FooPhones Audit

Submitted by

Niladri Mitra

Under the guidance of

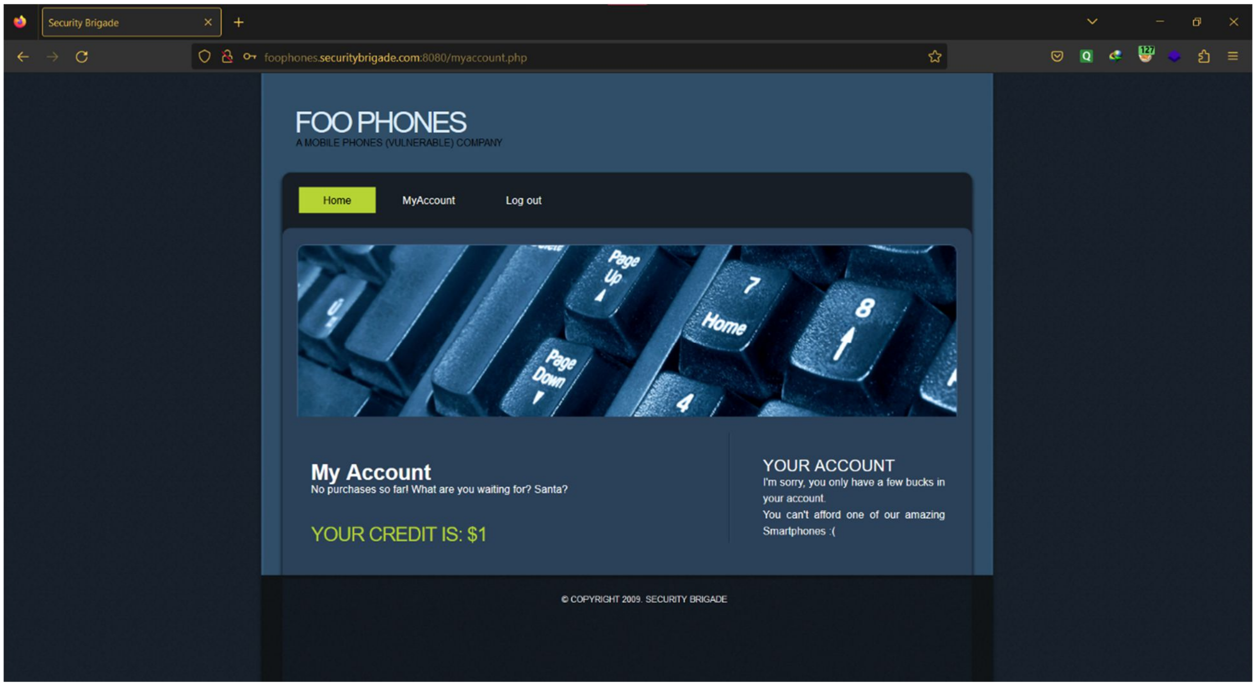
Rahul Shaw

Brute Force	
Risk Level	High
Description	It was+ observed that in the absence of lockout threshold, on running a brute force attack using a dictionary of known usernames and passwords, the attacker can obtain the correct username and password quickly.
Impact	Increased vulnerability to brute force attacks: Without a lockout threshold, attackers can make unlimited login attempts without any restrictions. This greatly increases the chances of successfully guessing the correct username and password combination, as the attacker can continue trying until they find the right one. Increased risk of unauthorized access: Successful brute force attacks can lead to unauthorized access to user accounts, potentially compromising sensitive information, such as personal data, financial details, or private communications.
Recommendation	It is recommended to implement the following configurations: 1. **Hide administrator and user login pages** by changing their default pages. 2. Use **longer passwords** with a large variety of characters. 3. Change the **default 'admin' username** to a unique one. 4. Implement an **account lockout** policy. https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks
Affected URL and Ports	http://foophones.securitybrigade.com:8080/login.php

Evidence (PoC)

i) On intercepting the authentication packet in BurpSuite and using BurpSuite Infiltrator, the correct account credentials could be retrieved using a dictionary of pre-defined values.

ii) On entering the credentials 'admin' and 'admin' on the login page, access was granted.



FOO PHONES

A MOBILE PHONES (VULNERABLE) COMPANY

My Account

No purchases so far! What are you waiting for? Santa?

YOUR CREDIT IS: $1

YOUR ACCOUNT

I'm sorry, you only have a few bucks in your account.

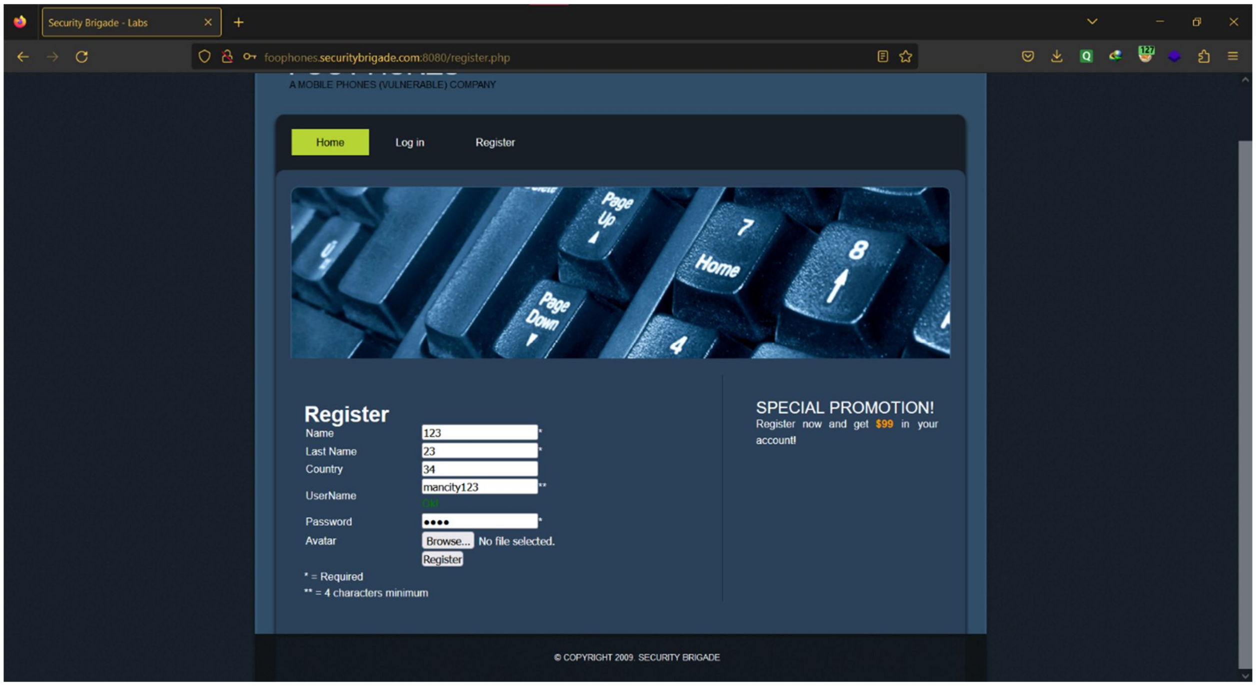
You can't afford one of our amazing Smartphones :(

© COPYRIGHT 2009. SECURITY BRIGADE

Cross Site Request Forgery (CSRF)	
Risk Level	Med
Description	It was observed that the attacker can create a duplicate link and send it to the victim which would immediately reset the password.
Impact	A successful CSRF attack can result in damaged client relationships, unauthorized fund transfers, changed passwords and data theft—including stolen session cookies.
Recommendation	It is recommended to implement the following configurations: 1. **Double-Submitting Cookies:** Two cookies are sent with each request – one in cookie header and one in custom header. 2. **Custom Headers for Requests:** Custom headers should be added to the requests which cannot be understood by the attacker. 3. **Enabling User Interaction:** User interaction should be required before any state-changing actions (eg. Captcha, OTP etc) https://www.imperva.com/learn/application-security/csrf-cross-site-request-forgery/?utm_content=&gad=1
Affected URL and Ports	http://foophones.securitybrigade.com:8080/register.php

Evidence (PoC)

When no CRSF token was found, a duplicate site was generated using CRSF PoC of BurpSuite and contained the malicious credentials. It was sent to the victim, who upon clicking it changed the credentials to the malicious ones.


Security Brigade - Labs
foophones.securitybrigade.com:8080/register.php
A MOBILE PHONES (VULNERABLE) COMPANY
Home
Log in
Register

Register

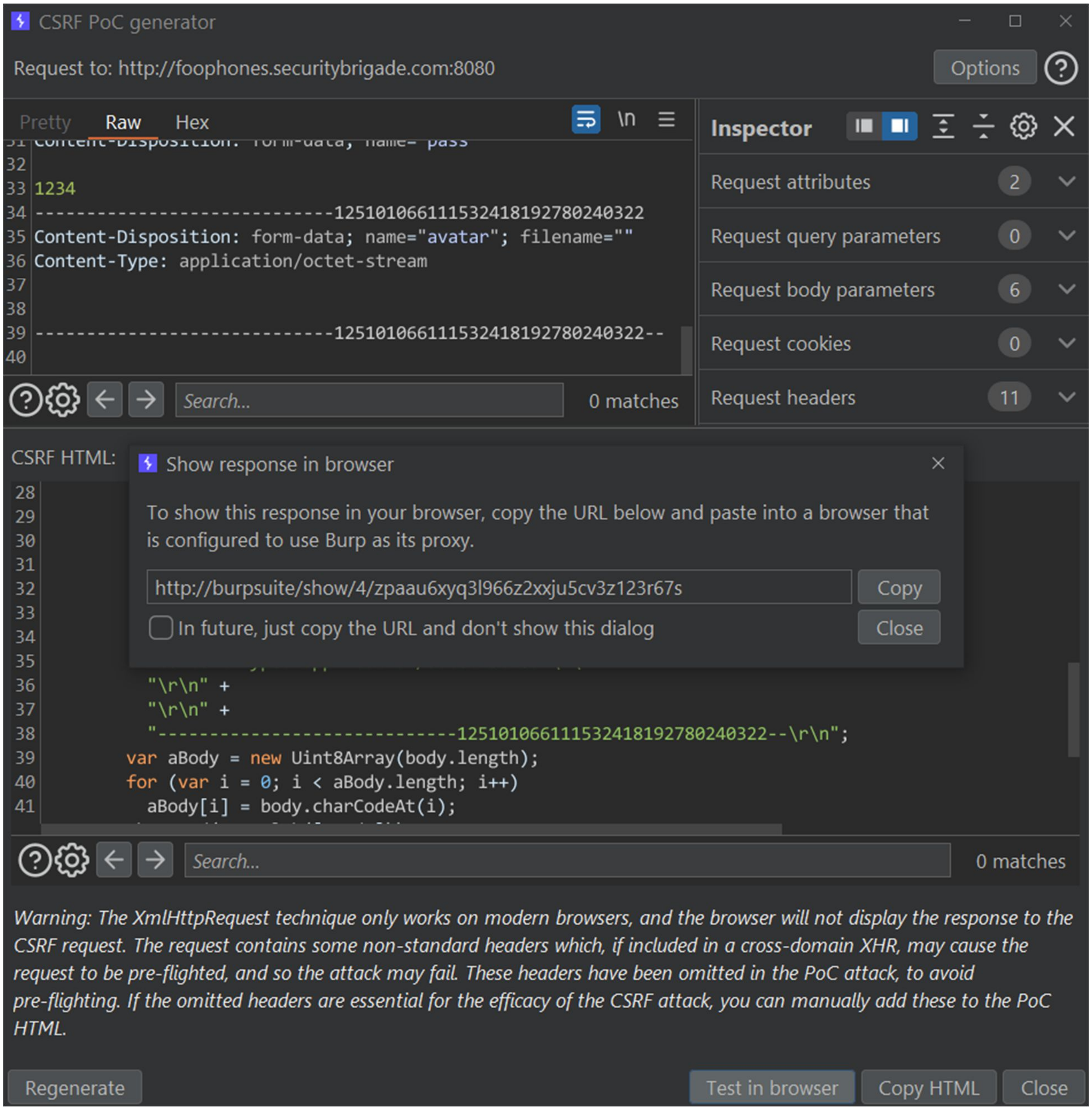
Name	123 *
Last Name	23 *
Country	34
UserName	mancity123 ** Ok!
Password	•••• *
Avatar	Browse... No file selected.
	Register

* = Required
** = 4 characters minimum

SPECIAL PROMOTION!
Register now and get $99 in your account!

© COPYRIGHT 2009. SECURITY BRIGADE

The username ‘mancity123’ was not originally present in the database.



Request to: http://foophones.securitybrigade.com:8080

```
Content-Disposition: form-data; name="pass"

1234
----------------------------1251010661115324181927802403222
Content-Disposition: form-data; name="avatar"; filename=""
Content-Type: application/octet-stream


----------------------------1251010661115324181927802403222--

```

To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

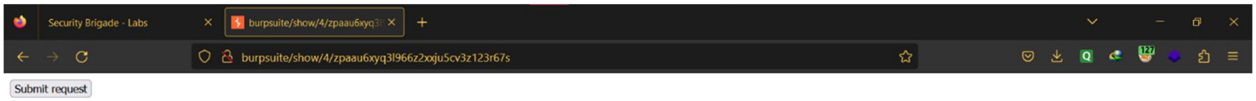
http://burpsuite/show/4/zpaau6xyq3l966z2xxju5cv3z123r67s

☐ In future, just copy the URL and don't show this dialog

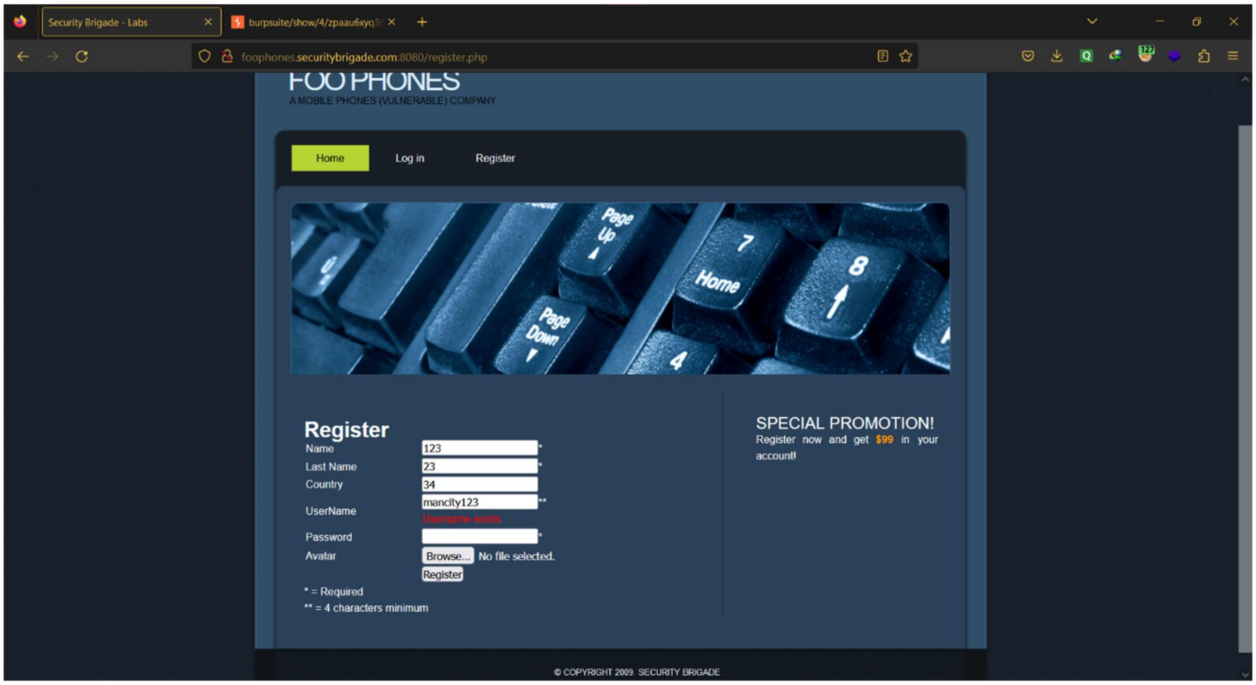
```
          "\r\n" +
          "\r\n" +
          "----------------------------1251010661115324181927802403222--\r\n";
        var aBody = new Uint8Array(body.length);
        for (var i = 0; i < aBody.length; i++)
          aBody[i] = body.charCodeAt(i);
```

Warning: The XmlHttpRequest technique only works on modern browsers, and the browser will not display the response to the CSRF request. The request contains some non-standard headers which, if included in a cross-domain XHR, may cause the request to be pre-flighted, and so the attack may fail. These headers have been omitted in the PoC attack, to avoid pre-flighting. If the omitted headers are essential for the efficacy of the CSRF attack, you can manually add these to the PoC HTML.

CSRF PoC is created using Burpsuite and sent to the victim


Security Brigade - Labs
burpsuite/show/4/zpaau6xyq3l
burpsuite/show/4/zpaau6xyq3l966z2xxju5cv3z123r67s
Submit request

Victim clicks on the ‘submit button’ and the new account gets registered.


Security Brigade - Labs
burpsuite/show/4/zpaau6xyq3l
foophones.securitybrigade.com:8080/register.php
FOO PHONES
A MOBILE PHONES (VULNERABLE) COMPANY
Home
Log in
Register
SPECIAL PROMOTION!
Register now and get $99 in your account!
Browse...
Register
© COPYRIGHT 2009. SECURITY BRIGADE

Register

Name 123 *
Last Name 23 *
Country 34
UserName mancity123 **
Username exists
Password *
Avatar No file selected.

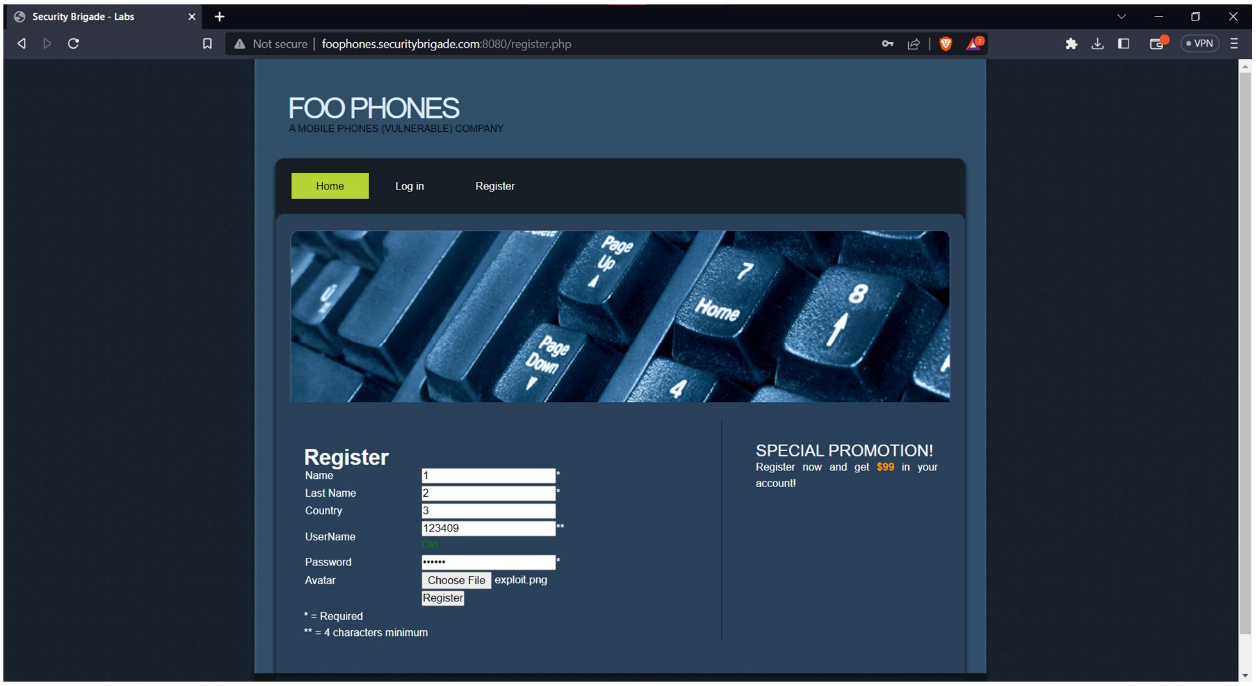
* = Required
** = 4 characters minimum

The account has been already entered in the database.

File Upload	
Risk Level	Med
Description	It was observed that all types of files can be uploadedThe attacker can upload all types of files in the avatar section.
Impact	If the uploaded file contains an exploit or malware which can leverage a vulnerability in server-side file handling, the file could be used to gain control of the server, causing severe business consequences and reputational damage.
Recommendation	It is recommended to implement the following configurations: 1. Allow only certain file extensions using a whitelist checker. 2. Set the maximum file size and file length according to requirement. 3. Name the files stored on the server randomly or use hash instead of the user-input names. 4. After the file has been uploaded, do not display its path. https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
Affected URL and Ports	http://127.0.0.1/dvwa/vulnerabilities/upload/ (8080)

Evidence (PoC)

Step 1: On uploading a file of the accepted format image, it was accepted.



FOO PHONES
A MOBILE PHONES (VULNERABLE) COMPANY

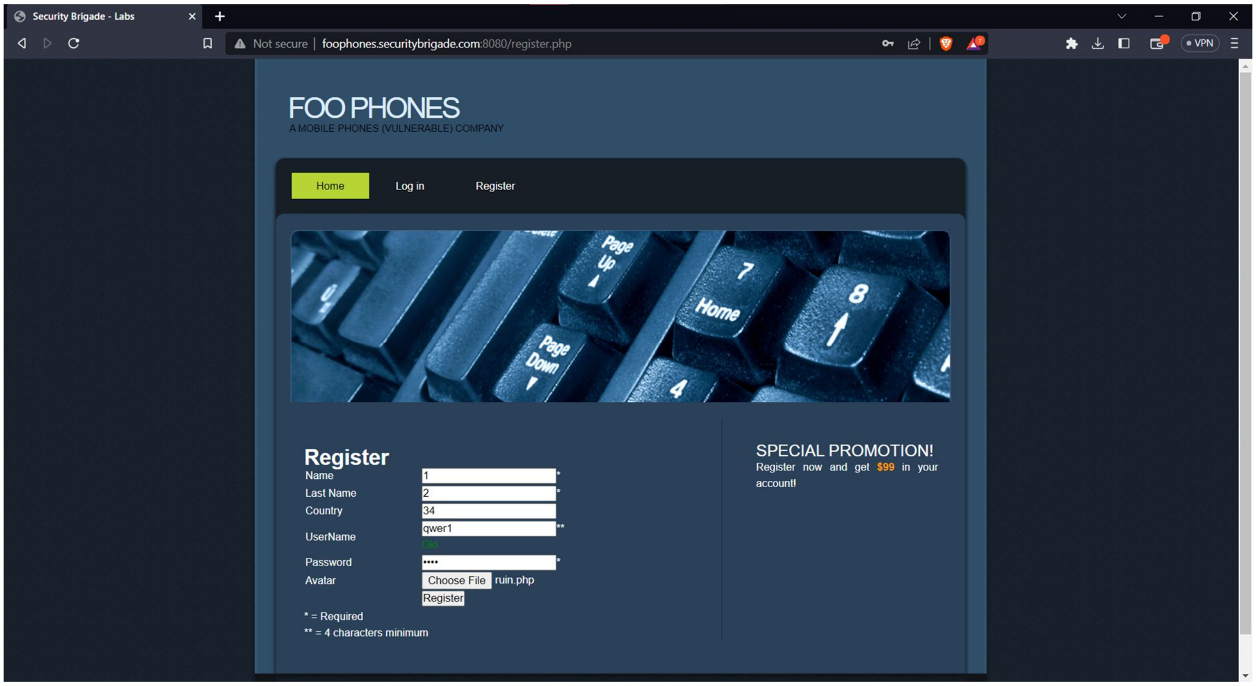
Register

Name	1 *
Last Name	2 *
Country	3
UserName	123409 ** Ok!
Password	•••••• *
Avatar	Choose File exploit.png
	Register

* = Required
** = 4 characters minimum

SPECIAL PROMOTION!
Register now and get $99 in your account!

Step 2: On uploading a file of other formats containing malicious code, it was accepted.



FOO PHONES
A MOBILE PHONES (VULNERABLE) COMPANY

Register

Name	1 *
Last Name	2 *
Country	34
UserName	qwer1 ** Ok!
Password	•••• *
Avatar	Choose File ruin.php
	Register

* = Required
** = 4 characters minimum

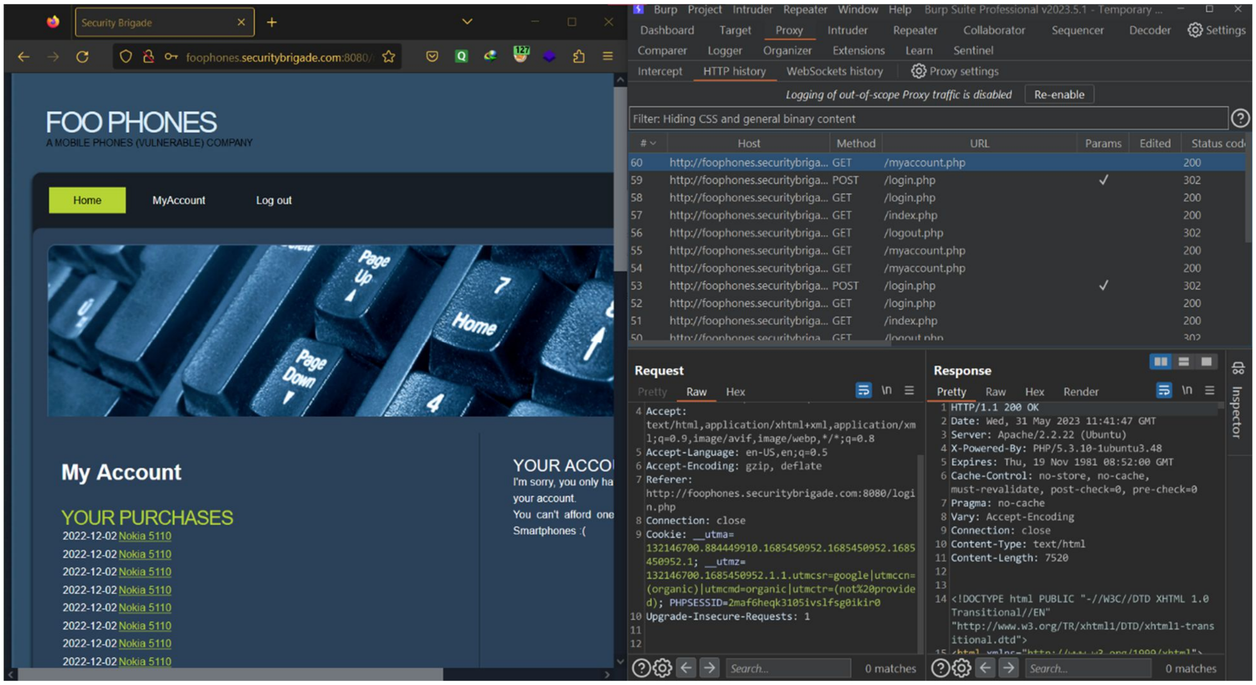
SPECIAL PROMOTION!
Register now and get $99 in your account!

Weak Session ID	
Risk Level	Med
Description	It was observed that the session ID of a user never changes and can be easily copied and used by the attacker.
Impact	This vulnerability allows an attacker to predetermine the session token value used by the victim. When the user logs in to a web application using that ID, the attacker knows the victim’s valid session ID and can use it to gain access to the user’s account.
Recommendation	It is recommended to implement the following configurations: 1. Always create a new session ID upon authentication. 2. Prevent MITM attacks with HTTPS, HSTS, and proper TLS security settings. 3. Prevent cookie overwrites by protecting the cookie with Host-prefix and Secure attribute. https://affinity-it-security.com/how-to-prevent-session-management-vulnerabilities/
Affected URL and Ports	http://foophones.securitybrigade.com:8080/login.php

PoC

Step 1: On changing the account credentials, the session ID is not changed.

Step 2: On logging out, the same session ID is sent in every request.


Security Brigade
foophones.securitybrigade.com:8080/
Burp Project Intruder Repeater Window Help Burp Suite Professional v2023.5.1 - Temporary ...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Organizer Extensions Learn Sentinel
Intercept HTTP history WebSockets history Proxy settings
Re-enable
Pretty Raw Hex
Pretty Raw Hex Render
Search...
0 matches
Inspector

FOO PHONES
A MOBILE PHONES (VULNERABLE) COMPANY

Home MyAccount Log out

My Account

YOUR PURCHASES

2022-12-02 Nokia 5110
2022-12-02 Nokia 5110
2022-12-02 Nokia 5110
2022-12-02 Nokia 5110
2022-12-02 Nokia 5110
2022-12-02 Nokia 5110
2022-12-02 Nokia 5110
2022-12-02 Nokia 5110

YOUR ACCO
I'm sorry, you only ha
your account.
You can't afford one
Smartphones :(

Logging of out-of-scope Proxy traffic is disabled

Filter: Hiding CSS and general binary content

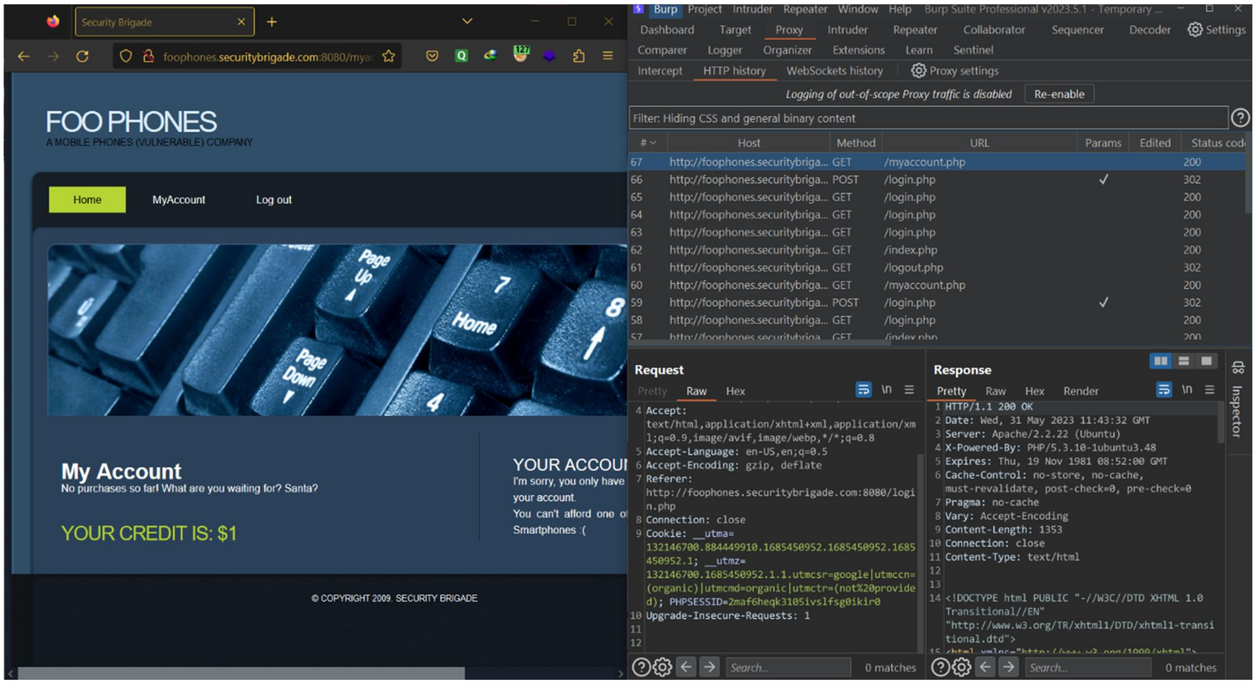
#	Host	Method	URL	Params	Edited	Status cod
60	http://foophones.securitybriga...	GET	/myaccount.php			200
59	http://foophones.securitybriga...	POST	/login.php	✓		302
58	http://foophones.securitybriga...	GET	/login.php			200
57	http://foophones.securitybriga...	GET	/index.php			200
56	http://foophones.securitybriga...	GET	/logout.php			302
55	http://foophones.securitybriga...	GET	/myaccount.php			200
54	http://foophones.securitybriga...	GET	/myaccount.php			200
53	http://foophones.securitybriga...	POST	/login.php	✓		302
52	http://foophones.securitybriga...	GET	/login.php			200
51	http://foophones.securitybriga...	GET	/index.php			200
50	http://foophones.securitybriga...	GET	/logout.php			302

Request

```
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:
http://foophones.securitybrigade.com:8080/login.php
Connection: close
Cookie: __utma=
132146700.884449910.1685450952.1685450952.1685450952.1; __utmz=
132146700.1685450952.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided); PHPSESSID=2maf6heqk3105ivslfsg0ikir0
Upgrade-Insecure-Requests: 1
```

Response

```
HTTP/1.1 200 OK
Date: Wed, 31 May 2023 11:41:47 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.48
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache,
must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Connection: close
Content-Type: text/html
Content-Length: 7520


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```


Security Brigade
foophones.securitybrigade.com:8080/mya
Burp Project Intruder Repeater Window Help Burp Suite Professional v2023.5.1 - Temporary ...
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings
Comparer Logger Organizer Extensions Learn Sentinel
Intercept HTTP history WebSockets history Proxy settings
Re-enable
Pretty Raw Hex
Pretty Raw Hex Render
Search...
0 matches
Inspector

FOO PHONES
A MOBILE PHONES (VULNERABLE) COMPANY

Home MyAccount Log out

My Account

No purchases so far! What are you waiting for? Santa?

YOUR CREDIT IS: $1

YOUR ACCOUI
I'm sorry, you only have
your account.
You can't afford one o
Smartphones :(

© COPYRIGHT 2009. SECURITY BRIGADE

Logging of out-of-scope Proxy traffic is disabled

Filter: Hiding CSS and general binary content

#	Host	Method	URL	Params	Edited	Status cod
67	http://foophones.securitybriga...	GET	/myaccount.php			200
66	http://foophones.securitybriga...	POST	/login.php	✓		302
65	http://foophones.securitybriga...	GET	/login.php			200
64	http://foophones.securitybriga...	GET	/login.php			200
63	http://foophones.securitybriga...	GET	/login.php			200
62	http://foophones.securitybriga...	GET	/index.php			200
61	http://foophones.securitybriga...	GET	/logout.php			302
60	http://foophones.securitybriga...	GET	/myaccount.php			200
59	http://foophones.securitybriga...	POST	/login.php	✓		302
58	http://foophones.securitybriga...	GET	/login.php			200
57	http://foophones.securitybriga...	GET	/index.php			200

Request

```
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:
http://foophones.securitybrigade.com:8080/login.php
Connection: close
Cookie: __utma=
132146700.884449910.1685450952.1685450952.1685450952.1; __utmz=
132146700.1685450952.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided); PHPSESSID=2maf6heqk3105ivslfsg0ikir0
Upgrade-Insecure-Requests: 1
```

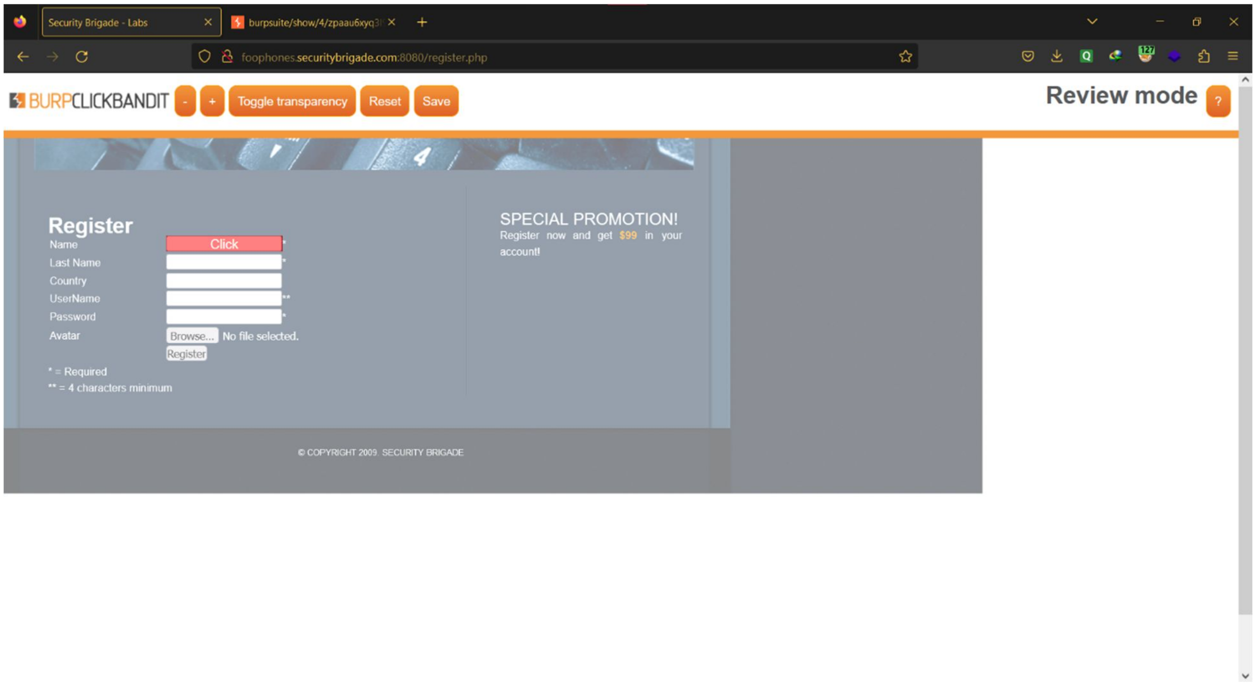
Response

```
HTTP/1.1 200 OK
Date: Wed, 31 May 2023 11:43:32 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.48
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache,
must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1353
Connection: close
Content-Type: text/html


<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

Clickjacking	
Risk Level	Med
Description	It was observed that the attacker can make the victim click on underlying buttons of the website while using a harmless looking website on top of it.
Impact	The attacker can make the victim select other not so important items from the shopping list and buy it without the victim knowing.
Recommendation	It is recommended to implement the following configurations: 1. Sending the proper Content Security Policy (CSP) frame-ancestors directive response headers that instruct the browser to not allow framing from other domains. 2. Properly setting authentication cookies with SameSite = Strict (or Lax), unless they explicitly need None (which is rare). 3. Employing defensive code in the UI to ensure that the current frame is the most top-level window. https://owasp.org/www-community/attacks/Clickjacking
Affected URL and Ports	i) http://foophones.securitybrigade.com:8080/login.php ii) http://foophones.securitybrigade.com:8080/index.php iii) http://foophones.securitybrigade.com:8080/register.php

PoC

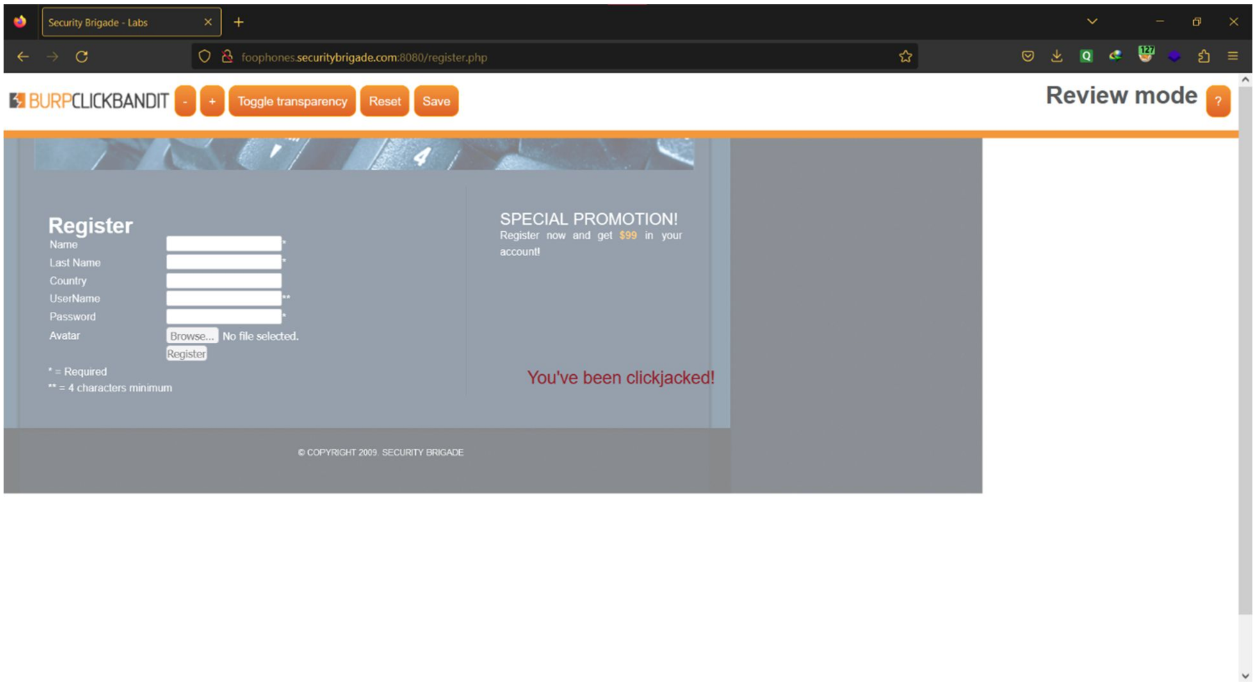
On using the clickbandit function on the site, it was seen that the underlying website was allowing the victim to click on the items.



* = Required
** = 4 characters minimum

SPECIAL PROMOTION!
Register now and get $99 in your account!

© COPYRIGHT 2009 SECURITY BRIGADE



* = Required
** = 4 characters minimum

SPECIAL PROMOTION!
Register now and get $99 in your account!

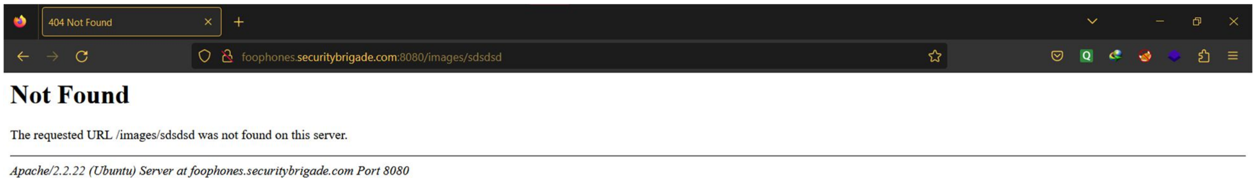
You've been clickjacked!

© COPYRIGHT 2009 SECURITY BRIGADE

Information Disclosure	
Risk Level	🟥 High
Description	It was observed that on encountering any error in the website URL, information about the backend server version and configuration is revealed.
Impact	Attackers can use this information to identify vulnerabilities in the server software and exploit them. In addition, if a particular web server version is known to be vulnerable to a specific exploit, the attacker would just need to use that exploit as part of their assault on the target web server. This can lead to unauthorized access to the server and sensitive data, loss of reputation, financial loss, and legal liabilities.
Recommendation	It is recommended to implement the following configurations: 1. Modifying server header field to not display such information. 2. Web Application Firewall (WAF) can be configured to block requests containing sensitive information.
Affected URL and Ports	http://foophones.securitybrigade.com:8080/

PoC

On entering a wrong URL, an error message is displayed along with the server information.



Not Found

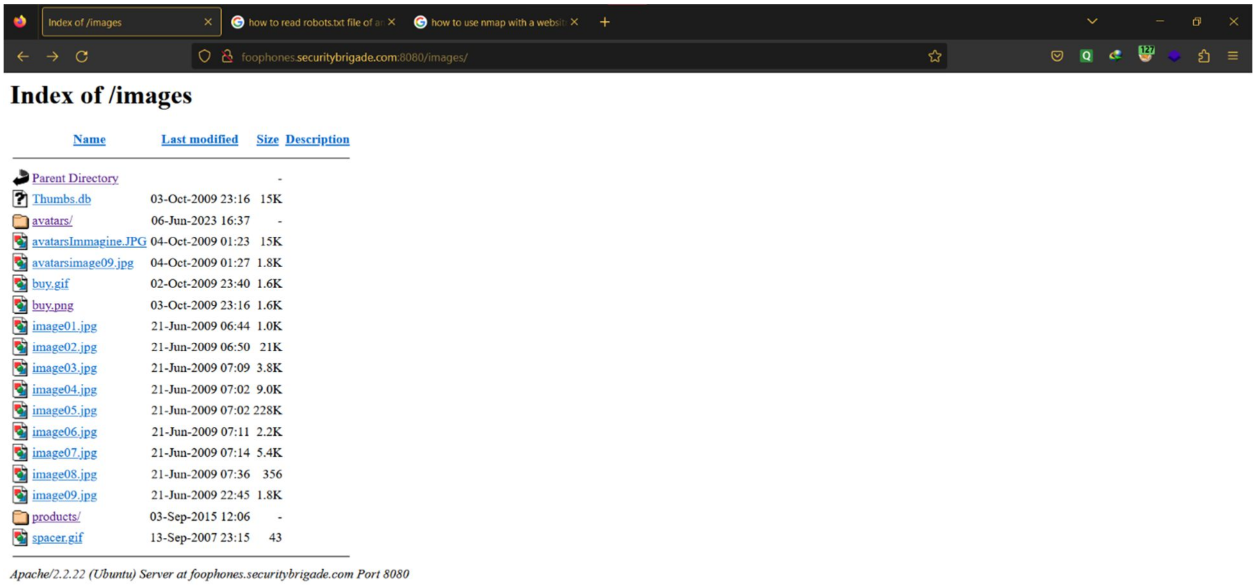
The requested URL /images/sdsdsd was not found on this server.

Apache/2.2.22 (Ubuntu) Server at foophones.securitybrigade.com Port 8080

Dir Listing	
Risk Level	Medium
Description	It is observed that on entering known directory names, the entire list is revealed.
Impact	Directory listing can lead to leaking sensitive information which can result in a huge impact on the business1. However, directory listings themselves do not necessarily constitute a security vulnerability.
Recommendation	It is recommended to implement the following configurations: 1. Create blank index.html and place it in each directory. This will prevent directory listing and display a blank page in the web browser. 2. Disable directory listing for the entire application. 3. In business needs, create a directory and enable directory listing only for that alone.
Affected URL and Ports	http://foophones.securitybrigade.com:8080/

PoC

On adding /images to the URL, the entire list of images files is displayed.



Index of /images
how to read robots.txt file of a
how to use nmap with a websit
127

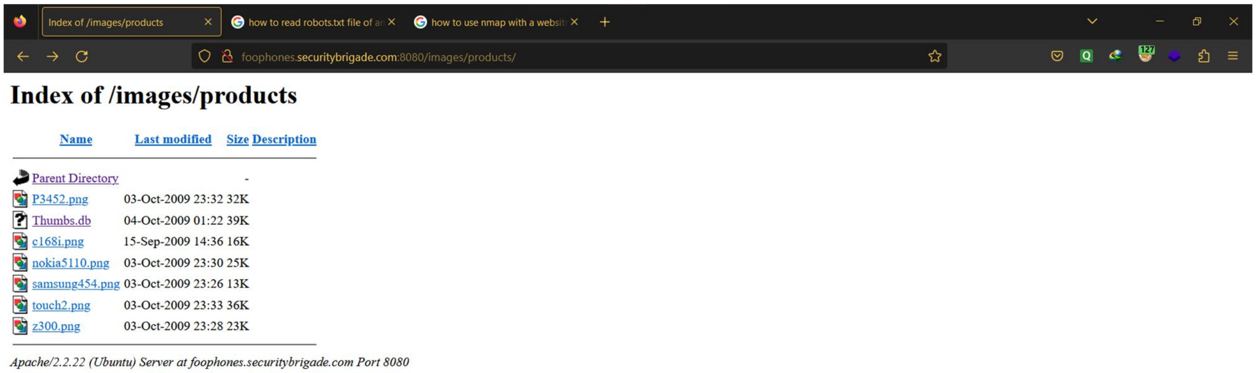
foophones.securitybrigade.com:8080/images/

Index of /images

Name	Last modified	Size	Description
Parent Directory		-	
Thumbs.db	03-Oct-2009 23:16	15K	
avatars/	06-Jun-2023 16:37	-	
avatarsImmagine.JPG	04-Oct-2009 01:23	15K	
avatarsimage09.jpg	04-Oct-2009 01:27	1.8K	
buy.gif	02-Oct-2009 23:40	1.6K	
buy.png	03-Oct-2009 23:16	1.6K	
image01.jpg	21-Jun-2009 06:44	1.0K	
image02.jpg	21-Jun-2009 06:50	21K	
image03.jpg	21-Jun-2009 07:09	3.8K	
image04.jpg	21-Jun-2009 07:02	9.0K	
image05.jpg	21-Jun-2009 07:02	228K	
image06.jpg	21-Jun-2009 07:11	2.2K	
image07.jpg	21-Jun-2009 07:14	5.4K	
image08.jpg	21-Jun-2009 07:36	356	
image09.jpg	21-Jun-2009 22:45	1.8K	
products/	03-Sep-2015 12:06	-	
spacer.gif	13-Sep-2007 23:15	43	

Apache/2.2.22 (Ubuntu) Server at foophones.securitybrigade.com Port 8080

On adding /scripts to the URL, the entire list of JavaScript files is displayed.

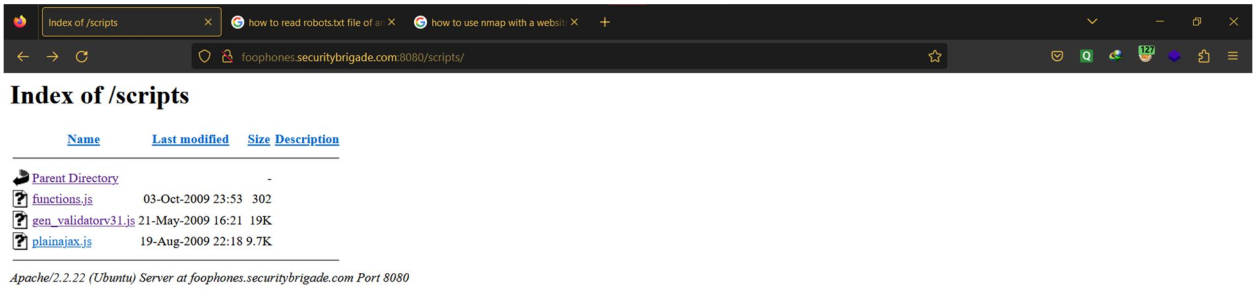

Index of /images/products
how to read robots.txt file of a
how to use nmap with a websit
foophones.securitybrigade.com:8080/images/products/
127

Index of /images/products

Name	Last modified	Size	Description
Parent Directory		-	
P3452.png	03-Oct-2009 23:32	32K	
Thumbs.db	04-Oct-2009 01:22	39K	
c168i.png	15-Sep-2009 14:36	16K	
nokia5110.png	03-Oct-2009 23:30	25K	
samsung454.png	03-Oct-2009 23:26	13K	
touch2.png	03-Oct-2009 23:33	36K	
z300.png	03-Oct-2009 23:28	23K	

Apache/2.2.22 (Ubuntu) Server at foophones.securitybrigade.com Port 8080

On adding /images/products to the URL, the entire list of product images files is displayed.


Index of /scripts
how to read robots.txt file of a
how to use nmap with a websit
foophones.securitybrigade.com:8080/scripts/
127

Index of /scripts

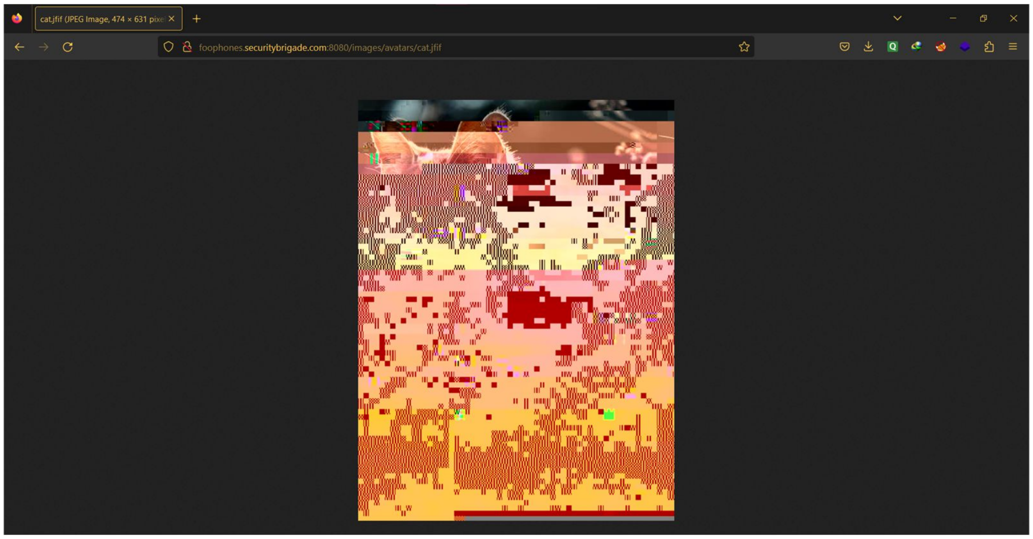
Name	Last modified	Size	Description
Parent Directory		-	
functions.js	03-Oct-2009 23:53	302	
gen_validatorv31.js	21-May-2009 16:21	19K	
plainajax.js	19-Aug-2009 22:18	9.7K	

Apache/2.2.22 (Ubuntu) Server at foophones.securitybrigade.com Port 8080

Local File Inclusion (LFI)	
Risk Level	High
Description	It was observed that files stored in the backend can be accessed and downloaded by entering the corresponding URLs.
Impact	The business impact of LFI can be severe as it can lead to sensitive data exposure, data tampering, and even complete server compromise. Attackers can use LFI to gain access to sensitive files such as configuration files, password files, and other sensitive data.
Recommendation	It is recommended to implement the following configurations: 1. Save all file paths in a secure database and give an ID for every single one, this way users only get to see their ID without viewing or altering the path. 2. Use verified and secured whitelist files and ignore everything else. 3. Check for scripts that take filenames as parameters. https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/local-file-inclusion/
Affected URL and Ports	http://foophones.securitybrigade.com:8080/images/avatars http://foophones.securitybrigade.com:8080/images/products http://foophones.securitybrigade.com:8080/images/

PoC

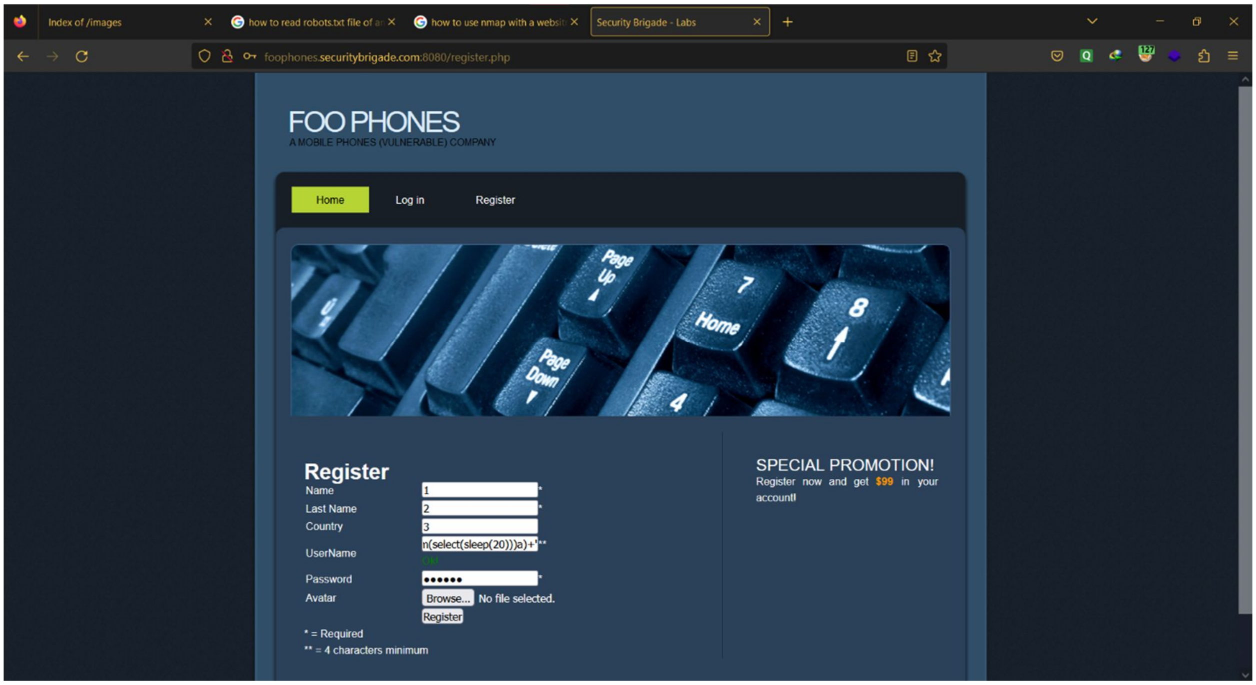
On adding /images/avatars/cat.jfif to the URL, the corresponding image is displayed.


cat.jfif (JPEG Image, 474 × 631 pixe
foophones.securitybrigade.com:8080/images/avatars/cat.jfif

SQL Injection	
Risk Level	🟥 High
Description	It was observed that on running time-based SQL injections, the response from the server is delayed by the specified time.
Impact	A successful attack can result in the unauthorized viewing of user lists, the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database, all of which are highly detrimental to a business.
Recommendation	Prepared statements or parameterized queries should be used to ensure that user input is properly sanitized and does not contain any malicious code. https://www.acunetix.com/vulnerabilities/web/content-type-is-not-specified/
Affected URL and Ports	http://foophones.securitybrigade.com:8080/register.php

PoC

i) On entering HICmENII'+(select*from(select(sleep(20)))a)+' in the username field of registration page, the server responds after 20 seconds.



Register

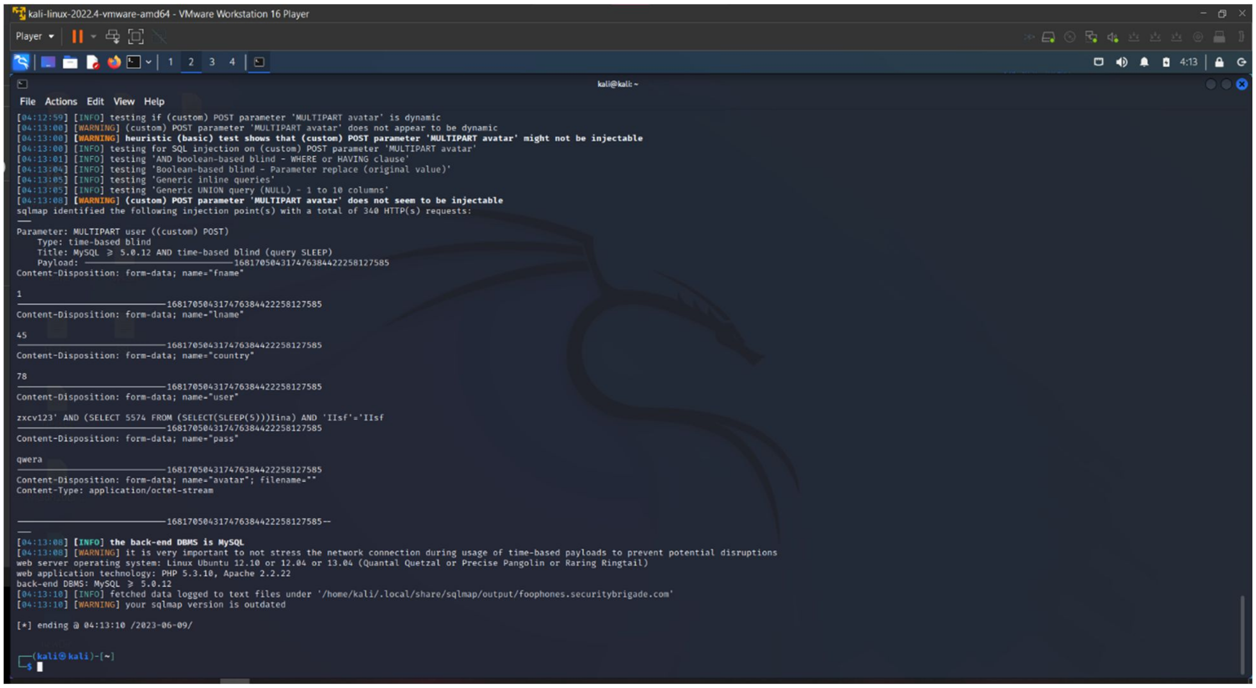
Name	1 *
Last Name	2 *
Country	3
UserName	n(select(sleep(20)))a)+' ** Ok!
Password	•••••• *
Avatar	Browse... No file selected.
	Register

* = Required
** = 4 characters minimum

SPECIAL PROMOTION!
Register now and get $99 in your account!

Index of /images
how to read robots.txt file of a
how to use nmap with a websi
Security Brigade - Labs
foophones.securitybrigade.com:8080/register.php
FOO PHONES
A MOBILE PHONES (VULNERABLE) COMPANY
Home
Log in
Register

ii) On using sqlmap, more similar commands are found which have a similar effect.



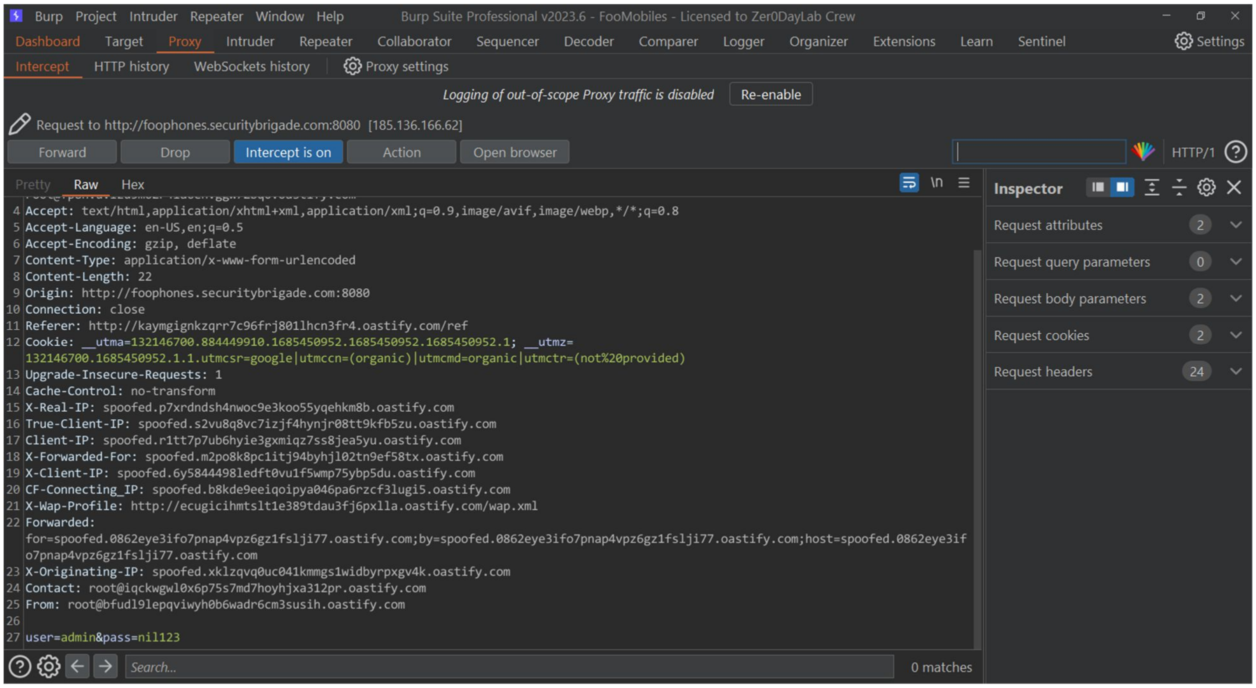
kali-linux-2022.4-vmware-amd64 - VMware Workstation 16 Player
Player
1
2
3
4
4:13
kali@kali: ~
File
Actions
Edit
View
Help

```
[04:12:59] [INFO] testing if (custom) POST parameter 'MULTIPART avatar' is dynamic
[04:13:00] [WARNING] (custom) POST parameter 'MULTIPART avatar' does not appear to be dynamic
[04:13:00] [WARNING] heuristic (basic) test shows that (custom) POST parameter 'MULTIPART avatar' might not be injectable
[04:13:00] [INFO] testing for SQL injection on (custom) POST parameter 'MULTIPART avatar'
[04:13:01] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[04:13:04] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[04:13:05] [INFO] testing 'Generic inline queries'
[04:13:05] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[04:13:08] [WARNING] (custom) POST parameter 'MULTIPART avatar' does not seem to be injectable
sqlmap identified the following injection point(s) with a total of 340 HTTP(s) requests:
---
Parameter: MULTIPART user ((custom) POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: ----------------------------168170504317476384422258127585
Content-Disposition: form-data; name="fname"

1
----------------------------168170504317476384422258127585
Content-Disposition: form-data; name="lname"

45
----------------------------168170504317476384422258127585
Content-Disposition: form-data; name="country"

78
----------------------------168170504317476384422258127585
Content-Disposition: form-data; name="user"

zxcv123' AND (SELECT 5574 FROM (SELECT(SLEEP(5)))Iina) AND 'IIsf'='IIsf
----------------------------168170504317476384422258127585
Content-Disposition: form-data; name="pass"

qwera
----------------------------168170504317476384422258127585
Content-Disposition: form-data; name="avatar"; filename=""
Content-Type: application/octet-stream


----------------------------168170504317476384422258127585--
---
[04:13:08] [INFO] the back-end DBMS is MySQL
[04:13:08] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
web server operating system: Linux Ubuntu 12.10 or 12.04 or 13.04 (Quantal Quetzal or Precise Pangolin or Raring Ringtail)
web application technology: PHP 5.3.10, Apache 2.2.22
back-end DBMS: MySQL ≥ 5.0.12
[04:13:10] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/foophones.securitybrigade.com'
[04:13:10] [WARNING] your sqlmap version is outdated

[*] ending @ 04:13:10 /2023-06-09/


┌──(kali㉿kali)-[~]
└─$ 
```

Cleartext Submission of Password	
Risk Level	Med
Description	It was observed that on intercepting requests from login or register pages, the user credentials are visible.
Impact	When passwords are sent in clear text, it becomes easy for the attacker to sniff the network and get the sensitive data.
Recommendation	It is recommended to implement the following configurations: 1. Use encryption: Implement secure encryption protocols, such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL), to ensure that data transmitted over networks is encrypted. 2. Hash and salt passwords: Use strong one-way hashing algorithms like bcrypt, scrypt, or Argon2 to convert passwords into irreversible hash values. Additionally, apply a unique salt to each password before hashing to enhance security. 3. Implement secure authentication protocols: Use industry-standard authentication protocols like OAuth, OpenID Connect, or SAML, which are designed to securely handle user authentication. These protocols offload the responsibility of password handling to trusted third-party providers. https://portswigger.net/kb/issues/00300100_cleartext-submission-of-password
Affected URL and Ports	http://foophones.securitybrigade.com:8080/register.php http://foophones.securitybrigade.com:8080/login.php

PoC

On intercepting request from login and register pages, the credentials are visible in plaintext.

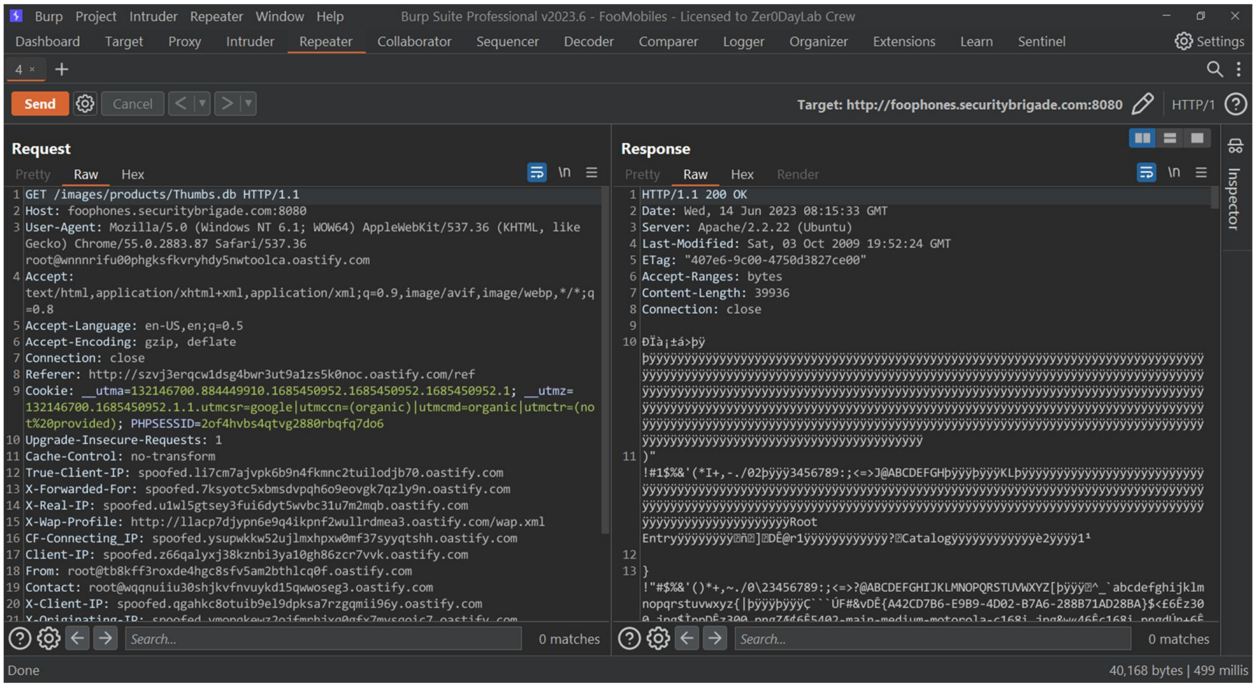

Burp Project Intruder Repeater Window Help
Burp Suite Professional v2023.6 - FooMobiles - Licensed to Zer0DayLab Crew
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Sentinel
Settings
Intercept HTTP history WebSockets history
Proxy settings
Logging of out-of-scope Proxy traffic is disabled
Re-enable
Request to http://foophones.securitybrigade.com:8080 [185.136.166.62]
Forward
Drop
Intercept is on
Action
Open browser
HTTP/1
Pretty Raw Hex
\n
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 2
Request headers 24
Search...
0 matches

```
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 22
Origin: http://foophones.securitybrigade.com:8080
Connection: close
Referer: http://kaymgignkzqrr7c96frj801lhcn3fr4.oastify.com/ref
Cookie: __utma=132146700.884449910.1685450952.1685450952.1685450952.1; __utmz=
132146700.1685450952.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided)
Upgrade-Insecure-Requests: 1
Cache-Control: no-transform
X-Real-IP: spoofed.p7xrdndsh4nwoc9e3koo55yqehkm8b.oastify.com
True-Client-IP: spoofed.s2vu8q8vc7izjf4hynjr08tt9kfb5zu.oastify.com
Client-IP: spoofed.r1tt7p7ub6hyie3gxmiqz7ss8jea5yu.oastify.com
X-Forwarded-For: spoofed.m2po8k8pc1itj94byhjl02tn9ef58tx.oastify.com
X-Client-IP: spoofed.6y5844498ledft0vu1f5wmp75ybp5du.oastify.com
CF-Connecting_IP: spoofed.b8kde9eeiqoipya046pa6rzcf3lugi5.oastify.com
X-Wap-Profile: http://ecugicihmtslt1e389tdau3fj6pxlla.oastify.com/wap.xml
Forwarded:
for=spoofed.0862eye3ifo7pnap4vpz6gz1fslji77.oastify.com;by=spoofed.0862eye3ifo7pnap4vpz6gz1fslji77.oastify.com;host=spoofed.0862eye3if
o7pnap4vpz6gz1fslji77.oastify.com
X-Originating-IP: spoofed.xklzqvq0uc041kmmgs1widbyrpxgv4k.oastify.com
Contact: root@iqckwgwl0x6p75s7md7hoyhjxa312pr.oastify.com
From: root@bfudl9lepqviwyh0b6wadr6cm3susih.oastify.com

user=admin&pass=nil123
```

Content Type Unspecified	
Risk Level	High
Description	It was observed that on any type of content can be included in the website request and it would be processed without filtering any content.
Impact	If a response does not specify a content type, then the browser will usually analyze the response and attempt to determine the MIME type of its content. This can have unexpected results, and if the content contains any user-controllable data may lead to cross-site scripting or other client-side vulnerabilities.
Recommendation	For every response containing a message body, the application should include a single Content-type header that correctly and unambiguously states the MIME type of the content in the response body.
Affected URL and Ports	http://foophones.securitybrigade.com:8080/

PoC

On request a database file in a part of the application where image file is required, the request gets processed successfully.

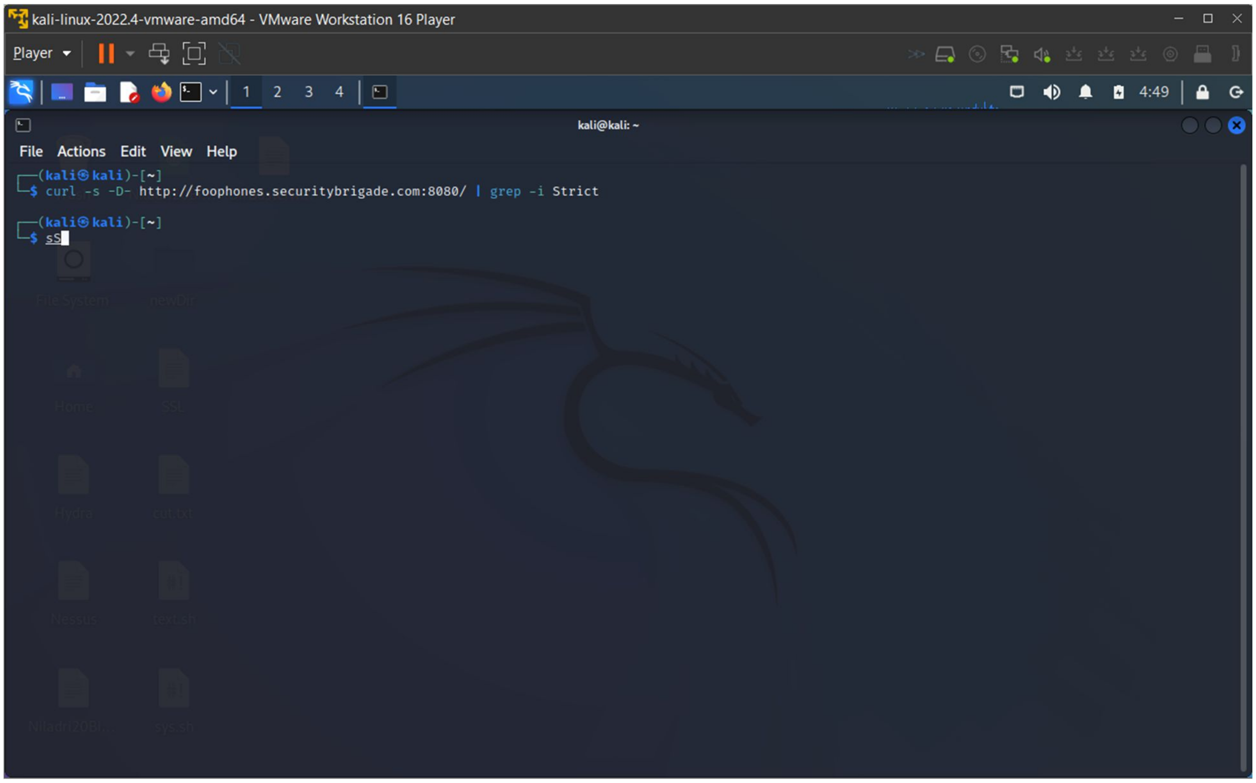


Request

```
GET /images/products/Thumbs.db HTTP/1.1
Host: foophones.securitybrigade.com:8080
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/55.0.2883.87 Safari/537.36
root@wnnnrifu00phgksfkvryhdy5nwtoolca.oastify.com
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
Connection: close
Referer: http://szvj3erqcw1dsg4bwr3ut9a1zs5k0noc.oastify.com/ref
Cookie: __utma=132146700.884449910.1685450952.1685450952.1685450952.1; __utmz=
132146700.1685450952.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(no
t%20provided); PHPSESSID=2of4hvbs4qtvg2880rbqfq7do6
Upgrade-Insecure-Requests: 1
Cache-Control: no-transform
True-Client-IP: spoofed.li7cm7ajvpk6b9n4fkmnc2tuilodjb70.oastify.com
X-Forwarded-For: spoofed.7ksyotc5xbmsdvpqh6o9eovgk7qzly9n.oastify.com
X-Real-IP: spoofed.u1wl5gtsey3fui6dyt5wvbc31u7m2mqb.oastify.com
X-Wap-Profile: http://llacp7djypn6e9q4ikpnf2wullrdmea3.oastify.com/wap.xml
CF-Connecting_IP: spoofed.ysupwkkw52ujlmxhpxw0mf37syyqtshh.oastify.com
Client-IP: spoofed.z66qalyxj38kznbi3ya10gh86zcr7vvk.oastify.com
From: root@tb8kff3roxde4hgc8sfv5am2bthlcq0f.oastify.com
Contact: root@wqqnuiiu30shjkvfnvuykd15qwwoseg3.oastify.com
X-Client-IP: spoofed.qgahkc8otuib9el9dpksa7rzgqmii96y.oastify.com
X-Originating-IP: spoofed.vmonqkewz2ojfmrhixq0qfx7mvsgoic7.oastify.com
```

Response

```
HTTP/1.1 200 OK
Date: Wed, 14 Jun 2023 08:15:33 GMT
Server: Apache/2.2.22 (Ubuntu)
Last-Modified: Sat, 03 Oct 2009 19:52:24 GMT
ETag: "407e6-9c00-4750d3827ce00"
Accept-Ranges: bytes
Content-Length: 39936
Connection: close

ÐÏà¡±á>þÿ
þÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
)"
!#1$%&'(*I+,-./02þÿÿÿ3456789:;<=>J@ABCDEFGHþÿÿÿþÿÿÿKLþÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿRoot
Entryÿÿÿÿÿÿÿÿÿ�ñ�]�DÊ@r1ÿÿÿÿÿÿÿÿÿÿÿÿÿ?�Catalogÿÿÿÿÿÿÿÿÿÿÿÿÿè2ÿÿÿÿ1¹

}
!"#$%&'()*+,~./0\23456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[þÿÿÿ�^_`abcdefghijklm
nopqrstuvwxyz{|þÿÿÿþÿÿÿÇ```ÚF#&vDÊ{A42CD7B6-E9B9-4D02-B7A6-288B71AD28BA}$<£6Êz30
0.jpg$ÌppDÊz300.png7Æ¢6Ê5402-main-medium-motorola-c168i.jpg&w«46Êc168i.pngdÚn+6Ê
```



kali-linux-2022.4-vmware-amd64 - VMware Workstation 16 Player
Player
1
2
3
4
4:49
kali@kali: ~
File
Actions
Edit
View
Help

```
┌──(kali㉿kali)-[~]
└─$ curl -s -D- http://foophones.securitybrigade.com:8080/ | grep -i Strict

┌──(kali㉿kali)-[~]
└─$ sS
```