ETHICAL HACKING PROJECT:

WEBPAGE VULNERABILITY TESTING

PRESENTED BY: NISHANT SOURAV
ECE DEPARTMENT.
NETAJI SUBHASH ENGINEERING COLLEGE

FABRIKAM

index

1. INTRODUCTION
2. OBJECT & TOOLS USED
3. WHY WE CHOOSE THIS WEBSITE ?
4. TARGET DETAILS
5. NIKTO
6. SNAP OF KALI USING NIKTO
7. VULNERABILITIES
8. UNISCAN
9. VULNERABILITIES
10. CONCLUSION
11. ACKNOWLEDGEMENT

Introduction

Web application vulnerabilities involve a system flaw or weakness in a web-based application. They have been around for years, largely due to not validating or sanitizing form inputs, misconfigured web servers, and application design flaws, and they can be exploited to compromise the application's security. These vulnerabilities are not the same as other common types of vulnerabilities, such as network or asset. They arise because web applications need to interact with multiple users across multiple networks, and that level of accessibility is easily taken advantage of by hackers.

FABRIKAM

OUR OBJECT:

www.jgec.ac.in
(Jalpaiguri govt. engineering college)

Tool used

1. NIKTO
2. Uniscan

TARGET DETAILS

Target IP: 182.50.135.94

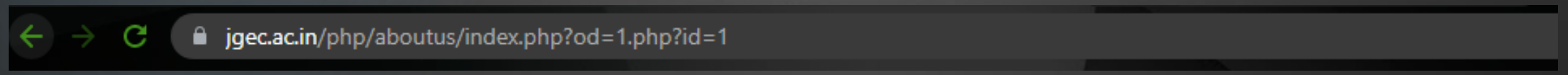
Target Hostname: www.jgec.ac.in

Target Port: 80

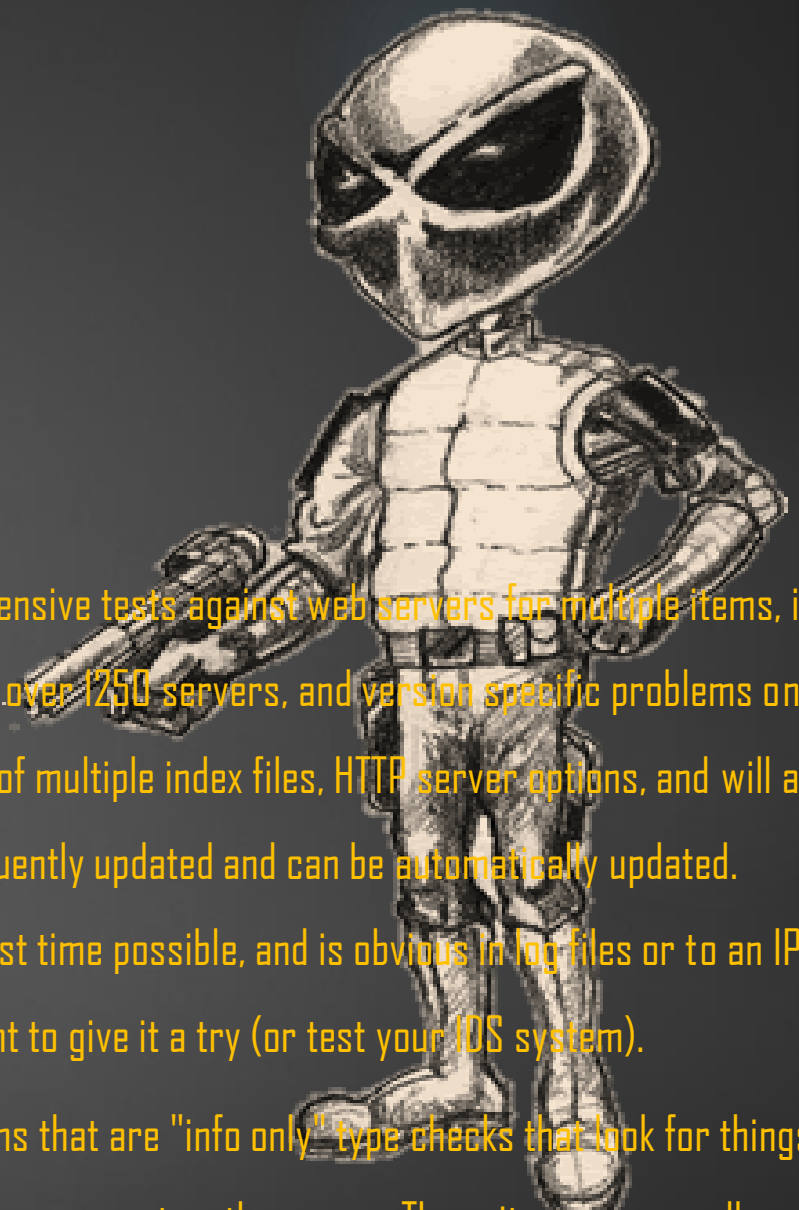
WHY WE CHOOSE THIS WEBSITE?

AS you can See the url of this window given below ,we have searched that either this web is secure or not using a injection on this website called php?id=1.

AS A RESULT WE FOUNT ITS NOT SECURE . & READY TO CHEK

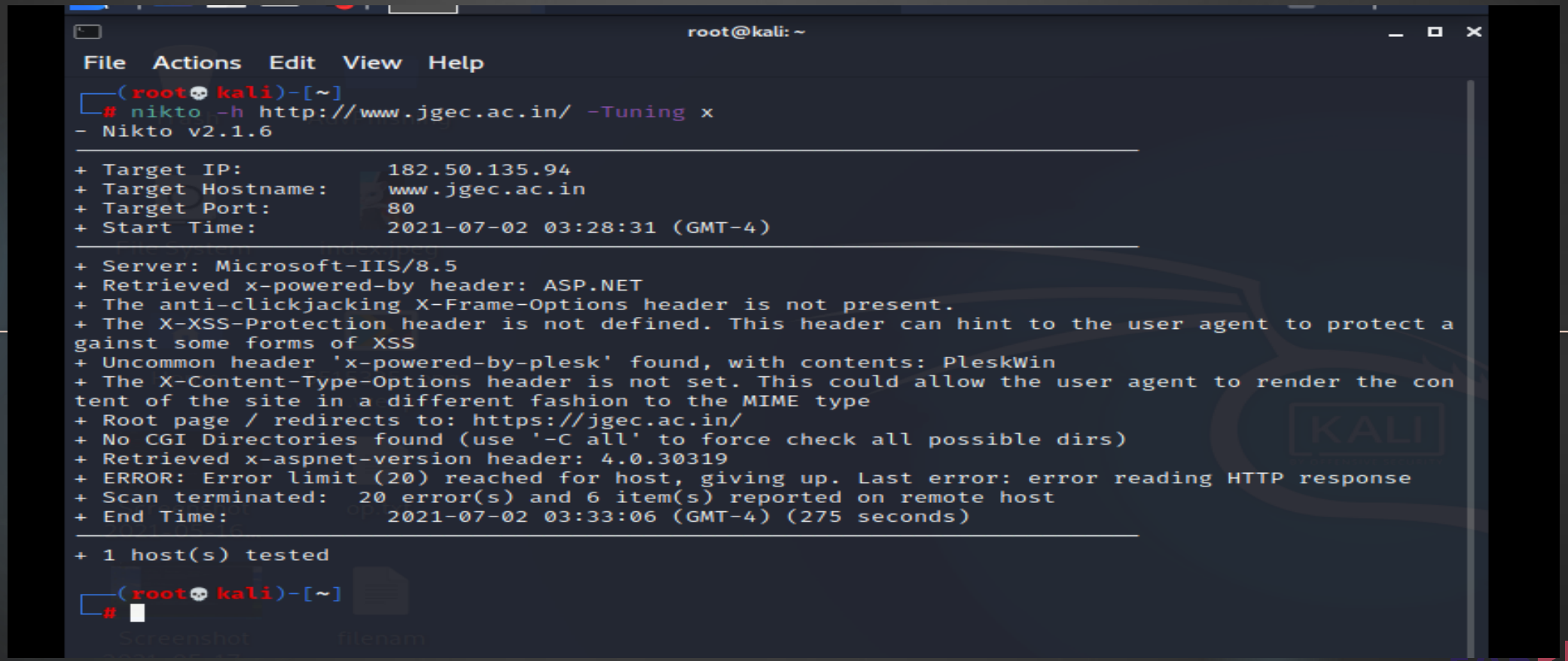


NIKTO



- Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.
  Nikto is not designed as a stealthy tool. It will test a web server in the quickest time possible, and is obvious in log files or to an IPS/IDS. However, there is support for LibWhisker's anti-IDS methods in case you want to give it a try (or test your IDS system).
- Not *every* check is a security problem, though most are. There are some items that are "info only" type checks that look for things that may not have a security flaw, but the webmaster or security engineer may not know are present on the server. These items are usually marked appropriately in the information printed. There are also some checks for unknown items which have been seen scanned for in log files.

SNAP OF KALI where we used NIKTO,



SERVER:

Microsoft –IIS/8.5

- **Weak or nonexistent authentication.** Authentication methods on the server may be unnecessarily weak. This permits an adversary to access the application, local data, or server data without first authenticating.

Vulnerability found:

The anti-click jacking X-Frame-Options header is not present.

CLICK JACKING:

Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.

PREVENTION:

Clickjacking attacks wrap a page the user trusts in an iframe, then renders invisible elements on top of the frame. To ensure that your site doesn't get used in a clickjacking attack, you need to make sure it cannot be wrapped in an iframe by a malicious site. This can be done by giving the browser instructions directly via HTTP headers, or in older browser by using client-side JavaScript (frame-killing).

LIMITATION:

- If the Clickjacking attack does not require the user to be authenticated, this attribute will not provide any protection.
- Additionally, while Same Site attribute is supported by most modern browsers, there are still some users (approximately 6% as of November 2020) with browsers that do not support it.
- The use of this attribute should be considered as part of a defence-in-depth approach, and it should not be relied upon as the sole protective measure against Clickjacking.

X-Frame

(XFO), is an HTTP response header, also referred to as an HTTP security header, which has been around since 2008. In 2013 it was officially published as RFC 7034, but is not an internet standard. This header tells your browser how to behave when handling your site's content. The main reason for its inception was to provide clickjacking protection by not allowing rendering of a page in a frame.

X-Frame Directives

1. Same origin_directive
2. Allow from uri –directive
3. Deny directive

IN OUR CASE _ VULNERABILITY HAVE DENY DIRECTIVE

FABRIKAM

Defending with X-Frame Options header:

- The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a <frame> or <iframe>.
- Sites can use this to avoid Clickjacking attacks, by ensuring that their content is not embedded into other sites.
- Set the X-Frame-Options header for all responses containing HTML content. The possible values are "DENY", "SAMEORIGIN", or "ALLOW-FROM uri

Vulnerability found:

The X-XSS-Protection header is not defined.

This header can hint to the user agent to protect a gainst some form of XSS

CROSS SITE-scripting

Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. It allows an attacker to circumvent the same origin policy, which is designed to segregate different websites from each other. Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform, and to access any of the user's data. If the victim user has privileged access within the application, then the attacker might be able to gain full control over all of the application's functionality and data.

IMPACT
of XSS vulitnerabilies.

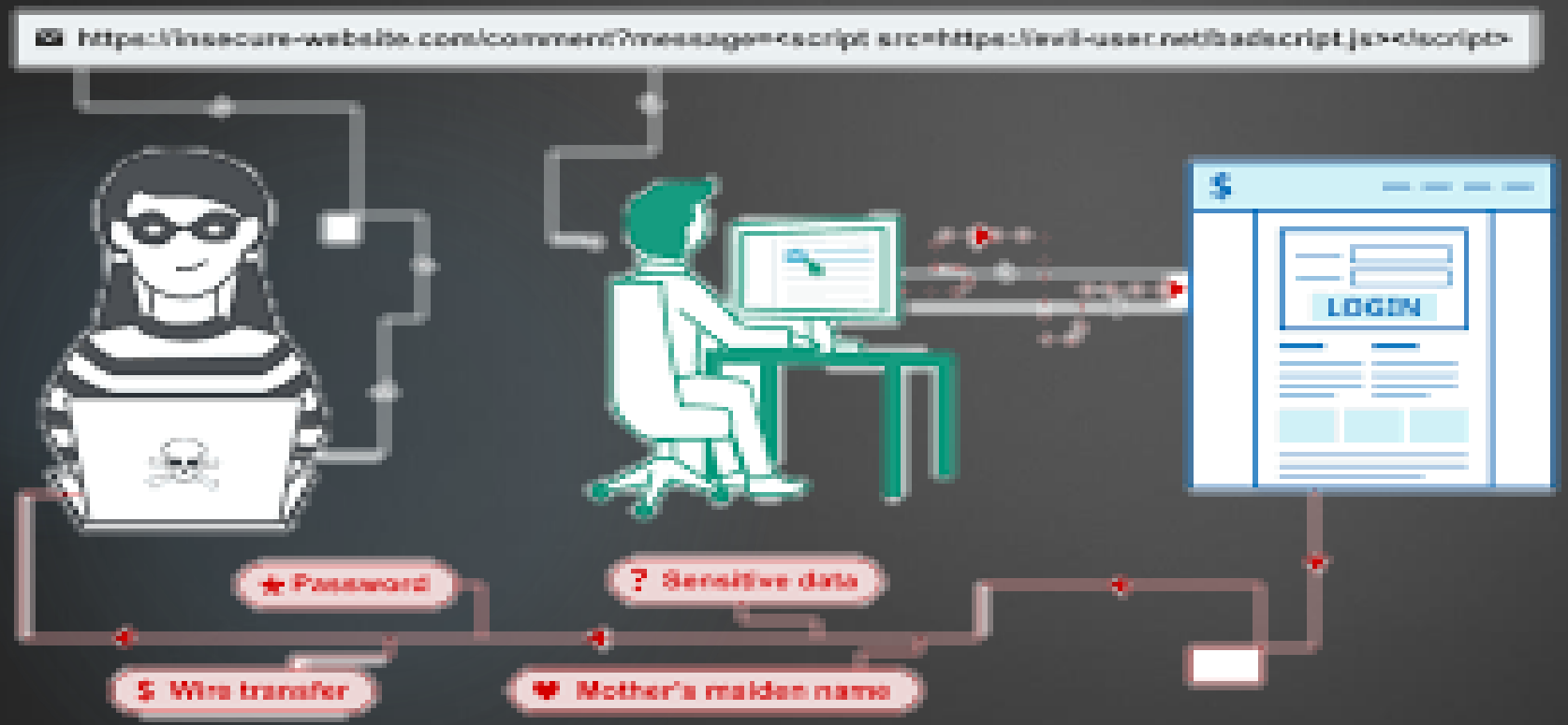
- In a brochureware application, where all users are anonymous and all information is public, the impact will often be minimal.
- In an application holding sensitive data, such as banking transactions, emails, or healthcare records, the impact will usually be serious.
- If the compromised user has elevated privileges within the application, then the impact will generally be critical, allowing the attacker to take full control of the vulnerable application and compromise all users and their data.

Requirement

of x- xss protection header

- THIS HEADER CAN HINT TO THE USER AGENT TO PROTECT AGAINST SOME FORMS OF XSS. THE HTTP X-XSS PROTECTION RESPONSE HEADER IS A FEATURE OFINTERNET EXPLORER, CHROME AND SAFARI THAT STOPS PAGES FROM LOADING WHEN THEY DETECT REFLECTED CROSS-SITE SCRIPTING (XSS) ATTACKS.

How does X-xss work ?



- Cross-site scripting works by manipulating a vulnerable web site so that it returns malicious JavaScript to users. When the malicious code executes inside a victim's browser, the attacker can fully compromise their interaction with the application.

Vulnerability found:

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

Vulnerability found:

Uncommon header: X-POWERED_BY_FLESK found with contents : PLESKWIN

Requirement

of x- xss protection header

- PLESK IS A GREAT CONTROL PANEL SYSTEM FOR VPS AND DEDICATED SERVERS BECAUSE ITS MENU IS END USER-FRIENDLY. IN OTHER WORDS, A SERVER UTILIZING PLESK IS SO EASY TO USE THAT ANYONE WITH LITTLE TO NO EXPERIENCE CAN START ADMINISTERING THEIR SERVER IMMEDIATELY.

PLESKWIN:

- THIS HEADER CAN HINT TO THE USER AGENT TO PROTECT AGAINST SOME FORMS OF XSS. THE HTTP X-XSS PROTECTION RESPONSE HEADER IS A FEATURE OFINTERNET EXPLORER, CHROME AND SAFARI THAT STOPS PAGES FROM LOADING WHEN THEY DETECT REFLECTED CROSS-SITE SCRIPTING (XSS) ATTACKS.

Vulnerability found:

Retrieved X-ASPNET version header: 4.0.30319

UNISCAN

Uniscan is a simple Remote File Include, Local File Include and Remote Command Execution vulnerability scanner.

Uniscan

Vulnerability Sc

Snap of using UNISCAN

```
File  Actions  Edit  View  Help
═══════════════════════════════════════════════════════════════
═
| Static tests:
| Plugin name: Local File Include tests v.1.1 Loaded.
| Plugin name: Remote Command Execution tests v.1.1 Loaded.
| Plugin name: Remote File Include tests v.1.1 Loaded.
|
|
| Local File Include:
|
|
| Remote Command Execution:
|
|
| Remote File Include:
═══════════════════════════════════════════════════════════════
═
Scan end date: 2-7-2021 4:33:1


HTML report saved in: report/jgec.ac.in.html

┌──(root💀kali)-[~/Desktop]
└─# 
```

Cross-Site Scripting (XSS):

Web Shell Finder:

STATIC TESTS

Local File Include:

Remote Command Execution:

Remote File Include:

SCAN TIME

Scan Finished: 2/7/2021 4:33:1

Report of UNISCAN

..\jgec.ac.in.html

Vulnerability found:

CRAWLER

```
Crawler Started:
Plugin name: External Host Detect v.1.2 Loaded.
Plugin name: E-mail Detection v.1.1 Loaded.
Plugin name: Code Disclosure v.1.1 Loaded.
Plugin name: Upload Form Detect v.1.1 Loaded.
Plugin name: Timthumb ⩽ 1.32 vulnerability v.1 Loaded.
Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
Plugin name: phpinfo() Disclosure v.1 Loaded.
Plugin name: FCKeditor upload test v.1 Loaded.
[+] Crawling finished, 555 URL's found!
```

CRAWLER

- A crawler is a program used by search engines to collect data from the internet.
- When a crawler visits a website it picks over the entire website's content (i.e. the text) and stores it in a databank. It also stores all the external and internal links to the website. The crawler will visit the stored links at a later point in time, which is how it moves from one website to the next. By this process the crawler captures and indexes every website that has links to at least one other website.

Vulnerability found:

EXTERNAL HOSTS:

EXTERNAL HOSTS

```
External hosts:
[+] External Host Found: https://cdn.rawgit.com
[+] External Host Found: https://stackpath.bootstrapcdn.com
[+] External Host Found: http://maxcdn.bootstrapcdn.com
[+] External Host Found: https://onlinecourses.nptel.ac.in
[+] External Host Found: http://s.w.org
[+] External Host Found: https://embed.tawk.to
[+] External Host Found: https://ajax.googleapis.com
[+] External Host Found: https://maxcdn.bootstrapcdn.com
[+] External Host Found: https://www.facebook.com
[+] External Host Found: https://www.ictema2020.com
[+] External Host Found: http://codersjgec.github.io
[+] External Host Found: http://fonts.googleapis.com
[+] External Host Found: https://cdn.jsdelivr.net
[+] External Host Found: https://www.instagram.com
[+] External Host Found: http://gmpg.org
[+] External Host Found: https://www.comsysconf.org
[+] External Host Found: http://vigyanchetana.in
[+] External Host Found: https://docs.google.com
[+] External Host Found: https://code.responsivevoice.org
[+] External Host Found: http://maps.googleapis.com
[+] External Host Found: http://nptel.ac.in
[+] External Host Found: https://www.googletagmanager.com
[+] External Host Found: http://cdnjs.cloudflare.com
[+] External Host Found: https://www.google.com
[+] External Host Found: https://unpkg.com
[+] External Host Found: http://nptelonlinecourses.iitm.ac.in
[+] External Host Found: https://goo.gl
[+] External Host Found: https://www.youtube.com
[+] External Host Found: https://cdnjs.cloudflare.com
```

Vulnerability found:

SOURCE CODE DISCLOSURE

```
Source Code Disclosure:

File Upload Forms:
[+] Upload Form Found: http://jgec.ac.in/TrekkersClub/blog.php
[+] Upload Form Found: http://jgec.ac.in/examination/update.html

Timthumb:
```

SOURCE CODE DISCLOSURE

Source code intended to be kept server-side can sometimes end up being disclosed to users. Such code may contain sensitive information such as database passwords and secret keys, which may help malicious users formulate attacks against the application

REMEDIATION

SOURCE CODE DISCLOSURE

- Server-side source code is normally disclosed to clients as a result of typographical errors in scripts or because of misconfiguration, such as failing to grant executable permissions to a script or directory. Review the cause of the code disclosure and prevent it from happening.

Vulnerability found:

WEB BACKDOORS:

WEB-BACKDOORS

When a site gets hacked, it seldom happens that the hacker has not left behind a malware to get access of the **website** again, in the future. This deliberate plantation of malicious codes in a **website** with an intention of further exploitation is known as "**website backdoor**".

How to protect against backdoor attacks?

Cloud Security Alliance noted that because many backdoor attacks are known for being able to prevent detection by many discovery tools, protecting against them can be difficult. However, there are strategies that can be leveraged to help reduce the risk of a breach of this kind.

"In this way, businesses should be choosy about the open-source applications they use and ensure that they come from a reputable source.

Network monitoring is also key when it comes to protection from backdoor attacks. Monitoring can help guarantee that any suspicious activity – such as information being gathered by a command and control server – is flagged with network administrators. IT staff can then react quickly to get to the root of the issue, stop the attack and mitigate any damage.

Another protection measure involves the use of an anti-malware solution. Trend Micro noted that because some backdoor attacks include the emulation of network traffic, the network activity therefore appears genuine and does not set off any alarms. However, an anti-malware system like Trend Micro Office Scan is able to detect backdoors if this kind.

Backdoor attacks present a considerable threat to businesses, but understanding how they happen and how they can be prevented can go a long way toward better protection.

Vulnerability found:

PHP INFO() DISCLOSURE:

```
PHPinfo() Disclosure:
[+] phpinfo() page: http://jgec.ac.in/phpinfo.php
        System: Windows NT SG2NWVPWEB070 6.3 build 9600 (Windows Server 2012 R2 Standard Edition)
i586
        PHP version: 5.6.40
        allow_url_fopen: On
        allow_url_include: Off
        disable_functions: <i>no value</i>
        OpenSSL Library Version: OpenSSL 1.0.2q  20 Nov 2018
```

PHP INFO disclosure

phpinfo() is a debug functionality that prints out detailed **information** on both the system and the **PHP** configuration.

An attacker can obtain **information** such as: Exact **PHP** version.

Exact OS and its version.

Vulnerability found:

TIMThumb

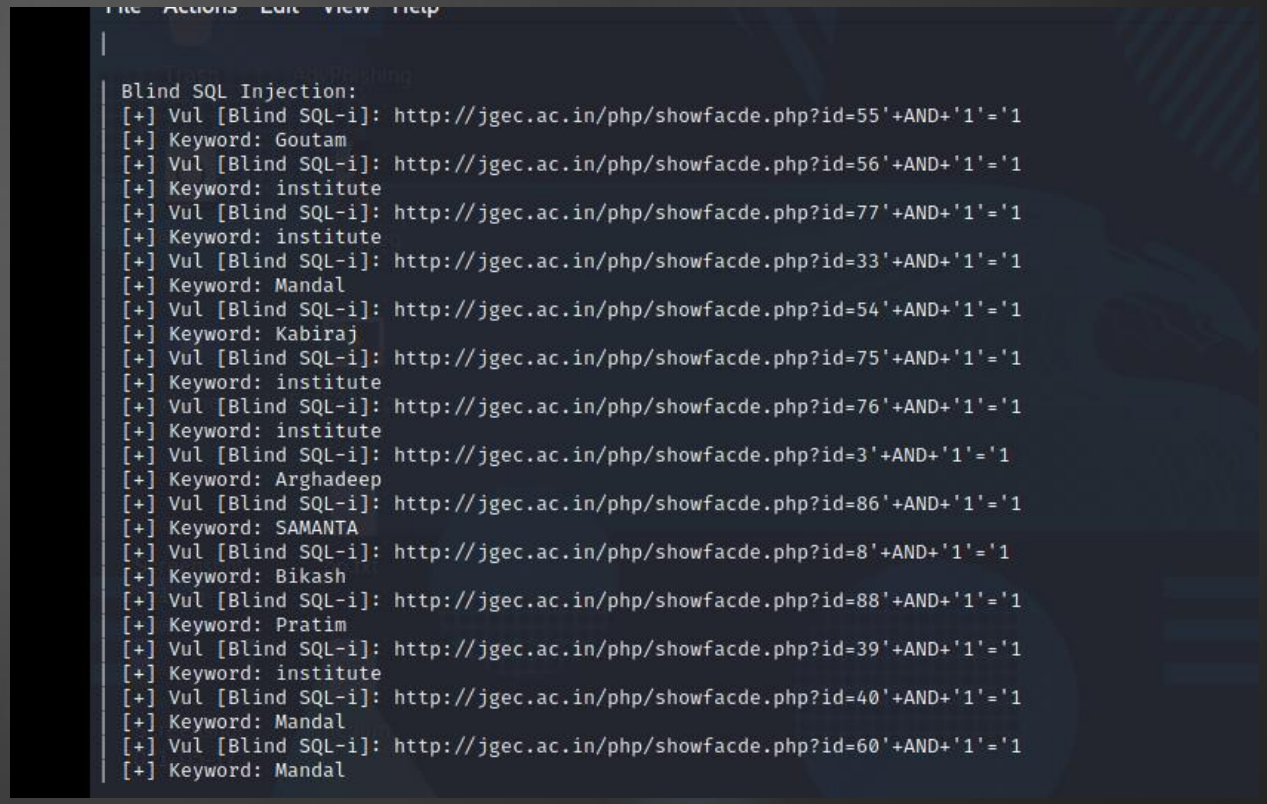
TimThumb is an image resizing script that many themes use or have used in the past. ... Different image sizes are created when images are uploaded, and WordPress uses the Featured Image for each post to determine which image to use as a thumbnail.

Vulnerability found:

BLIND SQL INJECTION

BLIND SQL injection

- Blind SQL (Structured Query Language) injection is a type of SQL Injection attack that asks the database true or false questions and determines the answer based on the applications response. This attack is often used when the web application is configured to show generic error messages, but has not mitigated the code that is vulnerable to SQL injection.



PREVENTION

- To protect yourself : Use secure coding practices, independent on the language. All common web development platforms (including of course PHP, Java, and ASP.NET but also Ruby or Python) have mechanisms that you can use to avoid SQL Injection vulnerabilities including Blind SQL Injections. Avoid dynamic SQL at all costs. The best choice is to use prepared statements also known as parameterized queries.

Vulnerability found:

PHP CGI ARGUMENT INJECTION

Remote code execution:

PHP is a widely-used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML. When PHP is used in a CGI-based setup (such as Apache's mod_cgid), the php-cgi receives a processed query string parameter as command line arguments which allows command-line switches, such as -s, -d or -c to be passed to the php-cgi binary, which can be exploited to disclose source code and obtain arbitrary code execution.

Email id that logged on this website , found through uniscan

E-mail Found: jhuma.dutta@rediffmail.com
E-mail Found: license@php.net
E-mail Found: principal@jgec.ac.in
E-mail Found: shamparoykarmakar@gmail.com
E-mail Found: rtitm@jgec.ac.in
E-mail Found: madhab_bec@rediffmail.com
E-mail Found: bcmjgec@gmail.com
E-mail Found: subratamech@rediffmail.com
E-mail Found: joe@example.com
E-mail Found: chakraborty.avik.ece@gmail.com
E-mail Found: chinmoyslg@gmail.com
E-mail Found: royghosh2015@gmail.com
E-mail Found: naim.hossain@me.jgec.ac.in
E-mail Found: nripen_mondal@rediffmail.com
E-mail Found: shrayasi.datta@gmail.com
E-mail Found: j.mehedi@gmail.com
E-mail Found: arup_paul05@rediff.com
E-mail Found: sumanta_munshi@rediffmail.com
E-mail Found: arijit.kundu@me.jgec.ac.in
E-mail Found: shubhasish.sarkar18@gmail.com
E-mail Found: nm1231@gmail.com
E-mail Found: mirwaiz.rahaman@ece.jgec.in
E-mail Found: debaratisahasarkar@gmail.com
E-mail Found: ad2106@ece.jgec.ac.in
E-mail Found: madhu.lusai@gmail.com
E-mail Found: basu.purba@gmail.com
E-mail Found: swarup11samanta@gmail.com
E-mail Found: suman.koner@gmail.com
E-mail Found: samirdas.jgec@gmail.com

Source Code Disclosure:

File Upload Forms:
Upload Form Found: http://jgec.ac.in/TrekkersClub/blog.php
Upload Form Found: http://jgec.ac.in/examination/update.html

Timthumb:

Web Backdoors:

E-mails:
E-mail Found: mafeezul_islam@rediffmail.com
E-mail Found: sagarnil2@rediffmail.com
E-mail Found: sandipan.ganguly24@gmail.com
E-mail Found: def@somemail.com
mail Found: smitra2000@gmail.com
mail Found: a.mahapatra2000@gmail.com
mail Found: souvikdatta.ju@gmail.com
mail Found: dipak.kole@cse.jgec.ac.in
mail Found: xxx@gmail.com
mail Found: verification@jgec.ac.in
mail Found: subhas.barman@gmail.com
mail Found: mandal_skm@rediffmail.com
mail Found: gcchell@rediffmail.com
mail Found: placement@jgec.ac.in
mail Found: noreply@sg2nwvpweb070.shr.prod.sin2.secureserver.net
mail Found: bo@example.com
mail Found: ashim_roy67@rediffmail.com
mail Found: angie@example.com
mail Found: mary@example.com
mail Found: ukmandalce@gmail.com
mail Found: gpandaee@gmail.com
mail Found: sp2131@it.jgec.ac.in
mail Found: mousarkar_jgec@rediffmail.com
mail Found: mytry007@gmail.com
mail Found: debamitasingha@gmail.com
mail Found: alokesh1982@gmail.com
mail Found: trekkersclub@jgec.ac.in
mail Found: ujjaldey54@gmail.com
mail Found: amitgupta4in@gmail.com
mail Found: gb_civil@rediffmail.com
mail Found: sudipmukherjee_63@rediffmail.com
mail Found: arghadeep.biswas@gmail.com
mail Found: grievancecell@jgec.ac.in
mail Found: haldarshobhraj78@gmail.com
mail Found: hazraanimesh53@gmail.com
mail Found: edc@jgec.ac.in
mail Found: tapati.kana.mondal@ee.jgec.ac.in
mail Found: santanu.das@ee.jgec.ac.in
mail Found: bhaskarlodh@jgec.ac.in
mail Found: jcvc@jgec.ac.in
mail Found: tanmoypaul856@gmail.com

Conclusion

FROM THE ABOVE SLIDE you can see vulnerability is proved that is , webpage or our object www.jgec.ac.in can easily be exploited and hence its data is not safe and any hacker can easily carried out these data. A **cyber attack** can maliciously disable computers, steal data, or use a breached computer as a launch point for other **attacks.** Cyberattacks against web applications occur every day.

ACKNOWLEDGEMENT

I WOULD LIKE TO THANK MY ETHICAL HACKING TRAINNER : MR.SWASTIK DEY & MR.IMRAN ROSHAN. AND ALSO MY HOD Prof. SABYASACHI BAGCHI.

WHO GAVE US THE OPPORTUNITY TO LEARN ETHICAL HACKING FROM TEAM COGNITO.

THANKYOU