

1. Injection:

SQL Injection: (←) → 健 @ Attps://phpapp.infosecaddicts.com ... ⊠ ∾ ☆ 👱 III\ 🗉 🤪 📥 🍪 📽 ≗ ©- ∃ ΤΘ ACMELAPTOP Register Acme is an online website where you can sell your laptop or services Dell Gate e PC^{*} S101 Hewl Ibm Sony acer | Intel Core2 Duo 2.0GHz / Glossy 15.6" WXGA high-definition widescreen display / 2GB DDR2 SDRA aq | Intel Core 2 Duo 2.1GHz / 4GB

Buying a laptop

| | ACMELAPTOP | | | | | | | |
|----|------------|--------|--------------------|-----------|--|---------|--|--|
| Ca | egories | Home | Buy | Career | About us | Contact | | |
| > | Acer | Compag | | | | | | |
| > | Compaq | Compaq | | | | | | |
| > | Dell | | Company | | Compaq Intel Core 2 Duo 2.1GHz / 4GB memory / 320GB hard drive / DVD�RW/DVD-RAM/DVD+R | | | |
| > | Gateway | 22.53 | Compadi | | | | | |
| > | Hewlett | | | # Box New | Double Layer | | | |
| > | lbm | | | | | | | |
| > | Sony | | | | | | | |
| > | Toshiba | | | | | | | |
| - | | | Home I Contact I I | on in I | | | | |

Forcing application to throw error message by entering a single (') in place of a number

| | phpapp.infosecaddicts.com/acre | | 👱 III\ 🖽 😽 🗕 I | 🕼 🖷 🕇 🧿 35 Gr = | | | | |
|------------|--------------------------------|---------------------|----------------|---|---|--|--|--|
| ACMELAPTOP | Register | | | | | | | |
| Categories | Home | Buy | Career | About us | Contact | | | |
| > Acer | Compag | | | | | | | |
| > Compaq | oompaq | | | | | | | |
| > Dell | TA SUBAR | Compact | | Compag Intel Core 2 Duo 2.1GHz / 4GB memory / | | | | |
| > Gateway | 2010 | Company - | | | 320GB hard drive / DVD RW/DVD-RAM/DVD+R | | | |
| > Hewlett | | | 🔐 Buy Now | Double Layer | | | | |
| > Ibm | | | | | | | | |
| > Sony | | - | | | | | | |
| > Toshiba | | | | | | | | |
| | | Home Contact Li | og in | | | | | |

Result:

| | ACM | ELAPTOF | Register | | | | | |
|----|------------|---------|----------|-----|-----|-----|----------|---------|
| Ca | tegories | | Home | Buy | Car | eer | About us | Contact |
| > | Acer | | | | | | | |
| > | Compaq | | | | | | | |
| > | Dell | | | | | | | |
| > | Gateway | | | | | | | |
| > | Hewlett | | | | | | | |
| > | Ibm | | | | | | | |
| > | Sony | | | | | | | |
| > | Toshiba | | | | | | | |

You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near "Compaq" at line 1



Bypassing Authentication:

Go to login page:

| Home | Buy |
|----------------------------|-------|
| LICEDNAME. | [] |
| USERINAME. | |
| PASSWORD: | |
| | Login |
| Attempt to fill out login | form: |
| USERNAME: shinobibughunter | |
| PASSWORD: | |

Hello "shinobibughunter", Password failed, if you have forgotten your password, click on forgot password.

Unable to login to application, but it does give information about how to further attack password.

2. Broken Authentication & Session Managment:

Brute Forced Login:

Go to Login Page:

| Home | Buy |
|------------------------|-------|
| USERNAME: PASSWORD: | |
| | Login |

Attempt to fill out the page and Capture with Burp's Proxy:



| Request | Response | |
|---------|----------|---|
| | | _ |

InfoSecAddicts

 Request Response

 Raw Params Headers Hex

 GET /login.php?error=Invalid+Paasword+tusername=test HTTP/1.1

 Most: phpape.infosecaddicts.com

 User-Agent: Kozill425.0 (Macintosh; Intel Kac OS X 10.13; rv:68.0) Gecko/20100101 Pirefox/68.0

 Accept: text/html,application/xhtml*xml,application/xml;g=0.9,*/*;g=0.8

 Accept-Encoding: gsip, deflate

 Referen: https://phpape.infosecaddicts.com

 Conction: close

 Conction: close

 Cocki: ____fdid=6029645e59a793349b3b819dae03f6e1564954288; _ga=Gal.2.781573113.1564954291; _asc=4=20d75b16c5e988ea135b1a1af;

 __tarkwoid=stinfosecaddicts.com:ApekTxgFrGüh88K0mg8xwoicFPurW+599KBtd825w0ontFQ=agWTRXHCBhX//::2; _atrips_mid=b53f835b-625c-4a04-8fe8-075c7bbca7cf;

 _fbp=fb.1.1564955138350-417041806; _gid=Gal.2.1143145789.1566082771; PMPAESEID=ng1rns9ge2abpad71nr6p4c6a3; _gat=1

Send to Intruder:

| Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts | | | |
|----------|--|--|---|---|--|---|--|--|--|---|---|------------------------------|---|--|---------------------------------------|
| 6 × . |] | | | | | | | | | | | | | | |
| Target | Positions Payloads Options | | | | | | | | | | | | | | |
| Pa Co | Payload Positions Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details. | | | | | | | | Start attack | | | | | | |
| At | Attack type: Sniper | | | | | | | | | | | | | | |
| | ist /ac ist: phi er-Age copt-1 copt-1 copt-2 forer:: istent intent | hentica app.inf ts: Kozi ext/hum nguager coding: https:/ yype: ap angth: on: clos cfduid d=erin .15695 (nscore testfre | te.php H1 Osecaddic 11a/5.0 ; 1,aplic. en-US,en gSID, di /phpapp.: plication 55 en =dc602964 fosecadd 5153850.4 -Regrest: sponse=21 | rrp/1.1 Ha.com Nacintoa Hioritoa Hioritoa Hioritaeo Nacourtoa Hioritaeo Hior | h; Intel ml+xml,ap dicta.com orm-urlen Habib019 :AptkfxgF ;gid=GA 5002997f4 | <pre>4ac OS X 10 plication/x (login.php? roded dae03f6e156 r6cath88x8rg L.2.1143145 ae3f1a09160</pre> | .13; rv:0 ml;q=0.9, error=Inn 4954200; 83#vvakfpn 789.15660 66 | 0.0) Gecks */*:g=0.8 *alid*Paaam _ga=GA1.2 uRU*559Ks 82771; PH3 | o/20100101 eord+50aer .701573113 d025ecent srssi0=ng | Firefox/60.0 name-ahinobibu .1564954281; rgr-agutaxa lrna9qe2abpad1 | ghunter _suc=4=204756 X//112; _str Lar6p406a3; _ | ol€c5e90 ipe_mid gat=1 | Men 13 bila isf; elsystatis-djac-da04-affat-affat Tabea Tef; | | Add § Clear § Auto § Refresh |

Select the attack:

| 1.01 | get rosmons | rayioaus | options | | | | | | | |
|------|--|--|---------------------------------|--------------------------|--------------------|--|--|--|--|--|
| ? | Payload Sets Two can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be custamized in different ways. | | | | | | | | | |
| | Payload set: 1 Payload count: 3 | | | | | | | | | |
| | Payload type: | Simple list | ¥ | Request count: 6 | | | | | | |
| ? | Payload Op This payload Paste Load Remove Clear | tions [Sim type lets you test Chris shinobibug | ple list] configure a simple | list of strings that are | rused as payloads. | | | | | |
| | Add | | | | | | | | | |
| | Add from list (Pro version only) | | | | | | | | | |

Start attack:



| Attack Save Columns | | | | | | | | | |
|---------------------|---------------------------|-------------------|-------------|------------|-------------|------------|----------|--------------------------|-----------|
| Results | Target Po | ositions Payloads | Options | | | | | | |
| Filter: Show | Filter: Showing all items | | | | | | | | |
| Request 🔺 | Position | Payload | | Status | Error | Timeout | Length | Comment | |
| 0 | | | | 302 | | | 580 | · · · | - |
| 1 | 1 | test | | 302 | | | 580 | | |
| 2 | 1 | Chris | | 302 | | | 581 | | |
| 3 | 1 | shinobibughunter | | 302 | | | 592 | | |
| 4 | 1 | G3t1n135 | | 302 | | | 584 | | |
| 5 | 1 | password | | 302 | | | 584 | | |
| 6 | 1 | 123 | | 302 | | | 579 | | |
| 7 | 2 | test | | 302 | | | 580 | | |
| 8 | 2 | Chris | | 302 | | | 580 | | |
| 9 | 2 | shinobibughunter | | 302 | | | 580 | | |
| 10 | 2 | G3t1n135 | | 302 | | | 580 | | |
| 11 | 2 | password | | 302 | | | 580 | | |
| 12 | 2 | 123 | | 302 | | | 580 | | |
| | | | | | | | | | |
| Request | Bernance | L | | | | | | | |
| Request | Response | | | | | | | | |
| Raw Pa | rams Head | ders Hex | | | | | | | |
| POST /aut | enticate. | php HTTP/1.1 | | | | | | | |
| Hoat: php: | upp.infoae | caddicts.com | | | | | | | |
| User-Agent | : Nozilla | 1/5.0 (Macintosh; | Intel Mac | OS X 1 | 0.13; rv: | 68.0) Geck | co/20100 |)101 Firefox/68.0 | |
| Accept: to | at/ntmit,a | u-US.ento=0.5 | -xmr, abbri | LC ATION / | xiii1;q-0.9 | ,^/^;y=0.c | , | | |
| Accept-End | oding: gz | ip, deflate | | | | | | | |
| Referer: | ittpa://ph | papp.infosecaddi | cta.com/lc | ogin.php | ?error=In | valid+Pass | word+&u | aername=ahinobibughunter | |
| Content-Tj | pe: appli | cation/x-www-for | m-urlencod | bed | | | | | |
| Connection | : close | | | | | | | | |
| Cookie: _ | cfduid=do | 6029645e59a79334 | 9535819dae | 03f6e15 | 64954288 | _ga=GA1.2 | .781579 | 113.1564954291; | • |
| ? < | + | > Type a search | term | | | | | | 0 matches |
| Finished | | | | | | | | | |

Attempt information findings:

| Home | • | | Bu | у | | | | |
|------------|--------------|---------------------------|-------------------------------------|----------|---------|--|--|--|
| | | | | | | | | |
| USERNAM | E: | shinobibu | ghunter | | | | | |
| | | | - | | | | | |
| PASSWORI | D: | ****** | | | | | | |
| | | Login | | | | | | |
| | | | | | | | | |
| Results: | | | | | | | | |
| ACMELAPTOP | | Hey | y ! Shinobibughunter Wel | -Come | | | | |
| Categories | Home | Buy | Career | About us | Contact | | | |
| > Acer | | Acme is an online website | where you can sell your laptop or s | ervices | | | | |
| - Dell | See PC \$101 | | | | | | | |





3. Cross-Site Scripting (XSS):

Reflected XSS:

| С | Open Contact Us page: | | | | | | | | | |
|-----|---|----------------------------|------------------------------|--|--|--|--|--|--|--|
| ¢ | $ \begin{array}{c} \leftarrow \rightarrow \\ \bigcirc \\ \bigcirc \\ \blacksquare \\ \end{array} \begin{array}{c} \bigoplus \\ \blacksquare \\$ | | | | | | | | | |
| | ACMELAPTOP | | | | | | | | | |
| Cat | tegories Home Buy Career About us Contact | | | | | | | | | |
| > | Acer | contactus | | | | | | | | |
| > | Compaq | contactus | | | | | | | | |
| > | Dell | 1116 Old Brike Road, Kensa | s City, MA | | | | | | | |
| > | Gateway | Phone - 1-800-LAPTOP | | | | | | | | |
| > | Hewlett | Email - info@acmelanton.co | m | | | | | | | |
| > | Ibm | Linar - mo@acheaptop.co | Email - Intogracmelaptop.com | | | | | | | |
| > | Sony | http://acmelaptop.com | http://acmelaptop.com | | | | | | | |
| > | foshiba | | | | | | | | | |
| | Home Contact Log in | | | | | | | | | |

Injecting string in URL (Keeping extension as usual)

Register

 \bigcirc ://phpapp.infosecaddicts.com/showfile.php?filename=<script>alert(123);</script> \rightarrow

\PTOP

Script gets executed:

| 123 | |
|-----|----|
| | ОК |

DOM-Based XSS:

Capture desired page in Proxy and Send to Repeater:



In Repeater, Change the "User-Agent" to: <script>alert(123);</script>





Result:

Response

Raw Headers Hex HTML Render

Please enable cookies. Error 1010 Ray ID: 50900937abaa714d • 2019-08-19 23:51:31 UTC

Access denied

What happened?

The owner of this website (phpapp.infosecaddicts.com) has banned your access based on your browser's signature (50900937abaa714d-ua62).

Cloudflare Ray ID: 50900937abaa714d • Your IP: 73.106.77.20 • Performance & security by Cloudflare

It creates an error giving an attacker an idea about the application

Stored XSS:

| cupture desired puge in rieky und send to repeater. |
|---|
| Intercept, HTTP history WebSockets history Options |
| Request to https://phpapp.infosecaddicts.com:443 [104.25.167.6] |
| Forward Drop Intercept is on Action |
| Raw Params Headers Hex |
| GET /showfile.php?filename=contactus.txt HTTP/1.1 |
| Host: phpapp.infosecaddicts.com |
| User-Agent: Nozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:68.0) Gecko/20100101 Firefox/68.0 |
| Accept: text/html,application/xhtml+xml,application/xml;g=0.9,*/*;g=0.8 |
| Accept-Ianguage: en-US,en;g=0.5 |
| Accept-Encoding: gzip, deflate |
| Referer: https://phpapp.infosecaddicts.com/showfile.php?filename=%3Cscript%3Ealert(hackable);%3C/script%3E |
| Connection: close |
| Cockie: _cfduid=6050286555173349558134a0276615454528; _g=Cll.2.78157111.5645421; _g=cl075655488a41551a1a7; _tarksu3d=rinifoseaddics=com:spektrgFredMB08876g8uverPredMB0878520energ=sputskatehz///rizj strip=nd=55268556556256-4204-8fe8-07567bbca7cf; _fbprfb.l15645515380.417041806; _gid=Cll.2.1143145789.1566082711; PHPEDE820=ng1rnslgatabpa71ar6pfe583; _gst=1 |
| Cache-Control max-age=0 |
| |

Capture desired page in Proxy and Send to Repeater:

In Repeater choose the "Params" tab and inject the script: <script>alert(document.domain)</script>:



InfoSecAddicts

| Request | | | | | | | | | |
|------------------------------|------------|---|--------|--|--|--|--|--|--|
| GET request to /showfile.php | | | | | | | | | |
| Туре | Name | Value | bbA | | | | | | |
| URL | filename | <script>alert(document.domain)</script> | | | | | | | |
| Cookie | cfduid | dc6029645e59a793349b3b819dae03f6e | Remove | | | | | | |
| Cookie | _ga | GA1.2.781573113.1564954291 | | | | | | | |
| Cookie | auc | 4e20d75b16c5e988ea135b1a1af | Lin | | | | | | |
| Cookie | tawkuuid | e::infosecaddicts.com::AptkfxgFF6GWh88 | | | | | | | |
| Cookie | stripe_mid | b53f835b-625c-4a04-8fe8-075c7bbca7cf | Down | | | | | | |
| Cookie | _fbp | fb.1.1564955153850.417041806 | Down | | | | | | |
| Cookie | _gid | GA1.2.1143145789.1566082771 | | | | | | | |
| Cookie | PHPSESSID | ng1rns9qe2abpsd71nr6p4c6s3 | | | | | | | |
| Cookie | _gat | 1 | | | | | | | |
| | | | | | | | | | |

Once again we get another error message, however, it gives the attacker information on what to try next:

Response Raw Headers Hex HTML Render

Please enable cookies.

Error 1010 Ray ID: 509016f6bd1bc530 • 2019-08-20 00:00:54 UTC

Access denied

What happened?

The owner of this website (phpapp.infosecaddicts.com) has banned your access based on your browser's signature (509016f6bd1bc530-ua62).

Cloudflare Ray ID: 509016f6bd1bc530 • Your IP: 73.106.77.20 • Performance & security by Cloudflare

4. Insecure Direct Object Reference:

Login to the Application:



| ACMELAPTOP | | 1 | Hey ! Shino | bibughunter Wel-(| Come | |
|------------|--|--|---------------------------|--|--|--|
| ories | Home | Buy | | Career | About us | |
| cer | | Acme is an online webs | ite where you ca | an sell your laptop or se | rvices | |
| ompaq | C | | | | | |
| ell | Cee PC S101 | | | | | |
| ateway | | | | | | |
| ewlett | AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA | | | | | |
| m | | | | | | |
| ony | | - | | | | |
| shiba | Best Featured Products | Best Featured Products | | | | |
| | Acer acer Intel Core2 Du WXGA high-definitio DDR2 SDRA | Jo 2.0GHz / Glossy 15.6" n widescreen display / 2GB | Co Co me RA | mpaq mpaq Intel Core 2 Duo 2 mory / 320GB hard drive M/DVD+R Double Layer | 2.1GHz / 4GB / DVD�RW/DVD- | |
| | dell Little Discriptio given by owner | n about this product as | gat gat sD | teway eway AMD Turion X2 R bile processor 2.0GHz / 3 RAM / Multifo | M-70* dual-core 3GB PC6400 DDR2 | |
| | Hewlett Intel Atom - 1.6GHz videscreen with 102 DDR2 / SSD (Solid 3 | / 10.1" TFT-LCD ¼ x 600 resolution / 1GB S | Ibn Inte 160 Ath | al Celeron 2.16Ghz, 2GB DGB, Vista Home, 15.4" d leros high | RAM, DVD Burner, lisplay / Built-in | |

Capture page in Proxy:

| | Intercept | HTTP history | WebSockets history | Options | | | | |
|---|--|--------------|--------------------|------------|---|---|--|--|
| (| Request to https://phpapp.infosecaddicts.com.443 [104.25.166.6] | | | | | | | |
| l | Forward | | Drop Intercep | ot is on | Action | E | | |
| | Raw Para | ms Headers | Hex | | | | | |
| G | GT /index. | php HTTP/1. | l licha com | | | _ | | |
| υ | aer-Agent: | Nozilla/5. | 0 (Nacintosh; Inte | A Mac OS | x 10.13; rv:68.0) Gecko/20100101 Firefox/68.0 | | | |
| a | scepti tex | t/html,appl: | ication/xhtml+xml, | applicat: | ion/sml;g=0.9,*/*;g=0.8 | | | |
| a | ccept-Lang | uage: en-US, | ,en;q=0.5 | | | | | |
| A | copt-Enco | ding: gzip, | deflate | | | | | |
| R | eferer: ht | tps://phpap | p.infosecaddicts.c | :om/login. | , php | | | |
| C | onnection: | close | | | | | | |
| c | ookie: cfduid=dc6029645e59a793949b3b819dae03f6e1564954288; ga=Gal.2.781573113.1564954291; auc=4e20d75b16c5e988ea135b1a1af; | | | | | | | |
| | <pre>_backsuid=e::infoaecadicts.com::AptktxgFF6GHn86K807g86worktPHsRH+585K8Ed825w0ontFQ+agNTBKX*cBhZ//ii2;</pre> | | | | | | | |
| | fbp=fb.1.1564955153850.417041806; _gid=GA1.2.1143145789.1566082771; PHPSESGID=nglrna9ge2abpad71nr6p4c6a3 | | | | | | | |
| 2 | John Contr | ol. max-ages | -0 | | | | | |
| • | TOUG-COULT | OT' HEV-EGG. | -0 | | | | | |

Send to Intruder:

| Intercept HTTP history WebSockets history Options | | | | | | | | | |
|--|---|--------|---|--|--|--|--|--|--|
| A Request to https://phpapp.infosecaddicts.com.443 [104.25.166.6] Forward Drop | | | | | | | | | |
| Raw Params Headers Hex | Raw Params Headers Hex | | | | | | | | |
| GAT /Inbex.pmp http:/li Nost:phpspp.infossocadiots.com User-Agent: Nozilla/5.0 (Macintosh; In Accept: text/html,application/xhtml*xm; Accept-Languages en-US_engr@.5 Accept-Languages en-US_engr@.5 Accept-text/phpapp.infosecaddiots. Consection close | GER /index.php strF/i.i Nast-phope.infosoeddicts.com Nast-phope.infosoeddicts.com Nast-phope.infosoeddicts.com Nast-phope.infosoeddicts.com Nast-phope.infosoeddicts.com/logis.php | | | | | | | | |
| Cookie:cfduid=dc6029645e59a793349b tawkuuid=e::infosecaddicts.com::Apt | Send to Spider | | .1564954291;auc=4e20d75b16c5e988ea135b1a1af; PO+aoNYENx4cENX//::2:atripe_mid=b53f835b-625c-4a04-8fe8-075c7bbca7cf; | | | | | | |
| fbp=fb.1.1564955153850.417041806; g | Do an active scan | | lrna9ge2abpad7lnr6p4c6a3 | | | | | | |
| Upgrade-Insecure-Requests: 1 Cache-Control: max-age=0 | Send to Intruder | ¥€+^+I | | | | | | | |
| | Send to Repeater | %+^+R | | | | | | | |
| | Send to Sequencer | | | | | | | | |
| Send to Comparer | | | | | | | | | |
| | Send to Decoder | | | | | | | | |
| | Request in browser | • | | | | | | | |
| | Engagement tools [Pro version only] | • | | | | | | | |

In Intruder select attack positions:

| GET /index.php \$4\$ HTTP/1.1 |
|--|
| Host: phpapp.infosecaddicts.com |
| User-Agent: Nozilla/5.0 (Nacintosh; Intel Mac OS X 10.13; rv:68.0) Gecko/20100101 Firefox/68.0 |
| Accept: text/html,application/xhtml+xml,application/xml;g=0.9,*/*;g=0.8 |
| Accept-Language: en-US,en;g=0.5 |
| Accept-Encoding: gzip, deflate |
| Referer: https://phpapp.infosecaddicts.com/login.php |
| Connection: close |
| Cookie:cfduid=dc6029645e59a793949b9b819dae09f6e1564954288; _ga=Ga1.2.781573113.1564954291;auc=4e20d75b16c5e988ea195b1a1af; |
| tawkssid=e::infonecaddicta.com::AptkfxgPP6GWh88K8Tg8EwvskfPHsRU+5E9K8td825wOcntPQ+agNYEWx40EhX//::2;atripe_mid=b53f835b-625c-4a04-8fe8=075c7bbca7cf; |
| _fbp=fb.1.1564955153850.417041806; _gid=gal.2.1143145789.1566082771; PMPsEssID=nglrns9ge2abpad7lnr6p4c6a3; _gat=1 |
| Upgrade-Insecure-Reguests: 1 |
| Cache-Control: max-age=0 |
| |
| |
| |
| |

Go to Payloads and select numbers & Click "Start Attack":



| Payload Sets You can define or defined in the Pos payload type can | te or more payload sets. The number of payload sets depends on the attack type sitions tab. Various payload types are available for each payload set, and each be customized in different ways. |
|---|---|
| Payload set: 1 Payload type No | Payload count: 1,000 mbers Request count: 1,000 |
| Payload Optio This payload type Number range | ns [Numbers] generates numeric payloads within a given range and in a specified format. |
| Type: | Sequential O Random |
| From: | 1 |
| To: | 1000 |
| Step: | 1 |
| How many: | |

You can see results of the attack in a variety of means.

| | | | | | | Intruder a | ttack 3 | | | |
|-------------|----------------------|----------------|----------------------|-------------|------------|------------|----------|----------------------|---------------|-----------|
| Attack Sa | ve Colur | nns | | | | | | | | |
| Results | Target | Positions | Payloads | Options | | | | | | |
| Filter: Sho | wing all it | ems | | | | | | | | ? |
| Request | Payloa | d | | Status | Error | Timeout | Length | Comment | | |
| 84 | 84 | | | 404 | | | 652 | | | |
| 85 | 85 | | | 404 | - | | 652 | | | |
| 86 | 86 | | | 404 | | | 652 | | | |
| 87 | 87 | | | 404 | | | 652 | | | |
| 88 | 88 | | | 404 | | | 652 | | | |
| 89 | 89 | | | 404 | | | 652 | | | |
| 90 | 90 | | | 404 | | | 652 | | | |
| 91 | 91 | | | 404 | | | 652 | | | |
| 92 | 92 | | | 404 | | | 652 | | | |
| 93 | 93 | | | 404 | | | 652 | | | |
| 94 | 94 | | | 404 | | | 652 | | | |
| 95 | 95 | | | 404 | | | 652 | | | |
| 97 | 97 | | | 404 | | | 652 | | | |
| 51 | 51 | | | 404 | | | 052 | | | |
| Request | Respon | ıse | | | | | | | | |
| Raw Pa | arams | Headers H | lex | | | | | | | |
| GET /inde | x.nhn 9 | 6 HTTP/1. | 1 | | | | | | | |
| Hoat: php | app.inf | osecaddic | ta.com | | | | | | | - |
| User-Agen | t: Nozi | 11a/5.0 (t | lacintosh | Intel Na | C OS X 1 | 0.13; rv: | 68.0) Ge | cko/20100101 Firefox | /68.0 | |
| Accept: t | :ext/ntm inquage: | en-US.en | tion/xntm. ta=0.5 | г+хmı,аррі | .1cation/: | xm1;d=0.8 | ,*/*;g=u | | | |
| Accept-En | coding: | gzip, de: | flate | | | | | | | |
| Referer: | https:/ | /phpapp.in | nfoaecadd: | lcta.com/] | .ogin.php | | | | | |
| Cookie: | on: Cloa cfduid | e =dc602964 | 5e59a79334 | 9535819da | e03f6e15 | 64954288: | ga=GA1 | .2.781573113.1564954 | 291: | |
| auc =4 e2 | 0d75b16 | c5e988ea1 | 35blalaf; | | | , | | | | |
| tawkooi | d=e::in | fosecaddid | cta.com::/ | Aptkf xgPP6 | GWh88K8T | g8swvukfP | HURU+589 | KStd825w0cntPQ+agNYB | Xx4cBhX//::2; | ٣ |
| ? | : + |) > T | ype a search | term | | | | | | 0 matches |
| 142 of 100 | 0 | | | | | | | | | |

Looking at the results may require further investigation.



5. Security Misconfiguration:

Go to the "Target" tab and then the site map in Burp:



Select Spider:



InfoSecAddicts

01 Host https://phpapp.infosecaddicts.com D / https://phpapp.infosecaddicts.com/ ▶ 🎒 acre2.php Remove from scope nse authenticate.php Spider this host career.php Hea Actively scan this host cdn-cgi Passively scan this host forgetpassword.p loa, ► 📒 icons Engagement tools [Pro version only] ► g: 🕨 🧮 images Compare site maps 🗋 index.php el Expand branch 🕨 🧮 js i11, Expand requested items ae. 🔻 😫 login.php k∕pι Collapse branch 🕐 error=Invalid-CD= error=Invalid-Delete host 11: error=Session ifo: Copy URLs in this host)f8: transfer=lapto Copy links in this host 🖻 md5.js Save selected items 🕨 🏟 register1.php Show new site map window shop.php Site map help showfile.php Style

You can see the directory of the site.

Choose a directory, in our case we'll choose "images":



Return to the browser and access the directory we selected by adding it to the URL:

https://phpapp.infosecaddicts.com/images/



< → ୯ ŵ

③ ▲ https://phpapp.infosecaddicts.com/images/

Index of /images

| | <u>Name</u> | Last modified | <u>Size</u> | Description |
|----------|------------------|------------------|--------------|-------------|
| | Parent Directory | | - | |
| <u>.</u> | Compaq.jpg | 2018-09-18 16:18 | 19K | |
| 2 | Thumbs.db | 2018-09-18 16:18 | 235K | |
| 5 | a1.jog.jpg | 2018-09-18 16:18 | 16K | |
| 5 | <u>a2.jpg</u> | 2018-09-18 16:18 | 15K | |
| 5 | <u>a3.jpg</u> | 2018-09-18 16:18 | 15K | |
| 5 | a4.jpg | 2018-09-18 16:18 | 10K | |
| 5 | <u>a5.jpg</u> | 2018-09-18 16:18 | 34K | |
| 5 | acer.jpg | 2018-09-18 16:18 | 5.3K | |
| 5 | <u>c1.jpg</u> | 2018-09-18 16:18 | 5.9K | |
| 5 | c2.jpg | 2018-09-18 16:18 | 7.1K | |
| 5 | c3.jpg | 2018-09-18 16:18 | 6.3K | |
| 5 | c4.jpg | 2018-09-18 16:18 | 6.7K | |
| 5 | c5.jpg | 2018-09-18 16:18 | 8.0K | |
| 5 | c6.jpg | 2018-09-18 16:18 | 1 .9K | |
| 5 | <u>d1.jpg</u> | 2018-09-18 16:18 | 6.3K | |
| 5 | <u>d2.jpg</u> | 2018-09-18 16:18 | 6.3K | |
| 5 | d3.jpg | 2018-09-18 16:18 | 2.2K | |
| 5 | d4.jpg | 2018-09-18 16:18 | 1.2K | |

Explore the links inside the directory.

6. Sensitive Data Exposure:

Insecure Processing of Credit Card Data

Select an item you wish to purchase:



Hey ! Shinobibughunter Wel-Come

| Home | Buy | Career | About us | Contact |
|------|-----------------------|-----------|--|--|
| Acer | | | | |
| | acer1 | 🕷 Buy Now | acer Intel Core2 Duo 2.0GHz / C high-definition widescreen displa | Glossy 15.6" WXGA y / 2GB DDR2 SDRA |
| | acer2 | 👬 Buy Now | acer i Intel Pentium M 740 1.73G 60GB hard drive / 14.1-inch XG& | Hz / 512MB DDR2 400 / A TFT LCD / CD- |
| | Home I Contact I Logo | sut i | | |

On the Payment Processing Page, fill out information and submit it:

Buy Career About us Contact BUY Fill buy on Acme Your Total Price 599.99 Your Quatity : 1 Your Name : Shinobibughunter ٢ Type of card: VISA Credit Card no: CVE number: Save information

Hey ! Shinobibughunter Wel-Come

Once you've the form has been submitted go back and attempt buy another item,

You'll see your Credit Card no. has been cached:

| Hey I Shinobibughunter Wel-Come | | | | | | | | |
|---------------------------------|-----|-------------------|----------|---------|--|--|--|--|
| Home | Buy | Career | About us | Contact | | | | |
| BUY | | | | | | | | |
| Fill buy on Acme | | | | | | | | |
| Your Total Price : | | 599.99 | | | | | | |
| Your Quatity : | | 1 | | | | | | |
| Your Name : | | Shinobibughunter | | | | | | |
| Type of card: | | VISA | | | | | | |
| Credit Card no: | | 4 | | | | | | |
| CVE number: | | 44444444444444444 | | | | | | |
| Save information | | | | | | | | |



Right click and choose Inspect element:

| Toshiba | credit card no. | 4 | | | | | |
|--|---|---|--|-------------------------------------|------------------|----------------|--|
| R Debugger | {} Style Editor | rk 🗄 Storage 🕇 Access | sibility 👩 Coo | kie Editor | 1 | 🗆 🗇 … × | |
| L Search HTML | + 1 | | :hov .cls + | Layout | Computed Changes | Fonts Anim - | |
| | | element () { | inline | | | | |
| | Inherited from tr | | Select a Flex container or item to continue. | | | | |
| | Credit Card no: | .contacttable 🗘 { | style.css:36 | ⇒ Grid | | | |
| ▼ | | <pre>font-size: 12px; text-plien; instifut</pre> | | CSS Grid is not in use on this page | | | |
| | <pre><input <="" class="bg_bid" id="credit_card_no" name="credit_card_no" pre="" type="text" value=""/></pre> | <pre>line-height: 15px; font-family: Arial; }</pre> | | - Box Model | | | |
| | size="20"> | | | | | | |
|) tr) td) table table border 5) thedy) tr) | td > form > table table border 4 > thody > tricontacttable > td > | | | margin | 0 | | |
| The state of the s | a rom room room and r | | | borde | 3 0 | | |
| y enter output | Paquata | | | | | Persist Logs X | |
| nora maninga Loga Illo Debug C35 XHR | nequests | | | | | | |

Select the Credit card section and find the name "credit_card_no":



As you can see, there isn't any "Auto-complete off" here and that is why the credit card number is being cached.

So the we have Insecure Processing of Credit Card Data.

7. Missing Function Level Access Control:

Testing for Access Controls:

Login using the lower-privileged account:

| we are we are we are we are addicts | |
|---|--|
| | |

| USERNAME: | test |
|-----------|-------|
| PASSWORD: | ••• |
| | Login |

Locate the area we are testing in Burp's Site map or HTTP history. Right click on the entry to bring up the context menu.

Click "Request in browser", then "In current session".

| Interc | cept | HTTP history | WebSocke | ts histor | y Options | | | | | | | | | |
|-----------|---|----------------------------------|--------------------------|---|----------------------------|--|--------|------------|------------|--------------|------------|------------|------------------------|-------------------|
| | Logging of out-of-scope Proxy traffic is disabled Re-enable | | | | | | | | | | | | | |
| Filter: H | Hiding | CSS, image and | l general bi | nary con | tent | | | | | | | | | |
| # | Host | | | Method | URL | | Para | Edited | Status | Length | MIME type | Extension | Title | Comment |
| 14 15 | https https | ://www.google ://stats.g.doub | -analytic leclick.net | GET GET | /r/collect? /r/collect? | v=1&_v=j78&a=103772 v=1&aip=1&t=dc&_r=3 | 1 | | 302 302 | 1000 977 | HTML | | 302 Moved 302 Moved | |
| 1 | https | ://phpapp.info | secaddic | GET | | | | | 200 | 9850 | HTML | php | Acme laptop | |
| 2 | http: | ://phpapp.info | secaddic | GET | https://phpa | pp.infosecaddicts.com/log | in.php | | 304 | 711 | script | js | | |
| 4 | https | ://ajax.cloudfla | are.com | GET | Remove from | scope | | | 304 | 695 | script | js | | |
| 5 | http: | ://phpapp.into | secaddic | GET | Spider from h | iere | | | 304 | 711 | script | JS | | |
| 13 | https | ://www.googie ://ekr.zdassets | -analytic | GET | Do an active s | can | | | 404 | 904 | text | JS | | |
| | nup. | ,,,, en izoussets | | GLI | Do a passive | scan | | | 101 | 504 | text | com | | |
| | | | | | Send to Intru | der | | 36+^+1 | | | | | | |
| | | | | | Send to Repea | ater | | 30 + ^ + R | | | | | | |
| | | | | | Send to Seque | encer | | | | | | | | |
| | | | | | Send to Comp | oarer (request) | | | | | | | | |
| - | | | | | Send to Comp | oarer (response) | | | - | | | | | , |
| - | | | | _ | Show response | se in browser | | | | | | | | |
| Requ | est [| Response | | | Request in br | owser | | • | In orig | inal session | n | | | |
| Raue | (Part | me Theadore | Her | | Engagement | tools [Pro version only] | | • | In curr | ent session | n | | | |
| Kaw | Para | ins neaders | Hex | | Show new his | tory window | | | | | | | | |
| HOat: 1 | ogin. phpai | php HTTP/L. | l dicta.com | | Add commen | t | | | | | | | | |
| User-A | gent: | Nozilla/5. | 0 (Nacint | osh; | Highlight • | | | | | efox/68.0 | | | | |
| Accept | : te: | ct/html,appl | ication/x | html+: | Delete item | | | | | | | | | |
| Accept | Accept-Language: en-US,en;q=U.5 Accept-Encoding: gzip. deflate | | | | Clear history | | | | | | | | | |
| Refere | r: hi | ttps://phpap | p.infoaec | addic | Copy URL | | | | | | | | | |
| Cookie | ±1000 | fduid=dc602 | 9645e59a7 | 993491 | Copy as curl | command | | | 954291 | : apg =4 | e20d75b16d | 5e988ea195 | blalaf: | |
| tawki | ouid | e::infoseca | dicts.co | m::Ap | Copy links | | | | NYEN 24 | eBhX//::2 | ;atripe | mid=b53f8 | 335b-625c-4a04-8 | fe8-075c7bbca7cf; |
| _fbp=fl | b.1.1 | 156495515385 | 0.4170418 | 06; _ | Save item | | | | ge2abp | ad71nr6p4 | lc6a3 | | | |
| Cache-0 | Conti | col: max-age | =0 | | Proxy history | help | | | | | | | | |
| | | | | the second se | | | | | | | | | | |

The "Request in browser" pop up window allows you to copy the URL of the required Repeat request in browser

| Fo repeat this request in your browser, copy the URL below and pas s configured to use Burp as its proxy. | ste into a browser that |
|--|-------------------------|
| http://burp/repeat/2/mjahpl6c0xdnnprtvio4ht8ycj8e1t97 | Сору |
| In future, just copy the URL and don't show this dialog | Close |

page.

Click the "Copy" button.

Post the URL into the browser to attempt access the individual page we're testing:



Q http://burp/repeat/1/07hypd3chu9c4totqsei43i6zrxnqe2n →
I http://burp/repeat/1/07hypd3chu9c4totqsei43i6zrxnqe2n — Visit

In this case we weren't successful. So it appears the appropriate controls are in place. **Not Found**

he requested URL /repeat/1/07hypd3chu9c4totqsei43i6zrxnqe2n was not found on this server.

pache/2.4.29 (Ubuntu) Server at www.inert.com Port 80

8. Cross-Site Request Forgery (CSRF):

Unable to find Cross-Site Request Forgery Vulnerability in this application

9. Test for Components with Known Vulnerabilities:

Go to the "HTTP history" tab:

| inter | reeper intri instarly incosocia | ets motory | options | | | | | | | | | | | |
|--------|---|------------|-----------------------------------|--------------|--------|--------|--------|-----------|-----------|-----------------------|---------|-----|-----------------|-----|
| | Logging of out-of-scope Proxy traffic is disabled Re-enable | | | | | | | | | | | | | |
| Filter | Filter: Hiding CSS, image and general binary content | | | | | | | | | | | | | |
| # | Host | Method | URL | Para 🔻 | Edited | Status | Length | MIME type | Extension | Title | Comment | SSL | IP | C |
| 33 | https://www.google-analytic | GET | /r/collect?v=1&_v=j78&a=407164 | ~ | | 302 | 1002 | HTML | | 302 Moved | | ~ | 64.233.185.138 | |
| 34 | https://aspdotnetapp.infose | GET | /bookdetail.aspx?id=1 | \checkmark | | 200 | 12948 | HTML | aspx | Book Detail Page | | ~ | 104.25.167.6 | |
| 35 | https://aspdotnetapp.infose | GET | /BasicSearch.aspx?Word= | 1 | | 200 | 16470 | HTML | aspx | Basic Search Page | | ~ | 104.25.166.6 | |
| 63 | https://aspdotnetapp.infose | GET | /BasicSearch.aspx?Word= | ~ | ~ | 403 | 3622 | HTML | aspx | Access denied aspdo | | ~ | 104.25.166.6 | |
| 64 | https://clients4.google.com | POST | /invalidation/lcs/request | \checkmark | | 204 | 321 | | | | | ~ | 173.194.219.102 | s / |
| 65 | https://play.google.com | POST | /log?format=json&hasfast=true&u | \checkmark | | 200 | 767 | JSON | | | | ~ | 172.217.10.174 | S |
| 66 | https://0.client-channel.goo | GET | /client-channel/channel/bind?ctyp | \checkmark | | 400 | 715 | HTML | | Unknown SID | | ~ | 64.233.177.189 | S |
| 68 | https://play.google.com | POST | /log?format=json&hasfast=true | \checkmark | | 200 | 929 | JSON | | | | ~ | 172.217.10.174 | N |
| 69 | https://play.google.com | POST | /log?format=json&hasfast=true&a | \checkmark | | 200 | 763 | JSON | | | | ~ | 172.217.10.174 | S |
| 70 | https://0.client-channel.goo | GET | /client-channel/channel/bind?ctyp | \checkmark | | 400 | 715 | HTML | | Unknown SID | | ~ | 64.233.177.189 | S |
| 77 | https://0.client-channel.goo | GET | /client-channel/channel/bind?ctyp | \checkmark | | 400 | 715 | HTML | | Unknown SID | | ~ | 64.233.177.189 | S |
| 79 | https://0.client-channel.goo | GET | /client-channel/channel/cbp?ctype | \checkmark | | 200 | 599 | JSON | | | | ~ | 64.233.177.189 | S |
| 83 | https://0.client-channel.goo | GET | /client-channel/channel/cbp?ctype | \checkmark | | 200 | 599 | JSON | | | | ~ | 64.233.177.189 | S 🖕 |
| 191 | https://www.google-analytic | CET | /r/collect?v=18. v=i788.a=151677 | ./ | | 303 | 1002 | HTM | | 302 Moved | , | ./ | 64 233 185 130 | 1.0 |
| - | | | | | | | | | | | | | | 7. |

Once you select an item, click on the "Response: tab.



In here you can see information regarding the web server used by the web application.

This information can help with information gathering process.

10.Redirects and Forwards:

After Intercepting our desired page go to spider:



Go to "Site map filter" to search for any redirects or forwards used by the Site map.



| Site | map Scope | | |
|---------|---|--------------------|-------------|
| Filter: | Hiding out of scope, unrequested and no | n-parameterized it | ems |
| ? | Filter by request type | Filter by MIME ty | /pe |
| 10 | Show only in-scope items | HTML | 🗹 Other te |
| 0 | Show only requested items | Script | ✓ Images |
| | Show only parameterized requests | XML | ✓ Flash |
| | Hide not-found items | CSS | 🗹 Other b |
| | Filter by search term | Filter by file e | xtension |
| | | Show onl | y: asp,aspx |
| | Regex | | |

We can "Filter by status code":

In this case we are searching for the "3xx" class of status codes. These status codes indicate that further action has to be taken by the user agent to fulfil a request.

| Target | Proxy Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project op | |
|-------------|---|--|------------------------|--------------|--|--|----------------------------------|---|--------------------------------|--|
| Site map | Scope | | | | | | | | | |
| Filter: Hid | ing out of scope | , unreques | sted and no | n-paramet | erized items | ; hiding 2x | x, 4xx and 5 | xx response | 15 | |
| | ter by request ty Show only in- Show only req Show only par Hide not-foun | pe scope iten uested iter ameterizer d items | ns ms d requests | Filter by | / MIME type ML √ ipt √ L √ S √ | Other text Images Flash Other binan | Filter b 2x 3x 4x 5x | y status cod x [success] x [redirecti x [request e x [server er | te Fo on] error] ror] | |
| Fil | ter by search ter | m | | Filter | by file exte | nsion | | Fil | ter by anno | |
| 8 | Regex Case sensitive Negative search | | | B Show only: | | asp,aspx,jsp js,gif,jpg,pn | .php g,css | | Show only | |

The "Site map" table should now only show HTTP requests of the "3xx" class.

You can now manually step through these requests to look for "interesting" URLs. These include any items in which the redirection target appears to be specified within a request parameter.



e

e/e are we are

are

are

everywhere

attackers defenders addicts

Send any HTTP requests that you want to investigate further to the "Repeater" tab.

| Filter: Hiding out of scope, unrequested and non-paran | neterized items; hiding 2xx, 4 | xx and 5 | <x responses<="" th=""><th></th><th></th><th></th><th></th></x> | | | | |
|--|--|----------|---|-----------|-----------------|------------------------|------------------------------------|
| https://phpapp.infosecaddicts.com | Host | Method | URL | Params | Status 🔺 Length | MIME type | Title |
| authenticate.php | https://phpapp.infose | POST | /authenticate.php | 1 | 302 576 | | |
| ▶ bome | https://phpapp.infose | POST | POST: response=&us | ername= | | | |
| icons | nttps://pnpapp.intose | POST | Remove from scope | | | | |
| images 🗧 | | | Spider from here | | | | |
| js | | | Do an active scan | | | | |
| ► Style | | | Do a passive scan | | | | |
| - septe | • | _ | Send to Intruder | | ೫+^+I | | |
| | | | Send to Repeater | | ≋+^+R | | |
| | Request Response | | Send to Sequencer | | | | |
| | Baux Bauana Haada | | Send to Comparer (re | quest) | | | |
| | Raw Faranis Heade | ers ne. | Send to Comparer (re | sponse) | | | |
| | POST /authenticate.p Hoat: phpapp.infoaec | addicts | Snow response in bro | wser | | | |
| | Accept-Encoding: gzi | p, defl | Request in browser | | | | |
| | Accept: */* Accept-Language: en | - | Engagement tools (Pr | o version | oniyj 🕨 | | |
| | User-Agent: Nozilla/ | 5.0 (00 | Compare site maps | | | 64; Trident/ | 5.0) |
| | Connection: close Referer: https://php | app.inf | Highlight | | | | |
| | Content-Type: applic | ation/s | Delete item | | - | | |
| | Content-Length: 19 Cookie: cfduid=dc6 | 0296454 | Conv LIRI | | .781573113.1 | 564954291; apg =4 e20c | |
| | _tawkssid=e::infoae | caddict | Copy as curl comman | d | td 825w0cn tPC | +agNYEWx4cBhX//::2; | |
| | atripe_mid=b53f835 PMPSESSID=nclrna9ce2 | b-625c- | Copy links | | | 850.41704180 | <pre>(6; _gid=Ga1.2.1143145)</pre> |
| | | | Save item | | | | |
| | reaponae=&uaername= | | Show new site map wi | ndow | | - | |
| | | ł | Site map help | | | - | |
| | | | and map | | | | |

On the "Repeater" tab, Click "Go" to check that the redirect occurs:



| Co Cancel > * Follow redirection |
|---|
| Request |
| Raw Params Headers Hex |
| POST /authenticate.php HTTP/1.1 |
| Host: phpapp.infosecaddicts.com |
| Accept-Encoding: gzip, deflate |
| Accept: */* |
| Accept-Language: en |
| User-Agent: Nozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; |
| x64; Trident/S.Uj |
| Commerce bit close |
| Conterf mttps://phpapp.in/caseadorets.com/rogin.php |
| Content-Ispe. approaction, x-www-rorm-bilencoded |
| Cookie: cfduid=dc6029645e59a793349b3b819dae03f6e1564954288; |
| ga=GA1.2.781573113.1564954291; auc=4e20d75b16c5e988ea135b1a1af; |
| tawkuuid=e::infosecaddicts.com::AptkfxoPP6GWh88K8To88wvukfPHuRU+589K8td |
| 825w0cntPQ+sqNYEMx4cBhX//::2; |
| atripe mid=b53f835b-625c-4a04-8fe8-075c7bbca7cf; |
| fbp=fb.1.1564955153850.417041806; gid=GA1.2.1143145789.1566082771; |
| PHPSESSID=nglrna9ge2abpad7lnr6p4c6a3 |
| response=&username= |
| |
| |
| |
| |

We get taken to here:

| Re Ra | sponse aw Headers Hex HTM | ML Render | | | | |
|----------|------------------------------|-----------|--------------|--------|----------------------------|-----------|
| | | Reg | gister | | | |
| Ca | tegories | Home | Buy | Career | About us | Contact |
| > | Acer | | | | | |
| > | Compaq | USERNAME: | | | | |
| > | Dell | | | | | |
| > | Gateway | PASSWORD: | | | | |
| > | Hewlett | | | | | |
| > | lbm | | Login | | | |
| > | Sony | | | No Us | ser found, please <u>r</u> | egister . |
| > | Toshiba | | | | | |
| | | Ho | me Contact | Log in | | |

So a Re-direction doesn't happen here.

