - ssierrormsg
    - ssistarttag
    - ssitimeformat
    - ssiundefinedecho
    - xbithack
- mod_info.html
  - #fragments
    - addmoduleinfo
- mod_isapi.html
  - #fragments
    - isapiappendlogtoerrors
    - isapiappendlogtoquery

- isapicachefile
- isapifakeasync
- isapilognotsupported
- isapireadaheadbuffer

mod_ldap.html
- #fragments
  - ldapcacheentries
  - ldapcachettl
  - ldapopcacheentries
  - ldapopcachettl
  - ldapsharedcachefile
  - ldapsharedcachesize
  - ldaptrustedca
  - ldaptrustedcatype

mod_log_config.html
- #fragments
  - cookielog
  - customlog
  - logformat
  - transferlog

mod_log_forensic.html
- #fragments
  - forensiclog

mod_logio.html

mod_mem_cache.html
- #fragments
  - mcachemaxobjectcount
  - mcachemaxobjectsize
  - mcachemaxstreamingbuffer
  - mcacheminobjectsize
  - mcacheremovalalgorithm
  - mcachesize

mod_mime_magic.html
- #fragments
  - mimemagicfile

mod_mime.html
- #fragments
  - addcharset
  - addencoding
  - addhandler
  - addinputfilter
  - addlanguage
  - addoutputfilter
  - addtype
  - defaultlanguage
  - modmimeusepathinfo
  - multiviewsmatch
  - removecharset
  - removeencoding

- removehandler
- removeinputfilter
- removelanguage
- removeoutputfilter
- removetype
- typesconfig

mod_negotiation.html
- #fragments
  - cachenegotiateddocs
  - forcelanguagepriority
  - languagepriority

mod_nw_ssl.html
- #fragments
  - nwssltrustedcerts
  - nwsslupgradeable
  - securelisten

mod_proxy_connect.html

mod_proxy_ftp.html

mod_proxy_http.html

mod_proxy.html
- #fragments
  - allowconnect
  - noproxy
  - proxy
  - proxybadheader
  - proxyblock
  - proxydomain
  - proxyerroroverride
  - proxyiobuffersize
  - proxymatch
  - proxymaxforwards
  - proxypass
  - proxypassreverse
  - proxypreservehost
  - proxyreceivebuffersize
  - proxyremote
  - proxyremotematch
  - proxyrequests
  - proxytimeout
  - proxyvia

mod_rewrite.html
- #fragments
  - rewritebase
  - rewritecond
  - rewriteengine
  - rewritelock
  - rewritelog
  - rewriteloglevel
  - rewritemap

- rewriteoptions
- rewriterule

mod_setenvif.html
- #fragments
  - browsermatch
  - browsermatchnocase
  - setenvif
  - setenvifnocase

mod_so.html
- #fragments
  - loadmodule

mod_speling.html
- #fragments
  - checkspelling

mod_ssl.html
- #fragments
  - sslcacertificatefile
  - sslcacertificatepath
  - sslcarevocationfile
  - sslcarevocationpath
  - sslcertificatechainfile
  - sslcertificatefile
  - sslcertificatekeyfile
  - sslciphersuite
  - sslengine
  - sslmutex
  - ssloptions
  - sslpassphrasedialog
  - sslprotocol
  - sslproxycacertificatefile
  - sslproxycacertificatepath
  - sslproxycarevocationfile
  - sslproxycarevocationpath
  - sslproxyciphersuite
  - sslproxyengine
  - sslproxymachinecertificatefile
  - sslproxymachinecertificatepath
  - sslproxyprotocol
  - sslproxyverify
  - sslproxyverifydepth
  - sslrandomseed
  - sslrequire
  - sslrequiressl
  - sslsessioncache
  - sslsessioncachetimeout
  - sslverifyclient
  - sslverifydepth

mod_status.html

mod_suexec.html

- #fragments
  - suexecusergroup
- mod_unique_id.html
- mod_userdir.html
  - #fragments
    - userdir
- mod_usertrack.html
  - #fragments
    - cookiedomain
    - cookieexpires
    - cookiename
    - cookiestyle
    - cookietracking
- mod_vhost_alias.html
- module-dict.html
- mpm_common.html
  - #fragments
    - acceptmutex
    - bs2000account
    - coredumpdirectory
    - enableexceptionhook
    - group
    - listen
    - listenbacklog
    - lockfile
    - maxclients
    - maxmemfree
    - maxrequestsperchild
    - maxsparethreads
    - minsparethreads
    - pidfile
    - scoreboardfile
    - sendbuffersize
    - serverlimit
    - startservers
    - startthreads
    - threadlimit
    - threadsperchild
    - user
- mpm_netware.html
  - #fragments
    - maxthreads
    - threadstacksize
- mpm_winnt.html
  - #fragments
    - win32disableacceptex
- mpmt_os2.html
- perchild.html
  - #fragments

- assignuserid
- childperuserid
- maxthreadsperchild
- numservers
- prefork.html
  - #fragments
    - maxspareservers
    - minspareservers
- quickreference.html
- threadpool.html
- worker.html
- platform
  - ebcdic.html
  - ebcdic.html.en
  - ebcdic.html.ko.euc-kr
  - netware.html
  - netware.html.en
  - netware.html.ko.euc-kr
  - perf-hp.html
  - perf-hp.html.en
  - perf-hp.html.ko.euc-kr
  - win_compiling.html
  - windows.html
- programs
  - #fragments
    - page-header
  - ab.html
    - #fragments
      - bugs
      - options
      - page-header
      - synopsis
  - ab.html.en
  - ab.html.ko.euc-kr
    - #fragments
      - bugs
      - options
      - page-header
      - synopsis
  - apachectl.html
    - #fragments
      - options
      - page-header
      - synopsis
  - apachectl.html.en
  - apachectl.html.ko.euc-kr
    - #fragments
      - options
      - page-header

- synopsis
- apxs.html
  - #fragments
    - examples
    - options
    - page-header
    - synopsis
- apxs.html.en
- apxs.html.ko.euc-kr
  - #fragments
    - examples
    - options
    - page-header
    - synopsis
- configure.html
- dbmmanage.html
- dbmmanage.html.en
- dbmmanage.html.ko.euc-kr
- htdigest.html
- htdigest.html.en
- htdigest.html.ko.euc-kr
- htpasswd.html
- htpasswd.html.en
- htpasswd.html.ko.euc-kr
- httpd.html
- httpd.html.en
- httpd.html.ko.euc-kr
- logresolve.html
- other.html
- rotatelogs.html
- suexec.html
- ru
  - mod
    - directives.html
  - programs
  - vhosts
- ssl
  - ssl_compat.html
  - ssl_compat.html.en
  - ssl_faq.html
  - ssl_faq.html.en
  - ssl_howto.html
  - ssl_howto.html.en
  - ssl_intro.html
  - ssl_intro.html.en
  - ssl_intro.html.ja.euc-jp
- style
  - css
    - manual-loose-100pc.css

- manual-print.css
- manual.css
- vhosts
  - #fragments
    - directives
    - page-header
    - support
  - details.html
  - details.html.en
  - details.html.ko.euc-kr
  - examples.html
  - examples.html.en
  - examples.html.ko.euc-kr
  - fd-limits.html
  - fd-limits.html.en
  - fd-limits.html.ja.euc-jp
  - fd-limits.html.ko.euc-kr
  - ip-based.html
  - mass.html
  - name-based.html
- bind.html
- configuring.html
- content-negotiation.html
- custom-error.html
- dns-caveats.html
- dso.html
- env.html
- filter.html
- glossary.html
- glossary.html.en
- glossary.html.ko.euc-kr
- handler.html
- index.html.de
- index.html.en
- index.html.ja.euc-jp
- index.html.ko.euc-kr
- index.html.ru.koi8-r
- install.html
- invoking.html
- license.html
- logs.html
- mpm.html
- new_features_2_0.html
- sections.html
- server-wide.html
- sitemap.html
- sitemap.html.de
  - #fragments
    - developer

- faq
- howto
- index
- misc
- modules
- page-header
- platform
- programs
- release
- ssl
- using
- vhosts

- sitemap.html.en
- sitemap.html.ja.euc-jp
- sitemap.html.ko.euc-kr
- stopping.html
- suexec.html
- upgrading.html
- urlmapping.html

- ssl
  - #fragments
    - documentation
    - mod-ssl
    - page-header
  - ssl_compat.html
    - #fragments
      - configuration
      - customlog
      - page-header
      - table1
      - table2
      - table3
      - variables
  - ssl_compat.html.en
  - ssl_faq.html
    - #fragments
      - about
      - aboutcerts
      - aboutconfig
      - aboutssl
      - adh
      - backtrace
      - badcert
      - ciphers
      - contact
      - coredump
      - coredumphelp
      - entropy
      - envvars

- establishing
- gid
- hang
- hashsymlinks
- history
- httpstest
- installation
- keyscerts
- keysize
- load
- lockicon
- mm
- msie
- mutex
- nn
- ownca
- page-header
- parallel
- passphrase
- pemder
- ports
- random
- realcert
- refused
- relative
- removepassphrase
- reportdetails
- resources
- sgc
- sharedciphers
- startup
- support
- verify
- verisign
- vhosts
- vhosts2
- wassenaar
- y2k

ssl_faq.html.en

ssl_howto.html

#fragments

- accesscontrol
- allclients
- arbitraryclients
- certauthenticate
- ciphersuites
- intranet
- onlystrong
- page-header

- realssl
- strongurl
- upgradeenc

ssl_howto.html.en

ssl_intro.html

- #fragments
  - AC96
  - MIME
  - PKCS
  - SSL2
  - SSL3
  - TLS1
  - X208
  - X509
  - certificates
  - cryptographictech
  - figure1
  - figure2
  - figure3
  - page-header
  - references
  - ssl
  - table1
  - table2
  - table4

ssl_intro.html.en

ssl_intro.html.ja.euc-jp

- #fragments
  - AC96
  - MIME
  - PKCS
  - SSL2
  - SSL3
  - TLS1
  - X208
  - X509
  - certificates
  - cryptographictech
  - figure1
  - figure2
  - figure3
  - page-header
  - references
  - ssl
  - table1
  - table2
  - table4

style

- css

- manual-chm.css
- manual-loose-100pc.css
- manual-print.css
- manual-zip-100pc.css
- manual-zip.css
- manual.css
- lang
- latex
  - atbeginend.sty
- xsl
- build.properties

vhost
- name-based.html

vhosts
- #fragments
  - directives
  - page-header
  - support
- details.html
  - #fragments
    - configparsing
    - hostmatching
    - page-header
    - tips
- details.html.en
- details.html.ko.euc-kr
  - #fragments
    - configparsing
    - hostmatching
    - page-header
    - tips
- examples.html
  - #fragments
    - default
    - intraextra
    - ip
    - ipport
    - migrate
    - mixed
    - name
    - page-header
    - port
    - purename
    - serverpath
    - twoips
- examples.html.en
- examples.html.ko.euc-kr
  - #fragments
    - default

- intraextra
- ip
- ipport
- migrate
- mixed
- name
- page-header
- port
- purename
- serverpath
- twoips

fd-limits.html
- #fragments
  - page-header
  - splitlogs

fd-limits.html.en

fd-limits.html.ja.euc-jp
- #fragments
  - page-header
  - splitlogs

fd-limits.html.ko.euc-kr
- #fragments
  - page-header
  - splitlogs

ip-based.html
- #fragments
  - howto
  - multiple
  - page-header
  - requirements
  - single

ip-based.html.en

ip-based.html.ko.euc-kr
- #fragments
  - howto
  - multiple
  - page-header
  - requirements
  - single

mass.html
- #fragments
  - combinations
  - homepages
  - homepages.rewrite
  - ipbased
  - motivation
  - oldversion
  - overview
  - page-header

- simple
- simple.rewrite
- xtra-conf
- mass.html.en
- mass.html.ko.euc-kr
- name-based.html
- name-based.html.de
- name-based.html.en
- name-based.html.ja.euc-jp
- name-based.html.ko.euc-kr
- bind.html
  - #fragments
    - ipv6
    - overview
    - page-header
    - virtualhost
- bind.html.en
- bind.html.ja.euc-jp
  - #fragments
    - ipv6
    - overview
    - page-header
    - virtualhost
- bind.html.ko.euc-kr
  - #fragments
    - ipv6
    - overview
    - page-header
    - virtualhost
- configuring.html
  - #fragments
    - htaccess
    - main
    - modules
    - page-header
    - scope
    - syntax
- configuring.html.en
- configuring.html.ja.euc-jp
- configuring.html.ko.euc-kr
- content-negotiation.html
  - #fragments
    - about
    - better
    - caching
    - extensions
    - methods
    - more
    - naming

- negotiation
- page-header

content-negotiation.html.en

content-negotiation.html.ja.euc-jp

- #fragments
  - about
  - better
  - caching
  - extensions
  - methods
  - more
  - naming
  - negotiation
  - page-header

content-negotiation.html.ko.euc-kr

- #fragments
  - about
  - better
  - caching
  - extensions
  - methods
  - more
  - naming
  - negotiation
  - page-header

custom-error.html

- #fragments
  - behavior
  - configuration
  - custom
  - page-header

custom-error.html.en

custom-error.html.ja.euc-jp

- #fragments
  - behavior
  - configuration
  - custom
  - page-header

custom-error.html.ko.euc-kr

- #fragments
  - behavior
  - configuration
  - custom
  - page-header

dns-caveats.html

- #fragments
  - appendix
  - denial
  - example

- main
- page-header
- tips

dns-caveats.html.en

dns-caveats.html.ja.euc-jp

- #fragments
  - appendix
  - denial
  - example
  - main
  - page-header
  - tips

dns-caveats.html.ko.euc-kr

- #fragments
  - appendix
  - denial
  - example
  - main
  - page-header
  - tips

dso.html

- #fragments
  - advantages
  - background
  - implementation
  - page-header
  - usage

dso.html.en

dso.html.ja.euc-jp

- #fragments
  - advantages
  - background
  - implementation
  - page-header
  - usage

dso.html.ko.euc-kr

- #fragments
  - advantages
  - background
  - implementation
  - page-header
  - usage

env.html

- #fragments
  - examples
  - page-header
  - setting
  - special
  - using

- env.html.en
- env.html.ja.euc-jp
  - #fragments
    - examples
    - page-header
    - setting
    - special
    - using
- env.html.ko.euc-kr
  - #fragments
    - examples
    - page-header
    - setting
    - special
    - using
- filter.html
  - #fragments
    - page-header
- filter.html.en
- filter.html.ja.euc-jp
  - #fragments
    - page-header
- filter.html.ko.euc-kr
- filter.html.ru.koi8-r
  - #fragments
    - page-header
- glossary.html
  - #fragments
    - certificate
    - certificationauthority
    - cgi
    - cipher
    - configurationfile
    - directive
    - dso
    - header
    - http
    - method
    - module
    - page-header
    - plaintext
    - privatekey
    - proxy
    - publickey
    - regex
    - ssi
    - ssl
    - tarball
    - uniformresourceidentifier

- url
- glossary.html.en
- glossary.html.ko.euc-kr
  - #fragments
    - certificate
    - certificationauthority
    - cgi
    - cipher
    - configurationfile
    - directive
    - dso
    - header
    - http
    - method
    - module
    - page-header
    - plaintext
    - privatekey
    - proxy
    - publickey
    - ssi
    - tarball
    - uniformresourceidentifier
    - url
- handler.html
  - #fragments
    - definition
    - examples
    - page-header
    - programmer
- handler.html.en
- handler.html.ja.euc-jp
  - #fragments
    - definition
    - examples
    - page-header
    - programmer
- handler.html.ko.euc-kr
- handler.html.ru.koi8-r
- index.html.de
- index.html.en
- index.html.ja.euc-jp
- index.html.ko.euc-kr
- index.html.ru.koi8-r
- install.html
  - #fragments
    - compile
    - configure
    - customize

- dbm
- download
- extract
- install
- overview
- page-header
- requirements
- test
- upgrading

install.html.de

- #fragments
  - compile
  - configure
  - customize
  - download
  - extract
  - install
  - overview
  - page-header
  - requirements
  - test
  - upgrading

install.html.en

install.html.ja.euc-jp

- #fragments
  - compile
  - configure
  - customize
  - download
  - extract
  - install
  - overview
  - page-header
  - requirements
  - test
  - upgrading

install.html.ko.euc-kr

- #fragments
  - compile
  - configure
  - customize
  - download
  - extract
  - install
  - overview
  - page-header
  - requirements
  - test
  - upgrading

- install.html.ru.koi8-r
  - #fragments
    - compile
    - configure
    - customize
    - download
    - extract
    - install
    - overview
    - page-header
    - requirements
    - test
- invoking.html
  - #fragments
    - boot
    - errors
    - info
    - page-header
    - startup
- invoking.html.de
  - #fragments
    - boot
    - errors
    - info
    - page-header
    - startup
- invoking.html.en
- invoking.html.ja.euc-jp
  - #fragments
    - boot
    - errors
    - info
    - page-header
    - startup
- invoking.html.ko.euc-kr
  - #fragments
    - boot
    - errors
    - info
    - page-header
    - startup
- invoking.html.ru.koi8-r
  - #fragments
    - boot
    - errors
    - info
    - page-header
    - startup
- license.html

- license.html.en
- logs.html
  - #fragments
    - accesslog
    - errorlog
    - other
    - page-header
    - piped
    - rotation
    - security
    - virtualhost
- logs.html.en
- logs.html.ja.euc-jp
  - #fragments
    - accesslog
    - errorlog
    - other
    - page-header
    - piped
    - rotation
    - security
    - virtualhosts
- logs.html.ko.euc-kr
  - #fragments
    - accesslog
    - errorlog
    - other
    - page-header
    - piped
    - rotation
    - security
    - virtualhost
- mpm.html
  - #fragments
    - choosing
    - defaults
    - introduction
    - page-header
- mpm.html.en
- mpm.html.ja.euc-jp
  - #fragments
    - choosing
    - defaults
    - introduction
    - page-header
- mpm.html.ko.euc-kr
- mpm.html.ru.koi8-r
  - #fragments
    - choosing

- defaults
- introduction
- page-header

new_features_2_0.html
- #fragments
  - core
  - module
  - page-header

new_features_2_0.html.de

new_features_2_0.html.en

new_features_2_0.html.fr

new_features_2_0.html.ja.euc-jp
- #fragments
  - core
  - module
  - page-header

new_features_2_0.html.ko.euc-kr

new_features_2_0.html.ru.koi8-r
- #fragments
  - core
  - module
  - page-header

sections.html
- #fragments
  - file-and-web
  - mergin
  - page-header
  - proxy
  - types
  - virtualhost
  - whatwhere

sections.html.en

sections.html.ja.euc-jp
- #fragments
  - file-and-web
  - mergin
  - page-header
  - proxy
  - types
  - virtualhost
  - whatwhere

sections.html.ko.euc-kr

server-wide.html
- #fragments
  - identification
  - locations
  - page-header
  - resource

server-wide.html.en

- server-wide.html.ja.euc-jp
  - #fragments
    - identification
    - locations
    - page-header
    - resource
- server-wide.html.ko.euc-kr
  - #fragments
    - identification
    - locations
    - page-header
    - resource
- sitemap.html
  - #fragments
    - developer
    - faq
    - howto
    - index
    - misc
    - modules
    - page-header
    - platform
    - programs
    - release
    - ssl
    - using
    - vhosts
- sitemap.html.de
  - #fragments
    - developer
    - faq
    - howto
    - index
    - misc
    - modules
    - page-header
    - platform
    - programs
    - release
    - ssl
    - using
    - vhosts
- sitemap.html.en
- sitemap.html.ja.euc-jp
- sitemap.html.ko.euc-kr
- stopping.html
  - #fragments
    - graceful
    - hup

- introduction
- page-header
- race
- term

stopping.html.de
- #fragments
  - graceful
  - hup
  - introduction
  - page-header
  - race
  - term

stopping.html.en

stopping.html.ja.euc-jp
- #fragments
  - graceful
  - hup
  - introduction
  - page-header
  - race
  - term

stopping.html.ko.euc-kr
- #fragments
  - graceful
  - hup
  - introduction
  - page-header
  - race
  - term

stopping.html.ru.koi8-r
- #fragments
  - graceful
  - hup
  - introduction
  - page-header
  - race
  - term

suexec.html
- #fragments
  - before
  - debug
  - enable
  - install
  - jabberwock
  - model
  - page-header
  - usage

suexec.html.en

suexec.html.ja.euc-jp

- #fragments
  - before
  - debug
  - enable
  - install
  - jabberwock
  - model
  - page-header
  - usage
- suexec.html.ko.euc-kr
  - #fragments
    - before
    - debug
    - enable
    - install
    - jabberwock
    - model
    - page-header
    - usage
- upgrading.html
  - #fragments
    - compile-time