

Sri Lanka Institute of Information Technology



**Sri Lanka Institute of
Information Technology**

IE2072 – WEB SECURITY

Year 2, Semester 2

(Assignment – Individual)-2023

_Journaling My Bug Bounty experiences _

Student Register Number	Student Name
IT21167096	DE ZOYSA A.S.

ACKNOWLEDGEMENT

As a second semester student at SLIIT majoring in cyber security, I (DE ZOYSA A.S.) was able to take the course Web Security. I was given the task of researching Web Audit as the subject.

I received guidance and help from several specialists in order to lead to a great conclusion. I benefited much from the information I learned during the lecture series. This appreciation is extended to Dr. Lakmal Rupasinghe, Ms. Chethana Liyanapathirana, and Ms. Tarsha. I appreciate the advice and assistance you provided so that I could complete the task with complete assurance.

My family and coworkers, who assisted and provided assistance in several ways, have my sincere gratitude.

ABSTRACT

Through bug bounty programs, businesses may crowdsource security testing to find and fix flaws. Although the idea of crowdsourcing security testing is relatively new, the fundamental origins may be found in penetration testing efforts. In the past five years, bug bounty schemes have begun to take off in the information security sector. Evaluations of both bug bounty programs and the platforms they are run on are necessary as bug bounty programs continue to spread. This study looked into the development, upkeep, and viability of bug bounty schemes. The bulk of bug bounty programs are managed by a small number of bug bounty platforms. These systems might be difficult to set up initially and keep up, but they provide many security advantages to any firm willing to use them. The results of this study finally showed that a bug reward oversight committee was required, and that there should be more public vulnerability reports. Most often, hackers taking part in bug bounty schemes are hired to find vulnerabilities. Since 2013, programs advertised on bug bounty sites like HackerOne have been responsible for the discovery of tens of thousands of vulnerabilities. As of July 2019, these platforms feature over 200 publicly listed programs. We provide the findings of an empirical research that was conducted utilizing data from two bug bounty platforms in order to comprehend the expenses and advantages of bug bounty programs for both individuals and organizations. We examine the costs and advantages of running bug bounty programs as well as the incentives offered to hackers who contribute to the discovery of vulnerabilities. The average expense of running a bug bounty program for a year is now less than the cost of hiring 2 additional software engineers.

Date	14.05.2023
Summary of the day's activities	<p>What do the terms "OWASP Top 10 Vulnerabilities" and "A Guide to OWASP Top 10 Testing" mean?</p> <p>Why are the OWASP Top 10 Vulnerabilities Important?</p> <p>What has changed in OWASP's Top 10 for 2021?</p> <p>Top 25 Security Reports by OWASP/CWE in Projects and Portfolios</p> <ul style="list-style-type: none"> • A typical resource for developers and online application security is the OWASP Top 10. It reflects a broader understanding of the most important security threats to online applications. • globally acknowledged as the initial step towards better secure code by developers. • Businesses should embrace this paper and begin the process of ensuring that the risks associated with their web applications are minimized. The best way to start transforming your organization's software development culture to one that results in more secure code is probably by using the OWASP Top 10. <p><u>Top 10 Security Risks in Web Applications</u></p> <ul style="list-style-type: none"> • Broken access control jumps up to the first spot in application A01:2021; 94% of applications were examined for broken access control in some way. More instances of Broken Access Control's 34 Common Weakness Enumerations (CWEs) than any other category were found in apps. • Sensitive Data Exposure, which was a general symptom rather than a fundamental cause, is now displaced by A02:2021-Cryptographic Failures, which jumps up one spot to #2. Here, flaws in cryptography—which frequently result in the leakage of sensitive data or system compromise—are the subject of fresh attention. • A03:2021 - Injection descends to the third place. The 33 CWEs mapped into this category had the second-highest frequency among applications, and 94% of the apps underwent some sort of injection testing. Currently, this category includes cross-site scripting. • A04:2021-Insecure Design is a brand-new category for 2021 that focuses on hazards associated with design defects. Threat modeling, safe design patterns and principles, and reference architectures should all be used more frequently if our business is to actually "move left." • A05:2021-Security Misconfiguration jumps up from #6 in the previous edition; 90% of apps were checked for misconfigurations of some kind. It's not unexpected to see this category advance given the increasing changes toward highly customizable software. This category now includes the old XML External Entities (XXE) category. • A06:2021-Vulnerable and Outdated Components, which was formerly known as Using Components with Known Vulnerabilities, is ranked #2 in the Top 10 community survey but also qualified for the list via data analysis

since there was sufficient information. This category rises from position nine in 2017 and is a well-known problem for which we struggle to test and evaluate risk. The default exploit and impact weights of 5.0 are taken into account when calculating their scores because it is the sole category without any Common Vulnerabilities and Exposures (CVEs) assigned to the included CWEs.

- Broken Authentication, which was previously A07:2021-Identification and Authentication problems, is dropping from the second spot and now contains CWEs that are primarily focused on identification problems. This category remains a crucial component of the Top
- A08:2021-Software and Data Integrity Failures is a brand-new category for 2021 that focuses on CI/CD pipelines, important data, and assumptions about software upgrades without checking integrity. One of the 10 CWEs in this category has one of the largest weighted impacts from Common Vulnerabilities and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data. 2017's insecure deserialization is now included in this broad category.
- before known as Insufficient Logging & Monitoring, A09:2021-Security Logging and Monitoring Failures is included from the industry survey (#3), rising up from #10 before. This category has been widened to encompass a wider range of failure kinds, is difficult to test for, and is underrepresented in the CVE/CVSS statistics. However, visibility, event alerting, and forensics can all be negatively impacted by failures in this area.

The OWASP Top 10: Why Is It Important?

The top 10 most significant risks to web application security are listed by OWASP Top 10 along with recommendations for how to address them. The study is based on an understanding reached by international security specialists. The severity of the vulnerabilities, the frequency of isolated security flaws, and the magnitude of their potential effects are used to assess the risks.

The report's objective is to give developers and specialists in web application security a better knowledge of the most prevalent security issues so that they may incorporate the report's conclusions into their security procedures. This can reduce the likelihood that such recognized threats will be present in their online apps.

The Top 10 list is managed by OWASP, who have done so since 2003. Every two to three years, they update the list to reflect new advances and changes in the AppSec industry. Many of the biggest companies in the world use OWASP as an internal Web application development standard, a valuable checklist, and a source of actionable information.

Auditors frequently interpret an organization's failure to handle the OWASP Top 10 as a warning that compliance standards may not be up to

par. The Top 10's incorporation into its software development life cycle (SDLC) demonstrates a broad appreciation for the finest secure development methods in the market.

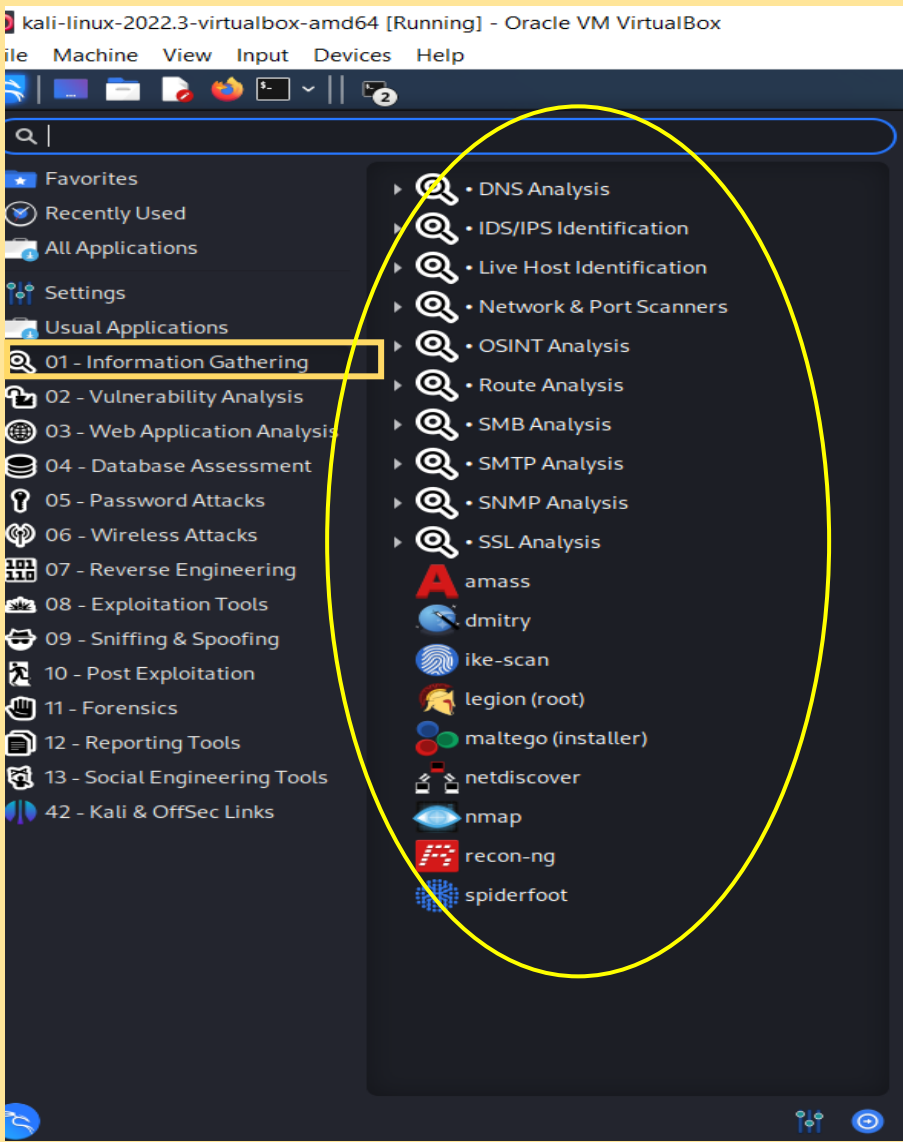

OWSAP TOP 10 vulnerabilities

OWASP Top 10

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging and Monitoring

- broken access control
Users are prevented from acting beyond the scope of their authorized permissions by access control, which enforces policy. Failures frequently result in the unauthorized exposure of information, the change or deletion of all data, or the execution of business operations outside the user's scope.
- Failures in Cryptography
Strong encryption is frequently not used to appropriately safeguard sensitive data in online apps and APIs. Such poorly protected data may be stolen or altered by attackers to commit identity theft, credit card fraud, and other crimes. Using a current (and properly set) encryption technique, sensitive data must be encrypted both at rest and while in transit.
- Injection
Untrusted data is supplied to an interpreter as part of a command or query, which can result in injection issues such as SQL, NoSQL, OS, and LDAP injection. The interpreter may be duped by the attacker's hostile data into issuing unwanted instructions or gaining unauthorized access to data.
- Unsecure Design
For the creation of safe software, pre-coding tasks are essential. Security needs and threat models should be gathered throughout the design phase of your development lifecycle, and development time should be allocated to accommodate these requirements. Your team should test the criteria and assumptions for anticipated and failure flows when the program is modified to make sure they are still correct and desired. Failure to do so will reveal important information to attackers and result in a failure to foresee new attack avenues.

	<p>What is the OWASP Top Ten?</p> <p>OWASP Top Ten is the list of the 10 most common application vulnerabilities. It also shows their risks, impacts, and countermeasures. Updated every three to four years, the latest OWASP vulnerabilities list was released September 24, 2021. Let's dive into some of the changes!</p> <p style="text-align: right;">* From the Survey</p> <p style="text-align: center;">Image credit to OWASP</p>
Challenges faced	Since it is the first day, there is no proper understanding of how to write the journal.
Tools or technique learned	<p>OWASP ZAP, Netsparker, Burpsuite</p>
Vulnerabilities discovered and explores	
References	https://www.sonarsource.com/solutions/security/owasp/ https://www.googleadservices.com/pagead/aclk?sa=L&ai=DChcSEWjayN6r_pf_AhX2mWYCHbhXDNQYABABGgJzbQ&ohost=www.google.com&cid=CAESbOD231aCC-9dy5I2PQMvRBZW2eexfOtmrL45mcDy5cRzLrbE4-2yrMs6_S5w_qtBEYaLZ0iFwTfQwIl2Qdz9UkEdL-NGpKxxV-YKfm-P8faPQHZFrpYWEYO_wHUYGLEmmmk9rNbf0y13djftw&sig=AOD64_0-dlXVOKXSxIGFPb9IylfdKNjxw&q&adurl&ved=2ahUKEwi4y9er_pf_AhWsRmwGHXvFCP8Q0Qx6BAgHEAE https://www.synopsys.com/glossary/what-is-owasp-top-10.html https://www.youtube.com/watch?v=BNg1KLjgl9I https://www.youtube.com/watch?v=3Zxuhwct9uk

Date	15.05.2023
Summary of the day's activities	<p>Learn what are the Bug Bounty methodologies and tools</p> <p>Searching subdomain with Reconnaissance hunting sub domains tools</p> <p>Port scanning and Vulnerability scanning</p>  <p><u>Reconnaissance tools</u></p> <p>🚩 Shodan - Using a number of criteria, users of the search engine Shodan may look for different kinds of servers that are online. A search engine of service banners, which are metadata that the server delivers back to the client, is another way that it has been characterized.</p> 

- Google Dorking-Google Dorking, sometimes known as Google hacking, is the use of Google search methods to break into unprotected websites or look for information that isn't displayed in open search results.

Using search strings and operators, the Google search engine operates similarly to an interpreter. For instance, you may claim that Google responds delicately to particular search terms when used with particular operators. To understand more about it, see the instruction on "what is Google Dorking" afterwards.

Enumeration tools

- Amass-

- Sublist3r-A Python program called Sublist3r is intended to list website subdomains using OSINT. It aids bug hunters and penetration testers in gathering subdomains for the site they are focusing on. Using a variety of search engines, including Google, Yahoo, Bing, Baidu, and Ask, Sublist3r lists subdomains.

```
madhusudan@kali:/opt/Sublist3r$ ./sublist3r.py

          SUBLIST3R

          # Coded By Ahmed Aboul-Ela - @aboul3la

Usage: python ./sublist3r.py [Options] use -h for help
Error: argument -d/--domain is required
madhusudan@kali:/opt/Sublist3r$
```

- Knockpy-A portable and modular Python 3 program called Knockpy was created to swiftly count the number of subdomains on a given domain using dictionary scanning and passive espionage.

```
root@kali:~/knock/knockpy# python3 knockpy.py logpac.com --no-http

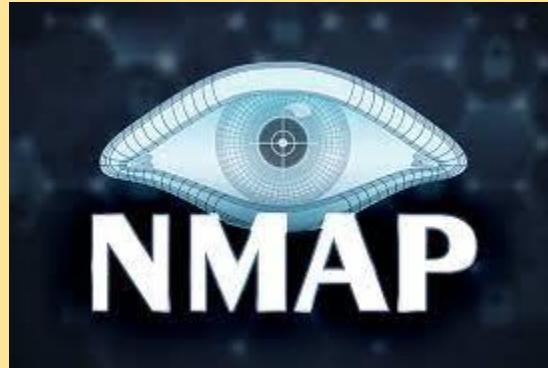
          v5.1.0
        Knockpy

local: 2022 | google: 0 | duckduckgo: 0 | virustotal: 0
Wordlist: 2022 | Target: logpac.com | Ip: 35.187.53.28
14:14:28

Ip address      Subdomain      Real hostname
-----
40.100.138.24   autediscover.logpac.com   autediscover.office.com
199.60.103.227  blog.logpac.com           group39.sites.hscoscdn30.net
[2% (ctrl-z) | DNS -> fw.logpac.com
```

Port Scanning tools

- ✚ Nmap-The network scanner Nmap was developed by Gordon Lyon. By sending packets and examining the answers, Nmap is used to identify hosts and services on a computer network. Nmap offers several tools for exploring computer networks, such as host discovery, service detection, and operating system detection.





Vulnerability scanning tools

- ✚ Burpsuite-Burp Suite is a comprehensive platform for evaluating the security of online applications. From the initial mapping and analysis of an application's attack surface through the discovery and exploitation of security flaws, its numerous tools operate in perfect harmony to assist the whole testing process. Burp provides you complete control and enables you to mix cutting-edge manual methods with cutting-edge automation to speed up, enhance, and enjoy your job.



- ✚ Nikto-Nikto is a free command-line vulnerability scanner for software that checks web servers for harmful files, CGIs, out-of-date server software, and other issues. It does both general and server-specific inspections. It also records any cookies and publishes them.

Challenges faced	<p>Some tools do not work in Kali Linux no matter how much you try</p> <p>Some tools do not understand how to work it</p> <p>Some vulnerabilities are not scanned.</p> <p>Vulnerabilities scan is not able to identify it exactly</p>
Tools or technique learned	<p>Reconnaissance : Shodan,Censys,google Dorking</p> <p>Enumeration tools loke Amass ,Sublist3r,Knockpy</p> <p>Port scanning tools:Nmap,Masscan</p> <p>Vulnerability scanning tools: Burpsuite,OWSAP ZAP,Nikto</p>
Vulnerabilities discovered and explores	
References	<p>https://owasp.org/www-project-web-security-testing-guide/v41/6-Appendix/A-Testing_Tools_Resource</p>

Date	16.05.2023
Summary of the day's activities	<p>Exploitation – Exploit databases like exploit-db or Metasploit and web exploitation tools like SqlMap or XSSer</p> <ul style="list-style-type: none"> ➤ A exploit database is what? The Exploit Database (ExploitDB) is a repository of exploits for the benefit of public security and provides information about what is included within. The ExploitDB is a very helpful tool for spotting potential holes in your network and for keeping up with recent assaults on other networks. ➤ Metasploit- The Metasploit Project is a computer security initiative that helps with penetration testing and the creation of IDS signatures while also disseminating knowledge about security flaws. Owner of it is security firm Rapid7, situated in Boston, Massachusetts.  <p><u>Web Explosion</u></p> <ul style="list-style-type: none"> ➤ SqlMap- An open source penetration testing tool called sqlmap automates the process of finding and exploiting SQL injection vulnerabilities and gaining control of database servers. A strong detection engine, numerous specialized features for the ultimate penetration tester, and a wide range of switches are included. These switches range from database fingerprinting to data retrieval from databases to accessing the underlying file system and running commands on the operating system via out-of-band connections. 

- XSSer- A framework created automatically called XSSer Cross Site "Scripter" (XSSer) is used to find, use, and report XSS flaws in web-based applications. It is a part of Kali Linux. In addition to detecting persistent, reflected, and DOM-based XSS, XSSer may scan a specified URL or Google for prospective targets based on a given query, authenticate using various methods, and carry out a variety of additional functions.

Traffic interception and manipulation:

- BurpSuite , - An integrated platform and graphical tool for doing security testing on online applications is called Burp Suite. From the initial mapping and analysis of an application's attack surface through the discovery and exploitation of security flaws, its numerous tools operate in perfect harmony to assist the whole testing process.



- OWASAP ZAP,- A free and open-source web application security tester is OWASP ZAP. It is designed to be utilized by both seasoned penetration testers and those who are new to application security. It has been granted Flagship status and is one of the most active Open Web Application Security Project initiatives.



- Fiddler- A web-debugging tool called Progress® Telerik® Fiddler Everywhere keeps track of, inspects, modifies, and logs all HTTP(S) traffic as well as sends queries to the Internet from your computer and tinkers with both incoming and outgoing data. Any browser, operating system, or platform may use this high-performance, cross-platform proxy.

	<ul style="list-style-type: none"> Learn Netsparker use.
Challenges faced	Even if they learn ,they don't understand how to work with them about exploit vulnerability
Tools or technique learned	OWASAP ZAP,Fiddler
Vulnerabilities discovered and explores	
References	https://owasp.org/www-pdf-archive/Intercept-proxies.pdf https://www.invicti.com/statics/help/netsparker-help.pdf

Date	19.05.2023
Summary of the day's activities	<p>Create Bug Bounty vulnerabilities scanning Report 1-Binance (Cryptocurrency Exchange)</p> <p>Information gathering</p>
Challenges faced	<p>Vulnerabilities are not found by nikto</p> <p>Because connection problem ,so kali linux did not loading much time</p>
Tools or technique learned	<p>Subdomains for hunting with knockpy</p> <pre> (kali㉿kali)-[~] └─\$ knockpy <domain name> </pre> <p>Open Ports Enumeration applying with nmap</p> <pre> (kali㉿kali)-[~] └─\$ sudo nmap -sS <domain name> </pre> <p>Checking for vulnerabilities using NIKTO</p> <pre> (kali㉿kali)-[~] └─\$ sudo nikto -h <domain name> </pre> <p>Scanned Vulnerabilities using Netsparker</p> <pre> (kali㉿kali)-[~] └─\$ sudo nikto -h <domain ip> </pre>
Vulnerabilities discovered and explores	<p>Weak Ciphers Enabled</p> <p>URL :https://www.casper.com/</p> <p>List of Supported Weak Ciphers :</p> <pre> TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000A) TLS_RSA_WITH_AES_128_CBC_SHA (0x002F) TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xC009) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xC00A) TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C) TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D) TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xC023) TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xC024) </pre>

	<p>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)</p> <p>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)</p> <p>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)</p> <p>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)</p> <ul style="list-style-type: none"> • Vulnerability Details <p>Netsparker detected that weak ciphers are enabled during secure communication (SSL).</p> <p>You should allow only strong ciphers on your web server to protect secure communication with your visitors.</p> <ul style="list-style-type: none"> • Impact <p>Attackers might decrypt SSL traffic between your server and your visitors.</p> <ul style="list-style-type: none"> • Actions to Take <p>For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.</p> <p>SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4</p> <p>Lighttpd:</p> <p>ssl.honor-cipher-order = "enable"</p> <p>ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"</p> <p>For Microsoft IIS, you should make some changes to the system registry.</p> <p>Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.</p> <ol style="list-style-type: none"> Click Start, click Run, type regedt32 or type regedit, and then click OK. In Registry Editor, locate the following registry key: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders Set "Enabled" DWORD to "0x0" for the following registry keys: SCHANNEL\Ciphers\DES 56/56 SCHANNEL\Ciphers\RC4 64/128 SCHANNEL\Ciphers\RC4 40/128 SCHANNEL\Ciphers\RC2 56/128 SCHANNEL\Ciphers\RC2 40/128 SCHANNEL\Ciphers\NULL SCHANNEL\Hashes\MD5 <ul style="list-style-type: none"> • Remedy <p>Configure your web server to disallow using weak ciphers.</p>
References	<p>https://hackerone.com/localtapiola?type=team</p>

Date	20.05.2023
Summary of the day's activities	Bug Bounty vulnerabilities scanning Report 2-LocalTapiola Information gathering
Challenges faced	Vulnerability found by nikto Because connection problem ,so kali linux did not loading much time
Tools or technique learned	<p>Subdomains for hunting with knockpy</p> <pre> (kali㉿kali)-[~] └─\$ knockpy <domain name> </pre> <p>Open Ports Enumeration applying with nmap</p> <pre> (kali㉿kali)-[~] └─\$ sudo nmap -sS <domain name> </pre> <p>Checking for vulnerabilities using NIKTO</p> <pre> (kali㉿kali)-[~] └─\$ sudo nikto -h <domain name> </pre> <p>Scanned Vulnerabilities using Netsparker</p> <pre> (kali㉿kali)-[~] └─\$ sudo nikto -h <domain ip> </pre>
Vulnerabilities discovered and explores	<p>Weak Ciphers Enabled</p> <p>[Possible] BREACH Attack Detected</p> <p>[Possible] Password Transmitted over Query String</p> <p>HTTP Strict Transport Security(HSTS)Errors and Warning</p> <p>Out-of-date Version (jQuery)</p> <p>Autocomplete is Enabled</p> <p>Cookie Not Marked as HttpOnly</p> <p>Cookie Not Marked as Secure</p> <p>Insecure Frame (External)</p> <p>Internal Server Error</p> <p>[Possible] Cross-site Request Forgery in Login Form</p> <p>Out-of-date Version (Moment.js)</p>

	<p>CVE-2003-1253 EDB-ID:23027 CVE-2002-1560 CVE-2000-0709 CVE-2001-1013 CVE-2002-1769 CVE-2002-2320 CVE-2002-1462 OSVDB:17660 OSVDB-59646 OSVDB-59645 OSVDB-53304</p>
References	<p>https://www.reddit.com/</p>

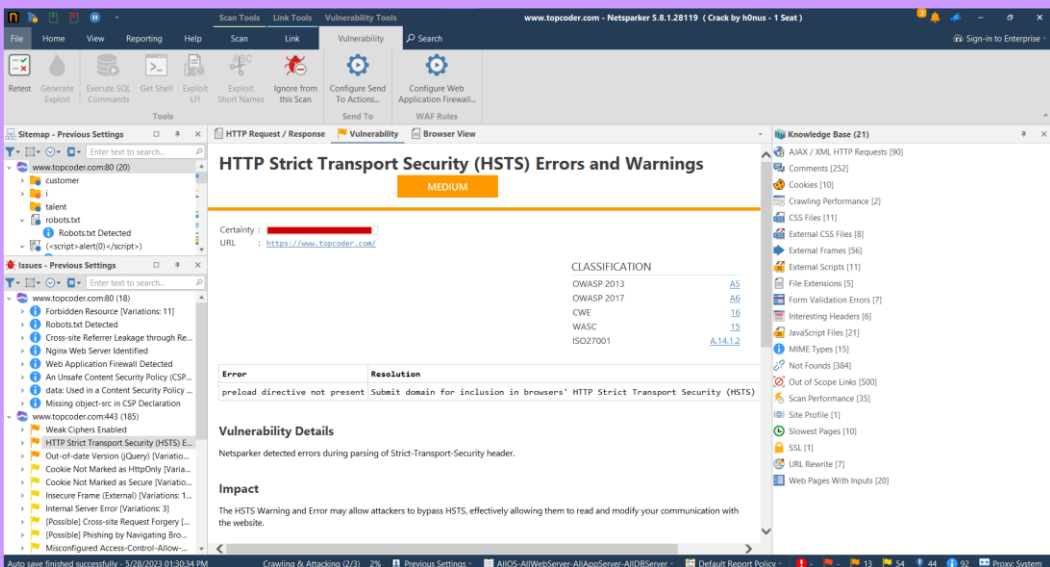
Date	21.05.2023
Summary of the day's activities	Create Bug Bounty vulnerabilities scanning Report 4-1Password.com Information gathering
Challenges faced	Vulnerability found by nikto Because connection problem ,so kali linux did not loading much time
Tools or technique learned	<p>Subdomains for hunting with knockpy</p> <pre> (kali㉿kali)-[~] └─\$ knockpy <domain name> </pre> <p>Open Ports Enumeration applying with nmap</p> <pre> (kali㉿kali)-[~] └─\$ sudo nmap -sS <domain name> </pre> <p>Checking for vulnerabilities using NIKTO</p> <pre> (kali㉿kali)-[~] └─\$ sudo nikto -h <domain name> </pre> <p>Scanned Vulnerabilities using Netsparker</p> <pre> (kali㉿kali)-[~] └─\$ sudo nikto -h <domain ip> </pre>
Vulnerabilities discovered and explores	<p>HTTP Strict Transport Security(HSTS)Errors and Warning [Possible] Cross-site Scripting</p> <p>CVE-2003-1204 OSVDB:2820 OSVDB-41361 OSVDB-3624 OSVDB-5106 OSVDB-11145 CVE-2001-1523 CVE-2003-1204 OSVDB:2820 OSVDB-2876</p>

	<p>CVE-2002-1954</p> <p>CVE-2002-1954</p> <p>OSVDB-3624</p> <p>OSVDB-41361</p> <p>CVE-2002-0931</p> <p>CVE-2001-1524</p> <ul style="list-style-type: none"> • OSVDB-3201 • CVE-2005-4838
References	<p>https://hackerone.com/crowdstrike/policy_scopes</p>

Date	22.05.2023
Summary of the day's activities	Bug Bounty vulnerabilities scanning Report 5-Casper.com Information gathering
Challenges faced	Vulnerability found by nikto Because connection problem ,so kali linux did not loading much time
Tools or technique learned	<p>Subdomains for hunting with knockpy</p> <pre> (kali㉿kali)-[~] └─\$ knockpy <domain name> </pre> <p>Open Ports Enumeration applying with nmap</p> <pre> (kali㉿kali)-[~] └─\$ sudo nmap -sS <domain name> </pre> <p>Checking for vulnerabilities using NIKTO</p> <pre> (kali㉿kali)-[~] └─\$ sudo nikto -h <domain name> </pre> <p>Scanned Vulnerabilities using Netsparker</p> <pre> (kali㉿kali)-[~] └─\$ sudo nikto -h <domain ip> </pre>
Vulnerabilities discovered and explores	<p>Weak Ciphers Enabled</p> <p>HTTP Strict Transport Security (HSTS) Policy Not Enabled</p> <p>Insecure Transportation Security Protocol Supported (TLS 1.0)</p>
References	https://hackerone.com/casper?type=team

Date	22.05.2023
Summary of the day's activities	Bug Bounty vulnerabilities scanning Report 6-Tesla Company Information gathering
Challenges faced	Vulnerability found by nikto Because connection problem ,so kali linux did not loading much time
Tools or technique learned	<p>Subdomains for hunting with knockpy</p> <pre> (kali@kali)-[~] └─\$ knockpy <domain name> Open Ports Enumeration applying with nmap (kali@kali)-[~] └─\$ sudo nmap -sS <domain name> Checking for vulnerabilities using NIKTO (kali@kali)-[~] └─\$ sudo nikto -h <domain name> Scanned Vulnerabilities using Netsparker (kali@kali)-[~] └─\$ sudo nikto -h <domain ip> </pre>
Vulnerabilities discovered and explores	Insecure HTTP Usage HTTP Strict Transport Security(HSTS)Errors and Warnings Missing X-Frame-Options Header
References	https://bugcrowd.com/tesla

Date	24.05.2023
Summary of the day's activities	Bug Bounty vulnerabilities scanning Report 7-Twitter Information gathering
Challenges faced	Vulnerability found by nikto Because connection problem ,so kali linux did not loading much time
Tools or technique learned	<p>Subdomains for hunting with knockpy</p> <pre> (kali㉿kali)-[~] └─\$ knockpy <domain name> </pre> <p>Open Ports Enumeration applying with nmap</p> <pre> (kali㉿kali)-[~] └─\$ sudo nmap -sS <domain name> </pre> <p>Checking for vulnerabilities using NIKTO</p> <pre> (kali㉿kali)-[~] └─\$ sudo nikto -h <domain name> </pre> <p>Scanned Vulnerabilities using Netsparker</p> <pre> (kali㉿kali)-[~] └─\$ sudo nikto -h <domain ip> </pre>
Vulnerabilities discovered and explores	<p>HTTP Strict Transport Security(HSTS)Errors and Warnings</p> <p>Weak Ciphers Enabled</p> <p>[Possible] BREACH Attack Detected</p> <p>[Possible] Phishing by Navigating Browser Tabs</p> <p>Missing X-Frame-Options HeaderCookie Not Marked as HttpOnly</p> <p>Cookie Not Marked as Secure</p>
References	https://hackerone.com/twitter?type=team

Date	23.05.2023												
Summary of the day's activities	Bug Bounty vulnerabilities scanning Report 8-Topcoder Information gathering												
Challenges faced	Vulnerability found by nikto Because connection problem ,so kali linux did not loading much time												
Tools or technique learned	<p>Subdomains for hunting with knockpy</p> <pre>(kali@kali)-[~] └─\$ knockpy <domain name></pre> <p>Open Ports Enumeration applying with nmap</p> <pre>(kali@kali)-[~] └─\$ sudo nmap -sS <domain name></pre> <p>Checking for vulnerabilities using NIKTO</p> <pre>(kali@kali)-[~] └─\$ sudo nikto -h <domain name></pre> <p>Scanned Vulnerabilities using Netsparker</p> <pre>(kali@kali)-[~] └─\$ sudo nikto -h <domain ip></pre>												
Vulnerabilities discovered and explores	<h3>HTTP Strict Transport Security(HSTS)Errors and Warnings</h3>  <p>The screenshot shows the Netsparker interface with the following details:</p> <ul style="list-style-type: none"> Classification Table: <table border="1"> <thead> <tr> <th>Classification</th> <th>Score</th> </tr> </thead> <tbody> <tr> <td>OWASP 2013</td> <td>A5</td> </tr> <tr> <td>OWASP 2017</td> <td>A6</td> </tr> <tr> <td>CWE</td> <td>16</td> </tr> <tr> <td>WASC</td> <td>13</td> </tr> <tr> <td>ISO27001</td> <td>A.14.1.2</td> </tr> </tbody> </table> Error Details: <p>Error: preload directive not present Resolution: Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS)</p> Vulnerability Details: <p>Netsparker detected errors during parsing of Strict-Transport-Security header.</p> Impact: <p>The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.</p> 	Classification	Score	OWASP 2013	A5	OWASP 2017	A6	CWE	16	WASC	13	ISO27001	A.14.1.2
Classification	Score												
OWASP 2013	A5												
OWASP 2017	A6												
CWE	16												
WASC	13												
ISO27001	A.14.1.2												

Risk type : Medium

URL : <https://www.topcoder.com/>

Error : preload directive not present

Resolution : Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS) preload list.

Vulnerability Details

Netsparker detected errors during parsing of Strict-Transport-Security header

Impact

The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.

Remedy

Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

Browser vendors declared:

If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:

In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists

The max-age must be at least 31536000 seconds (1 year)

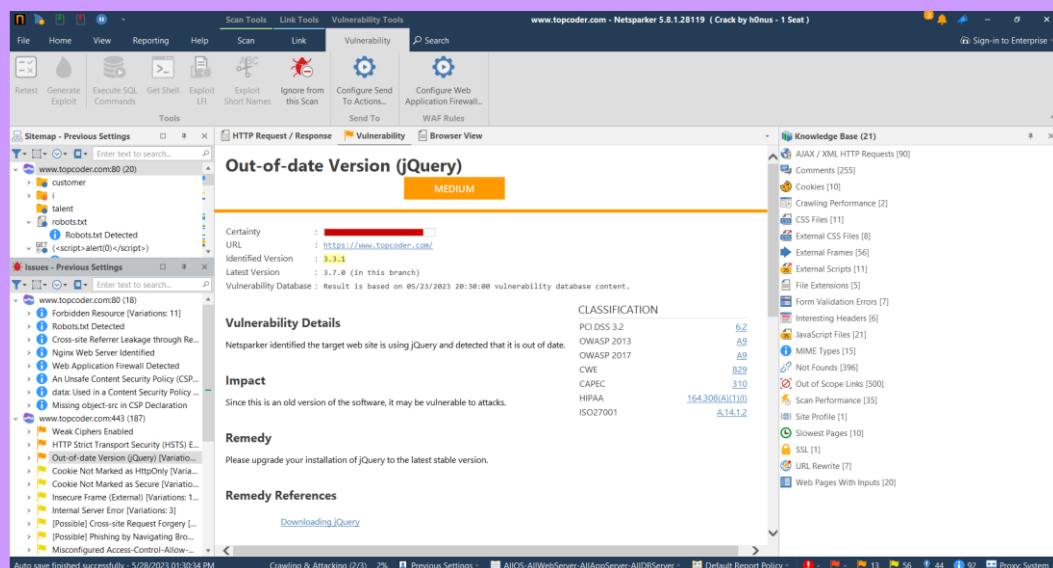
The includeSubDomains directive must be specified

The preload directive must be specified

If you are serving an additional redirect from your HTTPS site,

that redirect must have the HSTS header (rather than the page it redirects to)

Out-of-date Version(jQuery)



Risk type : Medium

URL : <https://www.topcoder.com/>

Identified Version : 3.3.1

Latest Version : 3.7.0 (in this branch)

Vulnerability Database :Result is based on 05/23/2023 20:30:00 vulnerability database content.

Vulnerability Details

Netsparker identified the target web site is using jQuery and detected that it is out of date **22 | Page** DE ZOYSA A.S. - IT21167096

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Remedy

Please upgrade your installation of jQuery to the latest stable version.

Remedy References : Downloading jQuery

Known Vulnerabilities in this Version

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Affected Versions : 1.9.0 to 3.4.1

External References : CVE-2020-11023
jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability
In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
Affected Versions : 1.9.0 to 3.4.1
External References : CVE-2020-11022
jQuery Prototype Pollution Vulnerability
jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.
Affected Versions : 1.0 to 3.3.1
External References : CVE-2019-11358

	Weak Ciphers Enabled Misconfigured Access-Control-Allow-Origin Header Cookie Not Marked as HttpOnly Cookie Not Marked as Secure
References	http://topcoder.com/

Date	24.05.2023
Summary of the day's activities	Bug Bounty vulnerabilities scanning Report 9-Canva Information gathering
Challenges faced	Vulnerability found by nikto Because connection problem ,so kali linux did not loading much time
Tools or technique learned	<p>Subdomains for hunting with knockpy</p> <pre> (kali㉿kali)-[~] └─\$ knockpy <domain name> </pre> <p>Open Ports Enumeration applying with nmap</p> <pre> (kali㉿kali)-[~] └─\$ sudo nmap -sS <domain name> </pre> <p>Checking for vulnerabilities using NIKTO</p> <pre> (kali㉿kali)-[~] └─\$ sudo nikto -h <domain name> </pre> <p>Scanned Vulnerabilities using Netsparker</p> <pre> (kali㉿kali)-[~] └─\$ sudo nikto -h <domain ip> </pre>
Vulnerabilities discovered and explores	<p>Missing X-Frame-Option Header</p> <p>Vulnerability Details, The X-Frame Alternatives The HTTP header field defines a policy that determines whether the sent resource should be rendered within a frame or an iframe by the browser. To prevent clickjacking attacks, servers can declare this policy in the header of their HTTP replies, ensuring that their content is not embedded in other sites or frames.</p> <p>Impact,</p> <p>Clickjacking occurs when an attacker employs numerous transparent or opaque layers to deceive a user into clicking on a button or link on a framed website when they intended to click on the top level page. As a result, the attacker is "hijacking" clicks intended for their website and redirecting them to another page, most likely controlled by another application, domain, or both.</p> <p>Keystrokes can likewise be hijacked using a similar manner. A skillfully prepared mix of stylesheets, iframes, and text boxes can fool a user into thinking they are</p>

putting in their email or bank account password, while in fact they are typing into an invisible frame controlled by the attacker.

- Remedy,
 - X-Frame-Options: DENY It completely denies to be loaded in frame/iframe.
 - X-Frame-Options: SAMEORIGIN It allows only if the site which wants to load has a same origin.
 - X-Frame-Options: ALLOW-FROM *URL* It grants a specific URL to load itself in a iframe. However please pay attention to that, not all browsers support this.

Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.

Employing defensive code in the UI to ensure that the current frame is the most top level window.

Cross-site Request Forgery

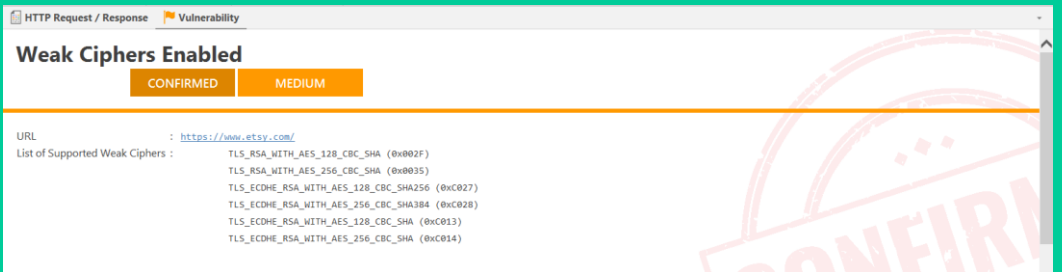
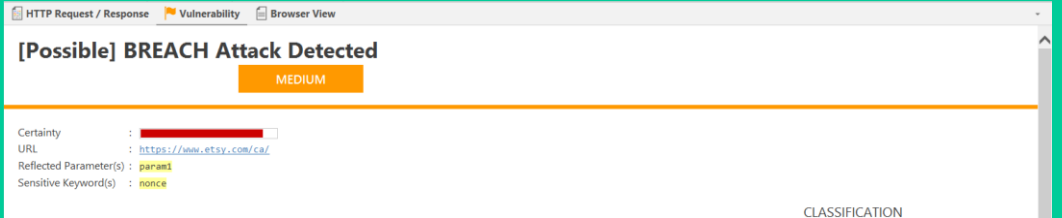
The screenshot displays the Burp Suite interface during a scan of www.canva.com. The 'Issues' panel on the left lists several security vulnerabilities, including 'Possible Cross-site Request Forgery' and 'Missing X-Frame-Options Header'. The 'Activity' panel at the bottom shows a list of HTTP requests, including a POST request to /cdn-cgi/trace.

Method	Target	Parameter	Duration	Current Activity	Overall Activity	Status
POST	https://www.canva.com/cdn-cgi/trace	[JSON] resources[0].i	2 s	[13/25] (Linux) Single Qa...	[5/34] Command Injection	Requesting
POST	https://www.canva.com/cdn-cgi/trace	[JSON] timingsV2.domCo...	1 s	[50/54] HTML Attribute HL...	[4/34] Cross-site Scripting	Waiting for CSRF
POST	https://www.canva.com/cdn-cgi/trace	[JSON] timingsV2.domain...	1 s	[10/45] Open (PHP) + Se...	[9/34] Code Evaluation	Requesting
POST	https://www.canva.com/cdn-cgi/trace	[JSON] resources[1].db	1 s	[7/60] (PHP) PCRE 'e' mod...	[34/34] Code Evaluation L...	Requesting

/cdn-cgi/trace: Cloudflare trace CGI found, which may leak some system information

References

<https://bugcrowd.com/canva>

Date	25.05.2023
Summary of the day's activities	Bug Bounty vulnerabilities scanning Report 10-ESTY Information gathering
Challenges faced	Vulnerability found by nikto Focus Areas Because connection problem ,so kali linux did not loading much time
Tools or technique learned	<p>Subdomains for hunting with knockpy</p> <pre> (kali㉿kali)-[~] └─\$ knockpy <domain name> Open Ports Enumeration applying with nmap (kali㉿kali)-[~] └─\$ sudo nmap -sS <domain name> Checking for vulnerabilities using NIKTO (kali㉿kali)-[~] └─\$ sudo nikto -h <domain name> Scanned Vulnerabilities using Netsparker (kali㉿kali)-[~] └─\$ sudo nikto -h <domain ip> </pre>
Vulnerabilities discovered and explores	<p>Weak Ciphers Enabled</p>  <p>[Possible]BREACH Attack Detected</p> 

HTTP Request / Response
Vulnerability

[Possible] Cross-site Scripting

MEDIUM

Certainty		<div style="background-color: #ff0000; height: 15px; width: 100%;"></div>
URL		<a href="https://www.etsy.com/dac/site-chrome/components/components.b8ed83608a5c28.site-chrome/header/header.b8ed83608a5c28.site-chrome/footer/footer.192876c1070fc8.gdpr/settings--verlay.192876c1070fc8.ces?variant=...</style></script><script>netsparker@000245C</script>">https://www.etsy.com/dac/site-chrome/components/components.b8ed83608a5c28.site-chrome/header/header.b8ed83608a5c28.site-chrome/footer/footer.192876c1070fc8.gdpr/settings--verlay.192876c1070fc8.ces?variant=...</style></script><script>netsparker@000245C</script>
Notes		Due to the Content-type header of the response, exploitation of this vulnerability might not be possible because of the browser used or because of the presence of certain web tools. We recommend that you fix this even if it is not an exploitable XSS vulnerability because it can allow an attacker to introduce other attacks to exploit it. As such, these issues are not confirmed; you will need to manually confirm them yourself. In general, lack of filtering in the response can cause Cross-site Scripting vulnerabilities in browsers with built-in mime sniffing (such as Internet Explorer).
Proof URL		<a href="https://www.etsy.com/dac/site-chrome/components/components.b8ed83608a5c28.site-chrome/header/header.b8ed83608a5c28.site-chrome/footer/footer.192876c1070fc8.gdpr/settings--verlay.192876c1070fc8.ces?variant=...</style></script><script>alert@000245C</script>">https://www.etsy.com/dac/site-chrome/components/components.b8ed83608a5c28.site-chrome/header/header.b8ed83608a5c28.site-chrome/footer/footer.192876c1070fc8.gdpr/settings--verlay.192876c1070fc8.ces?variant=...</style></script><script>alert@000245C</script>
Parameter Name		variant
Parameter Type		GET
Attack Pattern		```<</style></script><script>netsparker@000245C</script>

Certainty	:	
URL	:	<a href="https://www.etoy.com/dac/site-chrome/components/components_b8ed83608a5c28.site-chrome/header/header_b8ed83608a5c28.site-chrome/footer/footer_192876c1078fc8.gdpr/settings-?verlay=192876c1078fc8.css?variant=i%frame%2&src=http://r87.com/?<>i%frame>">https://www.etoy.com/dac/site-chrome/components/components_b8ed83608a5c28.site-chrome/header/header_b8ed83608a5c28.site-chrome/footer/footer_192876c1078fc8.gdpr/settings-?verlay=192876c1078fc8.css?variant=i%frame%2&src=http://r87.com/?<>i%frame>
Notes	:	Due to the Content-type header of the response, exploitation of this vulnerability might not be possible because of the browser used or because of the presence of certain web tools. We recommend that you fix this even if it is not an exploitable XSS vulnerability because it can allow an attacker to introduce other attacks to exploit it. But, these issues are not confirmed; you will need to manually confirm them yourself. In general, lack of filtering in the response can cause Cross-site Scripting vulnerabilities in browsers with built-in mime sniffing (such as Internet Explorer).
Parameter Name	:	variant
Parameter Type	:	GET
Attack Pattern	:	%3ciframe+src%3d%22http%3a%2f%2fr87.com%2f%3f%22%3e%3c%32fi%frame%3e

<https://bugcrowd.com/canva>