Digital ESSAY

# 「セッションのセッション」

坂口 裕靖

「クマすごいですね」「お、おう … まあ凄いけど … 開口一番また言う？」「もう冬じゃないですか。今シーズン最初で最大の降雪とかあったタイミングで、まだクマ出てますよ。冬眠しないんすかね？」「さあ … クマに聞いてみて欲しいかな」「聞いてみると言えば ai ですかね」「ん？ … そっち行く？」「はい。こないだ、試しにログインしてるかどうか確認するコードを作らせてみたんですよ」「ふーん。それってさ、割と決まりきってるんじゃないの？」「まあそうです。最初出してきたのはフツーの、なんのひねりもない 30 行のコードでした」「だよね。そんなに工夫するところないんじゃないの？」「まあそうなんですけど。それで、試しに叩いてみたんですよ。これってどういう脆弱性があるの？対策しないの？って」「ふむ。サンプルコード的なやつなら、それこそ穴だらけだろうね」「そうなんです。そうしたらセッション ID の再生成、セッションハイジャック対策、クロスサイトスクリプティング対策、認証の信頼性対策をした、82 行のコードになりました」「3 倍弱か。まあでも基本的なところは抑えてる感じかな？」「そうですね。セッションハイジャック対策として、ユーザーの IP アドレスを確認するってなってたんで、なんで？どうして？変わること考えられないの？とか指摘しました」「… そこまで攻めるの？」「いや、相手機械ですから。ワタシ、鉄腕アトムのロボットヘイターに近いです、心情的に」「うーん、まあ確かに機械だしプログラムだし … まあいいか」「いいんです。機械が痛みを知るようになったら考えます。とにかく、IP が同一であるという仮定を外したコードとして、ユーザーの user agent が全く同一文字列であることを確認するコードを出してきました。71 行と、ちょっと短くなってます」「ふむ。違うマシンからのアクセスではないことを確認するってこと？」「聞いたらそう言ってました。そんで他に改良するところないの？って聞いたら、いくつか必要なセキュリティパラメータがあるから教えろとか言ってきます」「おお、やる気あるね」「そんでもって、非活動タイムアウト時間、セッション絶対有効期限、データベース確認頻度、タイムアウトのリダイレクト先を教えろとのことで、まあ一応教えました」「… なんで一応？」「だってここいらへん、必要なら実際の値じゃなくて定数とかで定義すりゃいい話じゃないですか。機械だからわからんのでしょうなぁ」「お、人類の傲慢さ …」「とにかく、それで出てきたコードが 137 行でした」「倍になったね。なかなか頑張るね」「はい。それで、もっと改良できないか詰めてみました」「さすがロボットヘイター …」「そうしたらセッション再生成を頻繁に行うこと、user agent チェックの緩和という 2 点があがってきました」「なるほど？」「前者はまあ攻撃者に提供する時間を短くすることというわけですが、後者については、セッション途中でブラウザがアップデートしたりなんだりを回避するためだとか」「… そんなことある？」「まあ、実際にクロームが適当なタイミングでアップデートするの、無くはないですが …」「エッジケースだよねぇ」「エッジケースと言えば、セッション ID を更新した瞬間に複数のアクセスが発生した場合どうなる

One Point BUZZ WORD

## 20℃

洗濯洗剤としてジェルボールを使っているのですが、これ、冬の水温だとどうしても溶け残るという問題があります。まあアリエール様もいろいろと手を尽くしてくださっているのだろうとは思いますが、冬の溶け残り問題はまだ解決してませんな。溶け残りがどうなるかというと、ベッタベタなドロドロが服にくっついて残ったりという形になり、そのまま干すと悲惨な状態になるわけです。どうもジェルボールの外皮である、なんか寒天みたいなやつが溶けきれなくて残る感じなんですよね。特に青いやつは、見た目が打ち上げられたカツオノエボシみたいですわ。ぶよぶよ感といい、ブルー具合といい。春から秋の間は特に問題にならないんですけど、秋の終わりから春のはじめまでの水が冷たい期間、溶け残るように思います。とりあえずの対策としては、要するに水温が低いのが原因なわけですから、水温を上げてやればいいわけです。幸い今使っている洗濯機には温水洗浄モードがあるので、これを活用しています。具体的に今までの実績では、水温を 20℃以上に設定すると、さすがに溶け残りはないようです。ただ、そのかわりに運転時間が長くなるという問題があります。まあ 20℃はそこまで長くならないのですが、温度を上げるほど長い時間がかかるようになります。マニュアルによれば、12 kg の洗濯が 20℃モードでは 45 分なのに対し、60℃で運転すると 3 時間 25 分かかるようです。205 分ですから、20℃の 4.6 倍ぐらい時間がかかるわけですね。温度を上げない、フツーの洗濯だと大体 30 分ぐらいなので、50% のオーバーヘッドで溶け残りを回避できる感じでしょうか。運転中のどこに時間がかかってるかはよくわかりませんが、設定温度とかかる時間の相関が高そうなので、おそらくは洗濯に使う水の温度を上げる時間がかかるんじゃないでしょうか。12kg だと 72 リットルぐらい使うようだから、まあそれなりに大変そうではありますが。

のか、という問題があるじゃないですかー」「... あるんだ」「あるんですよ。同時に２本アクセスが発生したとして、最初に到達した方でセッション ID が更新されて、二番目のアクセスは古いセッション ID を抱えてきますから、セッション情報が食い違うわけです。と思ってエッジケースを検討して対策しろって命じました」「... 人類の傲慢 ...」「そうしたら、ダブルセッション ID 方式を提案してきました」「なにそれ？」「結局複数のアクセスが同時に発生し、その最初のアクセスでセッション ID が更新されちゃうのが問題なわけです。これら複数のアクセスはほんの短い時間に到達するわけですから、その間だけ、古いセッション ID に紐づくデータを取得できれば、セッション ID を更新するタイミングでの問題は回避できる、そのためには更新する前のセッション ID を保存しておいて、そっちからも読めるようにしておき、短い一定時間後に古いセッション ID を捨てれば良い、ということですね」「へー ...」「ちなみに、５分ごとに更新するとして、このエッジケースが発生する確率を見積もれ、と言ってみました」「あー。まあ、確率をお客さんから聞かれるってよくあるよね」「ai も当然、厳密な値はわかりませんとか前置きしつつ、競合期間を 200ms として、リクエスト頻度が 300 秒だとすれば、発生確率は 0.2/300=0.00067 と言ってきました」「ほほう。コンピューターらしくて、いいね！」「はいー。しかも大規模なアクセスがあると途端に顕在化するとかの指摘もありました」「ウッキウキじゃないの ...」「はいー。でまあ、このダブルセッション ID を組み込んだソース作れって言ったら、129 行のソースを出してきました」「あれ？短くなってない？」「そうなんですよ。よく見たら、そのダブルセッション ID は複雑だからパス、とか言いやがる」「やがるって ...」「しかも、user agent のチェック緩和は頭 30 文字を比較するコードになって て、コメントで『実際の実装では、ブラウザ名と OS 名のみを抽出し比較することが多い』とか抜かしやがる」「抜かすって ...」「ちょくちょく手を抜くんで侮れんですよ。だから、ダブルセッション ID と、ブラウザ名と OS 名を抽出したバージョンを作れって言ったんです」「要求してばかりだね」「いやいや、さっきパラメータ聞かれたじゃないですか。双方向っすよ」「ん、まあ ... そうか」「でまあ、そうやって出てきたコードが 156 行」「ふーん。意外と増えないんだね」「そう思うでしょ？でもね、『全体のコードは非常に長くなるため抜粋』とか言って、色々手を抜きやがるんですよ」「まあ、合理的では？」「そうなんですけど、やっぱ動くコードがほしいじゃないですか」「まあね。機械にやらせてるわけだし」「だから、省略しないでコード出せっつったんです」「そしたら？」「出して来ました。省略なしとは言いつつ、セッション情報の読み書きする部分はスケルトンですが、それでも全体で 266 行」「ほう。最初の 30 行から７倍ぐらいに膨れたんだね」「そうなりますね。ちなみにこの出してきたコードで、なんか外部ソースを丸パクしたところあったら何をパクったか教えろ、って言ったら」「そういうこと言うの？」「いいますよー。だって、著作権問題とかあったらやじゃないですか。また、参照不可なソースだと困るし」「まあそうか」「そしたら、何一つパクってません！ドキュメントのサンプルコードと似てるけど、パクってないもん！と」「... そんな感情的になる？」「なりません。脚色しました」「... だよね」「って感じでした。何ていうか、こう ... 叩けば叩くほど味が出てくる感じ？つーか、最初からそれ出せよ、とも思うわけですが」「まあねぇ。ジャブの応酬しないと難しいところはあるんじゃないの」「わかります。でもこれ、確実に言えるのは GIGO ってやつですね」「ジゴ？なにそれ、ガシャポンのアレ？あ、Back to the Future のやつ？」「んー、それが語源かどうかわからないですけど、Garbage In, Garbage Out ってやつですよ」「あー ... 聞いたことある」「ゴミをいれたらゴミしか出てこないってことです。正しい道筋で聞いてもちゃんとしたものが出てくるかどうかわからない以上、やっぱり読む能力は求められる気がしますね」「まあねー。旋盤のハンドル回せば削れるけど、欲しい形になるとは限らないもんね」「あ、いいですねそれ。まさにその通りです」「ふーん。それでどうなの？使えそう？」「ま、機械は使い潰してなんぼですから」「す、スパルタン ...」

**Hiroyasu Sakaguchi**
フリー IT エンジニア