





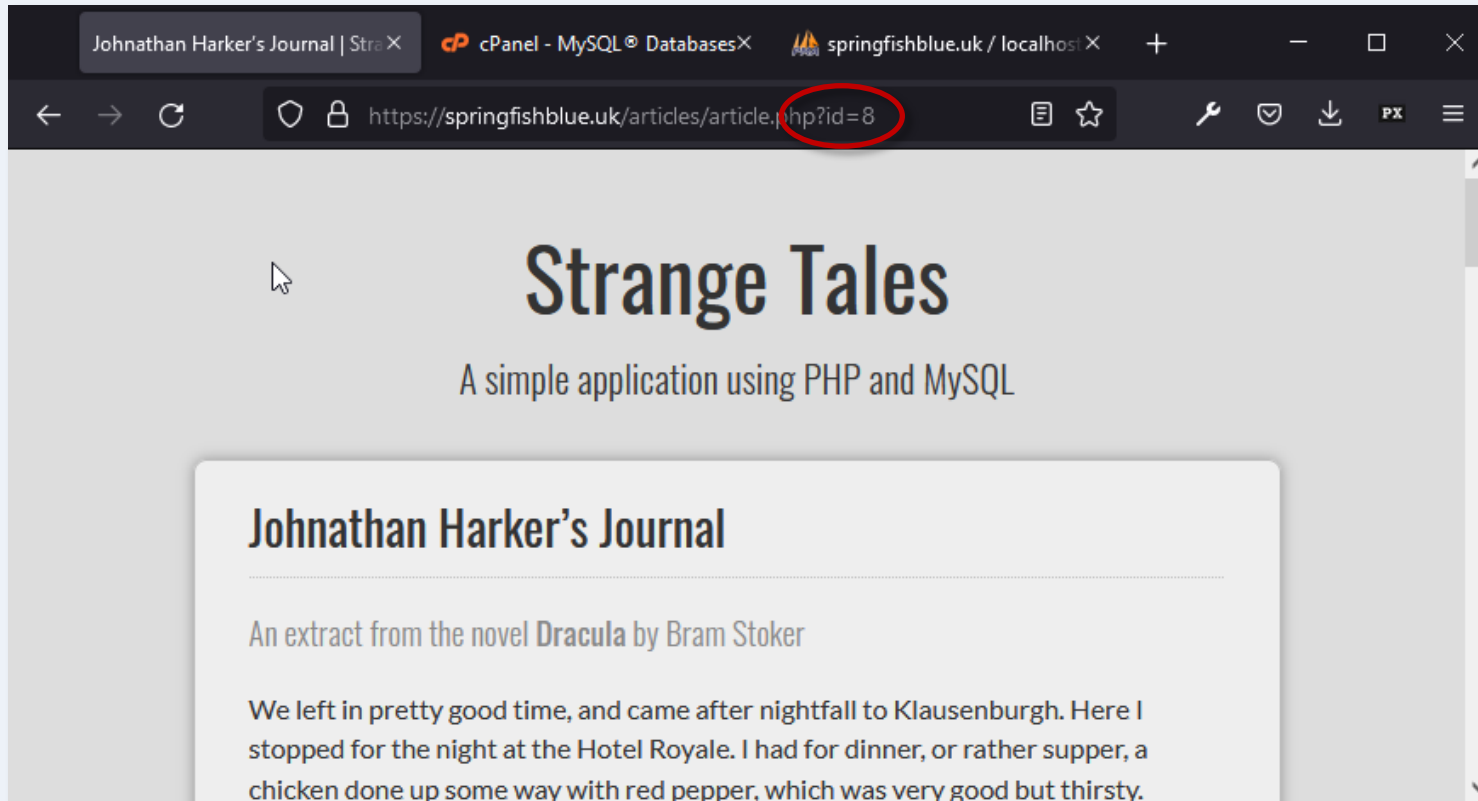
Website Security

Content Management

How are websites “attacked”?

- **Access using stolen credentials** 
Login details stolen using keyloggers etc.
- **SQL Injection** 
Malicious strings added to URL parameters.
- **Cross-Site Scripting (XSS)** 
Malicious scripts run via HTML forms etc.
- **Denial-of-Service (DoS)** 
Flooding a server with requests so that it becomes unavailable to legitimate users.

SQL Injection



SQL Injection is a technique hackers use to manipulate PHP code and insert their own scripts. They do this by replacing the seemingly innocuous URL parameter with their own code.

In the above example, "8" would be replaced with code that attempts to allow the hacker access to your database or to do practically anything else.



Unsafe code

```
<?php
$article=$_GET['id'];
$conn = mysqli_connect ($host, $user, $password, $name) or die ("Cannot open database.");
$query = "SELECT * FROM articles WHERE article_id = $article";
$result = mysqli_query($conn, $query) or die ("Error querying database.");
mysqli_close($conn);
$row = mysqli_fetch_array($result);
?>
```

URL: article.php?article_id=5



This script fragment takes the value given to it from GET, assigns it to a variable (`$article`) and uses that value in the SQL query. This is a **very** bad idea.

Safe code

```
<?php
# if $article has no value or is not a string integer, go to 404
if (isset($_GET['id']) && filter_var($_GET['id'], FILTER_VALIDATE_INT)) {
    $article=$_GET['id'];
}else{
    header('HTTP/1.0 404 Not Found');
    exit("<h1>Not Found</h1>\n<p>The submitted data is not valid.</p>");
}

# if we got this far, the data is safe, so go ahead and query the database
$conn = mysqli_connect ($host, $user, $password, $name) or die ("Cannot open database.");
$query = "SELECT * FROM articles WHERE article_id = $article";
$result = mysqli_query($conn, $query) or die ("Error querying database.");
mysqli_close($conn);
$row = mysqli_fetch_array($result);
?>
```

URL: article.php?article_id=5

This script fragment checks to see if the URL parameter conforms to the data type expected and if it doesn't, a 404 error is issued, and a message printed.

Context

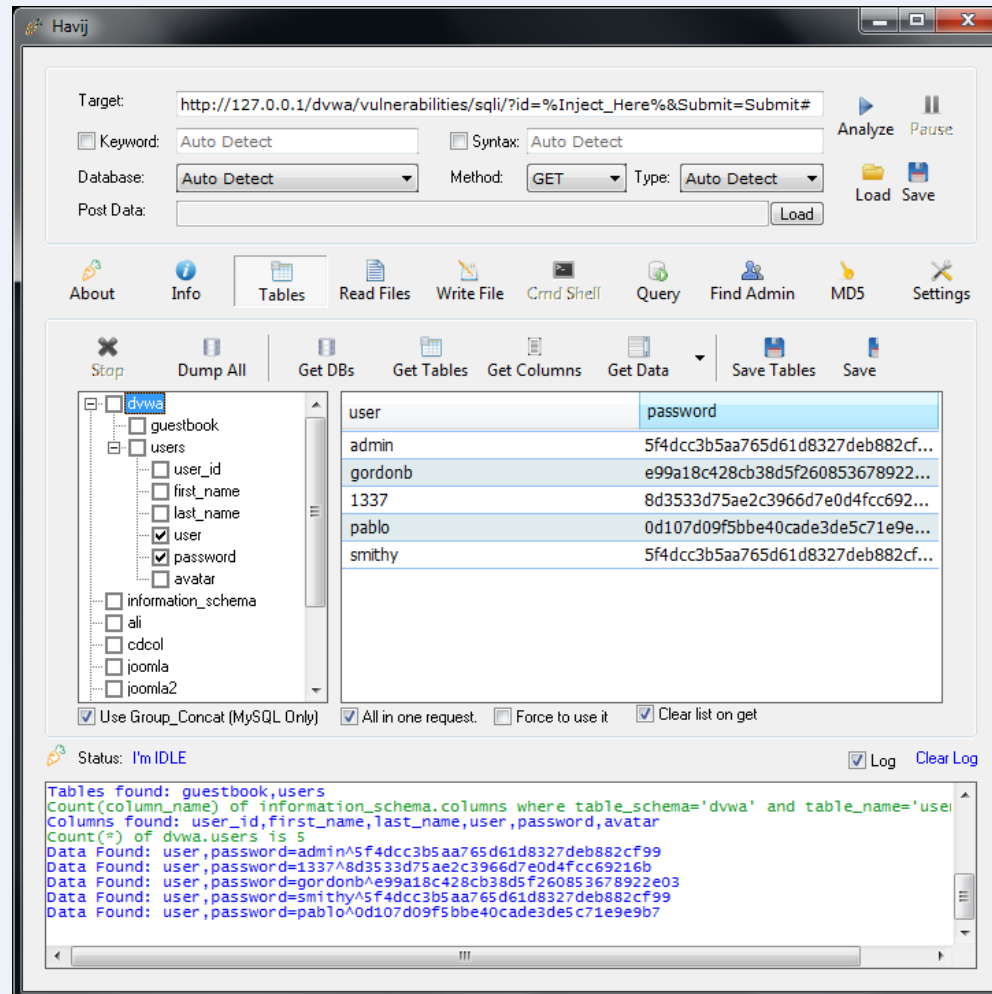
- There are many different types of SQL Injection attacks, depending on context.
- They can be used to circumvent secure logins.
- Or to list all information in a database.
- Or to drop (delete) a database table.
- Or to insert malicious scripts that do other things – ultimately, a hacker could gain control of a web server.
- Hackers actively look for security holes...

Server Logs

```
195.229.235.36 - - [25/Jan/2011:02:45:04 +0000]"GET  
/corner/article.php?id=999999.9+UNION+ALL+SELECT+0x313032  
35343830303536%2C0x31303235343830303536%2C0x3130323  
5343830303536%2C0x31303235343830303536-- HTTP/1.1"  
200 26037 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT  
5.1; SV1; .NET CLR 2.0.50727) Havij"
```

You may be able to spot unusual user agent names in your server logs. In the above example, "Havij" doesn't sound like any browser I've ever heard of. That's because it isn't a browser, it's a piece of software used by a hacker to look for security vulnerabilities.

Software for hacking



Havij is legal and free. The product description is chilling:

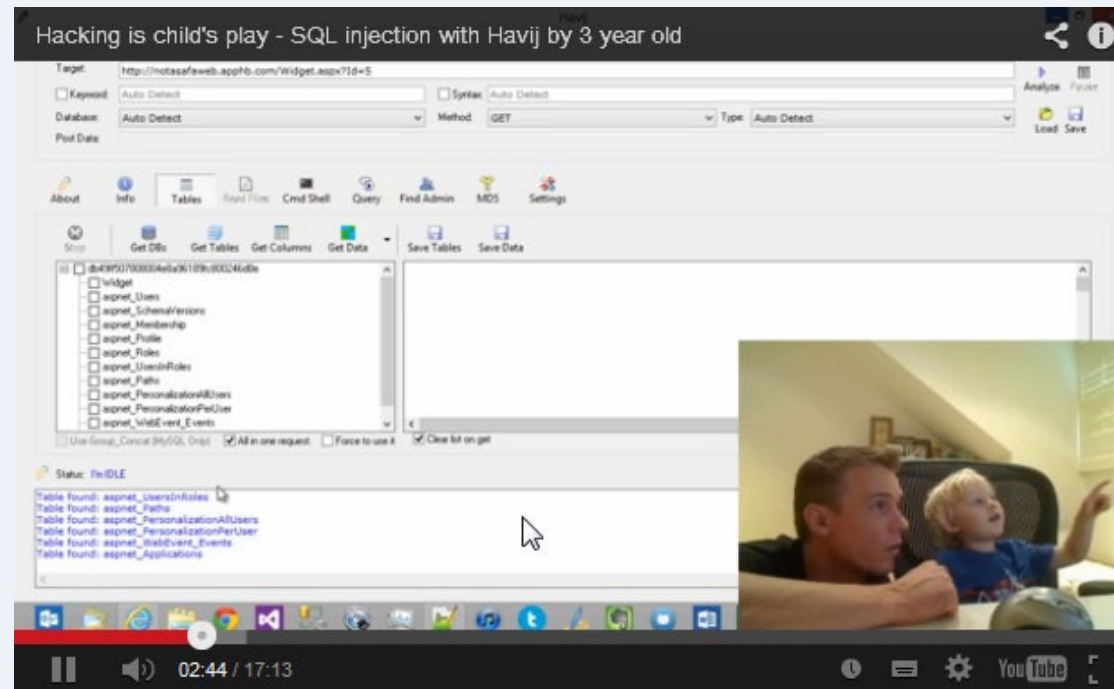
"Havij is an automated SQL Injection tool that helps penetration testers to find and exploit SQL Injection vulnerabilities on a web page.

It can take advantage of a vulnerable web application. By using this software user can perform back-end database fingerprint, retrieve DBMS users and password hashes, dump tables and columns, fetching data from the database, running SQL statements and even accessing the underlying file system and executing commands on the operating system.

The user friendly GUI (Graphical User Interface) of Havij and automated settings and detections makes it easy to use for everyone even amateur users."

There are [several other SQL injection tools](#) freely available. Currently, the most popular appears to be [SQLmap](#).

Hacking is child's play



This excellent video demonstrates how easy it is to hack an unprotected website using Havij. It explains exactly how it is done and, importantly, how to protect your website from such an attack.

[Hacking is child's play](#) – SQL injection with Havij by 3 year old

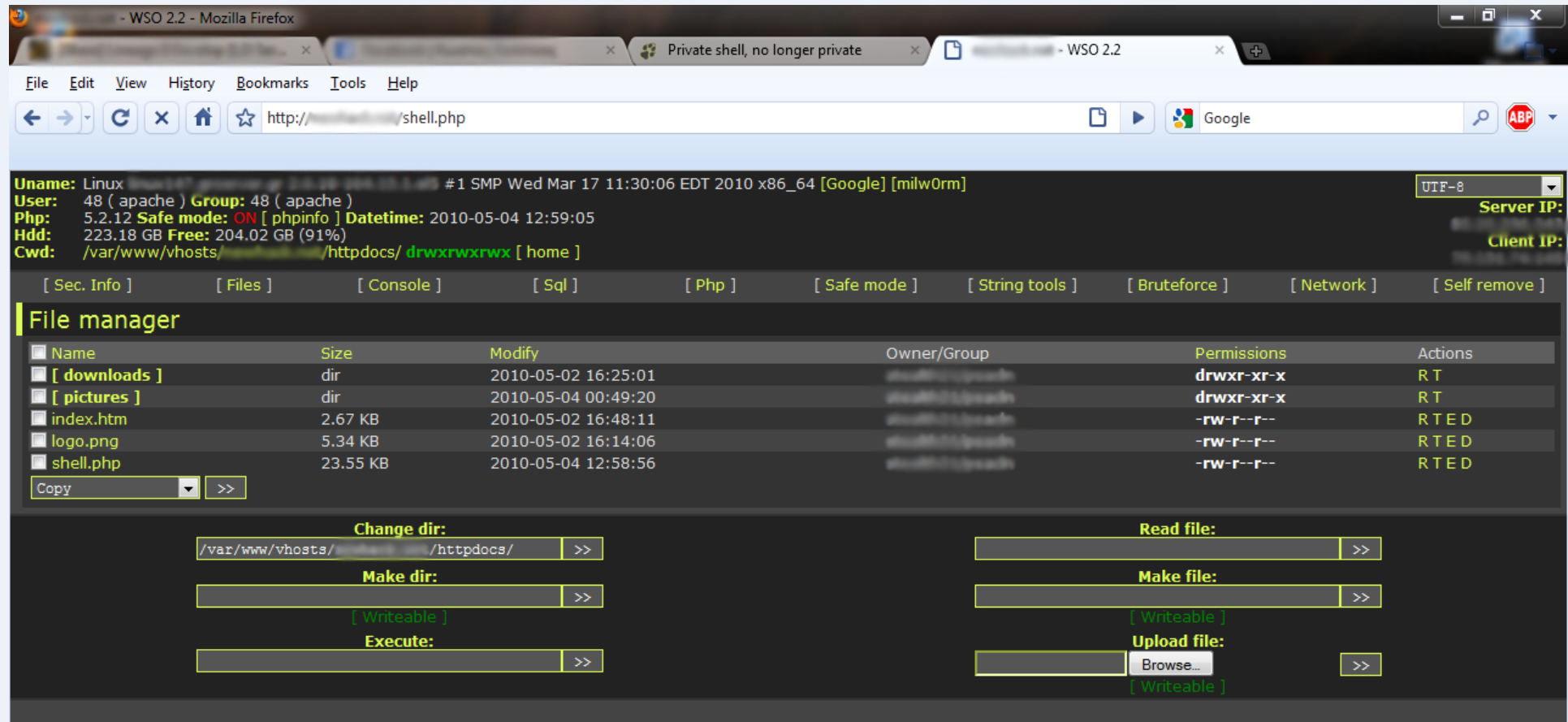
What can hackers do?

- Hackers can use a security hole to view information in databases or even add their own files to your site, leading to all sorts of possibilities.
- They can even add a file manager that only they have access to...

```
<?php # Web Shell by oRb
$auth_pass =
"b497dd1a701a33026f7211533620780d
";
$color = "#df5";
$default_action = 'FilesMan';
$default_use_ajax = true;
$default_charset = 'Windows-1251';
```

This is a script from an innocuous file called **.sym.php** – the leading period is used to hide the file.

Web Shell Software



Once a hacker finds a way to upload a file to your site, either via FTP or some vulnerability, they can install a file manager like the one above and eventually a “Root Kit”.

Root Kit

- A Root Kit is malicious software that hides itself but allows a hacker to gain “root” access over a computer – usually a web server.
- Once such software is in place, the hacker has complete control of the server and can even lock out legitimate admin users.
- The only safe way to recover from such an intrusion is a complete server rebuild and to fix the original vulnerability so that it can't happen again.

What can hackers do?

They can steal information from databases such as financial data, passwords, names, addresses, credit card details etc.

Lush website hack sees customers defrauded

Some customers who shopped online with Lush between October and January have had their card details stolen

Mark King and Charles Arthur
guardian.co.uk, Friday 21 January 2011 13.29 GMT
[Article history](#)



Lush says it became aware of hacker attacks in late December. Photograph: Guardian

Handmade cosmetics group [Lush](#) has admitted its website was hacked repeatedly by fraudsters over the past three months, putting thousands of customers at risk of having their card details stolen. But the company only informed customers last night.

Lush has taken down its website and replaced it with a statement: "We would like all customers that placed online orders with us between 4 Oct 2010 and 20 Jan 2011 to contact their banks for advice as their card details may have been compromised."

What can hackers do?

They can steal media valued at millions of dollars from organisations that really should be protecting their interests better.

Michael Jackson back catalog stolen in Sony hack



by [Steven Musil](#) | March 4, 2012 9:30 PM PST



Summary: Two U.K. men have been charged with illegally downloading the singer's entire 50,000-track back catalog, including unreleased songs.

Sony's sad security song isn't finished yet.

Hackers have reportedly broken into the music label's servers and downloaded Michael Jackson's entire 50,000-track catalog, including many songs that have never been released, according to a report in Britain's [Sunday Times](#) (behind paywall). Sony purchased the catalog in 2010 from Jackson's estate for \$250 million--billed as the biggest recording deal in history.



"Everything Sony purchased from the Michael Jackson estate was compromised," a source told the newspaper. "It caused them to check their systems and they found the breach. There was a degree of sophistication. Sony identified the weakness and plugged the gap."

Two men in the U.K. have been arrested and charged in the crime, according to [The Guardian](#). They have reportedly been released on bail and are scheduled to stand trial in January 2013.

What can hackers do?

They can hack into social network sites and harvest vast quantities of personal data.

15 February 2013 Last updated at 23:18 4.9K [Share](#) [f](#) [t](#) [e](#) [p](#)

Facebook was targeted by 'sophisticated' hackers

Facebook has revealed it was the target of a "sophisticated attack" by hackers last month, but found no evidence any user data had been compromised.

The US-based social network said that the attack occurred when employees visited a mobile developer website "that was compromised".



Facebook has one billion active users worldwide

Facebook said in a blog post that it was not the only company to have been attacked in this way.

More than one billion people use Facebook worldwide.

"Last month, Facebook security discovered that our systems had been targeted in a sophisticated attack," the California-based company said.

"The attack occurred when a handful of employees visited a mobile developer website that was compromised."

Malware was downloaded on to its employees' laptops, the firm said, adding: "As soon as we discovered the presence of the malware, we remediated all infected machines, informed law enforcement, and began a significant investigation that continues to this day."

"We have no evidence that Facebook user data was compromised in this attack," Facebook said in its blog post.

Related Stories

- [Hackers target 250,000 Twitter users](#)
- ['China hackers' attack NY Times](#)
- [Facebook changes privacy settings](#)

What can hackers do?

They can encrypt data and demand a ransom for its return.

Royal Mail

'All we have had is losses': Royal Mail dismisses 'absurd' \$80m ransom demand

'Under no circumstances will we pay that absurd amount,' delivery firm says, telling hackers it is not the booming company they think

Rob Davies

🐦 @ByRobDavies

Wed 15 Feb 2023 16.59 GMT

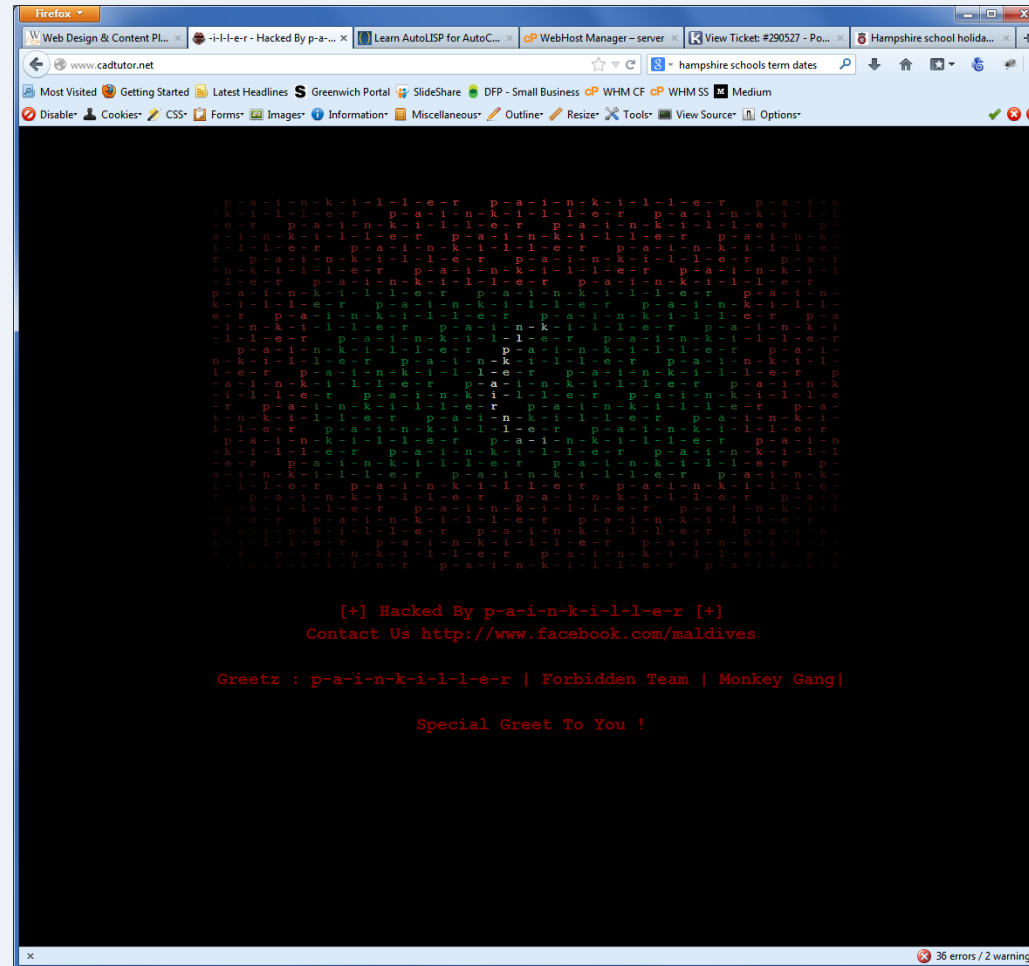


📷 Royal Mail was hit by a ransomware attack in January which has affected its international deliveries. Photograph: Maureen McLean/Rex/Shutterstock

Royal Mail rejected an “absurd” **ransom demand** for \$80m (£67m) from hackers linked to Russia, according to transcripts that offer a rare glimpse into negotiations when companies are hit by a ransomware cyberattack.

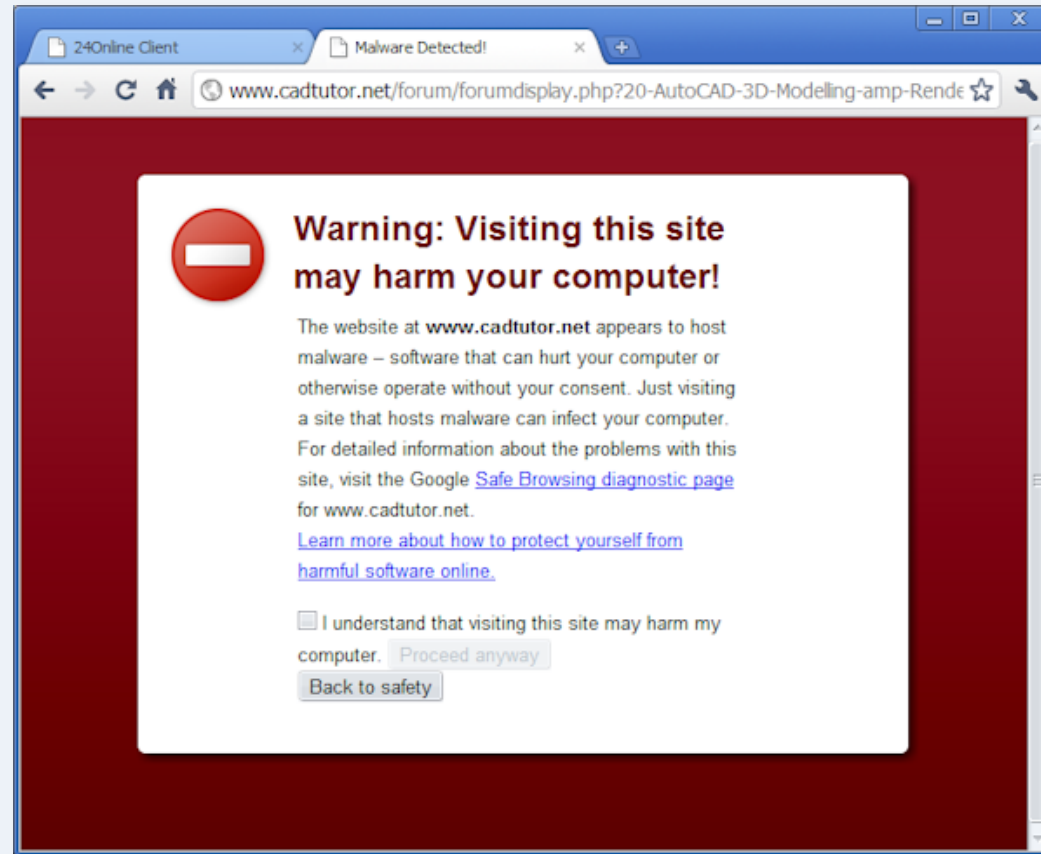
What can hackers do?

They can deface your site and completely change your homepage. This is the CADTutor site on 9th September 2013. Hackers took advantage of a vulnerability in the vBulletin forum software. Always keep your web applications up to date!

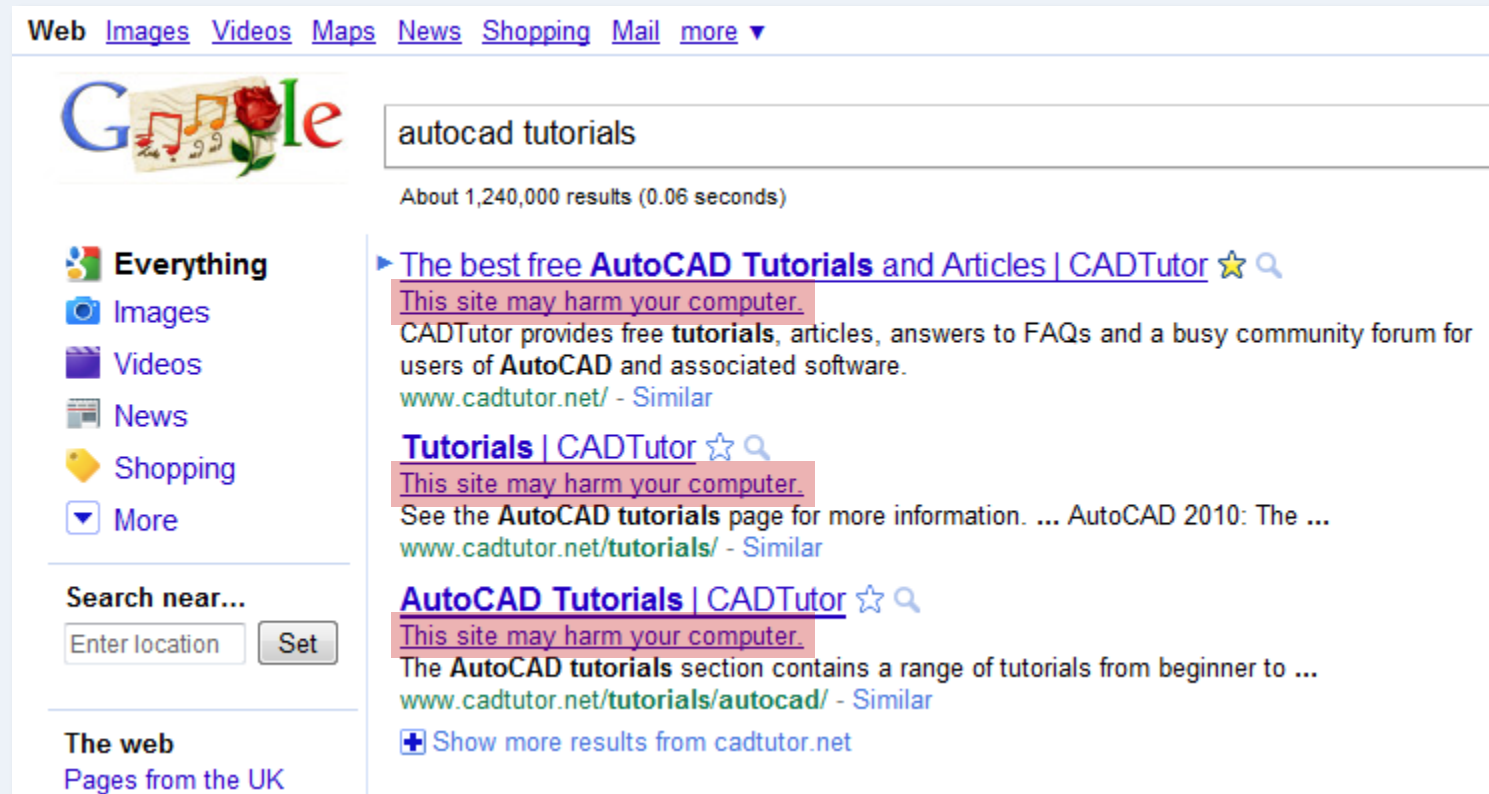


What can hackers do?

They can change files on your website so that they install viruses on your visitor's computers, causing your website to be blacklisted by Google.



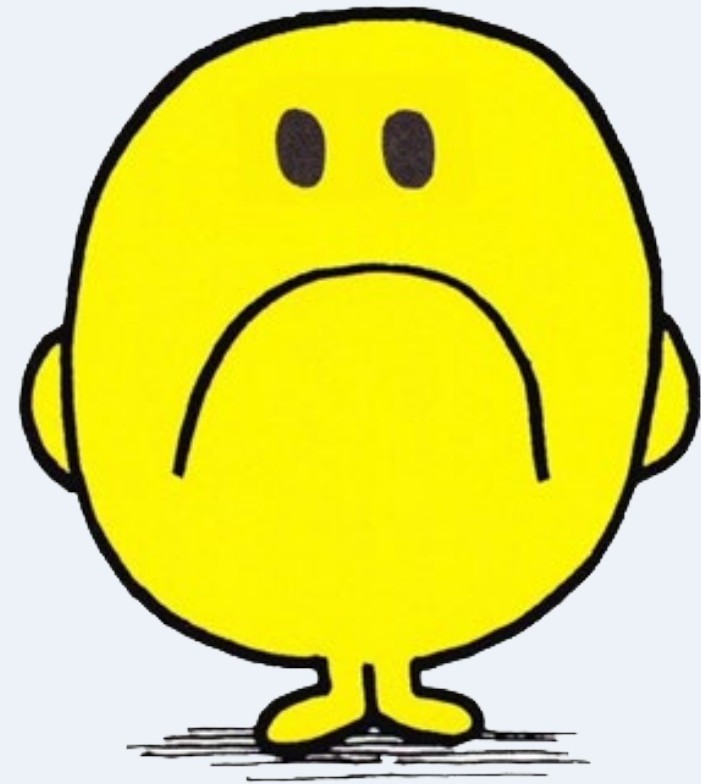
Google warns users about unsafe sites



If this happens to your site, you must resolve the problem and then use Google Search Console to request that Google scan your site and remove the notice if it is found to be clean.

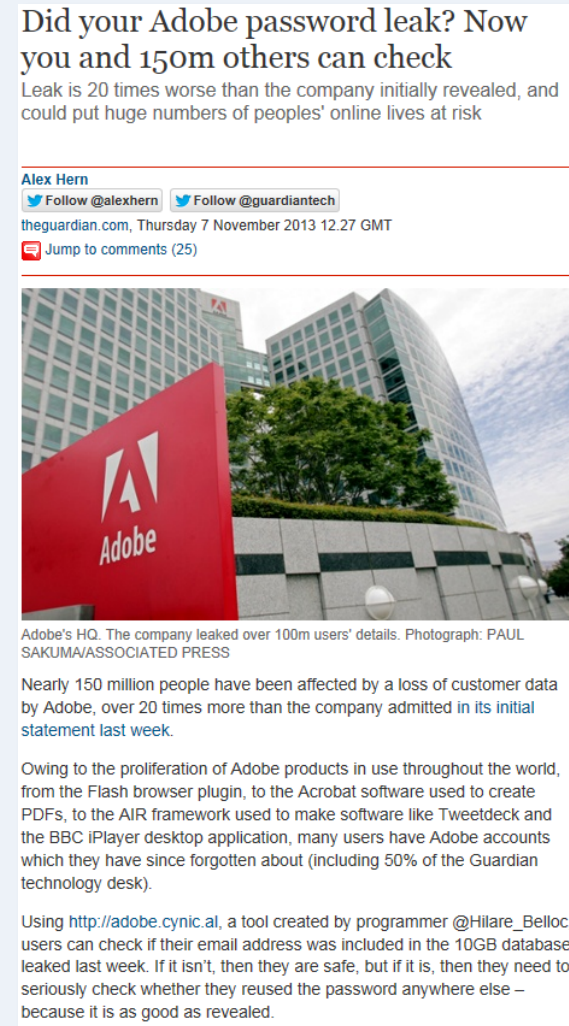
What can hackers do?

- They can make your life miserable and lose you lots of money.
- Hackers don't just target big organisations.
- They seek out small, vulnerable sites for practice and fun.



Currently...

- The hacking of websites is on the increase.
- Hacking software is freely available and increasingly sophisticated, though easy to use – anyone can do it.
- How can we prevent our site from being hacked?

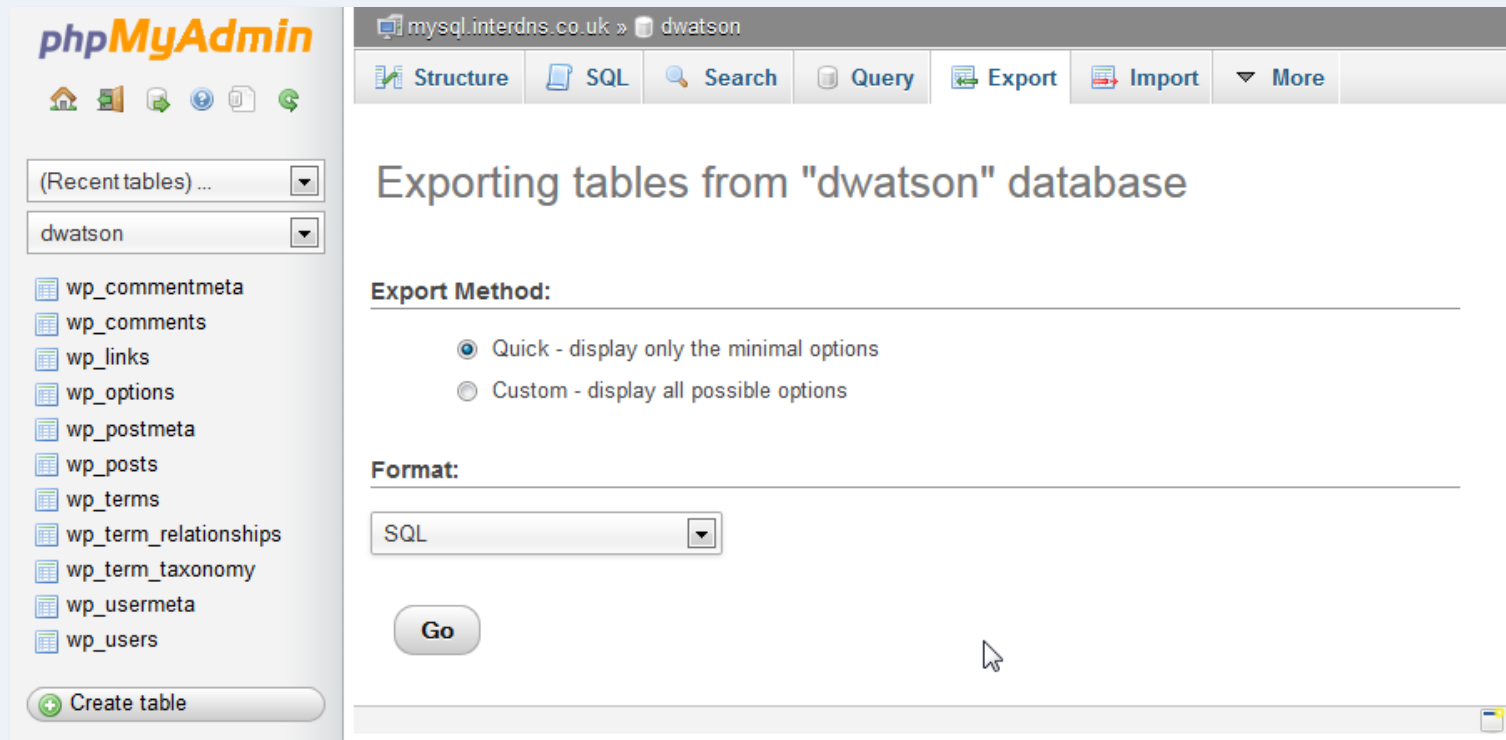


No website can be 100% secure
but if you take reasonable
precautions, you can
considerably reduce the risk...

Precautions

- Ensure you keep all your web applications (like WordPress) up-to-date and sign up for notifications and security alerts.
- Make sure all your own scripts are secure, check that you are validating and sanitising data correctly – get advice if you're not sure.
- Use strong passwords for **all** your access credentials.
- Use anti-virus software on your local computer and scan regularly – keylogging is a popular way for hackers to find out what passwords you use.

Backup your files and databases

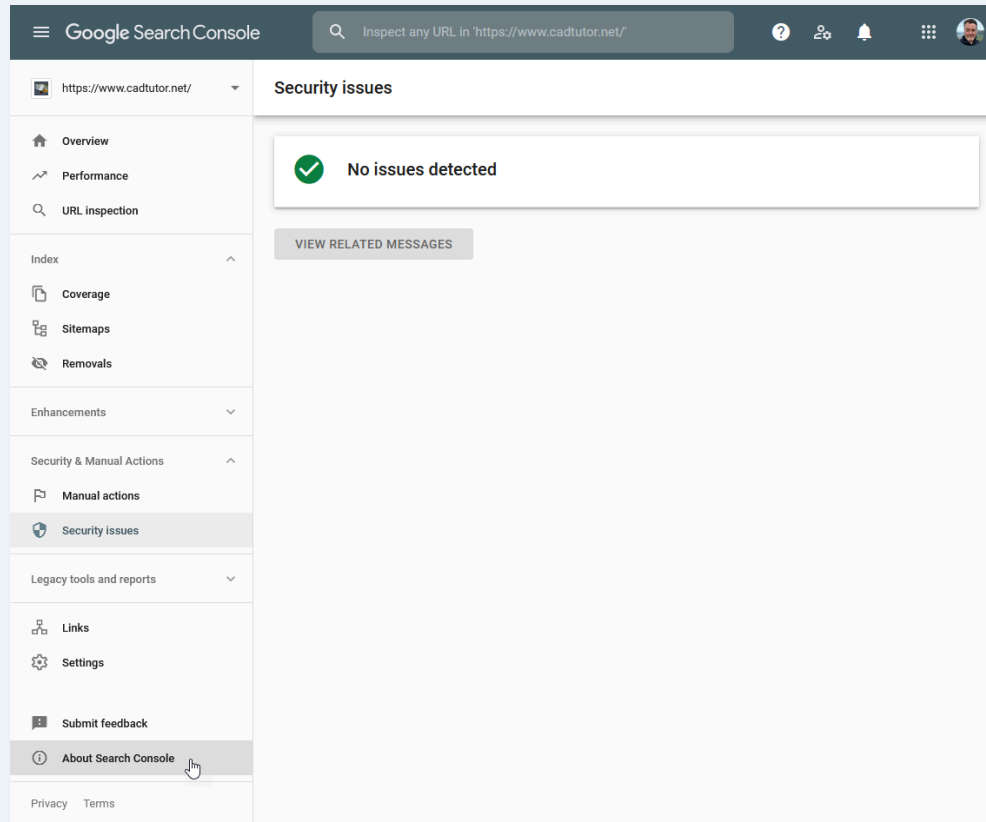


Keeping a backup of your website files is easy because they don't change unless you edit them yourself but on busy sites, databases are changing all the time. Make sure you implement a regular backup policy for your databases. Some control panels (e.g. cPanel) have backup tools you can use. Alternatively, you can use PHPMyAdmin to export your databases to text files (using the SQL format) that can be stored locally.

Precautions

- Monitor site traffic with analytics software and look for anything unusual.
- Check your site files via FTP and look for anything suspicious like changed dates on files or files you don't recognise.
- Talk to your host about best practices for security.
- Use IP restricted access to control panels.
- Place sensitive data above web root if your host allows access.
- Change the default name of admin folders.
- Understand how hackers operate.

Google Search Console



Use Google Search Console to monitor the health of your websites. Google will alert you immediately if any malware is discovered on your site.

There are lots of things you can do to reduce the risk, but you can't remove risk completely...

What if I get hacked?

1. Close the site immediately – use .htaccess to redirect all traffic to a temporary holding page:

`Redirect 302 / http://www.mysite.com/site-maintenance.html`

2. Report the problem to your web host and ask for advice.
3. Find the source of the problem.
4. Eradicate the problem.
5. Do not open the site until you are 100% sure it is safe for your visitors.
6. Request a Google review (if you've been blacklisted).

Where can I get help?

Some companies claim to be able to recover hacked sites for you but unless you have lots of money, you're pretty much on your own. However, if you have a good web host, they should be able to help and there is plenty of advice available, particularly from Google.

Google Search Central: [New first stop for hacked site recovery](#)

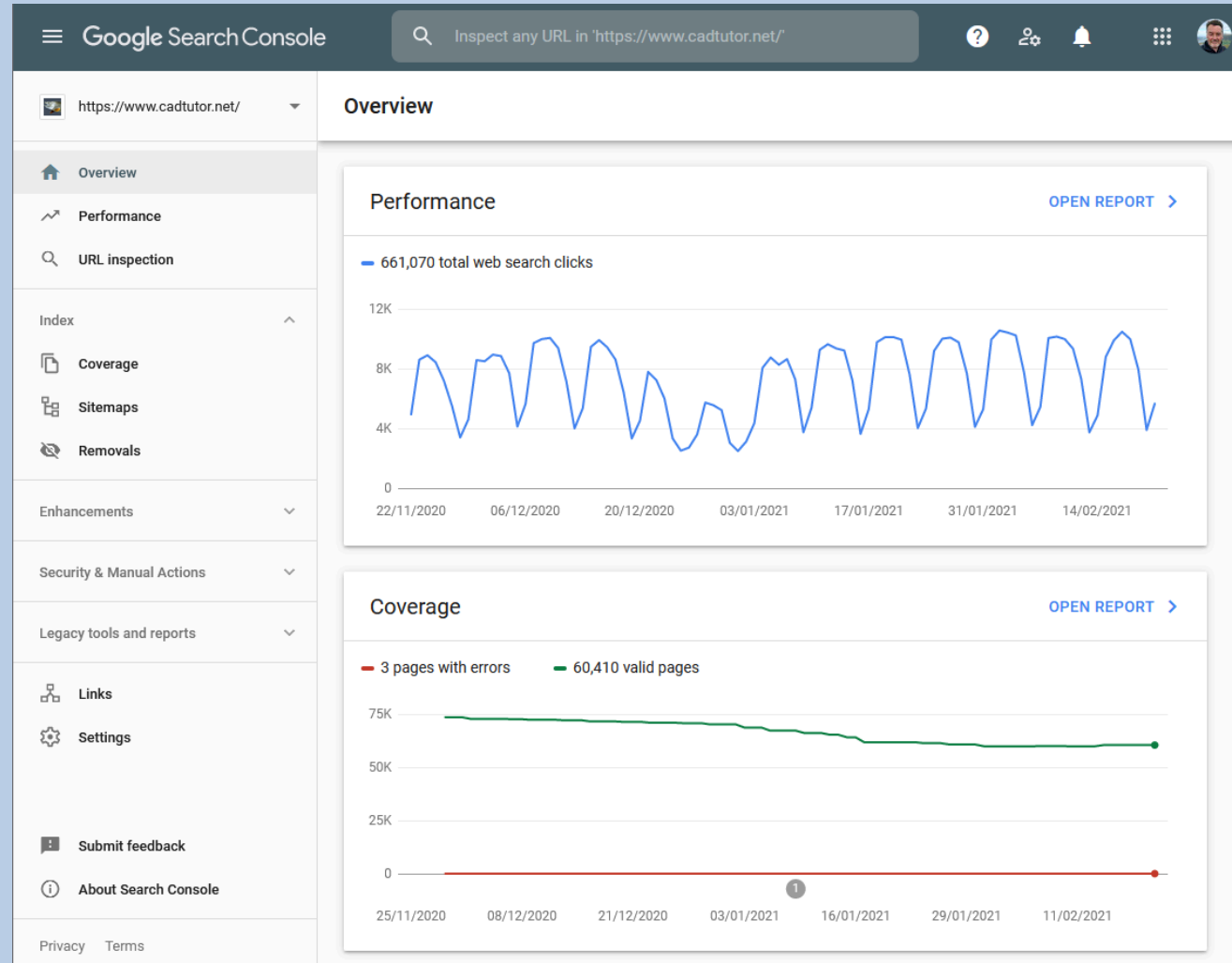
Google Search Central: [About malware and hacked sites](#)

Google Search Central: [Best practices against hacking](#)

[StopBadware.org](https://stopbadware.org)



Happy ending...



Reduce the risk. Always take a professional approach to your work and use all the tools available to you.

Stay safe