



Web Security – IE2062

Topic: Bug Bounty Report 3

Y2S2.WE.CS

Name: S.D.W.Gunaratne

(IT23241978)

Table of Content

1) How I started?

2) Introduction

2.1 Domain

1.2 Severity

3) Vulnerability

3.1 Vulnerability title

3.2 Vulnerability description

3.3 Affected components

3.4 Impact assessment




3.5 Steps to reproduce

3.6 Proof of concept

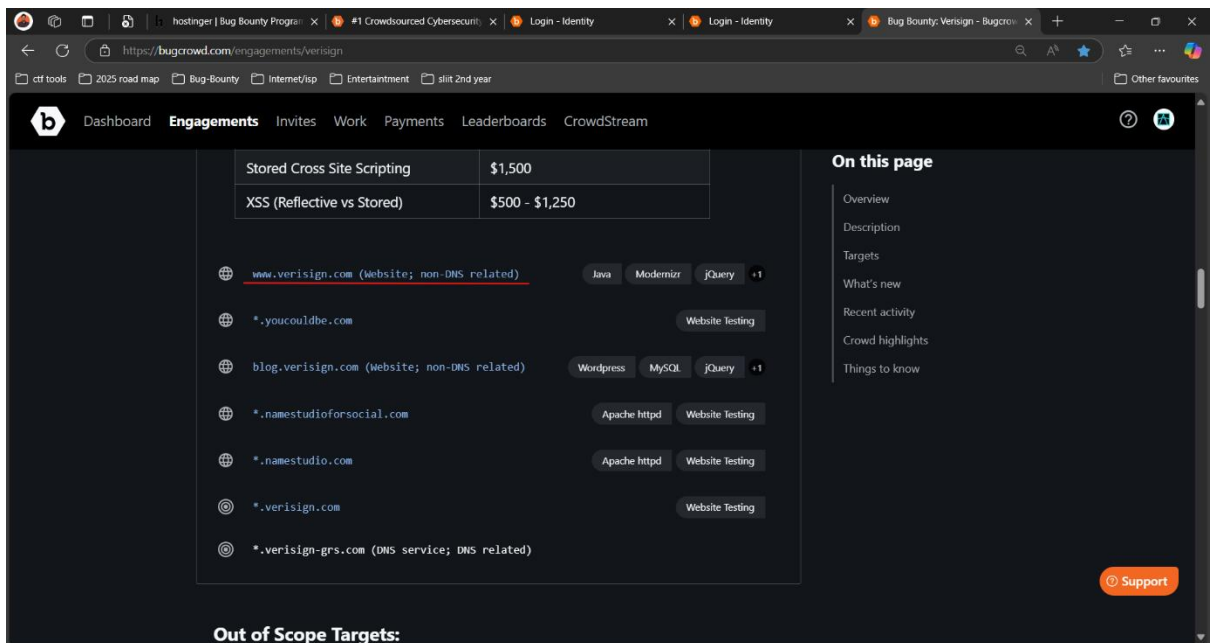
3.7 Proposed mitigation or fix

How I started?

1. Once I search from Bug crowd, I saw Verisign bug bounty program.

Title	Type	Scope rating	Min rewards	Max rewards	Compensation	Industry	More actions
 Verisign Verisign	 Bug Bounty	++++	\$100	\$10,000		 Technology	...

2. Then, I discovered full main domain allowed for scope, so that I choose.



The screenshot shows the Bugcrowd interface for the Verisign engagement. The top navigation bar includes Dashboard, Engagements, Invites, Work, Payments, Leaderboards, and CrowdStream. The main content area displays a table of stored XSS vulnerabilities with a reward of \$1,500. Below this, a list of in-scope targets is shown, including www.verisign.com, *.youcouldbe.com, blog.verisign.com, *.namestudioforsocial.com, *.namestudio.com, *.verisign.com, and *.verisign-grs.com. Each target has associated tags for technologies like Java, Modernizr, jQuery, Wordpress, MySQL, and Apache httpd. A sidebar on the right titled 'On this page' lists links for Overview, Description, Targets, What's new, Recent activity, Crowd highlights, and Things to know. A 'Support' button is located at the bottom right.

Target	Technologies
www.verisign.com (Website; non-DNS related)	Java, Modernizr, jQuery
*.youcouldbe.com	Website Testing
blog.verisign.com (Website; non-DNS related)	Wordpress, MySQL, jQuery
*.namestudioforsocial.com	Apache httpd, Website Testing
*.namestudio.com	Apache httpd, Website Testing
*.verisign.com	Website Testing
*.verisign-grs.com (DNS service; DNS related)	

Out of Scope Targets:

3. I use several methods/tools to do penetration testing.
4. First, I used Nmap. It helps me to find what are the open ports, Identify the web technologies such as webservers.

Scan Tools Profile Help

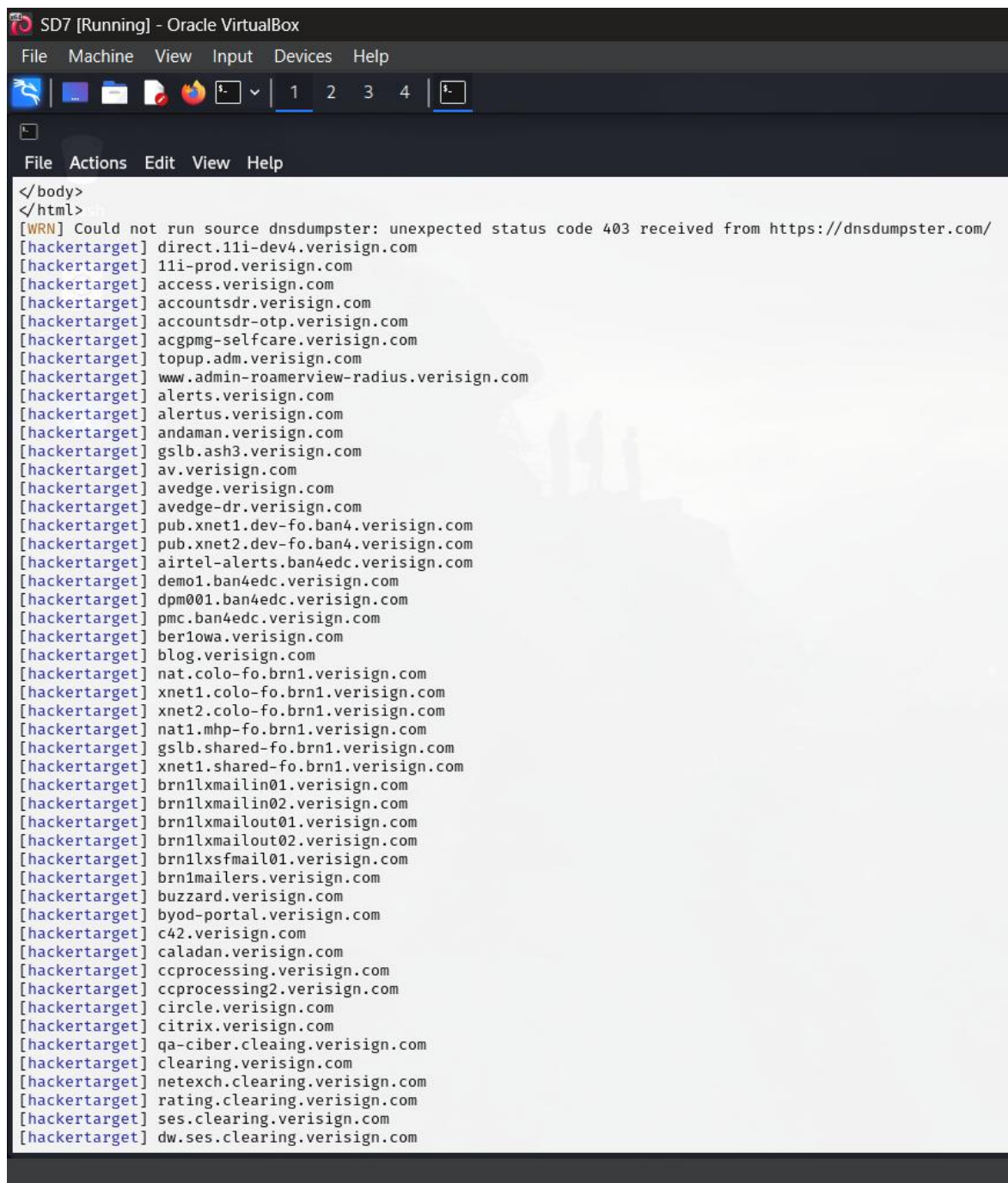
Target: Profile:

Command:

Hosts		Nmap Output				
OS	Host	Ports / Hosts	Topology	Host Details	Scans	
	www.verisign.co	<pre> nmap -T4 -A -v www.verisign.com Starting Nmap 7.95 (https://nmap.org) at 2025-04-27 14:16 Sri Lanka Standard Time NSE: Loaded 157 scripts for scanning. NSE: Script Pre-scanning. Initiating NSE at 14:16 Completed NSE at 14:16, 0.00s elapsed Initiating NSE at 14:16 Completed NSE at 14:16, 0.00s elapsed Initiating NSE at 14:16 Completed NSE at 14:16, 0.00s elapsed Initiating Ping Scan at 14:16 Scanning www.verisign.com (69.58.187.75) [4 ports] Completed Ping Scan at 14:16, 0.35s elapsed (1 total hosts) Initiating Parallel DNS resolution of 1 host. at 14:16 Completed Parallel DNS resolution of 1 host. at 14:16, 0.15s elapsed Initiating SYN Stealth Scan at 14:16 Scanning www.verisign.com (69.58.187.75) [1000 ports] Discovered open port 80/tcp on 69.58.187.75 Discovered open port 25/tcp on 69.58.187.75 Discovered open port 443/tcp on 69.58.187.75 Discovered open port 2000/tcp on 69.58.187.75 Discovered open port 5060/tcp on 69.58.187.75 Completed SYN Stealth Scan at 14:16, 21.55s elapsed (1000 total ports) Initiating Service scan at 14:16 Scanning 5 services on www.verisign.com (69.58.187.75) Service scan Timing: About 60.00% done; ETC: 14:18 (0:00:39 remaining) Service scan Timing: About 80.00% done; ETC: 14:19 (0:00:34 remaining) Completed Service scan at 14:19, 141.94s elapsed (5 services on 1 host) Initiating OS detection (try #1) against www.verisign.com (69.58.187.75) Retrying OS detection (try #2) against www.verisign.com (69.58.187.75) Initiating Traceroute at 14:19 Completed Traceroute at 14:19, 0.01s elapsed Initiating Parallel DNS resolution of 1 host. at 14:19 Completed Parallel DNS resolution of 1 host. at 14:19, 0.05s elapsed NSE: Script scanning 69.58.187.75. Initiating NSE at 14:19 Completed NSE at 14:19, 43.06s elapsed Initiating NSE at 14:19 Completed NSE at 14:21, 67.91s elapsed Initiating NSE at 14:21 Completed NSE at 14:21, 0.00s elapsed Nmap scan report for www.verisign.com (69.58.187.75) Host is up (0.020s latency). Not shown: 989 filtered tcp ports (no-response), 5 filtered tcp ports (admin-prohibited) </pre>				

Filter Hosts

- Secondly, I used Subfider tool to find hidden or forgotten web asserts. Because hidden web assert can have poor security, unpatched vulnerabilities.



The screenshot shows a terminal window titled "SD7 [Running] - Oracle VirtualBox". The window has a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". Below the menu bar is a toolbar with icons for file operations and a tab bar with tabs labeled "1", "2", "3", "4", and a terminal icon. The terminal window has its own menu bar with "File", "Actions", "Edit", "View", and "Help". The terminal output shows the following text:

```
</body>
</html>
[WRN] Could not run source dnsdumpster: unexpected status code 403 received from https://dnsdumpster.com/
[hackertarget] direct.11i-dev4.verisign.com
[hackertarget] 11i-prod.verisign.com
[hackertarget] access.verisign.com
[hackertarget] accountsdr.verisign.com
[hackertarget] accountsdr-otp.verisign.com
[hackertarget] acgpmg-selfcare.verisign.com
[hackertarget] topup.adm.verisign.com
[hackertarget] www.admin-roamerview-radius.verisign.com
[hackertarget] alerts.verisign.com
[hackertarget] alertus.verisign.com
[hackertarget] andaman.verisign.com
[hackertarget] gslb.ash3.verisign.com
[hackertarget] av.verisign.com
[hackertarget] avedge.verisign.com
[hackertarget] avedge-dr.verisign.com
[hackertarget] pub.xnet1.dev-fo.ban4.verisign.com
[hackertarget] pub.xnet2.dev-fo.ban4.verisign.com
[hackertarget] airtel-alerts.ban4edc.verisign.com
[hackertarget] demo1.ban4edc.verisign.com
[hackertarget] dpm001.ban4edc.verisign.com
[hackertarget] pmc.ban4edc.verisign.com
[hackertarget] ber1owa.verisign.com
[hackertarget] blog.verisign.com
[hackertarget] nat.colo-fo.brn1.verisign.com
[hackertarget] xnet1.colo-fo.brn1.verisign.com
[hackertarget] xnet2.colo-fo.brn1.verisign.com
[hackertarget] nat1.mhp-fo.brn1.verisign.com
[hackertarget] gslb.shared-fo.brn1.verisign.com
[hackertarget] xnet1.shared-fo.brn1.verisign.com
[hackertarget] brn1lxmailin01.verisign.com
[hackertarget] brn1lxmailin02.verisign.com
[hackertarget] brn1lxmailout01.verisign.com
[hackertarget] brn1lxmailout02.verisign.com
[hackertarget] brn1xsfm01.verisign.com
[hackertarget] brn1mailers.verisign.com
[hackertarget] buzzard.verisign.com
[hackertarget] byod-portal.verisign.com
[hackertarget] c42.verisign.com
[hackertarget] caladan.verisign.com
[hackertarget] ccprocessing.verisign.com
[hackertarget] ccprocessing2.verisign.com
[hackertarget] circle.verisign.com
[hackertarget] citrix.verisign.com
[hackertarget] qa-ciber.cleaing.verisign.com
[hackertarget] clearing.verisign.com
[hackertarget] netexch.clearing.verisign.com
[hackertarget] rating.clearing.verisign.com
[hackertarget] ses.clearing.verisign.com
[hackertarget] dw.ses.clearing.verisign.com
```

6. Thirdly, I used Wafwoof tool to find website is protected by a WAF (web application firewall). Because if WAF is active, so pen tester do their test without blocked, and they can do their testing with bypass WAF.

```
(root@kali2025)-[~]
# wafw00f https://www.verisign.com/

  404 Hack Not Found
  405 Not Allowed
  403 Forbidden
  502 Bad Gateway
  500 Internal Error

~ WAFW00F : v2.3.1 ~


[*] Checking https://www.verisign.com/
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[-] Number of requests: 7

(root@kali2025)-[~]
# █
```

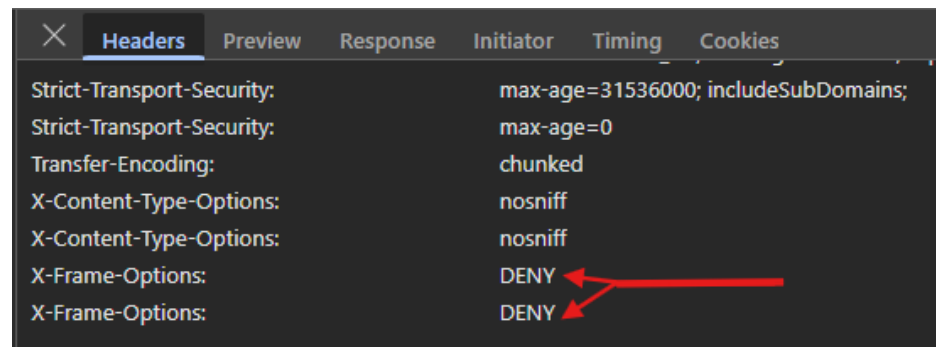
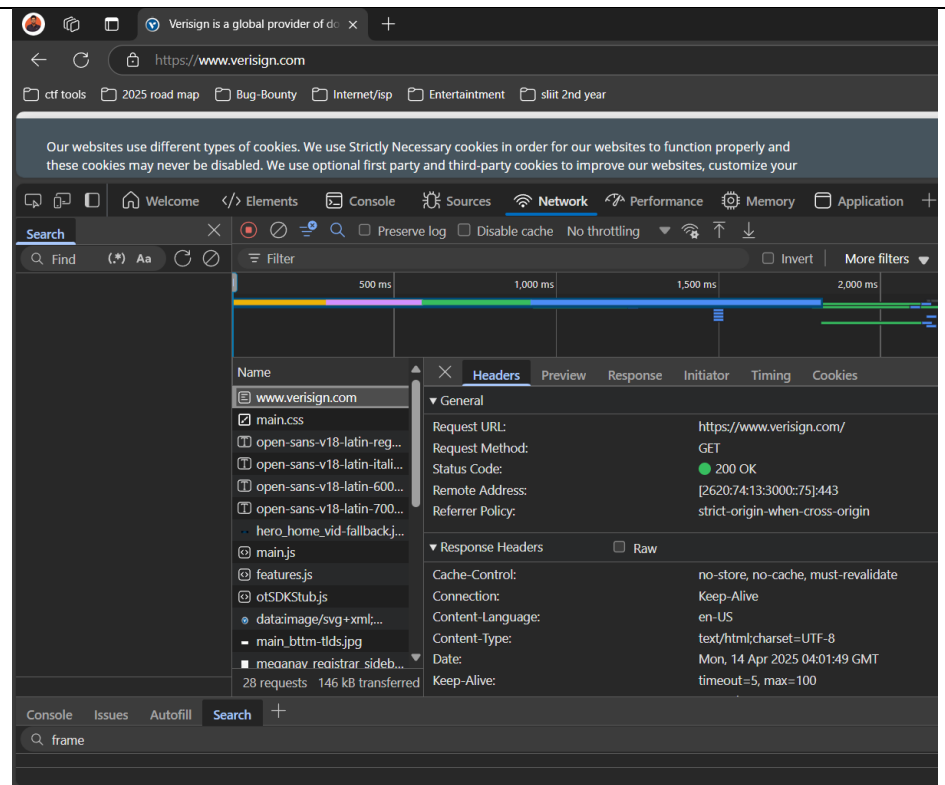
2) Introduction

2.1 Domain	https://www.verisign.com
2.2 Severity	<ul style="list-style-type: none">• Medium

3) Vulnerability

2.1 Vulnerability title	Multiple X-Frame-Options Header Entries CWE-1021 OWASP_2021_A05
2.2 Vulnerability description	<p>X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.</p> <p>Basic idea:</p> <ol style="list-style-type: none">1) why this X- Frame option header used? <ul style="list-style-type: none">• this is use for preventing from clickjacking attacks when user go tio the website, sometimes other web sites may try to load that site inside an iframe and it looks like window. To do that attacker use hidden links, or buttons to do that, So that's why we are using X-frame option. 

2.3 Affected components	Components: Web servers respond header issue: duplicate X frame headers in one response.
2.4 Impact assessment	In this scenario we have 2 same X-frame headers. So the issue is some browsers can be ignored both, so that this website is vulnerable to clickjacking attacks.
2.5 Steps to reproduce	In my case what happen is, my http responds header section we can see same header use in twice.
2.6 Proof of concept	<ul style="list-style-type: none"> • Search the website • Go to developer tools • Select network tab and refresh • Select main page and go to header option • Then check in the respond header, then we can find out there are 2 x-frame headers.



2.7 Proposed mitigation or fix

Ensure only a single X-Frame-Options header is present in the response. (just use once)

X-Frame-Options: DENY