



Department of
Bachelor of Computer Applications

Information Security & Mobile Applications – Section <A>

Network Security
Activity #02

Network Security Assessment Tools

[Sucuri, Qualys, UpGuard, Mozilla Observatory, ImmuniWeb]

Subject Code: 20BCAIS4C02

Class: IInd Year IInd Semester

Submitted On:

28-03-2022

By:

Suman Garai

20BCAR0246

Faculty In-Charge:

Dr. Mahesh V

Assistant Professor

Signature

Signature



JAIN
DEEMED-TO-BE UNIVERSITY

SCHOOL OF
COMPUTER
SCIENCE AND IT

Evaluation Criteria

Sr. No.	Criteria / Parameters	Total Marks	Marks Obtained
1	On-time submission Certification	05	
2	Certification of Completion	05	
3	Report (with Assessment Screenshots test attempted)	05	
4	Conclusion [Minimum one page without any kind of plagiarism]	10	
	TOTAL	25	
	CONVERT	10	



JAIN
DEEMED-TO-BE UNIVERSITY

SCHOOL OF
COMPUTER
SCIENCE AND IT

Table of Contents

Sl. No.	Title	Page No.
	Sucuri SiteCheck	
1	Introduction to the Tool Screenshots Conclusion	1 - 3
	Qualys SSL Tool	
2	Introduction to the Tool Screenshots Conclusion	4-6
	UpGuard	
3	Introduction to the Tool Screenshots Conclusion	7-9
	Observatory by Mozilla	
4	Introduction to the Tool Screenshots Conclusion	10-12
	ImmuniWeb	
5	Introduction to the Tool Screenshots Conclusion	13-15

Introduction to the Tool & Company

Sucuri is a managed security service provider for websites. Their cloud-based tools provide complete website security solution, including performance optimization via a CDN, mitigation of external attacks like vulnerability exploits and DDoS attacks, and professional response in the event of security incident. The team provides 24/7/365 customer service with a 97% satisfaction rate, and a median response time of 4 hours.

They've offered holistic website security solutions since 2008 including malware removal, malware monitoring and website protection services. Their Site Check website security monitor is used by thousands of website owners every month to monitor their websites for malware, blacklist status and other security issues and their Cloud Proxy Firewall safeguards sites and those who visit them from attacks of all kinds. Their passion is growing awareness of website security issues and stamping out web-based attacks. Join them at <https://sucuri.net>

What Site Check looks for on your site

- **Scan Website for Malware & Viruses**
Detect malicious code and infected file locations by scanning your external website source code.
- **Check Website Blacklist Status**
See if your website is blacklisted by website security authorities such as Google, PhishTank, etc.
- **Find Out-of-Date Software & Plugins**
Identify if your website is running an outdated CMS or vulnerable plugins and extensions.
- **Detect Website Security Issues**
Check your website for security anomalies, configuration issues, and security recommendations.

Screenshots

The screenshot displays the Sucuri website security scan interface. At the top, the Sucuri logo is on the left, and navigation links for 'Website Monitoring', 'Website Firewall', 'Website Backups', 'Knowledgebase', and 'Support' are on the right. The main header shows the scanned URL 'testhtml5.vulnweb.com'.

The scan results are presented in a clean, modern layout. Two green checkmarks indicate 'No Malware Found' and 'Site is not Blacklisted'. Below these, a table lists technical details: IP address (44.228.249.3), Hosting (Amazon AWS), Running on (Nginx 1.19.0), CMS (Unknown), and Powered by (Unknown). A 'More Details' link is provided.

A security risk level bar shows 'Medium Security Risk' on a scale from Minimal to Critical. Below this, a message states that the automated scan did not detect malware, but offers a link to sign up for a complete scan and manual audit.

The 'TLS Recommendations' section highlights that a password input field was detected on an unencrypted HTTP page, advising the use of HTTPS. It also notes that the HTTPS version of the website is not accessible due to a timeout.

Two side-by-side sections provide further details: 'Website Malware & Security' lists four checks (No malware, No injected spam, No defacements, No internal server errors) all marked as 'Low Risk'. 'Website Blacklist Status' lists six checks (Domain clean by Google Safe Browsing, McAfee, Sucuri Labs, ESET, PhishTank, Yandex, Opera) all marked as clean.

Below these are two boxes for 'Website Monitoring' and 'Website Firewall', both showing 'Not detected' status with 'Learn More' and 'Explore Sucuri Firewall' links respectively.

The 'Hardening Improvements' section contains two sub-sections: 'Protection' and 'Security Headers'. 'Protection' notes that no website application firewall was detected and recommends installing a cloud-based WAF. 'Security Headers' lists several missing security headers and provides instructions on how to add them, including Content-Security-Policy directives and default server banners.

At the bottom, a status message indicates the scan was performed 6 minutes ago and offers a link to force a re-scan. A search bar with the placeholder 'Scan another website...' and a 'Scan Website' button is located at the very bottom.

The footer contains copyright information for 2019 Sucuri Inc., links to Terms, Privacy, and a Help icon, and a 'SITECHECK' logo.

Conclusion

In this course, we took a look at Sucuri, where if we enter a URL like example.com and the Sucuri SiteCheck scanner will check the website for known malware, viruses, blacklisting status, website errors, out-of-date software, and malicious code.

Introduction to the Tool & Company

Founded in 1999 as one of the first SaaS security companies, Qualys has established strategic partnerships with leading cloud providers like Amazon Web Services, Microsoft Azure and the Google Cloud Platform, and managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, DXC Technology, Fujitsu, HCL Technologies, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA).

"SSL Labs is a collection of documents, tools and thoughts related to SSL. It's an attempt to better understand how SSL is deployed, and an attempt to make it better. I hope that, in time, SSL Labs will grow into a forum where SSL will be discussed and improved. SSL Labs is a non-commercial research effort, and we welcome participation from any individual and organization interested in SSL."

-- Ivan Ristić, Qualys

[illegible]

Conclusion

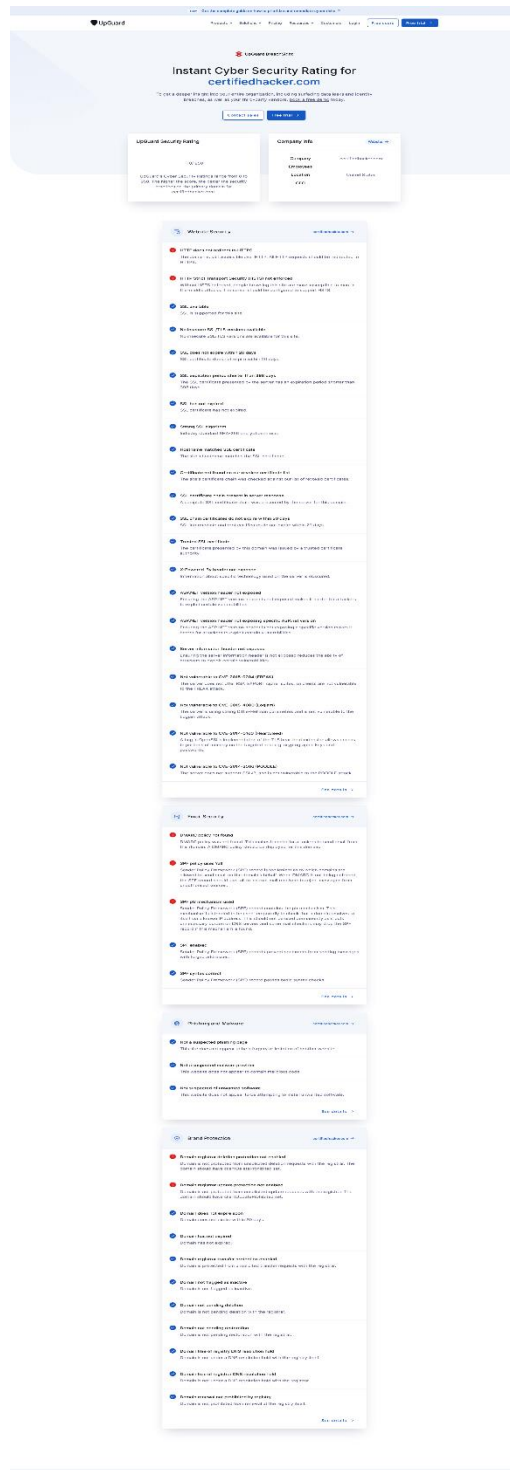
In this course, we took a look at Sucuri, which is a free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. Please note that the information you submit here is used only to provide you the service. They don't use the domain names or the test results, and we never will.

Introduction to the Tool & Company

UpGuard is a complete third-party risk and attack surface management platform. Our security ratings engine monitors millions of companies every day. UpGuard builds the most powerful and flexible tools for cybersecurity. Whether you're looking to prevent third-party data breaches, continuously monitor your vendors, or understand your attack surface, UpGuard's meticulously designed platform, and unmatched functionality helps you protect your most sensitive data. Hundreds of the world's most data-conscious companies are scaling faster and more securely by relying on UpGuard's platform.

UpGuard scans billions of digital assets daily across thousands of vectors. Data leak detection, vulnerability scanning and identity breach detection are just some of the advanced capabilities offered by the UpGuard platform.

Screenshots



Conclusion

In this test, we took a look at UpGuard, which is a free online service performs a deep analysis to prevent data breaches, discover leaked credentials, and protect customer data on the public Internet. It ensures Security and compliance at the core through Comprehensive security and Rigorous compliance

Introduction to the Tool & Company

Our The Mozilla HTTP Observatory is a set of tools to analyse your website and inform you if you are utilizing the many available methods to secure it. Observatory is a tool that is geared towards informing website owners of best practices for securing their sites, covering everything from personal blogs to eCommerce.

The tool uses a scoring system to determine how vulnerable or how well implemented security is on your website.


It is split into three projects:

- http-observatory - scanner/grader
- observatory-cli - command line interface
- http-observatory-website - web interface
-

Scanning sites with the HTTP Observatory can be scanned using:


- observatory.mozilla.org - the online interface
- observatory-cli - the official node.js command line interface
- java-http-observatory-api - a third party java library and command line interface

Screenshots


[Home](#)
[FAQ](#)
[Statistics](#)
[About](#)

[HTTP Observatory](#)
[TLS Observatory](#)
[SSH Observatory](#)
[Third-party Tests](#)

Scan Summary



Host:	www.bhadrinar.com
Scan ID #:	25432838 (unlinked)
Start Time:	March 28, 2022 3:45 PM
Duration:	3 seconds
Score:	30/100
Tests Passed:	7/11

Recommendation

[Initiate Rescan](#)

Wondering where to start?

Adding HTTPS protects your site's visitors from tracking, malware, and injected advertising.

Many services providers and certificate authorities now provide free HTTPS and digital certificates to make this as painless as possible!

- [Mozilla TLS Guidelines](#)
- [Mozilla TLS Configuration Generator](#)


Once you've successfully completed your change, click [Initiate Rescan](#) for the next piece of advice.

Test	Pass	Score	Reason	Info
Content Security Policy	✗	-75	Content Security Policy (CSP) header not implemented	①
Cookies	✓	0	All cookies use the <code>Secure</code> flag and all session cookies use the <code>HttpOnly</code> flag	①
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) filters or headers	①
HTTP Public Key Pinning	—	0	HTTP Public Key Pinning (HPKP) header cannot be set, as site contains an invalid certificate chain (optional)	①
HTTP Strict Transport Security	✗	-70	HTTP Strict Transport Security (HSTS) header cannot be set, as site contains an invalid certificate chain	①
Redirection	✗	-70	Does not redirect to an HTTPS site	①
Referrer Policy	—	0	Referrer-Policy header not implemented (optional)	①
Subresource Integrity	—	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin	①
X-Content-Type-Options	✗	-3	X-Content-Type-Options header not implemented	①
X-Frame-Options	✓	0	X-Frame-Options (XFO) header set to <code>SAMEORIGIN</code> or <code>DENY</code>	①
X-XSS-Protection	✓	0	X-XSS-Protection header set to <code>1; mode=block</code>	①

Cookies						
Name	Expires	Path	Secure	HttpOnly	SameSite	Prefixed
pleak_ext_social_login_jwt-session	Session	/	✓	✓	✗	✗

Grade History		
Date	Score	Grade
March 23, 2022 3:21 PM	30	D

[illegible]




[Home](#)
[FAQ](#)
[Statistics](#)
[About](#)

[HTTP Observatory](#)
[TLS Observatory](#)
[SSH Observatory](#)
[Third-party Tests](#)

This site uses an untrusted or invalid certificate. The following results ignore this error:

Scan Summary



Host:	www.bkdrfishar.com (43.248.68.26)
Scan ID #:	4964773
End Time:	March 28, 2022 1:43 PM
Compliance Level:	Non-compliant

Please note that non-compliance simply means that the server's configuration is either more or less strict than a pre-defined Mozilla configuration level.

Certificate Expiry: 58576622

Certificate Information	
Common name:	sd-bkusers.45 178 61 76.phk.page
Alternative Names:	sd-bkusers.45 178 61 76.phk.page
First Observed:	2022-09-23 (certificate #18078622)
Valid From:	2022-01-31
Valid To:	2022-09-01
Key:	RSA 2048 bits
Issuer:	R1
Signature Algorithm:	SHA256WithRSA

Cipher Suite	Code	Key size	AEAD	EPS	Protocols
ECDHHE-RSA-AES128-GCM-SHA256	0x0001_0x027	2048 bits	✓	✓	TLS 1.2
ECDFHE-RSA-AES128-GCM-SHA256	0x0001_0x030	2048 bits	✓	✓	TLS 1.3
DHE-RSA-AES128-GCM-SHA256	0x0001_0x033	2048 bits	✓	✓	TLS 1.3
DHE-RSA-AES256-GCM-SHA384	0x0001_0x037	2048 bits	✓	✓	TLS 1.2
ECDFHE-RSA-AES256-SHA384	0x0001_0x038	2048 bits	✗	✓	TLS 1.2
ECDFHE-RSA-AES256-SHA384	0x0001_0x039	2048 bits	✓	✓	TLS 1.3
DHE-RSA-AES256-SHA384	0x0001_0x040	2048 bits	✓	✓	TLS 1.2
DHE-RSA-AES256-SHA384	0x0001_0x043	2048 bits	✗	✓	TLS 1.3
ECDFHE-RSA-AES128-SHA	0x0001_0x022	2048 bits	✗	✓	TLS 1.0, TLS 1.1, TLS 1.2
ECDFHE-RSA-AES256-SHA	0x0001_0x024	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
DHE-RSA-AES128-SHA	0x0001_0x035	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
DHE-RSA-AES256-SHA	0x0001_0x039	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
ECDFHE-RSA-CAMELLIA128-SHA256	0x0001_0x077	2048 bits	✗	✓	TLS 1.2
ECDFHE-RSA-CAMELLIA128-SHA256	0x0001_0x076	2048 bits	✗	✓	TLS 1.3
DHE-RSA-CAMELLIA128-SHA256	0x0001_0x074	2048 bits	✗	✓	TLS 1.2
DHE-RSA-CAMELLIA256-SHA384	0x0001_0x085	2048 bits	✗	✓	TLS 1.2
DHE-RSA-CAMELLIA256-SHA	0x0001_0x088	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
DHE-RSA-CAMELLIA256-SHA	0x0001_0x045	2048 bits	✗	✓	TLS 1.2, TLS 1.1, TLS 1.0
RSA-AES128-GCM-SHA256	0x0001_0x026	2048 bits	✓	✗	TLS 1.2
RSA-AES256-GCM-SHA384	0x0001_0x029	2048 bits	✓	✗	TLS 1.2
RSA-AES128-SHA256	0x0001_0x02C	2048 bits	✗	✗	TLS 1.3
RSA-AES256-SHA256	0x0001_0x032	2048 bits	✗	✗	TLS 1.2
RSA-AES128-SHA	0x0001_0x025	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0
RSA-AES256-SHA	0x0001_0x028	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0
RSA-CAMELLIA128-SHA256	0x0001_0x078	2048 bits	✗	✗	TLS 1.2
RSA-CAMELLIA128-SHA256	0x0001_0x075	2048 bits	✗	✗	TLS 1.3
RSA-CAMELLIA256-SHA	0x0001_0x086	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0
RSA-CAMELLIA256-SHA	0x0001_0x043	2048 bits	✗	✗	TLS 1.2, TLS 1.1, TLS 1.0

Miscellaneous Information	
CAA Record:	No (?)
Cipher Preference:	Server selects preferred cipher (?)
Compatible Clients:	Android 3.0-7, Apple ATG 6, Baidu Jan 7013, BingBot Feb 7013, BingPreview Feb 7013, Chrome 72, Fido 19, Firefox 101, Googlebot Oct 2013, IE 11, JIRA 6013, Openbot 0.9.80, Opera 12.10, Safari 5, Tor 1.0.10, Yahoo Slurp Oct 2012, YandexBot May 2014
OCSP Stapling:	No (?)

Suggestions

Take a look at the [Mozilla "Modern" TLS configuration](#); it provides an extremely high level of security and performance and is compatible with all clients released in the last couple years. It is not recommended for general purpose websites that may need to service older clients such as Android 4.x, Internet Explorer 10, or Java 6.x.

Still want secure website, but need compatibility with those older clients?

No problem! The Mozilla "Intermediate" TLS configuration may be just right for you! It provides the similar level of security to the "Modern" configuration when used with current clients, but still supports older versions of web browsers and tools.

Please note that these suggestions may not be appropriate for your particular usage requirements! If they do sound like something you'd like assistance with, then [hear on board](#)!

Teleport me to Mozilla's configuration generator!

Conclusion

In this test, we took a look at Observatory by Mozilla, which is a free online service performs a deep analysis of website vulnerabilities. The tool also scans and rates the implementation of TLS on the website. It will check the certificate information and cipher suites used. While Observatory's TLS scan is not as robust as the Qualys SSL Labs SSL Server Test, it does integrate this test as a third-party scanner, along with other tools. After correctly configuring the security settings on your website, we will get a result. By utilizing tools like Mozilla Observatory, you can gain some level of assurance that your site's information is safe, but it's important to ensure that you are regularly monitoring your security and keeping your systems up to date to address any new concerns that arise.

Introduction to the Tool & Company

Our The ImmuniWeb® AI Platform helps enterprise customers from over 50 countries to test, secure and protect their applications, cloud and infrastructure, reduce supply chain attacks, prevent data breaches and maintain compliance requirements. ImmuniWeb® AI Platform leverages award-winning AI and Machine Learning technology for acceleration and intelligent automation of Attack Surface Management and Dark Web Monitoring. The data is later leveraged for a threat-aware and risk-based Application Penetration Testing for web, mobile, and API security testing. ImmuniWeb is the only company that offers a contractual zero false-positives SLA with a money-back guarantee. ImmuniWeb's AI technology is a recipient of numerous awards and recognitions, including Gartner Cool Vendor, IDC Innovator, and the winner of "SC Award Europe" in the "Best Usage of Machine Learning and AI" category. ImmuniWeb® Community Edition runs over 100,000 daily tests, being one of the largest application security communities. ImmuniWeb SA is an ISO 27001 certified and CREST accredited company.

The Website Security Test is a free online tool to perform web security and privacy tests:

- Non-intrusive GDPR compliance check related to web application security.
- Non-intrusive PCI DSS compliance check related to web application security.
- Analysis of CMS and its components for outdated versions and publicly-known vulnerabilities.
- Analysis of HTTP methods that may put web server, web application or website visitors at risk.
- Detailed analysis (syntax, validity, trustworthiness) of HTTP security headers:
 - Server
 - Strict-Transport-Security (also known as HSTS)
 - X-Frame-Options
 - Content-Security-Policy (also known as CSP)
 - Access-Control-Allow-Origin
 - Content-Security-Policy-Report-Only
 - Referrer-Policy
 - Permissions-Policy
- Analysis of altered, and thus potentially malicious, JS libraries.
- Analysis of ViewState for misconfigurations and security weaknesses.
- Analysis of web application cookies for security flags.
- Detection of domain's presence in various Blacklists.
- Detection of Cryptojacking within JS code.
- Detection of WAF presence.

Screenshots

The screenshot displays the ImmuniWeb website security test results for the domain **google-gruyere.appspot.com**. The interface is clean and professional, with a blue header and a white main content area. The top navigation bar includes links for 'AI Platform', 'Pricing', 'Community Edition', 'Compliance', 'Company', and 'Partners'. The main heading is 'Website Security Test of google-gruyere.appspot.com'. Below this, a summary section shows the test results: '128 Tests Running' and '71,143 Tests in 24 Hours'. A 'Your final score' section displays a large 'C+' grade. The 'Discovered Subdomains' section lists several subdomains, including 'google-gruyere.appspot.com', 'google-gruyere.appspot.com', and 'google-gruyere.appspot.com'. The 'Web Server Security Test' section shows details about the server, including the HTTP version (HTTP/1.1), the server signature (Google Frontend), and the WAF (No WAF detected). The 'Web Software Security Test' section shows details about the web application, including the CMS (No CMS fingerprinted on the website) and the components (No components were fingerprinted on the website). The 'GDPR Compliance Test' section shows details about the GDPR requirements, including the Privacy Policy (Privacy Policy was found on the website) and the website security (Website CMS and its components could not have been reliably fingerprinted). The 'PCI DSS Compliance Test' section shows details about the PCI DSS requirements, including the website security (Website CMS could not have been reliably fingerprinted) and the requirements (No publicly known vulnerabilities seem to be present on the website). The 'HTTP Headers Security Test' section shows details about the HTTP headers, including the missing required headers (Missing required HTTP headers) and the missing optional headers (Missing optional HTTP headers). The 'Content Security Policy Test' section shows details about the Content Security Policy, including the missing required headers (The header was not sent by the server) and the missing optional headers (The header was not sent by the server). The 'Cookies Privacy and Security Analysis' section shows details about the cookies, including the missing required headers (No cookies were sent by the web application). The 'External Content Privacy and Security Analysis' section shows details about the external content, including the missing required headers (No external content found on linked page).

Conclusion

In this test, we took a look at ImmuniWeb Community Edition, which provides a free website security and compliance monitoring with this Website Security Test. The award-winning ImmuniWeb® AI Platform helps enterprise customers from over 50 countries to test, secure and protect their applications, cloud and network infrastructure, to reduce supply chain attacks, to prevent data breaches and to maintain compliance requirements. You can add up to 3 websites for free that will be tested with the Website Security Test every 7 days. You will be notified by email about new vulnerabilities or misconfigurations. You can change or remove the hosts at any time.