



Web Security – IE2062

Topic: Bug Bounty Report 1

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

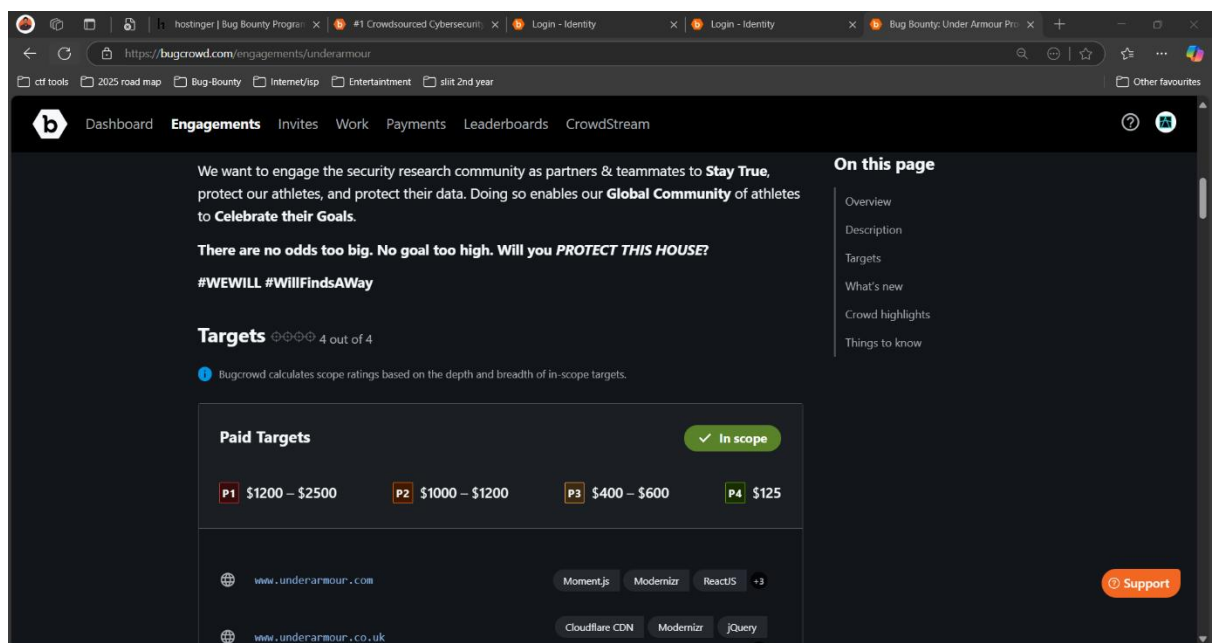
3.7 Proposed mitigation or fix

How I started?

1. Once I search from Bug crowd, I saw a Under Armour product security bug bounty program.



2. Then, I discovered full main domain allowed for scope, so that I choose <https://www.underarmour.com/>.



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 web servers.

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 14:08 Sri Lanka Standar
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:08
Completed NSE at 14:08, 0.00s elapsed
Initiating NSE at 14:08
Completed NSE at 14:08, 0.00s elapsed
Initiating NSE at 14:08
Completed NSE at 14:08, 0.00s elapsed
Initiating Ping Scan at 14:08
Scanning www.underarmour.com (151.101.1.91) [4 ports]
Completed Ping Scan at 14:08, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:08
Completed Parallel DNS resolution of 1 host. at 14:08, 0.03s elapsed
Initiating SYN Stealth Scan at 14:08
Scanning www.underarmour.com (151.101.1.91) [1000 ports]
Discovered open port 80/tcp on 151.101.1.91
Discovered open port 25/tcp on 151.101.1.91
Discovered open port 443/tcp on 151.101.1.91
Discovered open port 5060/tcp on 151.101.1.91
Discovered open port 2000/tcp on 151.101.1.91
Completed SYN Stealth Scan at 14:08, 6.74s elapsed (1000 total ports)
Initiating Service scan at 14:08
Scanning 5 services on www.underarmour.com (151.101.1.91)
Service scan Timing: About 80.00% done; ETC: 14:11 (0:00:39 remaining)
Completed Service scan at 14:11, 161.85s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against www.underarmour.com (151.101.1.91)
Retrying OS detection (try #2) against www.underarmour.com (151.101.1.91)
Initiating Traceroute at 14:11
Completed Traceroute at 14:11, 0.02s elapsed
Initiating Parallel DNS resolution of 1 host. at 14:11
Completed Parallel DNS resolution of 1 host. at 14:11, 0.04s elapsed
NSE: Script scanning 151.101.1.91.
Initiating NSE at 14:11
Completed NSE at 14:11, 31.96s elapsed
Initiating NSE at 14:11
```

5. 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 terminal displays a list of domains, each preceded by "[hackertarget]". The domains are: activesynceur.underarmour.com, activesynceudr.underarmour.com, activesynchk.underarmour.com, activesynchkdr.underarmour.com, advertising.underarmour.com, ams2-msc.underarmour.com, amsucvcse01.underarmour.com, amsucvcse02.underarmour.com, applicants.underarmour.com, apply.underarmour.com, armournet.underarmour.com, armournetlab.underarmour.com, athleteshunt.underarmour.com, b2b.underarmour.com, blackline.underarmour.com, cf.underarmour.com, mail5382.cf.underarmour.com, reply.cf.underarmour.com, click2connect.underarmour.com, combines.underarmour.com, depot.underarmour.com, developer.underarmour.com, ecomm-qa.underarmour.com, ecomm-qa-ext.underarmour.com, edmportal.underarmour.com, eem.underarmour.com, eemos.underarmour.com, eemosmda.underarmour.com, eemosmip.underarmour.com, eemostest.underarmour.com, eemostestmda.underarmour.com, eemostestmip.underarmour.com, eemtest.underarmour.com, em.underarmour.com, click.em.underarmour.com, mta.em.underarmour.com, mta2.em.underarmour.com, pages.em.underarmour.com, view.em.underarmour.com, emails.underarmour.com, click.emails.underarmour.com, cloud.emails.underarmour.com, cloudpages.emails.underarmour.com, mta.emails.underarmour.com, mta10.emails.underarmour.com, mta2.emails.underarmour.com, mta3.emails.underarmour.com, mta4.emails.underarmour.com, mta5.emails.underarmour.com, mta6.emails.underarmour.com, mta7.emails.underarmour.com, and mta8.emails.underarmour.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: ~
File Actions Edit View Help

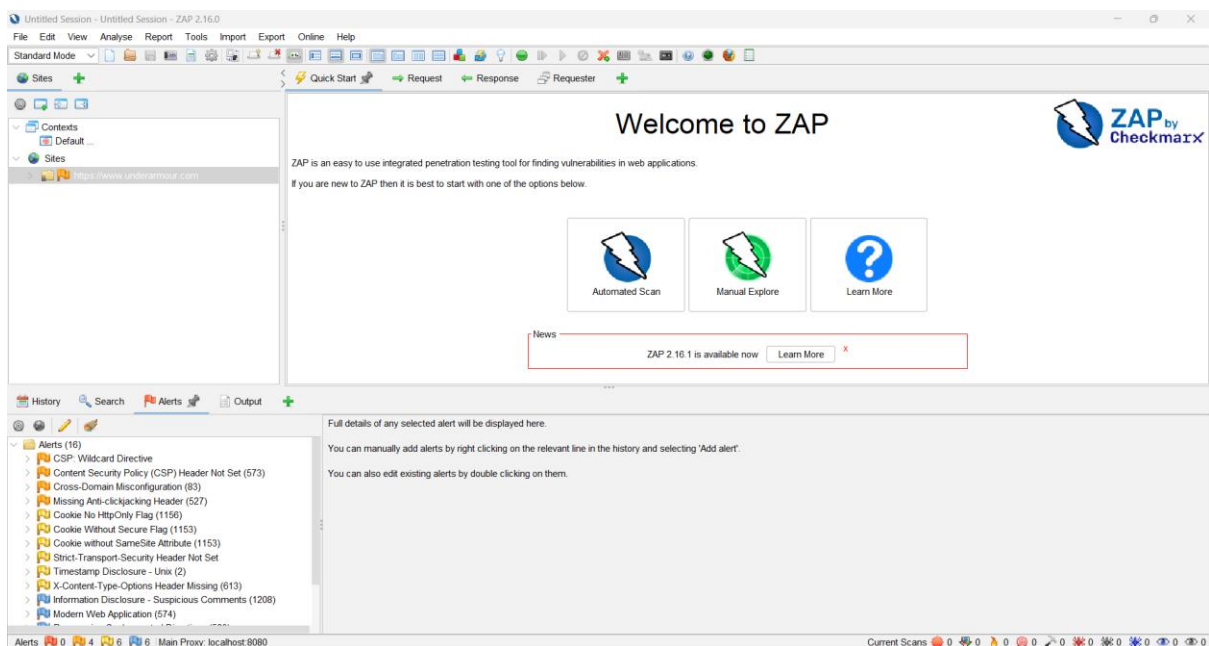
(root@kali2025)-[~]
# wafw00f https://www.underarmour.com/

~ WAFW00F : v2.3.1 ~

[*] Checking https://www.underarmour.com/
[+] Generic Detection results:
[*] The site https://www.underarmour.com/ seems to be behind a WAF or some sort of security solution
[~] Reason: The server returns a different response code when an attack string is used.
Normal response code is "406", while the response code to cross-site scripting attack is "418"
[~] Number of requests: 5

(root@kali2025)-[~]
#
```

7.Finally, I use OWASP zap to automatically find the vulnerabilities.

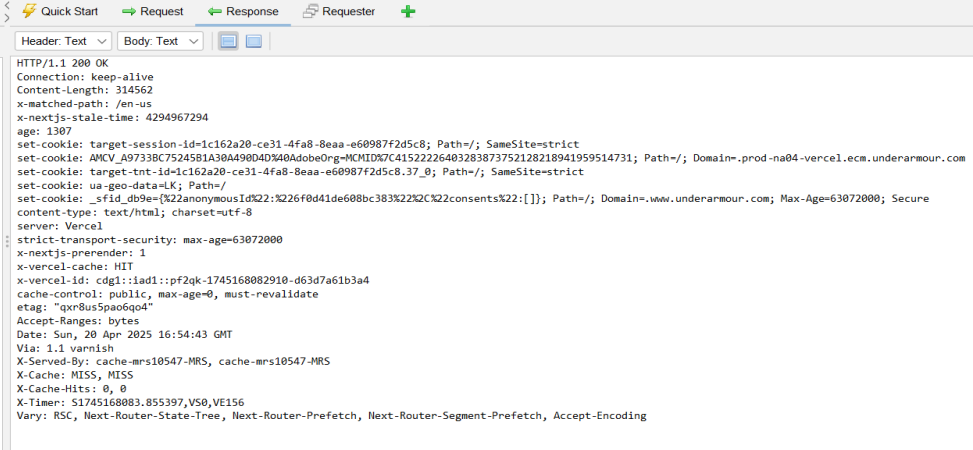


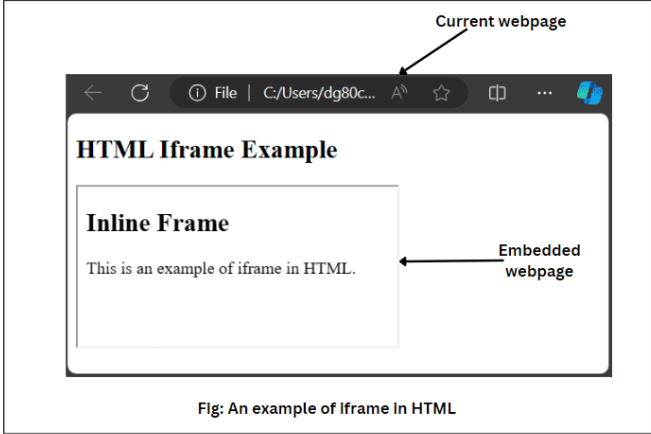
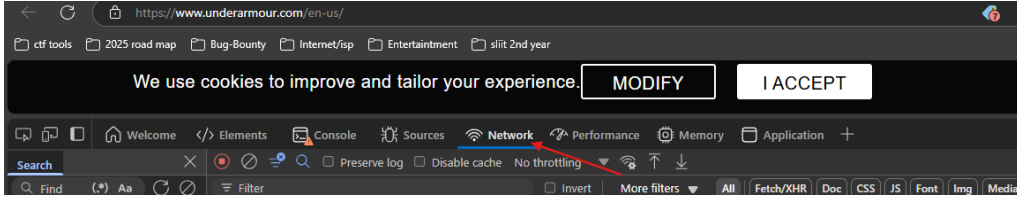
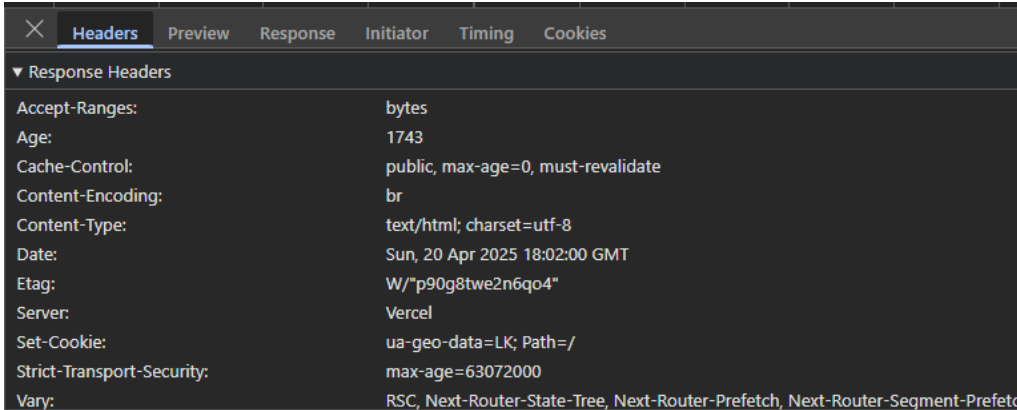
With getting these tool's support, I found below details about vulnerability.

2) Introduction

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

3) Vulnerability

3.1 Vulnerability title	Missing Anti-clickjacking Header OWASP_2021_A05 CWE-1021
3.2 Vulnerability description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
3.3 Affected components	<p>x-frame-options</p> <p>In this case effectuated component is https://prod-na04-vercel.ecm.underarmour.com/en-us</p> <p>To prevent Anti-clickjacking, we need X-Frame-Options Or Content-Security-Policy: frame-ancestors. But in this site, we can't see these in site response.</p> 
3.4 Impact assessment	<p>Because the headers don't exist, attackers can embed this page inside an iframe on an evil website.</p> <p>This makes Clickjacking attacks possible, where users are tricked into clicking on buttons or links that they do not see potentially leading to unauthorized operations or theft (data loss)</p>

	 <p>Fig: An example of IFRAME in HTML</p>																								
<p>3.5 Steps to reproduce</p>	<p>This how to reproduce: -</p> <ol style="list-style-type: none"> 1. Search URL(https://www.underarmour.com/) on our browser 2. Go to developer tools 3. Select Network option  <ol style="list-style-type: none"> 4. Refresh the page and check respond header 																								
<p>3.6 Proof of concept</p>	<ol style="list-style-type: none"> 5. While checking we can see, X-Frame-Options Or Content-Security-Policy with frame-ancestors are missing (not there)  <table border="1"> <thead> <tr> <th>Header</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Accept-Ranges:</td> <td>bytes</td> </tr> <tr> <td>Age:</td> <td>1743</td> </tr> <tr> <td>Cache-Control:</td> <td>public, max-age=0, must-revalidate</td> </tr> <tr> <td>Content-Encoding:</td> <td>br</td> </tr> <tr> <td>Content-Type:</td> <td>text/html; charset=utf-8</td> </tr> <tr> <td>Date:</td> <td>Sun, 20 Apr 2025 18:02:00 GMT</td> </tr> <tr> <td>Etag:</td> <td>W/"p90g8twe2n6qo4"</td> </tr> <tr> <td>Server:</td> <td>Vercel</td> </tr> <tr> <td>Set-Cookie:</td> <td>ua-geo-data=LK; Path=/</td> </tr> <tr> <td>Strict-Transport-Security:</td> <td>max-age=63072000</td> </tr> <tr> <td>Vary:</td> <td>RSC, Next-Router-State-Tree, Next-Router-Prefetch, Next-Router-Segment-Prefetch</td> </tr> </tbody> </table>	Header	Value	Accept-Ranges:	bytes	Age:	1743	Cache-Control:	public, max-age=0, must-revalidate	Content-Encoding:	br	Content-Type:	text/html; charset=utf-8	Date:	Sun, 20 Apr 2025 18:02:00 GMT	Etag:	W/"p90g8twe2n6qo4"	Server:	Vercel	Set-Cookie:	ua-geo-data=LK; Path=/	Strict-Transport-Security:	max-age=63072000	Vary:	RSC, Next-Router-State-Tree, Next-Router-Prefetch, Next-Router-Segment-Prefetch
Header	Value																								
Accept-Ranges:	bytes																								
Age:	1743																								
Cache-Control:	public, max-age=0, must-revalidate																								
Content-Encoding:	br																								
Content-Type:	text/html; charset=utf-8																								
Date:	Sun, 20 Apr 2025 18:02:00 GMT																								
Etag:	W/"p90g8twe2n6qo4"																								
Server:	Vercel																								
Set-Cookie:	ua-geo-data=LK; Path=/																								
Strict-Transport-Security:	max-age=63072000																								
Vary:	RSC, Next-Router-State-Tree, Next-Router-Prefetch, Next-Router-Segment-Prefetch																								

X-Cache:	MISS, MISS
X-Cache-Hits:	0, 0
X-Matched-Path:	/en-us
X-Nextjs-Prerender:	1
X-Nextjs-Stale-Time:	4294967294
X-Served-By:	cache-mrs10525-MRS, cache-mrs10525-MRS
X-Timer:	S1745172120.406166,VS0,VE188
X-Vercel-Cache:	HIT
X-Vercel-Id:	cdg1::iad1::h9nx2-1745172120472-8af511764291

About Clickjacking: -

It enables the attacker to trick the users into clicking something on the website without knowing it — this is referred to as Clickjacking. This one does by a small window on a website that can show another website inside it.

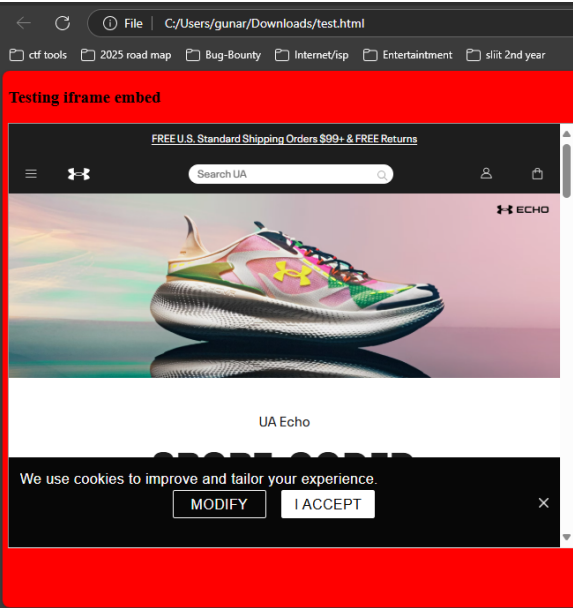
This is How the attacker tricks the user: -

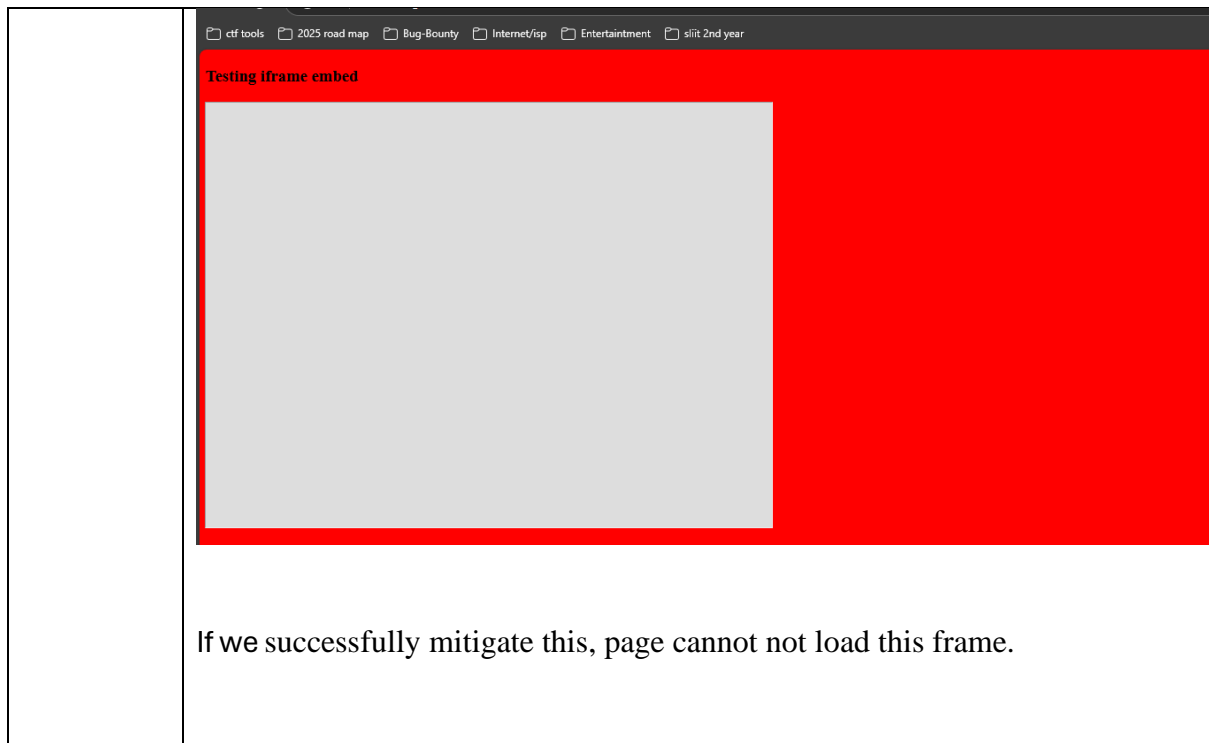
1. The hacker will make his own fake website.
2. In their site, they quietly load your true website inside a hidden window (a frame).
3. This is dangerous because, user might click links or button with their account without acknowledgement.

This is **how to do pen testing** this concept:

Use below code and make web site first and link our tested site :-
<https://prod-na04-vercel.ecm.underarmour.com/en-us>

```
<!DOCTYPE html>
<html>
  <head><title>Clickjacking Test</title></head>
  <body>
    <h3>Testing iframe embed</h3>
    <iframe src="https://prod-na04-vercel.ecm.underarmour.com/en-us"
width="800" height="600"></iframe>
  </body>
</html>
```

	 <p>In this scenario we can see this site loaded to our tested web page so, this is not safe. Ok,</p>
<p>3.7 Proposed mitigation or fix</p>	<p>Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.</p> <p>If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.</p> <p>If we successfully mitigate this problem our expected out look like this:</p>



Extra: - For this vulnerability I report this issue for bug crowd site, and I get this respond,

Dashboard

Engagements

Invites

Work

Payments

Leaderboards

CrowdStream

Submissions

Workflows

← Go back

Look! Your site can be shown inside another site — that's not safe.

Submitted 3 days ago · Last activity 3 days ago

ID	21974992-356f-4a5f-8b30-f0e1bd72423c
Submitted	29 Apr 2025 14:57:41 UTC
Target Location	www.underarmour.com
Target category	Web App
VRT	Server Security Misconfiguration > Lack of Security Headers > X-Frame-Options
Priority	P5
Bug url	https://prod-na04.vercel.ecm.underarmour.com/en-us
Description	<p>This report describes a Missing Anti-clickjacking Header vulnerability. Full technical details and PoC are included in the attached PDF. All information includes in pdf file.</p> <p>The real reason to do this bug bounty program is gaining new knowledge about web security as a beginner.</p>
Files attached	<div>Under%20Armour%20-%20bug%20bounty.pdf (418 KB)</div>

Status

Informational

This submission was reproducible but is considered informational. It may be that the issue is a best practice recommendation, low risk, has existing mitigations in place, or is an accepted business risk for the customer.

Reward

VRT version

1.15.1

Engagement

Under Armour Product Security

Closed on

29 Apr 2025

CrowdStream visibility

Choose to show your details with this submission in CrowdStream when accepted.

Please note: your username will always be shown with your submission if it is disclosed.

Show username

Show reward

Please note: This engagement does not currently disclose submission activity in CrowdStream.

Disclosure policy

Please note: This engagement does **not allow** disclosure. You may not release information about vulnerabilities found in this engagement to the public.

Need help?

Issues with a submission? Please visit Bugcrowd Support and create a support ticket.

Activity

ApolloCipher created the submission

3 days ago (29 Apr 2025 14:57:42 UTC)

teapot_bugcrowd sent a message

3 days ago (29 Apr 2025 15:08:38 UTC)

teapot_bugcrowd changed the state to Informational

3 days ago (29 Apr 2025 15:08:40 UTC)

Hi

Thank you for your submission, however, this issue is considered to be a P5 (Informational) finding as per Bugcrowd's Vulnerability Rating Taxonomy (VRT). Therefore, this finding typically does not qualify for a reward.

Typically, this is the case when an issue lacks a demonstrated risk and is considered security best practice. While that will apply regularly when we assign a submission a P5 rating, if you are able to exploit this finding further (or chain it with other findings) to meet the definition of another item within the VRT, please do submit a new report. We look forward to reading it!

As you progress with bug bounties it's important to consider not just the vulnerability but also the impact that this vulnerability has, so we encourage you to always explore any finding to better understand the impact it may have. Each submission should aim to answer the question as an attacker I could...

If you're unsure of the next steps to take this with submission, we recommend the Bugcrowd University as a starting point for learning how you can escalate bugs from a P5, into P4s or even P3 findings!

Best regards.

-Bugcrowd Security Operations Team

Send a message

WritePreview

ToEveryone

B

I

¶

<>

🔗

☰

☰

Your message to everyone here...

Embed images by dragging & dropping, selecting, or pasting them.

Add attachments

You can attach up to 20 files. Please keep individual upload size under 400MiB.

You can embed attachments (.jpg/.gif/.png, smaller than 5MB) into the Markdown fields. You can copy the embed code using the 'Copy as Markdown' button.

Send message


Terms & ConditionsPrivacy PolicySecurityDo Not Sell My Information

bugcrowd

Copyright © 2014 – 2025 Bugcrowd, Inc. All rights reserved.

DocsFAQResourcesBlogContactGet Help

12



ApolloCipher
LX Sri Lanka

ID not verified
 Start verification

Anyone can see your profile
 Update profile [privacy](#)

All-time points
0

Current rank
N/A

Accuracy
100.0%

Overview Achievements [Profile settings](#)

[Edit bio](#)

All time Last 90 days Current month

Performance Stats

Performance stats showcase your expertise based on past submissions to Bugcrowd. Track your performance stats to meet the criteria to join private programs. Learn more about private programs.


Vulnerabilities
1

Accuracy
100.00%

Priority percentiles

The priority percentile against other researchers based on valid reported vulnerabilities.


P1 - 0th
 P2 - 0th
 P3 - 0th
 P4 - 0th
 P5 - 47h



Reported vulnerabilities

Vulnerabilities scaled by technical severity in this period.

Critical (x4)
Severe (x20)
Moderate (x10)
Low (x3)




Submission type and severity



A look into the type and severity of vulnerabilities in this period.

VRT category	Count
Server Security Misconfiguration	1

Technical severity breakdown


Target type	Count
Web App	1


[Dashboard](#)
[Engagements](#)
[Invites](#)
[Work](#)
[Payments](#)
[Leaderboards](#)
[CrowdStream](#)





ACHIEVEMENTS [VIEW ALL ACHIEVEMENTS](#)

Achieved




Submission Shogun
Level 1




Bounty Bee Level 1

Leaderboard rankings [View leaderboard](#)






Submission Shogun
23943^{id}
1 submission



Bounty Bee
20626^{en}
1 engagement

Portfolio [Connect more accounts](#) [Support](#)

Add relevant content from your [connected accounts](#) to display them in your profile.

[Terms & Conditions](#)
[Privacy Policy](#)
[Security](#)
[Do Not Sell My Information](#)

[bugcrowd](#)
 Copyright © 2014 – 2025 Bugcrowd, Inc. All rights reserved.

[Docs](#)
[FAQ](#)
[Resources](#)
[Blog](#)
[Contact](#)
[Get Help](#)