Sri Lanka Institute of Information Technology

IE2072 - Foundations of Algorithms

Year 2, Semester 2

Individual Assignment

Bug Bounty vulnerabilities scanning report 10

Student Register Number	Student Name
IT21167096	DE ZOYSA A.S.

ESTY

Etsy is a global marketplace for unique and artistic goods. Our marketplaces, both online and offline, are where millions of people from all over the world come together to make, sell, and purchase unique goods. To help creative entrepreneurs launch, run, and grow their businesses, we also provide a number of Seller Services and tools. We want to keep commerce ethical. A bug bounty program has been run by Etsy since 2012. Our goal is to reward security researchers who adhere to ethical disclosure guidelines and contact us right away if they find a vulnerability that jeopardizes the security of our marketplace or users. We consider this to be best practice for the sector.

- <u>Scope and Rewards</u>

Scope of the security audit according to https://bugcrowd.com/etsy is as follows,

In Scope,

- ✓ www.etsy.com
- ✓ Etsy Mobile Application (Android)
- ✓ blog.etsy.com
- ✓ community.etsy.com
- ✓ etsypayments.com
- ✓ help.etsy.com

In-Scope Targets ✓ In scope

P4 $100 – $200 | P3 $300 – $800 | P2 $1000 – $5000 | P1 $5000 – $10000

Any publicly facing host owned by Etsy, including the below:	API Testing, Java, Android, +8
www.etsy.com	Varnish, jQuery, Google Cloud, +1
Etsy Mobile Application (Android)	Java, Android, Mobile Applicati..., +1
Etsy Mobile Application (iPhone)	Objective-C, SwiftUI, Swift, +2
Etsy API (see documentation below)	API Testing, HTTP
blog.etsy.com	Wordpress, MySQL, jQuery, +2
community.etsy.com	Angular, jQuery, Website Testing, +2
etsypayments.com	
help.etsy.com	

Out Scope,

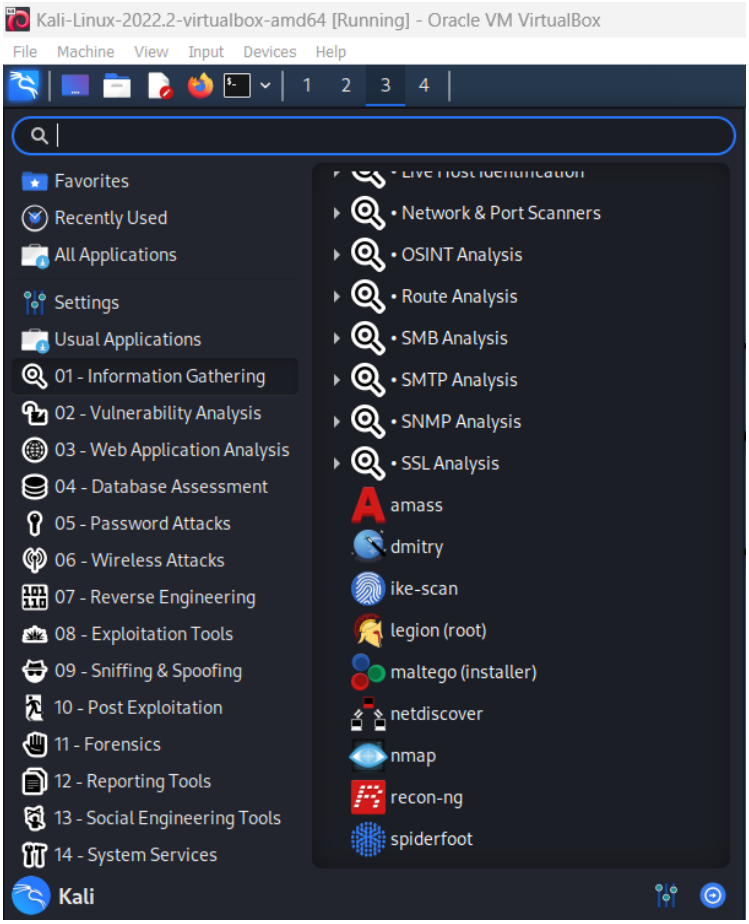
- ✓ icht.etsysecure.com

Out of scope targets | Out of scope

icht.etsysecure.com | API Testing | HTTP

Information Gathering

It is the process of collecting data from many sources for a range of purposes. Learning to create efficient information-gathering techniques will benefit studying in a variety of ways. Effective information collecting involves making better use of time, fostering critical thinking through the use of shifting/sorting strategies, and enlarging one's perspective and topic knowledge through the investigation of new sources. Additionally, obtaining knowledge may be useful for a number of purposes, but the major advantage in terms of academic studies is that one will become aware of more varied sources, viewpoints, and techniques that can improve one's academic work.



Focus Areas

This program is focused on vulnerabilities in Etsy's mobile & web application's. These applications are used by Etsy customers and sellers. Additionally, the developer APIs and portal is also in-scope.

- Unauthenticated access to users' accounts / information, especially PII (Personally Identifiable Information).
- Developer API vulnerabilities.

Subdomain for Hunting

Sub-domain enumeration is the process of listing sub-domains for one or more domains. In the process of reconnaissance, it's a crucial phase. Sub-domain enumeration can reveal several domains and sub-domains that are included in a security assessment, which increases the chance of finding vulnerabilities.

Finding applications using cryptic, abandoned sub-domains may reveal serious bugs.

Within a single company, the same vulnerabilities are routinely discovered across many domains and applications.

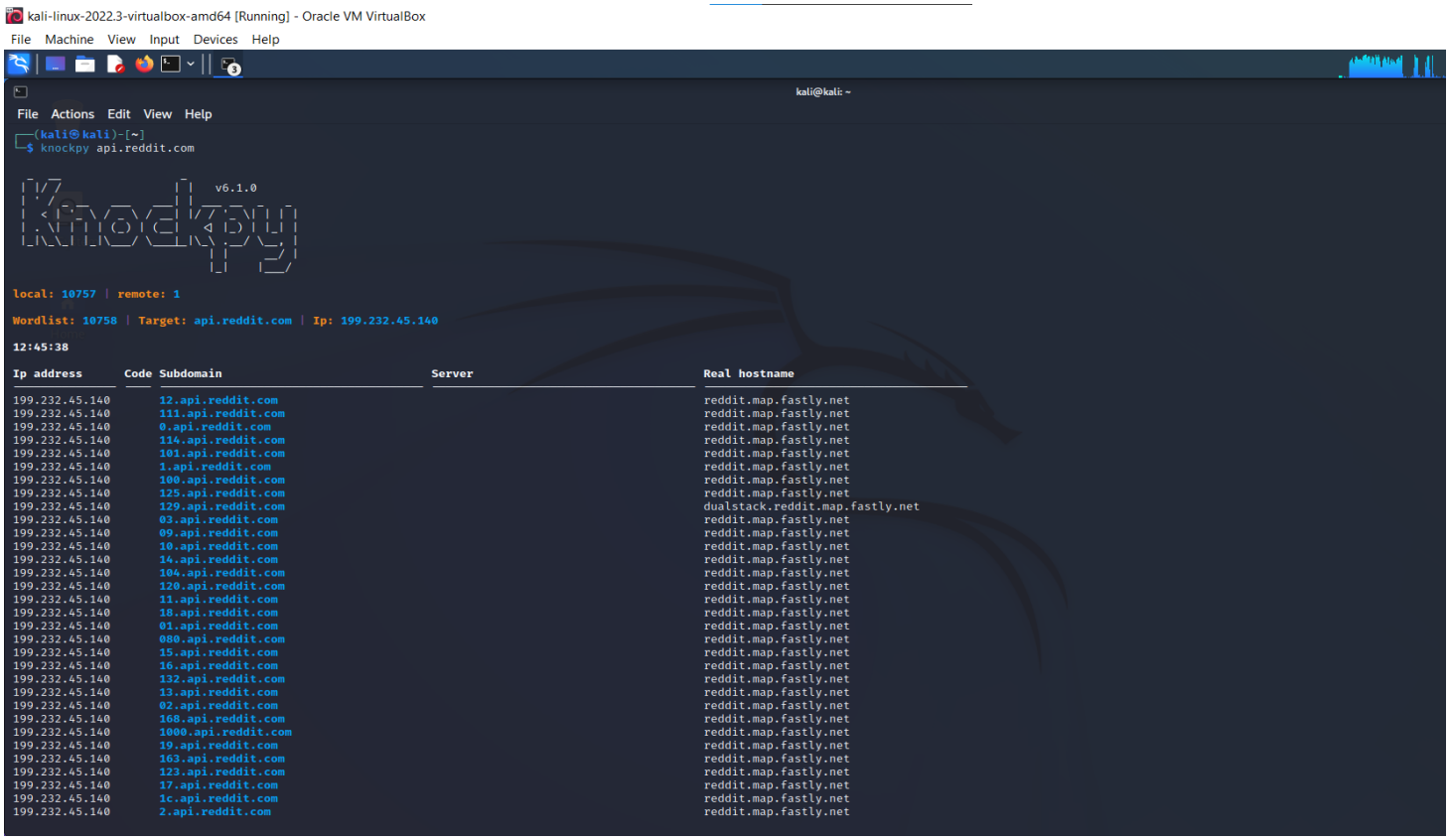
What is Knockpy?

With only a few lines of code, knockpy's python version of the knockoffs framework makes it simple to use knockoff-based inference. The modular design of Knockpy makes it simple for researchers and analysts to add features on top of it.

- searching subdomain by knockpy,

Knockpy is a portable and flexible Python3 utility that uses passive reconnaissance and dictionary scanning to swiftly enumerate subdomains on a specified domain.

How to Find Subdomain in Knockpy: knockpy <Domain Name>

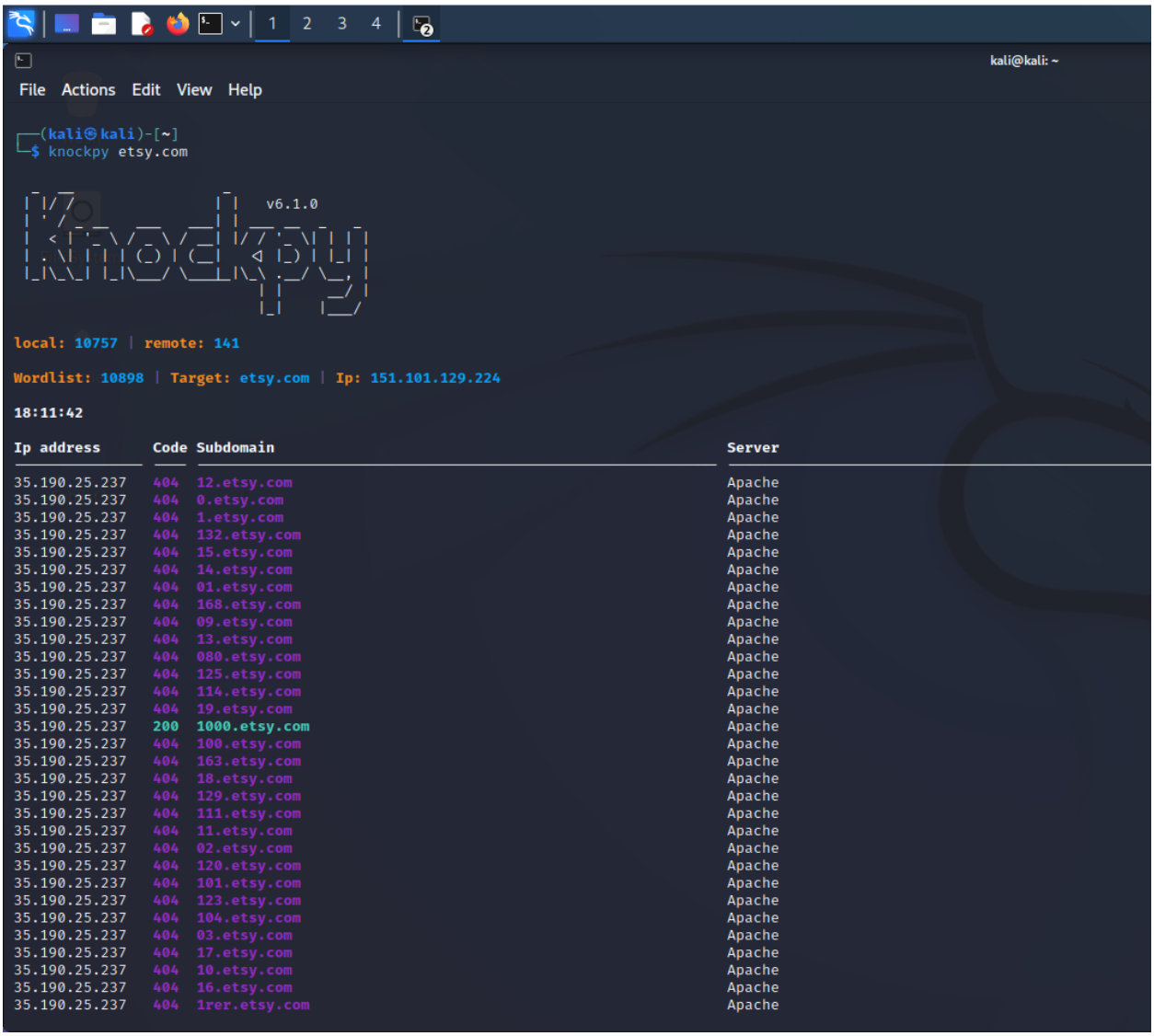


```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo amass enum -src -brute -d etsy.com
[sudo] password for kali:
[DNS]              etsy.com
[Brute Forcing]    education.etsy.com
[Brute Forcing]    system.etsy.com
[Brute Forcing]    v6.etsy.com
[Brute Forcing]    ns1.etsy.com
[Brute Forcing]    link.etsy.com
[Brute Forcing]    community.etsy.com
[Brute Forcing]    blog.etsy.com
[Brute Forcing]    developer.etsy.com
[Brute Forcing]    developers.etsy.com
[Brute Forcing]    help.etsy.com
[Brute Forcing]    investors.etsy.com
[Brute Forcing]    ops.ny4.etsy.com
[Brute Forcing]    ops.etsy.com
[Brute Forcing]    careers.etsy.com
[Brute Forcing]    gw.etsy.com
[Brute Forcing]    ns2.etsy.com
[Brute Forcing]    m.etsy.com
[Brute Forcing]    www.etsy.com

OWASP Amass v3.23.2                          https://github.com/owasp-amass/amass
___________________________________________________________________________________

19 names discovered - dns: 3, brute: 16
___________________________________________________________________________________

ASN: 13335 - CLOUDFLARENET - Cloudflare, Inc.
        104.16.0.0/14           2    Subdomain Name(s)
        162.159.128.0/22        1    Subdomain Name(s)
ASN: 0 - Not routed
        108.156.172.0/24        4    Subdomain Name(s)
ASN: 1299 - TELIANET
        23.40.124.0/22          2    Subdomain Name(s)
ASN: 54113 - FASTLY - Fastly
        151.101.0.0/21          2    Subdomain Name(s)
        199.232.36.0/22         1    Subdomain Name(s)
        151.101.244.0/22        1    Subdomain Name(s)
ASN: 15169 - GOOGLE - Google LLC
        35.224.0.0/14           1    Subdomain Name(s)
        34.117.0.0/16           2    Subdomain Name(s)
        35.190.0.0/16           2    Subdomain Name(s)
ASN: 396982 - GOOGLE-CLOUD-PLATFORM, US
        34.70.0.0/20            2    Subdomain Name(s)
        35.202.32.0/20          1    Subdomain Name(s)
ASN: 11377 - SENDGRID - SendGrid, Inc.
        167.89.0.0/17           4    Subdomain Name(s)
ASN: 16509 - AMAZON-02 - Amazon.com, Inc.
        54.230.112.0/22         4    Subdomain Name(s)
        2600:9000:237c::/48     8    Subdomain Name(s)

The enumeration has finished
```

Knockpy – Hunting for Subdomains.

Knockpy is a portable and flexible Python3 utility that uses passive reconnaissance and dictionary scanning to swiftly enumerate subdomains on a specified domain.

How to Find Subdomain in Knockpy: knockpy <Domain Name>



- Open Ports Enumeration applying with nmap

A port that is open is one that is actively receiving TCP or UDP packets. A port is in use and cannot be used for anything else if a service uses it. Open ports offer a security risk if the services operating on them are improperly configured, unsecure, or unpatched.

Using Nmap to List Open Ports

The most popular port security network scanner in the world is called Nmap. You may assess the efficacy of your firewall and security settings with the help of the Nmap hosted security tool

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap blog.etsy.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-25 14:16 EDT
Nmap scan report for blog.etsy.com (35.202.41.84)
Host is up (0.049s latency).
rDNS record for 35.202.41.84: 84.41.202.35.bc.googleusercontent.com
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 43.19 seconds
```

Open Ports,

PORT	STATE	SERVICE
25/tcp	open	smtp
80/tcp	open	http
443/tcp	open	https

Checking for vulnerabilities Using NIKTO,

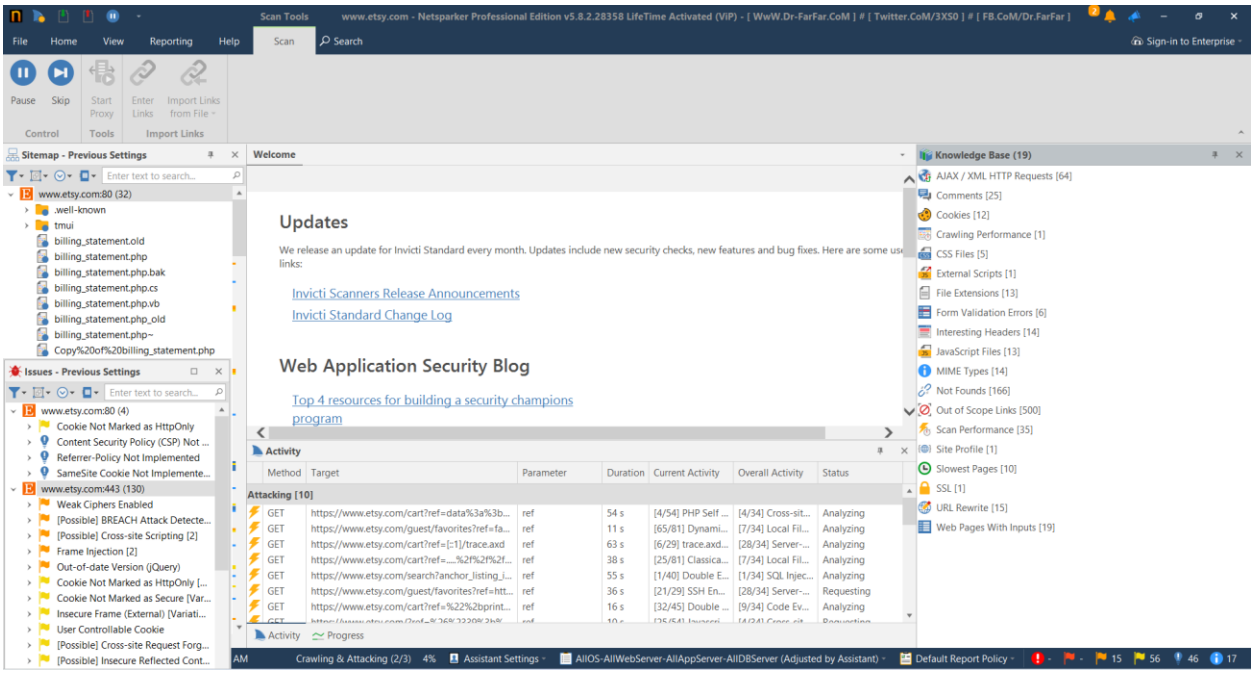
vulnerabilities are scanned by Nikto. But not any found vulnerability.

A security program called the Nikto web server scanner scans a website for thousands of possible security holes. This includes malicious files, services that have been set up improperly, vulnerable scripts, and other issues. It was created using plugins and is open source to allow for feature expansion. New security checks are frequently added to these plugins through regular updates. Many penetration testers and security analysts maintain the famous Nikto Web Vulnerability Scanner in their toolkit. It typically unearths valuable data about a web server or website that may be used for subsequent exploitation or vulnerability analysis.

```
┌──(kali㉿kali)-[~]
└─$ sudo nikto -h 35.202.41.84
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          35.202.41.84
+ Target Hostname:    35.202.41.84
+ Target Port:        80
+ Start Time:         2023-05-25 14:31:12 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/mis
sing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
^C

┌──(kali㉿kali)-[~]
└─$
```

Our targeted website does not have any Vulnerable issues.

Scanned Vulnerabilities Using Netsparker



1. Weak Ciphers Enabled
   - Risk Level: MEDIUM

Vulnerability Details

An attacker who can intercept connections can eavesdrop and interfere with any connection to the server that uses a weak encryption suite. Wi-Fi consumers are more prone to experience this. Depending on the encryption suites used, a connection may be intercepted right away.

Impact,

Attackers might decrypt SSL traffic between your server and your visitors.

Actions to Take

For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

For Microsoft IIS, you should make some changes to the system registry.

Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.

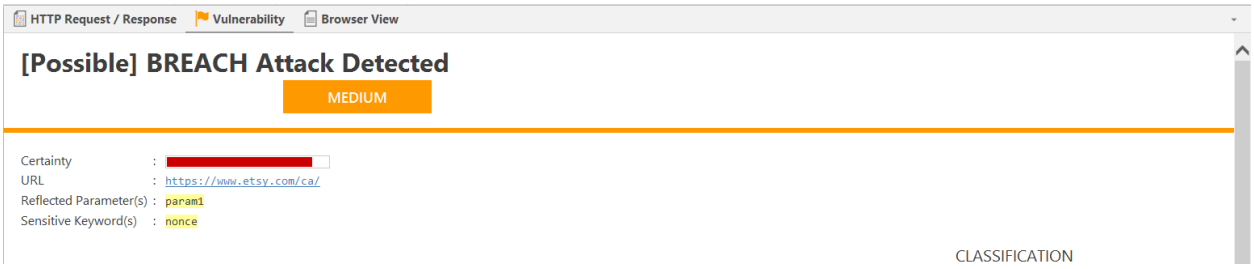
a. Click Start, click Run, type `regedt32` or type `regedit`, and then click OK.
b. In Registry Editor, locate the following registry key:
`HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
c. Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

Remedy,

Configure your web server to disallow using weak ciphers.

2. BREACH Attack Detected
    - Risk Level: MEDIUM



Vulnerability Details

BREACH (**Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext**) attack is possible on this website.

Due to elements that make BREACH attack possible, SSL/TLS protected traffic remains vulnerable and can be attacked to uncover information from the website.

Regardless of which version of SSL/TLS you use, attacks are still possible. Attacks do not require TLS-layer compression and they can work against any cipher suite.

Impact

Even if you use an SSL/TLS protected connection, an attacker can still view the victim's encrypted traffic and cause the victim to send HTTP requests to the vulnerable web server (by using invisible frames). Following these steps, an attacker could steal information from the website and do the following:

- Inject partial plaintext they have uncovered into a victim's requests.
- Measure the size of encrypted traffic.

Remedy,

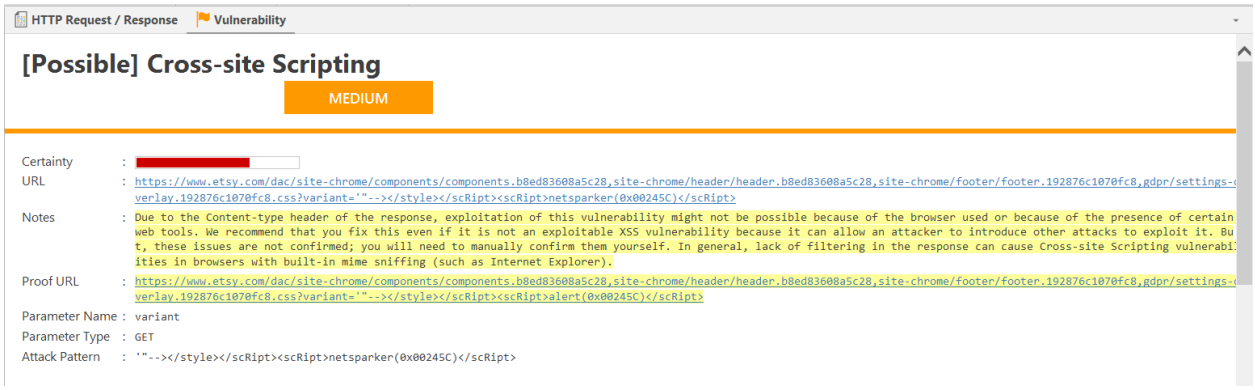
BREACH Attack issue because the target web page meets the following conditions that facilitate it:

- Served from a server that uses HTTP-level compression (ie. gzip)
- Reflects user-input in the HTTP response bodies
- Contains sensitive information (such as a CSRF token) in HTTP response bodies

To mitigate the issue, we recommend the following solutions:

- If possible, disable HTTP level compression
- Separate sensitive information from user input
- Protect vulnerable pages with CSRF token. The SameSite Cookie attribute will mitigate this issue, because to exploit this issue an attacker forces the victim to visit a target website using invisible frames. With the SameSite cookie attribute added, cookies that belong to the target won't be sent with a request that does not include top level navigation.
- Hide the length of the traffic by adding a random number of bytes to the responses.
- Add in a rate limit, so that the page maximum is reached five times per minute.

3. Cross-site Scripting
    - Risk Level: Medium



Vulnerability Details

This opens various attack possibilities, most notably hijacking the user's current session or modifying the design of the website by changing the HTML on the fly to steal the user's credentials. This occurs because the browser has interpreted the user's input as HTML/JavaScript/VBScript. Cross-site scripting attacks the application's users rather than the server. Although this is a drawback, because it allows attackers to hijack other users' sessions, an attacker may assault an administrator in order to take complete control of the program.

Impact,

There are many different attacks that can be leveraged through the use of XSS, including:

- Hijacking user's active session.
- Changing the look of the page within the victim's browser.
- Mounting a successful phishing attack.
- Intercepting data and performing man-in-the-middle attacks.

Remedy,

This issue occurs because the browser interprets the input as active HTML, JavaScript or VBScript. To avoid this, all input and output from the application should be filtered / encoded. Output should be filtered / encoded according to the output format and location.

There are a number of pre-defined, well-structured whitelist libraries available for many different environments. Good examples of these include OWASP Reform and Microsoft Anti-Cross-site Scripting libraries.

Additionally, you should implement a strong Content Security Policy (CSP) as a defense-in-depth measure if an XSS vulnerability is mistakenly introduced. Due to the complexity of XSS-Prevention and the lack of secure standard behavior in programming languages and frameworks, XSS vulnerabilities are still common in web applications.

CSP will act as a safeguard that can prevent an attacker from successfully exploiting Cross-site Scripting vulnerabilities in your website and is advised in any kind of application. Please make sure to scan your application again with Content Security Policy checks enabled after implementing CSP, in order to avoid common mistakes that can impact the effectiveness of your policy. There are a few pitfalls that can render your CSP policy useless, and we highly recommend reading the resources linked in the reference section before you start to implement one.

4. Frame Injection
    - Risk Level: Medium

Impact,

An attacker might use this vulnerability to redirect users to other malicious websites that are used for phishing and similar attacks. Additionally they might place a fake login form in the frame, which can be used to steal credentials from your users. It should be noted that attackers can also abuse injected frames in order to circumvent certain client side security mechanisms. Developers might overwrite functions to make it harder for attackers to abuse a vulnerability.

If an attacker uses a javascript: URL as src attribute of an iframe, the malicious JavaScript code is executed under the origin of the vulnerable website. However, it has access to a fresh window object without any overwritten functions.

Remedy,

- Where possible do not use users' input for URLs.
- If you definitely need dynamic URLs, make a list of valid accepted URLs and do not accept other URLs.
- Ensure that you only accept URLs which are located on accepted domains.
- Use CSP to whitelist iframe source URLs explicitly.