Detection and Profiling of Covert Web Activity: An Integrated Analysis Approach

Contents

Executive Summary

The objective of this project was to identify and analyze websites that may serve as covert communication platforms by leveraging advanced Google search techniques ("Google dorking") in combination with manual and automated investigation into the nature and security posture of several suspicious websites. Using a combination of WHOIS lookups, IP tracking, Google dorks, webpage inspection, and Python automation, the analysis focused on identifying covert behaviors, security vulnerabilities, and site authenticity. Particular attention was given to form inputs, cookie security, and exposed files, providing a holistic view of each site's visibility and risk profile.

Introduction

he purpose of this report is to analyze potentially covert and suspicious websites through a multi-faceted technical approach. Manual techniques such as WHOIS domain lookups and IP tracking were complemented by advanced methods, including Google dorks for targeted search queries and direct source code inspection. In addition, a Python script was employed to automate the assessment of site elements such as form inputs, cookie settings, and exposed files. This layered methodology enabled a thorough evaluation of site behavior, security features, and hidden risks.

Task Details and Working

UNDERSTANDING THE PATTERN :

The identification of covert messaging websites requires an understanding of the operational techniques historically employed by intelligence agencies, such as the CIA. These techniques focus on concealing secure communication channels within otherwise ordinary, public-facing websites. The purpose is to evade surveillance by masking secret functionality behind seemingly innocuous content.

Intelligence-Inspired Website Fronts

Intelligence agencies have utilized websites with benign themes—such as fan pages for sports teams, entertainment blogs, and hobbyist forums—as operational covers. These sites serve dual purposes: providing legitimate public content while secretly hosting covert channels for communication.

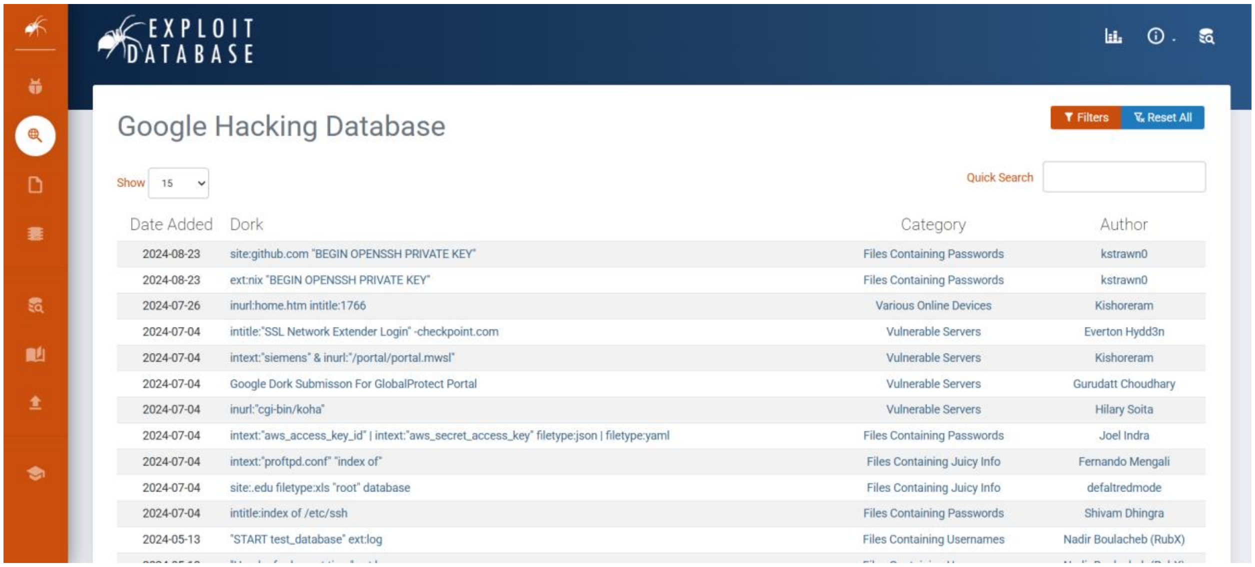
Core Features of Covert Messaging Sites

Based on my research and publicly available information, the following features are commonly associated with covert messaging websites:

- **Public-Facing Simple Content:**
  The main interface appears as an ordinary website, such as a fan page or personal blog, with no immediate indication of secure or secret features.
- **Hidden Password Fields or Dual-Layer Logins:**
  Secure login forms or password fields are embedded within the HTML source code, often hidden from direct view. They may only be accessible via specific actions, URLs, or triggers known to trusted users.
- **Repeated HTML Structures or Templates Across Sites:**
  Multiple covert sites may use identical or highly similar HTML, CSS, or JavaScript templates, suggesting the reuse of operational frameworks for consistency and plausible deniability.
- **Disguised Input Forms:**
  Input fields for passwords, messages, or agent identification are concealed or obfuscated, frequently using generic names (e.g., name="password", name="key") or hidden attributes, so as not to attract attention during casual inspection.

Google Dorking:

I sourced search queries from the Google Hacking Database (GHDB)



Google Hacking Database

Show 15

Quick Search

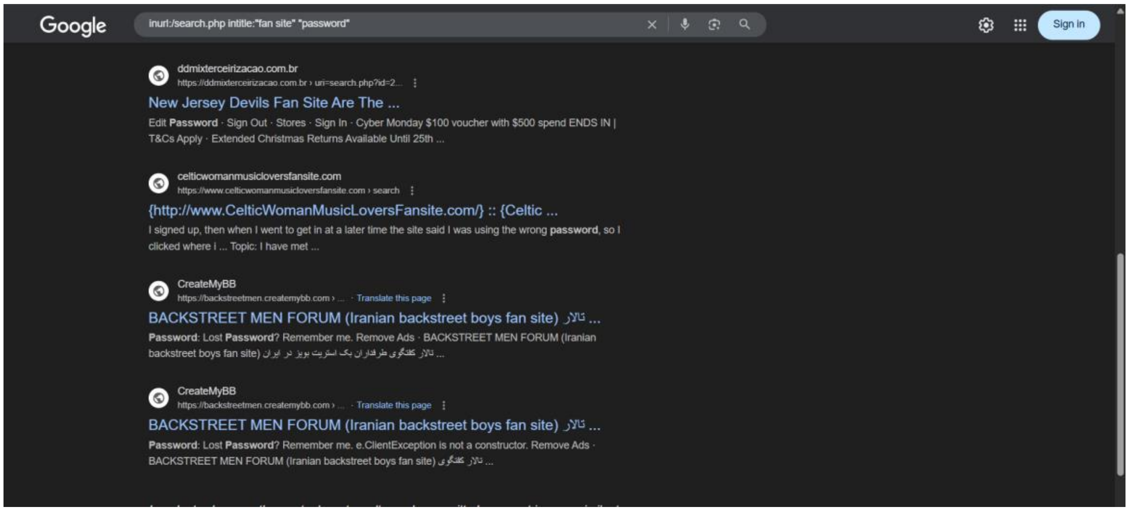
Date Added	Dork	Category	Author
2024-08-23	site:github.com "BEGIN OPENSSH PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-08-23	ext:nix "BEGIN OPENSSH PRIVATE KEY"	Files Containing Passwords	kstrawn0
2024-07-26	inurl:home.htm intitle:1766	Various Online Devices	Kishoreram
2024-07-04	intitle:"SSL Network Extender Login" -checkpoint.com	Vulnerable Servers	Everton Hydd3n
2024-07-04	intext:"siemens" & inurl:"/portal/portal.mwsl"	Vulnerable Servers	Kishoreram
2024-07-04	Google Dork Submisson For GlobalProtect Portal	Vulnerable Servers	Gurudatt Choudhary
2024-07-04	inurl:"cgi-bin/koha"	Vulnerable Servers	Hilary Soita
2024-07-04	intext:"aws_access_key_id" | intext:"aws_secret_access_key" filetype:json | filetype:yaml	Files Containing Passwords	Joel Indra
2024-07-04	intext:"proftpd.conf" "index of"	Files Containing Juicy Info	Fernando Mengali
2024-07-04	site:.edu filetype:xls "root" database	Files Containing Juicy Info	defaltredmode
2024-07-04	intitle:index of /etc/ssh	Files Containing Passwords	Shivam Dhingra
2024-05-13	"START test_database" ext:log	Files Containing Usernames	Nadir Boulacheb (RubX)

Applied them in Google Search by opening Chrome in o **Incognito**, to avoid personalized search bias and found websites with hidden login or communication features.

The resulting URLs were used for automated analysis.

ANALYSIS:

1. Find fan site pages that might unintentionally expose passwords.



inurl:/search.php intitle:"fan site" "password"

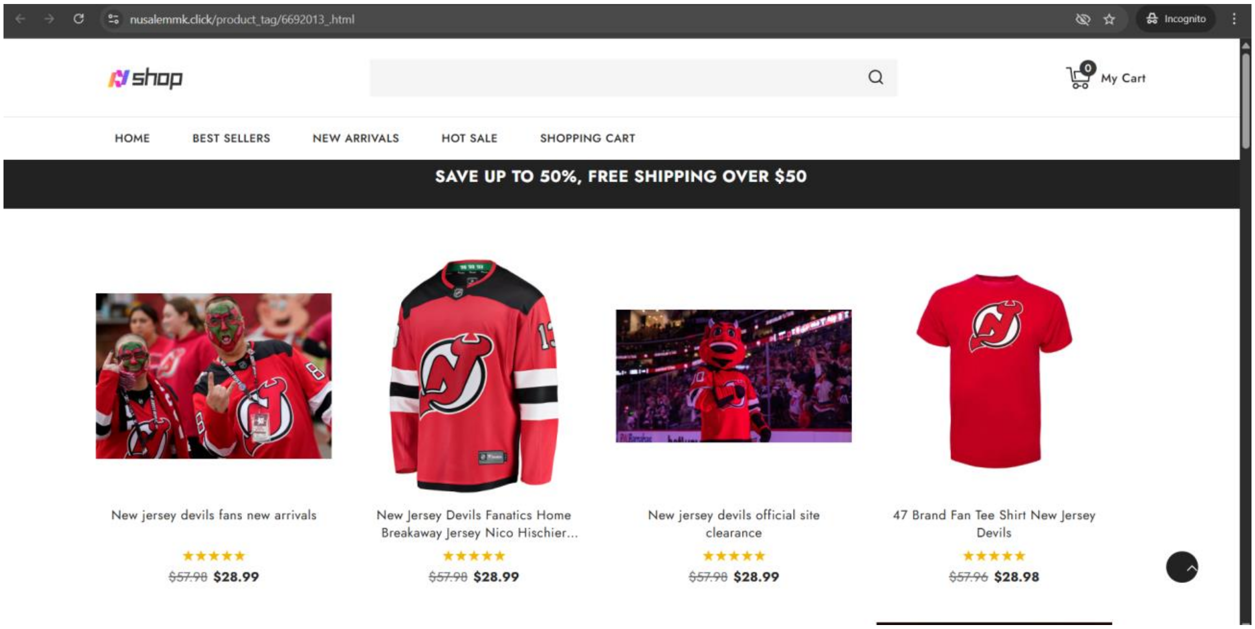
ddmixterceirizacao.com.br
https://ddmixterceirizacao.com.br › url=search.php?id=2...
New Jersey Devils Fan Site Are The ...
Edit **Password** · Sign Out · Stores · Sign In · Cyber Monday $100 voucher with $500 spend ENDS IN | T&Cs Apply · Extended Christmas Returns Available Until 25th ...

celticwomanmusicloversfansite.com
https://www.celticwomanmusicloversfansite.com › search
{http://www.CelticWomanMusicLoversFansite.com/} :: {Celtic ...
I signed up, then when I went to get in at a later time the site said I was using the wrong **password**, so I clicked where i ... Topic: I have met ...

CreateMyBB
https://backstreetmen.createmybb.com › ... · Translate this page
BACKSTREET MEN FORUM (Iranian backstreet boys fan site) تالار ...
Password: Lost **Password**? Remember me. Remove Ads · BACKSTREET MEN FORUM (Iranian backstreet boys fan site) تالار گفتگوی طرفداران بک استریت بویز در ایران ...

CreateMyBB
https://backstreetmen.createmybb.com › ... · Translate this page
BACKSTREET MEN FORUM (Iranian backstreet boys fan site) تالار ...
Password: Lost **Password**? Remember me. e.ClientException is not a constructor. Remove Ads · BACKSTREET MEN FORUM (Iranian backstreet boys fan site) تالار گفتگوی ...

https://nusalemmk.click/product_tag/6692013_.html



nusalemmk.click/product_tag/6692013_.html

shop

0 My Cart

HOME BEST SELLERS NEW ARRIVALS HOT SALE SHOPPING CART

SAVE UP TO 50%, FREE SHIPPING OVER $50

New jersey devils fans new arrivals
★★★★★
~~$57.98~~ $28.99

New Jersey Devils Fanatics Home Breakaway Jersey Nico Hischier...
★★★★★
~~$57.98~~ $28.99

New jersey devils official site clearance
★★★★★
~~$57.98~~ $28.99

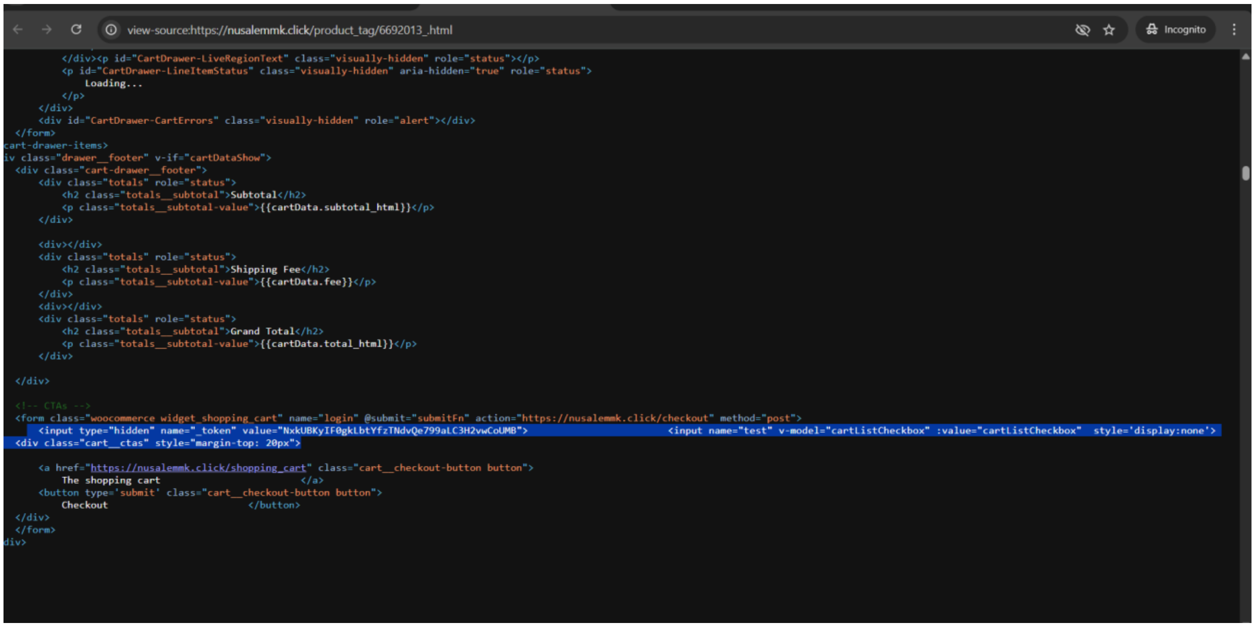
47 Brand Fan Tee Shirt New Jersey Devils
★★★★★
~~$57.96~~ $28.98

Results obtained from python script:

Form Details	**{
	"type": "number",
	"name": null,
	"placeholder": null,
	"style": null,
	"form_action": "/cart"
	}
	{
	"type": "hidden",
	"name": "_token",
	"placeholder": null,
	"style": null,
	"form_action": "https://nusalemmk.click/checkout"
	}
	{
	"type": null,
	"name": "test",
	"placeholder": null,
	"style": "display:none",
	"form_action": "https://nusalemmk.click/checkout"
	}**

Weak Cookies	Weak cookie: XSRF-TOKEN=eyJpdiI6IkhxRzA3a2pwU2Vick1jakwxV2VDeEE9PSIsInZhbHVlIjoiRHNuVVRJNTdGOHBoejJhVitTNk9rb0pKaFJodmpHYm5rVllDaUM0YXVBTm5wb1B5c2lNKzB3c2pRUks5TE9xbWRrNEVDN0liQnk3RFhHamIrakh2Vk5Od09VZEFJOU91RXp4Nk5VQ0ZGZjhQSjBRdnEvU3o2b1BOakpGZG1BUFMiLCJtYWMiOiIwNjYyNGI5NTVhMTNhYjgwNWVkNDNhOGU0Y2IzZGZmODQzMTBiMzIyYzIwZmQwZmJlYzU4NjVhNzQ5NDkyOGZiIiwidGFnIjoiIn0%3D; SameSite=Lax; Path=/; Max-Age=7200; Expires=Fri Weak cookie: laravel_session=eyJpdiI6Ing1cmlPVStaUExtd0dzV1kzOEFsZHc9PSIsInZhbHVlIjoieVhzak9qVkNMVlRrNEF6eW44SW8xWDhSMkFOcW9IN0JJL3A1UzBoT09pbFA1ZENia0M5ekZ2WWJUY09GSzIxVTRBT2F6c1pDbkpEcWhpWFZQcDRuc2NNT0lzZVdZRWVheUUyeTkrZDZ2dWljU29YK0hRSHJPQ0U0SmZjamNuNGoiLCJtYWMiOiJkYzAzZWQ2NTEzOTk4ZTU1MjRjNTYwMzg1YjdhM2EwOGIwNTNhNWEwMzRjNzUxZWEzNTJjZjY2Mzc3ZTM4MmM2IiwidGFnIjoiIn0%3D; HttpOnly; SameSite=Lax; Path=/; Max-Age=7200; Expires=Fri
Exposed Files/Dirs	https://nusalemmk.click/config.php [200] https://nusalemmk.click/backup [200] https://nusalemmk.click/backups [200] https://nusalemmk.click/db_backup [200] https://nusalemmk.click/database.sql [200] https://nusalemmk.click/dump.sql [200] https://nusalemmk.click/config.json [200]

- **Hidden Form Fields**

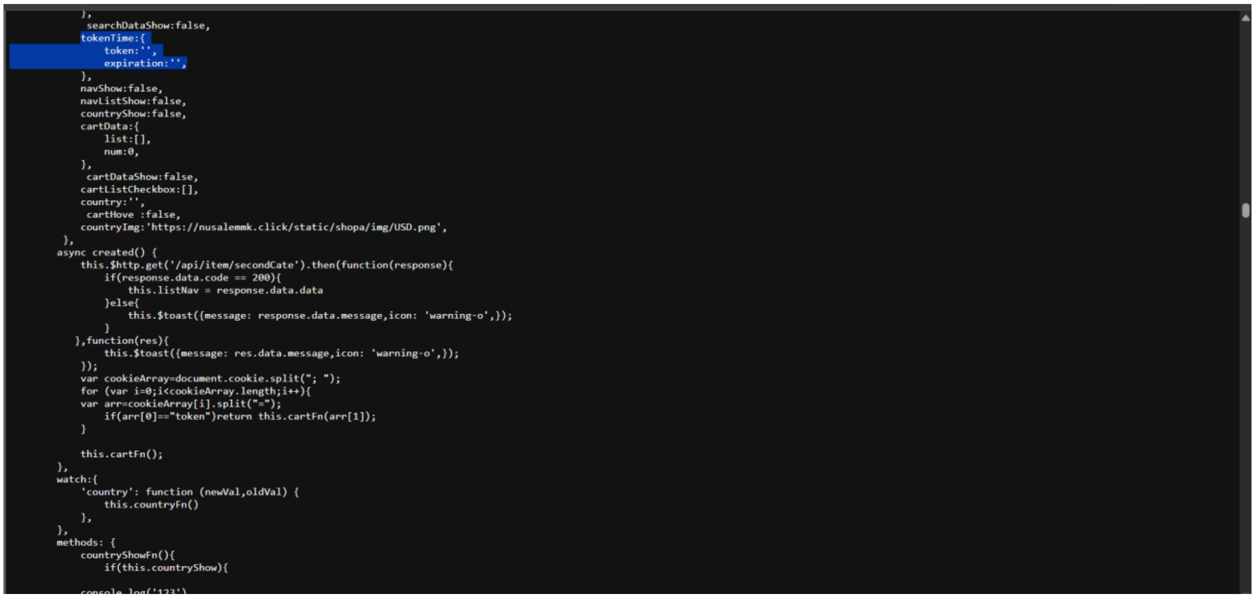

view-source:https://nusalemmk.click/product_tag/6692013_.html
Incognito

```
        </div><p id="CartDrawer-LiveRegionText" class="visually-hidden" role="status"></p>
        <p id="CartDrawer-LineItemStatus" class="visually-hidden" aria-hidden="true" role="status">
          Loading...
        </p>
      </div>
      <div id="CartDrawer-CartErrors" class="visually-hidden" role="alert"></div>
    </form>
cart-drawer-items>
iv class="drawer__footer" v-if="cartDataShow">
  <div class="cart-drawer__footer">
      <div class="totals" role="status">
          <h2 class="totals__subtotal">Subtotal</h2>
          <p class="totals__subtotal-value">{{cartData.subtotal_html}}</p>
      </div>

      <div></div>
      <div class="totals" role="status">
          <h2 class="totals__subtotal">Shipping Fee</h2>
          <p class="totals__subtotal-value">{{cartData.fee}}</p>
      </div>
      <div></div>
      <div class="totals" role="status">
          <h2 class="totals__subtotal">Grand Total</h2>
          <p class="totals__subtotal-value">{{cartData.total_html}}</p>
      </div>

  </div>

  <!-- CTAs -->
  <form class="woocommerce widget_shopping_cart" name="login" @submit="submitFn" action="https://nusalemmk.click/checkout" method="post">
      <input type="hidden" name="_token" value="NxkUBKyIF0gkLbtYfzTNdvQe799aLC3H2vwCoUMB">                        <input name="test" v-model="cartListCheckbox" :value="cartListCheckbox"  style='display:none'>
  <div class="cart__ctas" style="margin-top: 20px">

      <a href="https://nusalemmk.click/shopping_cart" class="cart__checkout-button button">
          The shopping cart                                  </a>
      <button type='submit' class="cart__checkout-button button">
          Checkout                                    </button>
  </div>
  </form>
div>
```

This code shows hidden form fields (_token, test), which can be used to trigger secret actions or restrict access to insiders only.

- **Obfuscated/Dynamic JavaScript**

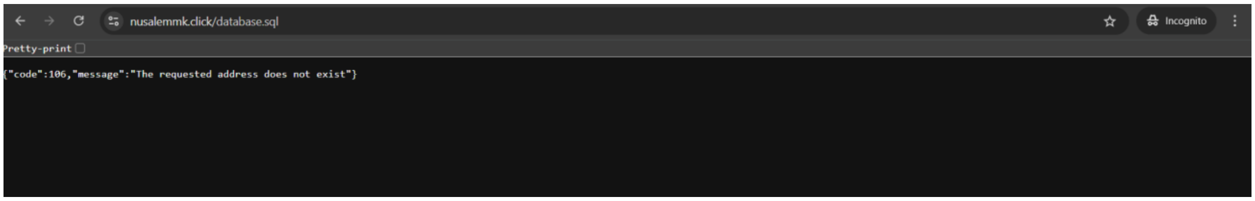
JavaScript contains long/hidden code with token, key, and login references — indicating possible hidden login/session logic.



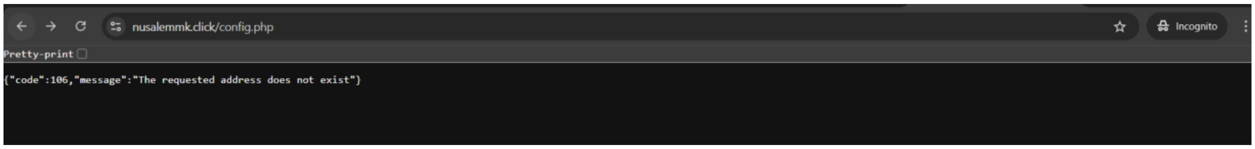
```
            },
             searchDataShow:false,
            tokenTime:{
                token:'',
                expiration:'',
            },
            navShow:false,
            navListShow:false,
            countryShow:false,
            cartData:{
                list:[],
                num:0,
            },
             cartDataShow:false,
            cartListCheckbox:[],
            country:'',
             cartHove :false,
            countryImg:'https://nusalemmk.click/static/shopa/img/USD.png',
         },
        async created() {
            this.$http.get('/api/item/secondCate').then(function(response){
                if(response.data.code == 200){
                    this.listNav = response.data.data
                }else{
                    this.$toast({message: response.data.message,icon: 'warning-o',});
                }
           },function(res){
                this.$toast({message: res.data.message,icon: 'warning-o',});
            });
            var cookieArray=document.cookie.split("; ");
            for (var i=0;i<cookieArray.length;i++){
            var arr=cookieArray[i].split("=");
                if(arr[0]=="token")return this.cartFn(arr[1]);
            }

            this.cartFn();
        },
        watch:{
            'country': function (newVal,oldVal) {
                this.countryFn()
            },
        },
        methods: {
            countryShowFn(){
                if(this.countryShow){

            console.log('123')
```

- **Exposed Files:**

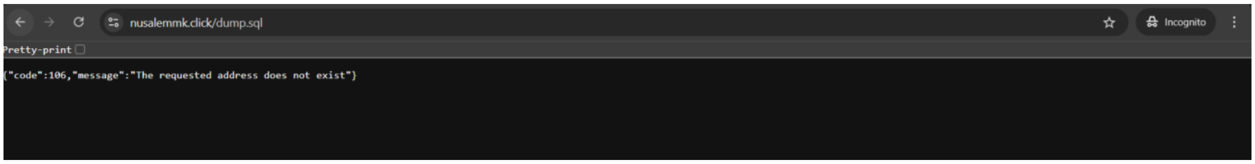
Highly sensitive files like config.php, database.sql, dump.sql, are directly accessible and publicly exposed, which is a major red flag.



```
{"code":106,"message":"The requested address does not exist"}
```



```
{"code":106,"message":"The requested address does not exist"}
```



```
{"code":106,"message":"The requested address does not exist"}
```

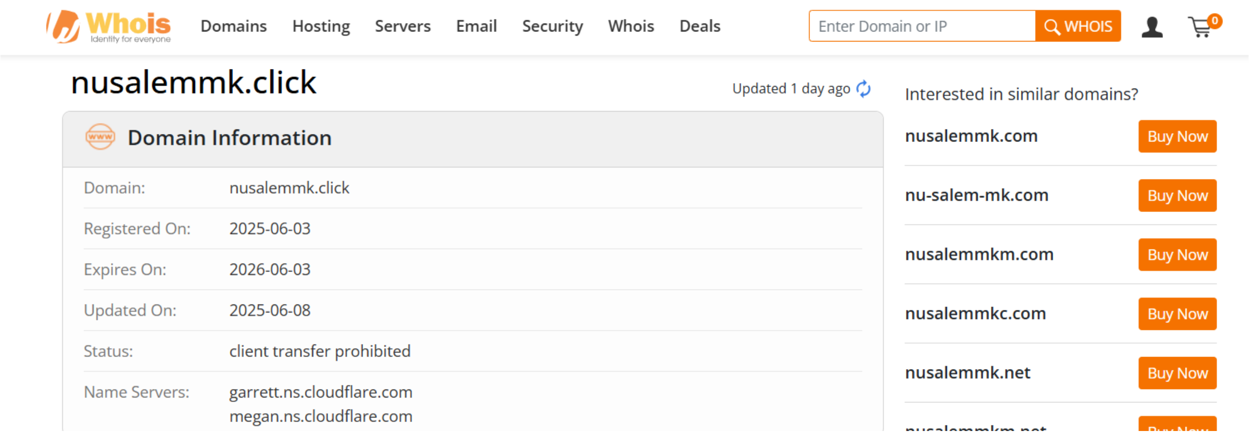
The server hides the real existence of sensitive files (like config.php, database.sql) by showing fake errors and using bot-deceptive behavior.

- **Weak Cookies**

Weak cookies are not just a technical flaw—they can be a deliberate or accidental "backdoor" for covert, persistent, or insider-only site access.

- **WHOIS & IP TRACKING**

The domain nusalemmk.click was registered recently (2025-06-03) with Sav.com, uses Cloudflare for privacy, and lists generic contact info. These factors, combined with the short registration period, are red flags for covert, spam, or temporary use.



nusalemmk.click

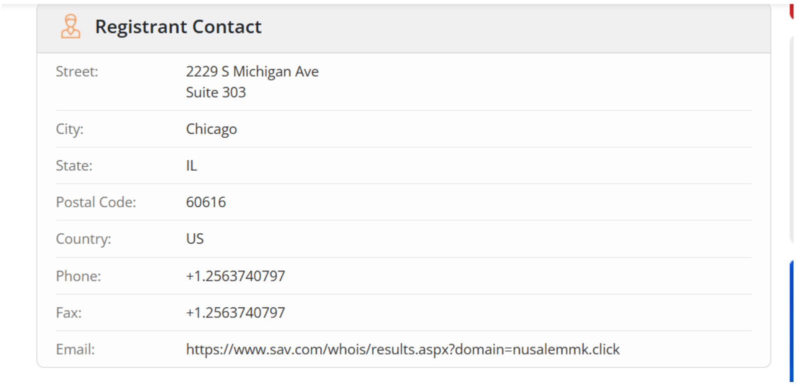
Updated 1 day ago

Domain Information

Domain:	nusalemmk.click
Registered On:	2025-06-03
Expires On:	2026-06-03
Updated On:	2025-06-08
Status:	client transfer prohibited
Name Servers:	garrett.ns.cloudflare.com megan.ns.cloudflare.com

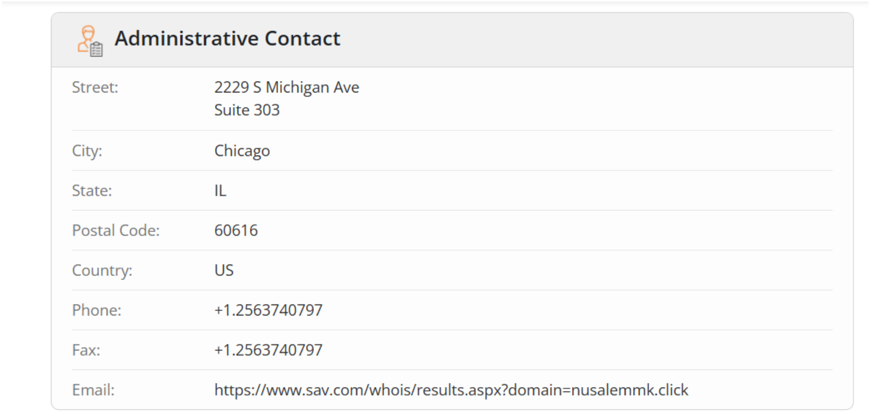
Interested in similar domains?

nusalemmk.com	Buy Now
nu-salem-mk.com	Buy Now
nusalemmkm.com	Buy Now
nusalemmkc.com	Buy Now
nusalemmk.net	Buy Now



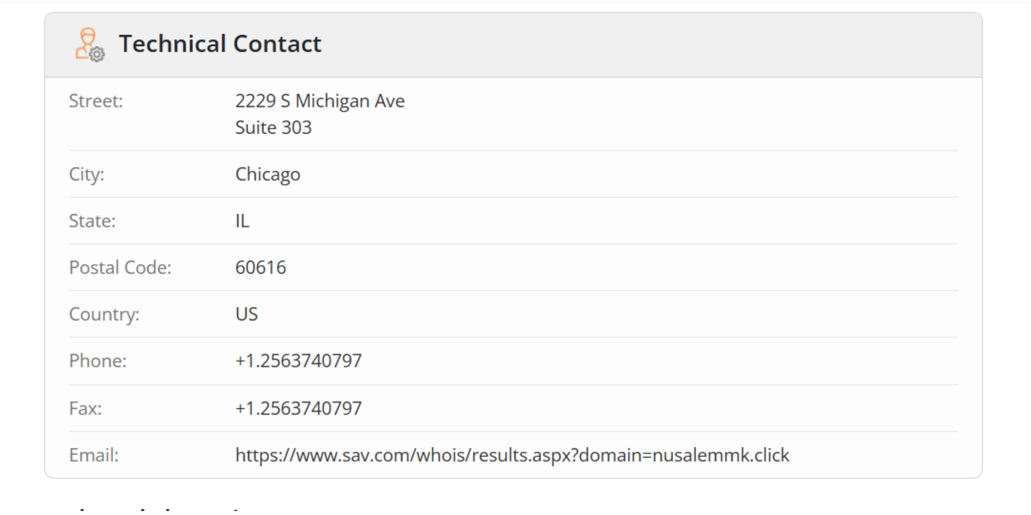
Registrant Contact

Street:	2229 S Michigan Ave Suite 303
City:	Chicago
State:	IL
Postal Code:	60616
Country:	US
Phone:	+1.2563740797
Fax:	+1.2563740797
Email:	https://www.sav.com/whois/results.aspx?domain=nusalemmk.click



Administrative Contact

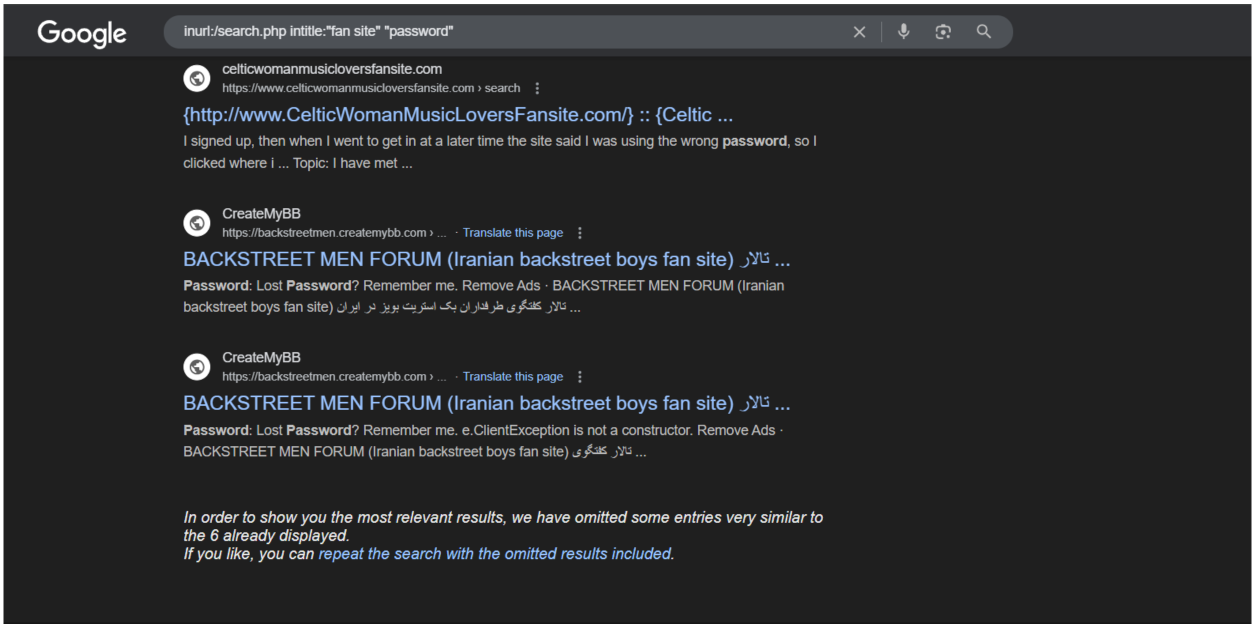
Street:	2229 S Michigan Ave Suite 303
City:	Chicago
State:	IL
Postal Code:	60616
Country:	US
Phone:	+1.2563740797
Fax:	+1.2563740797
Email:	https://www.sav.com/whois/results.aspx?domain=nusalemmk.click



Technical Contact

Street:	2229 S Michigan Ave Suite 303
City:	Chicago
State:	IL
Postal Code:	60616
Country:	US
Phone:	+1.2563740797
Fax:	+1.2563740797
Email:	https://www.sav.com/whois/results.aspx?domain=nusalemmk.click

2. Second suspicious website found



inurl:/search.php intitle:"fan site" "password"

celticwomanmusicloversfansite.com
https://www.celticwomanmusicloversfansite.com › search

{http://www.CelticWomanMusicLoversFansite.com/} :: {Celtic ...

I signed up, then when I went to get in at a later time the site said I was using the wrong **password**, so I clicked where i ... Topic: I have met ...

CreateMyBB
https://backstreetmen.createmybb.com › ... · Translate this page

BACKSTREET MEN FORUM (Iranian backstreet boys fan site) تالار ...

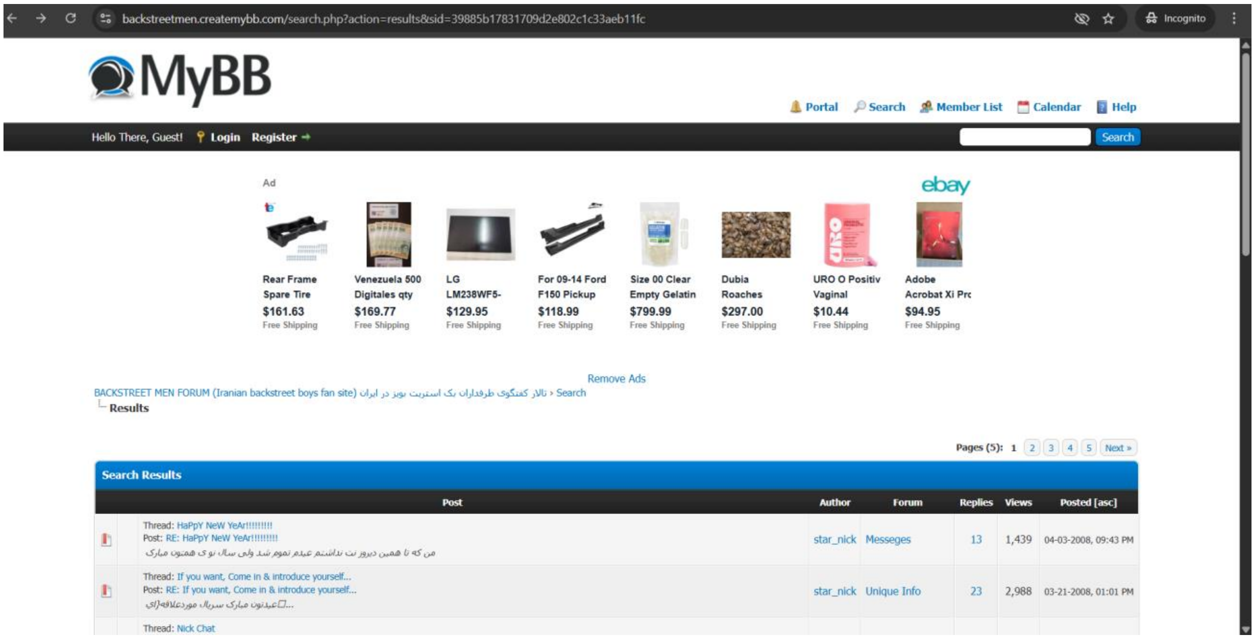
Password: Lost **Password**? Remember me. Remove Ads · BACKSTREET MEN FORUM (Iranian backstreet boys fan site) تالار گفتگوی طرفداران بک استریت بویز در ایران ...

CreateMyBB
https://backstreetmen.createmybb.com › ... · Translate this page

BACKSTREET MEN FORUM (Iranian backstreet boys fan site) تالار ...

Password: Lost **Password**? Remember me. e.ClientException is not a constructor. Remove Ads · BACKSTREET MEN FORUM (Iranian backstreet boys fan site) تالار گفتگوی ...

In order to show you the most relevant results, we have omitted some entries very similar to the 6 already displayed.
If you like, you can repeat the search with the omitted results included.



backstreetmen.createmybb.com/search.php?action=results&sid=39885b17831709d2e802c1c33aeb11fc
Incognito
MyBB
Portal
Search
Member List
Calendar
Help
Hello There, Guest!
Login
Register
Search
Ad
ebay
Rear Frame Spare Tire $161.63 Free Shipping
Venezuela 500 Digitales qty $169.77 Free Shipping
LG LM238WF5- $129.95 Free Shipping
For 09-14 Ford F150 Pickup $118.99 Free Shipping
Size 00 Clear Empty Gelatin $799.99 Free Shipping
Dubia Roaches $297.00 Free Shipping
URO O Positiv Vaginal $10.44 Free Shipping
Adobe Acrobat Xi Prc $94.95 Free Shipping
Remove Ads

BACKSTREET MEN FORUM (Iranian backstreet boys fan site) تالار گفتگوی طرفداران بک استریت بویز در ایران › Search
Results

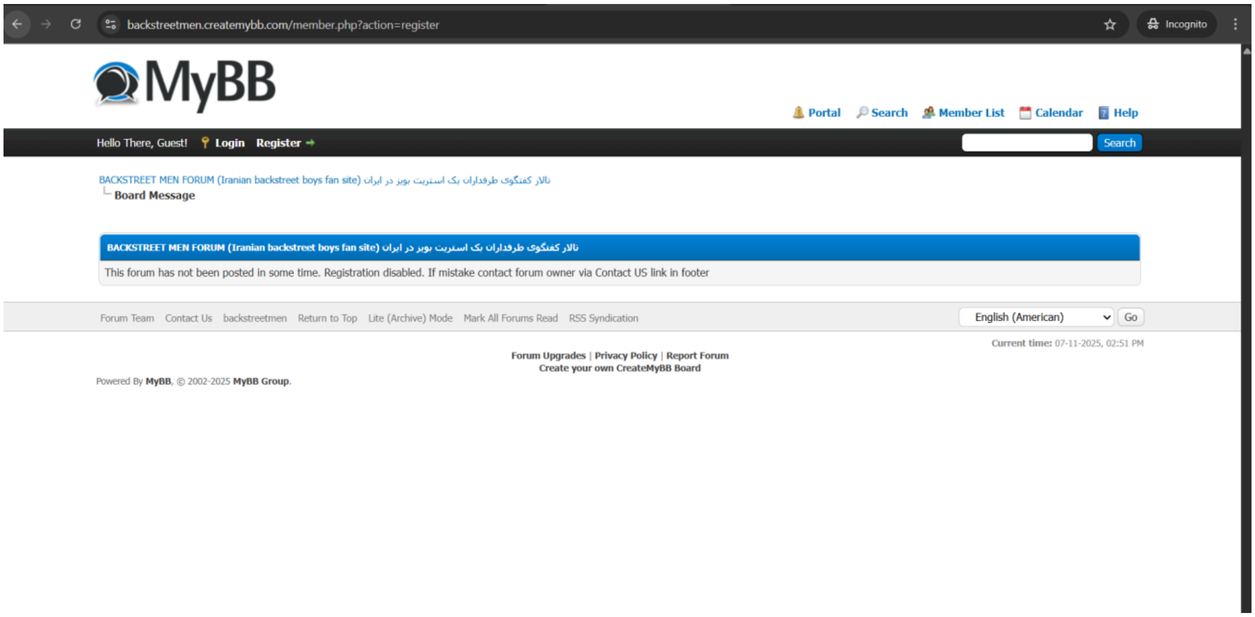
Pages (5): 1 2 3 4 5 Next »

Search Results

Post	Author	Forum	Replies	Views	Posted [asc]
Thread: HaPpY NeW YeAr!!!!!!!!! Post: RE: HaPpY NeW YeAr!!!!!!!!! من که تا همین دیروز نت نداشتم عیدم تموم شد ولی سال نو ی همتون مبارک	star_nick	Messeges	13	1,439	04-03-2008, 09:43 PM
Thread: If you want, Come in & introduce yourself... Post: RE: If you want, Come in & introduce yourself... عیدتون مبارک سریال موردعلاقه‌ای...	star_nick	Unique Info	23	2,988	03-21-2008, 01:01 PM
Thread: Nick Chat					

https://backstreetmen.createmybb.com/search.php?action=results&sid=39885b17831709d2e802c1c33aeb11fc

- The Backstreet Men Forum presents itself as a fan site, but registration is disabled and only existing users can log in via a modal popup. The forum is inactive, and outsiders are restricted from joining. This setup matches patterns seen in insider-only or covert platforms, where access and posting are limited to pre-approved members.



backstreetmen.createmybb.com/member.php?action=register

Hello There, Guest! Login Register

BACKSTREET MEN FORUM (Iranian backstreet boys fan site) تالار گفتگوی طرفداران بک استریت بویز در ایران
Board Message

BACKSTREET MEN FORUM (Iranian backstreet boys fan site) تالار گفتگوی طرفداران بک استریت بویز در ایران

This forum has not been posted in some time. Registration disabled. If mistake contact forum owner via Contact US link in footer

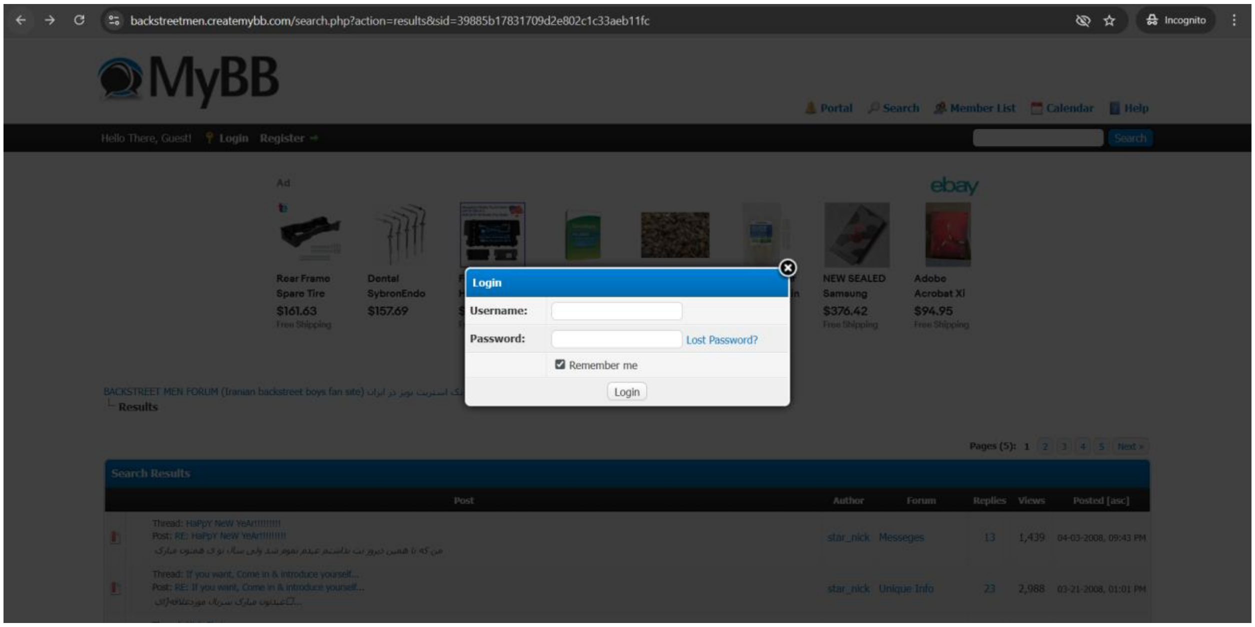
Forum Team Contact Us backstreetmen Return to Top Lite (Archive) Mode Mark All Forums Read RSS Syndication

English (American) Go

Current time: 07-11-2025, 02:51 PM

Forum Upgrades | Privacy Policy | Report Forum
Create your own CreateMyBB Board

Powered By MyBB, © 2002-2025 MyBB Group.



backstreetmen.createmybb.com/search.php?action=results&sid=39885b17831709d2e802c1c33aeb11fc

Login

Username:

Password: Lost Password?

☑ Remember me

Login

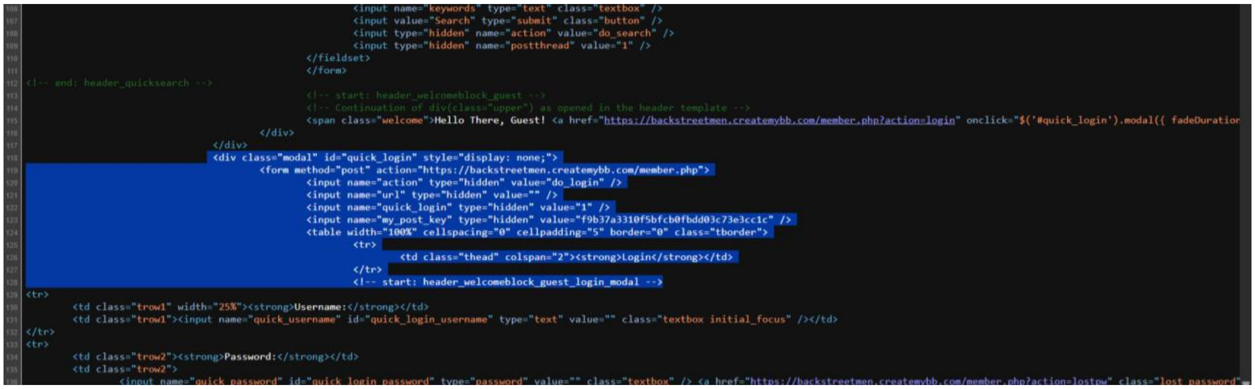
BACKSTREET MEN FORUM (Iranian backstreet boys fan site) ... بک استریت بویز در ایران
Results

Pages (5): 1 2 3 4 5 Next »

Search Results

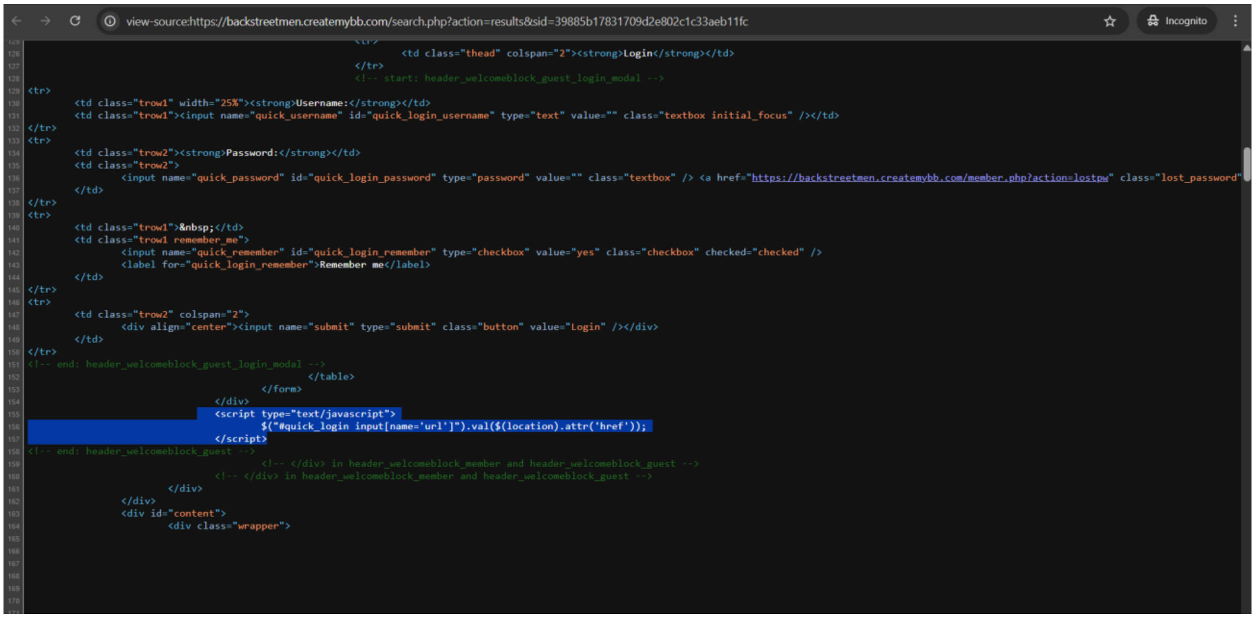
Post	Author	Forum	Replies	Views	Posted [asc]
Thread: HaPpY NeW YeAr!!!!!!!!! Post: RE: HaPpY NeW YeAr!!!!!!!!! من که تا همین دیروز نت نداشتم عیدم بموم شد ولی سال نو ی همتون مبارک	star_nick	Messeges	13	1,439	04-03-2008, 09:43 PM
Thread: If you want, Come in & introduce yourself... Post: RE: If you want, Come in & introduce yourself... عیدتون مبارک سریال موردعلاقه‌ات...	star_nick	Unique Info	23	2,988	03-21-2008, 01:01 PM

- Login button visible, but form is hidden in a modal that appears only on click.



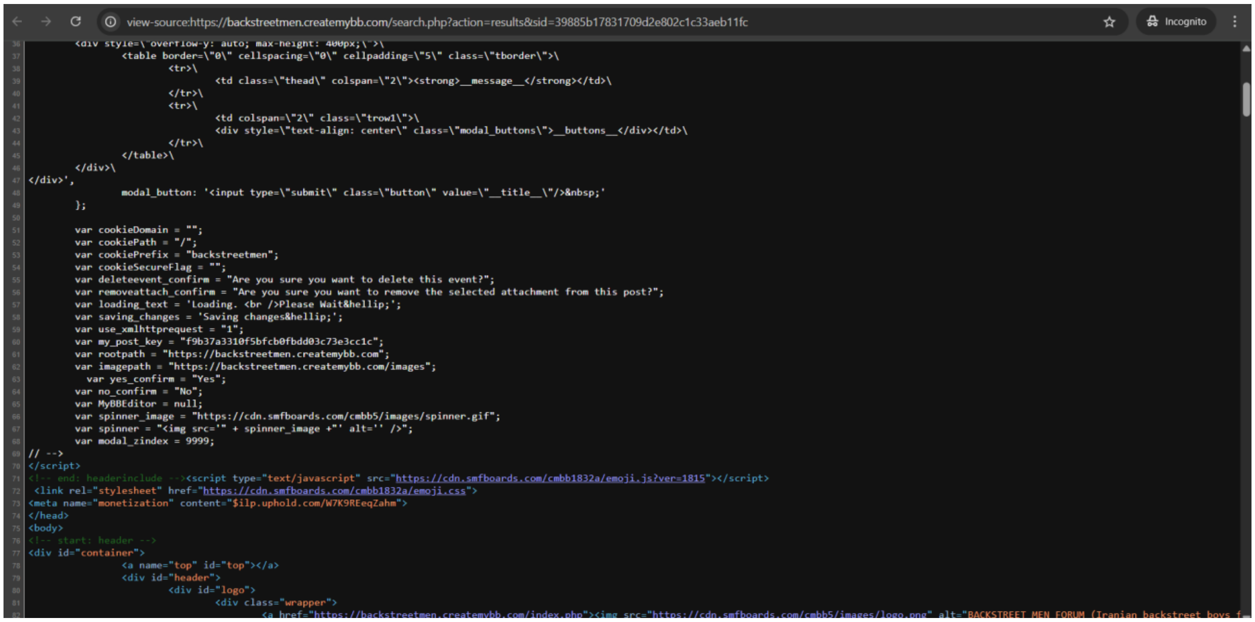
```
                                        <input name="keywords" type="text" class="textbox" />
                                        <input value="Search" type="submit" class="button" />
                                        <input type="hidden" name="action" value="do_search" />
                                        <input type="hidden" name="postthread" value="1" />
                                </fieldset>
                                </form>
<!-- end: header_quicksearch -->
                                <!-- start: header_welcomeblock_guest -->
                                <!-- Continuation of div(class="upper") as opened in the header template -->
                                <span class="welcome">Hello There, Guest! <a href="https://backstreetmen.createmybb.com/member.php?action=login" onclick="$('#quick_login').modal({ fadeDuration
                        </div>
                </div>
                <div class="modal" id="quick_login" style="display: none;">
                        <form method="post" action="https://backstreetmen.createmybb.com/member.php">
                                <input name="action" type="hidden" value="do_login" />
                                <input name="url" type="hidden" value="" />
                                <input name="quick_login" type="hidden" value="1" />
                                <input name="my_post_key" type="hidden" value="f9b37a3310f5bfcb0fbdd03c73e3cc1c" />
                                <table width="100%" cellspacing="0" cellpadding="5" border="0" class="tborder">
                                        <tr>
                                                <td class="thead" colspan="2"><strong>Login</strong></td>
                                        </tr>
                                        <!-- start: header_welcomeblock_guest_login_modal -->
<tr>
        <td class="trow1" width="25%"><strong>Username:</strong></td>
        <td class="trow1"><input name="quick_username" id="quick_login_username" type="text" value="" class="textbox initial_focus" /></td>
</tr>
<tr>
        <td class="trow2"><strong>Password:</strong></td>
        <td class="trow2">
                <input name="quick_password" id="quick_login_password" type="password" value="" class="textbox" /> <a href="https://backstreetmen.createmybb.com/member.php?action=lostpw" class="lost_password"
```

- quick_login, my_post_key, and url fields not shown in source until modal is triggered.
- JavaScript dynamically injects the current page into the form


view-source:https://backstreetmen.createmybb.com/search.php?action=results&sid=39885b17831709d2e802c1c33aeb11fc
Incognito

```
                                        </tr>
                                                <td class="thead" colspan="2"><strong>Login</strong></td>
                                        </tr>
                                        <!-- start: header_welcomeblock_guest_login_modal -->
<tr>
        <td class="trow1" width="25%"><strong>Username:</strong></td>
        <td class="trow1"><input name="quick_username" id="quick_login_username" type="text" value="" class="textbox initial_focus" /></td>
</tr>
<tr>
        <td class="trow2"><strong>Password:</strong></td>
        <td class="trow2">
                <input name="quick_password" id="quick_login_password" type="password" value="" class="textbox" /> <a href="https://backstreetmen.createmybb.com/member.php?action=lostpw" class="lost_password"
        </td>
</tr>
<tr>
        <td class="trow1">&nbsp;</td>
        <td class="trow1 remember_me">
                <input name="quick_remember" id="quick_login_remember" type="checkbox" value="yes" class="checkbox" checked="checked" />
                <label for="quick_login_remember">Remember me</label>
        </td>
</tr>
<tr>
        <td class="trow2" colspan="2">
                <div align="center"><input name="submit" type="submit" class="button" value="Login" /></div>
        </td>
</tr>
<!-- end: header_welcomeblock_guest_login_modal -->
                                                </table>
                                        </form>
                                </div>
                                <script type="text/javascript">
                                        $("#quick_login input[name='url']").val($(location).attr('href'));
                                </script>
<!-- end: header_welcomeblock_guest -->
                                        <!-- </div> in header_welcomeblock_member and header_welcomeblock_guest -->
                                <!-- </div> in header_welcomeblock_member and header_welcomeblock_guest -->
                        </div>
                </div>
                <div id="content">
                        <div class="wrapper">
```

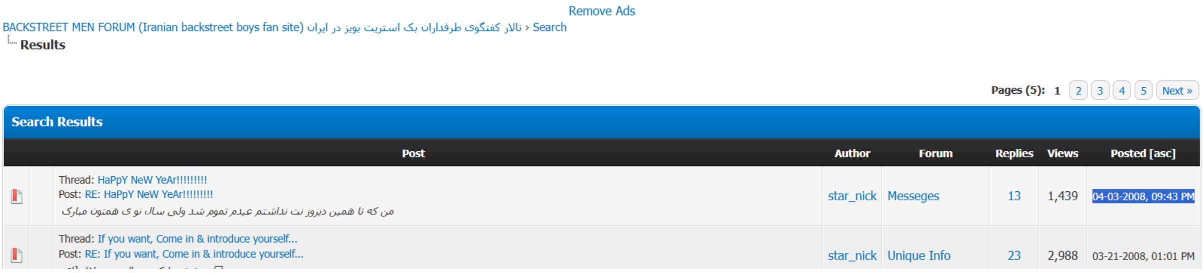
- Weak cookies allow login sessions to be stolen easily if the site isn't using secure HTTPS. This can let insiders or attackers access accounts without needing passwords. Since the login form is hidden and registration is disabled, it looks like only trusted people are meant to use it. The weak security might be left on purpose to quietly allow access without attracting attention.


view-source:https://backstreetmen.createmybb.com/search.php?action=results&sid=39885b17831709d2e802c1c33aeb11fc
Incognito

```
        <div style=\"overflow-y: auto; max-height: 400px;\">\
                <table border=\"0\" cellspacing=\"0\" cellpadding=\"5\" class=\"tborder\">\
                        <tr>\
                                <td class=\"thead\" colspan=\"2\"><strong>__message__</strong></td>\
                        </tr>\
                        <tr>\
                                <td colspan=\"2\" class=\"trow1\">\
                                <div style=\"text-align: center\" class=\"modal_buttons\">__buttons__</div></td>\
                        </tr>\
                </table>\
        </div>\
</div>',
                modal_button: '<input type=\"submit\" class=\"button\" value=\"__title__\"/>&nbsp;'
        };

        var cookieDomain = "";
        var cookiePath = "/";
        var cookiePrefix = "backstreetmen";
        var cookieSecureFlag = "";
        var deleteevent_confirm = "Are you sure you want to delete this event?";
        var removeattach_confirm = "Are you sure you want to remove the selected attachment from this post?";
        var loading_text = 'Loading. <br />Please Wait&hellip;';
        var saving_changes = 'Saving changes&hellip;';
        var use_xmlhttprequest = "1";
        var my_post_key = "f9b37a3310f5bfcb0fbdd03c73e3cc1c";
        var rootpath = "https://backstreetmen.createmybb.com";
        var imagepath = "https://backstreetmen.createmybb.com/images";
          var yes_confirm = "Yes";
        var no_confirm = "No";
        var MyBBEditor = null;
        var spinner_image = "https://cdn.smfboards.com/cmbb5/images/spinner.gif";
        var spinner = "<img src='" + spinner_image +"' alt='' />";
        var modal_zindex = 9999;
// -->
</script>
<!-- end: headerinclude --><script type="text/javascript" src="https://cdn.smfboards.com/cmbb1832a/emoji.js?ver=1815"></script>
 <link rel="stylesheet" href="https://cdn.smfboards.com/cmbb1832a/emoji.css">
<meta name="monetization" content="$ilp.uphold.com/W7K9REeqZahm">
</head>
<body>
<!-- start: header -->
<div id="container">
                <a name="top" id="top"></a>
                <div id="header">
                        <div id="logo">
                                <div class="wrapper">
                                        <a href="https://backstreetmen.createmybb.com/index.php"><img src="https://cdn.smfboards.com/cmbb5/images/logo.png" alt="BACKSTREET MEN FORUM (Iranian backstreet boys f
```

According to **OSINT (Open-Source Intelligence) gathering practices** and **covert communication indicators** used in intelligence operations ,covert websites often use:

- Non-obvious entry points (modals, triggers)
- Hidden login fields only accessible via JavaScript



Remove Ads

BACKSTREET MEN FORUM (Iranian backstreet boys fan site) تالار کفتگوی طرفداران بک استریت بویز در ایران › Search

Results

Pages (5): 1 2 3 4 5 Next »

Search Results

		Post	Author	Forum	Replies	Views	Posted [asc]
		Thread: HaPpY NeW YeAr!!!!!!!!! Post: RE: HaPpY NeW YeAr!!!!!!!!! من که تا همین دیروز نت نداشتم عیدم تموم شد ولی سال نو ی همتون مبارک	star_nick	Messeges	13	1,439	04-03-2008, 09:43 PM
		Thread: If you want, Come in & introduce yourself... Post: RE: If you want, Come in & introduce yourself...	star_nick	Unique Info	23	2,988	03-21-2008, 01:01 PM

The forum is largely inactive, as evidenced by the absence of recent posts and replies. This inactivity suggests reduced visibility and limited external scrutiny.

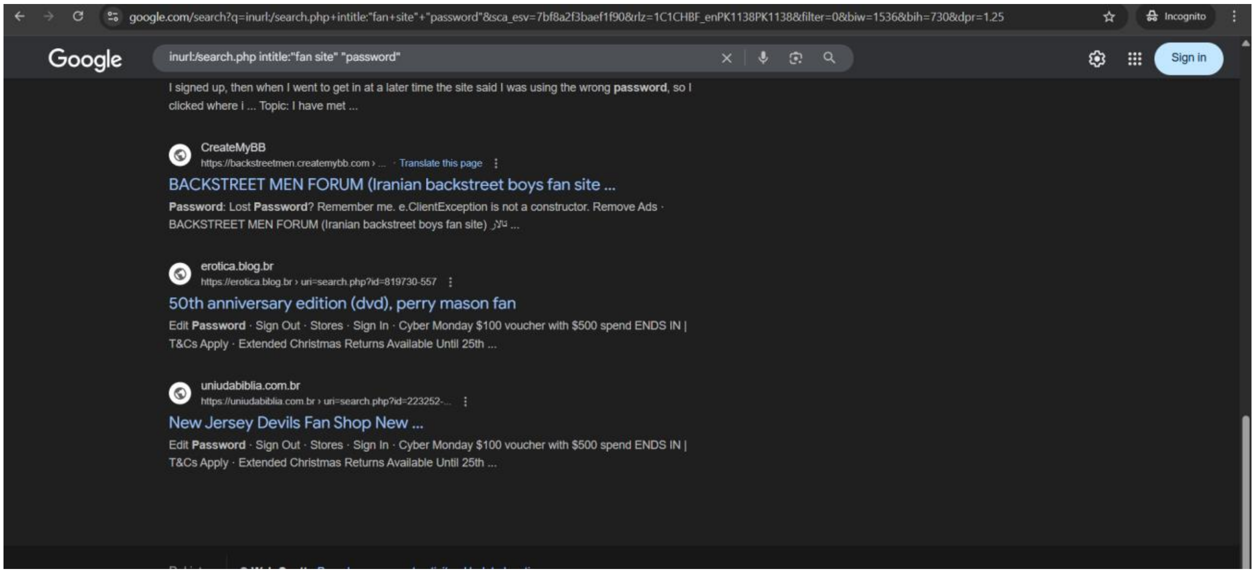
Python script results

Form Details	**{** **"type": "hidden",** **"name": "postthread",** **"placeholder": null,** **"style": null,** **"form_action": "https://backstreetmen.createmybb.com/search.php"** **}** **{** **"type": "hidden",** **"name": "action",** **"placeholder": null,** **"style": null,** **"form_action": "https://backstreetmen.createmybb.com/member.php"** **}** **{** **"type": "hidden",** **"name": "url",** **"placeholder": null,** **"style": null,** **"form_action": "https://backstreetmen.createmybb.com/member.php"** **}** **{** **"type": "hidden",** **"name": "quick_login",** **"placeholder": null,** **"style": null,** **"form_action": "https://backstreetmen.createmybb.com/member.php"** **}** **{** **"type": "hidden",** **"name": "my_post_key",** **"placeholder": null,** **"style": null,** **"form_action": "https://backstreetmen.createmybb.com/member.php"** **}** **{** **"type": "password",** **"name": "quick_password",**

	"placeholder": null,
	"style": null,
	"form_action": "https://backstreetmen.createmybb.com/member.php"
	}
	
	{
	"type": "hidden",
	"name": "action",
	"placeholder": null,
	"style": null,
	"form_action": "/search.php"
	}
	{
	"type": "hidden",
	"name": "sid",
	"placeholder": null,
	"style": null,
	"form_action": "/search.php"
	}
	{
	"type": "hidden",
	"name": "my_post_key",
	"placeholder": null,
	"style": null,
	"form_action": "/search.php"
	}

Weak Cookies	Weak cookie: backstreetmenmybb[lastvisit]=1752236508; expires=Sat Weak cookie: 11-Jul-2026 12:21:48 GMT; path=/ Weak cookie: backstreetmenmybb[lastactive]=1752236508; expires=Sat Weak cookie: 11-Jul-2026 12:21:48 GMT; path=/ Weak cookie: backstreetmensid=088424a05676c9bc688c566eef1b34c1; path=/; HttpOnly

3. Not suspicious but a website for fake traffic



google.com/search?q=inurl:/search.php+intitle:"fan+site"+"password"&sca_esv=7bf8a2f3baef1f90&rlz=1C1CHBF_enPK1138PK1138&filter=0&biw=1536&bih=730&dpr=1.25

inurl:/search.php intitle:"fan site" "password"

I signed up, then when I went to get in at a later time the site said I was using the wrong **password**, so I clicked where i ... Topic: I have met ...

CreateMyBB
https://backstreetmen.createmybb.com › ... · Translate this page

BACKSTREET MEN FORUM (Iranian backstreet boys fan site ...

Password: Lost **Password**? Remember me. e.ClientException is not a constructor. Remove Ads · BACKSTREET MEN FORUM (Iranian backstreet boys fan site) تالار ...

erotica.blog.br
https://erotica.blog.br › uri=search.php?id=819730-557

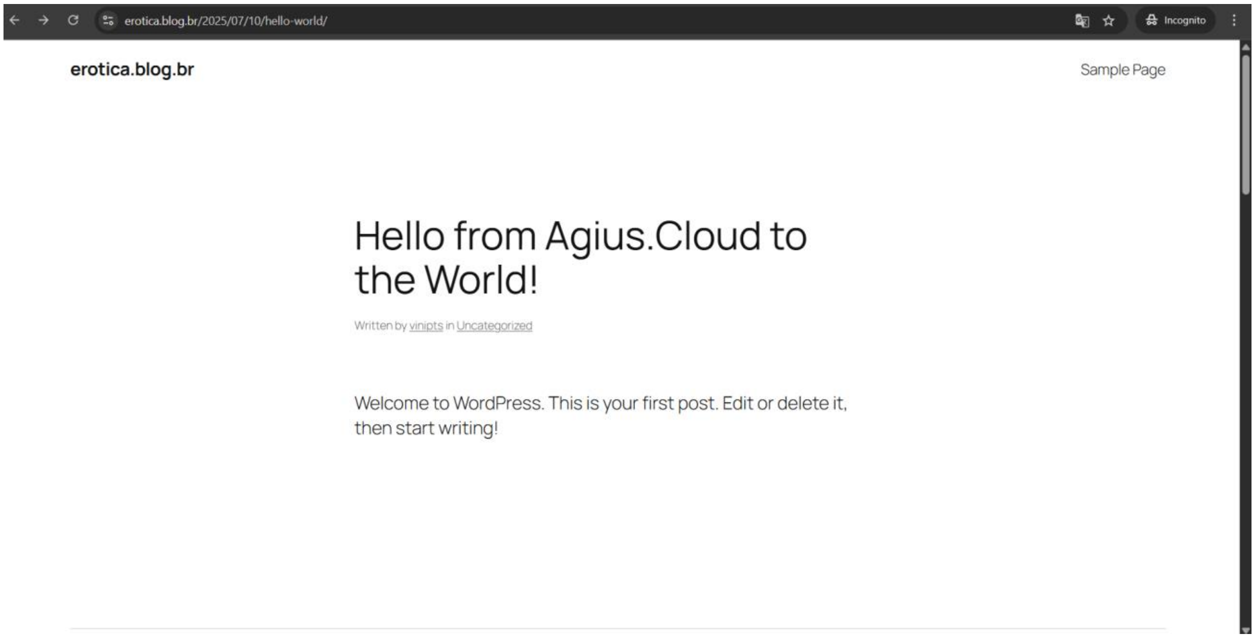
50th anniversary edition (dvd), perry mason fan

Edit **Password** · Sign Out · Stores · Sign In · Cyber Monday $100 voucher with $500 spend ENDS IN | T&Cs Apply · Extended Christmas Returns Available Until 25th ...

uniudabiblia.com.br
https://uniudabiblia.com.br › uri=search.php?id=223252-...

New Jersey Devils Fan Shop New ...

Edit **Password** · Sign Out · Stores · Sign In · Cyber Monday $100 voucher with $500 spend ENDS IN | T&Cs Apply · Extended Christmas Returns Available Until 25th ...



erotica.blog.br

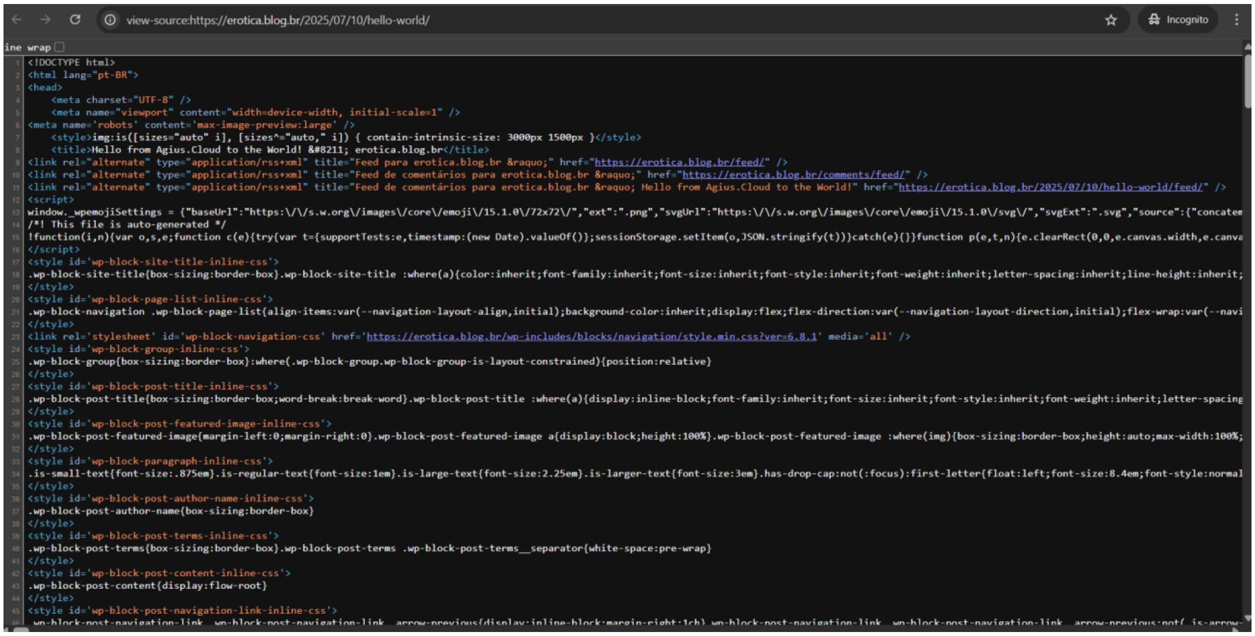
Sample Page

Hello from Agius.Cloud to the World!

Written by vinipts in Uncategorized

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

https://erotica.blog.br/2025/07/10/hello-world/



```
<!DOCTYPE html>
<html lang="pt-BR">
<head>
    <meta charset="UTF-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
<meta name='robots' content='max-image-preview:large' />
    <style>img:is([sizes="auto" i], [sizes^="auto," i]) { contain-intrinsic-size: 3000px 1500px }</style>
    <title>Hello from Agius.Cloud to the World! &#8211; erotica.blog.br</title>
<link rel="alternate" type="application/rss+xml" title="Feed para erotica.blog.br &raquo;" href="https://erotica.blog.br/feed/" />
<link rel="alternate" type="application/rss+xml" title="Feed de comentários para erotica.blog.br &raquo;" href="https://erotica.blog.br/comments/feed/" />
<link rel="alternate" type="application/rss+xml" title="Feed de comentários para erotica.blog.br &raquo; Hello from Agius.Cloud to the World!" href="https://erotica.blog.br/2025/07/10/hello-world/feed/" />
<script>
window._wpemojiSettings = {"baseUrl":"https:\/\/s.w.org\/images\/core\/emoji\/15.1.0\/72x72\/","ext":".png","svgUrl":"https:\/\/s.w.org\/images\/core\/emoji\/15.1.0\/svg\/","svgExt":".svg","source":{"concatem
/*! This file is auto-generated */
!function(i,n){var o,s,e;function c(e){try{var t={supportTests:e,timestamp:(new Date).valueOf()};sessionStorage.setItem(o,JSON.stringify(t))}catch(e){}}function p(e,t,n){e.clearRect(0,0,e.canvas.width,e.canva
</script>
<style id='wp-block-site-title-inline-css'>
.wp-block-site-title{box-sizing:border-box}.wp-block-site-title :where(a){color:inherit;font-family:inherit;font-size:inherit;font-style:inherit;font-weight:inherit;letter-spacing:inherit;line-height:inherit;
</style>
<style id='wp-block-page-list-inline-css'>
.wp-block-navigation .wp-block-page-list{align-items:var(--navigation-layout-align,initial);background-color:inherit;display:flex;flex-direction:var(--navigation-layout-direction,initial);flex-wrap:var(--navi
</style>
<link rel='stylesheet' id='wp-block-navigation-css' href='https://erotica.blog.br/wp-includes/blocks/navigation/style.min.css?ver=6.8.1' media='all' />
<style id='wp-block-group-inline-css'>
.wp-block-group{box-sizing:border-box}:where(.wp-block-group.wp-block-group-is-layout-constrained){position:relative}
</style>
<style id='wp-block-post-title-inline-css'>
.wp-block-post-title{box-sizing:border-box;word-break:break-word}.wp-block-post-title :where(a){display:inline-block;font-family:inherit;font-size:inherit;font-style:inherit;font-weight:inherit;letter-spacing
</style>
<style id='wp-block-post-featured-image-inline-css'>
.wp-block-post-featured-image{margin-left:0;margin-right:0}.wp-block-post-featured-image a{display:block;height:100%}.wp-block-post-featured-image :where(img){box-sizing:border-box;height:auto;max-width:100%;
</style>
<style id='wp-block-paragraph-inline-css'>
.is-small-text{font-size:.875em}.is-regular-text{font-size:1em}.is-large-text{font-size:2.25em}.is-larger-text{font-size:3em}.has-drop-cap:not(:focus):first-letter{float:left;font-size:8.4em;font-style:normal
</style>
<style id='wp-block-post-author-name-inline-css'>
.wp-block-post-author-name{box-sizing:border-box}
</style>
<style id='wp-block-post-terms-inline-css'>
.wp-block-post-terms{box-sizing:border-box}.wp-block-post-terms .wp-block-post-terms__separator{white-space:pre-wrap}
</style>
<style id='wp-block-post-content-inline-css'>
.wp-block-post-content{display:flow-root}
</style>
<style id='wp-block-post-navigation-link-inline-css'>
.wp-block-post-navigation-link .wp-block-post-navigation-link__arrow-previous{display:inline-block;margin-right:1ch}.wp-block-post-navigation-link .wp-block-post-navigation-link__arrow-previous:not(.is-arrow-
```

- The site looks like a normal blog (WordPress), but the URL is strange.

The address has words like “search.php”, “id=...”, and “name=perry mason fan site” — which makes it look like a login or a fan page, but you only see a normal blog page.

- There are NO hidden login boxes or secret password places in the code.

The page only shows the default “Hello World” post.

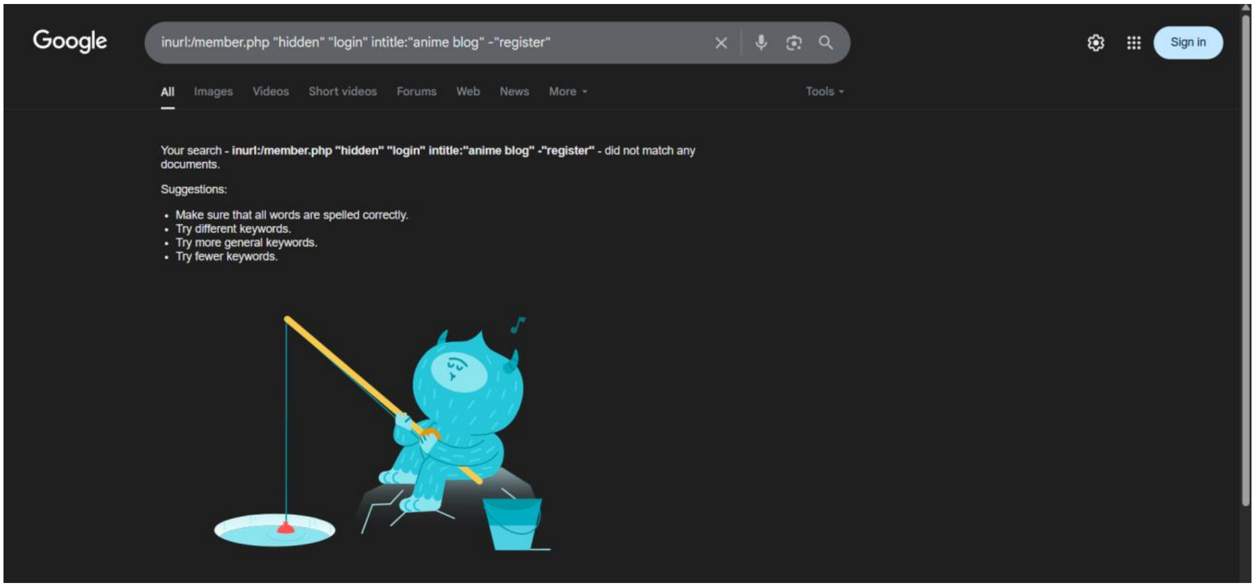
- There’s no real fan site or login here; it’s just the basic WordPress setup.
- The URL is misleading, and it uses confusing extra parts.

This could mean the site is trying to trick search engines, or is just set up as a “decoy” (fake site).

- No signs of secret communication or spy stuff.

This site isn’t a secret spy site or covert messaging page. It’s just a blog with a weird URL, probably used for testing, fake traffic, or search engine tricks.

Multiple Google dorks returned no visible results on Google Search, indicating possible deindexing, cloaking, or anti-bot/anti-crawl protections."

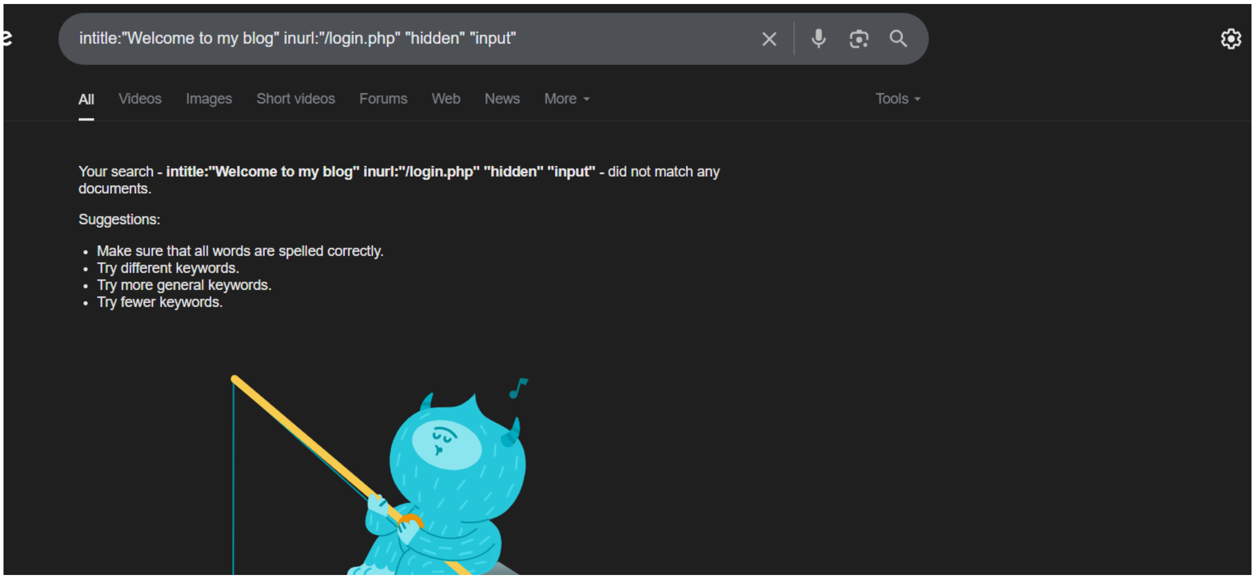


inurl:/member.php "hidden" "login" intitle:"anime blog" -"register"

Your search - **inurl:/member.php "hidden" "login" intitle:"anime blog" -"register"** - did not match any documents.

Suggestions:

- Make sure that all words are spelled correctly.
- Try different keywords.
- Try more general keywords.
- Try fewer keywords.

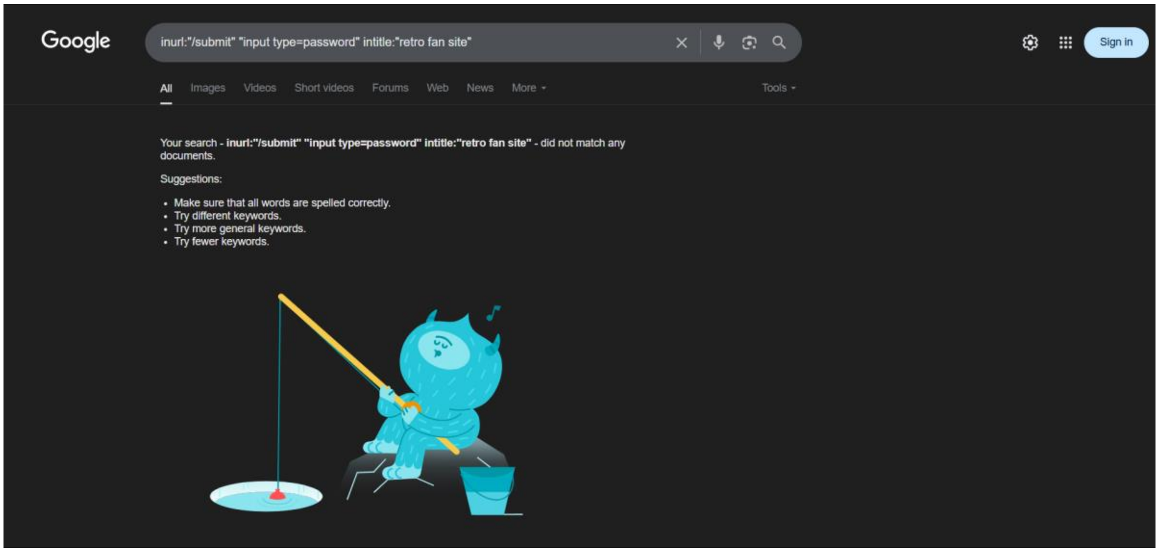


intitle:"Welcome to my blog" inurl:"/login.php" "hidden" "input"

Your search - **intitle:"Welcome to my blog" inurl:"/login.php" "hidden" "input"** - did not match any documents.

Suggestions:

- Make sure that all words are spelled correctly.
- Try different keywords.
- Try more general keywords.
- Try fewer keywords.

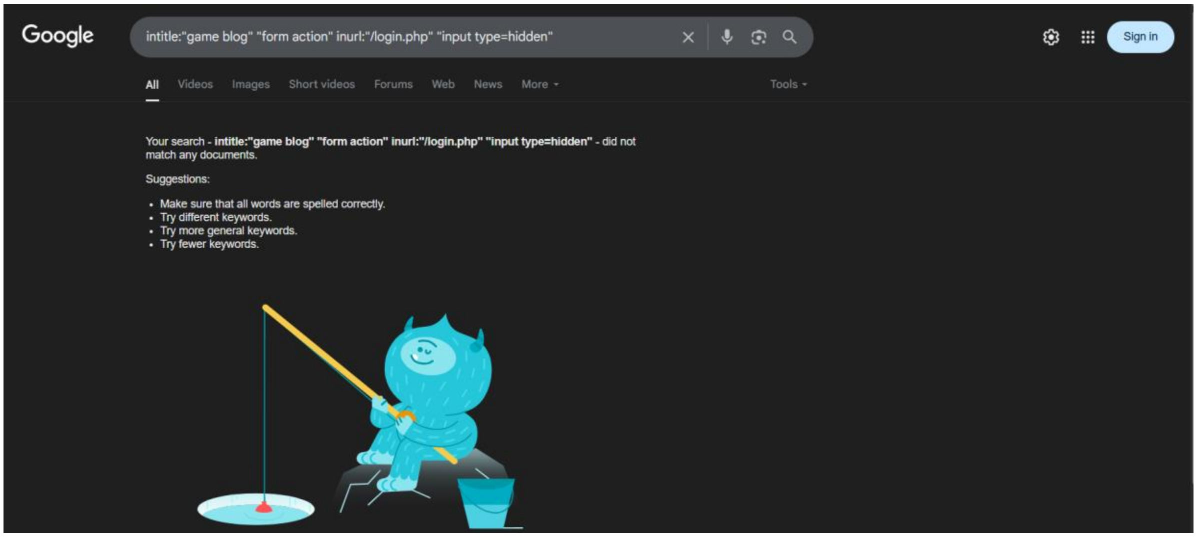


inurl:"/submit" "input type=password" intitle:"retro fan site"

Your search - **inurl:"/submit" "input type=password" intitle:"retro fan site"** - did not match any documents.

Suggestions:

- Make sure that all words are spelled correctly.
- Try different keywords.
- Try more general keywords.
- Try fewer keywords.

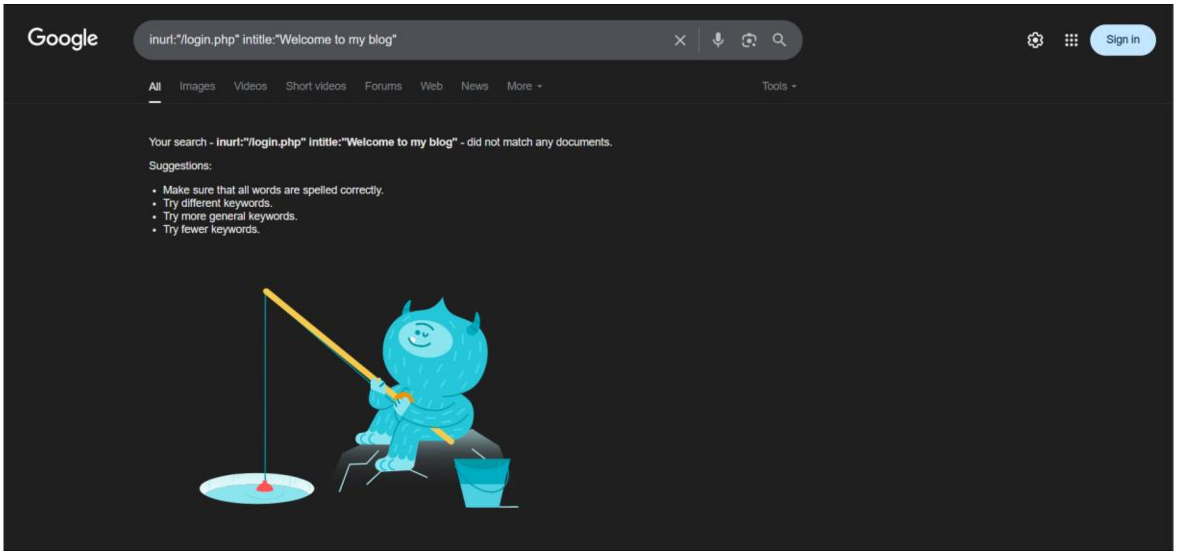


intitle:"game blog" "form action" inurl:"/login.php" "input type=hidden"

Your search - **intitle:"game blog" "form action" inurl:"/login.php" "input type=hidden"** - did not match any documents.

Suggestions:

- Make sure that all words are spelled correctly.
- Try different keywords.
- Try more general keywords.
- Try fewer keywords.



inurl:"/login.php" intitle:"Welcome to my blog"

Your search - **inurl:"/login.php" intitle:"Welcome to my blog"** - did not match any documents.

Suggestions:

- Make sure that all words are spelled correctly.
- Try different keywords.
- Try more general keywords.
- Try fewer keywords.

Learning Outcomes

- Developed proficiency in manual and automated web investigation techniques.
- Learned to interpret and leverage WHOIS and IP tracking data for site profiling.
- Used Google dorks to uncover hidden or sensitive site resources.
- Enhanced skills in web page source code inspection for detecting vulnerabilities.
- Gained experience in automating security checks using Python, focusing on form input validation, cookie security, and exposed files.
- Identified key patterns that distinguish covert/insider-only sites from typical public websites.
- Understood how to combine multiple data sources for a comprehensive risk assessment.

Conclusion

Through manual and automated techniques, the investigation revealed varying levels of transparency, security practices, and potential covert activity across the analyzed websites. Sites with open WHOIS data and public-facing content tended to be less suspicious, while those blocking crawlers, disabling registration, or exhibiting weak cookie security were flagged as higher risk. The use of Python automation enhanced the speed and consistency of vulnerability detection. Overall, the report demonstrates the value of combining manual expertise with automation to robustly assess modern web platforms for covert activity and security risks.

PYTHON SCRIPT:

```python
import requests
from bs4 import BeautifulSoup
import re
from urllib.parse import urljoin, urlparse
from docx import Document
from docx.shared import Pt

urls = [
    "https://backstreetmen.createmybb.com/search.php?action=results&sid=39885b178
31709d2e802c1c33aeb11fc",
    "https://nusalemmk.click/product_tag/6692013_.html",

]

sensitive_paths = [
    ".env", ".git/", "config.php", "wp-config.php", "backup", "backups",
"db_backup", "database.sql",
    "dump.sql", "config.json", "config.ini", "phpinfo.php"
]

def extract_form_details(soup):
    forms = soup.find_all("form")
    findings = []
    for form in forms:
        for inp in form.find_all("input"):
            details = {
                "type": inp.get("type"),
                "name": inp.get("name"),
                "placeholder": inp.get("placeholder"),
                "style": inp.get("style"),
                "form_action": form.get("action"),
            }
            findings.append(details)
    return findings

def check_security_headers(headers):
    weak_cookies = []
    cookies = headers.get("Set-Cookie")
    if not cookies:
        return weak_cookies
    for cookie in cookies.split(", "):
        cval = cookie.lower()
        if "=" not in cookie:
            continue
        has_secure = "secure" in cval
        has_httponly = "httponly" in cval
        if not (has_secure and has_httponly):
            weak_cookies.append(f"Weak cookie: {cookie}")
    return weak_cookies

def check_sensitive_paths(base_url):
    exposed = []
    parsed = urlparse(base_url)
    root = f"{parsed.scheme}://{parsed.netloc}/"
    for path in sensitive_paths:
        url = urljoin(root, path)
        try:
            resp = requests.get(url, timeout=7)
            if resp.status_code == 200 and ("Index of" in resp.text or len(resp.text) > 30):
                exposed.append(f"{url} [{resp.status_code}]")
            elif resp.status_code in (401, 403):
                continue
        except Exception:
            continue
    return exposed

results = []

for url in urls:
    print(f"Scraping: {url}")
    try:
        resp = requests.get(url, timeout=10)
        soup = BeautifulSoup(resp.text, "html.parser")

        form_details = extract_form_details(soup)
        weak_cookies = check_security_headers(resp.headers)
        exposed_files = check_sensitive_paths(url)

        results.append({
            "URL": url,
            "Form Details": '\n'.join(str(f) for f in form_details) if form_details else "-",
            "Weak Cookies": '\n'.join(weak_cookies) if weak_cookies else "-",
            "Exposed Files/Dirs": '\n'.join(exposed_files) if exposed_files else "-"
        })
```

```python
    except Exception as ex:
        print(f"Error scraping {url}: {ex}")
        results.append({
            "URL": url,
            "Form Details": "ERROR",
            "Weak Cookies": "-",
            "Exposed Files/Dirs": "-"
        })

# Write to Word document
document = Document()
document.add_heading("Website Security Scan Results", 0)

for result in results:
    document.add_heading(result["URL"], level=1)
    table = document.add_table(rows=0, cols=2)
    table.style = 'Light List Accent 1'
    for key in ["Form Details", "Weak Cookies", "Exposed Files/Dirs"]:
        row = table.add_row().cells
        row[0].text = key
        row[1].text = result[key]
        run = row[0].paragraphs[0].runs[0]
        run.font.bold = True
        run.font.size = Pt(11)
    document.add_paragraph()  # blank line

docx_path = "covert_websites_findings_form_cookies_files.docx"
document.save(docx_path)
print(f"Results saved to {docx_path}")
```