Tools that Attackers use:

Nmap

```
"GET /nice%20ports%2C/Tri%6Eity.txt%2ebak HTTP/1.0" 200 1924 "-" "-"
"POST / HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
"PROPFIND / HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
"PROPFIND / HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
"GET /.git/HEAD HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.ht
"POST /sdk HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
"GET /nmaplowercheck1618132114 HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.
"PROPFIND / HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
"GET /NmapUpperCheck1618132114 HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.
"GET /Nmap/folder/check1618132114 HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nm
"POST / HTTP/1.1" 200 1924 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
"GET /rest/admin/application-configuration HTTP/1.1" 200 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; r
"GET /rest/admin/application-version HTTP/1.1" 200 20 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.
"GET /rest/admin/application-configuration HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; r
"GET /rest/admin/application-version HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0
"GET /rest/admin/application-configuration HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; r
"GET /rest/admin/application-configuration HTTP/1.1" 200 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; r
"GET /rest/languages HTTP/1.1" 200 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
"GET /api/Challenges/?name=Score%20Board HTTP/1.1" 200 598 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; r
"GET /api/Challenges/?name=Score%20Board HTTP/1.1" 200 598 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; r
"GET /rest/products/search?q= HTTP/1.1" 200 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko
"GET /api/Quantitys/ HTTP/1.1" 200 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
"PUT /rest/continue-code/apply/6R8YrZYgwj1y2qMBPWQmEK8knv0pPT9iXp07Le4pO1RxXzbao3DV5J69NbXr HTTP/1.1" 200 50 "http:/
"GET /rest/user/whoami HTTP/1.1" 200 11 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100
"GET /rest/products/1/reviews HTTP/1.1" 200 172 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gec
"GET /rest/products/1/reviews HTTP/1.1" 200 172 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gec
"GET /rest/products/1/reviews HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko
"GET /rest/user/whoami HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/201001
"GET /rest/products/24/reviews HTTP/1.1" 200 30 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gec
"GET /rest/products/24/reviews HTTP/1.1" 200 30 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gec
"GET /rest/user/whoami HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/201001
"GET /rest/products/6/reviews HTTP/1.1" 200 170 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gec
"GET /rest/products/6/reviews HTTP/1.1" 200 170 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gec
"GET /rest/products/6/reviews HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko
"GET /rest/user/whoami HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/201001
"GET /rest/products/42/reviews HTTP/1.1" 200 413 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Ge
"GET /rest/products/42/reviews HTTP/1.1" 200 413 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Ge
"GET /rest/products/42/reviews HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Geck
"GET /rest/user/whoami HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/201001
"GET /rest/products/3/reviews HTTP/1.1" 200 185 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gec
"GET /rest/products/3/reviews HTTP/1.1" 200 185 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gec
```

Hydra

```
00] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
00] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
00] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
00] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
00] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
00] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
00] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
00] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
00] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
00] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
00] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
00] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
00] "GET /rest/user/login HTTP/1.0" 500 - "-" "Mozilla/5.0 (Hydra)"
00] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
00] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
00] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
00] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
00] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
00] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
00] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
00] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
00] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
00] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
00] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
00] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
00] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
00] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
00] "POST /rest/user/login HTTP/1.0" 401 26 "-" "Mozilla/5.0 (Hydra)"
```

Curl

```
"GET /api/Addresss HTTP/1.1" 200 275 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /api/Addresss/3 HTTP/1.1" 200 273 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/user/whoami HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/basket/1 HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/admin/application-configuration HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/deluxe-membership HTTP/1.1" 400 72 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/saveLoginIp HTTP/1.1" 200 347 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/products/search?q= HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /api/Quantitys/ HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/admin/application-configuration HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/user/whoami HTTP/1.1" 200 11 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/user/whoami HTTP/1.1" 200 11 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"POST /rest/user/login HTTP/1.1" 500 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/user/whoami HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/user/whoami HTTP/1.1" 200 11 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"POST /rest/user/login HTTP/1.1" 500 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/user/whoami HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/user/whoami HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"POST /rest/user/login HTTP/1.1" 500 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/user/whoami HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/user/whoami HTTP/1.1" 200 11 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"POST /rest/user/login HTTP/1.1" 500 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/user/whoami HTTP/1.1" 200 11 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/user/whoami HTTP/1.1" 200 11 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"POST /rest/user/login HTTP/1.1" 500 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/user/whoami HTTP/1.1" 200 11 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/user/whoami HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"POST /rest/user/login HTTP/1.1" 500 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/user/whoami HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/user/whoami HTTP/1.1" 200 11 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"POST /rest/user/login HTTP/1.1" 500 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/user/whoami HTTP/1.1" 304 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"GET /rest/user/whoami HTTP/1.1" 200 11 "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
"POST /rest/user/login HTTP/1.1" 500 - "http://192.168.10.4/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
```

SQLMap

```
oducts/search?q=1&QKqc=7074%20AND%201%3D1%20UNION%20ALL%20SELECT%201%2CNULL%2C%27%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E%27
oducts/search?q=1 HTTP/1.1" 200 - "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
oducts/search?q=6813 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
oducts/search?q=1.%22%27%28%2C.%2C%29%2C. HTTP/1.1" 500 - "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
oducts/search?q=5076-5075 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
oducts/search?q=1.9xqhL HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
oducts/search?q=1%27cjocta%3C%27%22%3ETuFsMe HTTP/1.1" 500 - "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
oducts/search?q=1%29%20AND%203747%3D9627%20AND%20%288054%3D8054 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
oducts/search?q=1%29%20AND%209700%3D9700%20AND%20%283503%3D3503 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
oducts/search?q=1%20AND%206384%3D1910 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
oducts/search?q=1%20AND%209700%3D9700 HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
oducts/search?q=1%20AND%206826%3D9654--%20qXOs HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
oducts/search?q=1%20AND%209700%3D9700--%20jEIr HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)"
oducts/search?q=1%27%29%20AND%208657%3D9050%20AND%20%28%27Hvrp%27%3D%27Hvrp HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlma
oducts/search?q=1%27%29%20AND%209700%3D9700%20AND%20%28%27IYGA%27%3D%27IYGA HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlma
oducts/search?q=1%27%20AND%203798%3D2857%20AND%20%27fSuk%27%3D%27fSuk HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)
oducts/search?q=1%27%20AND%209700%3D9700%20AND%20%27IyBx%27%3D%27IyBx HTTP/1.1" 200 30 "-" "sqlmap/1.5.2#stable (http://sqlmap.org)
oducts/search?q=%28SELECT%20%28CASE%20WHEN%20%288195%3D8761%29%20THEN%201%20ELSE%20%28SELECT%208761%20UNION%20SELECT%203788%29%20EN
oducts/search?q=%28SELECT%20%28CASE%20WHEN%20%285972%3D5972%29%20THEN%201%20ELSE%20%28SELECT%208493%20UNION%20SELECT%202338%29%20EN
oducts/search?q=1%29%20AND%20EXTRACTVALUE%287542%2CCONCAT%280x5c%2C0x717a6b7171%2C%28SELECT%20%28ELT%287542%3D7542%2C1%29%29%29%2C0
oducts/search?q=1%20AND%20EXTRACTVALUE%287542%2CCONCAT%280x5c%2C0x717a6b7171%2C%28SELECT%20%28ELT%287542%3D7542%2C1%29%29%29%2C0x71
oducts/search?q=1%20AND%20EXTRACTVALUE%287542%2CCONCAT%280x5c%2C0x717a6b7171%2C%28SELECT%20%28ELT%287542%3D7542%2C1%29%29%29%2C0x71
oducts/search?q=1%27%29%20AND%20EXTRACTVALUE%287542%2CCONCAT%280x5c%2C0x717a6b7171%2C%28SELECT%20%28ELT%287542%3D7542%2C1%29%29%29%
oducts/search?q=1%27%20AND%20EXTRACTVALUE%287542%2CCONCAT%280x5c%2C0x717a6b7171%2C%28SELECT%20%28ELT%287542%3D7542%2C1%29%29%29%2C0
oducts/search?q=1%29%20AND%205895%3DCAST%28%28CHR%28113%29%7C%7CCHR%28122%29%7C%7CCHR%28107%29%7C%7CCHR%28113%29%7C%7CCHR%28113%29%
oducts/search?q=1%20AND%205895%3DCAST%28%28CHR%28113%29%7C%7CCHR%28122%29%7C%7CCHR%28107%29%7C%7CCHR%28113%29%7C%7CCHR%28113%29%29%
oducts/search?q=1%20AND%205895%3DCAST%28%28CHR%28113%29%7C%7CCHR%28122%29%7C%7CCHR%28107%29%7C%7CCHR%28113%29%7C%7CCHR%28113%29%
oducts/search?q=1%27%29%20AND%205895%3DCAST%28%28CHR%28113%29%7C%7CCHR%28122%29%7C%7CCHR%28107%29%7C%7CCHR%28113%29%7C%7CCHR%28113%
oducts/search?q=1%27%20AND%205895%3DCAST%28%28CHR%28113%29%7C%7CCHR%28122%29%7C%7CCHR%28107%29%7C%7CCHR%28113%29%7C%7CCHR%28113%29%
```

Foxbuster

```
ff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /administartion HTTP/1.1" 200 1924 "-" "feroxbuster/2.2.1"
ff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /login HTTP/1.1" 200 1924 "-" "feroxbuster/2.2.1"
ff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /admin HTTP/1.1" 200 1924 "-" "feroxbuster/2.2.1"
ff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /backup HTTP/1.1" 200 1924 "-" "feroxbuster/2.2.1"
ff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /promotion HTTP/1.1" 200 6586 "-" "feroxbuster/2.2.1"
ff:192.168.10.5 - - [11/Apr/2021:09:34:33 +0000] "GET /ftp HTTP/1.1" 200 4852 "-" "feroxbuster/2.2.1"
ff:192.168.10.5 - - [11/Apr/2021:09:34:40 +0000] "GET /ftp/www-data.bak HTTP/1.1" 403 300 "-" "Mozilla/5.0 (X11; Linux
```

Vulnerable endpoint to Brute-Force

- **/rest/user/login**

Vulnerable endpoint to SQL-Injection

- **/rest/products/search**

Parameter that was used to SQL Injection

- **“q”**

Endpoint that attacker try to use to retrieve files

- **/ftp**

Section of website that attacker use

- **product reviews**

Timestamp of successful login

- **11/Apr/2021:09:16:31 +0000**

Information that attacker was able to retrieve from vulnerable endpoint

- **email**
- **password**

File that try to download

- **coupons_2013.md.bak**
- **www-data.bak**

Service and Account that were used to retrieve files

- **ftp**
- **anonymous**

Service and username that were used to gain shell access to server

- **ssh**
- **www-data**