DefenseCode

WebScanner Report

Software version: v2.0
27/2/2019 3:27:31 PM

General Information

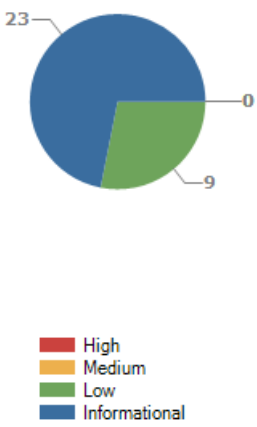
Project Name	Testing Scanner
Company Name	E-SPIN
Author Name	E-Spin
Contact E-mail	support@e-spincorp
Brief Description	here is example report using DefenseCode web scanner

Scan Information

Target URL	https://www.hackthissite.org/.
Scan time	00:12:23
Configuration profile	Default
Links processed	786

Description

Total vulnerabilities found	32
Threat level	9 (Low)
Additional note	



V U L N E R A B I L I T I E S

WebScanner has discovered one or more level 1 (low severity) vulnerabilities in target application. These vulnerabilities could be exploited by malicious users. Please check out the specific vulnerability's recommended actions in order to improve your website's security!

1 Internal Server Error Low

Description

The server responded with an HTTP status 500, indicating there is a server-side error. Reasons may vary, and the behavior should be analyzed carefully.

Solution

For appropriate solution specific to this vulnerability please visit http://www.defensecode.com/public/web_vulns/introduction.html

Vulnerable Files:

/forums/viewtopic.php **Risk: Low**

URL	https://www.hackthissite.org/forums/viewtopic.php?f=160&t=14048
Method	GET
HTTP Code Line	HTTP/1.1 500 Internal Server Error
Arguments	f=160&t=14048
Vulnerable Arguments	f
Vulnerability Match	Internal Server Error
Vulnerability Test Value	

Request:

```
GET /forums/viewtopic.php?f=160&t=14048 HTTP/1.0
Cookie: PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko)
Host: www.hackthissite.org
```

Description

The web page may disclose the physical path of the web root. While physical path disclosure is not a severe vulnerability by itself, this information can be leveraged by an attacker in combination with other vulnerabilities

Solution

For appropriate solution specific to this vulnerability please visit http://www.defensecode.com/public/web_vulns/introduction.html

Vulnerable Files:

/pages/programs/programs.php Risk: Low

URL	https://www.hackthissite.org/pages/programs/programs.php
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	x:\Documents and Settings\
Vulnerability Test Value	

Request:

```
GET /pages/programs/programs.php HTTP/1.0
Cookie: PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko)
Host: www.hackthissite.org
```

/user/view/oasis Risk: Low

URL	https://www.hackthissite.org/user/view/oasis
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	C:/Scotland/UK/
Vulnerability Test Value	

Request:

GET /user/view/oasis HTTP/1.0
Cookie:
PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAGEO=MY%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C;phpbb3_28pla_u=1;phpbb3_28pla_k=;phpbb3_28pla_sid=2742116b28379d2c56f4499250568a2e;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org

/pages/programs/programs.php **Risk: Low**

URL	https://www.hackthissite.org/pages/programs/programs.php?class=2
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	class=2
Vulnerable Arguments	class
Vulnerability Match	x:\Documents and Settings\
Vulnerability Test Value	

Request:

GET /pages/programs/programs.php?class=2 HTTP/1.0
Cookie:
PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAGEO=MY%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C;phpbb3_28pla_u=1;phpbb3_28pla_k=;phpbb3_28pla_sid=2742116b28379d2c56f4499250568a2e;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org
Referer: https://www.hackthissite.org/pages/programs/programs.php

/pages/programs/programs.php **Risk: Low**

URL	https://www.hackthissite.org/pages/programs/programs.php?os=2
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	os=2
Vulnerable Arguments	os
Vulnerability Match	x:\Documents and Settings\
Vulnerability Test Value	

Request:

GET /pages/programs/programs.php?os=2 HTTP/1.0
Cookie:
PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAGEO=MY%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C;phpbb3_28pla_u=1;phpbb3_28pla_k=;phpbb3_28pla_sid=2742116b28379d2c56f4499250568a2e;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org
Referer: https://www.hackthissite.org/pages/programs/programs.php

/pages/programs/programs.php

Risk: Low

URL	https://www.hackthissite.org/pages/programs/programs.php?cat=7
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	cat=7
Vulnerable Arguments	cat
Vulnerability Match	x:\Documents and Settings\
Vulnerability Test Value	

Request:

GET /pages/programs/programs.php?cat=7 HTTP/1.0
Cookie:
PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAGEO=MY%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C;phpbb3_28pla_u=1;phpbb3_28pla_k=;phpbb3_28pla_sid=2742116b28379d2c56f4499250568a2e;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org
Referer: https://www.hackthissite.org/pages/programs/programs.php

Description

The robots.txt is a file located in the root directory of a website. This file is used by the web site owners to provide information about which parts of their site are not to be accessed by the web crawlers ("robots", search engines). This is called The Robots Exclusion Protocol.

Solution

For appropriate solution specific to this vulnerability please visit http://www.defensecode.com/public/web_vulns/introduction.html

Vulnerable Files:

/robots.txt **Risk: Low**

URL	https://www.hackthissite.org/robots.txt
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	
Vulnerability Test Value	

Request:

```
GET /robots.txt HTTP/1.0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko)
Host: www.hackthissite.org
```

4 Session Cookie not set to HTTPOnly Low

Description

HTTPOnly option limits session cookie to transmissions on HTTP (or HTTPS), thus restricting access from other, non-HTTP APIs (such as JavaScript). As not set it makes a threat of session cookie theft via cross-site scripting (XSS).

Solution

For appropriate solution specific to this vulnerability please visit http://www.defensecode.com/public/web_vulns/introduction.html

Vulnerable Files:

/ **Risk: Low**

URL	https://www.hackthissite.org/.
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	
Vulnerability Test Value	

Request:

GET /. HTTP/1.0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org

5 X-Frame-Options Header Not Set Low

Description

The X-Frame-Options HTTP response header can be used to indicate whether a browser should be allowed to render a page inside a frame or iframe. Sites could use this to avoid clickjacking attacks by ensuring that their content is not embedded into other sites.

Solution

For appropriate solution specific to this vulnerability please visit http://www.defensecode.com/public/web_vulns/introduction.html

Vulnerable Files:

/ **Risk: Low**

URL	https://www.hackthissite.org/
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	X-Frame-Options
Vulnerability Test Value	

Request:

```
GET / HTTP/1.0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko)
Host: www.hackthissite.org
```

Description

Applications can sometimes leak information in form of version numbers, debugging information, error messages, system data, directory pathing and so on. This information can be used by an attacker to get in depth knowledge about the system.

Solution

For appropriate solution specific to this vulnerability please visit http://www.defensecode.com/public/web_vulns/introduction.html

Vulnerable Files:

/donate/ Risk: Informational

URL	https://www.hackthissite.org/donate/
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	donate@hackthissite.org, donate@hackthissite.org
Vulnerability Test Value	

Request:

```
GET /donate/ HTTP/1.0
Cookie: PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko)
Host: www.hackthissite.org
```

/advertise/ Risk: Informational

URL	https://www.hackthissite.org/advertise/
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	advertising@hackthissite.org, advertising@hackthissite.org, advertising@hackthissite.org

Vulnerability Test Value	

Request:

GET /advertise/ HTTP/1.0
Cookie: PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org

/pages/programs/programs.php **Risk: Informational**

URL	https://www.hackthissite.org/pages/programs/programs.php
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	ryanb58@100wpd.com
Vulnerability Test Value	

Request:

GET /pages/programs/programs.php HTTP/1.0
Cookie: PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org

/news/view/703 **Risk: Informational**

URL	https://www.hackthissite.org/news/view/703
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	andrewalanhacks@gmail.com, hdmoore.hacks@gmail.com
Vulnerability Test Value	

Request:

GET /news/view/703 HTTP/1.0
Cookie: PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org

/news/view/696

Risk: Informational

URL	https://www.hackthissite.org/news/view/696
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	reputablehacker@gmail.com
Vulnerability Test Value	

Request:

GET /news/view/696 HTTP/1.0
Cookie: PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org

/register/submit

Risk: Informational

URL	https://www.hackthissite.org/register/submit
Method	POST
HTTP Code Line	HTTP/1.1 200 OK
Arguments	username=%27+or+%27%27%3D%27&password=%27+or+%27%27%3D%27&password2=%27+or+%27%27%3D%27&question=1&answer=1&answer2=1&email=WebScan%40WebScannerEmailAddress.com&email2=WebScan%40WebScannerEmailAddress.com&on&validation=1&submit=1
Vulnerable Arguments	username
Vulnerability Match	WebScan@WebScannerEmailAddress.com, WebScan@WebScannerEmailAddress.com
Vulnerability Test Value	

Request:

POST /register/submit HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Cookie:
PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAGEO=MY%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org

username=%27+or+%27%27%3D%27&password=%27+or+%27%27%3D%27&password2=%27+or+%27%27%3D%27&question=1&answer=1&answer2=1&email=WebScan%40WebScannerEmailAddress.com&email2=WebScan%40WebScannerEmailAddress.com&on&validation=1&submit=1

/advertise

Risk: Informational

URL	https://www.hackthissite.org/advertise
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	advertising@hackthissite.org, advertising@hackthissite.org, advertising@hackthissite.org
Vulnerability Test Value	

Request:

GET /advertise HTTP/1.0
Cookie:
PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAGEO=MY%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org

/articles/read/1142

Risk: Informational

URL	https://www.hackthissite.org/articles/read/1142
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	

Vulnerability Match	boschhacklord@gmail.com, hack.consultant@hackermail.com, hack.consultant@hackermail.com
Vulnerability Test Value	

Request:

GET /articles/read/1142 HTTP/1.0
Cookie:
PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAGEO=MY%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C;phpbb3_28pla_u=1;phpbb3_28pla_k=;phpbb3_28pla_sid=2742116b28379d2c56f4499250568a2e;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org

/articles/read/1143

Risk: Informational

URL	https://www.hackthissite.org/articles/read/1143
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	svitransport2014@gmail.com, navilaquader@gmail.com
Vulnerability Test Value	

Request:

GET /articles/read/1143 HTTP/1.0
Cookie:
PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAGEO=MY%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C;phpbb3_28pla_u=1;phpbb3_28pla_k=;phpbb3_28pla_sid=2742116b28379d2c56f4499250568a2e;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org

/user/view/limdis

Risk: Informational

URL	https://www.hackthissite.org/user/view/limdis
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	

Vulnerability Match	limdis@hackthissite.org, Alexhopper112@gmail.com
Vulnerability Test Value	

Request:

GET /user/view/limdis HTTP/1.0
Cookie:
PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAGEO=MY%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C;phpbb3_28pla_u=1;phpbb3_28pla_k=;phpbb3_28pla_sid=2742116b28379d2c56f4499250568a2e;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org

/news/view/696/

Risk: Informational

URL	https://www.hackthissite.org/news/view/696/
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	reputablehacker@gmail.com
Vulnerability Test Value	

Request:

GET /news/view/696/ HTTP/1.0
Cookie:
PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAGEO=MY%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C;phpbb3_28pla_u=1;phpbb3_28pla_k=;phpbb3_28pla_sid=2742116b28379d2c56f4499250568a2e;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org

/news/view/703/2/30

Risk: Informational

URL	https://www.hackthissite.org/news/view/703/2/30
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	

Vulnerability Match	lawyer@presidency.com, me.....lawyer@presidency.com, lawyer@presidency.com, lawyer@presidency.com, me.....lawyer@presidency.com, lawyer@presidency.com
Vulnerability Test Value	

Request:

GET /news/view/703/2/30 HTTP/1.0
Cookie:
PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAGEO=MY%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C;phpbb3_28pla_u=1;phpbb3_28pla_k=;phpbb3_28pla_sid=2742116b28379d2c56f4499250568a2e;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org

/news/view/703/ **Risk: Informational**

URL	https://www.hackthissite.org/news/view/703/
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	andrewalanhacks@gmail.com, hdmoore.hacks@gmail.com
Vulnerability Test Value	

Request:

GET /news/view/703/ HTTP/1.0
Cookie:
PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAGEO=MY%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C;phpbb3_28pla_u=1;phpbb3_28pla_k=;phpbb3_28pla_sid=2742116b28379d2c56f4499250568a2e;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org

/user/view/mShred **Risk: Informational**

URL	https://www.hackthissite.org/user/view/mShred
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	

Vulnerable Arguments	
Vulnerability Match	mShred@hackthissite.org
Vulnerability Test Value	

Request:

GET /user/view/mShred HTTP/1.0
Cookie:
PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAGEO=MY%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C;phpbb3_28pla_u=1;phpbb3_28pla_k=;phpbb3_28pla_sid=2742116b28379d2c56f4499250568a2e;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org

/user/view/monstar%20boy

Risk: Informational

URL	https://www.hackthissite.org/user/view/monstar%20boy
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	Softwaretecnology.hk@gmail.com
Vulnerability Test Value	

Request:

GET /user/view/monstar boy HTTP/1.0
Cookie:
PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAGEO=MY%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C;phpbb3_28pla_u=1;phpbb3_28pla_k=;phpbb3_28pla_sid=2742116b28379d2c56f4499250568a2e;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org

/user/view/Nia777

Risk: Informational

URL	https://www.hackthissite.org/user/view/Nia777
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	Softwaretecnology.hk@gmail.com

Vulnerability Test Value	

Request:

GET /user/view/Nia777 HTTP/1.0
Cookie:
PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAGEO=MY%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C;phpbb3_28pla_u=1;phpbb3_28pla_k=;phpbb3_28pla_sid=2742116b28379d2c56f4499250568a2e;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org

/user/view/HackThisSite%20Staff

Risk: Informational

URL	https://www.hackthissite.org/user/view/HackThisSite%20Staff
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	admin@hackthissite.org, g1tha741741@yahoo.com.thak
Vulnerability Test Value	

Request:

GET /user/view/HackThisSite Staff HTTP/1.0
Cookie:
PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAGEO=MY%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C;phpbb3_28pla_u=1;phpbb3_28pla_k=;phpbb3_28pla_sid=2742116b28379d2c56f4499250568a2e;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org

/user/view/jakkmullahmullah

Risk: Informational

URL	https://www.hackthissite.org/user/view/jakkmullahmullah
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	Softwaretecnology.hk@gmail.com
Vulnerability Test Value	

Request:

GET /user/view/jakkmullahmullah HTTP/1.0
Cookie:
PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAGEO=MY%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C;phpbb3_28pla_u=1;phpbb3_28pla_k=;phpbb3_28pla_sid=2742116b28379d2c56f4499250568a2e;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org

/user/view/LoyalBlackspider

Risk: Informational

URL	https://www.hackthissite.org/user/view/LoyalBlackspider
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	scottstilinski20@gmail.com, scottstlinski20@gmail.com, scottstlinski20@gmail.com
Vulnerability Test Value	

Request:

GET /user/view/LoyalBlackspider HTTP/1.0
Cookie:
PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAGEO=MY%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C%7C;phpbb3_28pla_u=1;phpbb3_28pla_k=;phpbb3_28pla_sid=2742116b28379d2c56f4499250568a2e;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.hackthissite.org

/user/view/prof_zee

Risk: Informational

URL	https://www.hackthissite.org/user/view/prof_zee
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	tafadzwaephraim@gmail.com
Vulnerability Test Value	

Request:

```
GET /user/view/prof_zee HTTP/1.0
Cookie:
PHPSESSID=f23jd2blajfev9rmeis6v38sm7;OAGEO=MY%7C%7C%7C%7C%7C
%7C%7C%7C%7C%7C;phpbb3_28pla_u=1;phpbb3_28pla_k=;phpbb3_28pla_
sid=2742116b28379d2c56f4499250568a2e;OAID=deleted
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko)
Host: www.hackthissite.org
```

Description

Auto-complete stores completed form field and passwords locally in the browser, so that these fields are filled automatically when the user visits the site again. Sensitive data and passwords can be stolen if the user's system is compromised.

Solution

For appropriate solution specific to this vulnerability please visit http://www.defensecode.com/public/web_vulns/introduction.html

Vulnerable Files:

/user/login — Risk: Informational

URL	https://www.hackthissite.org/user/login
Method	POST
HTTP Code Line	
Arguments	Form: https://www.hackthissite.org/user/login
Vulnerable Arguments	Form: https://www.hackthissite.org/user/login
Vulnerability Match	Password Input Type
Vulnerability Test Value	

Request:

/register/submit — Risk: Informational

URL	https://www.hackthissite.org/register/submit
Method	POST
HTTP Code Line	
Arguments	Form: https://www.hackthissite.org/register/submit
Vulnerable Arguments	Form: https://www.hackthissite.org/register/submit
Vulnerability Match	Password Input Type
Vulnerability Test Value	

Request:

Description

HTTP Server Disclosure allows potential attackers to determine known vulnerabilities and the appropriate exploits to use during attacks.

Solution

For appropriate solution specific to this vulnerability please visit http://www.defensecode.com/public/web_vulns/introduction.html

Vulnerable Files:

/ **Risk: Informational**

URL	https://www.hackthissite.org/.
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	HackThisSite Load Balancer v2
Vulnerable Arguments	HackThisSite Load Balancer v2
Vulnerability Match	HackThisSite Load Balancer v2
Vulnerability Test Value	

Request:

```
GET /. HTTP/1.0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko)
Host: www.hackthissite.org
```