// HALBORN

deBridge

WebApp Pentest

Prepared by: **Halborn**

Date of Engagement: **December 20th, 2021 - January 17th, 2022**

Visit: **Halborn.com**

DOCUMENT REVISION HISTORY

VERSION	MODIFICATION	DATE	AUTHOR
0.1	Document Creation	01/10/2022	Afaq Abid
0.2	Document Edit	01/17/2022	Afaq Abid
0.3	Draft Review	01/18/2022	Gabi Urrutia
1.0	Remediation Plan	05/16/2022	Afaq Abid
1.1	Remediation Plan Review	05/17/2022	Gabi Urrutia

CONTACTS

CONTACT	COMPANY	EMAIL
Rob Behnke	Halborn	Rob.Behnke@halborn.com
Steven Walbroehl	Halborn	Steven.Walbroehl@halborn.com
Gabi Urrutia	Halborn	Gabi.Urrutia@halborn.com
Afaq Abid	Halborn	Afaq.Abid@halborn.com

EXECUTIVE OVERVIEW

1.1 INTRODUCTION

deBridge engaged Halborn to conduct a security assessment on their front-end web application, beginning on December 20th, 2021 and ending January 17th, 2022. This security assessment was scoped to the frontend web applications. Halborn was provided access to the source code of the application, and the testing environment to conduct security testing using tools to scan, detect, validate possible vulnerabilities found in the application and report the findings at the end of the engagement.

Halborn recommends performing further testing to validate extended safety and correctness in context to the whole infrastructure when issues are fixed and new features added.

1.2 AUDIT SUMMARY

The team at Halborn was provided one month for the engagement and assigned two full-time security engineers to audit the security of the assets in scope. The engineers are blockchain and smart contract security experts with advanced penetration testing, smart-contract hacking, and deep knowledge of multiple blockchain protocols.

The goals of our security audits are to improve the quality of the systems we review and aim for sufficient remediation to help protect users.

In summary, Halborn identified the real IPs behind the Cloudflare and was able to access deBridge Web Apps over live IPs.
Exposure of live IPs makes deBridge vulnerable to DDoS attack and causes service unavailable.
We also note that websites hosted on live IPs use the insecure HTTP protocol, which makes all the communication in clear text.

Due to its business impact, the deBridge Team must address this issue as a matter of priority.

On top of that, we have found some missing security headers, an outdated

version of TLS support, and version disclosure issues. These should also be resolved by following the best practices.

1.3 TEST APPROACH & METHODOLOGY

Halborn performed a combination of manual and automated security testing to balance efficiency, timeliness, practicality, and accuracy regarding the scope of the pentest. While manual testing is recommended to uncover flaws in logic, process and implementation; automated testing techniques assist enhance coverage of the infrastructure and can quickly identify flaws in it. The following phases and associated tools were used throughout the term of the audit:

- Mapping Application Content and Functionality
- Application Logic Flaws
- Input Handling
- CloudFlare Bypass
- Fuzzing of all input parameters
- Test for Injection (SQL/JSON/HTML/Command)

RISK METHODOLOGY:

Vulnerabilities or issues observed by Halborn are ranked based on the risk assessment methodology by measuring the **LIKELIHOOD** of a security incident and the **IMPACT** should an incident occur. This framework works for communicating the characteristics and impacts of technology vulnerabilities. The quantitative model ensures repeatable and accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the Risk scores. For every vulnerability, a risk level will be calculated on a scale of 5 to 1 with 5 being the highest likelihood or impact.

RISK SCALE - LIKELIHOOD

5 - Almost certain an incident will occur.
4 - High probability of an incident occurring.

3 - Potential of a security incident in the long term.
2 - Low probability of an incident occurring.
1 - Very unlikely issue will cause an incident.

RISK SCALE - IMPACT

5 - May cause devastating and unrecoverable impact or loss.
4 - May cause a significant level of impact or loss.
3 - May cause a partial impact or loss to many.
2 - May cause temporary impact or loss.
1 - May cause minimal or un-noticeable impact.

The risk level is then calculated using a sum of these two values, creating a value of 10 to 1 with 10 being the highest level of security risk.

10 - CRITICAL
9 - 8 - HIGH
7 - 6 - MEDIUM
5 - 4 - LOW
3 - 1 - VERY LOW AND INFORMATIONAL

1.4 SCOPE

The following URLs and their respective repositories are in scope:

- https://debridge.finance
- https://testnet.debridge.finance (app.debridge.finance)
  commit: b002d88f7bb4b9161051a77195c2731b369c1ef8
- https://testnet-explorer.debridge.finance (explorer.debridge.finance)
  commit: 262e850ff31ccc4768d81ec34b1d7be06a444e7d

2. ASSESSMENT SUMMARY & FINDINGS OVERVIEW

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
0	1	1	2	1

LIKELIHOOD

IMPACT

			(HAL-01)	
		(HAL-02)		
	(HAL-03) (HAL-04)			
(HAL-05)				

EXECUTIVE OVERVIEW

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION DATE
CLOUDFLARE BYPASS	High	SOLVED - 05/10/2022
INSECURE PROTOCOL HTTP SUPPORTED	Medium	SOLVED - 05/10/2022
MISSING SECURITY HEADERS	Low	SOLVED - 05/10/2022
OUTDATED VERSIONS OF TLS SUPPORTED	Low	SOLVED - 05/10/2022
NGINX VERSION DISCLOSURE	Informational	SOLVED - 05/10/2022

FINDINGS & TECH DETAILS

3.1 (HAL-01) CLOUDFLARE BYPASS - HIGH

Description:

deBridge Web Apps can be accessed through direct IP addresses and that they bypass the Cloudflare's protection. Cloudflare's web application firewall (WAF) protects your website against web vulnerabilities such as SQL injection, XSS, CSRF, and DDoS attacks. If a Cloudflare-protected service is directly accessible, it is possible to perform a direct DDoS attack or bypass the protections provided by WAF. In this case, if there is a potential vulnerability in the web application, the attacker could more easily exploit and steal sensitive data.

Proof-of-Concept:

http://X.X.4.54:X/ ---> testnet.debridge.finance
http://X.X.254.201/ ---> testnet.debridge.finance
http://X.X.144.170:X/ ---> solanadevnet.debridge.io
http://X.X.3.55:X/ ---> mainnet-explorer.debridge.finance
http://X.X.40.174:X/ ---> testnet.debridge.finance

Risk Level:

Likelihood - 4
Impact - 4

Recommendation:

We recommend that you add firewall rules on the server to only accept traffic from Cloudflare. The list of IP addresses used by Cloudflare can be found here: https://www.cloudflare.com/ips/

Remediation Plan:

SOLVED: The deBridge team fixed the issue by adding the appropriate checks.

3.2 (HAL-02) INSECURE PROTOCOL HTTP SUPPORTED - MEDIUM

Description:

We have identified that, deBridge Web Apps are hosted on a insecure protocol (HTTP), which makes communication between client and server in clear text. Attacker can sniff the traffic and steal sensitive information about the users.

Proof-of-Concept:

http://X.X.4.54:X/
http://X.X.40.174:X/
http://X.X.254.201/
http://X.X.144.170:X/
http://X.X.3.55:X/

Risk Level:

Likelihood - 3
Impact - 3

Recommendation:

It is recommended to implement HTTPS and redirect all communication over HTTPS only.

Remediation Plan:

SOLVED: The deBridge team fixed the issue by adding the appropriate checks.

3.3 (HAL-03) MISSING SECURITY HEADERS - LOW

Description:

We have identified that there are important security Headers missing in the deBridge Web Apps. These headers used by client browser and enhance the security for end users against common attacks.

Important missing security headers; **Strict-Transport-Security**, **X-Frame-Options**, **X-Content-Type-Options** and **Content-Security-Policy** response headers.

- Strict-Transport-Security (HSTS) HTTP Strict Transport Security is an important security header to implement, as it makes the browser only communicate over HTTPS. Recommended value "Strict-Transport-Security: max-age=31536000; includeSubDomains".
- X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site, you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
- X-Content-Type-Options prevents a browser from trying to MIME-sniff the content-type and forces it to stick to the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
- Content-Security-Policy is an effective measure to protect your site from XSS attacks. By whitelisting approved content sources, you can prevent the browser from loading malicious assets.

Results:

```
┌──(kali㉿kali)-[~]
└─$ http --headers https://debridge.finance/
HTTP/1.1 200 OK
CF-Cache-Status: DYNAMIC
CF-RAY: 6c94f4a69bbe898f-SIN
Connection: keep-alive
Content-Encoding: gzip
Content-Type: text/html
Date: Thu, 06 Jan 2022 12:30:06 GMT
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Last-Modified: Tue, 30 Nov 2021 21:56:48 GMT
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=D6PF5I3TadCdzk8E5kAiz
ycTppsKTYXF4Z9IHxCzHpYZo%3D"}],"group":"cf-nel","max_age":604800}
Server: cloudflare
Transfer-Encoding: chunked
```

```
┌──(kali㉿kali)-[~]
└─$ http --headers https://testnet.debridge.finance/
HTTP/1.1 200 OK
CF-Cache-Status: DYNAMIC
CF-RAY: 6c94f870c99d87d5-SIN
Connection: keep-alive
Content-Encoding: gzip
Content-Type: text/html
Date: Thu, 06 Jan 2022 12:32:41 GMT
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Last-Modified: Mon, 13 Dec 2021 22:05:13 GMT
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=oBHsedH5GYm1yclOWacZl
4mhSVQLva3y%2FBKAOLV5aN1ZJaJUElJiOtxJYA%3D%3D"}],"group":"cf-nel","max_age":604800}
Server: cloudflare
Transfer-Encoding: chunked
```

```
┌──(kali㉿kali)-[~]
└─$ http --headers https://testnet-explorer.debridge.finance/
HTTP/1.1 200 OK
CF-Cache-Status: DYNAMIC
CF-RAY: 6c94f6c55d8b4679-SIN
Connection: keep-alive
Content-Encoding: gzip
Content-Type: text/html
Date: Thu, 06 Jan 2022 12:31:33 GMT
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Last-Modified: Thu, 30 Dec 2021 14:18:52 GMT
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=BMW8kc555yKWi%2FXF0xF
ve%2Bmp1G2aro4hYssaUCwsIoiR9w3QUBI%2Fl%2BGo4i7KtKVQ%3D%3D"}],"group":"cf-nel","max_age":604800}
Server: cloudflare
Transfer-Encoding: chunked
```

Risk Level:

Likelihood - 2

Impact - 2

Recommendation:

It is recommended to define the Strict-Transport-Security, X-Content-Type-Options=nosniff, Content-Security-Policy and X-Frame-Options response headers with the appropriate policies.

Reference:

Strict-Transport-Security

X-Content-Type-Options

X-Frame-Options

Content-Type

Remediation Plan:

SOLVED: The deBridge team fixed the issue by configuring the security headers. Moreover, the CSP header was not implemented as it blocks wallets like Metamask.

3.4 (HAL-04) OUTDATED VERSIONS OF TLS SUPPORTED - LOW

Description:

We have identified that scoped URLs are compatible with deprecated versions of TLS v1.0 and TLS v1.1 which are not considered secure and contain a number of cryptographic design flaws. While attacks that target weak cipher suites or algorithms are complex to execute, with the constant progress of computational power, these attacks become easier to pull off over time. As such, it is recommended to configure the connection to comply with security best practices.

Analysis:

```
 Testing protocols via sockets except NPN+ALPN

 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      offered (deprecated)
 TLS 1.1    offered (deprecated)
 TLS 1.2    offered (OK)
 TLS 1.3    offered (OK): final
 NPN/SPDY   not offered
 ALPN/HTTP2 h2, http/1.1 (offered)

 Testing cipher categories

 NULL ciphers (no encryption)                not offered (OK)
 Anonymous NULL Ciphers (no authentication)  not offered (OK)
 Export ciphers (w/o ADH+NULL)               not offered (OK)
 LOW: 64 Bit + DES, RC[2,4] (w/o export)     not offered (OK)
 Triple DES Ciphers / IDEA                   not offered
 Obsolete CBC ciphers (AES, ARIA etc.)       offered
 Strong encryption (AEAD ciphers)            offered (OK)
```

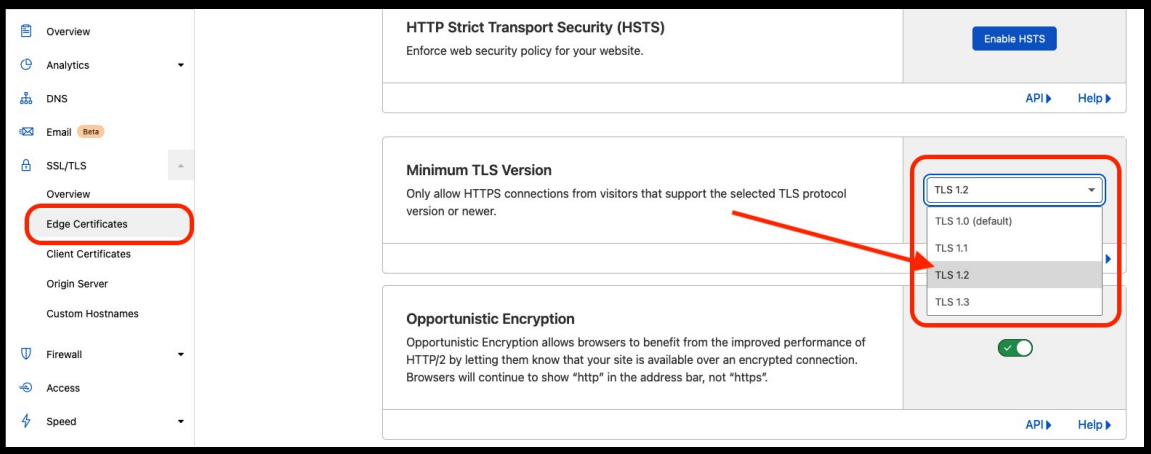
Risk Level:

Likelihood - 2

Impact - 2

Recommendation:

It should be noted that all major browser vendors coordinated to remove support for TLSv1.0 and TLSv1.1 in March 2020; however, these deprecated versions will still be available for outdated browser versions.



It is recommended to adhere to security best practices and use only TLS v1.2, TLS v1.3 as these are considered safe and strong and also disable support for older versions.

Remediation Plan:

SOLVED: The deBridge team fixed the issue by setting the TLS v1.2 and TLS v1.3 only for communication.

3.5 (HAL-05) NGINX VERSION DISCLOSURE - INFORMATIONAL

Description:

We have identified that the deBridge Web applications reveal the exact version of the nginx server in the server response header.

This gives an attacker an idea of the exact version number of the backend technology stack which allows them to craft and target attacks specifically designed for this version of application.

Proof of concept:

Listing 1

```
1 HTTP/1.1 301 Moved Permanently
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Thu, 13 Jan 2022 09:06:06 GMT
4 Content-Type: text/html
5 Content-Length: 178
6 Connection: keep-alive
7 Location: https://mainnet-explorer.debridge.finance/
```

Risk Level:

Likelihood - 1
Impact - 1

Recommendation:

By updating the nginx.conf with the following, you can remediate this:

Listing 2

```
http {
    ...
    server_tokens off;
    ...
}
```

Remediation Plan:

SOLVED: The deBridge team fixed the issue by adding the appropriate checks.

PERFORMED TESTS

4.1 XSS Injection

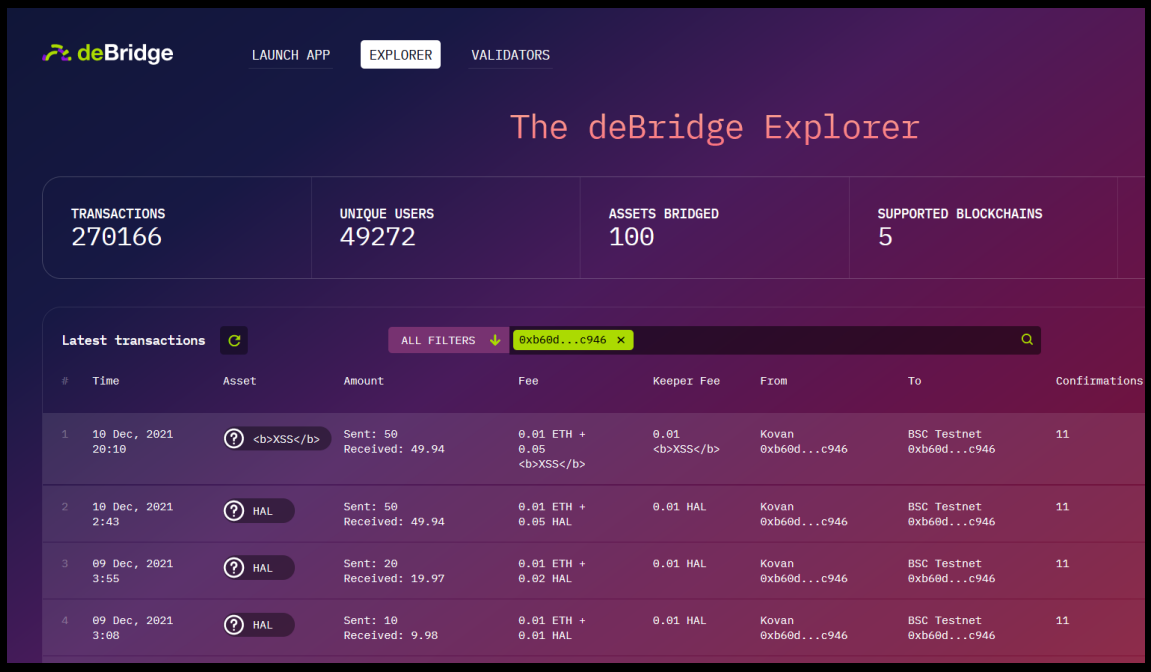
Description:

Cross Site Scripting (XSS) is one of the most popular and vulnerable attacks which is known by every advanced tester. It is considered as one of the riskiest attacks for the web applications and can bring harmful consequences too.

Goal:

Determine the strength of the application on protecting against XSS attacks on both Admin and User side.

Screenshots/Videos:



Result:

No Cross-site scripting that we could detect at this point.

4.2 Fuzzing

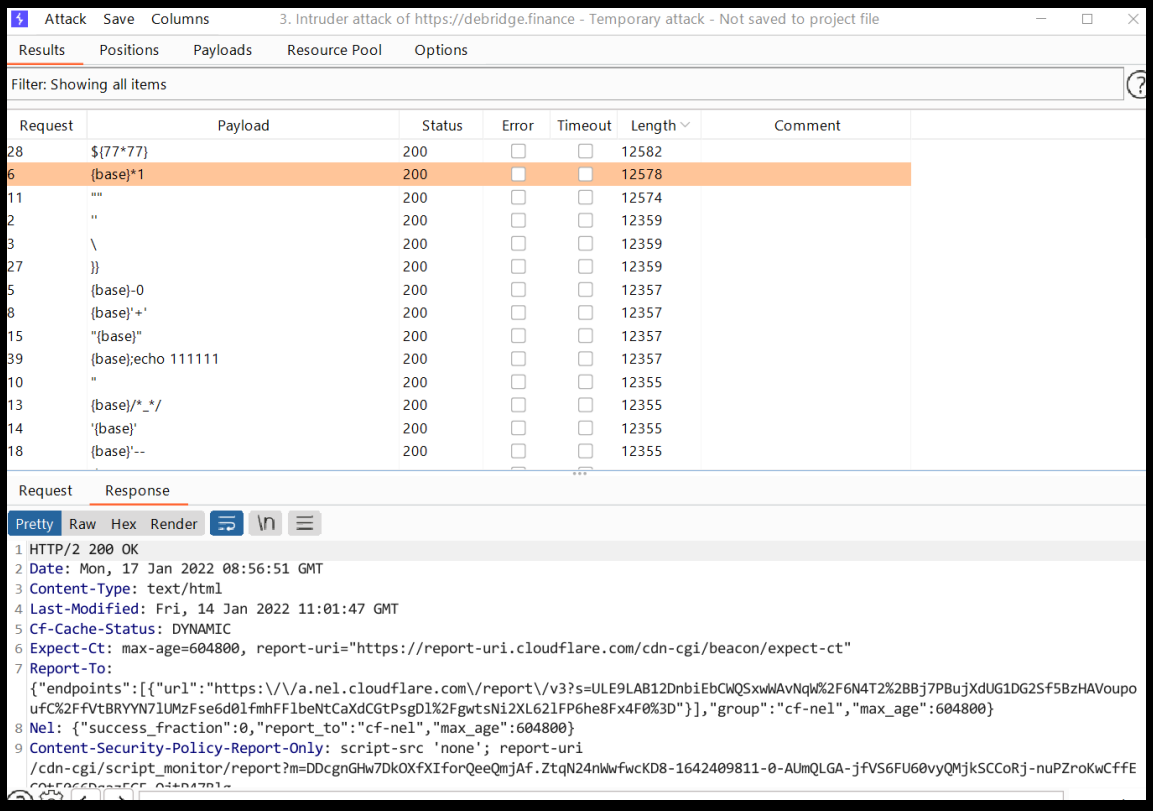
Description:

Fuzz testing or Fuzzing is a Black Box software testing technique, which basically consists of a wide range of invalid and unexpected data into an application, then monitoring the application for exceptions and crashes.

Goal:

Fuzz parameters and determine any unexpected crashes against provided input handling to find vulnerabilities.

Screenshots/Videos:



Result:

No exceptions/vulnerabilities found.

4.3 Directory Bruteforce

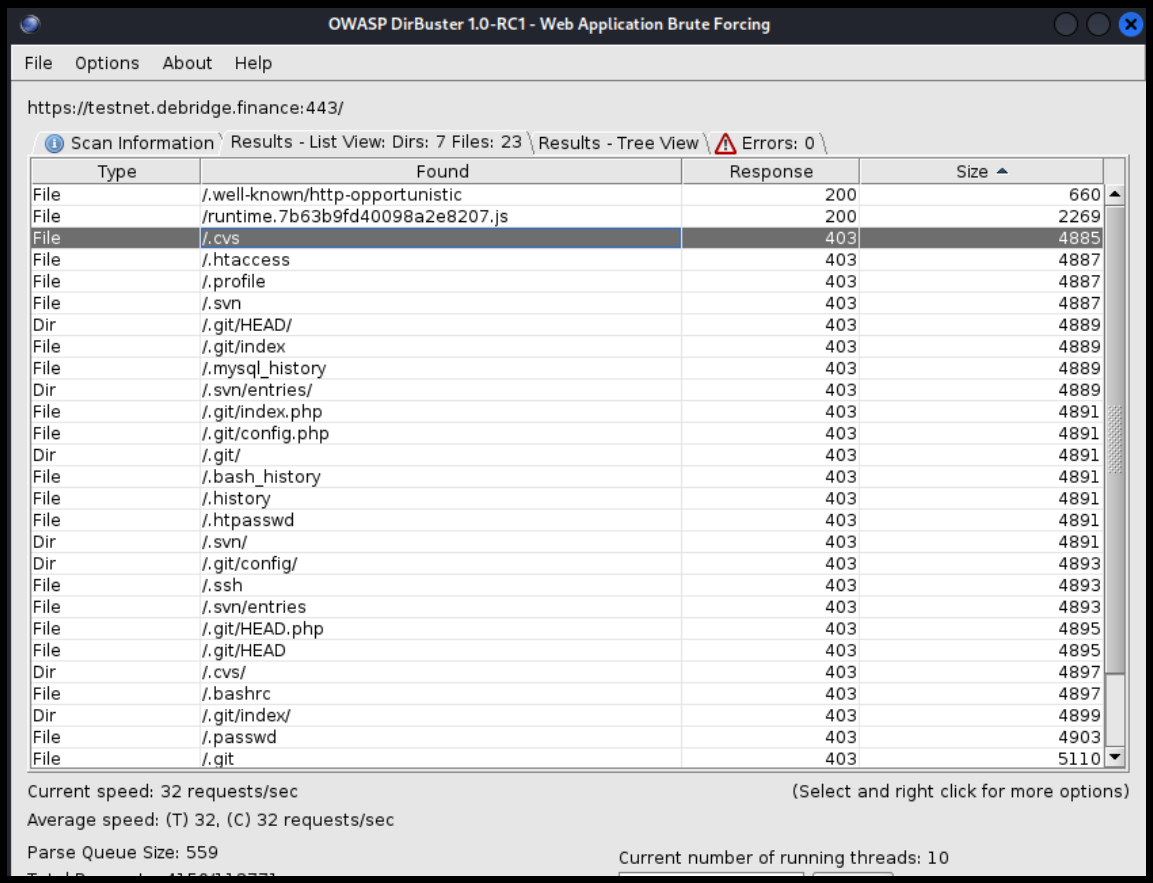
Description:

DirBuster is a technique designed to brute force directories and files names on web/application servers. DirBuster searches for hidden pages and directories on a web server. Sometimes developers will leave a page accessible, but unlinked. DirBuster is meant to find these potential vulnerabilities.

Goal:

Determine hidden/vulnerable pages and directories on a web server that is not required (or shouldn't even be public) and this could help a malicious user to conduct further attacks.

Screenshots/Videos:



Result:

No vulnerable/sensitive directory that we could detect at this point.

THANK YOU FOR CHOOSING

// HALBORN