GRED Web Check

Early Warning System Against Website Malware Injection

(whitepaper revision 2023-MAR)

SecureBrain
A Hitachi Group Company

Overview

In the present landscape, a website for your business is no longer optional. It is key to reaching the target audience that is the most likely to become loyal clientele. Without an official online presence, you run the risk of losing a significant share of profit opportunities.

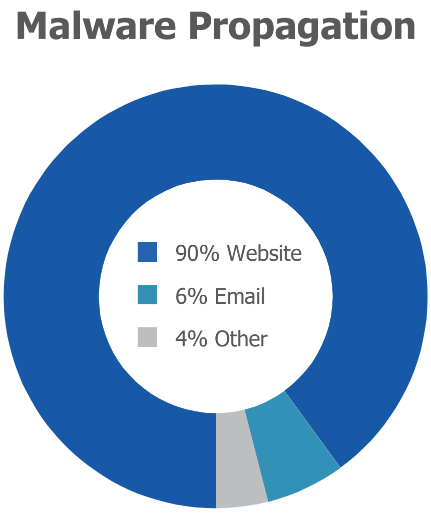
Nevertheless, there are intricacies that make managing a website challenging. When it comes to cybersecurity, hackers are an ever-present threat to the integrity of your online presence. Even with minimal know-how, hackers are able to introduce malware to your website. The presence of malware puts you and your customer's privacy at risk.

Instances like this not only threatens the safety of your clients but it also casts a negative light onto your business. According to research, in 2019, 62% of consumers are already not confident about the security of the data they share with websites and retailers. As a business, you don't want your brand to be associated with this negative connotation. After all, your website is a reflection of the kind of company that you run. It should be running as smoothly as your day-to-day operation; if they can't trust your site, then they won't trust you as a brand.

Arguably, one of the most common forms of cyber breaches is the introduction of malware otherwise known as website malware injection. According to the most recent Google Transparency report, over 50,000 websites are deemed unsafe because of the presence of malware. Despite the sobering statistics, traditional website security options fail to effectively prevent attacks and safeguard a website from malicious software.

GRED Web Check is a service that is necessary for you to manage a website with peace of mind. It acts as an early warning solution capable of alerting a web administrator in the event of a real-time attack. This cloud-based solution continuously runs security checks ensuring that your website is free from malware at all times.

Threats and Risks: Common Website Malware Injections



"Malware now spread mostly through tainted website..."
USA Today (2013)

The recent Malwarebytes survey has revealed a shift of instances in malware injections from individuals to organizations and businesses. Over the last few years, consumer malware reports have dipped by 2%. Consequently, business detections have increased by more than 10%. Needless to say, getting acquainted with common website malware injection is all the more important in light of the recent trend.

There are several ways malware can be introduced onto a website. Drive-by downloads or DBDs are a type of malware attack that downloads malicious programs onto a device without the consent of the user. This type of malware can hijack a device, track information and activity, as well as, disable the device completely.

What makes DBDs particularly concerning especially for businesses is the fact that it can infiltrate legitimate websites. Through SQL injections, CMS vulnerabilities, or HTML content modification, hackers are able to attack consumers through a website unbeknownst to its administrator.

Aside from DBDs, hackers are able to penetrate websites through hostile JavaScript, web server modules, and website defacement.

Status Quo: Traditional Website Security

Malware has existed for as long as there have been computers in production. In fact, the first malware was detected almost four decades ago in 1982. With that said, securing a website is also not a new innovation.

Traditional web administrators rely on several measures in order to ensure that the pages that they manage are free from malicious software. While these options are effective for more common threats, a system is no match to more sophisticated malware. Among the most common traditional website security options are:

Web Application Firewall or WAF

Web Application Firewall or WAF is undoubtedly one of the most popular website security options available in the market today. This type of security mechanism filters threats by analyzing HTTP traffic before it reaches the server.

While effective, using WAF to your operation's advantage takes time and effort. Specific filters have to be put in place in order to make this security measure work. There is quite a substantial amount of friction required to install a WAF on a website. Moreover, because of the restrictive and complex nature of its detection system, a WAF can be easily bypassed by a hacker.

Web Content Integrity Check

Otherwise known as File Integrity Monitoring, Web Content Integrity Check monitor's a website by detecting recent uploads, edits, or removals. This security option works by taking a log of a website's files and comparing it with the site's current version. This method is effective in uncovering website defacement threats.

Most websites today are rife with dynamic content. Unfortunately, Web Content Integrity Checks only works for static HTML pages.

Vulnerability Assessments

Traditional web administrators rely on penetration and vulnerability checks in order to ensure that the pages that they manage are free from vulnerabilities. While effective, this security option is not the most economical. The cost prevents companies from undergoing these checks in the recommended period of time. Because of these lapses, the websites remain vulnerable to malware attacks.

SOC Outsourcing

Outsourcing a website's security operations center or SOC is a way to ensure its effectiveness. Third-party companies that provide this service, after all, are experts in the field. Aside from their expert knowledge, the SOC outsourcing option takes the burden of effort off of the website owner. This measure guarantees security with minimal effort.

However, SOC outsourcing comes with a hefty price tag. Especially for a small operation, outsourcing security efforts might not be the most cost-effective solution.

It should be emphasized that there is nothing wrong with employing traditional means of website security. However, these options are not enough to truly secure the integrity of a website. It is important to have an early warning beacon to remain informed in instances of attacks and minimize the effects of the infiltrations.

Fortified Defense:
GRED Web Check Solution

The failure of traditional website security checks lies in the downtime between detection and action. The shortcomings in the regularity of these safeguards allow malware to exist on a website for long periods of time before it is addressed. At that point, these attacks may have already caused severe damage to your online presence, your search engine status, and the integrity of your website visitor's systems.

In order to safeguard your operations and your client's sensitive information, your business needs an application that conducts continuous testing and allows for real-time malware warnings.

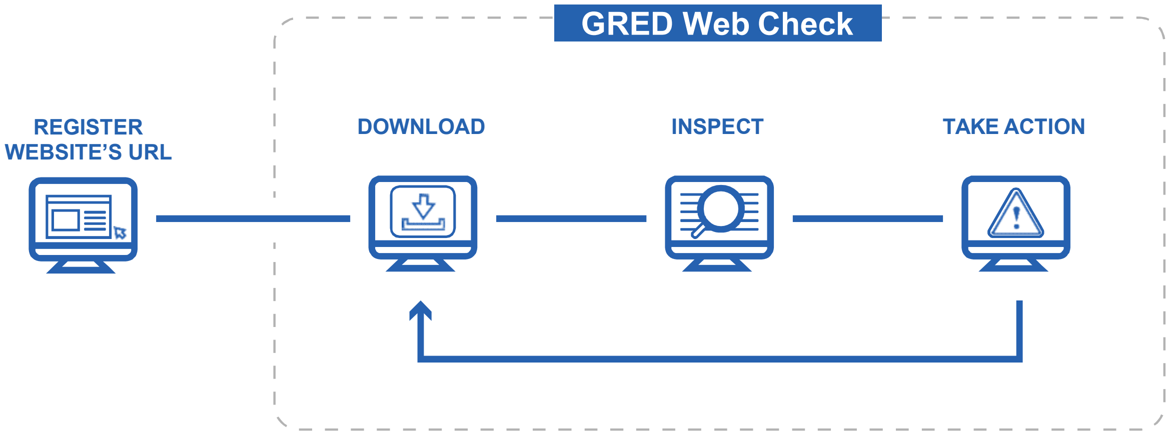
What is GRED Web Check?

Specifically designed to address website malware injections, SecureBrain's **GRED Web Check** is an invaluable tool that could improve the quality of your operations. It is an early warning system created to monitor a website 24 hours a day, 7 days a week, and 365 days in a year.

The service that **GRED Web Check** provides is particularly unique in the field because it is completely cloud-based and does not require any installations on the website. It requires neither any hardware purchase nor any software downloads.

It is simple. It is effective. It is exactly what you need for your business.

How Does it Work?



One of the best things about **GRED Web Check** is that it is fully automated and runs 24/7. Any web administrator would be able to operate **GRED Web Check** with ease.

At the onset, the administrator is required to register their website's URL onto **GRED Web Check.** Following the registration, the system takes over and conducts an analysis of the entire website. This analysis is done in three parts - Download, Inspection, and the Web Portal.

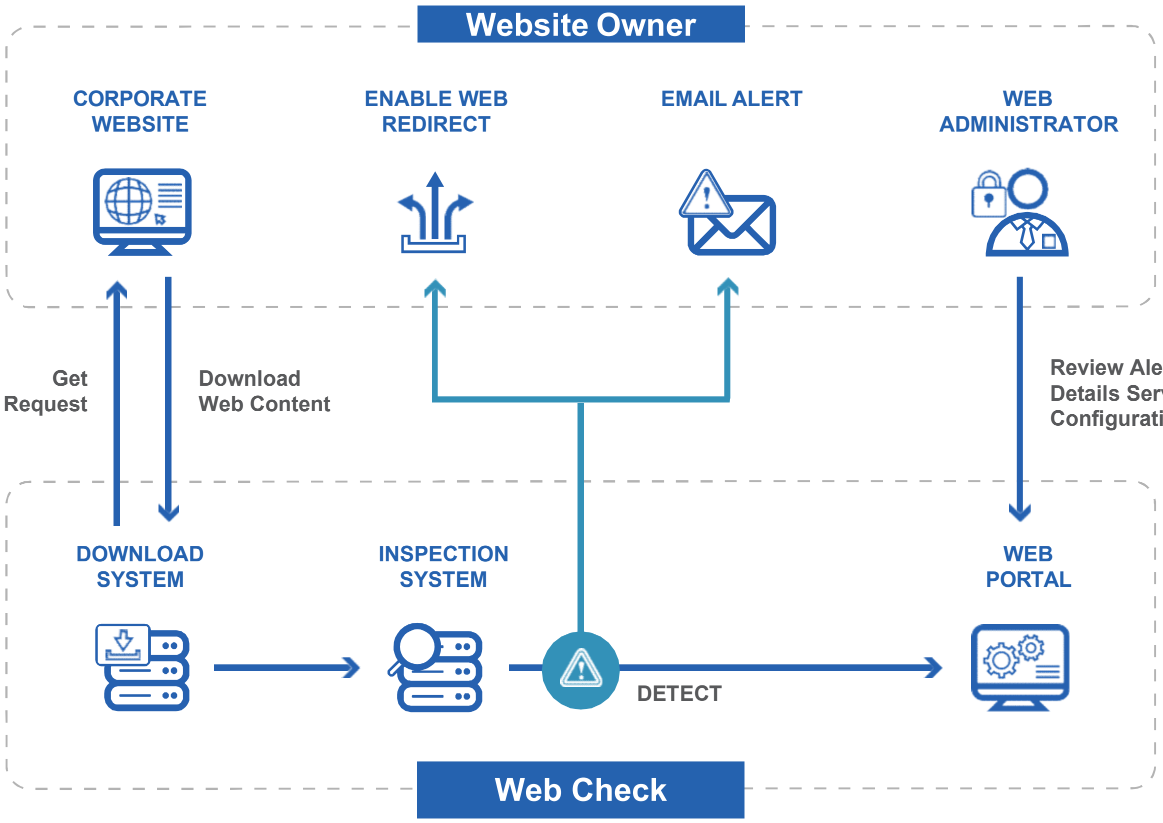
During the download phase, **GRED Web Check** analyses the entire website. It uses hyperlinks to navigate through all the pages and subsequently downloads information that needs to be inspected for malware.

After all the pages have been retrieved, the inspection phase commences. Using static analysis, **GRED Web Check** combs through all pages in order to look for malicious software. Should the application detect malware, the web portal is activated. This portal sends an alert email to the administrator and redirects any subsequent website visitors to a secure page.

Digging Deeper: Exploring the GRED Web Check Systems

GRED Web Check is an invaluable tool that enables administrators or even business owners to manage and monitor websites with ease. The beauty of this product lies with the built in systems that ensure the safety of a website from malware and other malicious software.

With that said, in order to truly grasp the importance of this product to your operation, it is time to dig deeper and explore all three systems that make **GRED Web Check** a necessity.



Download System

After registering a website onto the **GRED Web Check** database, the application proceeds with the download system.

In this phase, **GRED Web Check** scans through the site in the same fashion as a potential client. Then, it downloads all available web content including dynamic information generated from server-side scripting and database retrievals. It is also during this stage that the application browses through HTML pages, URL links, and most importantly, EXE and ZIP links that can introduce malware to the visitors of the website.

The download system is done continuously in order to ensure that all web content is accounted for at all times. Following this phase, **GRED Web Check** proceeds with Inspection.

Inspection System

The Inspection system is responsible for sifting through the data collected by the download system and locating malicious software introduced by hackers lurking within the website.

It is in this stage that **GRED Web Check** DBD triggers on scripts that can launch and wreak havoc on a site. It uses a large whitelist database to distinguish known safe scripts from unknown scripts that cannot be trusted. The database allows **GRED Web Check** to identify scripts before it causes severe and irreparable damage.

GRED Web Check conducts the inspection stage through static analysis. The application favors this type of inspection for a number of reasons:

Static versus Dynamic

Traditionally, there are two methods used in malware detection - static analysis and dynamic analysis. Both are widely used and carry their own set of advantages and disadvantages.

Dynamic analysis involves running the malware and observing its behavior to determine its purpose, the severity of the damage that it can create, and the actions that need to be taken in order to circumvent the attack. While this type of analysis is able to detect a wider range of malware, it is also notoriously slow.

Static analysis, on the other hand, identifies malware without the need to run the script. It does so by locating the unique signature that every malware binary code has. It is significantly faster in detecting common malware that plagues most websites. It is the more efficient means in locating and inspecting malicious software.

Inspection System Target List

GRED Web Check uses static analysis in order to detect the different malware present on a website. Because the application runs a signature-based inspection, there are common types of malware that **GRED Web Check** is an expert in detecting. These types of threats and scenarios include but aren't limited to:

- DBD download trigger JavaScript and iframe
- Hostile JavaScript
- Script execution from untrusted domains
- Suspicious EXE and ZIP files
- Website Content Defacement
- Phishing
- Bogusware
- Google Search Engine Blacklist
- Law Enforcement Blacklist
- Government-issued Blacklist

Web Portal

When the Inspection System detects malware on a website, the Web Portal takes over and takes action against the identified threat. The Web Portal process is two-fold. It first gathers enough data in order to create a summary report detailing the threat. It explains the detail of the attack as well as the specific script injected on to the afflicted website.

Aside from the summary report on the Web Portal, an email is also sent to the administrator to alert them of the current situation.

The Web Portal system is an integral part of **GRED Web Check**. It allows website owners to act upon threats within minutes of its detection. The application minimizes the impact of the malware on the website and its visitors.

Redirect Feature

A quick and surefire way to lose a potential customer is through an unmaintained and unsafe website. With traditional means of malware detection, malicious software goes unchecked until a website visitor informs the administrator about the presence of malware. Not only does this sully the company’s reputation, but it also exposes potential clients and their data to serious security risks.

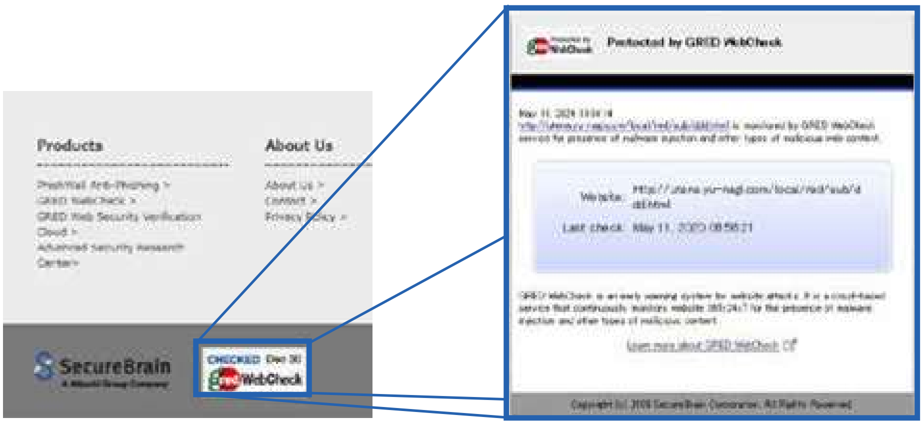
One of the best features of **GRED Web Check** is the Redirect function. In the case that the inspection system detects malware on a website, the application automatically redirects subsequent visitors to a safe version of the web page. This prevents the malware from reaching more victims in such a case wherein the administrator can’t get to the problem right away.

The Redirect function only requires the website manager to install a small JavaScript on the website. Once installed, redirection can already be enabled and disabled through the web portal.

Seal Feature

GRED Web Check provides an unmatched level of security to a website. It also allows users to display a security seal on their website. This provides visitors and potential clients the assurance that the website they are visiting is safe, well-maintained, and free from malware.

Visitors can click through the seal. This displays the security rating of the web page as well as the date of the most recent inspection. Without a doubt, **GRED Web Check** is a must for companies that are looking to grow their reputation online.


Products
PhishWall Anti-Phishing >
GRED WebCheck >
GRED Web Security Verification Cloud >
Advanced Security Research Center>
About Us
About Us >
Contact >
Privacy Policy >
SecureBrain
A Hitachi Group Company
CHECKED Dec 30
WebCheck
Protected by GRED WebCheck

May 11, 2020 [illegible]
[illegible] is monitored by GRED WebCheck service for presence of malware injection and other types of malicious web content.

Website: [illegible]
Last check: May 11, 2020 08:58:21

GRED WebCheck is an early warning system for website attacks. It is a cloud-based service that continuously monitors website 365/24/7 for the presence of malware injection and other types of malicious content.

Learn more about GRED WebCheck

Copyright (c) 2020 SecureBrain Corporation. All Rights Reserved.

Additional GRED Web Check Features

Aside from **GRED Web Check**'s world-class core functions, the system also offers additional features that fortify a website against the most sophisticated malware.

Cross-domain Script Detection

GRED Web Check is able to identify external scripts that are inserted on a legitimate page before it causes severe damage. These attacks are particularly worrisome because it targets visitors and uses real webpages as a vehicle to execute the malicious script.

Defacement Detection

Website defacement occurs when hackers change, remove, or add content on a website without the knowledge of the owner. This type of threat not only damages the reputation of a brand but it also exposes the website as unsecure.

GRED Web Check is able to detect visual changes on the top page of a website. The application subsequently notifies the administrator in the case of anattack.

Monitor Specific Tag Attribute Changes

Aside from visual content, **GRED Web Check** is also equipped to monitor changes in not only the website's JavaScript code but also changes in domain links within the HTML content. This includes edits on the anchor tag, img tag, etc.

Simplified Vulnerability Assessment

GRED Web Check can streamline a website's vulnerability assessment. This application is able to run conduct a port scan assessment as well as perform Joomla assessment using joomscan.

Health Check Detection

Frequent website downtime can be instrumental in an operation losing business. **GRED Web Check** is equipped to run scans and confirm the availability of all registered pages.

Broken Link Detection

Ensuring that a website is devoid of broken links is important in maintaining search engine rankings. Search engines like google penalize pages for incorporating links that don't exist. **GRED Web Check** not only detects broken links but it also itemizes the links that need to be replaced or edited.

Executable File Check

For example, Windows executable files or .exe files are often used as delivery systems for malware. **GRED Web Check** inspects these files to check for the presence of malicious software.

GRED Web Check: Distribution and Pricing

GRED Web Check is brought to you by Japan's leading security software provider, Securebrain. This pricing for the application varies depending on inspection frequency and the number of web pages to be inspected and maintained.

There is a package that fits the budget and requirements of every scale of operations from small to medium businesses to multinational enterprises.

At present, volume discount and OEM is available. OEM partners are able to rebrand GRED Web Check's Web Portal with their own logo on the header and the footer. As of 2021, over 30 companies have opted to OEM **GRED Web Check**.

To learn more about **GRED Web Check** pricing and functions, do visit https://www.securebrain.co.jp/eng/website-scanner/ for more information and a two-week trial of the service.

GRED Web Check for Your Business

There are various ways hackers can infiltrate a website. From content defacement to information theft, the consequences of leaving a website unprotected are serious and severe. It can be the difference between gaining customers or losing loyal clientele. Needless to say, choosing an early warning detection system like the GRED Web Check for your operations is an investment worth making.

Protect Your Company's Image

Your website is a reflection of the kind of company that you run. It is your operations online business card. Needless to say, a website riddled with malware puts out a statement that your business is not to be trusted.

With that said, **GRED Web Check** ensures that all website visitors are protected from various types of common malware. The seal feature provides them the peace of mind that every time they click-through your website, their systems are protected. In business, there are very few things as important as your reputation. **GRED Web Check** ensures that the reputation that you built remains intact.

Avoid Expensive Repairs

It doesn't take a computer expert to understand the fact that the longer a malware lurks on a website, the more damage it creates for the website owner and its visitors.

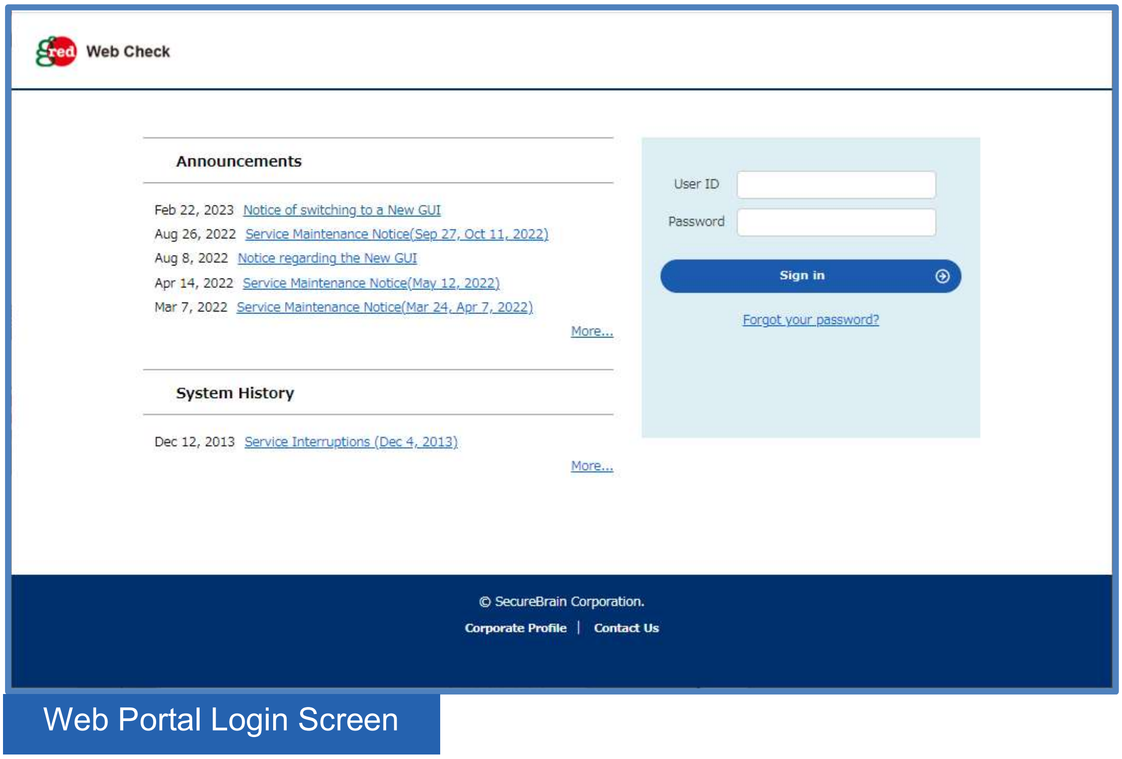
Needless to say, early detection is valuable. Programs like **GRED Web Check** ensure that casualties are kept to a minimum. Moreover, the application's redirect function prevents subsequent malware infections and contains the issue.

Opting to subscribe to this security service prevents you from spending thousands of dollars on website repairs.

Secure your Customer's Loyalty and Patronage

With a formidable and trustworthy website, **GRED Web Check** allows you to expand your client base online without the risk of malware infection and spread. It provides you an avenue to reach more opportunities and close more deals.

Appendix:
Screenshots of Web Portal



Announcements

Feb 22, 2023 Notice of switching to a New GUI
Aug 26, 2022 Service Maintenance Notice(Sep 27, Oct 11, 2022)
Aug 8, 2022 Notice regarding the New GUI
Apr 14, 2022 Service Maintenance Notice(May 12, 2022)
Mar 7, 2022 Service Maintenance Notice(Mar 24, Apr 7, 2022)
More...

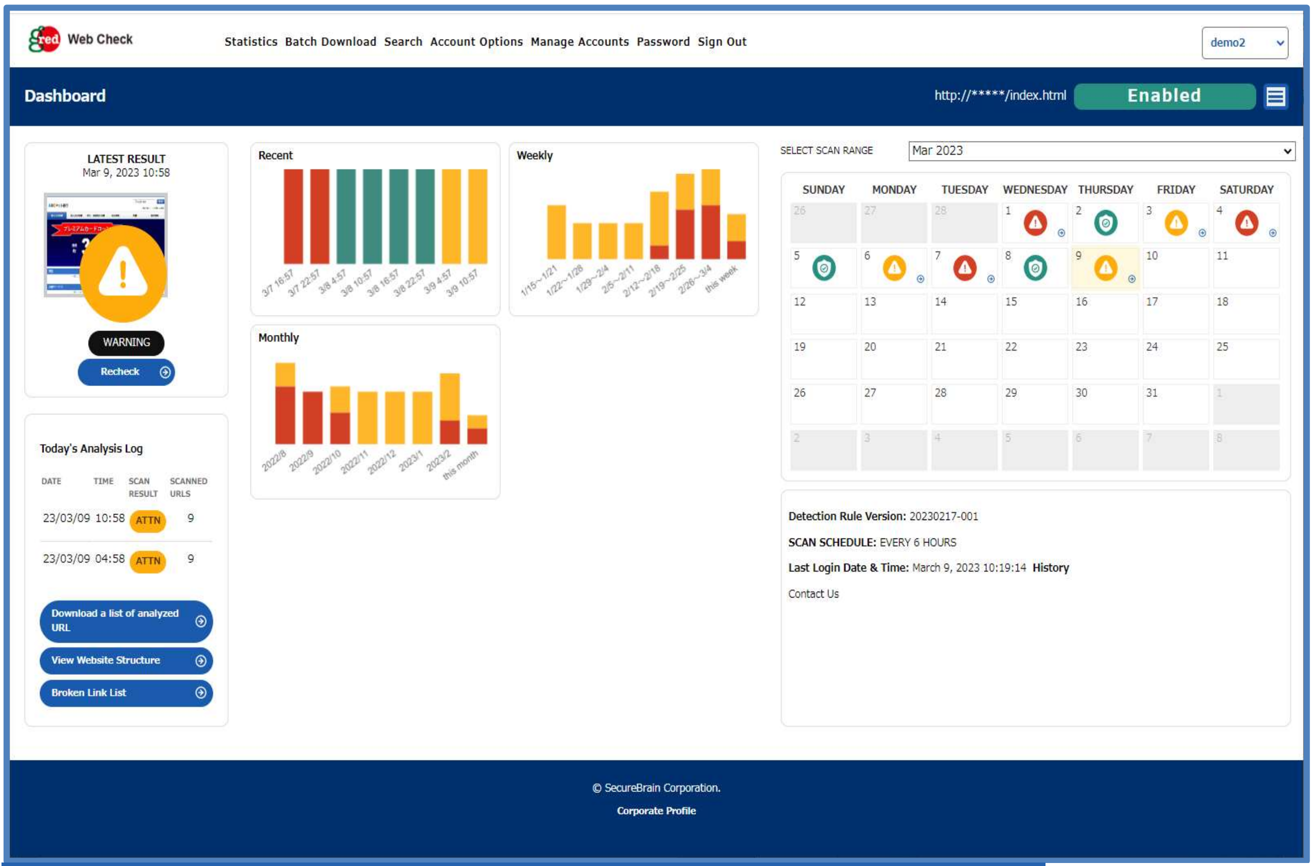
System History

Dec 12, 2013 Service Interruptions (Dec 4, 2013)
More...

User ID
Password

© SecureBrain Corporation.
Corporate Profile | Contact Us

Web Portal Login Screen



Today's Analysis Log

DATE	TIME	SCAN RESULT	SCANNED URLS
23/03/09	10:58	ATTN	9
23/03/09	04:58	ATTN	9

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
26	27	28	1 ⚠	2 ✓	3 ⚠	4 ⚠
5 ✓	6 ⚠	7 ⚠	8 ✓	9 ⚠	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1
2	3	4	5	6	7	8

Detection Rule Version: 20230217-001

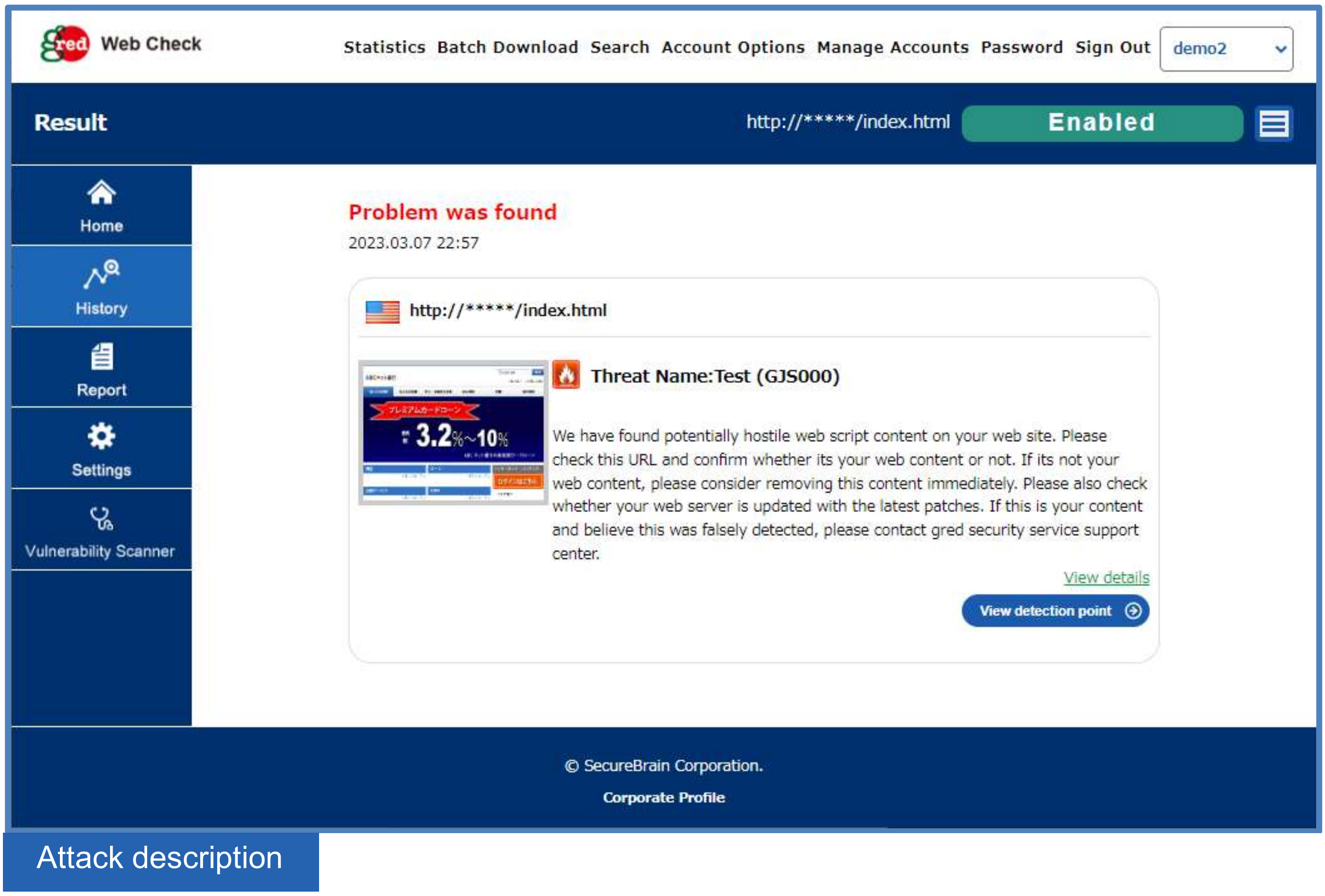
SCAN SCHEDULE: EVERY 6 HOURS

Last Login Date & Time: March 9, 2023 10:19:14 **History**

Contact Us

© SecureBrain Corporation.
Corporate Profile

Confirm details on web portal
Calendar will give you quick glance at check results. Red date mean ALERT!



Problem was found

2023.03.07 22:57

http://*****/index.html

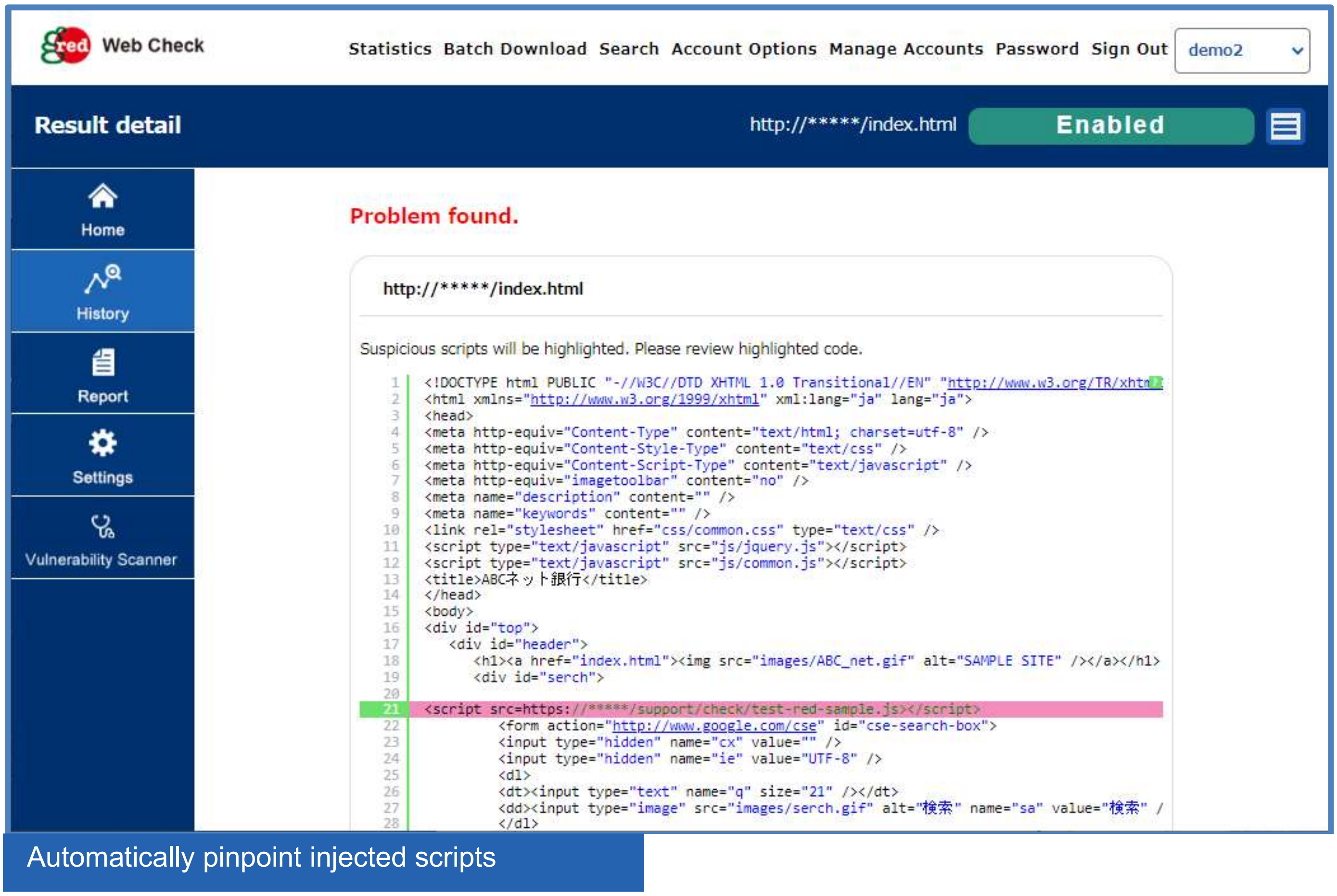
Threat Name:Test (GJS000)

We have found potentially hostile web script content on your web site. Please check this URL and confirm whether its your web content or not. If its not your web content, please consider removing this content immediately. Please also check whether your web server is updated with the latest patches. If this is your content and believe this was falsely detected, please contact gred security service support center.

© SecureBrain Corporation.

Corporate Profile

Attack description



Problem found.

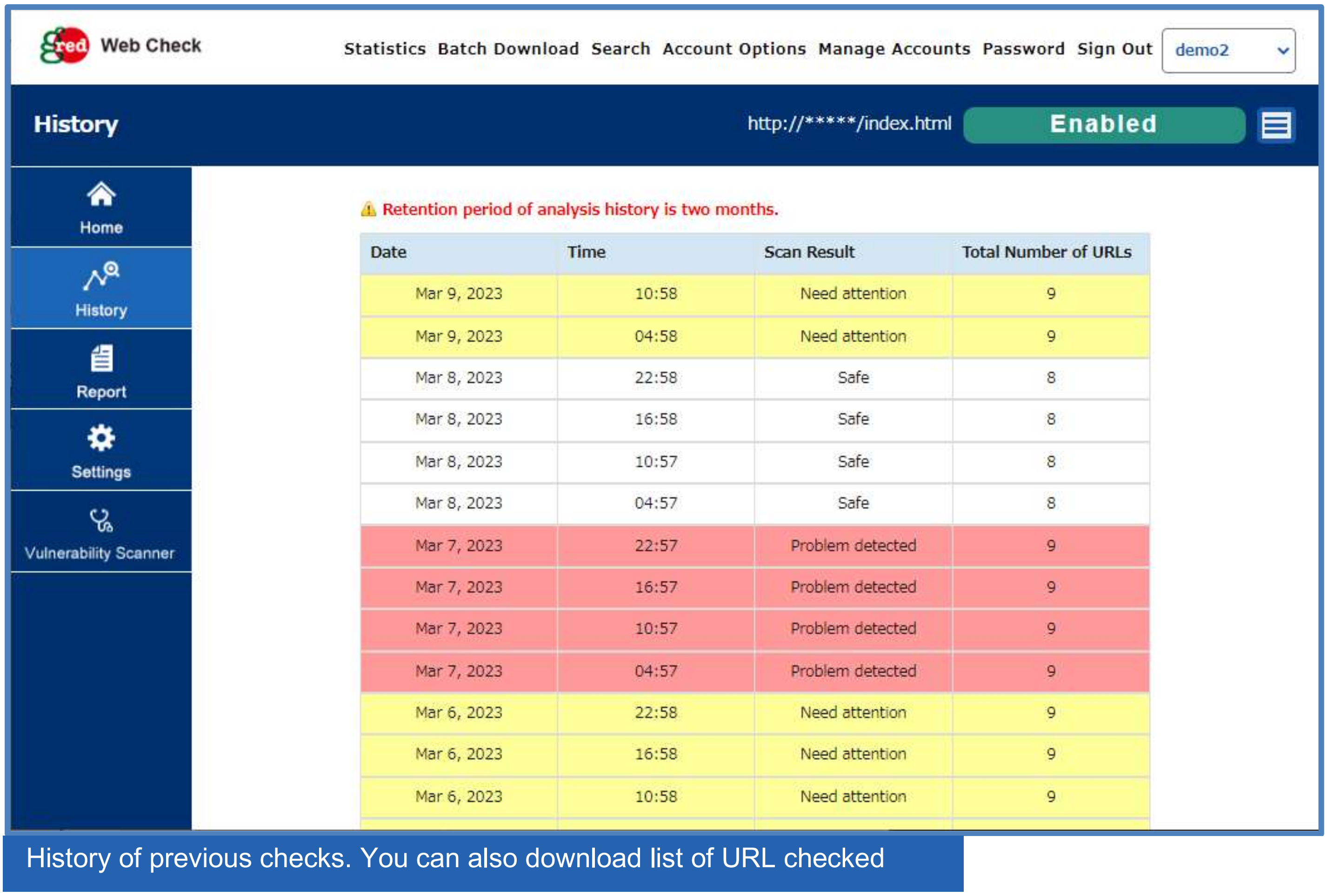
http://*****/index.html

Suspicious scripts will be highlighted. Please review highlighted code.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtm
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="ja" lang="ja">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta http-equiv="Content-Style-Type" content="text/css" />
<meta http-equiv="Content-Script-Type" content="text/javascript" />
<meta http-equiv="imagetoolbar" content="no" />
<meta name="description" content="" />
<meta name="keywords" content="" />
<link rel="stylesheet" href="css/common.css" type="text/css" />
<script type="text/javascript" src="js/jquery.js"></script>
<script type="text/javascript" src="js/common.js"></script>
<title>ABCネット銀行</title>
</head>
<body>
<div id="top">
   <div id="header">
      <h1><a href="index.html"><img src="images/ABC_net.gif" alt="SAMPLE SITE" /></a></h1>
      <div id="serch">

<script src=https://*****/support/check/test-red-sample.js></script>
         <form action="http://www.google.com/cse" id="cse-search-box">
         <input type="hidden" name="cx" value="" />
         <input type="hidden" name="ie" value="UTF-8" />
         <dl>
         <dt><input type="text" name="q" size="21" /></dt>
         <dd><input type="image" src="images/serch.gif" alt="検索" name="sa" value="検索" /
         </dl>
```

Automatically pinpoint injected scripts



⚠ Retention period of analysis history is two months.

Date	Time	Scan Result	Total Number of URLs
Mar 9, 2023	10:58	Need attention	9
Mar 9, 2023	04:58	Need attention	9
Mar 8, 2023	22:58	Safe	8
Mar 8, 2023	16:58	Safe	8
Mar 8, 2023	10:57	Safe	8
Mar 8, 2023	04:57	Safe	8
Mar 7, 2023	22:57	Problem detected	9
Mar 7, 2023	16:57	Problem detected	9
Mar 7, 2023	10:57	Problem detected	9
Mar 7, 2023	04:57	Problem detected	9
Mar 6, 2023	22:58	Need attention	9
Mar 6, 2023	16:58	Need attention	9
Mar 6, 2023	10:58	Need attention	9

History of previous checks. You can also download list of URL checked

GRED Web Check by Securebrain

With almost two decades of experience, Securebrain is considered as Japan’s leading security software provider. Based in Tokyo, our company aims to provide a wide array of security options forevery type of business within and outside of Japan.

SecureBrain runs its own research center in order to ensure that we are providing the leading technologies in website malware detection and protection. Our team of researchers is dedicated to identifying new online website security risks and developing solutions to current and future threats.

We have secured the business of several multinational companies as well as government contracts that are specifically geared towards cybercrime and security.

SecureBrain
A Hitachi Group Company

https://www.securebrain.co.jp/eng